IT Governance Institute®

4.0

Deutsche Ausgabe

KPMG

Control Objectives
Management Guidelines
Maturity Models

IT Governance Institute®
Das IT Governance Institute (ITGI) (*www.itgi.org)* wurde 1998 gegründet, um international das Wissen und die Standards in der Ausrichtung und Steuerung von Unternehmens-IT zu verbessern. Effektive IT-Governance hilft dabei, sicherzustellen, dass die IT Geschäftsziele unterstützt, Investitionen in die IT optimiert und angemessenes IT-bezogenes Risiko- und Changemanagement betrieben werden. Das IT-Governance Insitute bietet Forschungsergebnisse, elektronische Ressourcen und Fallstudien an, um Unternehmensführungen und Aufsichtsräten bei der Wahrnehmung der IT-Governance Verantwortlichkeiten hilfreich zu sein.

Disclaimer
IT Governance Institute (the "Owner") has designed and created this publication, titled COBIT® 4.0 (the "Work"), primarily as an educational resource for chief information officers, senior management, IT management and control professionals. The Owner makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, chief information officers, senior management, IT management and control professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Das IT Governance Institute ("Eigentümer") hat diese Publikation mit dem Titel COBIT 4.0 („Werk") primär als Ausbildungsunterlage für Chief Information Officers, Senior Management, IT-Management und Führungspersonen erstellt. Der Eigentümer unterstellt nicht, dass die Verwendung des Werkes positive Ergebnisse gewährleistet. Das Werk sollte nicht als vollständig oder exklusiv bezüglich Informationen, Abläufen, Verifikationen oder Tests verstanden werden. Zur Bestimmung der Korrektheit jeglicher Information, des Ablaufs oder Tests sollen CIO, Senior Management und Führungspersonen ihr professionelles Urteilsvermögen betreffend die jeweiligen spezifischen Rahmenbedingungen des Systems oder der IT-Umgebung anwenden.

Translation
Translated into German from the English language version of COBIT 4.0 by KPMG Austria (Vienna) with the permission of the IT Governance Institute.
COBIT 4.0 wurde im Original vom IT Governance Institute in englischer Sprache publiziert. Für die Übersetzung in die deutsche Sprache zeichnet KPMG Österreich in Wien verantwortlich. Die exklusive Genehmigung zur Übersetzung wurde vom IT Governance Institute erteilt.
Um sowohl die Lesbarkeit für den deutschsprachigen Raum sicherzustellen, aber auch die Verbindung zum englischen Original nicht zu verlieren, wurde darauf verzichtet, häufig in der IT gebrauchte Ausdrücke zu übersetzen. Demzufolge wurden nicht nur gebräuchliche Anglizismen übernommen, sondern auch die Bezeichnung der Domänen, Prozesse und Control Objectives in der ursprünglichen Fassung belassen. Zur Unterstützung eines besseren Verständnisses wurde bei Bedarf eine deutschsprachige Übersetzung hinzugefügt. Der in früheren deutschsprachigen Versionen von COBIT verwendete Term „Kontrolle" als Übersetzung des englischen „Control" wurde in dieser Ausgabe nicht verwendet. Wenngleich die Übersetzung mit „Kontrolle" nicht grundsätzlich falsch ist, ist sie missverständlich, als dass durch Controls sowohl Maßnahmen zur Vermeidung oder Erkennung und Beseitigung unerwünschter Zustände, als auch Maßnahmen zur Herbeiführung von gewünschten Zuständen verstanden werden; Letzeres wird im üblichen Sprachgebrauch nicht als „Kontrolle" bezeichnet und bildet den Hauptteil der „Objectives". Controls bilden den Oberbegriff der entsprechenden Maßnahmen und Kontrollen.
Zur Sicherstellung einer besseren Lesbarkeit unter gleichzeitiger Berücksichtigung der weiblichen IT-Governance Professionals wurden männliche und weibliche Formen, soweit dies die Lesbarkeit nicht wesentlich beeinflusst, angeführt.

Disclosure

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*
ISBN 1-933284-37-4
COBIT 4.0
Printed in the United States of America

DANKSAGUNGEN

Das IT Governance Institute bedankt sich bei:

Übersetzungsteam
Jimmy Heschl, CISA, CISM, KPMG, Österreich
Markus Gaulke, CISA, CISM, KPMG, Deutschland
Peter R. Bitterli, CISA, Bitterli Consulting, Schweiz

sowie
Simone Eder, Christian Focke, Christian Hofer, Patrick Liegl, Michael Sampl und Garry Tan, KPMG Österreich

Review durch
Peter R. Bitterli, CISA
Michael Schirmbrand, CISA, CISM, CPA

Board of Trustees
Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, International President
Abdul Hamid Bin Abdullah, CISA, CPA, Auditor General's Office, Singapore, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Jean-Louis Leignel, MAGE Conseil, France, Vice President
Lucio Augusto Molina Focazzio, CISA, Colombia, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Bent Poulsen, CISA, CISM, VP Securities Services, Denmark, Vice President
Frank Yam, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi, USA, Trustee
Ronald Saull, CSP, Great-West Life and IMG Financial, Canada, Trustee
Erik Guldentops, CISA, CISM, Belgium, Advisor, IT Governance Institute

ITGI Committee
William C. Boni, CISM, Motorola, USA, Chair
Jean-Louis Leignel, MAGE Conseil, France, Vice Chair
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Tony Hayes, Queensland Health, Australia
Anil Jogani, CISA, FCA, Tally Solutions Limited, UK John W. Lainhart IV, CISA, CISM, IBM, USA
Michael Schirmbrand, CISA, CISM, CPA, KPMG, Austria
Eddy Schuermans, CISA, PricewaterhouseCoopers, Belgium
Ronald Saull, CSP, Great-West Life and IMG Financial, Canada

COBIT Steering Committee
Dan Casciano, CISA, Ernst & Young LLP, USA
Roger Debreceny, Ph.D., FCPA, University of Hawaii, USA
Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgium
Steven De Haes, University of Antwerp Management School, Belgium
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Jimmy Heschl, CISA, CISM, KPMG, Austria
John W. Lainhart IV, CISA, CISM, IBM, USA
Ronald Saull, CSP, Great-West Life and IMG Financial, Canada
Michael Schirmbrand, CISA, CISM, CPA, KPMG, Austria
Eddy Schuermans, CISA, PricewaterhouseCoopers, Belgium
Roger Southgate, CISA, CISM, FCCA, UK
Mark Stanley, CISA, Toyota Financial Services, Canada
Dirk Steuperaert, CISA, PricewaterhouseCoopers

INHALTSVERZEICHNIS

Wir freuen uns über Ihr Feedback zu COBIT 4.0. Verwenden Sie bitte das Formular auf www.heschl.at/cobitfeedback, um uns Ihre Kommentare zu senden.

EXECUTIVE OVERVIEW

EXECUTIVE OVERVIEW

Für viele Unternehmen stellen die Informationen und die unterstützende Technologie den wertvollsten, jedoch zumeist am wenigsten verstandenen Vermögensgegenstand dar. Erfolgreiche Unternehmen erkennen den Nutzen der Informationstechnologie und verwenden sie, um den Stakeholder-Value zu erhöhen. Diese Unternehmen verstehen und managen auch die damit zusammenhängenden Risiken, wie die steigende Anforderung hinsichtlich regulatorischer Compliance und der Abhängigkeit vieler Geschäftsprozesse von der IT.

Der Bedarf für die Sicherstellung des Wertbeitrags der IT, das Management von mit IT zusammenhängenden Risiken und die erhöhten Anforderungen für die Steuerung der Informationen sind wesentliche Elemente der Enterprise Governance. Wertbeitrag, Risiko und Steuerung sind die wesentlichen Bestandteile von IT-Governance.

IT-Governance ist die Verantwortung von Führungskräften und Aufsichtsräten und besteht aus Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die Unternehmens-IT dazu beiträgt, die Organisationsstrategie und -ziele zu erreichen und zu erweitern.

Im Weiteren integriert und institutionalisiert IT-Governance Good Practices, um sicherzustellen, dass die Unternehmens-IT die Unternehmensziele unterstützt. Folglich ermöglicht IT-Governance dem Unternehmen, das volle Potential seiner Informationen auszuschöpfen, dadurch den Nutzen zu maximieren, günstige Gelegenheiten zu realisieren und Wettbewerbsvorteile zu gewinnen. Diese Ergebnisse erfordern ein Framework zur Steuerung der IT, das in das Framework des Committee of Sponsoring Organisations der Treadway Commission (COSO) Internal Control-Integrated Framework, dem akzeptierten Steuerungsframework für Enterprise Governance und Risikomanagement integriert ist und dieses sowie ähnliche Frameworks unterstützt.

Organisationen sollen den Anforderungen an Qualität, an Fürsorgepflicht (engl.: *fiduciary requirements*) und Sicherheit der Informationen sowie für alle Unternehmenswerte gerecht werden. Das Management soll gleichzeitig die Verwendung von IT-Ressourcen (inklusive Anwendungen, Information, Infrastruktur, Personal) optimieren. Zur Erfüllung dieser Verantwortung, sowie zur Sicherstellung der Zielerreichung, sollte das Management den Status der unternehmensweiten IT-Architektur verstehen und entscheiden, welche Governance und Steuerungsmöglichkeiten angewandt werden sollen.

Control Objectives for Information and related Technology (COBIT®) stellt Good Practices in Form eines Domänen- und Prozess-Frameworks zur Verfügung und enthält Aktivitäten in einer handhabbaren und logischen Struktur. Die Good Practices von COBIT beinhalten die Sichtweise unterschiedlicher Experten, welche einen klaren Steuerungs- und weniger einen Umsetzungsfokus haben. Diese Praktiken unterstützen bei der Verbesserung von Investitionen im Umfeld von IT, sichern die Leistungserbringung und einen Beurteilungsmaßstab, falls Unregelmäßigkeiten auftreten.

Um es der IT zu ermöglichen, erfolgreich die Geschäftsanforderungen zu erfüllen, sollte vom Management ein Internes Kontroll-/Steuerungssystem oder –framework umgesetzt werden. Das COBIT Framework hilft hierbei durch

- eine Verbindung zu den Geschäftsanforderungen,
- die Einbindung von IT-bezogenen Aktivitäten in ein allgemein akzeptiertes Prozessmodell,
- die Identifikation von wesentlichen, zu steuernden IT-Ressourcen und
- die Definition von zu berücksichtigenden Control Objectives.

Die Orientierung von COBIT am Kerngeschäft besteht aus einer Verbindung von Unternehmenszielen zu IT-Zielen, dem Bereitstellen von Messgrößen und Reifegradmodellen, um die Zielerreichung zu messen und aus der Identifikation der jeweiligen Verantwortlichkeiten im Fachbereich und der IT.

Die Prozessorientierung von COBIT wird durch das Prozessmodell dargestellt, welches die IT in 34 Prozesse, untergliedert in Planung, Entwicklung, Betrieb und Monitoring strukturiert, wodurch eine ganzheitliche Sicht auf die IT etabliert wird. Unternehmensweite Architekturmodelle helfen dabei, die wesentlichen Ressourcen für den Prozesserfolg zu identifizieren, zB Anwendungen, Informationen, Infrastruktur und Personal.

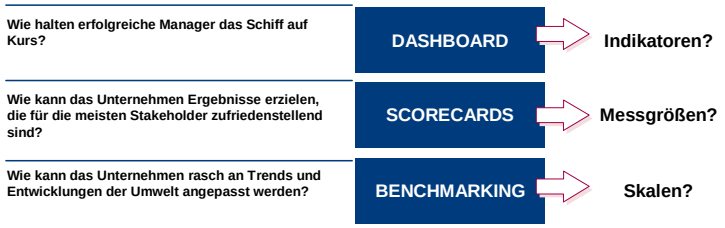
Um die Informationen anbieten zu können, die eine Organisation zur Zielerreichung benötigt, müssen die IT-Ressourcen durch eine Reihe von natürlich gruppierten Prozessen verwaltet werden.

Aber wie kann ein Unternehmen seine IT steuern, so dass sie die benötigten Informationen bereitstellt? Wie werden die Risiken gemanagt und wie können die IT-Ressourcen abgesichert werden, von denen die Organisation so abhängig ist? Wie kann das Unternehmen sicherstellen, dass die IT die Ziele erreicht und das Kerngeschäft unterstützt?

Erstens benötigt das Management Control Objectives, die das eigentliche Ziel der Implementierung von Richtlinien, Praktiken und Verfahren (*engl.: Policies, Practices und Procedures*) sowie der Organisationsstruktur darstellen, um zu gewährleisten, dass

- Unternehmensziele erreicht und
- ungeplante Vorkommnisse verhindert oder entdeckt und korrigiert werden.

Abbildung 1 – Management Information



Zweitens, in den heutigen, komplexen Umgebungen benötigt das Management laufend kompakte und aktuelle Informationen, um schwierige Entscheidungen bezüglich Risiko und Steuerung schnell und erfolgreich treffen zu können. Was soll gemessen werden und wie? Unternehmen benötigen eine objektive Messung zur Beurteilung, wo sie stehen und wo Verbesserungen notwendig sind. Sie müssen Management-Werkzeuge umsetzen, um die Verbesserungen zu überwachen. Abbildung 1 zeigt geläufige Fragen und auch die Managment-Werkzeuge, die üblicherweise verwendet werden, um Antworten zu erhalten. Aber diese Dashboards benötigen Indikatoren, Scorecards benötigen Messgrößen und Benchmarking benötigt Skalen für den Vergleich.

Eine Antwort auf die Anforderung, angemessene IT-Steuerungs- und Performanceniveaus zu bestimmen und zu beurteilen, ist die COBIT-spezifische Definition der folgenden Bereiche:

- **Benchmarking** des Potentials der IT-Prozesse in Form des Reifegradmodells (*engl.: Maturity Model*), das vom Capability Maturity Model des Software Engineering Institute abgeleitet wurde.
- **Ziele und Metriken der IT-Prozesse**, um deren Output und Performance festzulegen und zu messen, wobei auf die Grundlagen der Balanced Business Scorecard von Robert Kaplan und David Norton zurückgegriffen wird.
- **Ziele für Aktivitäten**, um, basierend auf den detaillierten Control Objectives, die Prozesse unter Kontrolle zu bringen.

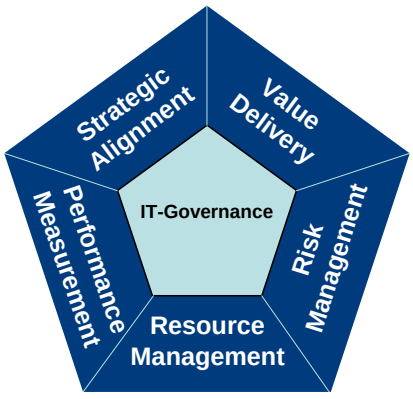
Die Beurteilung des Prozesspotentials auf Basis des COBIT Reifegradmodells ist ein wesentlicher Teil der Umsetzung von IT-Governance. Nachdem kritische IT-Prozesse und IT-Controls identifiziert wurden, ermöglicht es das Reifegradmodell, Lücken im Potential zu identifizieren und gegenüber dem Management aufzuzeigen. Auf dieser Basis können Umsetzungspläne erstellt werden, um die Prozesse auf den gewünschten Zielreifegrad zu bringen.

Folglich unterstützt COBIT IT-Governance durch die Bereitstellung eines Frameworks, welches die folgenden Bereiche sicherstellt:

- IT ist auf das Kerngeschäft ausgerichtet
- IT unterstützt das Geschäft und maximiert den Gewinn
- Mit IT-Ressourcen wird verantwortungsbewusst umgegangen
- IT-Risiken werden angemessen gemanagt

Leistungsmessung ist ein wesentlicher Bestandteil von IT-Governance. Sie wird von COBIT unterstützt und berücksichtigt Festsetzung und laufendes Monitoring von messbaren Zielvorgaben,was IT-Prozesse abliefern müssen (Prozess-Output) und wie die Leistungserbringung erfolgt (Prozess-Potential und Performance). Zahlreiche Umfragen haben aufgezeigt, dass der Mangel an Transparenz von IT-Kosten, Wertbeitrag und Risiken eine der wichtigsten Antriebskräfte für IT-Governance darstellt. Wenngleich auch andere Kernbereiche dazu beitragen, so wird doch Transparenz primär durch Performance-Messung erreicht.

Abbildung 2 – Kernbereiche der IT-Governance



- **Strategic Alignment** (Strategische Ausrichtung) konzentriert sich auf: die Sicherstellung des Verbunds von Unternehmens- und IT-Zielen; auf die Festlegung, Beibehaltung und Validierung des Wertbeitrags; den Abgleich zwischen operativem Betrieb des Unternehmens und jenem der IT
- **Value Delivery** (Schaffen von Werten/Nutzen) beschäftigt sich mit der Realisierung des Wertbeitrags im Leistungszyklus, der Sicherstellung, dass IT den strategisch geplanten Nutzen generiert und konzentriert sich auf die Kostenoptimierung und die Erbringung des intrinsischen Nutzens der IT.
- **Resource Management** (Ressourcenmanagement) kümmert sich um die Optimierung von Investitionen in IT-Ressourcen und ein geregeltes Management derselben. IT-Ressourcen sind Applikationen, Information, Infrastruktur und Personal. Wesentlicher Bestandteil ist auch die Optimierung von Wissen und der Infrastruktur.
- **Risk Management** (Risikomanagement) erfordert eine Risiko-Awareness bei der Unternehmensleitung, ein klares Verständnis über die Risikobereitschaft (*engl: risk appetite*) ein Verständnis für Compliance-Erfordernisse, Transparenz über die für das Unternehmen wichtigsten Risiken und die Integration der Verantwortlichkeit für Risikomanagement in der Organisation.
- **Performance Measurement** (Messen von Performance) verfolgt und überwacht die Umsetzung der Strategie, Umsetzung von Projekten, Verwendung von Ressourcen, Prozessperformance und Leistungserbringung (*engl: Service Delivery*). Es wird beispielsweise eine Balanced Scorecard verwendet, um die Strategie in Aktivitäten zu übersetzen und diese messbar zu machen, die für die Zielerreichung notwendig sind. Die Messung geht hierbei über die Anforderungen des Rechnungswesens hinaus.

Diese Kernbereiche der IT-Governance beschreiben die Themen, die das operative Management bei der Steuerung der IT im Unternehmen berücksichtigen muss. Das operative Management verwendet hierbei Prozesse, um die Aktivitäten zu organisieren und zu managen. COBIT stellt ein generisches Prozessmodell zur Verfügung, das sämtliche, üblicherweise in der IT vorzufindenden Aktivitäten beinhaltet. Dieses Modell ist ein allgemeines Basismodell und sowohl für ManagerInnen der operativen IT, als auch für jene von Kerngeschäftsprozessen verständlich. Das COBIT Prozessmodell wurde auf die Kernbereiche der IT-Governance umgelegt (siehe Anhang II), um eine Verbindung zwischen dem operativen Management der ausführenden Ebene und der Steuerungsebene herzustellen.

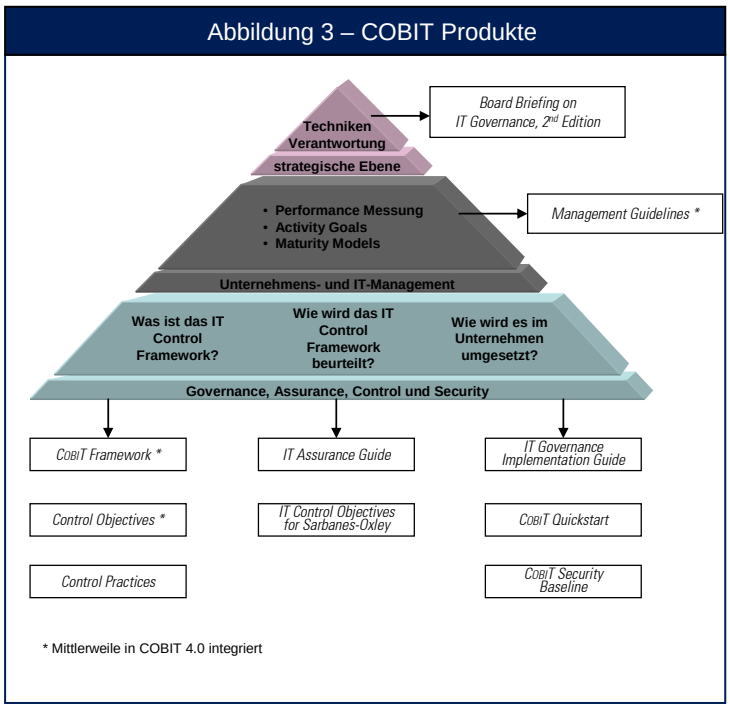
Um effektive Governance erreichen zu können, verlangt die Geschäftsführung, dass vom operativen Management für alle IT-Prozesse Controls auf Basis eines Frameworks festgelegt werden. Die IT Control Objectives von COBIT sind nach IT-Prozessen strukturiert, folglich bietet dieses Framework eine klare Verbindung zwischen den Anforderungen der IT-Governance, den IT-Prozessen und IT-Controls.

COBIT konzentriert sich auf die wesentlichen Erfordernisse, um ein angemessenes Management und eine angemessene Steuerung der IT umzusetzen und ist auf strategischer Ebene angesiedelt. COBIT wurde an andere, detaillierte IT-Standards und Best-Practices (siehe Anhang III) angepasst und mit diesen harmonisiert. COBIT integriert diese unterschiedlichen Standards, in dem die wesentlichen Ziele in einen gemeinsamen Rahmen integriert werden, der auch die Verbindung zur Corporate Governance und den Unternehmenserfordernissen herstellt.

COSO (und andere Frameworks) gilt allgemein als das Framework für ein angemessenes Internal Control System (auch: Internes Kontrollsystem). COBIT ist das allgemein anerkannte Framework für ein angemessenes Internal Control System in der IT.

Die Produkte von COBIT wurden in drei Ebenen gegliedert (siehe Abbildung 3), die die folgenden Bereiche unterstützen:
- Strategische Ebene (Geschäftsführung, Aufsichtsrat, etc)
- Unternehmens- (Linien-) und IT-Management
- Spezialisten der Bereiche Governance, Assurance, Control und Security

Abbildung 3 – COBIT Produkte



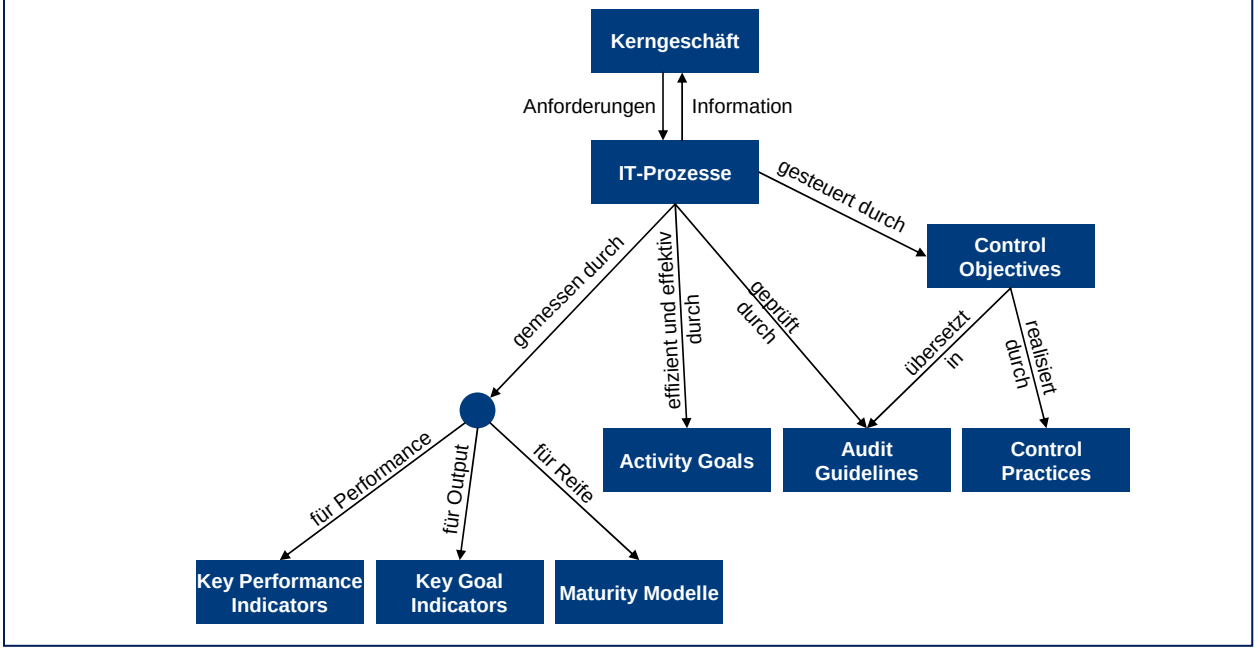
Primäre Publikation für die strategische Ebene ist das
- *Board Briefing on IT-Governance, 2nd Edition*, welches erstellt wurde, um Führungsgremien eine Hilfestellung zu geben, warum IT-Governance von Bedeutung ist, welche Probleme auftreten und welche Rollen die Gremien übernehmen müssen.

Für das Unternehmens- und IT-Management sind die
- *Management Guidelines* wichtig. Sie enthalten Werkzeuge, um Verantwortliche zu benennen, Performance zu messen, Benchmarks durchzuführen und Lücken im Potential aufdecken zu können. Die Management Guidelines geben Antworten auf die typischen Fragen des Managements: Wie weit sollen wir in der Steuerung der IT gehen und sind Kosten und Nutzen ausgewogen? Was sind Indikatoren für eine gute Leistung? Welche Techniken sollen für das Management der IT angewandt werden? Was machen andere? Wie messen wir uns und wie liegen wir im Vergleich?

Für Spezialisten der Bereiche Governance, Assurance, Control und Security:
- *Framework*—Enthält eine Erklärung, wie COBIT die Ziele der IT-Governance nach Best Practices nach IT-Domänen und IT-Prozessen organisiert und mit den Unternehmensanforderungen verbindet.
- *Control Objectives*—Umfassen generische Best Practice Steuerungsvorgaben für sämtliche Aktivitäten und Aufgaben der IT.
- *Control Practices*—Geben eine Anleitung, welche Controls warum und wie zu implementieren sind.
- *IT-Control Objectives for Sarbanes-Oxley*—Enthält eine Anweisung, wie mit den COBIT Control Objectives Compliance hergestellt werden kann.
- *IT-Governance Implementation Guide*—Liefert eine generische Road-Map zur Umsetzung von IT-Governance unter Verwendung der Bestandteile von COBIT.
- *COBIT Quickstart*—Enthält Basis-Controls für kleine Organisationen und einen möglichen Start für größere Unternehmen.
- *COBIT Security Baseline*—Hilft dem Unternehmen, die wesentlichsten Schritte zur Umsetzung von Informationssicherheit im Unternehmen zu tätigen.

Diese Komponenten stehen untereinander in Zusammenhang und liefern eine für die unterschiedlichen Zielgruppen wichtige Unterstützung für Governance, Management, Steuerung und Revision. Eine Übersicht gibt die Abbildung 4.

Abbildung 4 – Zusammenhänge der COBIT Produkte



COBIT ist ein Framework und unterstützendes Werkzeug, das ManagerInnen ermöglicht, die Lücke in Bezug auf die Steuerungserfordernis, technischen Fragestellungen und Unternehmensrisiken zu schließen und den Grad der Control an die Stakeholder zu kommunizieren. COBIT ermöglicht die Entwicklung von klaren Richtlinien und Good Practices für die Steuerung der IT über das gesamte Unternehmen. COBIT wird laufend aktualisiert und mit anderen Standards harmonisiert. Folglich wurde COBIT zum Integrator für IT-Best Practices und das übergeordnete Framework für IT-Governance, das dabei unterstützt, Risiken und Wertbeiträge der IT zu managen. Die Prozessstruktur von COBIT und der übergeordnete, geschäftsorientierte Ansatz ermöglichen eine gesamthafte Betrachtung der IT und der Entscheidungen, die in der IT getroffen werden müssen.

Der Nutzen der Verwendung von COBIT als Framework für IT-Governance ist:

- Verbesserte Ausrichtung, die auf den Unternehmenserfordernissen basiert
- Eine für das Management verständliche Sicht auf Aktivitäten der IT
- Klare, auf Prozessen basierende Zuweisung von Ownership und Verantwortlichkeiten
- Allgemeine Akzeptanz bei Drittparteien und Regulatoren
- Gemeinsames Verständnis bei allen Stakeholdern, das auf einer gemeinsamen Sprache basiert
- Erfüllung der Anforderung von COSO für ein Kontrollsystem über die IT

Auf den nachstehenden Seiten dieses Dokuments finden Sie eine Beschreibung des COBIT Frameworks und aller wesentlichen Bestandteile von COBIT, die nach den IT-Domänen und 34 IT-Prozessen von COBIT gegliedert sind. Dies ergibt eine nützliche Referenz für die hauptsächliche COBIT Ausrichtung. Weitere hilfreiche Informationen sind in den Anhängen enthalten.

Die Umsetzung wird durch einige Produkte von ISACA/ITGI unterstützt, die auch Online-Tools, Umsetzungsanleitungen, Referenzen und Ausbildungsmaterial umfassen. Die neuesten Informationen befinden sich auf *www.isaca.org/cobit.*

Diese Seite wurde absichtlich freigelassen

FRAMEWORK

COBIT FRAMEWORK

DER BEDARF NACH EINEM STEUERUNGS-FRAMEWORK FÜR IT-GOVERNANCE

Warum

Die Geschäftsführung sieht immer mehr den wesentlichen Einfluss von Informationen auf den Unternehmenserfolg. Das Management verlangt ein besseres Verständnis für die Art und Weise, in der Informationstechnologie (IT) betrieben wird und über die Möglichkeit, IT für die Erreichung von Wettbewerbsvorteilen zu nutzen. Genauer gesagt, wollen die leitenden Gremien wissen, ob Informationen durch die Organisation derart gemanagt werden, dass die folgenden Punkte sichergestellt sind:

- Erreichung der Ziele
- Fähigkeit und Flexibilität, um zu lernen und sich zu verändern
- Vernünftiger Umgang mit den relevanten Risiken
- Erkennung und Ergreifung von Chancen

Erfolgreiche Unternehmen verstehen die Risiken,realisieren den Nutzen der IT und erreichen einen Weg, um

- die IT-Strategie der Unternehmensstrategie anzupassen,
- die Strategie und Ziele der IT in der Organisation herunter zu brechen,
- Organisationsstrukturen zu etablieren, welche die Umsetzung von Strategie und Zielen ermöglichen,
- Konstruktive Beziehungen und Kommunikation zwischen Kerngeschäft, IT und externen Partnern zu betreiben und
- die IT-Performance zu messen.

Unternehmen können ohne die Anwendung und Umsetzung eines Governance und Control Frameworks für die IT nicht in effektiver Weise die Unternehmens- und Governance-Erfordernisse erfüllen, um

- eine Verbindung zu den Unternehmenserfordernissen herzustellen,
- die Performance in der Erreichung der Erfordernisse transparent zu gestalten,
- die Aktivitäten in ein allgemein akzeptiertes Prozessmodell zu gliedern,
- die wesentlichen Ressourcen zu identifizieren und wirksam einzusetzen,
- die zu beachtenden Control Objectives der Führung festzulegen.

Des weiteren werden Governance und Control Frameworks zu Best Practices im IT-Management und sind ein Unterstützungsfaktor für die Erstellung von IT-Governance und die Erreichung der Compliance mit einer immer größer werdenden Anzahl an Regulativen.

Aus unterschiedlichen Gründen werden Best Practices in der IT immer mehr befolgt:

- ManagerInnen von Kerngeschäftsprozessen und Mitglieder von Steuerungsgremien verlangen einen verbesserten Return für IT-Investitionen, zB in dem die IT-Leistungen zu erbringen hat, wleche die Werte für die Stakeholder erhöhen.
- Unsicherheiten in Zusammenhang mit steigenden Ausgaben für IT.
- Der Bedarf regulativer Anforderungen hinsichtlich Steuerung der IT im Bereich Privacy oder Finanzreporting (zB Sarbanes-Oxley Act, Basel II) oder in speziellen Bereichen wie Pharma-, Kredit- oder Gesundheitswesen.
- Die Auswahl von Dienstleistern und das Management von Outsourcing und Beschaffung.
- Steigende Komplexität von mit IT zusammenhängenden Risiken wie Netzwerksicherheit.
- Initiativen im Bereich der IT-Governance, welche die Anwendung von Control Frameworks und Best Practices unterstützen. Diese ermöglichen die Überwachung und Verbesserung von kritischen Aktivitäten der IT für eine Steigerung des Wertbeitrages und eine Reduktion der Geschäftsrisiken.
- Der Bedarf, Kosten zu optimieren, in dem immer mehr standardisierte und immer weniger spezifisch entwickelte Ansätze verfolgt werden.
- Der wachsende Reifegrad und die daraus folgende Akzeptanz von anerkannten Frameworks wie COBIT, ITIL, ISO 17799, ISO 9001, CMM und PRINCE2.
- Der Bedarf, die Performance des eigenen Unternehmens an gleichartigen Unternehmen und an allgemein anerkannten Standards zu messen (Benchmarking).

Wer

Ein Governance und Control Framework dient unterschiedlichen internen und externen Stakeholdern, die ihrerseits unterschiedliche Bedürfnisse verfolgen:

- Stakeholder innerhalb des Unternehmens, deren Ziel es ist, einen Nutzen aus den IT-Investitionen zu ziehen
  - Jene, die Investitionsentscheidungen treffen
  - Jene, die über Anforderungen entscheiden
  - Jene, die IT-Services verwenden
- Interne und externe Stakeholder, die IT-Services bereitstellen
  - Jene, die die IT-Organisation und IT-Prozesse managen
  - Jene, die Potentiale entwickeln
  - Jene, die Services betreiben
- Interne und externe Stakeholder, die eine Steuerungs- und Risikoverantwortung tragen
  - Jene mit Aufgaben im Bereich Security, Privacy und/oder Risiko
  - Jene, die Compliance-Funktionen übernehmen
  - Jene, die Assurance-Funktionen verlangen oder vornehmen

Was

Um die oben aufgeführten Anforderungen zu erfüllen, soll ein IT-Governance und IT-Control Framework:

- einen Business-Fokus bereitstellen, um die Ausrichtung von IT-Zielen und Unternehmenszielen zu ermöglichen.
- eine Prozessorientierung aufbauen, welche den Umfang und den Grad der Abdeckung definiert und einfach handzuhaben ist,
- dadurch allgemein anerkannt sein, dass darin akzeptierte Best Practices und Standards enthalten sind und das Framework technologieunabhängig ist,
- eine gemeinsame Sprache etablieren mit Begriffen und Definitionen, die allgemein, für alle Stakeholder verständlich ist,
- bei der Erfüllung von gesetzlichen Anforderungen helfen, in dem es an allgemeinen Standards der Corporate Covernance (zB COSO) ausgerichtet ist und IT-Controls beinhaltet, die von der externen Revision und vom Gesetzgeber erwartet werden.

WIE COBIT DEN BEDARF DECKT

Auf den in den vorderen Kapiteln beschriebenen Bedarf reflektierend, wurde das COBIT Framework mit den folgenden Charakteristiken definiert: fokussiert auf das Business, orientiert an Prozessen, basierend auf Controls und getrieben von Messung.

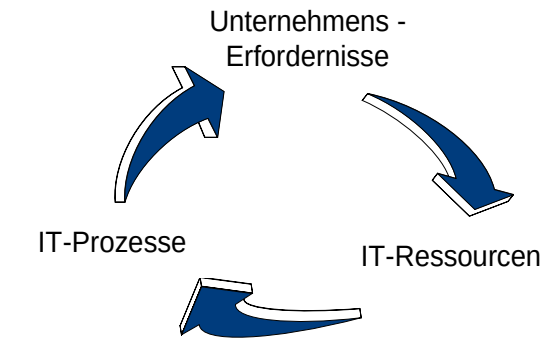
Fokussiert auf das Business

Die Unternehmensorientierung ist das Hauptthema von COBIT. COBIT wurde erstellt, um nicht nur von IT-Dienstleistern, Usern und Revisoren gelesen zu werden, sondern auch – oder gerade besonders – als umfassende Anweisung für das Management und Prozessverantwortliche im Kerngeschäft.

Das COBIT Framework basiert auf dem folgenden Prinzip (siehe auch Abbildung 5): Um die für die Erreichung der Ziele des Unternehmens erforderlichen Informationen bereitzustellen, muss das Unternehmen die IT-Ressourcen durch eine strukturierte Menge an Prozessen managen und steuern, die gewährleisten, dass die entsprechenden Services bereitgestellt werden.

Das COBIT Framework liefert Werkzeuge, die helfen, die Ausrichtung auf die Unternehmenserfordernisse sicherzustellen.

Abbildung 5 – Grundlegendes Prinzip von COBIT



DIE INFORMATION CRITERIA VON COBIT

Um die Unternehmensziele zu erreichen, müssen die Informationen bestimmten Kriterien entsprechen, welche in COBIT als unternehmensspezifische Erfordernisse an Informationen bezeichnet werden. Auf den breiteren qualitativen und fiduziären Sicherheitserfordernissen wurden sieben einzelne, einander sicherlich überlappende Information Critera wie folgt definiert:

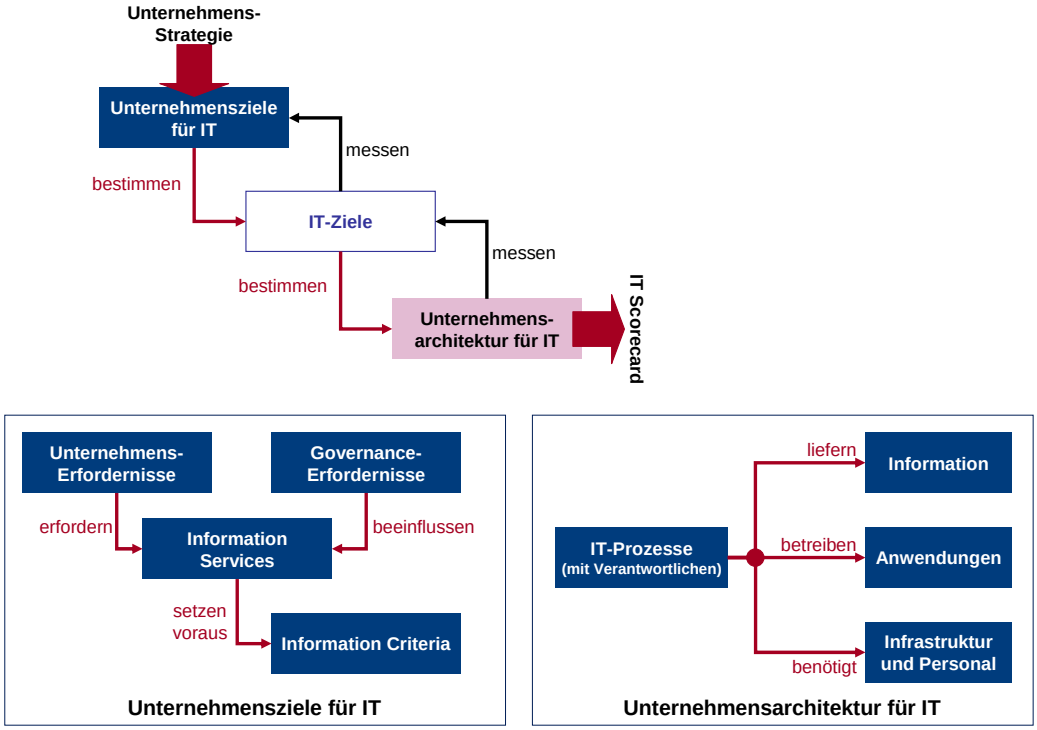
- Effectiveness (Wirksamkeit) behandelt die Relevanz und Angemessenheit von Informationen für den Geschäftsprozess sowie die angemessene Bereitstellung hinsichtlich Zeit, Richtigkeit, Konsistenz und Verwendbarkeit
- Efficiency (Wirtschaftlichkeit) behandelt die Bereitstellung von Information durch die optimale (produktivste und wirtschaftlichste) Verwendung von Ressourcen
- Confidentiality (Vertraulichkeit) behandelt den Schutz von sensitiven Informationen gegen unberechtigte Offenlegung
- Integrity (Integrität) bezieht sich auf die Richtigkeit und Vollständigkeit von Informationen sowie deren Gültigkeit in Übereinstimmung mit Unternehmenswerten und Erwartungen
- Availability (Verfügbarkeit) bezieht sich darauf, dass Informationen derzeit und in Zukunft für den Geschäftsprozess verfügbar sind. Sie betrifft auch den Schutz notwendiger Ressourcen und deren Leistungen
- Compliance (Compliance) behandelt die Einhaltung von Gesetzen, Regulativen und vertraglichen Vereinbarungen, welche der Geschäftsprozess berücksichtigen muss, zB extern auferlegte Kriterien sowie interne Richtlinien
- Reliability (Verlässlichkeit) bezieht sich auf die Angemessenheit bereitgestellter Informationen, die vom Management verwendet werden, um die Gesellschaft zu leiten und seine Treue- und Governance-Pflichten ausüben zu können

UNTERNEHMENSZIELE UND IT-ZIELE

Während die Information Criteria eine generische Methode zur Definition des Informationsbedarfs darstellen, liefern die in COBIT definierten generischen Unternehmens- und IT-Ziele eine spezifischere Basis, um die Unternehmensanforderungen festzulegen und um Metriken zu entwickeln, die die Messung deren Erreichung erlauben. Jedes Unternehmen setzt Informationstechnologie ein, um Vorhaben des Geschäfts zu unterstützen; diese können als Unternehmensziele für die IT angesehen werden. Im Anhang I befindet sich eine Matrix mit generischen Unternehmenszielen und IT-Zielen und wie diese zu den Information Criteria verbunden werden können. Diese generische Matrix kann als Beispiel für die Bestimmung der Zusammenhänge zwischen den unternehmensspezifischen Erfordernissen, Zielen und Metriken für das Unternehmen herangezogen werden.

Wenn IT erfolgreich Services zur Unterstützung der Unternehmensstrategie erbringen will, sollten hinsichtlich der Anforderungen klare Verantwortlichkeiten und Vorgaben durch das Kerngeschäft (den Kunden) sowie ein klares Verständnis über den durch die IT (den Dienstleister) zu deckenden Bedarf (WAS und WIE) bestehen. Abbildung 6 zeigt, wie die Unternehmensstrategie durch die Verantwortlichen im Kerngeschäft in Vorgaben für die Nutzung von IT-unterstützten Vorhaben umzusetzen sind (Unternehmensziele für IT). Diese Vorgaben wiederum sollten zu einer klaren Festlegung der IT-eigenen Ziele (IT-Ziele) führen, welche wiederum IT-Ressourcen und deren Leistungen (Unternehmensarchitektur für IT) definieren, welche für eine erfolgreiche Erfüllung der sich aus der Strategie ergebenden Aufgaben erforderlich sind. Alle diese Ziele sollten in einer Geschäftssprache ausgedrückt werden, welche vom Kunden verstanden wird; und dies wird in Kombination mit einer wirksamen Ausrichtung der Hierarchie der Ziele sicherstellen, dass das Kerngeschäft bestätigen kann, dass die IT wahrscheinlich die Unternehmensziele unterstützen kann.

Abbildung 6 – Definition von IT-Zielen und der Unternehmensarchitektur für IT



Nachdem die abgeglichenen Ziele festgelegt wurden, müssen diese einem Monitoring unterliegen, um sicherzustellen, dass die tatsächliche Leistungserbringung den Erwartungen entspricht. Dies wird durch von den Zielen abgeleitete Metriken erreicht und in der IT Scorecard in einer Form festgehalten, die der Kunde verstehen und verfolgen kann und die es dem Leistungserbringer ermöglicht, den Fokus auf die internen Vorgaben zu legen.

Der Anhang I enthält eine Übersicht über die Art, wie generische Unternehmensziele mit den IT-Zielen, IT-Prozessen und Information Criteria in Verbindung stehen. Die Tabellen helfen bei der Darstellung des Umfangs von COBIT und der gesamthaften, unternehmensorientierten Verbindung zwischen COBIT und den treibenden Faktoren des Kerngeschäfts.

IT-RESSOURCEN

Die IT Organisation arbeitet in Richtung dieser Ziele durch eine klar bestimmte Menge von Prozessen, die Fertigkeiten von Personen und (technologische) Infrastruktureinrichtungen verwendet, um automatisierte Unternehmensanwendungen zu betreiben und Informationen zu verarbeiten. Diese Ressourcen bilden – wie aus Abbildung 6 hervorgeht – gemeinsam mit den Prozessen die Unternehmensarchitektur der IT.

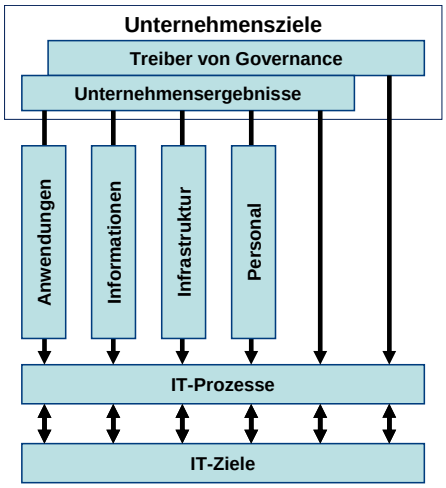
Um auf die Unternehmenserfordernisse an die IT reagieren zu können, muss das Unternehmen in Ressourcen zur Bereitstellung von angemessenen, technischen Möglichkeiten(zB ein Enterprise Resource Planning System) investieren, um die Unternehmenfähigkeiten (zB Umsetzung einer Supply Chain) zu unterstützen, was zum gewünschten Resultat (zB erhöhte Verkaufszahlen und Gewinne) führt.

Die in COBIT identifizierten IT-Ressourcen sind wie folgt definiert:

- Applications (Anwendungen) sind automatisierte Anwendungen und manuelle Verfahren, die Informationen verarbeiten
- Information (Informationen) sind die Daten in all ihren Formen: Durch Informationssysteme eingelesen, verarbeitet oder ausgegeben, in jeder im Unternehmen verwendeten Form
- Infrastructure (Infrastruktur) sind die Technologien und Anlagen (Hardware, Betriebssysteme, Datenbankmanagementsysteme, Netzwerke, Multimedia, etc und die Einrichtungen, die diese beherbergen und unterstützen)
- People (Personal) sind jene Personen, die für Planung, Organisation, Beschaffung, Implementierung, Betrieb, Unterstützung, Monitoring und Evaluierung der Informationssysteme und Services benötigt werden. Sie können – je nach Bedarf - intern, outgesourct oder vertraglich gebunden sein.

Abbildung 7 zeigt eine Zusammenfassung des Einflusses der Unternehmensziele für IT darauf, wie IT-Ressourcen durch die IT-Prozesse gemanagt werden müssen, um die IT Ziele zu erreichen.

Abbildung 7 – Management von IT-Ressourcen, um IT-Ziele zu erreichen



Orientiert an Prozessen

COBIT gliedert IT-Aktivitäten in einem generischen Prozessmodell in vier Domänen (engl.: *Domain*). Diese Domänen sind: „Plan and Organise“ (plane und organisiere), „Acquire and Implement“ (beschaffe und implementiere), „Deliver and Support“ (erbringe und unterstütze) und „Monitor and Evaluate“ (überwache und beurteile). Die Domänen richten sich an die üblichen Verantwortlichkeiten von planen, bauen, betreiben und überwachen.

Das COBIT Framework enthält ein Referenzprozessmodell und eine gemeinsame, für alle im Unternehmen gültige Sprache, um die IT-Aktivitäten zu betrachten und zu managen. Die Einführung eines operativen Modells und einer für alle Beteiligten gemeinsamen Sprache ist einer der wichtigsten und ersten Schritte in Richtung guter Governance. COBIT enthält außerdem ein Framework, um IT-Performance zu messen und zu beurteilen, mit Dienstleistern zu kommunizieren und um Best Management Practices zu integrieren. Ein Prozessmodell unterstützt die Eigentümerschaft für Prozesse und ermöglicht die Definition von Aufgaben und Verantwortlichkeiten.

Um IT effektiv zu steuern, ist es wichtig, die Aktivitäten und Risiken innerhalb der IT zu kennen, die gemanagt werden müssen. Diese können wie folgt zusammengefasst werden:

PLAN AND ORGANISE (PLANE UND ORGANISIERE, PO)

Diese Domäne deckt Strategie und Taktik ab und betrifft die Identifikation, wie die IT am besten zur Erreichung der Unternehmensziele beitragen kann. Des weiteren muss die Umsetzung der strategischen Vision nach unterschiedlichen Gesichtspunkten geplant, kommuniziert und gemanagt werden. Schlussendlich soll eine geeignete Organisation und technologische Infrastruktur vorhanden sein. Diese Domäne beantwortet typischerweise die folgenden Fragen des Managements:

- Sind IT und Unternehmen aufeinander ausgerichtet?
- Nutzt das Unternehmen die IT-Ressourcen optimal?
- Versteht jeder in der Organisation die IT-Ziele?
- Sind IT-Risiken verstanden und werden sie gemanagt?
- Ist die Qualität der IT-Systeme ausreichend für die Anforderungen des Geschäfts?

ACQUIRE AND IMPLEMENT (BESCHAFFE UND IMPLEMENTIERE, AI)

Um die IT-Strategie umzusetzen, müssen IT-Lösungen identifiziert, entwickelt oder beschafft sowie umgesetzt und in die Geschäftsprozesse integriert werden. Zusätzlich werden Änderungen und Wartung von bestehenden Systemen durch diese Domäne abgedeckt, um sicherzustellen, dass die Lösungen weiterhin den Unternehmenszielen entsprechen. Die Domäne beantwortet typischerweise die folgenden Fragen des Managements:

- Entsprechen die Ergebnisse neuer Projekte mit hoher Wahrscheinlichkeit den Unternehmensanforderungen?
- Werden neue Projekte wahrscheinlich rechtzeitig und innerhalb des Budgets fertig gestellt?
- Werden die neuen Systeme nach ihrer Fertigstellung korrekt funktionieren?
- Werden Changes ohne unnötige Beeinträchtigung der gegenwärtigen Geschäftsprozesse durchgeführt?

DELIVER AND SUPPORT (ERBRINGE UND UNTERSTÜTZE, DS)

Diese Domäne beschäftigt sich mit der eigentlichen Erbringung der benötigten Leistungen, was Leistungserbringung (engl.: *Service Delivery*), Management der Sicherheit und Kontinuität, Service Support für BenutzerInnen und Management von Daten und Einrichtungen umfasst. Sie beantwortet typischerweise die folgenden Fragen des Managements:

- Werden IT-Services entsprechend den Prioritäten des Unternehmens erbracht?
- Sind IT-Kosten optimiert?
- Können Anwender die IT-Systeme produktiv und sicher nutzen?
- Ist eine angemessene Vertraulichkeit, Integrität und Verfügbarkeit gegeben?

MONITOR AND EVALUATE (ÜBERWACHE UND EVALUIERE, ME)

Alle IT-Prozesse müssen regelmäßig hinsichtlich ihrer Qualität und Einhaltung von Kontrollanforderungen beurteilt werden. Diese Domäne behandelt Management der Performance, Überwachung von Internal Controls, Einhaltung von Regulativen und die Gewährleistung von Governance. Sie beantwortet typischerweise die folgenden Fragen des Managements:

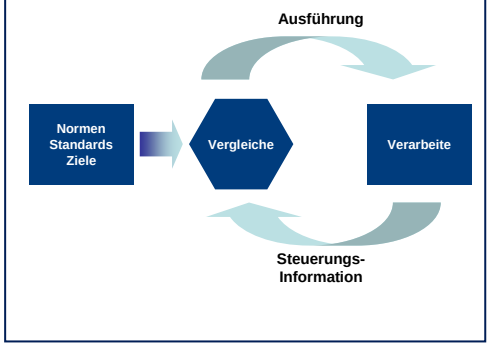
- Wird die Performance der IT gemessen, um Probleme zu erkennen, bevor es zu spät ist?
- Stellt das Management sicher, dass Internal Controls effektiv und effizient sind?
- Kann die IT-Performance zurück zu den Unternehmenszielen verknüpft werden?
- Werden Risiko, Control, Compliance und Performance gemessen und wird darüber berichtet?

Basierend auf Controls

PROZESSE ERFORDERN CONTROLS

Eine Control wird definiert als jene Richtlinien, Verfahren, Praktiken und Organisationsstrukturen, die entwickelt wurden, um ausreichende Sicherheit zu geben, dass die Unternehmensziele erreicht werden und dass unerwünschte Ereignisse verhindert oder erkannt und korrigiert werden.

Abbildung 8 – Control Modell



Ein IT-Control Objective ist eine Aussage über das gewünschte Ergebnis oder den zu erreichenden Zweck, der mit der Umsetzung von, in bestimmten Aktivitäten integrierten Controls (engl.: *control procedure*), erreicht werden soll. Die Control Objectives von COBIT sind Minimalanforderungen für eine wirksame Steuerung jedes IT-Prozesses.
Eine Anleitung gibt das standardisierte Control Modell der Abbildung 8. Das Modell basiert auf den Prinzipien der folgenden Analogie: Falls die Raumtemperatur (Standard) der Heizung (Prozess) eingestellt ist, wird das System laufend die Raumtemperatur (Steuerungsinformation) überprüfen (vergleichen) und der Heizung das Signal (Anweisung) geben, mehr oder weniger Hitze zu liefern.

Das operative Management setzt Prozesse ein, um die laufenden IT-Aktivitäten zu organisieren und zu managen. COBIT stellt ein generisches Prozessmodell zu Verfügung, welches alle normalerweise in IT-Funktionen vorzufindenden Prozesse beinhaltet und liefert so ein allgemeines, für das operative IT-Management und das Unternehmensmanagement verständliches Referenzmodell. Um wirksame Governance zu erreichen, müssen vom operativen Management Controls implementiert werden, die in ein für alle IT-Prozesse festgelegtes Control Framework integriert sind. Nachdem die IT-Control Objectives von COBIT nach IT-Prozessen gegliedert sind, bildet dieses Framework einen eindeutigen Zusammenhang zwischen den Erfordernissen der IT-Governance, IT-Prozesse und den IT-Controls.

Jeder IT-Prozess von COBIT enthält ein übergeordnetes Control Objective sowie mehrere detaillierte Control Objectives. In Summe stellen sie die Eigenschaften von angemessen gemanagten Prozessen dar.

Die detaillierten Control Objectives werden durch zwei, den Domänen entsprechende Buchstaben, einer Prozessnummer und einer Control Objective Nummer referenziert. Zusätzlich zu den detaillierten Control Objectives gelten für jeden COBIT Prozess generische Kontrollanforderungen, welche durch PCn (engl.: *Process Control*) gekennzeichnet sind. Diese sollten zusammen mit den detaillierten Control Objectives des Prozesses berücksichtigt werden, um ein vollständiges Bild der Kontrollanforderungen zu erhalten.

PC1 Process Owner (Prozesseigner)
Definiere für jeden COBIT Prozess einen Eigentümer, damit die Verantwortung klar wird.

PC2 Repeatability (Wiederholbarkeit)
Definiere jeden COBIT Prozess in einer Art und Weise, dass er wiederholbar ist.

PC3 Goals and Objectives (Ziele und Vorgaben)
Entwickle für jeden COBIT Prozess klare Ziele und Vorgaben für dessen wirksame Ausführung.

PC4 Roles and Responsibilities (Rollen und Verantwortlichkeiten)
Definiere für jeden COBIT Prozess eindeutige Rollen, Aktivitäten und die Verantwortlichkeiten für dessen wirksame Ausführung.

PC5 Process Performance (Performance des Prozesses)
Messe die Performance jedes COBIT Prozesses im Vergleich zu seinen Zielen.

PC6 Policy, Plans and Procedures (Policy, Pläne und Verfahren)
Dokumentiere, überprüfe, aktualisiere und unterzeichne alle Richtlinien, Pläne und Verfahren, welche einen COBIT Prozess treiben und kommuniziere diese an alle Beteiligten.

Wirksame Controls reduzieren Risiken, erhöhen die Wahrscheinlichkeit für die Erbringung von Wertbeiträgen und verbessern die Effizienz durch die Verringerung von Fehlern und die Anwendung eines konsistenten Management Ansatzes.

Des weiteren stellt COBIT für jeden Prozess folgende Beispiele zur Verfügung, die illustrativer, aber nicht einschränkender oder vollständiger Natur sind:
- Generische Inputs und Outputs
- Aktivitäten und Anweisungen für Rollen und Verantwortlichkeiten in einem RACI-Chart
- Key Activity Goals, die wichtigsten Aktivitäten
- Metriken

Zusätzlich zur Akzeptanz der notwendigen Controls müssen Prozesseigner verstehen, welche Inputs von anderen Prozesseignern erforderlich sind und welche Outputs von diesen benötigt werden. COBIT enthält für jeden Prozesse generische Beispiele der wesentlichsten Inputs und Outputs, inklusive der externen Anforderungen. Einige Outputs sind Inputs in allen anderen Prozessen, was in der Output-Tabelle durch ‚ALLE' ersichtlich ist; diese Outputs (Vorgaben für Qualitätsstandards und Anforderungen an Metriken, das IT-Prozess-Framework, dokumentierte Rollen und Verantwortlichkeiten, das unternehmensweite IT-Control-Framework, IT-Richtlinien und persönliche Rollen und Verantwortlichkeiten), sind jedoch nicht in allen Prozessen als eigener Input angeführt.

Das Verständnis für die Rollen und Verantwortlichkeiten aller Prozesse ist ein wesentlicher Faktor für eine wirksame Steuerung. COBIT enthält für alle Prozesse RACI-Charts (Diagramme, die anzeigen, wer zuständig (engl.: *responsible*), verantwortlich (engl.: *accountable*), konsultiert (engl.: *consulted*) und informiert (engl.: *informed*) ist). Verantwortlich (engl.: *accountable*) bedeutet die Letztverantwortung, also die Person, die Vorgaben gibt oder Aktivitäten bewilligt. Zuständig (engl.: *responsible*) sind Personen, welche die Aktivität durchführen; die beiden anderen Rollen (konsultiert und informiert) stellen sicher, dass alle benötigten Beteiligten integriert sind und den Prozess unterstützen.

UNTERNEHMENS- UND IT-CONTROLS

Das unternehmensweite Internal Control System (auch: Internes Kontrollsystem) hat auf drei Ebenen Auswirkungen auf die IT:
- durch das obere Management des Unternehmens werden Unternehmensziele festgelegt, Richtlinien aufgestellt und Entscheidungen hinsichtlich Ressourceneinsatz und –management zur Erreichung der Unternehmensstrategie getroffen. Der gesamthafte Ansatz für Governance und Steuerung wird durch die Unternehmensführung erstellt und im gesamten Unternehmen kommuniziert. Das Control-Umfeld (auch: Kontrollumgebung) der IT wird durch diese Vorgaben und Richtlinien beeinflusst.
- Auf der Ebene der Geschäftssprozesse werden Controls auf spezifische Geschäftsaktivitäten angewandt. Die meisten Geschäftsprozesse sind automatisiert und über IT-Anwendungen integriert, was dazu führt, dass viele der Controls auf dieser Ebene ebenfalls automatisiert sind. Diese Controls werden auch als Anwendungskontrollen (engl.: *Application Controls*) bezeichnet. Einige Controls der Geschäftsprozesse sind jedoch weiterhin manuell, wie Freigaben für Transaktionen, Funktionstrennung und manuelle Abstimmungen. Controls auf der Ebene der Geschäftsprozesse sind folglich eine Kombination von manuellen, durch die Mitarbeiter der Fachbereiche ausgeführten Controls, Controls der Unternehmenssteuerung und automatisierten Anwendungskontrollen. Beide liegen hinsichtlich ihrer Festlegung und Ausführung in Verantwortung der Fachbereiche, obwohl Design und Entwicklung der Anwendungskontrollen die Unterstützung durch die IT benötigen.
- Um die Geschäftsprozesse zu unterstützen, bietet die IT IT-Services an, die als geteilte Services üblicherweise in mehreren Geschäftsprozessen verwendet werden. Beispielsweise werden Entwicklungs- und operative IT-Prozesse sowie ein Großteil der Infrastruktur (zB Netzwerke, Datenbanken, Betriebssysteme oder Storage) für das gesamte Unternehmen erbracht. Die in allen IT-Services angewandten Controls werden als IT General Controls bezeichnet. Das verlässliche Funktionieren dieser IT General Controls ist notwendig, damit Verlass auf die Anwendungskontrollen ist. Zum Beispiel kann schlechtes Change-Management (auf Grund von Fehlern oder durch Vorsatz) die Verlässlichkeit einer automatisierten Integritätsprüfung unterlaufen.

IT GENERAL CONTROLS UND ANWENDUNGSKONTROLLEN

IT General Controls (auch anwendungsunabhängige Controls) sind jene, die in IT-Prozessen und Services integriert sind, zB:
- Systementwicklung
- Change-Management (Änderungswesen)
- Security
- Betrieb

In Geschäftsprozesse integrierte Controls werden allgemein als Anwendungskontrollen bezeichnet. Beispiele dafür sind:
- Vollständigkeit
- Richtigkeit
- Gültigkeit
- Genehmigung
- Funktionstrennung

COBIT geht davon aus, dass das Design und die Implementierung von automatisierten Controls in der Verantwortung der IT (abgedeckt durch die Prozesse der Domäne Acquire and Implement (Beschaffe und Implementiere)) liegt und auf den Unternehmenserfordernissen basieren, die durch die Information Criteria von COBIT festgelegt sind. Das operative Management und die Control-Verantwortlichkeit für Anwendungskontrollen liegt jedoch nicht in der IT, sondern bei den Eigentümern der Geschäftsprozesse.

IT betreibt und unterstützt die Anwendungsdienste und die dafür notwendigen Datenbanken und Infrastruktur.

Die COBIT IT-Prozesse decken deshalb die IT General Controls, nicht aber die Anwendungskontrollen ab, da die Verantwortung hierfür beim Eigentümer des Geschäftsprozesses liegt und diese Controls, wie oben beschrieben, in die Geschäftsprozesse integriert sind.

Die folgende Liste stellt die empfohlenen Control Objectives für Anwendungen dar, die durch ACn (engl.: *Application Controls*) gekennzeichnet sind.

Entstehung und Genehmigung

AC1 Data Preparation Procedures (Verfahren zur Aufbereitung)
Verfahren zur Aufbereitung von Daten sind vorhanden und werden durch Fachabteilungen angewandt. In diesem Umfeld hilft das Design von Eingabeformularen, sicherzustellen, dass Fehler und Auslassungen minimiert werden. Während der Datenerstellung stellen Verfahren zur Fehlerbehandlung ausreichend sicher, dass Fehler und Unregelmäßigkeiten aufgedeckt, kommuniziert und korrigiert werden.

AC2 Source Document Authorisation Procedures (Verfahren zur Genehmigung von Quelldokumenten)
Berechtigtes Personal, das in seinem Verantwortungsbereich agiert, bereitet Quelldokumente vor. Die Funktionen für Erstellung und Freigabe von Quelldokumenten sind angemessen getrennt.

AC3 Source Document Data Collection (Sammlung von Quelldokumenten)
Verfahren stellen sicher, dass alle freigegebenen Quelldokumente vollständig und richtig sind, festgehalten werden und rechtzeitig zur Datenerfassung weitergeleitet werden.

AC4 Source Document Error Handling (Fehlerbehandlung für Quelldokumente)
Verfahren zur Fehlerbehandlung stellen bei der Entstehung der Daten ausreichend sicher, dass Fehler und Unregelmäßigkeiten erkannt, kommuniziert und korrigiert werden.

AC5 Source Document Retention (Aufbewahrung von Quelldokumenten)
Verfahren stellen sicher, dass Originaldokumente angemessene Zeit aufbewahrt werden oder durch die Organisation neu erstellt werden können, sowohl um Rückgewinnung oder die Wiedererstellung von Daten zu ermöglichen, als auch um rechtliche Anforderungen zu erfüllen.

Dateneingabe

AC6 Data Input Authorisation Procedures (Verfahren zur Genehmigung von Eingaben)
Verfahren stellen sicher, dass nur autorisierte Personen Daten erfassen.

AC7 Accuracy, Completeness and Authorisation Checks (Prüfung von Richtigkeit, Vollständigkeit und Genehmigung)
Für die Weiterverarbeitung übertragene Transaktionsdaten (durch Personen erzeugt, durch Systeme generiert oder über Interfaces eingegeben) werden durch eine Vielzahl an Controls hinsichtlich Richtigkeit, Vollständigkeit und Gültigkeit geprüft. Verfahren stellen des weiteren sicher, dass Daten so nahe wie möglich an ihrem Entstehungsort validiert und bearbeitet werden.

AC8 Data Input Error Handling (Fehlerbehandlung während der Eingabe)
Verfahren für die Korrektur oder neuerliche Übertragung von Daten, die fehlerhaft erfasst wurden, sind vorhanden und werden befolgt.

Datenverarbeitung
AC9 Data Processing Integrity (Integrität der Verarbeitung)
Verfahren für die Verarbeitung von Daten stellen sicher, dass die Funktionstrennung gewahrt wird und durchgeführten Arbeiten routinemäßig verifiziert werden. Die Verfahren stellen sicher, dass angemessene Aktualisierungscontrols, zB Staffettenkontrollsummen (engl. *run-to-run control totals*) und Controls für die Aktualisierung von Stammdaten angewandt werden.

AC10 Data Processing Validation and Editing (Validierung der Verarbeitung)
Verfahren stellen sicher, dass die Validierung, Authentifikation und Bearbeitung so nahe wie möglich an der Quelle der Informationen erfolgt. Wichtige Entscheidungen, die auf Informationen von Artificial-Intelligence Systemen basieren, werden durch Personen getroffen.

AC11 Data Processing Error Handling (Fehlerbehandlung in der Verarbeitung)
Fehlerbehandlung-Routinen ermöglichen die Identifikation von fehlerhaften Transaktionen, ohne dass diese verarbeitet werden und ohne eine unnötige Störung der Verarbeitung anderer gültiger Geschäftsvorfälle.

Datenausgabe
AC12 Output Handling and Retention (Handhabung und Aufbewahrung von Output)
Handhabung und Aufbewahrung von Output von IT-Anwendungen entsprechen den festgelegten Verfahren und berücksichtigen Anforderungen der Privacy und Security.

AC13 Output Distribution (Verteilung von Output)
Verfahren für die Verteilung von IT-Output sind festgelegt, kommuniziert und werden befolgt.

AC14 Output Balancing and Reconciliation (Abstimmung von ausgegebenen Informationen)
Ausgegebene Informationen werden routinemäßig mit den relevanten Prüfsummen abgestimmt. Prüfspuren unterstützen die Nachverfolgung von Verarbeitungen und die Abstimmung beschädigter Informationen.

AC15 Output Review and Error Handling (Überprüfung und Fehlerbehandlung von Output)
Verfahren stellen sicher, das der Lieferant und die verantwortlichen Anwender die Richtigkeit von Outputs überprüfen. Ebenso sind Verfahren für die Identifikation und Behandlung von in der Ausgabe enthaltenen Fehlern etabliert.

AC16 Security Provision for Output Reports (Vorkehrungen für die Sicherheit von Outputs)
Verfahren sind im Einsatz, welche die Einhaltung der Sicherheit von Output (vor und nach dessen Verteilung zu Benutzern) gewährleisten.

Grenzen
AC17 Authenticity and Integrity (Authentizität und Integrität)
Die Authentizität und Integrität von Informationen, die von außerhalb der Organisation stammen, unabhängig davon, ob sie durch Telefon, Voice-Mail, Papier, Fax oder E-Mail empfangen wurden, werden angemessen geprüft, bevor potentiell kritische Aktivitäten unternommen werden.

AC18 Protection of Sensitive Information During Transmission and Transport (Schutz sensitiver Informationen während Übertragung und Transport)
Angemessener Schutz gegen unberechtigten Zugriff, Veränderung oder Falschadressierung von sensitiven Informationen wird während deren Übertragung und Transport sichergestellt.

Getrieben durch Messung

Ein grundsätzliches Bedürfnis aller Unternehmen ist, den Status der eigenen IT-Systeme zu verstehen und zu entscheiden, welches Maß an Management und Steuerung das Unternehmen anwenden soll.

Eine objektive Sicht auf die unternehmenseigene Performance zu erhalten, ist jedoch nicht leicht. Was soll gemessen werden und wie? Unternehmen müssen messen, wo sie stehen und wo Verbesserungsmaßnahmen notwendig sind und sie müssen dem Management Werkzeuge zur Verfügung zu stellen, um diese Verbesserungen zu überwachen.

Um das richtige Maß zu finden, sollte sich das Management fragen: Wie weit sollen wir gehen und entsprechen die Kosten dem Nutzen?

Diese Fragen behandelt COBIT durch die Bereitstellung von:
- Reifegradmodellen, die ein Benchmarking und die Identifikation notwendiger Potentialverbesserungen ermöglichen.
- Performancezielen und Metriken für die IT-Prozesse, die zeigen, wie Prozesse die Ziele des Kerngeschäfts und der IT erfüllen, und, basierend auf den Prinzipien der Balanced Scorecard ,für die interne Messung der Prozessperformance angewandt werden.
- Zielen für Aktivitäten, die eine wirksame Prozessperformance ermöglichen.

REIFEGRADMODELL

Von der Unternehmensleitung privater und öffentlicher Organisationen wird immer verlangt, zu berücksichtigen, wie gut die IT gemanagt wird. Als Reaktion darauf vrlangen Business Cases Entwicklungen für Verbesserungen und das Erreichen des angemessenen Niveaus für Management und Steuerung der Informationsinfrastruktur. Wenngleich wenige sagen würden, dass dieses Ziel nicht positiv sei, sollten sie die folgenden Fragen zur Abwägung von Kosten- Nutzenüberlegungen berücksichtigen:

- Was machen die Mitbewerber und wie stehen wir in Relation zu ihnen?
- Was ist eine akzeptable Best Practice der Branche und wie stehen wir in Relation dazu?
- Auf Basis der beiden Vergleiche: Können wir sagen, dass wir genug machen?
- Wie identifizieren wir die Anforderungen, die erfüllt sein müssen, um angemessenes Management und Steuerung der IT-Prozesse zu erreichen?

Es kann schwierig sein, auf diese Fragen sinnvolle Antworten zu finden. IT-Management sieht sich laufend nach Werkzeugen für Benchmarks und Self-Assessments um, um die notwendigen Antworten wirtschaftlich zu eruieren. Durch die Verwendung der Prozesse und der High-Level Control Objectives von COBIT sollte der Prozesseigner in der Lage sein, sich laufend gegen diese Control Objectives zu messen. Dies erfüllt drei Bedürfnisse:

- Eine relative Aussage, wo das Unternehmen steht
- Eine Art und Weise, effizient zu entscheiden, welcher Weg eingeschlagen werden soll
- Ein Werkzeug, um den Grad der Zielerreichung zu messen

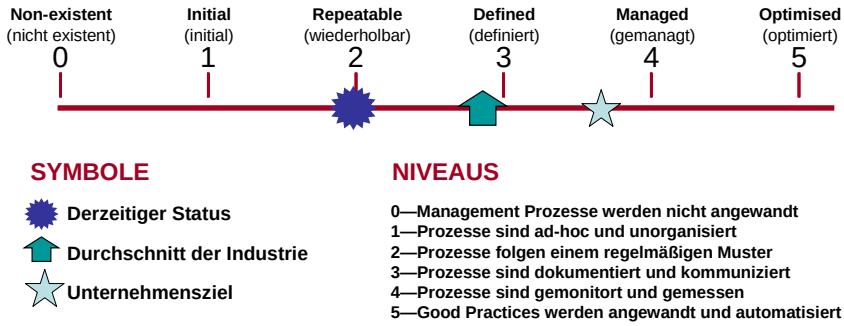
Die Reifegradmodellierung hinsichtlich Management und Steuerung von IT-Prozessen basiert auf einer Methode der Organisationsbewertung, so dass die Organisation sich selbst vom Niveau nicht-existent (0) bis zu optimiert (5) messen kann. Dieser Ansatz ist vom Maturity Model des Software Engineering Institutes abgeleitet, das den Reifegrad der Softwareentwicklung beurteilt. Unabhängig vom Modell sollten die Stufen nicht zu fein gewählt werden, da dies zu einer erschwerten Verwendbarkeit des Systems führt und eine Exaktheit suggeriert, die nicht haltbar ist, da der grundsätzliche Zweck in der Identifikation von Problemfeldern und der Priorisierung von Maßnahmen zur Verbesserung liegt. Der Zweck ist nicht, den Grad der Einhaltung von Control Objectives zu bestimmen.

Die Reifegrade sind als Profile der IT-Prozesse erstellt, die das Unternehmen als Beschreibung seines derzeitigen und zukünftigen Zustandes erkennt. Sie wurden nicht als ein Modell von Schwellwerten festgelegt, in dem die Erreichung der nächsten Stufe von der vollständigen Erfüllung der Anforderungen der darunter liegenden Stufe abhängig ist. Durch die Verwendung der Reifegradmodelle, welche für alle der 34 COBIT IT-Prozesse festgelegt wurden, kann das Management die folgenden Punkte identifizieren:

- Die derzeitige Performance—Wo sich das Unternehmen heute befindet.
- Den gegenwärtigen Status vergleichbarer Unternehmen—Der Vergleich.
- Das Unternehmensziel für die Verbesserung—Wo das Unternehmen sein will.

Um diese Ergebnisse in Managementberichten, in denen sie als Mittel zur Untermauerung des Business-Case für zukünftige Pläne verwendet werden, einfach darzustellen, empfiehlt sich eine graphische Darstellungsmethode (Abbildung 9).

Abbildung 9 – Graphische Darstellung des Reifegradmodells



Für jeden der 34 COBIT IT-Prozesse wurde ein Reifegradmodell festgelegt, das eine inkrementelle Beurteilungsskala von (0) nicht existent bis (5) optimiert enthält. Die Entwicklung basiert auf dem generischen Reifegradmodell, welches in Abbildung 10 dargestellt ist.

COBIT ist ein Framework, das für IT-Prozessmanagement mit starkem Steuerungsfokus erstellt wurde. Die Skalen müssen praktikabel in der Anwendung und leicht zu verstehen sein. Das Thema des IT-Prozessmanagements ist in sich komplex und subjektiv und wird demzufolge am einfachsten durch angeleitete Bewertungen in Angriff genommen, welche Bewusstsein schaffen, eine breite Akzeptanz finden und zur Verbesserung motivieren. Diese Bewertungen können entweder gesamthaft anhand der Beschreibungen der Reifegrade oder genauer, auf Basis der einzelnen Aussagen in den Reifegraden der Beschreibungen durchgeführt werden. Welcher Weg auch immer genommen wird, sind Kenntnisse über die untersuchten Prozesse hierzu erforderlich.

Abbildung 10 – Generisches Reifegradmodell

0 Non-existent (nicht existent). Es ist kein Prozess erkennbar. Das Unternehmen nicht einmal den Bedarf erkannt, dass das Thema in Angriff genommen werden soll.

1 Initial (initial). Es bestehen Anzeichen, dass das Unternehmen den Bedarf erkannt hat, das Thema zu behandeln. Es existieren jedoch keine standardisierten Prozesse, es ist vielmehr ein ad-hoc-Ansatz in Verwendung, der individuell und situationsbezogen angewandt wird. Der gesamthafte Managementansatz ist nicht organisiert.

2 Repeatable (wiederholbar). Prozesse wurden soweit entwickelt, dass gleichartige Verfahren von unterschiedlichen Personen angewandt werden, die dieselbe Aufgabe übernehmen. Es besteht kein formales Training oder eine Kommunikation der Standardverfahren und die Verantwortung ist Einzelpersonen überlassen. Es wird stark auf das Wissen von Einzelpersonen vertraut, demzufolge sind Fehler wahrscheinlich.

3 Defined (definiert). Verfahren wurden standardisiert und dokumentiert und durch Trainings kommuniziert. Die Einhaltung der Prozesse ist jedoch der Einzelperson überlassen und die Erkennung von Abweichungen ist unwahrscheinlich. Die Verfahren sind nicht ausgereift und sind ein formalisiertes Abbild bestehender Praktiken.

4 Managed (gemanagt). Es ist möglich, die Einhaltung von Verfahren zu überwachen und zu messen sowie Aktionen dort zu ergreifen, wo Prozesse nicht wirksam funktionieren. Prozesse werden laufend verbessert und folgen Good Practices. Automatisierung und Werkzeugunterstützung findet eingeschränkt und nicht integriert statt.

5 Optimised (optimiert). Prozesse wurden, basierend auf laufender Verbesserung und Vergleichen mit anderen Unternehmen, auf ein Best-Practice-Niveau verbessert. IT wird integriert für die Workflow-Automatisierung verwendet, stellt Werkzeuge für die Verbesserung der Qualität und Wirksamkeit zur Verfügung und macht das Unternehmen flexibel, sich Änderungen anzupassen.

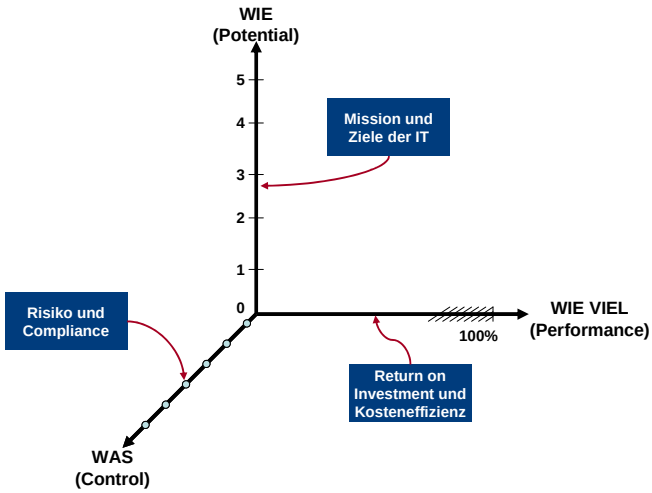
Der Vorteil am Ansatz des Reifegradmodells liegt darin, dass es für das Management relativ einfach ist, sich in der Skala wiederzufinden und zu erkennen, wo Handlungsbedarf für eine Performanceverbesserung notwendig ist. Die Skala enthält 0, denn es besteht die Möglichkeit, dass keinerlei Prozesse existieren. Die Skala von 0 bis 5 basiert auf dem einfachen Modell, das zeigt, wie sich ein Prozess von einem nicht existenten zum optimierten Potential entwickelt.

Prozesspotential ist jedoch nicht mit der Prozessperformance gleichzusetzen. Das erforderliche Potential, welches durch die Unternehmens- und IT-Ziele bestimmt wird, muss nicht über alle Bereiche der IT-Umgebung gleich hoch sein. Beispielsweise kann es nicht durchgängig gleich sein oder nur für eine eingeschränkte Anzahl von Systemen oder Einheiten. Performancemessung, wie in den nächsten Absätzen dargestellt, ist für die Bestimmung der tatsächlich für das Unternehmen vorhandenen Performance der IT-Prozesse notwendig.

Während ein angemessen angewandtes Potential bereits Risiken reduziert, muss ein Unternehmen dennoch die Controls analysieren, welche notwenidg sind, um die Risikoreduktion und die Generierung von Wertbeiträgen in Übereinstimmung mit der Risikobereitschaft und den Unternehmenszielen sicherzustellen. Diese Controls werden durch die Control Objectives von COBIT unterstützt. Im Anhang III befindet sich ein Reifegradmodell für Internal Controls, das die Reife einer Unternehmung hinsichtlich Erstellung und Betrieb von Internal Controls darstellt. Oft wird eine derartige Beurteilung durch externe Vorgaben initiiert, aber idealer Weise sollte sie, wie in den COBIT Prozessen *PO6 Communicate Management Aims and Directions (Kommuniziere Managementziele und –ausrichtung)* und *ME2 Monitor and Evaluate Internal Control (Monitore und evaluiere Internal Controls)* beschrieben, institutionalisiert sein.

Potenzial, Performance und Controls sind, wie in Abbildung 11 dargestellt, unterschiedliche Dimensionen der Prozessreife.

Abbildung 11 – Die drei Dimensionen von Reife



Das Reifegradmodell ist ein Weg für die Messung des Entwicklungsgrades von Management-Prozessen, zB hinsichtlich deren Entwicklungsstand. Wie weit diese entwickelt sein müssen, hängt primär von den IT-Zielen und den Anforderungen der Unternehmensziele ab, die diese unterstützen. In welchem Ausmaß dieses Potential entwickelt wird, hängt im Wesentlichen vom durch das Unternehmen geforderten Return on Investment ab. Es wird beispielsweise kritische Prozesse geben, die ein vermehrtes und ein strengere Securitymanagement erfordern als andere, weniger wichtige Prozesse. Andererseits wird die Detaillierung und Reife der in den Prozessen integrierten Controls von der Risikoakzeptanz und den Compliance-Anforderungen abhängen.

Die Skala des Reifegradmodells hilft den Berufsleuten, dem Management zu erklären, wo Unzulänglichkeiten im IT-Prozessmanagement bestehen und welche Ziele für den künftigen Status gesetzt werden. Der richtige Reifegrad wird durch die Unternehmensziele, das operative Umfeld und die Industriepraktiken beeinflusst. Genauer gesagt, hängt der Reifegrad von der Abhängigkeit des Unternehmens von der IT, der technischen Reife und, eigentlich am Wichtigsten, vom Wert der Information ab.

Eine strategisch wichtige Messlatte für die Verbesserung von Management und Steuerung von IT-Prozessen kann durch einen Blick in aufkommende, internationale Standards und Best-In-Class Praktiken gefunden werden. Die heute aufkommenden Praktiken entsprechen dem morgen erwarteten Leistungsniveau und sind demzufolge nützlich für die Planung, wo das Unternehmen im Verlaufe der Zeit sein möchte.

Reifegradmodelle werden auf Basis des generischen, in Abbildung 10 dargestellten, qualitativen Modells entwickelt, in dem die folgenden, jeweils verbesserten Attribute eingefließen:
- Bewusstsein und Kommunikation
- Richtlinien, Standards und Verfahren
- Werkzeuge und Automatisierung
- Fähigkeiten und Erfahrung
- Zuständigkeit und Verantwortlichkeit
- Zielsetzung und Messung

Die Attribute der Reife sind in der Tabelle in Abbildung 12 dargestellt, welche die Charakteristiken auflistet, wie IT-Prozesse gemanagt werden und die Entwicklung von einem nicht existenten zum optimierten Prozess beschreibt. Diese Attribute können für eine umfassende Beurteilung, Gap-Analyse und Verbesserungsplanung verwendet werden.

Zusammengefasst stellen Reifegradmodelle ein generisches Profil der Entwicklungsstufen von Unternehmen hinsichtlich Management und Steuerung von IT-Prozessen dar. Sie sind:
- Eine Menge von Anforderungen und ermöglichenden Aspekten der unterschiedlichen Reifegrade.
- Ein Skala, mit der ein Unterschied auf einfache Weise messbar gemacht wird.
- Eine Skala, die sich für einen pragmatischen Vergleich anbietet.
- Die Basis für die Ist- und Soll-Positionierung.
- Eine Unterstützung für die Gap-Analyse, um die notwendigen Aktivitäten zur Erreichung des gewählten Niveaus zu bestimmen.
- Zusammengefasst: Ein Bild davon, wie die IT im Unternehmen gemanagt wird.

Die Reifegradmodelle von COBIT sind auf Potential, nicht notwendiger Weise auf Performance fokussiert. Sie sind weder eine unbedingt zu erreichende Zahl, noch wurden sie erstellt, um die Basis einer formalisierten Zertifizierung mit exakten Niveaus darzustellen, die j schwierig zu überschreiten sind. Sie wurden jedoch entworfen, um jederzeit anwendbar zu sein, mit Niveaus, die eine Beschreibung darstellen, die Unternehmen für ihre Prozesse als passend erkennen können. Das richtige Niveau wird durch die Art des Unternehmens, dessen Umwelt und Strategie bestimmt.

Performance oder, wie das Potential genutzt und umgesetzt wird, sind auf Kosten-Nutzen-Erwägungen basierende Entscheidungen. Zum Beispiel könnte ein hoher Grad an Sicherheit nur für die kritischsten Systeme des Unternehmens angewandt werden.

Auch wenn ein höherer Reifegrad die Steuerung des Prozesses verbessert, muss das Unternehmen dennoch auf Basis von Einflussgrößen für Risiko und Wertbeiträgen analysieren, welche Steuerungsmechanismen angewandt werden sollen. Die in diesem Framework beschriebenen generischen IT- und Unternehmensziele helfen bei dieser Analyse. Die Steuerungsmechanismen werden durch die COBIT Control Objectives unterstützt und konzentrieren sich darauf, was im Prozess getan wird; die Reifegradmodelle konzentrieren sich darauf, wie gut ein Prozess gemanagt wird. Der Anhang III enthält ein generisches Reifegradmodell für den Status der Internal Control Umgebung und die Entwicklung von Internal Controls in einem Unternehmen.

Eine korrekt umgesetzte Control Umgebung ist erreicht, wenn alle drei Aspekte der Reife (Potential, Performance und Control) berücksichtigt sind. Die Verbesserung der Reife vermindert Risiken und erhöht die Effizienz, welche zur Verringerung von Fehlern, zu vorhersagbaren Prozessen und zu einer wirtschaftlichen Verwendung von Ressourcen führt.

	Bewusstsein und Kommunikation	Policies, Standards und Verfahren	Werkzeuge und Automatisierung	Skills und Expertise	Zuständigkeit und Verantwortlichkeit	Zielsetzung und Messung
1	Kenntnis über den Bedarf für den Prozess entsteht. Die Themen werden sporadisch kommuniziert.	Es sind ad-hoc Ansätze für Prozesse und Verfahren im Einsatz. Prozesse und Policies sind nicht definiert.	Einige Werkzeuge existieren; Nutzung basiert auf Desktop-Tools. Es existiert keine geplante Herangehensweise für den Tool-Einsatz.	Für den Prozess notwendige Skills sind nicht festgehalten. Ein Schulungsplan existiert nicht und formales Training ist nicht in Verwendung.	Zuständigkeiten und Verantwortlichkeiten sind nicht festgelegt. Übernahme von Themen basiert auf Eigeninitiative und reaktiv.	Ziele sind nicht klar und werden nicht gemessen.
2	Bewusstsein für Handlungsbedarf besteht. Das Management kommuniziert den Gesamtbedarf.	Ähnliche allgemeine Prozesse entwickeln sich, aber basieren auf Intuition und individueller Expertise. Teile des Prozesses sind auf Grund individueller Expertise wiederholbar; etwas Dokumentation und informelle Kenntnis über Policies und Verfahren existiert.	Allgemeine Ansatze für den Tooleinsatz sind erkennbar, aber Lösungen wurden durch Einzelpersonen entwickelt. Werkzeuge von Herstellern wurden beschafft, aber werden unter Umständen nicht angewandt und sind eventuell nur Staubfänger / Schrankware (engl. *shelfware*)	Minimalerfordernisse von Skills wurden für kritische Bereiche festgelegt. Trainings werden eher bedarfsgesteuert als geplant durchgeführt und informelles Training-on-the-Job wird eingesetzt.	Einzelpersonen vermuten deren Zuständigkeit und werden üblicherweise verantwortlich gemacht, obwohl dies nicht formell festgelegt wurde. Es besteht Unklarheit über die Zuständigkeit wenn Probleme auftreten und eine Kultur von Schuldzuweisung ist verbreitet.	Einige Ziele werden gesetzt; finanzbezogene Messungen wurden entwickelt aber sind nur der Geschäftsführung bekannt. Monitoring ist inkonsistent und auf Einzelbereiche konzentriert.
3	Verständnis für Handlungsbedarf besteht. Das Management kommuniziert formeller und strukturierter.	Verwendung von Good Practices entwickelt sich. Der Prozess, Policies und Verfahren sind für wesentliche Aktivitäten definiert und dokumentiert.	Ein Plan zur Verwendung und Standardisierung von Werkzeugen zur Automatisierung von Prozessen wurde entwickelt. Werkzeuge werden in deren Haupteinsatzbereichen angewandt, aber nicht immer in Abstimmung mit dem Plan und sind nicht integriert.	Erfordernisse für Skills sind für alle Bereiche definiert und dokumentiert. Ein formeller Schulungsplan wurde entwickelt, aber formalisiertes Training erfolgt nach wie vor auf Basis von Eigeninitiative.	Prozesszuständigkeiten und -verantwortlichkeit ist definiert und Prozesseigner wurden festgelegt. Der Prozesseigner hat of nicht die volle Autorität, die Zuständigkeiten zuzuweisen.	Einige Ziele und Messgrößen der Wirksamkeit sind definiert, aber nicht kommuniziert und es besteht eine Verbindung zu den Unternehmenszielen. Messprozesse sind in Entwicklung, werden aber nicht durchgängig angewandt. Ideen der IT-Balanced-Scorecard werden umgesetzt und Ursachen für Abweichungen (engl. *root-cause*) analysiert.
4	Die Anforderungen werden umfassend verstanden. Reife Kommunikationstechniken werden angewandt und standardisierte Kommunikationswerkzeuge sind im Einsatz.	Der Prozess ist rund und vollständig; interne Best Practices werden angewandt. Sämtliche Aspekte des Prozesses sind dokumentiert und wiederholbar. Policies wurden vom Management freigegeben. Standards zur Weiterentwicklung des Prozesses existieren und werden befolgt.	Werkzeuge werden entsprechend einem standardisierten Plan umgesetzt und einige sind mit anderen Werkzeugen integriert. Werkzeuge werden in wichtigen Bereichen eingesetzt, um das Prozessmanagement zu automatisieren und wichtige Aktivitäten und Controls zu überwachen.	Erfordernisse für Skills werden routinemäßig für alle Bereiche aktualisiert, notwendige Kenntnisse werden sichergestellt und Zertifizierungen werden unterstützt. Reife Schulungstechniken werden entsprechend dem Plan angewandt und Knowledge-Sharing wird gefördert. Interne Experten werden einbezogen und die Wirksamkeit des Schulungsplans wird beurteilt.	Prozesszuständigkeiten und -verantwortlichkeit sind anerkannt und arbeiten so, dass der Prozesseigner seine/ihre Verantwortung erfüllen kann. Eine Belohnungskultur ist verbreitet, die zu Verbesserungen motiviert.	Effizienz und Effektivität wird gemessen und kommuniziert und ist mit Unternehmenszielen und dem strategischen IT-Plan verbunden. Die IT-Balanced-Scorecard ist in erkannten Problembereichen umgesetzt und Root-Cause-Analysen sind standardisiert. Laufende Verbesserung ist in Entwicklung.
5	Zukunftsgerichtetes und fortgeschrittenes Verständnis für die Anforderungen. Proaktive Kommunikation der Themen auf Basis von Trends, die Kommunikationstechnik ist ausgereift und integrierte Kommunikationswerkzeuge sind im Einsatz.	Externe Best Practices und Standards werden angewandt. Die Prozessdokumentation wurde zu automatisierten Workflows entwickelt. Prozesse, Policies und Verfahren sind festgelegt und integriert und ermöglichen ein vollständiges, durchgängiges Management und Verbesserung.	Standardisierte Werkzeug-Sets werden im gesamten Unternehmen angewandt. Werkzeuge sind vollständig mit anderen Werkzeugen integriert und ermöglichen eine durchgängige Unterstützung des Prozesses. Werkzeuge werden eingesetzt, um die Prozessverbesserung zu unterstützten und Abweichungen werden automatisch erkannt.	Die Organisation unterstützt formell die laufende Entwicklung von Skills, die auf klar definierten persönlichen und organisationsweiten Zielen fundieren. Schulung und Bildung unterstützt externe Best Practices und die Verwendung von Konzepten und Techniken der Spitzenklasse. Knowledge-Sharing gehört zur Unternehmenskultur und Wissensbasierte Systeme werden entwickelt. Externe und Branchenexperten werden konsultiert.	Prozesseigner sind befähigt, Entscheidungen zu treffen und Maßnahmen zu ergreifen. Verantwortlichkeiten sind akzeptiert und wurden über die gesamte Organisation gleichartig herunter gebrochen.	Es besteht ein integriertes System zur Performancemessung, welches IT-Performance mit Unternehmenszielen durch eine umfassende IT-Balanced-Scorecard verbindet. Abweichungen werden gesamthaft und durchgängig ausgewertet und Ursachen analysiert. Kontinuierliche Verbesserung gehört zum Alltag.

Abbildung 12 – Attribute der Reife

PERFORMANCE-MESSUNG

Ziele und Metriken sind in COBIT auf drei Ebenen festgelegt:

- IT-Ziele und Metriken, die definieren, was die Geschäftsbereiche von der IT erwarten (was die Geschäftsbereiche verwenden würden, um die IT zu messen)
- Prozessziele und Metriken, die definieren, was der IT-Prozess liefern muss, um die Ziele der IT zu unterstützen (wie der IT-Prozesseigner gemessen werden würde)
- Metriken der Prozessperformance (um zu messen, wie gut die Prozessperformance ist, um festzustellen, ob die Ziele erreicht werden)

In COBIT werden zwei Typen von Metriken verwendet: Goal Indicators und Performance Indicators. Die jeweiligen untergeordneten Goal Indicators werden zu Performance Indicators der höheren Ebene.

Key Goal Indicators (KGI) legen Messgrößen fest, die dem Management – danach – aufzeigen, ob ein IT-Prozess die Unternehmenserfordernisse erfüllt hat. Dies wird üblicherweise in Anlehnung an die Information Criteria kommuniziert:

- Verfügbarkeit von Informationen, die von den Geschäftsprozessen benötigt werden.
- Mangel an Risiken bezüglich Integrität und Vertraulichkeit
- Kosteneffizienz von Prozessen und des Betriebs
- Bestätigung der Verlässlichkeit, Wirksamkeit und Compliance

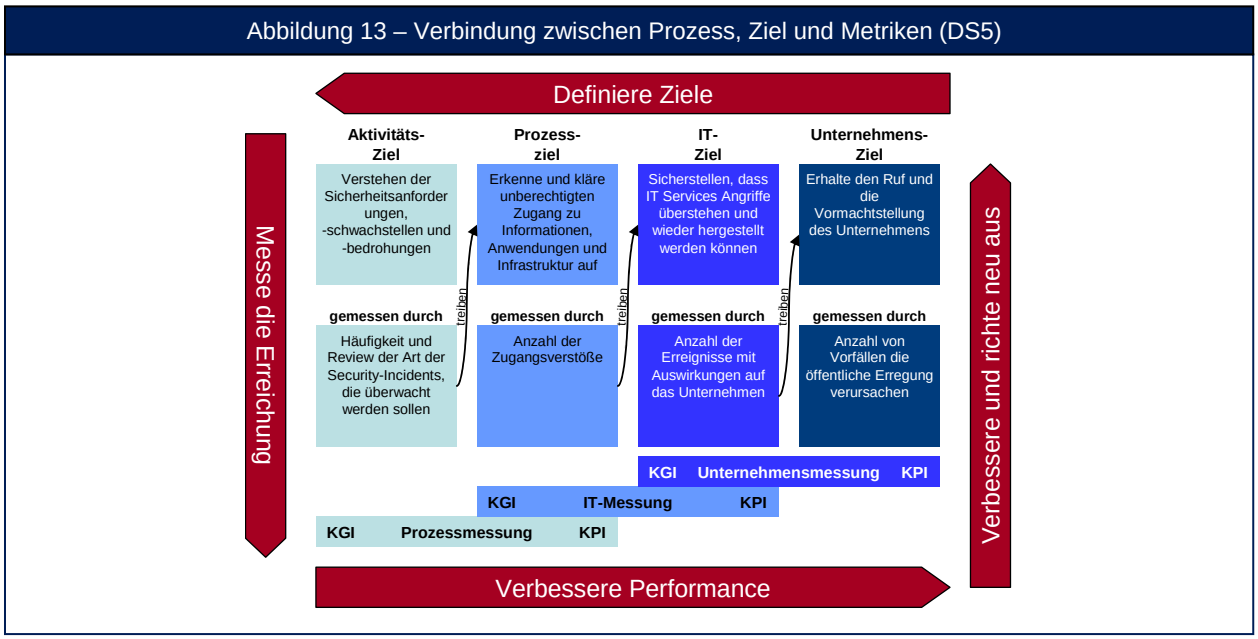
Key Performance Indicators (KPI) definieren Messgrößen, die bestimmen, wie gut die Performance von IT-Prozessen hinsichtlich der Unterstützung der Zielerreichung liegt. KPIs sind Früh-Indikatoren dafür, ob ein Ziel wahrscheinlich erreicht wird oder nicht. Sie geben einen guten Einblick in Potential, Praktiken und Fähigkeiten. Sie messen die Ziele von Aktivitäten, welche jene Handlungen darstellen, die der Prozesseigner erledigen muss, um eine wirksame Prozessperformance zu erreichen.

Wirksame Metriken sollten die folgenden Charakteristiken aufweisen:

- Ein gutes Verhältnis zwischen Aussagekraft und Aufwand (dh Aussage zur Performance und der Zielerreichung im Verhältnis zum Aufwand, diese Messdaten zu erfassen)
- Intern vergleichbar sein (zB Prozent einer festgelegten Basis über den Zeitverlauf)
- Extern vergleichbar sein, unabhängig von der Unternehmensgröße oder -branche
- Besser wenige gute Metriken (vielleicht sogar eine sehr gute Zahl, die auf unterschiedliche Weise beeinflusst werden könnte), als eine lange Liste niedriger Qualität
- Leicht zu messen sein und soll nicht mit dem Ziel zu verwechselt werden.

Abbildung 13 zeigt die Verbindung zwischen Prozess-, IT- und Unternehmenszielen und zwischen den unterschiedlichen Metriken mit Beispielen des Prozesses *DS5 Ensure systems security (Stelle Security von Systemen sicher)*.

Abbildung 13 – Verbindung zwischen Prozess, Ziel und Metriken (DS5)

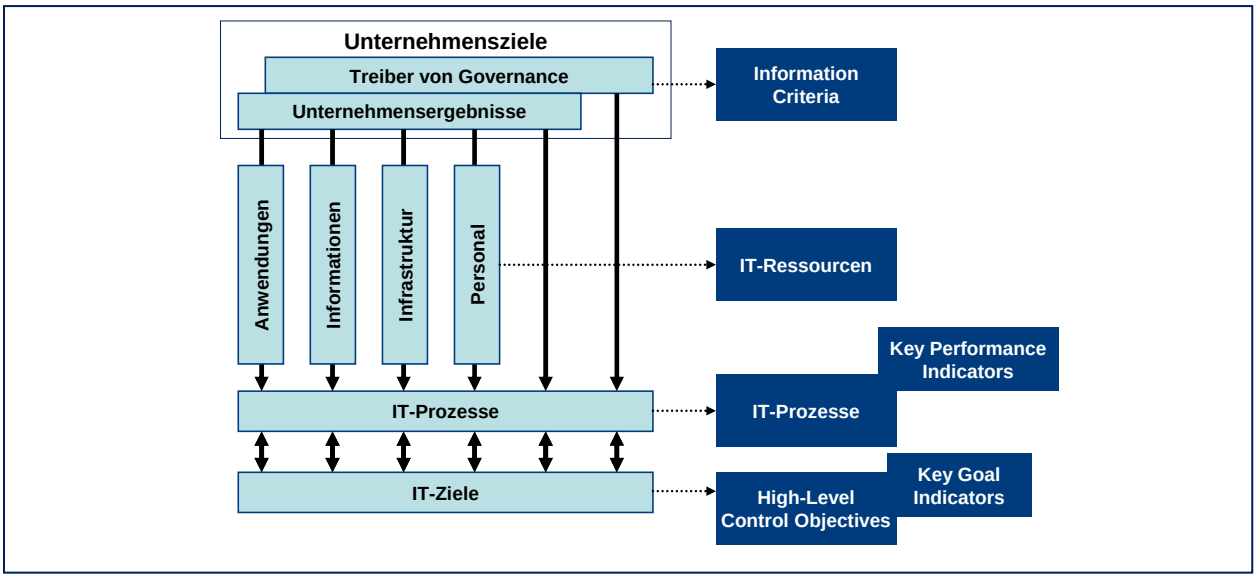


Ziele werden Top-Down festgelegt, in dem die Unternehmensziele eine Anzahl an IT-Zielen zu deren Unterstützung bestimmen; die IT-Ziele beeinflussen die unterschiedlichen Prozessziele und jedes Prozessziel wird die Aktivitätsziele vorgeben. Die Erreichung der Ziele wird durch Metriken des Output gemessen (als Key Goal Indicator oder KGI bezeichnet) und treiben das höher liegende Ziel weiter. Zum Beispiel treibt die Metrik, die für die Erreichung des Aktivitätszieles verwendet wird, die erforderliche Performance (als Key Performance Indicator oder KPI bezeichnet) des Prozessziels. Metriken ermöglichen es dem Management, die Performance zu korrigieren und wieder auf die Ziele auszurichten.

Das Framework-Modell von COBIT

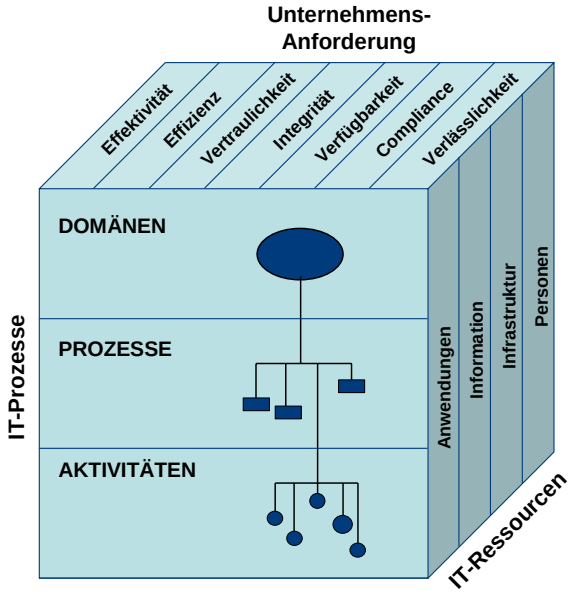
Das COBIT Framework verbindet Anforderungen des Unternehmens hinsichtlich Information und Governance mit den Zielen für die IT-Servicefunktion. Das COBIT Prozessmodell ermöglicht es, dass IT-Aktivitäten und Ressourcen, basierend auf den welches auf den COBIT Control Objectives, richtig gemanagt werden und durch die Verwendung der KGI und KPI Metriken ausgerichtet und überwacht werden, was in Abbildung 14 dargestellt wird:

Abbildung 14 – COBIT Management, Control, Alignment und Monitoring



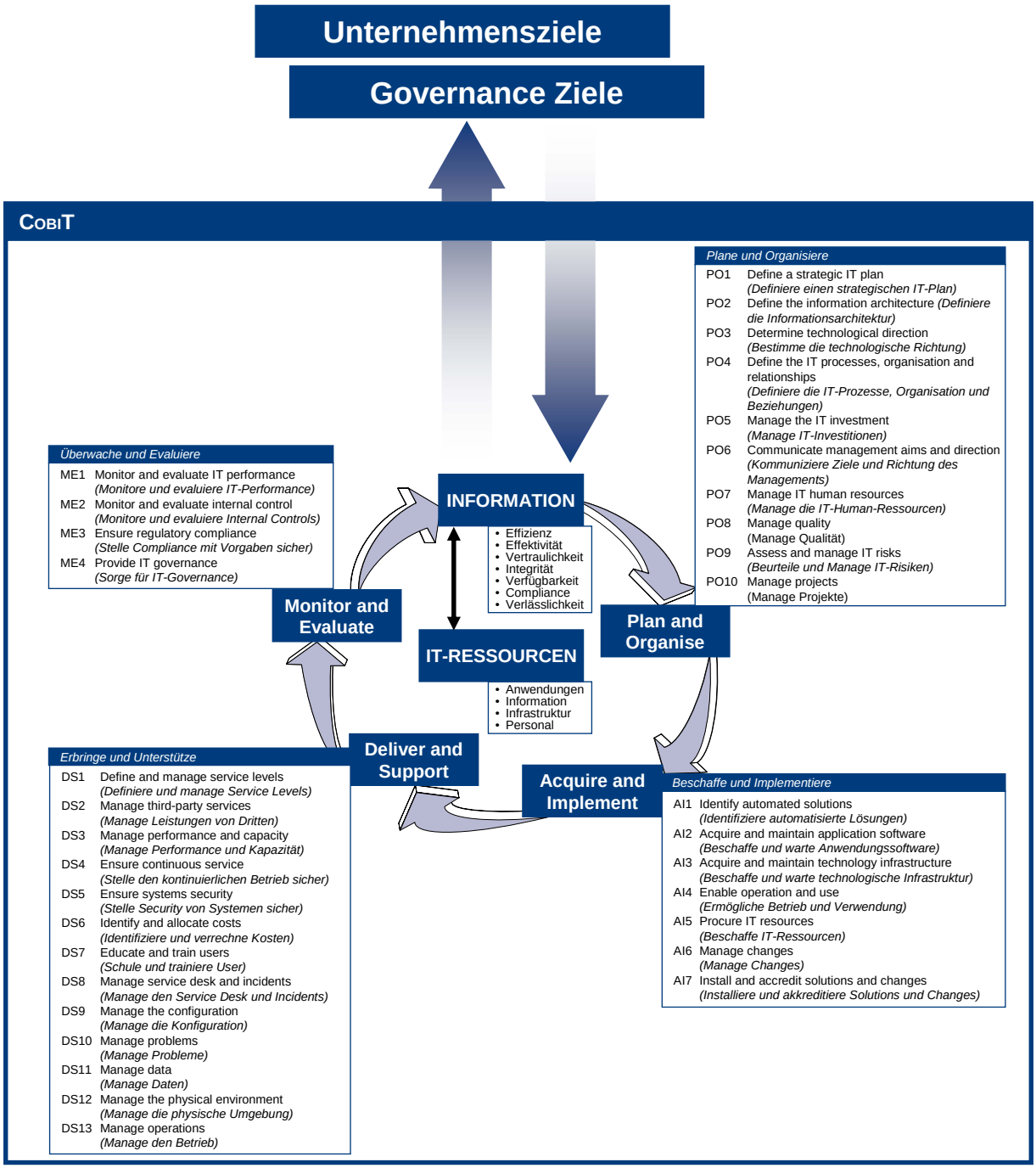
Zusammengefasst werden IT-Ressourcen durch IT-Prozesse gemanagt, um IT-Ziele zu erreichen, die auf Unternehmenserfordernisse ausgerichtet sind. Dies ist, wie im COBIT-Würfel der Abbildung 15 dargestellt, das Grundprinzip des COBIT Frameworks.

Abbildung 15 – Der COBIT Würfel



In einem höheren Detaillierungsgrad wird das übergeordnete COBIT Framework graphisch in Abbildung 16 dargestellt. Diese enthält das COBIT Prozessmodell, welches aus 4 Domänen und 34 generischen Prozessen besteht, mit Hilfe derer IT-Ressourcen gemanagt werden, um dem Unternehmen die Informationen entsprechend den Anforderungen vom Kerngeschäft und der Governance zu liefern.

Abbildung 16 – Gesamthaftes COBIT Framework



Die allgemeine Akzeptanz von COBIT

COBIT basiert auf der Analyse und Harmonisierung existierender IT-Standards und bewährter Praktiken und ist mit allgemein anerkannten Grundsätzen von Governance in Einklang gebracht. COBIT ist auf hoher Ebene angesiedelt, durch Unternehmenserfordernisse getrieben, deckt sämtliche Aktivitäten der IT ab und konzentriert sich eher darauf, *Was* erreicht werden soll, als *Wie* wirksame Governance, Management und Steuerung erreicht werden. Folglich fungiert COBIT als Integrator von Praktiken für IT-Governance und richtet sich an die Geschäftsleitung, das Unternehmens- und IT-Management und an Fachkräfte aus den Bereichen Assurance, Security, aber auch Audit und Control. COBIT wurde entwickelt, um komplementär und gemeinsam mit anderen Standards und Best Practices verwendet zu werden.

Die Umsetzung von Best Practices sollte in Einklang mit dem unternehmensweiten Governance- und Control Framework stehen, das für die Organisation geeignet ist und mit anderen eingesetzten Methoden und Verfahren integriert werden soll. Standards und Best Practices sind kein Wundermittel und ihre Wirksamkeit hängt stark davon ab, wie sie tatsächlich umgesetzt wurden und wie sie auf dem Laufenden gehalten werden. Sie sind am hilfreichsten, wenn sie als eine Reihe von Grundsätzen und als Ausgangspunkt für das Zusammenstellen spezifischer Verfahren angewandt werden. Um zu verhindern, dass Verfahren verstauben, müssen das Management und die MitarbeiterInnen verstehen, was getan werden muss, wie etwas getan werden muss und warum dies wichtig ist.

Um die Ausrichtung der Best Practices auf die Unternehmensanforderungen zu erreichen, empfiehlt es sich, COBIT auf höchster Ebene als übergeordnetes Control Framework zu verwenden, das auf einem IT-Prozessmodell basiert, welches generisch für jedes Unternehmen passen müsste. Spezielle Praktiken und Standards, die eigenständige Themen abdecken, können mit dem COBIT Framework abgestimmt (gemappt) werden, womit eine Hierarchie von Materialien zur Anleitung entsteht.

COBIT wendet sich an verschiedene Anwender:

- Geschäftsleitung—Um Wertbeiträge aus IT-Investitionen zu erhalten und Risiken und Investitionen in Control in der häufig schwer einschätzbaren IT-Welt auszubalancieren.
- ManagerInnen von Kernprozessen—Um Gewissheit über die Führung zu erhalten und die Steuerung von IT-Services abzusichern, die intern oder durch externe Partner erbracht werden.
- IT-Management—Um die IT-Services zu erbringen, die das Geschäft zur kontrollierten und gemanagten Unterstützung der Unternehmensstrategie erfordert.
- Revisoren—Um ihre Aussagen zu untermauern und/oder dem Management Ratschläge für Internal Controls zu geben.

COBIT wurde durch ein unabhängiges, gemeinnütziges (engl.: *not-for-profit*) Forschungsinstitut erstellt und weiterentwickelt, welches auf die Expertise der Mitglieder, von Branchenkennern und Experten aus Control und Security baut. Der Inhalt basiert auf regelmäßig durchgeführten Forschungen im Bereich bewährter IT-Best Practices und wird laufend gepflegt, um ein objektives und zweckmäßiges Hilfsmittel für alle Arten von Anwendern zu bieten.

COBIT orientiert sich an den Zielen und der Breite von IT-Governance, in dem sichergestellt wird, dass das Control Framework umfassend und an Grundätzen der unternehmensweiten Governance ausgerichtet ist, und wird deswegen von Gremien der Unternehmensführung (zB Aufsichtsrat, Verwaltungsrat), vom Gremium der Geschäftsleitung (zB Vorstand), Revisoren und Regulatoren akzeptiert. Im Anhang II findet sich ein Mapping, das die Verbindung von den detaillierten Control Objectives von COBIT zu den fünf Kerngebieten der IT-Governance und den COSO Control Activities darstellt.

Abbildung 17 gibt einen Überblick über die Zusammenhänge der verschiedenen Elemente des COBIT-Framework und den IT-Governance-Domänen.

Abbildung 17 – COBIT Framework und IT-Governance-Domänen

	Ziele	Metriken	Verfahren	Reifegrad-modelle
Strategic alignment	P	P		
Value delivery		P	S	P
Risk management		S	P	
Resource management		S	P	P
Performance measurement	P	P		S

P=Primär S=Sekundäre Unternstützung

VERWENDUNG DES BUCHES

Navigation im COBIT Framework

Für jeden IT-Prozess ist ein High-Level übergeordnetes Control Objective angegeben, welches gemeinsam mit den Kernzielen und Metriken in Form eines Wasserfalls dargestellt wird.

Abbildung 18 –COBIT Navigation

Für jeden einzelnen IT-Prozess werden die detaillierten Control Objectives als generische Handlungsanweisungen für die im Management des Prozesses minimal anzuwendenden Best Practices angegeben, um sicherzustellen, dass der Prozess gesteuert werden kann.

Übersicht über die Kernbestandteile von COBIT

Das COBIT Framework besteht aus den folgenden Kernbestandteilen, die in den nachfolgenden Kapiteln dieser Publikation beschrieben werden, welche in die 34 IT-Prozesse gegliedert sind. Sie geben ein vollständiges Bild, wie jeder Prozess gesteuert, gemanagt und gemessen wird. Jeder Prozess wird in vier Teilen behandelt, die jeweils etwa eine Seite umfassen:

- Abschnitt 1 enthält eine Prozessbeschreibung, die die Prozessziele zusammenfasst, das High-Level Control Objective in einem Wasserfallmodell dargestellt. Diese Seite enthält auch die Verknüpfung des Prozesses mit den Information Criteria, den IT-Ressourcen und den IT-Governance Domänen, wo ‚P' für primäre Verbindung und ‚S' für sekundäre Verbindung steht.
- Abschnitt 2 enthält die detaillierten Control Objectives für diesen Prozess
- Abschnitt 3 enthält Prozessinputs und –outputs, RACI-Charts, Ziele und Metriken
- Abschnitt 4 enthält das Reifegradmodell für den Prozess

Eine weitere Möglichkeit, den Inhalt bezüglich Prozess-Performance zu betrachten, ist:

- Prozessinputs sind Informationen, die ein Prozesseigner von anderen benötigt
- Die Prozessbeschreibungen der Control Objectives beschreiben, was der Prozesseigner tun muss
- Der Prozessoutput beschreibt, was der Prozessverantwortliche zu liefern hat
- Die Ziele und Metriken zeigen, wie der Prozess gemessen werden soll
- Das RACI-Chart definiert, was an wen delegiert werden muss
- Das Reifegradmodell zeigt, was zur Verbesserung gemacht werden muss

Die Rollen im RACI-Chart sind für alle Prozesse die folgenden:

- Chief Executive Officer (CEO): die Geschäftsleitung
- Chief Financial Officer (CFO): der Finanzchef
- Business Executive: die Führungskraft im Fachbereich
- Chief Information Officer (CIO): der Leiter der Informatik
- Geschäftsprozesseigner
- Leitung Betrieb
- Chief Architect
- Leitung Entwicklung
- Leitung IT-Administration (für große Unternehmen, umfasst Funktionen wie HR-Management, Budgetierung und Internal Control)
- Projektbüro
- Compliance, Audit, Risk und Security (Gruppen mit Funktionen im Control Bereich, die keine operativen Verantwortungen in der IT tragen)

In einigen Prozessen wurden weitere, für den jeweiligen Prozess spezifische Rollen mit aufgenommen, zB Service Desk/Incident-Manager für DS 8.

Bitte beachten Sie, dass obwohl diese Unterlagen auf der Arbeit hunderter Experten basieren und einem umfassenden Review unterzogen wurden, die Inputs, Outputs, Verantwortlichkeiten, Metriken und Ziele beispielhaften Charakter haben und nicht verbindlich oder erschöpfend sind. Sie stellen eine Basis an Expertenwissen dar, von dem Unternehmen all das auswählen sollten, was für sie wirtschaftlich und wirksam; auf ihre Strategien, Ziele und Richtlinien angewandt werden kann.

Anhänge

Die folgenden weiterführenden Informationen befinden sich am Ende dieses Buches:

I. Verbindung von Unternehmenszielen und IT-Zielen (drei Tabellen)
II. Mapping von IT-Prozessen zu IT-Governance Domänen, COSO, IT-Ressourcen und Information Criteria von COBIT
III. Reifegradmodell für Internal Control
IV. Hauptsächliche Quellen, die für COBIT 4.0 verwendet wurden

PLAN AND ORGANISE

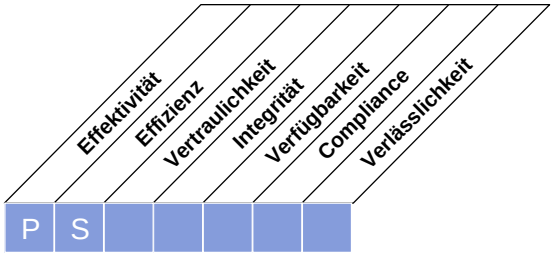
PO1 Define a Strategic IT Plan
(Definiere einen strategischen IT-Plan)
PO2 Define the Information Architecture
(Definiere die Informationsarchitektur)
PO3 Determine Technological Direction
(Bestimme die technologische Richtung)
PO4 Define the IT Processes, Organisation and Relationships
(Definiere die IT-Prozesse, Organisation und Beziehungen der IT)
PO5 Manage the IT Investment
(Manage IT-Investitionen)
PO6 Communicate Management Aims and Direction
(Kommuniziere Ziele und Richtung des Managements)
PO7 Manage IT Human Resources
(Manage die IT-Human-Ressourcen)
PO8 Manage Quality
(Manage Qualität)
PO9 Assess and Manage IT Risks
(Beurteile und Manage IT-Risiken)
PO10 Manage Projects
(Manage Projekte)

Diese Seite wurde absichtlich freigelassen

HIGH-LEVEL CONTROL OBJECTIVE

PO1 Define a Strategic IT Plan (*Definiere einen strategischen IT-Plan)*

Eine strategische IT-Planung wird benötigt, um alle IT-Ressourcen in Übereinstimmung mit der Unternehmensstrategie und deren Prioritäten zu managen und zu steuern. Die IT und die Business Stakeholder sind verantwortlich dafür, sicherzustellen, dass der optimale Wertbeitrag aus den Projekt- und Service-Portfolios generiert wird. Der strategische Plan sollte das Verständnis der Stakeholder über die Möglichkeiten und Grenzen der IT verbessern, die gegenwärtige Performance bewerten sowie den Umfang von notwendigen Investitionen ermitteln. Die Unternehmensstrategie und deren Prioritäten müssen sich in Portfolios wieder finden und durch die taktischen IT-Pläne umgesetzt werden, die konkrete Ziele, Pläne und Aufgaben festlegen, die sowohl von der IT, als auch von den Geschäftsbereichen akzeptiert werden.



Kontrolle über den IT-Prozess,

Define a Strategic IT Plan *(Definiere einen strategischen IT Plan)*

der die Anforderung des Unternehmens an die IT bezüglich

der Unterstützung oder Erweiterung der Unternehmensstrategie sowie der Governance-Anforderungen unter Wahrung von Transparenz hinsichtlich Nutzen, Kosten und Risiken

durch die Konzentration auf

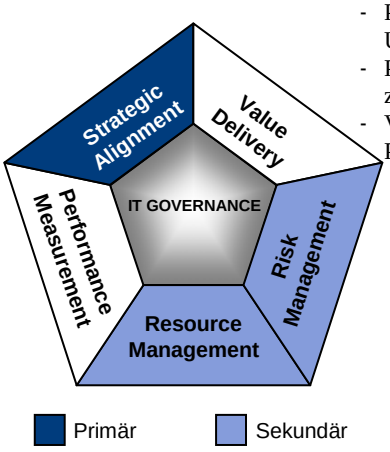
die Zusammenführung von IT- und Unternehmensmanagement im Bereich der Überleitung von Unternehmensanforderungen in IT-Serviceangebote und die Entwicklung von Strategien für die Erbringung dieser Services in transparenter und wirksamer Weise, *zufrieden stellt,*

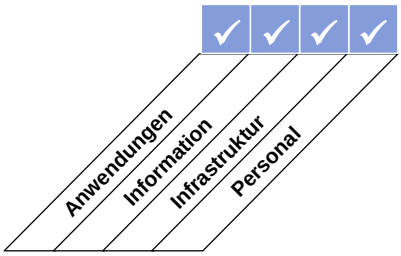
wird erreicht durch

- Zusammenarbeit mit der Geschäftsleitung und dem oberen Management in der Ausrichtung der strategischen IT-Planung auf derzeitige sowie künftige Geschäftsanforderungen
- Verstehen des derzeitigen IT-Potentials
- Erstellung eines Schemas für die Priorisierung von Geschäftszielen, das die Geschäftsanforderungen quantifiziert

und gemessen durch

- Prozent der IT-Ziele im strategischen IT-Plan, die den strategischen Unternehmensplan unterstützen
- Prozent der IT-Projekte im IT-Projektportfolio, die direkt auf den taktischen IT-Plan zurückgeführt werden können
- Verzögerung zwischen Aktualisierungen der strategischen und der taktischen IT-Pläne





DETAILLIERTE CONTROL OBJECTIVES

PO1 Define a Strategic IT Plan *(Definiere einen strategischen IT-Plan)*

PO1.1 IT Value Management (Management des Wertbeitrags der IT)
Arbeite mit dem Kerngeschäft zusammen, um sicherzustellen, dass unternehmensweite Portfolio von IT-unterstützten Investitionen Programme enthalten, welche stichhaltige Business-Cases aufweisen. Erkenne, dass es notwendige, laufende und dem Ermessen überlassene Investitionen gibt, die sich bei der Zuteilung von Finanzmitteln in Komplexität und Entscheidungsspielraum unterscheiden. IT-Prozesse sollten eine effektive und effiziente Bereitstellung der IT-Komponenten für Programme und ein Frühwarnsystem bieten für alle Planabweichungen (inklusive Kosten, Terminplan oder Funktionalität), welche die im Programm geplanten Ergebnisse beeinträchtigen können. IT-Services sollten entsprechend vernünftiger und durchsetzbarer Service Level Agreements erbracht werden. Verantwortlichkeiten für die Erreichung des Wertbeitrags und für Kostenkontrolle sind klar festgelegt und werden überwacht. Führe eine angemessene, transparente, wiederholbare und vergleichbare Beurteilung von Busines-Cases durch, welche eine Aussage zur finanziellen Rechtfertigung, zum Risiko einer Nichterbringung eines Potentials und zum Risiko einer Nichtausschöpfung von erwartetem Nutzen zum Inhalt hat.

PO1.2 Business-IT Alignment (Ausrichtung Kerngeschäft und IT)
Unterrichte die Geschäftsführung über aktuelle technologische Möglichkeiten und künftige Richtungen, über die Möglichkeiten, welche die IT bietet sowie über die durch das Unternehmen zu ergreifenden Maßnahmen, um diese Möglichkeiten nutzen zu können. Stelle sicher, dass das Geschäft, an dem die IT ausgerichtet ist, verstanden wird. Die Geschäfts- und IT-Strategie sollten integriert und allgemein kommuniziert werden; es sollte eine klare Verbindung zwischen Unternehmenszielen, IT-Zielen, erkannten Möglichkeiten und Grenzen des Potentials geben. Identifiziere, in welchen Bereichen die Geschäftsstrategie von der IT kritisch abhängt und vermittle zwischen den Erfordernissen des Kerngeschäfts und der Technologie, damit vereinbarte Prioritäten festgehalten werden können.

PO1.3 Assessment of Current Performance (Bewertung der gegenwärtigen Performance)
Bewerte die Performance der bestehenden Pläne und Informationssysteme auf deren Beitrag zu Geschäftszielen, Funktionalität, Stabilität, Komplexität, Kosten, Stärken und Schwächen.

PO1.4 IT Strategic Plan (Strategischer IT-Plan)
Erstelle in Zusammenarbeit mit den relevanten Stakeholdern einen strategischen IT-Plan, welcher festlegt, inwieweit die IT zu den strategischen Zielen des Unternehmens beiträgt und der die damit verbundenen Kosten und Risiken aufzeigt. Der Plan bestimmt, inwieweit die IT die durch IT ermöglichten Investitionsvorhaben und die operative Leistungserbringung unterstützt. Er definiert, wie die Ziele erreicht und gemessen werden und wie diese durch die Stakeholder formell freigegeben werden. Der strategische IT-Plan sollte das Investitions- und operative Budget, Finanzierungsquellen, die Sourcing-Strategie, die Beschaffungsstrategie, sowie rechtliche und regulatorische Anforderungen abdecken. Der strategische IT-Plan sollte detailliert genug gehalten sein, um die Definition von taktischen IT-Plänen zu ermöglichen.

PO1.5 IT Tactical Plans (Taktische IT-Pläne)
Erstelle ein Portfolio von taktischen IT-Plänen, welche vom strategischen IT-Plan abgeleitet wurden. Diese taktischen Pläne beschreiben notwendige IT-Vorhaben, Anforderungen an Ressourcen und wie die Verwendung von Ressourcen und die Generierung von Nutzen überwacht und gemanaged werden. Die taktischen Pläne sollten genügend detailliert gehalten sein, um die Festlegung von Projektplänen zu ermöglichen. Manage die taktischen Pläne und Initiativen aktiv durch die Analyse von Projekt- und Service-Portfolios. Dies umfasst die regelmäßige Abstimmung von Anforderungen und Ressourcen, den Abgleich derselben mit strategischen und taktischen Zielen und erwartetem Nutzen und das Ergreifen geeigneter Maßnahmen bei Abweichungen.

PO1.6 IT Portfolio Management (IT-Portfoliomanagement)
Manage das Portfolio an IT-unterstützten Investitionsvorhaben, die für die Erreichung der strategischen Unternehmensziele erforderlich sind, aktiv und in Abstimmung mit dem Kerngeschäft, in dem die Programme identifiziert, definiert, evaluiert, priorisiert, ausgewählt, initiiert, gemanaged und gesteuert werden. Dies umfasst auch die Abklärung der erwünschten Geschäftsergebnisse, die Sicherstellung, dass Programmziele die Erzielung der Ergebnisse unterstützten, das Verstehen des Gesamtaufwands, um die Ergebnisse zu erreichen, die Zuweisung klarer Verantwortlichkeiten mit unterstützenden Maßnahmen, die Definition von Projekten innerhalb des Programms, die Bereitstellung von Ressourcen und Finanzmitteln, die Übertragung von Autorität und die Beauftragung von erforderlichen Projekten zu Beginn des Programms.

MANAGEMENT GUIDELINES

PO1 Define a Strategic IT Plan *(Definiere einen strategischen IT-Plan)*

Von	Inputs
PO5	Kosten-/Nutzenbericht
PO9	Risikobewertung
PO10	Aktualisiertes IT-Projektportfolio
DS1	Neue / überarbeitete Anforderungen für Services; Aktualisiertes IT-Service Portfolio
*	Unternehmensstrategie und -prioritäten
*	Programmportfolio
ME1	Performance Inputs für die IT-Planung
ME4	Bericht zum Status der IT-Governance; Strategische Vorgaben des Unternehmens für die IT

Outputs	Nach						
Strategischer IT-Plan	PO2...PO6		PO8	PO9	AI1	DS1	
Taktischer IT-Plan	PO2...PO6		PO9	AI1	DS1		
IT-Projektportfolio	PO5	PO6	PO10	AI6			
IT-Serviceportfolio	PO5	PO6	PO9	DS1			
IT Sourcing-Strategie	DS2						
IT-Beschaffungsstrategie	AI5						

* Input außerhalb COBIT

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Verlinke Kerngeschäftsziele mit den IT Zielen	C	I	A/R	R	C						
Identifiziere kritische Abhängigkeiten und gegenwärtige Performance.	C	C	R	A/R	C	C	C	C	C		C
Erstelle einen strategischen IT-Plan.	A	C	C	R	I	C	C	C	C	I	C
Erstelle einen taktischen IT-Plan.	C	I		A	C	C	C	C	C	R	I
Analysiere Programm-Portfolios und manage Projekt- und Service Portfolios.	C	I	I	A	R	R	C	R	C	C	I

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Zusammenarbeit mit dem Top- und Unternehmensmanagement in der Ausrichtung der strategischen IT-Planung auf die derzeitigen sowie künftigen Unternehmensanforderungen
- Das Verstehen des derzeitigen IT-Potentials
- Übersetzung der strategischen IT-Planung in taktische Pläne
- Die Erstellung eines Schemas für die Priorisierung von Unternehmenszielen, das Unternehmenserfordernisse quantifiziert

treiben

Prozessziele

- Definiere, wie Unternehmensanforderungen in Serviceangebote umgesetzt werden
- Definiere die Strategie, Services anzubieten
- Trage zum Management des Portfolios der IT-utnerstützter Geschäftsinvestitionen bei
- Erstelle Klarheit bezüglich des Einflusses von Risiken auf Ziele und Ressourcen der IT
- Sorge für Transparenz und Verständnis hinsichtlich Kosten, Nutzen, Strategie, Konzepte und Service Levels

treiben

IT-Ziele

- Reagiere auf Geschäftsanforderungen in Übereinstimmung mit der Unternehmensstrategie
- Reagiere auf Anforderungen der Governance entsprechend der Geschäftsführungsvorgaben

werden gemessen durch

Key Performance Indicators

- Verzögerung zwischen der Aktualisierung von strategischen/taktischen Unternehmensplänen und der Aktualisierung von strategischen/taktischen IT-Plänen
- % von Meetings zur strategischen/taktischen IT-Planung mit aktiver Beteiligung von Mitgliedern aus Kernprozessen
- Verzögerung zwischen der Aktualisierung des strategischen zur derjeniger der taktischen IT-Pläne
- % von taktischen IT-Plänen, welche die vorgegebene Struktur/Inhalte einhalten
- % von IT-Vorhaben/Projekten, die durch Kerngeschäftsverantwortlichen getrieben

werden gemessen durch

Key Goal Indicators

- % der IT-Ziele des strategischen IT-Plans, die den strategischen Unternehmensplan unterstützen
- % von IT-Vorhaben des taktischen IT-Plans, die den taktischen Unternehmensplan unterstützen
- % von IT-Projekten im IT-Projektportfolio, die direkt auf den taktischen IT-Plan zurückverfolgt werden können

werden gemessen durch

IT Key Goal Indicators

- Grad der Zustimmung von Kernprozesseignern der strategischen/taktischen IT-Pläne
- Grad der Einhaltung mit Unternehmens- und Governance-Anforderungen
- Grad der Zufriedenheit des Kerngeschäfts mit dem derzeitigen Status (Anzahl, Umfang etc.) von Projekt- und Applikationsportfolio

MATURITY MODEL

PO1 Define a Strategic IT Plan *(Definiere einen strategischen IT-Plan)*

Die Reife des Management des Prozesses *Define a Strategic IT Plan (Definiere einen strategischen IT-Plan)*, der die Geschäftsanforderungen an die IT erfüllt, die Geschäftsstrategie und Governance-Anforderungen zu unterstützen und zu erweitern, unter Wahrung von Transparenz hinsichtlich Nutzen, Kosten und Risiken, ist:

0 Non-existent (nicht existent):
Eine strategische IT-Planung wird nicht durchgeführt. Es existiert beim Management kein Bewusstsein über die Notwendigkeit einer strategischen IT-Planung zur Unterstützung der Unternehmensziele.

1 Initial (initial):
Die Notwendigkeit der strategischen IT-Planung ist dem IT-Management bekannt. Die IT-Planung wird bei Bedarf und in Reaktion auf bestimmte Unternehmensanforderungen durchgeführt. Die strategische IT-Planung wird ab und zu bei IT-Managementmeetings besprochen. Der Abgleich zwischen Unternehmenserfordernissen, Anwendungen und Technologien erfolgt reaktiv und nicht entsprechend einer unternehmensweiten Strategie. Die strategische Risikohaltung wird informell, von Projekt zu Projekt festgelegt.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Die strategische IT-Planung wird bei Bedarf mit dem Unternehmensmanagement ausgetauscht. Die Aktualisierung der IT-Pläne erfolgt als Reaktion zu Anforderungen des Management. Strategische Entscheidungen werden auf Projektbasis getroffen, ohne Übereinstimmung mit einer übergeordneten Strategie der Organisation. Risiko und Nutzen von wesentlichen strategischen Entscheidungen werden intuitiv festgelegt.

3 Defined (definiert):
Eine Richtlinie definiert, wann und wie eine strategische IT-Planung durchzuführen ist. Für die strategische IT-Planung wird ein strukturierter Ansatz verwendet, welcher dokumentiert und an allen Mitarbeitern bekannt ist. Der IT-Planungsprozess ist einigermaßen vernünftig und stellt sicher, dass eine angemessene Planung wahrscheinlich durchgeführt wird. Dennoch liegt die Implementierung des Prozesses im Ermessen einzelner Manager, und es existiert kein Verfahren, den Prozess zu überprüfen. Die übergeordnete IT-Strategie legt durchgängig die Risiken fest, die die Organisation bereit ist, als Innovator oder Nachzügler einzugehen. Die IT-Strategien bezüglich Finanzen, Technik und Personal beeinflussen zunehmend die Anschaffung neuer Produkte und Technologien. Die strategische IT–Planung wird in Meetings des Unternehmensmanagement diskutiert.

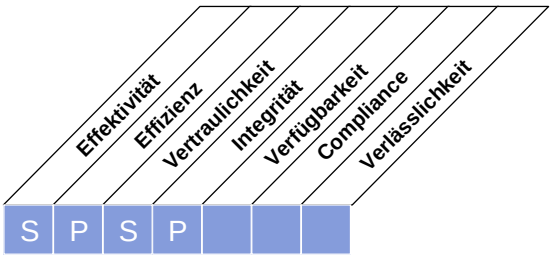
4 Managed and measurable (gemanaged und messbar):
Strategische IT-Planung ist ein Routineverfahren und Ausnahmen würden vom Management erkannt. Die strategische IT-Planung ist eine definierte Management-Tätigkeit mit Verantwortungen im Bereich des Top-Management. Das Management kann den strategischen IT-Planungsprozess überwachen, darauf basierend weise Entscheidungen treffen, sowie die Wirksamkeit des Prozesses messen. Es wird sowohl eine kurzfristige als auch eine langfristige IT-Planung durchgeführt, sie wird innerhalb der Organisation herunter gebrochen und im Bedarfsfall aktualisiert. Die IT-Strategie und die Unternehmensstrategie sind in zunehmenden Maß aufeinander abgestimmt, indem Geschäftsprozesse und wertsteigernde Leistungen behandelt werden, und der Einsatz der Applikationen und Technologien durch Business Process Reengineering verbessert wird. Es gibt einen sauber definierten Prozess zur Bestimmung des Einsatzes von internen und externen Ressourcen, welche für Applikationsentwicklung und Betrieb benötigt werden.

5 Optimised (optimiert):
Die strategische IT-Planung basiert auf einem dokumentierten, lebenden Prozess, der bei der Bestimmung von Unternehmenszielen laufend berücksichtigt wird. Sie resultiert in einem erkennbaren, durch IT-Investitionen beeinflussten Nutzen. Risiko und Wert steigernde Überlegungen werden fortlaufend in den strategischen IT-Planungsprozess eingearbeitet. Es werden realistische langfristige IT-Pläne entwickelt und fortlaufend aktualisiert, um die sich ändernde Technologie und wirtschaftsbezogenen Entwicklungen widerzuspiegeln. Ein Benchmarking mit wohlverstandenen und verlässlichen Branchenwerten findet statt und wird in den Strategieformulierungsprozess integriert. Der strategische Plan beinhaltet, wie neue technologische Entwicklungen die Generierung von neuen Leistungspotentialen im Kerngeschäft antreiben und die Wettbewerbsfähigkeit des Unternehmens verbessern können.

HIGH-LEVEL CONTROL OBJECTIVE

PO2 Define the Information Architecture *(Definiere die Informationsarchitektur)*

Die IT sollte ein Modell zur Abbildung der Informationen im Unternehmen erstellen und laufend aktualisieren und die geeigneten Systeme zur Optimierung der Verwendung dieser Information definieren. Dies umfasst die Entwicklung eines unternehmensweiten Data Dictionary, das die Syntaxregeln, ein Datenklassifikationsschemas und Sicherheitsstufen festlegt. Dieser Prozess verbessert die Qualität der Entscheidungsfindung des Managements, indem sichergestellt wird, dass verlässliche und gesicherte Informationen bereitgestellt werden – und ermöglicht die Rationalisierung der Informationssystem-Ressourcen, um angemessen den Unternehmensstrategien zu entsprechen. Dieser IT-Prozess wird auch benötigt, um die Verantwortung für die Integrität und Sicherheit der Daten zu verbessern, und um die Wirksamkeit und Steuerungsmöglichkeit über die gemeinsame Verwendung von Informationen über Anwendungen und Einheiten zu erhöhen.



Kontrolle über den IT-Prozess,

Define the Information Architecture (*Definiere die Informationsarchitektur*)

der die Anforderung des Unternehmens an die IT bezüglich

der agilen Reaktion auf Anforderungen, verlässliche und stabile Informationen bereitzustellen und Applikationen nahtlos in die Geschäftsprozesse zu integrieren

durch die Konzentration auf

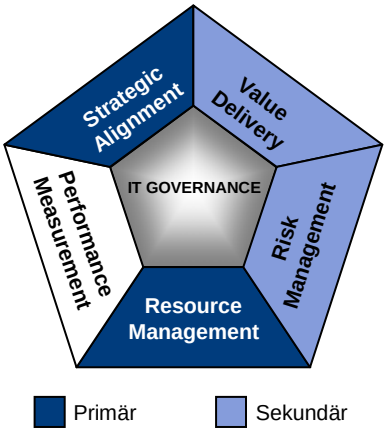
den Aufbau eines unternehmensweiten Datenmodells, welches ein Datenklassifikationsschema für die Gewährleistung der Integrität und Konsistenz aller Daten beinhaltet, *zufrieden stellt,*

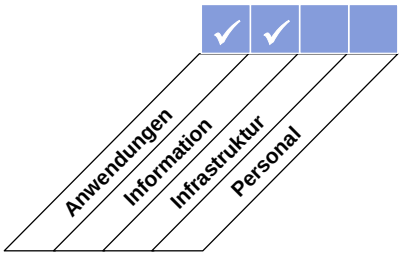
wird erreicht durch

- die Sicherstellung der Genauigkeit der Informationsarchitektur sowie des Datenmodells
- die Zuweisung von Datenverantwortlichkeiten
- die Klassifikation der Informationen unter Anwendung eines vereinbarten Klassifikationsschemas

und gemessen durch

- den Prozentanteil der redundanten/doppelten Datenelemente
- den Prozentanteil der Applikationen, welche nicht den Anforderungen der Informationsarchitektur genügen
- die Häufigkeit der durchgeführten Aktivitäten zur Validierung von Daten





DETAILLIERTE CONTROL OBJECTIVES

PO2 Define the Information Architecture *(Definiere die Informationsarchitektur)*

PO2.1 Information Architecture Model (Informationsarchitekturmodell)
Errichte und unterhalte ein Modell der Unternehmensinformation, um die Entwicklung von Anwendungen und Entscheidungsprozesse zu unterstützen, in Übereinstimmung mit den IT-Plänen wie in PO1 beschrieben. Dieses Modell erleichtert die optimale Errichtung, Verwendung und gemeinsame Benutzung von Informationen durch das Kerngeschäft, und auf eine Art, die die Datenintegrität erhält und dabei flexibel, funktionell, kostengünstig, fristgerecht, sicher und fehlertolerant ist.

PO2.2 Enterprise Data Dictionary and Data Syntax Rules (Unternehmensweites Data Dictionary und Datensyntaxregeln)
Führe ein unternehmensweites Data Dictionary, welches die Datensyntaxregeln der Organisation enthält. Dieses Data Dictionary ermöglicht den gemeinsamen Zugriff auf Datenelemente über Anwendungen und Systeme, fördert unter den IT- und Businessanwendern ein gemeinsames Datenverständnis und verhindert das Entstehen von inkompatiblen Datenelementen.

PO2.3 Data Classification Scheme (Datenklassifikationsschema)
Richte ein im gesamten Unternehmen anwendbares Klassifikationsschema ein, dem die Kritikalität und Sensitivität (zB öffentlich, vertraulich, streng geheim) der Unternehmensdaten zugrunde liegt. Dieses Schema beinhaltet Details über Dateneigentümerschaft, die Festlegung von angemessenen Sicherheitsstufen und Schutzmechanismen und eine kurze Beschreibung der Vorgaben für die Datenaufbewahrung und -zerstörung, Kritikalität und Sensitivität. Das Schema ist Grundlage für die Anwendung von Controls wie zB Zutrittskontrollen, Archivierung oder Verschlüsselung.

PO2.4 Integrity Management (Handhabung der Integrität)
Definiere und implementiere Verfahren zur Sicherstellung der Integrität und Konsistenz aller in elektronischer Form gespeicherten Daten, wie Datenbanken, Data Warehouses und Datenarchiven.

MANAGEMENT GUIDELINES

PO2 Define the Information Architecture *(Definiere die Informationsarchitektur)*

Von	Inputs
PO1	Strategische und taktische IT-Pläne
PO1	Taktischer IT Plan
AI1	Machbarkeitsstudie bezüglich Unternehmenserfordernissen
AI7	Post-Implementation-Review
DS3	Performance- und Kapazitätsinformation
ME1	Performance Inputs für die IT-Planung

Outputs	Nach						
Data Dictionary	AI2	DS11					
Datenklassifikationsschema	AI2						
Informationsarchitektur	DS5	PO3					
Klassifizierte Daten	DS1	DS4	DS5	DS11	DS12		
Optimierter Geschäftsanwendungsplan	AI2	PO3					
Verfahren und Tools zur Klassifikation	*						

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Erstelle und unterhalte ein Modell für Unternehmensinformationen		C	I	A	C		R	C	C		C
Erstelle und unterhalte ein unternehmensweites Data Dictionary				I	C		A/R	R			C
Entwickle und unterhalte ein Datenklassifikationsschema	I	C	A	C	C	I	C	C			R
Stelle Dateneignern Verfahren und Tools für die Klassifizierung von Informationssystemen zur Verfügung	I	C	A	C	C	I	C	C			R
Verwende das Informationsmodell, das Data Dictionary und das Klassifizierungsschema, um optimierte Business Systeme zu planen	C	C	I	A	C		R	C			I

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele
- Sicherstellen der Genauigkeit der Informationsarchitektur sowie des Datenmodells
- Die Zuweisung von Daten-verantwortlichkeiten
- Die Klassifikation von Information unter Anwendung eines vereinbartes Klassifikationsschemas
- Sicherstellen der Konsistenz aus IT-Infrastruktur-Komponenten (Informationsarchitektur, Data Dictionary, Applikationen, Datensyntax, Klassifizierungsschema und Security Levels)
- Aufrechterhalten der Datenintegrität

treiben

Prozessziele
- Führe ein Modell für Unternehmens-informationen
- Reduziere Datenredundanz
- Unterstütze ein effektives Informationsmanagement

treiben

IT-Ziele
- Optimiere die Verwendung von Information
- Integriere die Anwendungen und Technologielösungen nahtlos in Geschäftsprozesse
- Reagiere auf Geschäftsanforderungen in Übereinstimmung mit der Unternehmensstrategie
- Stelle IT-Agilität her

werden gemessen durch

Key Performance Indicators
- Häufigkeit der Updates des Modell für Unternehmensinformationen
- % der Datenelemente, die keinen Eigentümer haben
- Häufigkeit der durchgeführten Aktivitäten zur Validierung von Daten
- Beteiligungsgrad der User Community

werden gemessen durch

Key Goal Indicators
- % der Datenelemente, die nicht Teil des Modells für Unternehmensinformationen sind
- % Nicht-Entsprechung mit dem Datenklassifikationsschema
- % der Applikationen, welche nicht den Informationsarchitekturen entsprechen

werden gemessen durch

IT Key Goal Indicators
- % der zufriedenen User, welche das Modell für Unternehmensinformationen verwenden (zB ist das Data Dictionary benutzerfreundlich?)
- % der redundanten/doppelten Datenelemente

MATURITY MODEL

PO2 Define the Information Architecture *(Definiere die Informationsarchitektur)*

Die Reife des Management des Prozesses *Define the Information Architecture (Definiere die Informationsarchitektur)*, der die Geschäftsanforderungen an die IT erfüllt, rasch auf Anforderungen reagieren zu können, verlässliche und konsistente Informationen zu liefern und Anwendungen lückenlos in die Geschäftsprozesse zu integrieren, ist:

0 Non-existent (nicht existent):
Es existiert kein Bewusstsein für die Bedeutung der Informationsarchitektur für die Organisation. Das für die Entwicklung dieser Architektur nötige Wissen, die Fachkenntnisse sowie die Aufgaben sind im Unternehmen nicht vorhanden.

1 Initial (initial):
Das Management erkennt die Notwendigkeit einer Informationsarchitektur. Die Entwicklung von einzelnen Komponenten der Informationsarchitektur geschieht ad hoc. Die Festlegungen beziehen sich eher auf Daten als auf Informationen und werden durch Angebote von Softwareanbietenden vorgegeben. Über die Notwendigkeit einer Informationsarchitektur wird fallweise und inkonsistent kommuniziert.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Ein Informationsarchitektur-Prozess entwickelt sich und ähnliche, wenn auch informelle und intuitive Verfahren werden von verschiedenen Personen im Untenehmen befolgt. Die Fertigkeiten zur Erstellung der Informationsarchitektur werden durch tägliche Erfahrung und wiederholte Anwendung von Techniken erworben. Taktische Anforderungen bringen die Entwicklung von Komponenten der Informationsarchitektur durch Einzelpersonen voran.

3 Defined (definiert):
Die Bedeutung der Informationsarchitektur wird verstanden und akzeptiert, und die Verantwortung für die Umsetzung ist zugeordnet und klar kommuniziert. Damit im Zusammenhang stehende Verfahren, Werkzeuge und Techniken sind, wenn auch nicht ausgeklügelt, standardisiert und dokumentiert, und sie sind Bestandteil informeller Fortbildungsveranstaltungen. Grundlegende Richtlinien zur Informationsarchitektur inklusive einiger strategischer Erfordernisse sind entwickelt worden, aber die Einhaltung der Richtlinien, Standards und Werkzeuge wird nicht durchgängig eingefordert. Die Stelle eines formell definierten Datenadministrators ist vorhanden, setzt unternehmensweite Standards und beginnt über die Durchführung und Verwendung der Informationsarchitektur zu berichten. Der Einsatz automatisierter Werkzeuge entwickelt sich, aber die verwendeten Prozesse und Regeln werden durch die Vorgaben der Anbieter von Datenbanksoftware bestimmt. Formelle Fortbildungsveranstaltungen werden festgelegt, dokumentiert und konsequent durchgeführt.

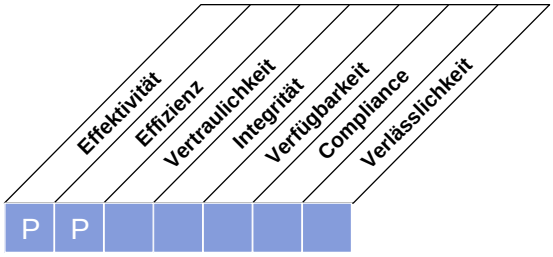
4 Managed and measurable (gemanagt und messbar):
Die Entwicklung und Umsetzung der Informationsarchitektur werden vollständig durch festgelegte Methoden und Techniken unterstützt. Die Verantwortung für die Umsetzung des Architekturenentwicklungsprozesses wird durchgesetzt und der Erfolg der Informationsarchitektur gemessen. Unterstützende automatisierte Werkzeuge sind weit verbreitet, aber noch nicht integriert. Grundsätzliche Messgrößen sind definiert und ein Messsystem ist etabliert. Der Prozess der Festlegung der Informationsarchitektur verläuft proaktiv und konzentriert sich auf künftige Anforderungen des Unternehmens. Die Verantwortlichen der Datenadministration nehmen aktiv an jeder Applikationsentwicklung teil, um die Konsistenz sicherzustellen. Ein automatisiertes Repository ist fertig implementiert. Komplexere Datenmodelle werden implementiert, um den Informationsgehalt der Datenbanken wirksam zu nutzen. Executive Information und Decision Support Systeme verwenden wirksam die verfügbare Information.

5 Optimised (optimiert):
Die Informationsarchitektur ist auf allen Ebenen konsistent umgesetzt. Der Wert der Informationsarchitektur für das Unternehmen wird laufend betont. IT-Mitarbeiter besitzen das notwendige Fachwissen und Qualifikationen für die Entwicklung und Aufrechterhaltung einer robusten und bedarfsgesteuerten Informationsarchitektur, die sämtliche Unternehmenserfordernisse abdeckt. Die von der Informationsarchitektur zur Verfügung gestellten Informationen werden durchgängig und umfassend angewendet. Für die Entwicklung und Instandhaltung der Informationsarchitektur wird von Best Practice Verfahren, einschließlich einem kontinuierlichem Verbesserungsprozess, umfassend Gebrauch gemacht. Die Strategie für die wirksame Verwendung von Informationen durch Data Warehousing- und Data Mining-Technologien ist definiert. Die Informationsarchitektur verbessert sich ständig und berücksicht unübliche Informationen für Prozesse, Organisationen und Systeme.

HIGH-LEVEL CONTROL OBJECTIVE

PO3 Determine Technological Direction *(Bestimme die technologische Richtung)*

Die IT sollte die technologische Ausrichtung zur Unterstützung des Kerngeschäfts festlegen. Dies erfordert die Erstellung eines technologischen Infrastrukturplans und die Einrichtung eines Architekturgremiums, das klare und realistische Erwartungen darüber erzeugt und steuert, was Technologie durch Produkte, Services und Betriebsmechanismen anbieten kann. Der Plan sollte regelmäßig aktualisiert werden und Aspekte wie Systemarchitektur, technologische Ausrichtung, Beschaffungspläne, Standards, Migrationsstrategien und Kontinuitätsvorsorge umfassen. Dies unterstützt die zeitnahe Reaktion auf Änderungen der Wettbewerbsumgebung, Skaleneffekte für Personal und Investitionen sowie verbesserte Interoperabilität von Plattformen und Anwendungen.



Kontrolle über den IT-Prozess,

Determine Technological Direction *(Bestimme die technologische Richtung)*

der die Anforderung des Unternehmens an die IT bezüglich

der Verfügbarkeit von stabilen und kosteneffektiven, integrierten und standardisierten Anwendungssystemen, Ressourcen und Potentialen, die aktuelle und zukünftige Geschäftsanforderungen erfüllen,

durch die Konzentration auf

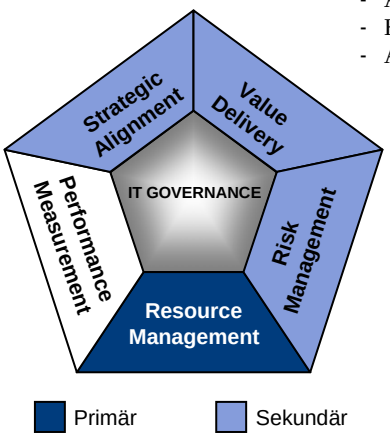
die Festlegung und Implementierung eines technologischen Infrastrukturplans, der Architektur und den Standards, welche technologische Möglichkeiten erkennen und wirksam einsetzen, *zufrieden stellt,*

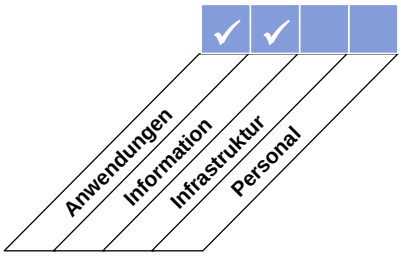
wird erreicht durch

- Aufstellung eines Gremiums, um die Architektur anzuleiten und auf Compliance zu überprüfen
- Erstellung des technischen Infrastrukturplans, welcher Kosten, Risiken und Anforderungen im Gleichgewicht hält
- Festlegung der technischen Infrastrukturstandards, basierend auf den Anforderungen der Informationsarchitektur

und gemessen durch

- Anzahl und Typ der Abweichungen vom technologischen Infrastrukturplan
- Häufigkeit der Reviews/Aktualisierungen des technologischen Infrastrukturplans
- Anzahl der technologischen Plattformen nach Funktion im gesamten Unternehmen





DETAILLIERTE CONTROL OBJECTIVES

PO3 Determine Technological Direction *(Bestimme die technologische Richtung)*

PO3.1 Technological Direction Planning (Planung der technologischen Ausrichtung)
Analysiere bestehende und künftige Technologien und plane, welche technologische Richtung für die Umsetzung der IT-Strategie und der Architektur der Geschäftsanwendungen angemessen ist. Identifiziere im Plan, welche Technologien ein Potential zur Generierung von Geschäftschancen in sich bergen. Der Plan sollte für die Komponenten der Infrastruktur die Systemarchitektur, technologische Richtung, Migrationsstrategien sowie Aspekte im Rahmen der Notfallplanung (engl.: *contingency*) behandeln.

PO3.2 Technical Infrastructure Plan – Scope and Coverage (Technischer Infrastrukturplan – Umfang und Abdeckung)
Erstelle und unterhalte einen technischen Infrastrukturplan, der mit den strategischen und taktischen IT-Plänen abgestimmt ist. Der Plan basiert auf der technologischen Ausrichtung und umfasst Maßnahmen zur Notfallvorkehrung und Vorgaben für die Beschaffung von technischen Ressourcen. Er betrachtet Änderungen im Wettbewerb, Skaleneffekte bei Stellenbesetzung und Investitionen, sowie die verbesserte Interoperabilität von Plattformen und Applikationen.

PO3.3 Monitoring of Future Trends and Regulations (Überwachung von zukünftigen Trends und Bestimmungen)
Entwickle einen Prozess, um Trends von Branche/Sektor, Technologie, Infrastruktur sowie der rechtlichen und regulatorischen Rahmenbedingungen zu überwachen. Berücksichtige die Auswirkungen dieser Trends bei der Erstellung des technologischen IT-Infrastrukturplans.

PO3.4 Technology Standards (Technologische Standards)
Etabliere ein technologisches Forum, das Technologierichtlinien, Beratung zu Infrastrukturprodukten und Anleitung zur Auswahl von Technologien bereitstellt, messe die Compliance mit diesen Standards und Richtlinien, um konsistente, effektive und sichere technische Lösungen unternehmensweit bereitzustellen. Dieses Forum legt technologische Standards und Methoden, basierend auf deren Geschäftsrelevanz, Risiken und Einhaltung externer Anforderungen fest.

PO3.5 IT Architecture Board (IT-Architekturgremium)
Schaffe ein IT-Architekturgremium, das Vorgaben im Bereich der Architektur erstellt und Ratschläge für ihre Anwendung und Einhaltung bereitstellt. Diese Einheit lenkt das Design der IT-Architektur und stellt sicher, dass diese die Unternehmensstrategie unterstützt und die Anforderungen der regulatorischen Compliance und der Notfallplanung berücksichtigt werden. Dies geschieht im Kontext der Unternehmensarchitektur.

MANAGEMENT GUIDELINES

PO3 Determine Technological Direction *(Bestimme die technologische Richtung)*

Von	Inputs
PO1	Strategische und taktische IT-Pläne
PO2	Optimierter Geschäftsanwendungsplan; Informationsarchitektur
AI3	Überarbeitung technologischer Standards
DS3	Performance- und Kapazitätsinformation

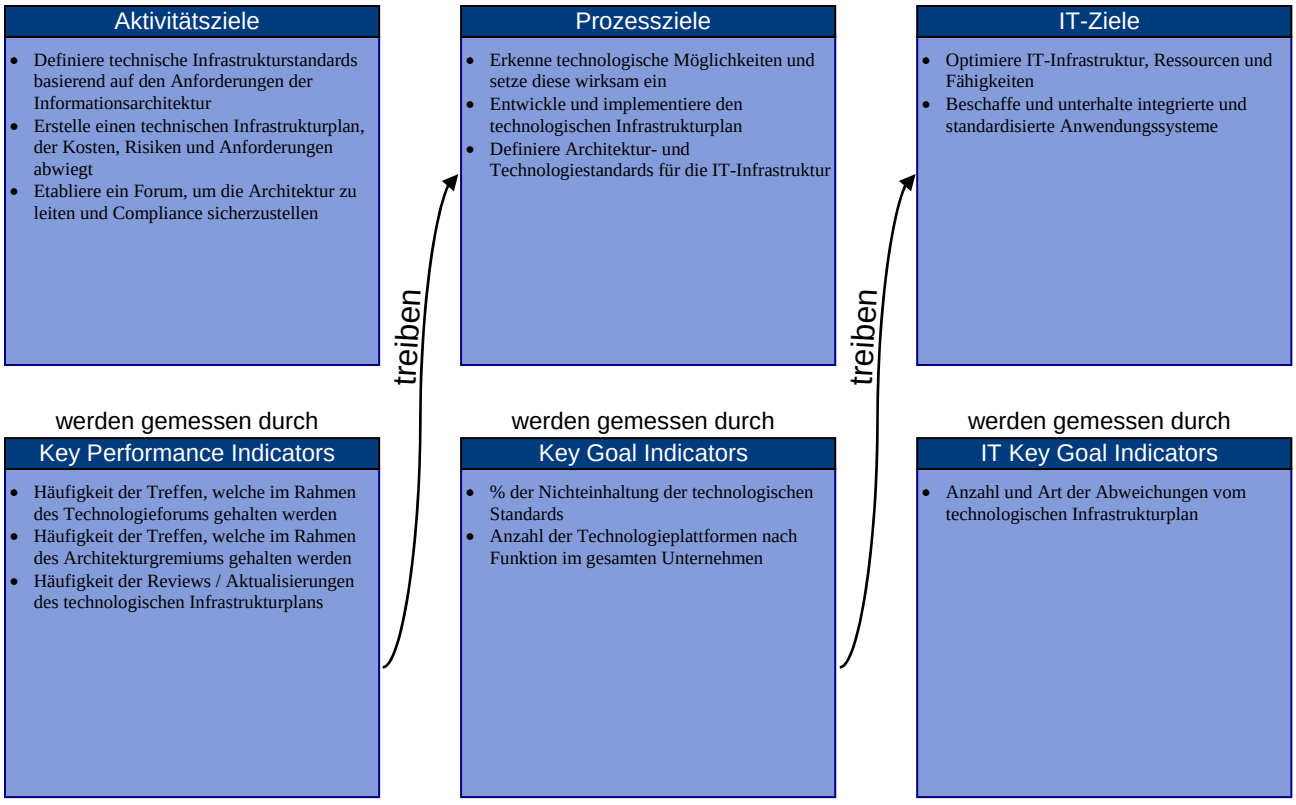
Outputs	Nach						
Anforderungen an Infrastruktur	PO5						
Infrastrukturplan der Technologie	AI3						
Regelmäßige 'state of technology' Aktualisierungen	AI1	AI2	AI3				
Technologiestandards	AI1	AI3	AI7	DS5			
Standards und Möglichkeiten	AI3						

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Erstelle und untererhalte den technologischen Infrastrukturplan		I	I	A		C	R	C	C		C
Erstelle und unterhalte Technologie-Standards				A		C	R	C	I	I	I
Veröffentliche Technologie-Standards		I	I	A		I	R	I	I	I	I
Überwache die technologische Entwicklung		I	I	A		C	R	C		C	C
Definiere die (zukünftige) (strategische) Verwendung neuer Technologien		C	C	A		C	R	C		C	C

RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN



MATURITY MODEL

PO3 Determine Technological Direction *(Bestimme die technologische Richtung)*

Die Reife des Management des Prozesses *Determine Technological Direction (Bestimme die technologische Richtung)*, der die Geschäftsanforderungen an die IT erfüllt, stabile und stabile und kosteneffektive, integrierte und standardisierte Anwendungssysteme, Ressourcen und Potentiale zu haben, welche aktuelle und zukünftige Geschäftsanforderungen erfüllen, ist:

0 Non-existent (nicht existent):
Es gibt kein Bewusstsein über die Wichtigkeit der Planung der technologischen Infrastruktur für das Unternehmen. Das für die Entwicklung eines technologischen Infrastrukturplans erforderliche Wissen und Expertise sind nicht vorhanden. Es fehlt das Verständnis, dass eine Planung für technologische Änderungen notwendig ist, um Ressourcen wirksam zuzuweisen.

1 Initial (initial):
Das Management erkennt die Notwendigkeit, eine Planung der technologischen Infrastruktur durchzuführen. Die Entwicklung technischer Komponenten und die Umsetzung von aufkommenden Technologien erfolgen ad hoc und isoliert. Es gibt eine reaktive und auf den operativen Betrieb fokussierte Herangehensweise für die Planung der Infrastruktur. Die technologische Ausrichtung wird durch oft widersprüchliche Entwicklungspläne der Anbieter von Hardware, Systemsoftware und Applikationen getrieben. Die Kommunikation möglicher Auswirkungen von Änderungen an der Technologie ist inkonsistent.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Die Notwendigkeit und die Wichtigkeit einer technologischen Planung sind kommuniziert. Die Planung ist taktisch und fokussiert auf die technische Lösung von technischen Problemen, anstatt auf die Anwendung von Technologie zur Unterstützung der Unternehmensanforderungen. Die Beurteilung von technologischen Änderungen wird einzelnen Personen überlassen, welche intuitiven, aber ähnlichen Verfahren folgen. Personen erhalten ihre Fähigkeiten bezüglich technologischer Planung durch praktisches Lernen und wiederholtes Anwenden von Techniken. Allgemeine Techniken und Standards entwickeln sich für die Erstellung von Infrastrukturkomponenten.

3 Defined (definiert):
Das Management ist sich der Wichtigkeit des technologischen Infrastrukturplans bewusst. Der Prozess zur Entwicklung des technologischen Infrastrukturplans ist halbwegs vernünftig und ist ausgerichtet auf den strategischen IT-Plan. Es existiert ein definierter, dokumentierter und gut kommunizierter technologischer Infrastrukturplan, der jedoch nicht durchgängig angewandt wird. Die Ausrichtung der technologischen Infrastruktur beinhaltet ein Verständnis darüber, in welchen Belangen bez. Verwendung von Technologie die Organisation führen bzw. nachfolgen möchte. Dies basiert auf Risiken und einer Ausrichtung an der Unternehmensstrategie. Wichtige Anbieter werden, basierend auf dem Verständnis ihrer langfristigen Technologie- und Produktentwicklungspläne ausgewählt, welche mit der Ausrichtung der Organisation übereinstimmen. Es gibt formale Schulungen und Kommunikation von Rollen und Verantwortlichkeiten.

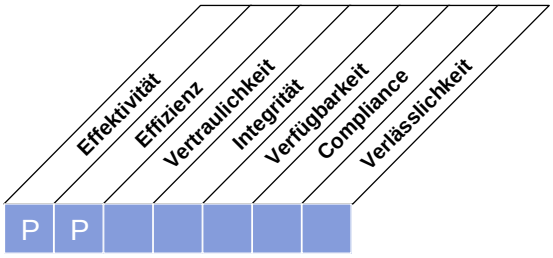
4 Managed and measurable (gemanaged und messbar):
Das Management stellt die Entwicklung und Aufrechterhaltung des technologischen Infrastrukturplanes sicher. IT-Mitarbeiter haben die für die Entwicklung des technologischen Infrastrukturplans notwendige Fachwissen und Fertigkeiten. Die möglichen Auswirkungen von sich ändernden und entstehenden Technologien werden miteinbezogen. Das Management kann Abweichungen vom Plan identifizieren und Probleme vorhersagen. Die Verantwortung für die Entwicklung und Aufrechterhaltung des technologischen Infrastrukturplanes wurde zugewiesen. Der Prozess zur Entwicklung des technologischen Infrastrukturplans ist ausgeklügelt und reagiert auf Änderungen. Interne bewährte Praktiken wurden in den Prozess einbezogen. Die Strategien des Human Resource Management sind an der technologischen Richtung ausgerichtet, um sicherzustellen, dass IT-Mitarbeiter mit technologischen Änderungen umgehen können. Migrationspläne für die Einführung neuer Technologien sind definiert. Outsourcing und Partnering werden wirksam eingesetzt, um auf notwendiges Fachwissen und Fertigkeiten zuzugreifen. Das Management hat die Akzeptanz von Risiken durch den führenden oder folgenden Einsatz von neuen Technologien zur Entwicklung neuer Geschäftsmöglichkeiten oder betrieblichen Nutzeffekten analysiert.

5 Optimised (optimiert):
Es existiert eine Forschungseinheit, die aufkommende und entstehende Technologien untersucht und das Unternehmen gegen Industrienormen beurteilt. Die Ausrichtung des technologischen Infrastrukturplanes wird an Stelle von Technologieanbietern durch Industrie- und internationale Standards und -Entwicklungen getrieben. Die möglichen geschäftlichen Auswirkungen von technologischen Änderungen werden auf hoher Führungsebene untersucht. Bei einer neuen oder geänderten technologischen Richtung gibt es eine formale Genehmigung auf Ebene der Geschäftstleitung. Das Unternehmen besitzt einen robusten technologischen Infrastrukturplan, der die Geschäftsanforderungen widerspiegelt und geändert werden kann, falls sich Änderungen in der Geschäftsumgebung ergeben. Es gibt einen permanenten und durchgesetzten Prozess, um den technologischen Infrastrukturplan zu verbessern. Industrie Best Practices werden umfassend angewandt, um die technische Richtung zu bestimmen.

HIGH-LEVEL CONTROL OBJECTIVE

PO4 Define the IT Processes, Organisation and Relationships *(Definiere die IT-Prozesse, Organisation und Beziehungen)*

Eine IT-Organisation muss unter Berücksichtigung der Anforderungen für Personal, Qualifikationen, Funktionen, Verantwortung, Entscheidungsbefugnis, Rollen, Zuständigkeiten und Überwachung festgelegt werden. Diese Organisation muss in ein IT-Prozess-Framework integriert werden, welches Transparenz und Steuerung sowie die Beteiligung der Geschäftsführung und Unternehmensleitung sicherstellt. Ein IT-Strategieausschuss sollte sicherstellen, dass die Unternehmensleitung die IT beaufsichtigt und mindestens ein Steering Committee etabliert ist, an denen Mitglieder der Kerngeschäftsprozesse und IT teilnehmen, und das die Priorisierung von IT-Ressourcen in Übereinstimmung mit den Unternehmensanforderungen vornimmt. Prozesse, administrative Richtlinien und Verfahren müssen für alle Funktionen festgelegt werden, wobei eine spezielles Augenmerk auf Steuerung, Qualitätssicherung, Risikomanagement, Informationssicherheit, Eigentümerschaft für Daten und Systeme sowie Funktionstrennung gelegt wird. Um eine zeitnahe Unterstützung der Geschäftsanforderungen sicherzustellen, muss die IT in die relevanten Entscheidungsprozesse involviert sein.



Kontrolle über den IT-Prozess,

Define the IT processes, organisation and relationships (*Definiere IT-Prozesse, Organisation und Beziehungen*)

der die Anforderung des Unternehmens an die IT bezüglich

der agilen Reaktion auf die Unternehmensstrategie, die ebenso Governance-Anforderungen erfüllt und festgelegte und kompetente Anlaufstellen anbietet,

durch die Konzentration auf

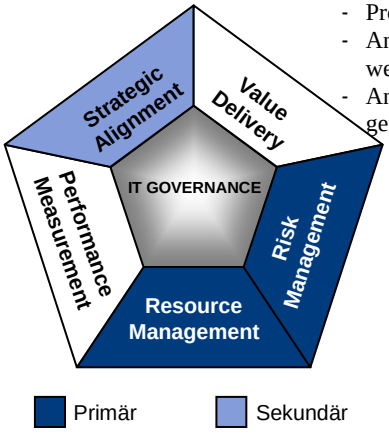
die Erstellung von transparenten, flexiblen und reagierenden IT-Organisationsstrukturen und die Definition und Umsetzung von IT-Prozessen mit EignerInnen, Rollen und Verantwortlichkeiten, die in die Entscheidungsprozesse des Unternehmen eingebunden sind, *zufrieden stellt,*

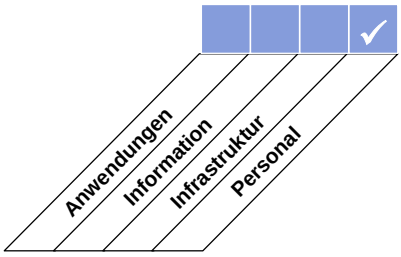
wird erreicht durch

- Festlegung eines Frameworks der IT-Prozesse
- Aufstellung von angemessenen Organisationseinheiten und -strukturen
- Festlegung von Rollen und Verantwortlichkeiten

und gemessen durch

- Prozent der Rollen mit dokumentierten Stellenbeschreibungen und Befugnissen
- Anzahl der Unternehmenseinheiten/-prozesse, die nicht durch die IT unterstützt werden, die aber gemäß der Strategie unterstützt werden sollten
- Anzahl der wesentlichen IT-Aktivitäten außerhalb der IT-Organisation, die nicht genehmigt sind oder die nicht den IT-Organisationsstandards entsprechen





DETAILLIERTE CONTROL OBJECTIVES

PO4 Define the IT Processes, Organisation and Relationships *(Definiere die IT-Prozesse, Organisation und Beziehungen)*

PO4.1 IT Process Framework (Framework der IT-Prozesse)
Definiere ein Framework der IT-Prozesse, um den strategischen IT-Plan umzusetzen. Dieses Framework umfasst die Struktur und Beziehung von IT-Prozessen (zB um Lücken und Überlappungen bei den Prozessen zu managen), Eigentümerschaft, Reifegrad, Messung der Performance, Verbesserung, Compliance, Qualitätsziele und Pläne, um diese zu erreichen. Es bildet die Integration der IT-spezifischen Prozesse, der Prozesse im Unternehmensmanagement, Geschäftsprozesse und den Change Prozessen des Unternehmens. Das Framework der IT-Prozesse sollte in ein Qualitätsmanagementsystem und ein Framework der Internal Controls integriert sein.

PO4.2 IT Strategy Committee (IT-Strategieausschuss)
Etabliere einen IT-Strategieausschuss auf Ebene der Unternehmensleitung. Dieser Ausschuss stellt sicher, dass IT-Governance, als Teil der Corporate Governance angemessen adressiert wird. Er berät bei der strategischen Ausrichtung und beurteilt im Namen der Unternehmensleitung wesentliche Investitionen.

PO4.3 IT Steering Committee (IT-Lenkungsausschuss)
Etabliere einen IT-Lenkungsausschuss (oder ein äquivalentes Gremium), das sich aus Mitgliedern der Unternehmensleitung, Kerngeschäftsprozess- und IT-Management zusammensetzt, um,

- die Prioritäten der durch IT unterstützten Programme in Abstimmung mit der Unternehmensstrategie und deren Prioritäten festzulegen,
- Stati von Projekten zu verfolgen und Ressourcenkonflikte zu lösen und
- die Service-Levels und Verbesserung von Services zu monitoren.

PO4.4 Organisational Placement of the IT Function (Organisatorische Eingliederung der IT-Organisation)
Platziere die IT-Organisationseinheit in die Gesamtorganisation unter Beachtung der Bedeutung der IT für das Unternehmen, speziell deren Kritikalität für die Unternehmensstrategie und die Abhängigkeit des operativen Betriebs von der IT. Die Stelle, an die der/die CIO berichtet, entspricht der Bedeutung der IT im Unternehmen.

PO4.5 IT Organisational Structure (IT-Organisationsstruktur)
Entwickle eine interne und externe IT-Organisationsstruktur, die die Unternehmenserfordernisse widerspiegelt. Etabliere außerdem einen Prozess, der periodisch die IT-Organisationsstruktur überprüft, um die Anforderungen an die Personalausstattung und die Beschaffungsstrategien den erwarteten Unternehmenszielen und sich ändernden Umständen anzugleichen.

PO4.6 Roles and Responsibilities (Rollen und Verantwortlichkeiten)
Definiere und kommuniziere Rollen und Verantwortlichkeiten für alle Mitarbeiter der Organisation, die mit Informationssystemen in Verbindung stehen, um ausreichend Autorität für die Umsetzung der festgelegten Rollen und Verantwortlichkeiten zu ermöglichen. Erstelle Rollenbeschreibungen und aktualisiere diese regelmäßig. Diese beschreiben sowohl Autorität als auch Verantwortung, umfassen eine Festlegung der Kenntnisse und Erfahrungen, die für die Position erforderlich sind, und können auch geeignet für die Performancebeurteilungen. Rollenbeschreibungen sollten die Verantwortung für Internal Control umfassen.

PO4.7 Responsibility for IT Quality Assurance (Verantwortung für IT-Qualitätssicherung)
Weise die Verantwortung für die Ausführung der Qualitätssicherungsfunktion zu und statte die Qualitätssicherungsgruppe mit geeignetem Qualitätssicherungssystemen, Controls und Kommunikationsexpertise aus. Die organisatorische Eingliederung, die Verantwortlichkeiten und Größe der Qualitätssicherungsgruppe stellt den Bedarf der Organisation sicher.

PO4.8 Responsibility for Risk, Security and Compliance (Verantwortung für Risiko, Sicherheit und Compliance)
Verankere Eigentümerschaft und Verantwortung für IT-bezogene Risiken im Kerngeschäft auf angemessen hoher Ebene. Definiere und weise Rollen zu, die für das Management von IT-Risiken kritisch sind, inklusive spezifischer Verantwortung für Informationssicherheit, physische Sicherheit und Compliance. Etabliere die Verantwortlichkeit für Risiko- und Sicherheitsmanagement auf unternehmensweiter Ebene, um unternehmensweite Belange zu regeln. Weitere Verantwortlichkeiten für Sicherheitsmanagement können bei Bedarf systemspezifisch zugewiesen werden, um relevante Sicherheitsbelange zu behandeln. Hole von der Geschäftsführung die grundsätzliche Stossrichtung hinsichtlich der IT-Risikobereitschaft und die Freigabe von IT-Restrisiken ein.

PO4.9 Data and System Ownership (Daten- und Systemeignerschaft)
Unterstütze das Kerngeschäft mit Verfahren und Werkzeugen, um die Übernahme der Eigentümerschaft für Daten- und Informationssysteme zu ermöglichen. Eigner fällen Entscheidungen hinsichtlich der Klassifikation von Informationen und Systemen und dem der Klassifikation entsprechenden Schutz.

PO4.10 Supervision (Beaufsichtigung)
Bette angemessene Verfahren zur Beaufsichtigung in die IT-Organisation ein, um sicherzustellen, dass Rollen und Verantwortlichkeiten korrekt ausgeführt werden, um beurteilen zu können, ob das Personal ausreichende Autorität und Ressourcen zur Übernahme ihrer Rollen und Verantwortlichkeiten besitzen, und, um allgemein die Key Performance Indicators überblicken zu können.

PO4.11 Segregation of Duties (Funktionstrennung)
Etabliere eine Trennung von Rollen und Verantwortlichkeiten, die die Wahrscheinlichkeit reduziert, dass eine Einzelperson einen kritischen Prozess untergräbt. Das Management stellt weiters sicher, dass das Personal ausschließlich genehmigte, ihrer Stelle und Position entsprechende Aktivitäten ausführt.

PO4.12 IT Staffing (Stellenbesetzung der IT)
Evaluiere Anforderungen an die Stellenbesetzung regelmäßig oder nach wesentlichen Änderungen im Unternehmen, Betrieb oder der IT-Umgebung, um sicher zu stellen, dass die IT-Organisation eine ausreichende Zahl kompetenter Mitarbeiter hat. Die Stellenbesetzung beachtet auch Zusammenarbeit zwischen Unternehmens- und IT-Personal, funktionsübergreifende Ausbildung, Job Rotation und Möglichkeiten zum Outsourcing.

PO4.13 Key IT Personnel (Schlüsselpersonal der IT)
Bestimme und identifiziere Schlüsselpersonal der IT und minimiere die übermäßige Abhängigkeit von diesen. Ein Plan sollte existieren, um im Notfall mit ihnen Kontakt aufnehmen zu können.

PO4.14 Contracted Staff Policies and Procedures (Policies und Verfahren für beigezogenes Personal)
Definiere Policies und Verfahren für die Steuerung der Aktivitäten von Consultants und anderem Vertragspersonal der IT-Funktion, um sicher zu stellen, dass der Schutz der Informationen und Informationssysteme der Organisation gewährleistet ist und die vertraglichen Vereinbarungen erreicht werden.

PO4.15 Relationships (Beziehungen)
Erstelle und unterhalte eine optimale Koordinations-, Kommunikations- und Verbindungsstruktur zwischen der IT-Organisation und den verschiedenen anderen Interessen innerhalb und außerhalb der IT, wie beispielsweise die Geschäftsführung, Bereichsleiter, Unternehmenseinheiten, einzelne User, Lieferanten, Security Officers, Risk Manager, die unternehmensweite Compliance Gruppe, Outsourcer und Management von ausgelagerten Einheiten.

Diese Seite wurde absichtlich freigelassen

MANAGEMENT GUIDELINES

PO4 Define the IT Processes, Organisation and Relationships *(Definiere die IT-Prozesse, Organisation und Beziehungen)*

Von	Inputs
PO1	Strategische und taktische IT-Pläne
PO7	Personalrichtlinien und -verfahren der IT, IT Skills Matrix, Stellenbeschreibungen
PO8	Aktivitäten zur Qualitätsverbesserung
PO9	IT-bezogene Risikominderungs-Pläne
ME1	Plan der Verbesserungsmaßnahmen
ME2	Report zur Wirksamkeit von IT Controls
ME3	Katalog rechtlicher und regulatorischer Anforderungen in Bezug auf die IT-Service-Delivery
ME4	Verbesserungen des Prozess Frameworks

Outputs	Nach						
Dokumentierte Rollen und Verantwortlichkeiten	PO7						
Dokumentierte Systemeigner	AI7	DS6					
Organisation und Beziehungen der IT	PO7						
IT-Prozess-Framework	ME4						
IT-Prozess-Framework, dokumentierte Rollen und Verantwortlichkeiten	ALL						

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Erstelle IT Organisationsstrukturen, inklusive Ausschüssen und Verbindungen zu Stakeholdern und Anbietern	C	C	C	A		C	C	C	R	C	I
Designe das Framework für IT-Prozesse	C	C	C	A		C	C	C	R	C	C
Identifiziere SystemeignerInnen		C	C	A	C	R	I	I	E	I	I
identifiziere DateneignerInnen		I	A	C	C	I	R	I	E	I	C
Erstelle und implementiere IT-Rollen und Verantwortlickeiten, inklusive Beaufsichtigung und Funktionstrennung		I	I	A	I	C	C	C	R	C	C

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Festlegung eines Frameworks der IT-Prozesse
- Entwicklung von geeigneten Organisationseinheiten und -strukturen

treiben

Prozessziele

- Entwickle flexible und reagierende IT Organisationsstrukturen und Beziehungen
- Definiere klar EignerInnen, Rollen und Verantwortlichkeiten für alle IT Prozesse und Beziehungen zu Stakeholdern

treiben

IT-Ziele

- Reagiere auf Anforderungen der Governance entsprechend der Geschäftsführungs-vorgaben
- Reagiere auf Geschäftsanforderungen in Übereinstimmung mit der Unternehmens-strategie
- Stelle IT-Agilität her

werden gemessen durch

Key Performance Indicators

- % der Rollen mit dokumentierten Stellen-beschreibungen und Befugnissen
- Anzahl der IT-Betriebsfunktionen/-prozesse, die mit den Unternehmensbetriebsstrukturen verknüpft sind
- Frequenz der Meetings der Strategie- und Lenkungsausschüsse

werden gemessen durch

Key Goal Indicators

- Anzahl der aus Optik der Funktionstrennung widersprüchlichen Verantwortlichkeiten
- Anzahl der Eskalationen oder ungelösten Vorfälle auf Grund von mangelnder oder nicht ausreichend zugewiesener Verantwortung
- % der Stakeholder, die mit der Reaktivität (engl.: *responsiveness*) der IT zufrieden sind

werden gemessen durch

IT Key Goal Indicators

- Zufriedenheit der Stakeholder (Befragungen)
- Anzahl der Vorhaben, die auf Grund der Trägheit der IT oder Nichtverfügbarkeit der entsprechenden Leistungen verzögert wurden
- Anzahl der Geschäftsprozesse, die nicht durch die IT-Organisation unterstützt werden, obwohl sie gemäss Strategie unterstützt sein sollten
- Anzahl der wesentlichen IT-Aktivitäten außerhalb der IT-Organisation, die nicht bewilligt sind oder die nicht den IT-Organisationsstandards unterstehen

MATURITY MODEL

PO4 Define the IT Processes, Organisation and Relationships *(Definiere die IT-Prozesse, Organisation und Beziehungen)*

Die Reife des Management des Prozesses *Define the IT Processes, Organisation and Relationships (Definiere die Prozesse, Organisation und Beziehungen der IT)*, der die Geschäftsanforderungen an die IT erfüllt, agil auf die Unternehmensstrategie reagieren zu können und dabei die Governance-Anforderungen erfüllt und festgelegte und kompetente Anlaufstellen anbietet, ist:

0 Non-existent (nicht existent):
Die IT-Organisation ist nicht wirksam aufgestellt, um sich auf die Erreichung der Unternehmensziele zu konzentrieren.

1 Initial (initial):
Die Aktivitäten und Organisationseinheiten der IT sind reaktiv und in inkonsistenter Form implementiert. Die Involvierung der IT in Unternehmensprojekte erfolgt erst in späteren Phasen. Die IT-Organisation wird als Unterstützungsfunktion, ohne eine gesamthafte Organisationsperspektive angesehen. Es besteht ein implizites Verständnis für den Bedarf nach einer IT-Organisation – jedoch werden Rollen und Verantwortlichkeiten weder formalisiert noch durchgesetzt.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Die IT-Organisation ist dergestalt organisiert, dass sie taktisch, aber inkonsistent auf Kundenbedürfnisse und Beziehungen mit Lieferanten reagiert. Der Bedarf für eine strukturierte Organisation und Lieferanten-Management ist kommuniziert, aber Entscheidungen sind immer noch von Wissen und Fähigkeiten von Schlüsselpersonen abhängig. Es entwickeln sich grundlegende Verfahren, um die IT-Organisation und Beziehungen zu Lieferanten zu managen.

3 Defined (definiert):
Festgelegte Rollen und Verantwortlichkeiten bestehen für die IT-Organisation und Drittparteien. Die IT-Organisation wurde entsprechend der IT-Strategie entwickelt, dokumentiert und kommuniziert. Das Internal Control Environment ist festgelegt. Es besteht eine Formalisierung der Beziehungen mit anderen Parteien, inklusive Lenkungsausschüsse, Internal Audit und Lieferanten-Management. Die IT-Organisation ist funktional gesehen vollständig. Es bestehen Definitionen der von der IT und von Usern auszuführenden Funktionen. Wichtige Erfordernisse hinsichtlich Stellenbesetzung und Fähigkeiten sind festgelegt und werden erreicht. Es besteht eine formale Definition der Beziehungen mit Usern und Drittparteien. Die Trennung von Funktionen und Verantwortlichkeiten ist festgelegt und wird umgesetzt.

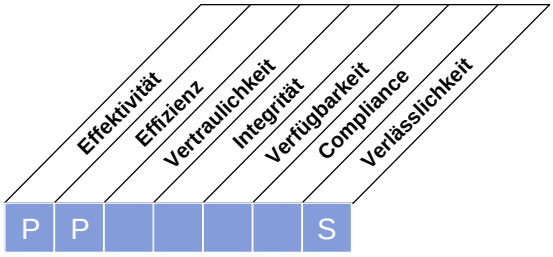
4 Managed and measurable (gemanaged und messbar):
Die IT-Organisation reagiert proaktiv auf Änderungen und enthält alle Rollen, die notwendig sind, um die Unternehmenserfordernisse zu erfüllen. IT-Management, Prozesseigner, Verantwortung und Zuständigkeit sind festgelegt und ausgewogen. Interne Good Practices wurden für die Organisation der IT umgesetzt. Das IT-Management besitzt die notwendige Fachkenntnisse und Fähigkeiten, um die erwünschte Organisation und Beziehungen zu definieren, umzusetzen und zu monitoren. Messbare Größen zur Unterstützung der Unternehmensziele und von Usern festgelegte Erfolgsfaktoren sind standardisiert. Eine Übersicht der vorhandenen Fachkenntnisse ist verfügbar, um die Besetzung von Stellen in Projekten und die Entwicklung des Personals zu unterstützen. Die Balance zwischen intern vorhandenen und von extern beizuziehenden Fähigkeiten ist festgelegt und wird durchgesetzt. Die Organisationsstruktur der IT entspricht dem Unternehmensbedarf, in dem die Bereitstellung von Services den strategischen Unternehmensanforderungen und nicht isolierten Technologien folgt.

5 Optimised (optimiert):
Die Organisationsstruktur der IT ist flexibel und adaptiv. Best Practices der Industrie werden angewandt. Technologie wird in hohem Maß eingesetzt, um das Monitoring der Performance der Organisation und Prozesse der IT zu unterstützen. Ein kontinuierlicher Verbesserungsprozess ist im Einsatz.

HIGH-LEVEL CONTROL OBJECTIVE

PO5 Manage the IT Investment *(Manage IT-Investitionen)*

Erstelle und unterhalte ein Framework zum Management der Investitionsprogramme, an denen IT beteiligt ist. Dieses umfasst Kosten, Nutzen, Priorisierung innerhalb des Budgetrahmens, einen formalen Budgetierungsprozess und eine Budgetverwaltung. Arbeite mit den Stakeholdern zusammen, um in Abstimmung mit den strategischen und taktischen IT-Plänen die Gesamtkosten und den Gesamtnutzen zu identifizieren und zu steuern, und notwendige Maßnahmen bei Bedarf initiieren zu können. Der Prozess stärkt die Partnerschaft zwischen der IT und den Stakeholdern des Kerngeschäfts, ermöglicht die wirksame und wirtschaftliche Verwendung von IT-Ressourcen und generiert Transparenz und Verantwortung für die Total-Cost-of-Ownership, die Realisierung von Wertbeiträgen und den Return-on-Investment für Investitionen, an denen IT beteiligt ist.



Kontrolle über den IT-Prozess,

Manage the IT Investment (*Manage IT Investitionen*)

der die Anforderung des Unternehmens an die IT bezüglich

der kontinuierlichen und nachweisbaren Verbesserung der Kosteneffizienz von IT und deren Beitrag zur Rentabilität durch die, den Erwartungen der Endbenutzer entsprechende, integrierte und standardisierte Services

durch die Konzentration auf

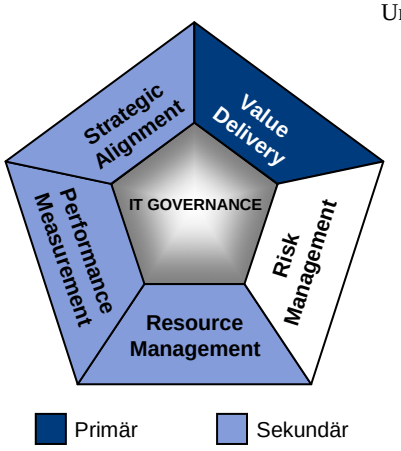
wirksame und wirtschaftliche Entscheidungen zu IT-Investitionen und Portfolios und durch Festlegung und Verfolgung des IT-Budgets im Einklang mit der IT-Strategie und den Investitionsentscheidungen, *zufrieden stellt,*

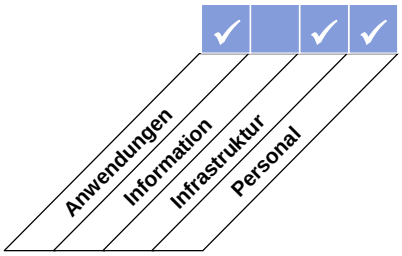
wird erreicht durch

- Planung und Freigabe eines Budgets
- Festlegung formaler Investitionskriterien (ROI, Amortisationszeit, NPV)
- Messung des Wertbeitrags und Bewertung gegen die Prognose

und gemessen durch

- prozentuelle Reduktion der Stückkosten der erbrachten IT-Services
- Prozentanteil der Budgetabweichung verglichen mit dem Gesamtbudget
- prozentueller Anteil der IT-Ausgaben, ausgedrückt in Werttreibern des Unternehmens (zB Verkaufswachstum infolge erhöhter Konnektivität)





DETAILLIERTE CONTROL OBJECTIVES

PO5 Manage the IT-Investment *(Manage IT-Investitionen)*

PO5.1 Financial Management Framework (Framework für das Management von Finanzen)
Entwickle ein finanzielles Framework IT, das den Budgetierungsprozess und Kosten-/Nutzenanalysen vorantreibt und das auf Portfolios für Investitionen, Services und Anlagen aufgebaut ist. Unterhalte das Portfolio IT-gestützter Investitionsprogramme, IT-Services und IT-Werten, das die Basis für das aktuelle IT-Budget darstellt. Liefere dem Kerngeschäft einen Input für Neu-Investitionen unter Berücksichtigung der aktuellen IT-Werte und IT Service Portfolios. Neuinvestitionen und Unterhalt von Service- und Asset Portfolios haben einen Einfluss auf künftige IT-Budgets. Kommuniziere die Kosten- und Nutzenaspekte dieser Portfolios in den Budgetpriorisierungs-, Kostenmanagement- und Nutzenmanagement-Prozessen.

PO5.2 Priorisation Within IT Budget (Priorisierung innerhalb des IT-Budgets)
Implementiere einen Entscheidungsfindungsprozess, der die Zuordnung der IT-Ressourcen für den laufenden Betrieb, Projekte und Unterhalt priorisiert. Dies mit dem Ziel, den Beitrag von IT-gestützten Investitionsprogrammen und anderer IT-Services und IT–Werten zu maximieren.

PO5.3 IT Budgeting Process (IT-Budgetierungsprozess)
Führe einen Prozess zur Erstellung und Steuerung des Budgets ein, der die Prioritäten für IT-unterstützte Investitionsprogramme widerspiegelt und die laufenden Kosten für Betrieb und Unterhalt der bestehenden Infrastruktur umfasst. Der Prozess sollte die Entwicklung eines gesamthaften IT-Budgets, sowie jenes von individuellen Programmen unterstützen, und sich auf die jeweiligen IT-Komponenten dieser Programme konzentrieren. Der Prozess sollte den laufenden Review, Anpassungen und Freigaben von Gesamtbudgets und Budgets für einzelne Programme ermöglichen.

PO5.4 Cost Management (Kostenmanagement)
Etabliere einen Kostenmanagement-Prozess, der die aktuellen Kosten mit dem Budget vergleicht. Kosten sollten überwacht und berichtet werden. Eventuelle Abweichungen sollten rechtzeitig identifiziert und deren Auswirkungen auf Programme beurteilt werden. Gemeinsam mit den Programm-Sponsoren aus den Kerngeschäftsprozessen sollten geeignete Sanierungsmaßnahmen definiert werden, gegebenenfalls sollte der Business-Case angepasst werden.

PO5.5 Benefit Management (Nutzenmanagement)
Implementiere einen Prozess, der den Nutzen monitort. Der von der IT erwartete Beitrag zu den Geschäftsergebnissen, entweder als Komponente von IT-unterstützten Investitions-Programmen oder als Teil der regelmäßigen Betriebsunterstützung, sollte identifiziert, vereinbart, gemonitort und berichtet werden. Die Reports sollten einem Review unterzogen werden und, wo die Möglichkeit einer Erhöhung des IT-Beitrags besteht, sollten geeignete Aktionen festgelegt und durchgeführt werden. Wenn sich der Beitrag der IT zum Programm ändert oder wo Änderungen anderer Projekte das Programm beeinflussen, sollte der Business-Case des Programms aktualisiert werden.

MANAGEMENT GUIDELINES

PO5 Manage the IT Investment *(Manage IT-Investitionen)*

Von	Inputs
PO1	Strategische und taktische IT-Pläne, Projektportfolio, IT-Serviceportfolio
PO3	Anforderungen an Infrastruktur
PO10	Aktualisiertes IT-Projektportfolio
AI1	Machbarkeitsstudie bezüglich Unternehmens-erfordernisse
AI7	Post-Implementation-Review
DS3	Performance- und Kapazitätsplan (Anforderungen)
DS6	IT-Finanzen
ME4	Erwarteter Wertbeitrag von IT-unterstützten Investitionen im Kerngeschäft

Outputs	Nach						
Kosten-/Nutzenbericht	PO1	AI2	DS6	ME1	ME4		
IT-Budgets	DS6						
Aktualisiertes IT-Serviceportfolio	DS1						
Aktualisiertes IT-Projektportfolio	PO10						

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Unterhalte das Programm-Portfolio	A	R	R	R	C					I	I
Unterhalte das Projekt-Portfolio	I	C	A/R	A/R	C		C	C		C	I
Unterhalte das Service-Portfolio	I	C	A/R	A/R	C	C				C	I
Entwickle und unterhalte einen IT-Budgetierungsprozess	I	C	C	A/R		C	C	C	R	C	
Identifiziere, kommuniziere und monitore IT-Investitionen, Kosten und Wertbeiträge für das Unternehmen	I	C	C	A/R		C	C	C	R	C	C

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Festlegung formaler Investitionskriterien (ROI, Amortisationszeit, NPV)
- Planung und Freigabe eines Budgets
- Messung des Wertbeitrags und Bewertung gegen die Prognose

treiben

Prozessziele

- Ermöglichen von IT-Investitions- und Portfolioentscheidungen
- Setzen und verfolgen des IT-Budgets in Übereinstimmung mit der IT-Strategie und den IT-Investitionsentscheidungen
- Optimierung von IT-Kosten und Maximierung des IT-Nutzens

treiben

IT-Ziele

- Verbessere die Kosteneffizienz der IT und ihren Beitrag zum Unternehmenserfolg
- Stelle Transparenz von und Verständnis für IT-Kosten, Nutzen, Strategie, Richtlinien und Service Levels sicher
- Stelle sicher, dass die IT eine kosteneffiziente Servicequalität, eine kontinuierliche Verbesserung und Bereitschaft für zukünftige Veränderungen zeigt

werden gemessen durch

Key Performance Indicators

- Prozent der Projekte mit vorab definierten Nutzen
- Prozent der bepreisten IT-Services
- Prozent der Projekte mit einem nachträglichen Review
- Frequenz des Nutzenreporting
- Prozent der Projekte, von denen eine Performance-Information (Kosten-performance, Planungsperformance und Risikoprofil) verfügbar ist

werden gemessen durch

Key Goal Indicators

- Anzahl von Budgetabweichungen
- % der Budgetabweichung verglichen mit dem Gesamtbudget
- % der Reduktion der Stückkosten bei erbrachten IT-Services
- % der IT Investitionen, die den vorab definierten Nutzen erbringen

werden gemessen durch

IT Key Goal Indicators

- % der IT-Investitionen, die den vorab bestimmten Geschäftsnutzen erreichen oder übertreffen
- % der IT Value Driver abgebildet auf die Business Value Driver
- % der IT-Ausgaben im Verhältnis zu Business Value Driver (z.B.: Verkaufs-wachstum infolge erhöhter Konnektivität)

MATURITY MODEL

PO5 Manage the IT Investment *(Manage IT-Investitionen)*

Die Reife des Management des Prozesses *Manage the IT Investment (Manage IT-Investitionen), der* die Geschäftsanforderungen an die IT erfüllt der kontinuierlichen und nachweisbaren Verbesserung der Kosteneffizienz der IT und deren Beitrag zur Rentabilität durch die, den Erwartungen der Endbenutzer entsprechende, integrierte und standardisierte Service ist:

0 Non-existent (nicht existent):
Es existiert kein Bewusstsein für die Bedeutung der Auswahl von Investitionen und Budgetierung der IT. Investitionen und Ausgaben der IT werden nicht verfolgt oder gemonitort.

1 Initial (initial):
Das Unternehmen erkennt den Bedarf für ein Management der IT-Investitionen, aber dieser wird inkonsistent kommuniziert. Die Zuweisung der Verantwortlichkeiten für die Auswahl von Investitionen und die Budgetentwicklung der IT erfolgt durch einen ad-hoc Ansatz. Isolierte Umsetzungen für die Auswahl von Investitionen und Budgetierung der IT erfolgt mit informeller Dokumentation. IT-Investitionen werden auf einer ad-hoc Basis begründet. Reaktive und kurzfristige Budgetentscheidungen werden getroffen.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Es besteht ein grundsätzliches Bewusstsein für den Bedarf einer richtigen Auswahl und Budgetierung von IT-Investitionen vorhanden. Der Bedarf für einen Auswahl- und Budegtierungsprozess wird kommuniziert. Dessen Einhaltung ist der Initiative von Einzelpersonen im Unternehmen überlassen. Allgemeine Techniken, um Komponenten des IT-Budgets zu entwickeln, entstehen. Reaktive und taktische Budgetentscheidungen werden getroffen.

3 Defined (definiert):
Richtlinien und Prozesse für Investitionen und Budgetierung sind festgelegt, dokumentiert und kommuniziert und decken die wesentlichen Unternehmens- und Technologiebereiche ab. Das IT-Budget ist auf die strategischen IT- und Unternehmenspläne ausgerichtet. Prozesse für Budgetierung und Auswahl von IT-Investitionen sind formalisiert, dokumentiert und kommuniziert. Formale Schulungen werden abgehalten, basieren aber primär noch immer auf Einzelinitiativen. Es erfolgt eine formale Genehmigung der Auswahl von Investitionen und Budgets der IT. Das IT-Personal verfügt über die Erfahrung und Fachkenntnisse, welche notwendig sind zur Entwicklung des IT-Budgets und der Empfehlung geeigneter IT-Investitionen.

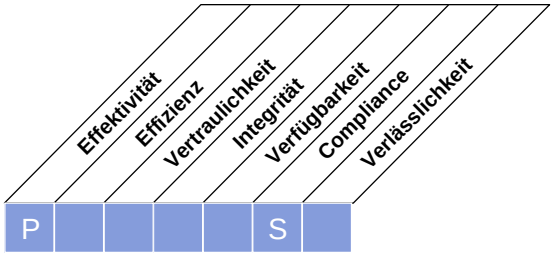
4 Managed and measurable (gemanaged und messbar):
Zuständigkeiten und Verantwortlichkeiten für die Auswahl von Investitionen und Budgetierung sind einer bestimmten Person zugeteilt. Budgetabweichungen werden identifiziert und geklärt. Formale Kostenanalysen werden durchgeführt. Diese beziehen direkte und indirekte Kosten für bereits bestehende Abläufe als auch für vorgeschlagene Investitionen unter Berücksichtigung sämtlicher Kosten über den gesamten Lebenszyklus mit ein. Ein pro-aktiver und standardisierter Prozess für Budgetierung wird verwendet. Die Auswirkungen der Verlagerung der Entwicklungs- und Betriebskosten von Hard- und Software hin zu Systemintegration und IT-Personalwesen wird in den Investitionsplänen berücksichtigt. Nutzen und Ertrag werden in finanziellen als auch in nicht finanziellen Werten berechnet.

5 Optimised (optimiert):
Branchenspezifische Best Practise-Ansätze werden dazu verwendet, Kosten zu benchmarken und Ansätze zur Effizienzsteigerung der Investitionen zu identifizieren. Analysen technologischer Entwicklungen werden im Prozess für die Auswahl von Investitionen und der Budgetierung miteinbezogen. Der Investitionsmanagement-Prozess wird durch Erfahrungen aus der Analyse aktueller Investitionsperformance kontinuierlich verbessert. Investitionsentscheidungen berücksichtigen Trends von Preis- und Performanceverbesserungen. Alternative Finanzierungslösungen werden unter Berücksichtigung der bestehenden Kapitalstruktur des Unternehmens formell evaluiert und geprüft. Es existiert eine proaktive Identifikation von Abweichungen. Eine Analyse der langfristigen Entwicklung von Kosten und Nutzen über den gesamten Lebenszyklus geht in die Investitionsentscheidungen ein.

HIGH-LEVEL CONTROL OBJECTIVE

PO6 Communicate Management Aims and Direction *(Kommuniziere Ziele und Richtung des Managements)*

Das Management sollte ein unternehmensweites IT Control Framework entwickeln, sowie Richtlinien festlegen und kommunizieren. Ein laufendes Programm zur Kommunikation sollte umgesetzt werden, um die vom Management freigegebenen und unterstützte(n) Mission, Ziele von Services, Richtlinien, Verfahren etc. zu kommunizieren. Die Kommunikation unterstützt das Erreichen von IT-Zielen und stellt das Bewusstsein und Verständnis von Unternehmens- und IT-Risiken, Zielen und Ausrichtung sicher. Der Prozess sollte die Einhaltung von relevanten Gesetzen und Vorschriften sicherstellen.



Kontrolle über den IT-Prozess,

Communicate management aims und direction (*Kommuniziere Ziele und Richtung des Managements*)

der die Anforderung des Unternehmens an die IT bezüglich

der richtigen und zeitgerechten Information über derzeitige und zukünftige IT-Services, damit verbundene Risken und Verantwortlichkeiten

durch die Konzentration auf

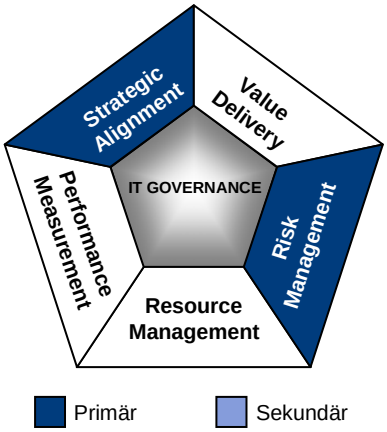
die Bereitstellung von richtigen, verständlichen und freigegebenen Richtlinien, Standards und Anleitungen und sonstigen, in ein IT Control Framework eingebetteter Dokumentationen für Stakeholder, *zufrieden stellt,*

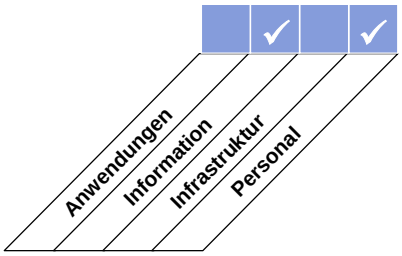
wird erreicht durch

- Festlegung eines IT Control Frameworks
- Erstellung und Rollout der IT-Richtlinien
- Durchsetzung der IT-Richtlinien

und gemessen durch

- Anzahl der Geschäftsunterbrechungen aufgrund von Ausfällen von IT-Services
- Prozentsatz der Stakeholder, die das IT Control Framework verstehen
- Prozentsatz der Stakeholder, welche die Richtlinien nicht einhalten





DETAILLIERTE CONTROL OBJECTIVES

PO6 Communicate Management Aims and Direction *(Kommuniziere Ziele und Richtung des Managements)*

PO6.1 IT Policy and Control Environment (IT-Richtlinien und Control-Umfeld)
Lege die Elemente des IT Control-Umfelds fest, das mit der Philosophie und dem Arbeitsstil des Unternehmensmanagement übereinstimmt. Diese Elemente umfassen Erwartungen/Anforderungen hinsichtlich Generierung von Wertbeiträgen aus Investitionen in IT, die Risikobereitschaft, Integrität, ethische Werte, Kompetenz des Personals, Verantwortlichkeit und Zuständigkeit. Das Control-Umfeld gründet auf einer Kultur, welche die Nutzenerbringung unterstützt und dabei das Management signifikanter Risiken unterstützt, die Zusammenarbeit über mehrere Abteilungen hinweg und Teamwork fördert, Compliance und laufende Prozessverbesserung fördert und Prozessabweichungen (inklusive Fehler) vernünftig handhabt.

PO6.2 Enterprise IT Risk and Internal Control Framework (Unternehmensweites Framework für IT-Risiken und Internal Controls)
Entwickle und unterhalte ein Framework, das den unternehmensweiten, übergeordneten Ansatz zum Risikomanagement und Internal Controls darstellt, um Nutzen zu generieren und gleichzeitig die Ressourcen und Systeme der schützt. Das Framework sollte in das IT-Prozessmodell und das Qualitätsmanagementsystem integriert sein und den übergeordneten Unternehmenszielen entsprechen. Es sollte ausgerichtet sein auf die Maximierung der Erfolge der Nutzenerbringung unter gleichzeitiger Minimierung von Risiken für Informationswerte mittels vorbeugender Maßnahmen, rechtzeitiger Identifikation von Unregelmäßigkeiten, Begrenzung von Verlusten und der zeitnahen Wiederherstellung der Unternehmenswerte.

PO6.3 IT Policies Management (Management der IT-Richtlinien)
Entwickle und unterhalte einen Satz von Richtlinien zur Unterstützung der IT-Strategie. Diese Richtlinien sollten die Absicht der Richtlinie, Rollen und Verantwortlichen, Prozesse zur Ausnahmebehandlung, Ansatz zur Compliance und Referenzen zu Verfahren, Standards und Anleitungen umfassen. Die Richtlinen sollten die wichtigsten Themen, wie Qualität, Sicherheit, Vertraulichkeit, Internal Controls und Schutz von geistigem Eigentum behandeln. Die Relevanz der Richtlinien sollte regelmäßig bestätigt und bewilligt werden.

PO6.4 Policy Rollout (Kommunikation der IT-Richtlinien)
Stelle sicher, dass IT-Richtlinien an alle relevanten Mitarbeiter kommuniziert und in Kraft gesetzt werden, und dass sie zu einem integralen Bestandteil der Unternehmensabläufe werden. Die eingesetzten Kommunikationstechniken sollten Ressourcen- und Kenntnisbedarf und deren Auswirkungen berücksichtigen.

PO6.5 Communication of IT Objectives and Direction (Kommunikation von Zielen und Ausrichtung der IT)
Stelle sicher, dass das Bewusstsein und Verständnis für Ziele und Ausrichtung des Unternehmens und der IT im gesamten Unternehmen kommuniziert werden. Die kommunizierte Information sollte eine klar festgelegte Mission, Ziele von Services, Security, Internal Controls, Qualität, Ethische- und Verfahrensgrundsätze, Richtlinien, Verfahren, etc. umfassen und in ein kontinuierliches Kommunikationsprogramm eingebettet sein, das durch die Geschäftsführung Wort und Tat unterstützt wird. Das Management sollte speziell darauf achten, dass IT-Sicherheitsbewusstsein und die Botschaft vermittelt wird, dass für IT-Sicherheit alle verantwortlich sind.

MANAGEMENT GUIDELINES

PO6 Communicate Management Aims and Direction *(Kommuniziere Ziele und Richtung des Managements)*

Von	Inputs
PO1	Strategische und taktische IT-Pläne; IT-Service- und Projektportfolio
PO9	Richtlinien zum IT-Risikomanagement
ME2	Report zur Wirksamkeit von IT-Controls

Outputs	Nach
IT-Richtlinien	ALLE
Unternehmensweites IT-Control-Framework	ALLE

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Etablieren und Führen einer IT Kontrollumgebung und Frameworks	I	C	I	A/R	I	C		C	C		C
Entwickeln und Unterhalten von IT-Richtlinien	I	I	I	A/R		C	C	C	R		C
Kommunizieren des IT Control Framework sowie Ziele und Ausrichtung der IT	I	I	I	A/R					R		C

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele
- Definition eines IT Control Frameworks
- Erstellen und ausrollen von IT-Richtlinien
- Durchsetzen von IT Policies

werden gemessen durch

Key Performance Indicators
- Frequenz von Reviews und Updates der Richtlinien
- Zeitverzögerung zwischen Freigabe der Richtlinien und deren Kommunikation an User
- Frequenz von Reviews und Updates des IT Control Frameworks

treiben

Prozessziele
- Entwickle gemeinsames und umfassendes IT Control Framework
- Entwickle einen Set von gemeinsamen und umfassenden IT-Richtlinien
- Kommuniziere die Strategie, Richtlinien und das Control Framework der IT

werden gemessen durch

Key Goal Indicators
- % der Stakeholder, die die IT–Richtlinien verstehen
- % der Stakeholder, die das IT Control Framework verstehen
- % der Stakeholder, die Richtlinien nicht einhalten

treiben

IT-Ziele
- Stelle Transparenz von und Verständnis für IT-Kosten, Nutzen, Strategie, Richtlinien und Service Levels sicher
- Stelle sicher, dass automatischen Transaktionen und Informationsaustausch vertraut werden kann
- Stelle den Schutz von kritischen und vertraulichen Informationen vor unberechtigtem Zugriff sicher
- Stelle sicher, dass der Einfluss einer IT-Service-Störung oder -Änderung auf das Geschäft minimiert ist
- Stelle die angemessene Verwendung und Performance der Anwendungen und technischen Lösungen sicher
- Stelle sicher, dass IT-Services und Infrastruktur Ausfällen auf Grund von Fehlern, bewussten Angriffen oder Katastrophen standhalten können und ihre Wiederherstellung gewährleistet ist

werden gemessen durch

IT Key Goal Indicators
- Anzahl der Fälle, wo vertrauliche Informationen kompromittiert wurden.
- Anzahl der Unterbrechungen im Kerngeschäft auf Grund von IT Service-Ausfällen
- Verständnis für Kosten, Nutzen, Strategie, Richtlinien und Service Levels der IT

MATURITY MODEL

PO6 Communicate Management Aims and Direction *(Kommuniziere Ziele und Richtung des Managements)*

Die Reife des Management des Prozesses *Communicate Management Aims and Direction (Kommuniziere Ziele und Richtung des Management)*, der die Geschäftsanforderungen an die IT erfüllt der richtigen und zeitgerechten Information über derzeitige und zukünftige IT-Services, damit verbundene Risken und Verantwortlichkeiten ist:

0 Non-existent (nicht existent):
Es wurde kein positives Information Control-Umfeld durch das Management geschaffen. Es besteht kein Verständnis für den Bedarf der Einführung von Richtlinien, Verfahren, Standards und Compliance-Prozessen vorhanden.

1 Initial (initial):
Das Management handelt im Bezug auf die Anforderungen für ein Information Control-Umfeld reaktiv. Richtlinien, Verfahren und Standards werden dann ad-hoc entwickelt und kommuniziert, wenn ein konkreter, anlassbezogener Bedarf besteht. Die Entwicklungs-, Kommunikations- und Compliance-Prozesse sind informell und inkonsistent.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Es besteht ein grundsätzliches Bewusstsein für den Bedarf und die Anforderungen eines wirksamen Information Control-Umfelds, die Praktiken sind aber großteils informell. Das Management hat den Bedarf von Richtlinien, Verfahren und Standards zur Steuerung kommuniziert, deren Entwicklung ist aber den einzelnen Manager und Geschäftsbereichen überlassen. Qualität wird als wünschenswerte und zu verfolgende Philosophie gesehen, aber die Praktiken sind den einzelnen Managern überlassen. Schulungen werden bei Bedarf auf einer individuellen Basis durchgeführt.

3 Defined (definiert):
Ein vollständiges Information Control- und Qualitätsmanagement wurde durch das Management entwickelt, dokumentiert und kommuniziert. Dieses umfasst ein Framework für Richtlinien, Verfahren und Standards. Der Entwicklungsprozess für Richtlinien ist strukturiert, wird unterhalten und ist den Mitarbeitern bekannt. Bestehende Richtlinien, Verfahren und Standards sind angemessen formuliert und decken die Schlüsselthemen ab. Das Management hat die Wichtigkeit des IT-Sicherheitsbewussteins adressiert und entsprechende Maßnahmen veranlasst. Formelle Schulungen werden angeboten, um das Information Control-Umfeld zu unterstützen, diese werden aber nicht rigoros eingesetzt. Obwohl es ein umfassendes Entwicklungs-Framework für Control-Richtlinien und Standards gibt, wird die Einhaltung dieser Richtlinien und Standards nicht durchgängig überwacht. Es gibt ein umfassendes Framework zur Entwicklung. Methoden, um das Sicherheitsbewusstsein zu vorantreiben, wurden standardisiert und formalisiert.

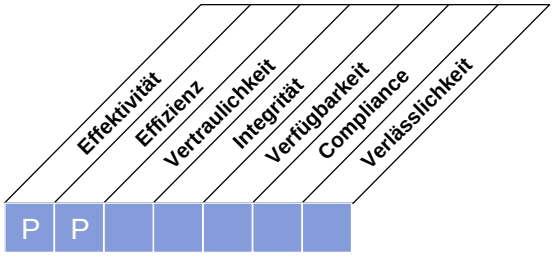
4 Managed and measurable (gemanaged und messbar):
Das Management übernimmt die Verantwortung für die Kommunikation der Richtlinien für Internal Controls, hat Verantwortlichkeiten delegiert und ausreichend Ressourcen zugeteilt, um das Umfeld an wesentliche Änderungen anzupassen. Ein positives, proaktives Information Control-Umfeld wurde etabliert, welches auch Aussagen hinsichtlich Qualitäts- und IT-Security-Bewusstsein umfasst. Ein vollständiger Satz von Richtlinien und Standards wurde entwickelt, überarbeitet und kommuniziert und sie setzen sich aus internen anerkannten Praktiken zusammen. Ein Framework für die Verbreitung und anschließende Prüfung der Compliance wurde eingeführt.

5 Optimised (optimiert):
Das Information Control-Umfeld ist auf das strategische Management-Framework sowie die Vision ausgerichtet und wird regelmäßig reviewed, aktualisiert und kontinuierlich verbessert. Interne und externe Experten werden eingesetzt, um sicher zu stellen, dass Best Practice-Verfahren unter Berücksichtigung von Control-Vorgaben und Kommunikationstechniken eingesetzt werden. Monitoring, Self-Assessment und Compliance-Prüfungen werden sind durchgängig im Unternehmen eingesetzt. Technologie wird verwendet, um Richtlinien und Wissensbasen für Awareness zu unterhalten und um die Kommunikation mittels Büroautomatisierung und Werkzeugen zum Computer-Based-Training zu optimieren.

HIGH-LEVEL CONTROL OBJECTIVE

PO7 Manage IT Human Resources *(Manage die IT-Human-Ressourcen)*

Beschaffe, unterhalte und motiviere kompetente Arbeitskräfte für die Erstellung und den Betrieb von IT-Services für das Kerngeschäft. Dies wird erreicht durch die Anwendung von definierten und akzeptierten Praktiken, die Recruiting, Training, Performance-Evaluierung, Beförderung und Beschäftigungsbeendigung unterstützen. Dieser Prozess ist von Bedeutung, da Personal einen wichtigen Aktivposten darstellt und Governance sowie das Internal Control-Umfeld stark von der Motivation und der Kompetenz des Personals abhängen.



Kontrolle über den IT-Prozess,

Manage IT human resources (*Manage die IT-Human-Ressourcen*)

der die Anforderung des Unternehmens an die IT bezüglich

kompetenter und motivierter Mitarbeiter für die Erstellung und Betrieb der IT-Services

durch die Konzentration auf

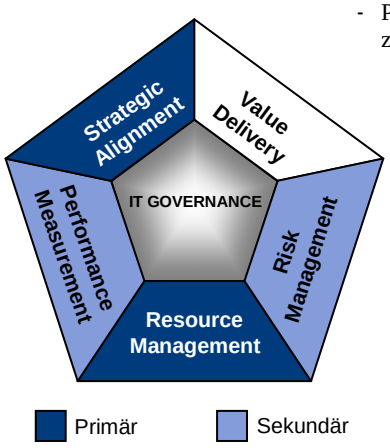
Anwerben und Schulung von Personal, das durch klare Karrierewege motiviert werden kann, der Zuweisung von Rollen, die mit den Fähigkeiten übereinstimmen, Einführen eines definierten Reviewprozesses, das Erstellen von Stellenbeschreibungen, und die Sicherstellung des Bewusstseins für die Abhängigkeit vom jeden Einzelnen , *zufrieden stellt,*

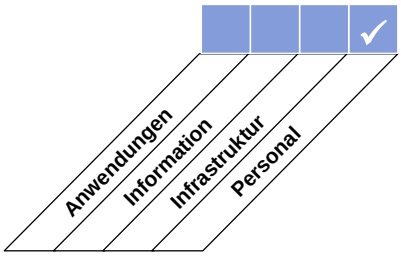
wird erreicht durch

- Review der Mitarbeiter-Performance
- Anwerben und Schulung von IT-Personal, um taktische IT-Pläne zu unterstützen
- Entschärfen des Risikos einer zu großen Abhängigkeit von Schlüsselressourcen

und gemessen durch

- Zufriedenheitsgrad der Stakeholder mit den Fähigkeiten und Fachkenntnissen des IT-Personals
- Fluktuationsrate des IT-Personals
- Prozentanteil des IT-Personals, das entsprechend der Erfordernisse der Stelle zertifiziert ist





DETAILLIERTE CONTROL OBJECTIVES

PO7 Manage IT Human Resources *(Manage die IT-Human-Ressourcen)*

PO7.1 Personnel Recruitment and Retention (Personalrekrutierung und -bindung)
Stelle sicher, dass der IT-Personalrekrutierungsprozess übereinstimmt mit den unternehmensweiten Richtlinien und Verfahren für Personal (zB Anstellung, positive Arbeitsumgebung und Orientierung). Das Management implementiert Prozesse, die sicherstellen, dass die Organisation angemessenes IT-Personal einsetzt, welche die notwendigen Fähigkeiten besitzen, Unternehmensziele zu erreichen.

PO7.2 Personnel Competencies (Kompetenzen des Personals)
Überprüfe regelmäßig, dass das Personal die nötige Kompetenz besitzt, um seine Aufgaben anhand seiner Bildung, Schulungen und/oder Erfahrungen durchzuführen. Definiere Anforderungen für IT-Kernkompetenzen und stelle sicher, dass diese, wo geeignet, durch Programme für Qualifikation und Zertifizierung unterhalten werden.

PO7.3 Staffing of Roles (Besetzung von Rollen)
Definiere, monitore und überwache Rollen, Verantwortlichkeiten und den Vergütungsrahmen der Mitarbeiter – einschließlich der Erfordernis, Richtlinien und Verfahren des Management, ethische Grundsätze und professionelle Praktiken einzuhalten. Die Bedingungen des Angestelltenverhältnisses sollten die Verantwortlichkeiten der Mitarbeiter hinsichtlich Informationssicherheit, Internal Controls und Compliance mit Regulativen betonen. Der Grad der Überwachung sollte an die Sensitivität der Position und dem Ausmaß der zugewiesenen Verantwortlichkeiten angepasst sein.

PO7.4 Personnel Training (Ausbildung des Personals)
Biete dem IT-Personal bei der Anstellung eine entsprechend Einweisung an und führe laufend Schulungen durch, um Wissen, Fähigkeiten, Begabungen und ein Bewusstsein für Internal Controls und Security auf dem Niveau zu erhalten, das notwendig ist, um die Unternehmensziele zu erreichen.

PO7.5 Dependence Upon Individuals (Abhängigkeit von Einzelpersonen)
Minimiere die Gefahr kritischer Abhängigkeiten von Schlüsselpersonen durch Wissensaufzeichnung (engl.: *knowledge capture*) (Dokumentation), Teilen von Wissen, Nachfolgeplanung und Vertretung von Personal.

PO7.6 Personnel Clearance Procedures (Verfahren zur Überprüfung von Personal)
Schließe Hintergrund-Checks im IT Recruiting-Prozess ein. Das Ausmaß und die Häufigkeit der Überprüfung dieser Checks sind von der Sensitivität und/oder der Kritikalität der Funktion abhängig; und sie sollten für Angestellte, Vertragspartner und Lieferanten durchgeführt werden.

PO7.7 Employee Job Performance Evaluation (Beurteilung der Leistung von Mitarbeitern)
Fordere auf regelmäßiger Basis die Durchführung zeitgerechter Beurteilung in Bezug auf individuelle Ziele, welche von den Unternehmenszielen, bestehenden Standards und spezifischen Aufgaben abgeleitet werden. Mitarbeiter sollten, wo möglich in der Leistung und in Ihrem Verhalten unterstützt werden.

PO7.8 Job Change and Termination (Stellenwechsel und Kündigung)
Ergreife rasch Aktionen bei Jobwechsel, insbesondere bei der Auflösung des Arbeitsverhältnisses. Der Wissenstransfer muss vorbereitet sein, Verantwortlichkeiten neu zugewiesen und Zugriffsrechte entfernt werden, um Risken zu minimieren und die Fortführung der Funktion zu gewährleisten.

MANAGEMENT GUIDELINES

PO7 Manage IT Human Resources *(Manage die IT-Huma<n-Ressourcen)*

Von	Inputs
PO4	Organisation und Beziehungen der IT; Dokumentierte Rollen und Verantwortlichkeiten
AI1	Machbarkeitsstudie bezüglich Unternehmenserfordernissen

Outputs	Nach						
Personalrichtlinien und -verfahren der IT	PO4						
IT Skills Matrix	PO4	PO10					
Stellenbeschreibungen	PO4						
Skills und Fertigkeiten von Benutzern, inkl. individuellem Training; spezifische Trainingsanforderungen	DS7						

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Identifiziere IT-Fähigkeiten, Stellenbeschreibungen, Gehaltsstufen und Personalperformance-Benchmarks		C		A		C	C	C	R	C	
Befolge für IT relevante HR-Richtlinien und Verfahren (Rekrutierung, Anstellung, Hintergrund-Checks, Gehalt, Schulung, Beurteilung, Beförderung				A		R	R	R	R	R	C

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Anwerben und Schulung von IT-Personal, um taktische IT-Pläne zu unterstützen
- Abschwächen des Risikos einer zu großen Abhängigkeit von Schlüsselressourcen
- Review von Mitarbeiter-Performance

werden gemessen durch

Key Performance Indicators

- % der IT-MitarbeiterInnen, die Entwicklungspläne abgeschlossen haben
- % der IT-MitarbeiterInnen mit dokumentierten und validierten rechtzeitigen Reviews
- % der IT-Stellen mit Stellenbeschreibungen und Qualifikationsanforderungen
- Durchschnittliche Anzahl der Schulungs- und Entwicklungstage (inklusive Coaching) pro Person pro Jahr
- Rate der IT-Mitarbeiterrotation
- % des zertifizierten IT-Personals, im Verhältnis zu den Erfordernissen der Stelle
- Durchschnittliche Anzahl der Tage um offene IT-Rollen zu füllen

treiben

Prozessziele

- Aufbau professioneller HR Management Verfahren in der IT
- Effektiver Einsatz des gesamten IT-Personals und gleichzeitige Minimierung der Abhängigkeit von Schlüsselpersonen

werden gemessen durch

Key Goal Indicators

- % der IT MitarbeiterInnen, die das Kompetenzprofil für die in der Strategie geforderten Rollen besitzen
- % der besetzten IT Rollen
- % der durch ungeplante Abwesenheit verlorenen Arbeitstage
- % der IT Mitarbeiter, die den jährlichen Schulungsplan absolvieren
- Ist zu Soll Relation von internen und externen MitarbeiterInnen
- % der MitarbeiterInnen, die einer Überprüfung unterzogen wurden
- % der IT Rollen, die eine qualifizierte Vertretung besitzen

treiben

IT-Ziele

- Beschaffe und erhalte IT-Skills, die der IT-Strategie entsprechen
- Stelle IT-Agilität her

werden gemessen durch

IT Key Goal Indicators

- Grad der Zufriedenheit von Stakeholdern mit der Expertise und Fertigkeiten von IT MitarbeiterInnen
- % des zufriedenen IT Personals (zusammengesetzte Messgröße)
- Fluktuation des IT Personals

MATURITY MODEL

PO7 Manage IT Human Resources *(Manage die IT-Human-Ressourcen)*

Die Reife des Management des Prozesses *Manage IT Human Resources (Manage die Human-Ressourcen)*, der die Geschäftsanforderungen an die IT erfüllt der kompetenten und motivierten Mitarbeiter für Erstellung und Betrieb der IT-Services ist:

0 Non-existent (nicht existent):
Es besteht kein Bewusstsein vorhanden für die Wichtigkeit der Abstimmung des Management der Human-Ressourcen der IT mit dem technologischen Planungsprozess für die Organisation. Es ist keine Person oder Gruppe formell für das Management der Human-Ressourcen verantwortlich.

1 Initial (initial):
Das Management erkennt die Notwendigkeit das Management der Human-Ressourcen der IT. Der Management-Prozess der Human-Ressourcen der ist informell und reaktiv. Er ist betrieblich fokussiert auf die Beschaffung und das Management von IT-Personal. Ein Bewusstsein entwickelt sich für die Auswirkungen der schnellen Geschäfts- und Technologieveränderungen sowie zunehmend komplexeren Lösungen für den Bedarf an neuen Fähigkeiten und Kompetenzniveaus.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Ein mittelfristiger Vorgehensansatz für die Anstellung und Verwaltung von IT-Personal besteht auf Grund projektspezifischer Anforderungen, nicht aber auf Grund eines verstandenen Gleichgewichts von intern und extern verfügbarem Personal. Es erfolgen informelle Schulungen für neues Personal, das dann Schulungen erhält, wenn Bedarf besteht.

3 Defined (definiert):
Es gibt einen definierten und dokumentierten Prozess für das Management der Human-Ressourcen der IT. Es existiert ein Plan für das Management der Human-Ressourcen der IT. Ein strategischer Ansatz für die Anstellung und Verwaltung von IT-Personal ist vorhanden. Es wurde ein formeller Schulungsplan entworfen, der den Bedarf an Human-Ressourcen der IT abdeckt. Ein Programm zur Personalrotatien, das für die Erweiterung der technischen und unternehmerischen Fähigkeiten entwickelt wurde, ist etabliert.

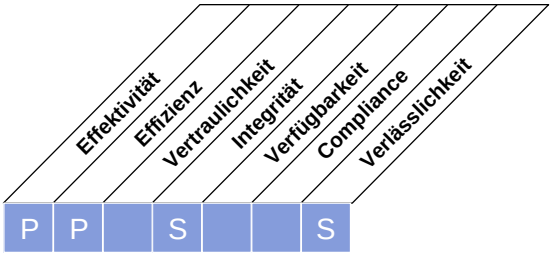
4 Managed and measurable (gemanaged und messbar):
Die Verantwortung für die Entwicklung und Wartung eines Managementplans für Human-Ressourcen der IT wurde einer spezifischen Person oder Gruppe mit der notwendigen Erfahrung und Fertigkeiten für die Entwicklung und den Unterhalt des Plans zugewiesen. Der Prozess zur Entwicklung und Wartung des Managementplans der Human-Ressourcen der IT reagiert auf Veränderungen. Die Organisation hat standardisierte Messgrößen entwickelt, die ihr erlauben, Abweichungen vom Managementplan der Human-Ressourcen der IT zu identifizieren, mit spezieller Beachtung des Managment von Wachstum und Fluktuation des IT-Personals. Reviews von Vergütungen und der Performance werden durchgeführt und mit anderen IT-Organisationen und bewährten Praktiken verglichen. Das Management der Human Ressurcen ist pro-aktiv und berücksichtigt Pfade der Entwicklung der Berufskarriere.

5 Optimised (optimiert):
Der Managementplan der Human-Ressourcen der IT wird laufend aktualisiert, um den sich ändernden Unternehmensanforderungen zu entsprechen. Das Management der Human-Ressourcen der IT ist in die Technologie-Planung eingebunden, um die optimale Entwicklung und Einsatz der verfügbaren IT-Fertigkeiten sicher zu stellen. Das Management der Human-Ressourcen der IT ist in die strategische Ausrichtung der Organisation integriert und entspricht dieser. Die Bestandteile des Das Management der Human-Ressourcen der IT entsprechen hinsichtlich Vergütung, Performance-Reviews, Teilnahme in Branchenforen, Wissenstransfer, Schulung und Patenschaften den Best-Practices der Branche. Schulungsprogramme werden für alle neuen technischen Standards und Produkte entwickelt, bevor diese in der Organisation eingesetzt werden.

HIGH-LEVEL CONTROL OBJECTIVE

PO8 Manage Quality *(Manage Qualität)*

Ein Qualitätsmanagementsystem sollte entwickelt und unterhalten werden, welches bewährte Entwicklungs- und Beschaffungsprozesse und -standards umfasst. Dies wird durch die Planung, Implementierung und Unterhalt des Qualitätsmanagementsystems und durch die Erstellung von klaren Qualitätsanforderungen, Verfahren und Richtlinien erreicht. Qualitätsanforderungen sollten als quantifizierbare und umsetzbare Indikatoren festgelegt und kommuniziert werden. Eine laufende Verbesserung wird durch eine kontinuierliche Überwachung, Analyse, Behebung von Abweichungen und Kommunikation der Ergebnisse an die Stakeholder erreicht. Qualitätsmanagement ist wesentlich, um sicherzustellen, dass die IT für die Stakeholder einen Wertbeitrag zum Kerngeschäft, laufende Verbesserungen und Transparenz erbringt.



Kontrolle über den IT-Prozess,

Manage Quality (*Manage Qualität*)

der die Anforderung des Unternehmens an die IT bezüglich

der kontinuierlichen und messbaren Qualitätsverbesserung der erbrachten IT-Services

durch die Konzentration auf

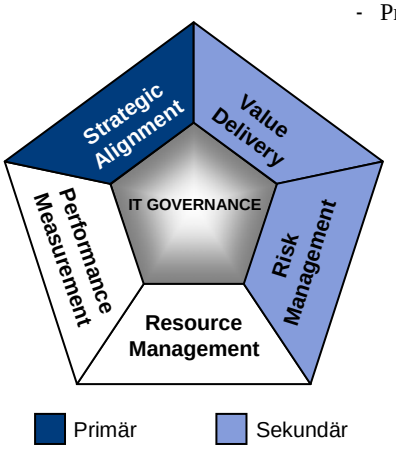
die Definition eines Qualitätsmanagementsystems (QMS), laufende Performanceüberwachung gegen vordefinierte Ziele und die Implementierung eines Programms für kontinuierliche Verbesserung der IT-Services, *zufrieden stellt,*

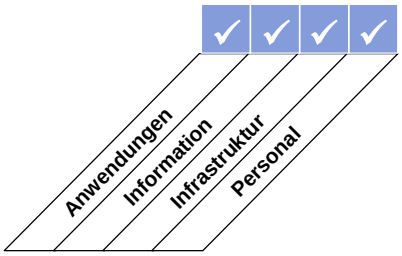
wird erreicht durch

- Festlegung der Qualitätsstandards und -praktiken
- Überwachung und Prüfung interner und externer Performance gegen die definierten Qualitätsstandards und -praktiken
- kontinuierliche Verbesserung des QMS

und gemessen durch

- Prozent der mit der IT-Qualität (gewichtet nach Bedeutung) zufriedenen Stakeholder
- Prozent der durch die Qualitätssicherung formal und periodisch geprüften IT-Prozesse, die den Qualitätsvorgaben und -zielen entsprechen
- Prozent der Prozesse, die Reviews der Qualitätssicherung (QA) unterliegen





DETAILLIERTE CONTROL OBJECTIVES

PO8 Manage Quality *(Manage Qualität)*

PO8.1 Quality Management System (Qualitätsmanagement-System)
Entwickle und unterhalte ein QMS, das einen standardisierten, formalen und kontinuierlichen Ansatz hinsichtlich Qualitätsmanagement bietet, der an die Unternehmenserfordernisse ausgerichtet ist. Das QMS identifiziert Qualitätsanforderungen und -kriterien, wesentliche IT-Prozesse mit deren Abfolge und Interaktion und die Richtlinien, Kriterien und Methoden für die Definition, Erkennung, Korrektur und Verhinderung der Nichteinhaltung. Das QMS sollte die organisatorische Struktur für Qualitätsmanagement festlegen, und die Rollen, Aufgaben und Verantwortlichkeiten abdecken. Alle wesentlichen Bereiche entwickeln ihre Qualitätsplane entsprechend der Kriterien und Richtlinien und zeichnen Qualitätsinformationen auf. Monitore und messe die Wirksamkeit und Akzeptanz des QMS und verbessere es, wenn notwendig.

PO8.2 IT Standards and Quality Practices (Standards und Qualitätssicherungs-Verfahren der IT)
Identifiziere und unterhalte Standards, Methoden und Praktiken für die wesentlichen IT-Prozesse, um die Organisation in der Erreichung der Ziele des QMS zu unterstützen. Wende Best-Practices der Branche bei der Verbesserung oder Anpassung der Qualitätspraktiken der Organisation an.

PO8.3 Development and Acquisition Standards (Entwicklungs- und Beschaffungs-Standards)
Übernehme und unterhalte – dem Lebenszyklus eines Endproduktes folgenden – Standards für alle Entwicklungen und Beschaffungen und berücksichtige Freigaben von wichtigen Milestones auf Basis von vereinbarten Abnahme-Kriterien. Zu berücksichtigende Punkte umfassen Standards zur Programmierung, Namenskonventionen, Dateiformate, Designstandards für Datenschema und Data Dictionaries, Standards für das User-Interface, Interoperabilität, Effizienz der Systemperformance, Skalierbarkeit, Standards für Entwicklung und Tests, Validierung der Anforderungen, Testpläne sowie Modul-, Regressions- und Integrationstests.

PO8.4 Customer Focus (Kundenorientierung)
Stelle sicher, dass sich das Qualitätsmanagement auf Kunden fokussiert, indem ihre Anforderungen erhoben werden und diese mit den IT-Standards und -Praktiken in Einklang gebracht werden. Rollen und Verantwortlichkeiten für die Konfliktbewältigung zwischen Usern/Kunden und der IT-Organisation sind festgelegt.

PO8.5 Continuous Improvement (Kontinuierliche Verbesserung)
Ein allgemeiner Qualitätsplan, der eine kontinuierliche Verbesserung fördert, wird regelmäßig gewartet und kommuniziert.

PO8.6 Quality Measurement, Monitoring and Review (Messung, Management und Review der Qualität)
Definiere, plane und implementiere Maßnahmen für das regelmäßige Monitoring der Compliance mit dem QMS und den Nutzen, den das QMS bringt. Messung, Monitoring und Aufzeichnung der Information sollte von den Prozesseignern verwendet werden, um geeignete korrektive und präventive Maßnahmen zu treffen.

MANAGEMENT GUIDELINES

PO8 Manage Quality *(Manage Qualität)*

Von	Inputs
PO1	Strategische und taktische IT-Pläne
PO10	Detaillierte Projektpläne
ME1	Plan der Verbesserungsmaßnahmen

Outputs	Nach						
Beschaffungsstandards	AI1	AI2	AI3	AI5	DS2		
Entwicklungsstandards	PO10	AI1	AI2	AI3	AI7		
Anforderungen an Qualitätsstandards und Metriken	ALLE						
Aktivitäten zur Qualitätsverbesserung	PO4	AI6					

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Definiere ein Qualitätsmanagementsystem	C		C	A/R	I	I	I	I	I	I	C
Erstelle und unterhalte ein Qualitätsmanagementsystem	I	I	I	A/R	I	C	C	C	C	C	C
Erstelle und kommuniziere Qualitätsstandards in der Organisation		I		A/R	I	C	C	C	C	C	C
Erstelle und manage den Qualitätsplan für kontinuierliche Verbesserung				A/R	I	C	C	C	C	C	C
Messe, überwache und überprüfe Compliance mit den Qualitätszielen				A/R	I	C	C	C	C	C	C

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Definieren der Qualitätsstandards und -praktiken
- Überwachen und Prüfen interner und externer Performance gegen die definierten Qualitätsstandards und -praktiken

treiben

Prozessziele

- Stelle Qualitätsstandards und -kultur für IT-Prozesse auf
- Stelle eine effiziente und effektive IT-Qualitätssicherungsfunktion auf.
- Überwache die Wirksamkeit der IT-Prozesse und IT-Projekte

treiben

IT-Ziele

- Stelle die Enduser-Zufriedenheit mit den Serviceangeboten und Service Levels sicher
- Reduziere Mängel und Nacharbeit bei Lösungen und dem Servicebetrieb
- Setze Projekte pünktlich und im Budgetrahmen und unter Einhaltung der Qualitätsstandards um

werden gemessen durch

Key Performance Indicators

- % von Projekten, die QA-Review erhalten
- % der IT-Mitarbeiter, die Qualitätsbewußtseins-/-management Training erhalten
- % von IT-Prozessen und -Projekten mit aktiver Beteiligung der Stakeholder an der Qualitätssicherung
- % der Prozesse, die QA-Review erhalten.
- % der Stakeholder, die sich an der Qualitätsüberwachung beteiligen

werden gemessen durch

Key Goal Indicators

- % der Fehler, die vor der Inbetriebnahme erkannt wurden
- % Reduktion in der Anzahl der schwerwiegenden Störungen pro User und Monat
- % der durch eine QA überprüften und abgenommenen IT-Projekte, die den Qualitätsvorgaben und -zielen entsprechen
- % der regelmäßig durch eine QA formell überprüften IT-Prozesse, die den Qualitätsvorgaben und -zielen entsprechen

werden gemessen durch

IT Key Goal Indicators

- % der Stakeholder, die mit der IT-Qualität (gewichtet durch Bedeutung) zufrieden sind

MATURITY MODEL

PO8 Manage Quality *(Manage Qualität)*

Die Reife des Management des Prozesses *Manage Quality (Manage Qualität)*, der die Geschäftsanforderungen an die IT erfüllt der kontinuierlichen und messbaren Qualitätsverbesserung der erbrachten IT-Services ist:

0 Non-existent (nicht existent):
Im Unternehmen existiert kein Planungsprozess für das QMS und keine Methodik für den Systementwicklungs-Lebenszyklus. Das obere Management und die IT-Mitarbeiter erkennen keine Notwendigkeit für ein Qualitätsprogramm. Qualitätsreviews über Projekte und den Betrieb finden nicht statt.

1 Initial (initial):
Dem Management ist die Notwendigkeit eines QMS bewusst. Wo es ein QMS gibt, wird es von Einzelpersonen betrieben. Das Management führt informelle Beurteilungen der Qualität durch.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Ein Programm zur Festlegung und Überwachung von QMS-Aktivitäten innerhalb der IT wurde eingeführt. Bestehende QMS-Aktivitäten beziehen sich auf projekt- und prozessorientiere Initiativen der IT und nicht auf unternehmensweite Prozesse.

3 Defined (definiert):
Ein definierter QMS-Prozess wurde durch das Management kommuniziert und bezieht das Management der IT und der End-Anwender mit ein. Es wird ein Schulungs- und Trainingsprogramm entwickelt, um alle Organisationsebenen über Qualität zu unterrichten. Grundlegende Qualitätserwartungen wurden festgelegt und werden in Projekten und innerhalb der IT-Organisation geteilt. Übliche Werkzeuge und Praktiken des Qualitätsmanagements tauchen auf. Erhebungen zur Qualitätszufriedenheit werden geplant und teilweise durchgeführt.

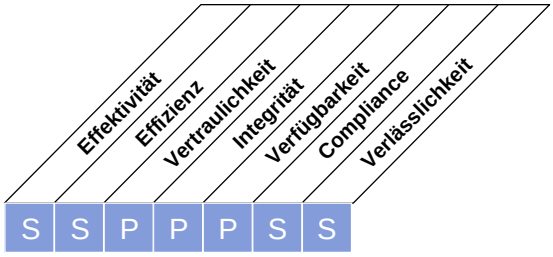
4 Managed and measurable (gemanaged und messbar):
Das QMS wird in allen Prozessen angesprochen, inklusive der von Dritten abhängigen Prozessen. Eine standardisierte Wissensbasis für Qualitätsmetriken wurde eingeführt. Methoden zur Kosten/Nutzen-Analyse werden eingesetzt, um QMS-Initiativen zu bewerten. Benchmarking im Vergleich zu Industrie und Mitbewerbern entsteht. Ein Schulungs- und Trainingsprogramm wird eingesetzt, um alle Organisationsebenen in Bezug auf Qualität zu unterrichten. Werkzeuge und Praktiken wurden standardisiert und ursprungsbezogene Analysen werden periodisch angewendet. Erhebungen zur Qualitätszufriedenheit werden konsistent durchgeführt. Ein standardisiertes Programm zur Qualitätsmessung ist etabliert und gut strukturiert. Das IT-Management entwickelt eine Wissensbasis für Qualitätsmetriken.

5 Optimised (optimiert):
Das QMS ist in alle IT-Aktivitäten integriert und wird durchgesetzt. Die QMS-Prozesse sind flexibel und an Änderungen der IT-Umgebung anpassbar. Die Wissensbasis für Qualitätsmetriken ist um externe Best Practices erweitert. Benchmarking gegenüber externen Standards wird routinemäßig durchgeführt. Die Erhebung der Qualitätszufriedenheit ist ein andauernder Prozess und führt zu ursprungsbezogenen Analysen und Optimierungsaktionen. Auf Ebene des Qualitätsmanagement-Prozesses existiert eine unabhängige Bestätigung der Vorgehensweise.

HIGH-LEVEL CONTROL OBJECTIVE

PO9 Assess and Manage IT Risks *(Beurteile und Manage IT-Risiken)*

Erstelle und unterhalte ein Risikomanagement-Framework. Das Framework dokumentiert ein allgemeines und vereinbartes Niveau von IT-Risiken, Strategien zur Risikoreduktion und vereinbarten Restrisiken. Alle potentiellen Einflüsse auf die Ziele der Organisation, die durch ein ungeplantes Ereignis hervorgerufen werden, sollten identifiziert, analysiert und bewertet werden. Strategien der Risikoreduktion sollten umgesetzt werden, um das Restrisiko auf ein akzeptiertes Niveau zu reduzieren. Das Ergebnis der Bewertung sollte für die Stakeholder verständlich sein und in finanzbezogenen Kennzahlen kommuniziert werden, um den Stakeholdern zu ermöglichen, das Risiko auf ein akzeptables Toleranzniveau zu bringen.



Kontrolle über den IT-Prozess,

Assess and Manage IT Risks (*Beurteile und Manage IT-Risiken*)

der die Anforderung des Unternehmens an die IT bezüglich

der Analyse und Kommunikation der IT-Risiken und deren potenzielle Auswirkungen auf Geschäftsprozesse und -ziele

durch die Konzentration auf

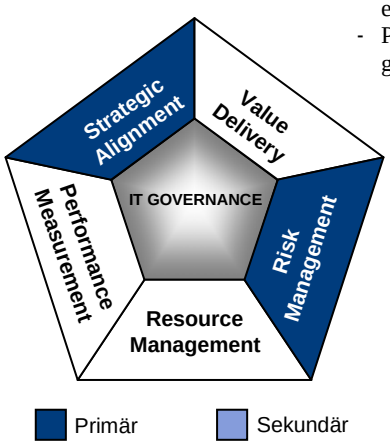
die Entwicklung eines Risikomanagement-Framework, welches in Business und Operational Risikomanagement-Frameworks, Risikobewertung, Risikobegrenzung und Kommunikation der ungeklärten Risiken integriert ist, *zufrieden stellt,*

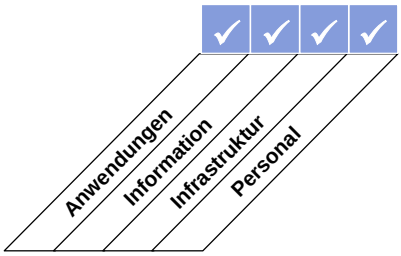
wird erreicht durch

- Sicherstellen, dass das Risikomanagement vollständig in die internen und externen Management-Prozesse eingebettet und konstant angewendet ist
- Durchführen von Risikobewertungen
- Empfehlen und Kommunizieren von Plänen zur Risikominimierung

und gemessen durch

- Prozent der kritischen IT-Ziele, die von der Risikobeurteilung abgedeckt sind
- Prozent der identifizierten kritischen IT-Risiken, für die Maßnahmenpläne entwickelt worden sind
- Prozent der Risikomanagement-Maßnahmenpläne, die zur Implementierung genehmigt worden sind





DETAILLIERTE CONTROL OBJECTIVES

PO9 Assess and Manage IT Risks *(Beurteile und Manage IT-Risiken)*

PO9.1 IT and Business Risk Management Alignment (Abstimmung des Risikomanagements der IT und des Unternehmens)
Integriere die Frameworks für IT-Governance, Risikomanagement und Controls in das unternehmensweite Modell für Risikomanagement. Dies beinhaltet die Ausrichtung bezüglich des Risikoappetits des Unternehmens und dem Grad der Risikotoleranz.

PO9.2 Establishment of Risk Context (Festlegung des Risikokontext)
Entwickle den Kontext, in den das Risikobeurteilungs-Framework eingebettet wird, um die Angemessenheit der Ergebnisse sicher zu stellen. Dies umfasst die Bestimmung der internen und externen Rahmenbedingungen für jede Risikobewertung, die Ziele der Bewertung und die Kriterien, nach denen Risiken evaluiert werden.

PO9.3 Event Identification (Ereignisidentifikation)
Identifiziere sämtliche Ereignisse (Bedrohungen oder Verletzbarkeiten) mit einer potentiellen Auswirkung auf die Ziele oder den Betrieb des Unternehmens; einschließlich der folgenden Aspekte: Geschäftstätigkeit, Verordnungen, Recht, Technologie, Handelspartner, Personal und Betrieb. Bestimme die Art der Auswirkungen – positiv, negativ oder beides – und unterhalte diese Informationen.

PO9.4 Risk Assessment (Bewertung von Risiken)
Bewerte regelmäßig, unter Anwendung qualitativer und quantitativer Methoden, die Wahrscheinlichkeit und Auswirkungen aller identifizierten Risiken. Die Wahrscheinlichkeit und Auswirkungen, die mit inhärenten und Restrisiken verbunden sind, sollten einzeln, pro Kategorie und auf Basis eines Portfolios bestimmt werden.

PO9.5 Risk Response (Maßnahmen zur Risikobehandlung)
Bestimme einen Risikoeigner und betroffene Prozesseigner, entwickle und unterhalte Risikoantworten, um sicher zu stellen, dass kostengünstige Controls und Sicherheitsmaßnahmen die Ausgesetztheit bezüglich Risiken kontinuierlich reduzieren. Die Risikoantwort sollte Risikostrategien, wie Vermeidung, Reduktion, Teilung oder Akzeptanz identifizieren. Berücksichtige bei der Entwicklung der Maßnahmen die Kosten und den Nutzen und wähle Maßnahmen, die das Restrisiko innerhalb des festgelegten Toleranzniveaus halten.

PO9.6 Maintenance and Monitoring of a Risk Action Plan (Erhalt und Monitoring eines Plans zur Risikobehandlung)
Priorisiere und Plane die Kontrollaktivitäten auf allen Ebenen, um die Risikoantworten wie festgelegt umzusetzen; einschließlich Kosten, Nutzen und Verantwortlichkeiten für die Ausführung. Hole Genehmigung für die empfohlenen Aktivitäten und Freigaben für alle verbleibenden Risiken ein und stelle sicher, dass zugesagte Aktivitäten durch die betroffenen Prozesseigner verantwortet werden. Monitore die Umsetzung der Pläne und berichte der Geschäftsführung sämtliche Abweichungen.

MANAGEMENT GUIDELINES

PO9 Assess and Manage IT Risks *(Beurteile und Manage IT-Risiken)*

Von	Inputs
PO1	Strategische und taktische IT-Pläne; IT-Service- und Projektportfolio
PO10	Risikomanagementplant für Projekte
DS2	Lieferanten-Risiken
DS4	Ergebnisse Contingency-Tests
DS5	Security-Bedrohungen und Schwachstellen
ME1	Historische Risiken (Trends und Ereignisse)
ME4	Unternehmensweiter Risikofreudigkeit bezüglich IT-Risiken

Outputs	Nach						
Risikobewertung	PO1	DS4	DS5	DS12	ME4		
Risikobeurteilung und -berichterstattung	ME4						
Richtlinien zum IT-Risikomanagement	PO6						
IT-bezogene Risikominderungs-Pläne	PO4	AI6					

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Bestimme die Ausrichtung des Risikomanagements (zB beurteile Risiken)	A	R/A	C	C	R/A	I					I
Verstehe relevante strategische Geschäftsziele		C	C	R/A	C	C					I
Verstehe relevante Ziele der Unternehmensprozesse				C	C	R/A					I
Identifiziere interne IT-Ziele und stelle die Verbindung zum Risiko her					R/A		C	C	C		I
Identifiziere Ereignisse, die mit Zielen zusammenhängen [manche sind business-orientiert (Geschäftsbereich ist A); manche sind IT-orientiert (IT ist A, Geschäftsbereich ist C)]	I			A/C	A	R	R	R	R		C
Beurteile Risiken, die mit Ereignissen zusammenhängen				A/C	A	R	R	R	R		C
Evaluiere die Risikoreaktion	I	I	A	A/C	A	R	R	R	R		C
Priorisiere und plane Control-Aktivitäten	C	C	A	A/C	R	R	C	C	C		C
Bewillige und stelle das Budget für Risikomaßnahmenpläne sicher		A	A		R	I	I	I	I		I
Unterhalte und überwache einen Risikomaßnahmenplan	A	C	I	R	R	C	C	C	C	C	R

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Sicherstellen, dass das Risikomanagement vollständig in Managementprozesse eingebettet ist
- Durchführen regelmäßiger Risikobeurteilungen mit Senior Manager und Schlüsselpersonen
- Empfehlen und Kommunizieren der Risikominderungsmaßnahmenpläne

treiben

Prozessziele

- Bestimme und reduziere die Wahrscheinlichkeit und Auswirkung von IT-Risiken.
- Bilde kosteneffektive Maßnahmenpläne für kritische IT-Risiken

treiben

IT-Ziele

- Schütze die Erreichung der IT-Ziele
- Schaffe Klarheit über die Geschäftsauswirkungen der Risiken von IT-Zielen und -Ressourcen
- Übernimm die Verantwortung für und schütze alle IT-Anlagen

werden gemessen durch

Key Performance Indicators

- % des IT-Budgets, welches in Risikomanagement-Aktivitäten (Beurteilung und Begrenzung) investiert wurde
- Häufigkeit der Reviews des IT-Risikomanagement-Prozesses
- % von Risikobeurteilungen, die abgezeichnet wurden
- Anzahl der durchgeführten Risikoüberwachungsberichte in der vereinbarten Häufigkeit
- % von identifizierten IT-Ereignissen, die in Risikobeurteilungen genutzt werden
- % der Risikomanagement-Maßnahmenpläne, die für die Implementierung genehmigt sind

werden gemessen durch

Key Goal Indicators

- % von identifizierten kritischen IT-Ereignissen, die beurteilt wurden
- Anzahl der neu identifizierten IT-Risiken (im Vergleich zum vorhergehenden Durchlauf)
- Anzahl der signifikanten Störungen, die durch nicht vom Risikobeurteilungsprozess identifizierten Risiken verursacht wurden
- % von identifizierten kritischen IT-Risiken mit entwickeltem Maßnahmeplan

werden gemessen durch

IT Key Goal Indicators

- % von kritischen IT-Zielen, die durch Risikobeurteilung abgedeckt sind
- % von IT-Risikobeurteilungen, die in den IT-Risikobeurteilungsansatz integriert sind

MATURITY MODEL

PO9 Assess and Manage IT Risks *(Beurteile und Manage IT-Risiken)*

Die Reife des Management des Prozesses *Assess and Manage IT Risks (Beurteile und Manage IT-Risiken)*, der die Geschäftsanforderungen an die IT erfüllt der Analyse und Kommunikation der IT-Risiken und deren potenzielle Auswirkungen auf Geschäftsprozesse und -ziele ist:

0 Non-existent (nicht existent):
Für Prozesse und Geschäftsentscheidungen werden keine Risikoeinschätzung vorgenommen. Das Unternehmen berücksichtigt die Auswirkungen von Sicherheitsschwachstellen und Unsicherheiten der Projektentwicklung nicht. Das Risikomanagement wird als unrelevant für die Beschaffung von IT-Lösungen und die Ablieferung von IT-Services angesehen.

1 Initial (initial):
IT-Risiken werden ad hoc berücksichtigt. Informelle Einschätzungen von Projektrisiken finden je nach Anforderungen eines Projektes statt. Risikoeinschätzungen werden vereinzelt in einem Projektplan identifiziert, aber selten an spezifische Manager übertragen. Bestimmte IT-bezogene Risiken wie Sicherheit, Verfügbarkeit und Integrität werden gelegentlich auf einer projektbezogenen Basis betrachtet. IT-bezogene Risiken, die alltägliche Betriebsprozesse betreffen, werden selten in Management-Meetings besprochen. Wenn Risiken berücksichtigt wurden, waren die ergriffenen risikomindernden Maßnahmen inkonsistent. Es besteht ein wachsendes Bewusstsein dafür, dass IT-Risiken wichtig sind und berücksichtigt werden müssen.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Es existiert ein unreifer und in Entwicklung stehender Ansatz zur Risikoeinschätzung, aber es ist dem Projektmanager überlassen, diesen anzuwenden. Das Risikomanagement siedelt sich meistens auf einer übergeordneten Ebene an und wird üblicherweise nur bei wesentlichen Projekten oder als Reaktion auf Probleme angewendet. Erst wenn Risiken identifiziert werden, werden Maßnahmen zur Risikoreduktion gestartet.

3 Defined (definiert):
Eine unternehmensweite Risikomanagement-Politik definiert, wann und wie Risikoeinschätzungen vorgenommen werden. Das Risikomanagement folgt einem festgelegten und dokumentierten Prozess. Das Risikomanagement-Training ist für alle Mitarbeiter verfügbar. Die Entscheidung, dem Risikomanagement-Prozess zu folgen und sich schulen zu lassen, liegt beim Einzelnen. Die Methodik zur Risikoeinschätzung ist überzeugend und korrekt und stellt sich, dass Schlüsselrisiken des Geschäfts identifiziert werden. Ein Prozess zur Reduktion von Schlüsselrisiken wird üblicherweise institutionalisiert, sobald die Risiken identifiziert wurden. Stellenbeschreibungen berücksichtigen Risikomanagement-Verantwortlichkeiten.

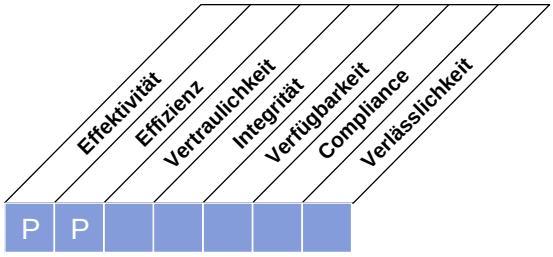
4 Managed and measurable (gemanaged und messbar):
Die Einschätzung und Verwaltung von Risiken sind Standardverfahren. Ausnahmen im Risikomanagement-Prozess werden an das IT-Management berichtet. Die Verantwortung des IT-Risikomanagements liegt auf der oberen Management-Ebene. Das Risiko wird sowohl auf der Ebene einzelner Projekte als auch regulär im Hinblick auf den IT-Gesamtbetrieb eingeschätzt und reduziert. Das Management wird auf Veränderungen in der Geschäfts- und IT-Umgebung hingewiesen, welche die IT-bezogenen Risikoszenarien signifikant beeinflussen könnten. Das Management ist in der Lage, die Risikoposition zu überwachen und sachkundige Entscheidungen über die zu akzeptierende Auswirkungen zu treffen. Alle identifizierten Risiken haben einen zugewiesenen Eigentümer und das obere und IT-Management hat den für das Unternehmen tolerierbaren Risikolevel festgelegt. Das IT-Management hat standardisierte Metriken zur Risikoeinschätzung und Definition von Risiko/Return-Raten entwickelt. Das Management budgetiert für ein Projekt für das operationelle Risikomanagement, um Risiken auf einer geregelten Basis neu zu beurteilen. Eine Risikomanagement-Datenbasis wurde entwickelt und ein Teil des Risikomanagement-Prozesses beginnt, automatisiert zu werden. Das IT-Management berücksichtigt Strategien zur Risikoreduktion.

5 Optimised (optimiert):
Das Risikomanagement befindet sich auf dem Level eines strukturierten, unternehmensweit durchgesetzten und gut verwalteten Prozesses. Good Practices werden im gesamten Unternehmen angewendet. Das Aufzeichnen, Analysieren und Berichten von Risikomanagement-Daten ist stark automatisiert. Leitlinien werden von operativ Verantwortlichen festgelegt und die IT-Organisation nimmt an Peergoups teil, um Erfahrungen auszutauschen. Das Risikomanagement ist in alle Geschäfts- und IT-Prozesse wirklich integriert, wird akzeptiert und involviert die User der IT-Services umfassend. Wenn Betrieb- und Investitions-Entscheidungen der IT ohne Beachtung des Risikomanagement-Plans getroffen werden, wird das Management dies erkennen und entsprechend reagieren. Das Management bewertet kontinuierlich Strategien zur Risikoreduktion.

HIGH-LEVEL CONTROL OBJECTIVE

PO10 Manage Projects *(Manage Projekte)*

Erstelle ein Programm- und Projektmanagement-Framework für das Management sämtlicher IT-Projekte. Das Framework sollte die korrekte Priorisierung und Koordination aller Projekte sicherstellen. Das Framework sollte einen Masterplan, die Zuweisung von Ressourcen, die Festlegung von Ergebnissen, die Freigaben durch Benutzer, eine phasenorientierten Ansatz bis zur Ablieferung, Qualitätssicherung, einen formalen Testplan, sowie Tests und einen Review nach Projektabschluss umfassen, um ein Projektrisikomanagement und einen Wertbeitrag für das Business sicherzustellen. Dieser Ansatz reduziert das Risiko von unerwarteten Kosten und eines Scheitern des Projektes, verbessert die Kommunikation zu und die Einbindung des Business und der Endbenutzer, stellt den Wertbeitrag und die Qualität der Projekt-Ergebnisse sicher und maximiert den Beitrag zu den IT-unterstützten Programmen.



Kontrolle über den IT-Prozess,

Manage Projects (*Manage Projekte*)

der die Anforderung des Unternehmens an die IT bezüglich

der Erbringung der Projektergebnisse innerhalb dem vereinbarten Zeitrahmen, Budget und Qualität

durch die Konzentration auf

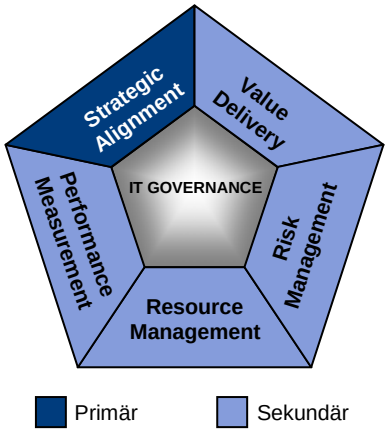
einen festgelegten Programm- und Projektmanagementansatz, der auf IT-Projekte angewandt wird, was die Beteiligung durch Stakeholder an und Überwachung von Projektrisiken und Projektfortschritt ermöglicht, *zufrieden stellt,*

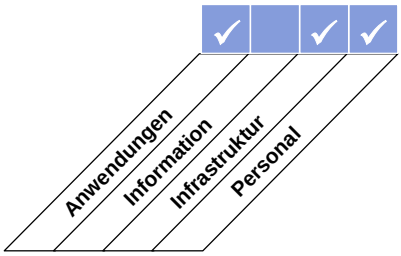
wird erreicht durch

- Festlegung und Durchsetzung der Frameworks und Ansätze für Programme und Projekte
- Veröffentlichung von der Projektmanagement-Anleitungen
- Durchführung der Projektplanung für jedes Projekt, das im Projektportfolio aufgeführt ist

und gemessen durch

- Prozent der Projekte, die die Erwartungen der Stakeholder erfüllen (zeitgerecht, innerhalb des Budgets und die Anforderungen treffend - gewichtet nach Bedeutung)
- Prozent der Projekte, die Post-Implementation Reviews erhalten
- Prozent der Projekte, die Projektmanagement-Standards und -praktiken folgen





DETAILLIERTE CONTROL OBJECTIVES

PO10 Manage Projects *(Manage Projekte)*

PO10.1 Programme Management Framework (Programmmanagement-Framework)
Unterhalte das Projekt-Programm in Verbindung mit dem Portfolio an IT-gestützten Investitionsprogrammen – durch Identifikation, Festlegung, Evaluierung, Priorisierung, Auswahl, Initiierung, Management und Steuerung von Projekten. Stelle sicher, dass die Projekte die Ziele des Programms unterstützen. Koordiniere die Aktivitäten und gegenseitigen Abhängigkeiten von mehreren Projekten, manage den Beitrag aller Projekte innerhalb des Programms zu den erwarteten Ergebnissen und löse Ressorcenbedarf und -konflikte.

PO10.2 Project Management Framework (Projektmanagement-Framework)
Erstelle und unterhalte ein allgemeines Projektmanagement-Framework, das den Umfang und Grenzen des Projektmanagements sowie die für alle unternommenen Projekte anzuwendenden Methodologien definiert. Diese Methodologien sollten mindestens die Initiierungs-, Planungs-, Ausführungs-, Controlling- und Projektabschlussphasen umfassen, sowie die Kontrollpunkte und Freigaben. Das Framework und die unterstützenden Methodologien sollten in das unternehmensweite Projektportfoliomanagement und die Programmmanagement-Prozesse integriert werden.

PO10.3 Project Management Approach (Projektmanagement-Ansatz)
Etabliere einen generischen Projektmanagement-Ansatz passend für Projekte unterschiedlicher Größe, Komplexität und rechtlicher Rahmenbedingungen. Die Struktur zur Projektsteuerung kann Rollen, Verantwortlichkeiten und Zuständigkeiten von Programm- und Projektsponsoren, Lenkungsausschuss, Projektbüro und Projektmanager und die Mechanismen, durch die diese die Verantwortlichkeiten übernehmen können (wie Berichterstattung und Phasen-Reviews). Stelle sicher, dass alle IT-Projekte Sponsoren mit ausreichender Autorität besitzen, um die Verantwortung für die Projektumsetzung im Rahmen der strategischen Gesamtprogramms umzusetzen.

PO10.4 Stakeholder Commitment (Beteiligung der Stakeholder)
Hole die Zusage und Beteiligung der betroffenen Stakeholder bei der Festlegung und Ausführung des Projektes im Rahmen des übergeordneten IT-gestützten Investitionsprogramms ein.

PO10.5 Project scope statement (Beschreibung des Projektumfangs)
Definiere und dokumentiere die Art und den Umfang des Projekts, um unter den Stakeholdern ein gemeinsames Verständnis für den Projektumfang zu bestätigen und zu entwickeln – und wie dieses Projekt sich verhält mit anderen Projekten innerhalb des IT-gestützten Investitionsprogramms. Die Definition sollte vor der Projektinitiierung durch die Programm- und Projektsponsoren formal freigegeben sein.

PO10.6 Project Phase Initiation (Initiierung von Projektphasen)
Stelle sicher, dass die Initialisierung wesentlicher Projektphasen formell verabschiedet und allen Stakeholdern kommuniziert wird. Die Genehmigung der Initialisierungsphase sollte auf Entscheiden der Programmsteuerung basieren. Die Genehmigung der nachfolgenden Phasen sollte auf einer Überprüfung und Abnahme der Ergebnisse der vorhergehenden Phase basieren und einer Abnahme eines aktualisierten Business-Case anlässlich der nächsten größeren Überprüfung des Programms. Im Fall sich überlappender Projektphasen sollte ein Punkt zur Freigabe durch die Programm- und Projektsponsoren festgelegt werden, um die Projektfortführung zu genehmigen.

PO10.7 Integrated Project Plan (Integrierter Projektplan)
Erstelle einen formellen und genehmigten integrierten (die Unternehmens- und IT Ressourcen umfassenden) Projektplan zur Steuerung der Projektumsetzung und Projektsteuerung während des gesamten Projekts. Die Aktivitäten und gegenseitigen Abhängigkeiten von mehreren Projekten innerhalb eines Programms sollten verstanden und dokumentiert sein. Der Projektplan sollte während der Projektlaufzeit unterhalten werden. Der Projektplan und die Änderungen daran sollten entsprechend der Frameworks zur Programm- und Projektsteuerung genehmigt werden.

PO10.8 Project Resources (Projekt-Ressourcen)
Lege die Verantwortlichkeiten, Beziehungen, Kompetenzen und Leistungskriterien der Projektteam-Mitglieder fest und spezifiziere für das Projekt die Grundlage für die Beschaffung und Zuweisung kompetenter Mitarbeiter und/oder Vertragsnehmer. Die Beschaffung von Produkten oder Diensten, welche für jedes Projekt benötigt werden, sollten geplant und gemanagt werden, um die Projektziele durch Verwendung der Beschaffungspraktiken des Unternehmens zu erreichen.

PO10.9 Project Risk Management (Projekt-Risikomanagement)
Beseitige oder reduziere spezifische, mit einzelnen Projekten in Verbindung stehende Risiken durch einen systematischen Prozess zur Planung, Identifikation, Analyse, Reaktion, Monitoring und Steuerung der Bereiche oder Ereignisse, die das Potential besitzen, unerwünschte Änderungen zu verursachen. Die Risiken, denen der Projektmanagement-Prozesses ausgesetzt ist, und der Projektergebnisse sollten festgehalten und zentral aufgezeichnet werden.

PO10.10 Project Quality Plan (Projekt-Qualitätsplan)
Bereite einen Qualitätsmanagementplan vor, der das Projekt-Qualitätssystem und dessen Umsetzung beschreibt. Der Plan sollte formell geprüft und durch alle betroffenen Parteien abgenommen werden und dann in den Projektplan integriert werden.

PO10.11 Project Change Control (Steuerung der Änderung von Projekten)
Entwickle ein System zur Steuerung von Änderungen für alle Projekte, so dass alle grundlegenden Änderungen am Projekt (zB Kosten, Zeitplan, Umfang und Qualität) angemessen überprüft, freigegeben und, entsprechend der Vorgaben des Programms und des Projekt-Governance-Frameworks, in den integrierten Projektplan eingearbeitet werden.

PO10.12 Project Planning of Assurance Methods (Planung von Bestätigungs-Methoden)
Identifiziere während der Projektplanung Bestätigungs-Methoden, die zur Unterstützung der Akkreditierung von neuen oder geänderten Systemen benötigt werden, und nehme diese in den integrierten Projektplan auf. Die Aufgaben sollten Gewissheit verschaffen, dass Internal Controls und Sicherheitseigenschaften den festgelegten Anforderungen entsprechen.

PO10.13 Project Performance Measurement, Reporting and Monitoring (Messung, Berichterstattung und Monitoring der Projektperformance)
Messe die Projektperformance an hand der wesentlichen Projektkriterien (zB Umfang, Zeitplan, Qualität, Kosten und Risiken). Identifiziere sämtliche Abweichungen vom Plan, beurteile deren Auswirkungen auf das Projekt und das übergeordnete Programm; berichte die Ergebnisse an die wesentlichen Stakeholder. Empfehle, implementiere und überwache – wo notwendig – Verbesserungsmaßnahmen entsprechend der Frameworks für Programm- und Projektsteuerung.

PO10.14 Project Closure (Projektabschluss)
Fordere, dass am Ende jedes Projektes die Projekt-Stakeholder bestätigen, ob das Projekt die geplanten Ergebnisse und den geplanten Nutzen erbracht hat. Identifiziere und kommuniziere alle offenen Aktivitäten, die notwendig sind, um die geplanten Projektergebnisse und den Nutzen des Programms zu erzielen, und identifiziere und dokumentiere die Lessons-Learned für künftige Projekte und Programme.

MANAGEMENT GUIDELINES

PO10 Manage Projects *(Manage Projekte)*

Von	Inputs
PO1	Projektportfolio
PO5	Aktualisiertes IT-Projektportfolio
PO7	IT Skills Matrix
PO8	Entwicklungsstandards
AI7	Post-Implementation-Review

Outputs	Nach						
Report der Projektperformance	ME1						
Risikomanagementplan für Projekte	PO9						
Projektmanagementanleitungen	AI1 ... AI 7						
Detaillierte Projektpläne	PO8	AI1 ... AI 7	DS6				
Aktualisiertes IT-Projektportfolio	PO1	PO5					

RACI-CHART*

Aktivitäten / Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Definiere ein Programm-/Portfolio-Management-Framework für IT-Investition			I	I	C	A	C	C			I
Erstelle und unterhalte ein IT-Projekt-Management-Framework						C		C			
Erstelle und unterhalte ein IT-Projektüberwachungs-, -messungs- und -management-System					C	A	R	R		R	C
Erstelle Projektaufträge, Termin-, Qualitäts-, Budget-, Kommunikations- und Risikomanagementpläne			I	I	C	A/R	C	C		C	C
Stelle die Beteiligung und das Engagement der Projekt-Stakeholder sicher					I	A	I	I		I	
Stelle die wirksame Steuerung der Projekte und Projektänderungen sicher					I	I		I			I
Definiere und implementiere Methoden für die Projektkontrolle und Reviews											

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Definition und Durchsetzung der Frameworks und Vorgehensansätze für Programme und Projekte
- Herausgabe der Projektmanagement-Anleitungen
- Durchführung der Projektplanung für jedes im Projektportfolio aufgeführte Projekt

werden gemessen durch

Key Performance Indicators

- % der Projekte, die Projektmanagement-Standards und -praktiken folgen
- % der zertifizierten oder geschulten Projektmanager
- % der Projekte, für die Post-Implementation Reviews durchgeführt werden
- % von Stakeholder, die sich an den Projekten beteiligen (Anteil der Einbindung)

treiben

Prozessziele

- Bilde Kontrollmechanismen für die Projektverfolgung und Kosten/Zeit
- Schaffe Transparenz des Projektstatus
- Führe rechtzeitig Projektmanagement Entscheidungen bei kritischen Meilensteinen durch

werden gemessen durch

Key Goal Indicators

- % von zeitgerechten und im Budgetrahmen liegenden Projekten
- % der Projekte, die die Erwartungen der Stakeholder erfüllen

treiben

IT-Ziele

- Reagiere auf Geschäftsanforderungen in Übereinstimmung mit der Unternehmensstrategie
- Setze Projekte pünktlich und im Budgetrahmen, entsprechend der Qualitätsstandards um
- Reagiere auf Anforderungen der Governance entsprechend der Geschäftsführungs-vorgaben

werden gemessen durch

IT Key Goal Indicators

- % der Projekte, die die Erwartungen der Stakeholder erfüllen (zeitgerecht, im Budgetrahmen und die Anforderungen treffend – gewichtet nach Bedeutung)

MATURITY MODEL

PO10 Manage Projects *(Manage Projekte)*

Die Reife des Management des Prozesses *Manage Projects (Manage Projekte)*, der die Geschäftsanforderungen an die IT erfüllt der Erbringung der Projektergebnisse innerhalb dem vereinbarten Zeitrahmen, Budget und Qualität ist:

0 Non-existent (nicht existent):
Verfahren zum Projektmanagement finden keine Anwendung und das Unternehmen berücksichtigt die Geschäftsauswirkungen von schlechter Projektleitung und Fehlern bei der Projektentwicklung nicht.

1 Initial (initial):
Die Entscheidung zur Nutzung von Verfahren und Ansätzen für das Projektmanagement innerhalb der IT bleibt den einzelnen IT -Managern überlassen. Eine Verpflichtung des Managements zur klaren Projekteigentümerschaft und zum Projektmanagement existiert nicht. Kritische Entscheidungen zum Projektmanagement werden ohne Input des Management der Anwender oder der Kunden getroffen. Kunden und Abnehmer werden kaum in die Festlegung von IT-Projekten einbezogen. Innerhalb der IT existiert keine klare Organisation für das Management von Projekten. Rollen und Verantwortlichkeiten für das Projektmanagement sind nicht festgelegt. Projekte, Zeitpläne und Meilensteine sind, wenn überhaupt, schlecht definiert. Die Aufwände der Projektmitarbeiter und Projektausgaben werden nicht verfolgt und mit Budgets abgeglichen.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Das Senior-Management hat ein Bewusstsein für die Notwendigkeit des IT-Projektmanagements entwickelt und kommuniziert. Das Unternehmen ist daran, bestimmte Techniken und Methoden fallweise zu entwickeln und anzuwenden. In IT-Projekten werden informell geschäftliche und technische Ziele definiert. Die Stakeholder des Projektes werden nur begrenzt in das IT-Projektmanagement eingebunden. Erste Leitlinien wurden für viele Aspekte des Projektmanagements entwickelt. Die Entscheidung zur Umsetzung der Leitlinien zum Projektmanagement bleibt den einzelnen Projektleitern überlassen.

3 Defined (definiert):
Die Verfahren und Methodologie zum IT-Projektmanagement wurden eingeführt und kommuniziert. Die IT-Projekte werden mit geeigneten geschäftlichen und technischen Zielen definiert. Das obere IT- und Geschäftsmanagement beginnt sich für das Management von IT-Projekten zu engagieren und wird eingebunden. Innerhalb der IT wird ein Projektmanagement-Office, mit ersten Rollen und Verantwortlichkeiten, festgelegt. IT-Projekte werden mit festgelegten und aktualisierten Meilensteilen, Zeitplänen, Budget- und Performance-Messungen überwacht. Schulungen für Projektmanagement stehen zur Verfügung. Die Schulungen für Projektmanagement sind aber hauptsächlich das Ergebnis der Initiativen einzelner Mitarbeiter. Verfahren zur Qualitätssicherung und Aktivitäten zur Nach-Implementierung von Systemen wurden festgelegt, werden allgemein jedoch nicht von den IT-Managern angewendet. Die Projekte beginnen als Portfolios verwaltet zu werden.

4 Managed and measurable (gemanaged und messbar):
Nach Projektabschluss fordert das Management definierte und standardisierte Projekt-Metriken und Erfahrungsberichte zum Review. Das Projektmanagement wird nicht nur innerhalb der IT, sondern unternehmensweit gemessen und bewertet. Verbesserungen der Maßnahmen zum Projektmanagement-Prozess werden formalisiert und mit Mitarbeitern des Projektteams, die auf Verbesserungen geschult sind, besprochen. Das IT-Management hat eine Projektorganisationsstruktur, mit dokumentierten Rollen, Verantwortlichkeiten und Bewertungskriterien der Mitarbeiter-Performance eingeführt. Kriterien zur Bewertung des Erfolgs bei jedem Meilenstein wurden eingeführt. Nutzen und Risiko werden vor, während und nach Abschluss eines Projekts gemessen und verwaltet. Die Projekte richten sich vermehrt an den Zielen des Unternehmens als nur an IT-spezifischen Zielen aus. Das obere Management sowie die Stakeholder unterstützen die Projekte stark und aktiv. Relevantes Training zum Projektmanagement wird für die Mitarbeiter im Projektmanagement-Office und in der IT-Funktion geplant.

5 Optimised (optimiert):
Eine bewährte, den kompletten Lebenszyklus von Projekten und Programmen betreffende Methodologie, wurde eingeführt, durchgesetzt und in die gesamte Unternehmenskultur integriert. Eine anhaltende Initiative zur Identifizierung und Institutionalisierung von Best Practices zum Projektmanagement wurde eingeführt. Eine IT-Strategie zur Besetzung und Mittelbeschaffung von Entwicklungs- und Betriebsprojekten wurde definiert und implementiert. Ein integriertes Projektmanagement-Office ist für Projekte und Programme vom Beginn bis hin zur Nach-Implementierung verantwortlich. Die unternehmensweite Planung von Programmen und Projekten stellt sicher, dass User- und IT-Ressourcen optimal genutzt werden, um strategische Initiativen zu unterstützen.

Diese Seite wurde absichtlich freigelassen

ACQUIRE AND IMPLEMENT

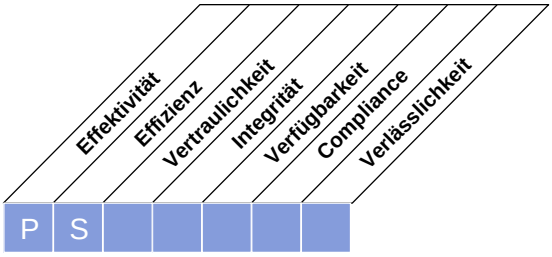
AI1 Identify Automated Solutions
(Identifiziere automatisierte Lösungen)
AI2 Acquire and Maintain Application Software
(Beschaffe und warte Anwendungssoftware)
AI3 Acquire and Maintain Technology Infrastructure
(Beschaffe und warte technologische Infrastruktur)
AI4 Enable Operation and Use
(Ermögliche Betrieb und Verwendung)
AI5 Procure IT Resources
(Beschaffe IT-Ressourcen)
AI6 Manage Changes
(Manage Changes)
AI7 Install and Accredit Solutions and Changes
(Installiere und akkreditiere Lösungen und Changes)

Diese Seite wurde absichtlich freigelassen

HIGH-LEVEL CONTROL OBJECTIVE

AI1 Identify Automated Solutions *(Identifiziere automatisierte Lösungen)*

Der Bedarf an neuen Anwendungen oder Funktionen erfordert vor einer Beschaffung oder Entwicklung eine Analyse, um sicherzustellen, dass die Unternehmensanforderungen mit einem wirksamen und wirtschaftlichen Ansatz abgedeckt sind. Dieser Prozess deckt die Festlegung des Bedarfs ab, die Berücksichtigung alternativer Möglichkeiten, die Überprüfung der technischen und wirtschaftlichern Machbarkeit, die Durchführung einer Risikoanalyse sowie einer Kosten-/Nutzen-Analyse und das Fällen einer endgültigen Entscheidung für eine Eigenentwicklung oder Beschaffung (engl.: *make or buy*). Alle diese Schritte versetzen Organisationen in die Lage, die Kosten für die Beschaffung und Implementierung von Lösungen zu minimieren und dabei sicherzustellen, dass diese dem Unternehmen helfen, seine Ziele zu erreichen.



Kontrolle über den IT-Prozess,

Identify Automated Solutions (*Identifiziere automatisierte Lösungen*)

der die Anforderung des Unternehmens an die IT bezüglich

der Überleitung der funktionalen Geschäfts- und Control-Anforderungen in ein wirksames und wirtschaftliches Design von automatisierten Lösungen

durch die Konzentration auf

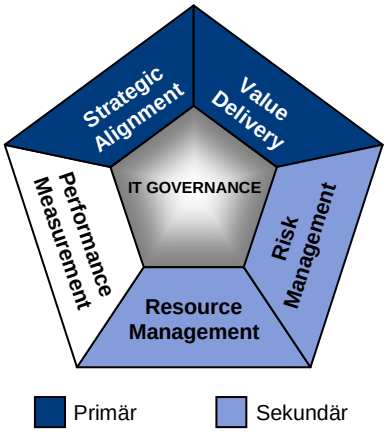
die Identifizierung technisch machbarer und kosteneffektiver Lösungen, *zufrieden stellt,*

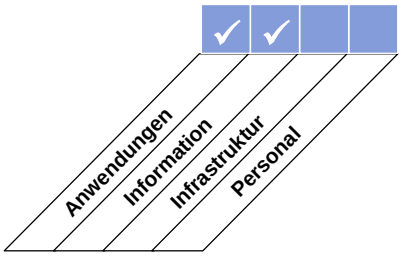
wird erreicht durch

- Festlegung von Unternehmens- und technischen Anforderungen
- Durchführung von Machbarkeitsstudien laut Entwicklungsstandards
- Freigabe (oder Ablehnung) der Ergebnisse von Anforderungs- und Machbarkeitsstudien

und gemessen durch

- Anzahl der Projekte, bei denen der prognostizierte Nutzen aufgrund falscher Annahmen in der Machbarkeitsstudie nicht erreicht wurde
- Prozent der Machbarkeitsstudien, die vom Geschäftsprozesseigner abgenommen wurden
- Prozent der BenutzerInnen, die mit der gelieferten Funktionalität zufrieden sind





DETAILLIERTE CONTROL OBJECTIVES

AI1 Identify Automated Solutions *(Identifiziere automatisierte Lösungen)*

AI1.1 Definition and Maintenance of Business Functional and Technical Requirements (Festlegung und Aktualisierung von funktionalen Geschäfts- und technischen Erfordernissen)
Identifiziere, priorisiere, spezifiziere und vereinbare die funktionalen Geschäfts- und technischen Erfordernisse, die den vollen Umfang aller nötigen Initiativen abdecken, um die vom IT-gestützten Investitionsprogramm erwarteten Ergebnisse zu erreichen. Definiere Kriterien für die Abnahme der Anforderungen. Diese Initiativen sollten sämtliche auf Grund der Art des Unternehmensgeschäfts, den Geschäftsprozessen, der Fertigkeiten und Fähigkeiten von Mitarbeitern, Organisationsstrukturen oder der Basistechnologie erforderlichen Änderungen beinhalten.

Die Anforderungen berücksichtigen funktionale Erfordernisse des Kerngeschäfts, die technologische Ausrichtung des Unternehmens, Leistungsfähigkeit, Kosten, Verlässlichkeit, Kompatibilität, Auditierbarkeit, Sicherheit (engl.: *security*), Verfügbarkeit und Kontinuität, Ergonomie, Verwendbarkeit (engl.: *usability*), Betriebssicherheit (engl.: *safety*) und gesetzliche Bestimmungen. Entwickle Prozesse, um die Integrität, Richtigkeit und Aktualität von Unternehmensanforderungen als Basis für die Steuerung der laufenden Systembeschaffung und -entwicklung sicherzustellen und zu steuern. Der Eigentümer (engl.: *owner*) dieser Anforderungen sollte der Business Sponsor sein.

AI1.2 Risk Analysis Report (Risikoanalyse-Bericht)
Identifiziere, dokumentiere und analysiere im Rahmen der Anforderungsdefinition Risiken, die mit den Geschäftsprozessen einhergehen. Risiken beinhalten Gefährdungen der Datenintegrität, Sicherheit, Verfügbarkeit, Datenschutz und die Einhaltung von Gesetzen und Verordnungen. Als Teil der Anforderungen sollten benötigte Maßnahmen für Internal Controls und Prüfspuren identifiziert werden.

AI1.3 Feasibility Study and Formulation of Alternative Courses of Action (Machbarkeitsstudie und Formulierung von alternativen Umsetzungsmöglichkeiten)
Führe eine Machbarkeitsstudie durch, die die Möglichkeit der Implementierung der Anforderungen prüft. Darin sollten alternative Vorgehensweisen für Software, Hardware, Services und Fähigkeiten identifiziert werden, welche die festgelegten funktionalen Geschäfts- und technischen Erfordernisse erfüllen. Ebenso sollte die technologische und wirtschaftliche Machbarkeit (Analyse von potentiellen Kosten und Nutzen) jeder identifizierten Alternative im Zusammenhang mit dem IT-gestützten Investitionsprogramm evaluiert werden. Als Folge der Beurteilung von Faktoren wie Änderungen an Geschäftsprozessen, Technologie und Fähigkeiten können bei der Entwicklung der Machbarkeitsstudie mehrere Iterationen notwendig sein. Mit Unterstützung der IT-Organisation soll das Management der Kernprozesse die Machbarkeitsstudie sowie die alternativen Vorgehensweisen bewerten und eine Empfehlung an den Auftraggeber (engl.: *business sponsor*) abgeben.

AI1.4 Requirements and Feasibility Decision and Approval (Freigabe der Anforderungsdefinition und Machbarkeit)
Der Auftraggeber (engl.: *business sponsor*) genehmigt und unterzeichnet entsprechend der vorab definierten Phasen die funktionalen Geschäfts- und technischen Anforderungen sowie die Ergebnisse der Machbarkeitsstudie. Jede Freigabe folgt auf Basis der erfolgreichen Beendigung von Qualitätsreviews. Der Auftraggeber trifft die endgültige Entscheidung hinsichtlich der Lösungsauswahl und Beschaffungsansatz.

MANAGEMENT GUIDELINES

AI1 Identify Automated Solutions *(Identifiziere automatisierte Lösungen)*

Von	Inputs
PO1	Strategische und taktische IT-Pläne
PO3	Regelmäßige 'state of technology' Aktualisierungen; Technologiestandards
PO8	Beschaffungs- und Entwicklungsstandards
PO10	Projektmanagementanleitungen; Detaillierte Projektpläne
AI6	Beschreibung Change-Prozess
DS1	SLAs
DS3	Performance- und Kapatizätsplan

Outputs	Nach					
Machbarkeitsstudie bezüglich Unternehmenserfordernissen	PO2	PO5	PO7	AI2 ... AI5		

RACI-CHART*

Aktivitäten / Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Definiere funktionale und technische Geschäftsanforderungen			C	C	R	C	R	R		A/R	I
Etabliere Prozesse für Integrität/Aktualität der Anforderungen				C		C		C		A/R	C
Identifiziere, dokumentiere und analysiere das Geschäftsprozessrisiko			A/R	R	R	R	C	R		R	C
Führe eine Machbarkeitsstudie und Auswirkungsanalyse der Umsetzung der vorgeschlagenen Geschäftsanforderungen			A/R	R	R	C	C	C		R	C
Bewerte den IT-betrieblichen Nutzen der vorgeschlagenen Lösungen		I	R	A/R	R	I	I	I		R	
Bewerte den Unternehmensnutzen der vorgeschlagenen Lösungen			A/R	R		C	C	C	I	R	
Entwickle einen Prozess zur Freigabe der Anforderungen			C	A/R		C	C	C		R	C
Genehmige und nimm vorgeschlagene Lösungen ab		C	A/R	R	R	C	C	C	I	R	C

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

Aktivitätsziele

- Festlegung von Unternehmens- und technischen Anforderungen
- Durchführung von Machbarkeitsstudien laut Entwicklungsstandards
- Frühzeitige Berücksichtigung von Security- und Control-Erfordernissen
- Freigabe (oder Ablehnung) der Ergebnisse von Anforderungs- und Machbarkeitsstudie

treiben

werden gemessen durch

Key Performance Indicators

- % der Projekte im Jahresplan der IT, für die Machbarkeitsstudien durchgeführt werden
- % der vom Geschäftsprozesseigner abgezeichneten Machbarkeitsstudien

Prozessziele

- Identifiziere Lösungen, die den User-Anforderungen entsprechen
- Identifiziere Lösungen, die technisch umsetzbar und kostengünstig sind
- Entscheide über „buy vs. build" zur Optimierung des Wertbeitrags und Minimierung der Risiken

treiben

werden gemessen durch

Key Goal Indicators

- % der mit der Genauigkeit der Machbarkeitsstudie zufriedenen Stakeholder
- Grad, zu dem sich der definierte Nutzen von der Machbarkeitsstudie bis zur Umsetzung verändert
- % der Anwendungen im Portfolio, die nicht Architekturkonform sind
- % der Machbarkeitsstudien, die entsprechend der geplanten Zeit und Kosten erstellt wurden

IT-Ziele

- Definiere, wie funktionale geschäftliche und Steuerungsanforderungen in wirksame und wirtschaftliche automatisierte Lösungen überführt werden.
- Reagiere auf Geschäftsanforderungen in Übereinstimmung mit der Unternehmensstrategie

werden gemessen durch

IT Key Goal Indicators

- Anzahl der Projekte, die den prognostizierten Nutzen aufgrund falscher Annahmen in der Machbarkeitsstudie nicht erreichen
- % der User, die mit der gelieferten Funktionalität zufrieden sind

MATURITY MODEL

AI1 Identify Automated Solutions *(Identifiziere automatisierte Lösungen)*

Die Reife des Management des Prozesses *Identify Acquire and Maintain Application Software (Beschaffe und warte Anwendungssoftware)*, der die Geschäftsanforderungen an die IT erfüllt, die funktionalen Geschäfts- und Control-Anforderungen in ein wirksames und wirtschaftliches Design von automatisierten Lösungen zu übersetzen, ist:

0 Non-existent (nicht existent):
Das Unternehmen verlangt keine Identifikation funktionaler und operativer Anforderungen für die Entwicklung, Implementierung oder Modifikation von Lösungen wie zum Beispiel Systeme, Services, Infrastruktur, Software und Daten. Das Unternehmen hat kein Bewusstsein über vorhandene, potentiell für das Geschäft relevante Technologielösungen entwickelt.

1 Initial (initial):
Man ist sich der Notwendigkeit bewusst, Anforderungen festzulegen und Technologielösungen zu identifizieren. Einzelne Gruppen diskutieren informell in Meetings Bedürfnisse und Anforderungen werden fallweise dokumentiert. Lösungen werden von einzelnen Personen entweder aufgrund eingeschränkter Marktkenntnis oder als Reaktion auf Lieferanten-Angebote identifiziert. Es bestehen minimale strukturierte Recherchen und Analysen vorhandener Technologie.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Einige intuitive Ansätze zur Identifikation von IT-Lösungen existieren und variieren innerhalb des Unternehmens. Lösungen werden informell aufgrund der internen Erfahrung und des Wissens der IT-Funktion identifiziert. Der Erfolg jedes Projekts hängt von der Fachkenntnis einiger weniger Schlüsselpersonen ab. Die Qualität der Dokumentation und der Entscheidungsfindung variiert beträchtlich. Unstrukturierte Ansätze zur Festlegung von Anforderungen und Identifikation von Technologielösungen werden angewandt.

3 Defined (definiert):
Eindeutige und strukturierte Ansätze für die Bestimmung von IT-Lösungen bestehen. Der Ansatz zur Bestimmung der IT-Lösungen verlangt die berücksichtigung von Alternativen, welche hinsichtlich Unternehmens- oder Benutzeranforderungen, technologische Möglichkeiten, wirtschaftliche Machbarkeit, Risikobewertung und anderer Faktoren beurteilt werden. Der Prozess zur Bestimmung von IT-Lösungen wird für manche Projekte – basierend Faktoren wie Entscheidungen der einzelnen involvierten Mitarbeiter, zugesagte Zeit des Managements und Größe sowie Priorität der ursprünglichen Geschäftsanforderungen. Strukturierte Ansätze werden zur Festlegung von Anforderungen und Identifikation von IT Lösungen verwendet.

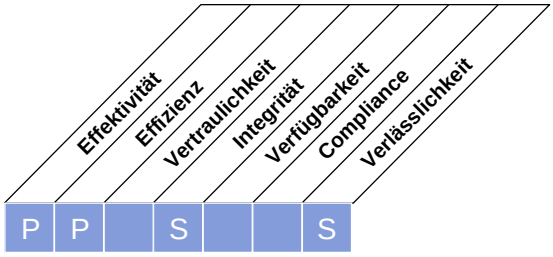
4 Managed and measurable (gemanaged und messbar):
Eine bewährte Methodik zur Identifikation und Bewertung von IT-Lösungen existiert und wird für die meisten Projekte angewendet. Die Projektdokumentation hat eine hohe Qualität und jede Projektphase wird korrekt genehmigt. Anforderungen werden gut ausformuliert und sind mit vordefinierten Strukturen abgestimmt. Lösungsalternativen werden inklusive der Analyse von Kosten und Nutzen in Betracht gezogen. Die Methodik ist klar, festgelegt, allgemein verstanden und messbar. Es gibt eindeutig definierte Schnittstellen zwischen dem IT-Management und dem Unternehmensmanagement für die Identifikation und Bewertung von IT-Lösungen.

5 Optimised (optimiert):
Die Methodik zur Identifikation und Bewertung von IT-Lösungen ist Gegenstand kontinuierlicher Verbesserung. Die Beschaffungs- und Implementierungsmethodik hat die erforderliche Flexibilität für große und kleine Projekte. Die Methodik wird durch interne und externe Wissensbestände unterstützt, welche Referenzmaterial über Technologielösungen beinhalten. Die Methodik selber produziert Dokumentation in einer vordefinierten Struktur, welche die Erstellung und den Unterhalt erleichtert. Neue Möglichkeiten werden häufig identifiziert, um durch Technologieeinsatz Wettbewerbsvorteile zu erreichen, Business Process Reengineering zu beeinflussen und die Effizienz gesamthaft zu verbessern. Das Management erkennt und reagiert entsprechend, wenn IT-Lösungen ohne die Betrachtung alternativer Technologien oder funktionaler Geschäftsanforderungen freigegeben werden.

HIGH-LEVEL CONTROL OBJECTIVE

AI2 Acquire and Maintain Application Software *(Beschaffe und warte Anwendungssoftware)*

Anwendungen müssen entsprechend der Unternehmenserfordernissen vorhanden sein. Dieser Prozess deckt den Entwurf der Anwendungen, die angemessene Berücksichtigung von Anwendungskontrollen und Security-Erfordernissen und die eigentliche Entwicklung und Konfiguration entsprechend der vorgegebenen Standards ab. Dies ermöglicht Organisationen, den Geschäftsbetrieb mit den richtigen automatisierten Anwendungen zu unterstützen.



Kontrolle über den IT-Prozess,

Acquire and Maintain Application Software (*Beschaffe und erhalte Anwendungssoftware*)

der die Anforderung des Unternehmens an die IT bezüglich

zeitgerechter und kostengünstiger Bereitstellung von Anwendungen entsprechend der Unternehmenserfordernisse

durch die Konzentration auf

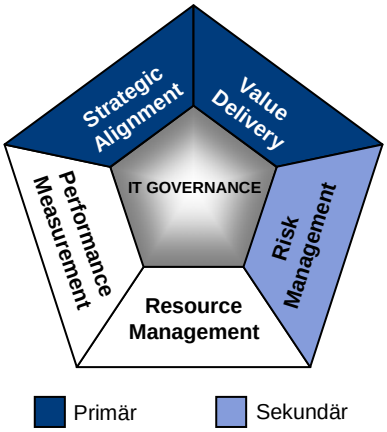
die Sicherstellung des Vorhandenseins eines zeitgerechten und kostenwirksamen Entwicklungsprozesses, *zufrieden stellt,*

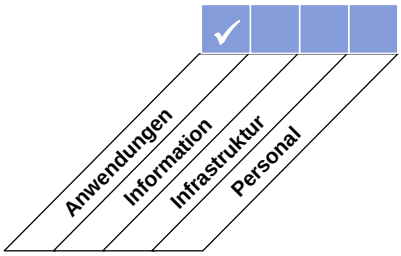
wird erreicht durch

- Überführung von Unternehmenserfordernissen in Entwurfsspezifikationen
- Einhaltung von Entwicklungsstandards für alle Modifikationen
- Trennung der Tätigkeiten von Entwicklung, Test und Betrieb

und gemessen durch

- Anzahl von Problemen pro Anwendung in der Produktion, welche eine sichtbare Stillstandzeit verursachen
- Prozent der mit der gelieferten Funktionalität zufriedenen User





DETAILLIERTE CONTROL OBJECTIVES

AI2 Acquire and Maintain Application Software *(Beschaffe und warte Anwendungssoftware)*

AI2.1 High-level Design (Grobdesign)
Überführe Unternehmenserfordernisse in eine grobe Designspezifikation für die Softwareentwicklung unter Berücksichtigung der technologischen Ausrichtung der Organisation sowie der Informationsarchitektur. Lasse die Designspezifikation genehmigen, um sicherzustellen, dass das Grobdesign den Anforderungen entspricht.

AI2.2 Detailed Design (Detailliertes Design)
Erstelle ein detailliertes Design und technische Software-Anforderungen an die Anwendung. Definiere Abnahmekriterien für die Anforderungen. Lasse die Anforderungen abnehmen, um sicherzugehen, dass sie dem Grobdesign entsprechen. Hierbei zu berücksichtigende Aspekte sind unter anderem: Festlegung und Dokumentation von Eingabeerfordernissen, Schnittstellendefinition, Benutzerschnittstelle, Design der Sammlung von Quelldaten, Anwendungsspezifikation, Festlegung und Dokumentation von Dateianforderungen, Verarbeitungserfordernisse, Definition der Anforderungen für Ausgaben, Steuerung und Auditierbarkeit, Sicherheit und Verfügbarkeit sowie Test. Führe eine neuerliche Bewertung durch, wenn während der Entwicklung oder Wartung wesentliche technische oder logische Änderungen auftreten.

AI2.3 Application Control and Auditability (Anwendungskontrollen und Nachvollziehbarkeit)
Stelle sicher, dass Unternehmenskontrollen angemessen in Anwendungskontrollen übergeleitet werden, sodass die Verarbeitung richtig, vollständig, zeitgerecht, autorisiert und nachvollziehbar erfolgt. Dabei speziell zu berücksichtigende Themen sind wie Autorisierungsmechanismen, Integrität von Informationen, Zugriffsschutz, Backup und der Entwurf der Prüfspur.

AI2.4 Application Security and Availability (Sicherheit und Verfügbarkeit der Anwendung)
Behandle Anforderungen an Sicherheit und Verfügbarkeit der Anwendung in Bezug auf identifizierte Risiken, unter Berücksichtigung der Datenklassifikation, der Informationssicherheitarchitektur der Organisation und dem Risikoprofil. Berücksichtige dabei unter anderem Aspekte wie Zugriffsberechtigungen und Rechtemanagement, den Schutz sensitiver Informationen auf allen Ebenen, Authentisierung und Transaktionsintegrität sowie automatische Wiederherstellung.

AI2.5 Configuration and Implementation of Acquired Application Software (Konfiguration und Implementierung von beschaffter Anwendungssoftware)
Ändere und implementiere zugekaufte, automatisierte Funktionen unter Anwendung der Verfahren für Konfiguration, Abnahme und Test. Zu berücksichtigende Gesichtspunkte sind: Validierung gegenüber Vertragsbedingungen, die Informationsarchitektur der Organisation, bestehende Anwendungen, Interoperabilität mit bestehende Anwendungen und Datenbanksystemen, Systemperformance, Dokumentation und Benutzerhandbücher, Pläne für Integrations und Systemtests.

AI2.6 Major Upgrades to Existing Systems (Wesentliche Upgrades bestehender Systeme)
Im Falle von wesentlichen Upgrades vorhandener Systeme, die in signifikanten Änderungen im derzeitigen Design und/oder der Funktionalität resultieren, folge einem ähnlichen Prozess wie für die Entwicklung neuer Systeme. Berücksichtige Auswirkungsanalyse, Kosten-/Nutzenanalyse und Anforderungsmanagement.

AI2.7 Development of Application Software (Entwicklung von Anwendungssoftware)
Stelle sicher, dass automatisierte Funktionalität entsprechend der Designspezifikationen, Entwicklungs- und Dokumentationsstandards und Qualitätsanforderungen entwickelt wird. Bestätige und beschließe jede wichtige Phase im Software-Entwicklungsprozess nach erfolgreichen Reviews von Funktionalität, Leistung und Qualität. Berücksichtige hierbei: die Bestätigung, dass die Designspezifikationen mit den geschäftlichen, funktionalen und technischen Erfordernissen übereinstimmt; die Freigabe von Change-Requests; sowie die Bestätigung, dass die Anwendungssoftware mit vorhandenen Produktionssystemen kompatibel und für eine Migration bereit ist. Stelle außerdem sicher, dass alle rechtlichen und vertraglichen Aspekte für durch Dritte entwickelte Anwendungssoftware identifiziert und behandelt werden.

AI2.8 Software Quality Assurance (Software-Qualitätssicherung)
Entwickle einen Softwarequalitätssicherungsplan, stelle benötigte Ressourcen bereit und setze den Plan um, um die in der Anforderungsdefinition und den Qualitätsrichtlinien und Verfahren der Organisation festgelegte Qualität zu erreichen. Beachte im Qualitätssicherungsplan die Spezifikation von Qualitätskriterien sowie einen Validierungs- und Verifikationsprozess, der auch Inspektion, Walkthroughs und Testen beinhaltet.

AI2.9 Application Requirements Management (Management von Anforderungen an die Anwendung)
Stelle sicher, dass während Entwurf, Entwicklung und Implementierung der Status jeder Anforderung (einschließlich der abgelehnten Anforderungen) nachvollzogen werden kann und Änderungen von Anforderungen in einem etablierten Change-Management-Prozess genehmigt werden.

AI2.10 Application Software Maintenance (Wartung von Anwendungssoftware)
Entwickle eine Strategie und einen Plan für Wartung und Release von Software. Beachte dabei unter anderem Releaseplanung und -steuerung, Ressourcenplanung, Fehlerbehandlung und -behebung (engl: *bugfixing und fault correction*), geringfügige Verbesserungen, Pflege der Dokumentation, Notfalls-Changes, Interdependenzen mit anderen Anwendungsprogrammen und Infrastruktur, Strategien für Upgrades, vertragliche Konditionen wie Support und Upgrades, periodische Reviews gegenüber den Unternehmensanforderungen, Risiken und Sicherheitsanforderungen.

MANAGEMENT GUIDELINES

AI2 Acquire and Maintain Application Software *(Beschaffe und warte Anwendungssoftware)*

Von	Inputs
PO2	Data Dictionary; Datenklassifikationsschema; Optimierter Geschäftsanwendungsplan
PO3	Regelmäßige 'state of technology' Aktualisierungen
PO5	Kosten-/Nutzenberichte
PO8	Beschaffungs- und Entwicklungsstandards
PO10	Projektmanagementrichtlinien; Detaillierte Projektpläne
AI1	Machbarkeitsstudie bezüglich Unternehmenserfordernissen
AI6	Beschreibung Change-Prozess

Outputs	Nach						
Spezifikation von anwendungsspezifischen Sicherheitsmaßnahmen	DS5						
Wissen über Anwendungen und Standardsoftware	AI4						
Beschaffungsentscheidungen	AI5						
Vorabversionen von SLAs	DS1						
Verfügbarkeits-, Kontinuitäts- und Recovery Spezifikation	DS3	DS4					

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Überleitung von Unternehmensanforderungen in Grobdesign-Spezifikationen					C		C	A/R		R	C
Vorbereitung detaillierter Design- und technischer Software-				I	C	C	C	A/R		R	C
Spezifikation von Anwendungskontrollen innerhalb des Designs					R	C		A/R		R	R
Anpassung und Implementierung beschaffter automatisierter Funktionalität					C	C		A/R		R	C
Entwicklung formalisierter Methoden und Prozesse zum Management des Anwendungsentwicklungsprozesses				C		C	C	A	C	R	C
Entwicklung eines Software-Qualitätssicherungsplans für das Projekt					I		C	R		A/R	C
Verfolgung und Management von Anwendungsanforderungen								R		A/R	
Entwicklung eines Wartungsplans für Software-Anwendungen				C		C		A/R		C	

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Überleitung von Unternehmensanforderungen in Designspezifikationen
- Einhaltung der Entwicklungsrichtlinien für sämtliche Modifikationen
- Priorisierung der Anforderungen auf Basis der Unternehmensrelevanz
- Trennung von Entwicklung, Test und operativen Tätigkeiten
- Wirksamer Einsatz von Investitionen in vorhandene Technologie

treiben

Prozessziele

- Beschaffe und unterhalte Anwendungen, die kostenwirksam die festgehaltenen Unternehmensanforderungen erfüllen
- Beschaffe und unterhalte mit der IT-Strategie und IT-Architektur abgestimmte Anwendungen
- Stelle sicher, dass der Entwicklungsprozes rasch und kostenwirksam ist

treiben

IT-Ziele

- Definiere, wie funktionale geschäftliche und Kontrollanforderungen in wirksame und wirtschaftliche automatisierte Lösungen überführt werden
- Beschaffe und unterhalte integrierte und standardisierte Anwendungssysteme

werden gemessen durch

Key Performance Indicators

- % der Anwendungssoftwareprojekte, für die ein Qualitätssicherungsplan entwickelt und ausgeführt wird
- % der Anwendungssoftwareprojekte, für die ein angemessenes Review und eine Abnahme der Einhaltung von Entwicklungsstandards durchgeführt wird
- Durchschnittlich benötigte Zeit, um Funktionalität zu realisieren, basierend auf Messgrößen wie Function Points oder Lines of Code
- Durchschnittlich benötigter Programmieraufwand zur Funktionalitätsrealisierung basierend auf Messgrößen wie Function Points oder Lines of Code

werden gemessen durch

Key Goal Indicators

- % der Entwicklungsprojekte, die innerhalb des vorgesehenen Zeit und des vorgehenen Budgets bleiben
- % des Entwicklungsaufwands, der für den Unterhalt vorhandener Anwendungen aufgebracht wird
- Anzahl der Probleme pro Anwendung in der Produktion, die sichtbare Stillstandzeit verursachen
- Anzahl berichteter Fehler pro Monat (pro Function Point)

werden gemessen durch

IT Key Goal Indicators

- % der Projekte, die Unternehmensänderungen innerhalb des geforderten Zeitrahmens herbeiführen
- Anzahl der Projekte, bei denen der festgelegte Nutzen aufgrund schwachen Anwendungsdesigns oder -entwicklung nicht erreicht wurde
- Prozent der mit der gelieferten Funktionalität zufriedenen User

MATURITY MODEL

AI2 Acquire and Maintain Application Software *(Beschaffe und warte Anwendungssoftware)*

Die Reife des Management des Prozesses *Identify Acquire and Maintain Application Software (Beschaffe und warte Anwendungssoftware)*, der die Geschäftsanforderungen an die IT erfüllt, Anwendungen entsprechend der Unternehmenserfordernisse rechtzeitig und zu vernünftigen Kosten bereitzustellen, ist:

0 Non-existent (nicht existent):
Es gibt keinen Prozess für Entwurf und Spezifikation von Anwendungen. Typischerweise werden Anwendungen basierend auf verkäufergetriebenen Angeboten, Markenwiedererkennung oder der Vertrautheit der IT-Mitarbeiter mit spezifischen Produkten mit geringer oder keiner Beachtung der tatsächlichen Anforderungen beschafft.

1 Initial (initial):
Man ist sich bewusst, dass ein Prozess für Beschaffung und Unterhalt von Anwendungen notwendig ist – die Ansätze für Beschaffung und Unterhalt der Anwendungssoftware variieren von Projekt zu Projekt. Eine Vielzahl individueller Lösungen für bestimmte Unternehmensanforderungen wurde vermutlich unabhängig voneinander beschafft, was zu Ineffizienz in Wartung und Support führt. Die Sicherheit und Verfügbarkeit der Anwendung wird bei Entwurf oder Beschaffung nur geringfügig beachtet.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Es existieren unterschiedliche, jedoch ähnliche, Prozesse für Beschaffung und Unterhalt von Anwendungen basierend auf der Fachkenntnis der IT-Abteilung. Die Erfolgsrate für Anwendungen hängt in hohem Maße von den innerbetrieblichen Kenntnissen und den Erfahrungswerten in der IT ab. Die Wartung ist normalerweise problematisch und leidet, falls internes Wissen aus der Organisation verloren geht. Die Anwendungssicherheit und -verfügbarkeit wird bei Entwurf oder Beschaffung von Anwendungssoftware nur geringfügig beachtet.

3 Defined (definiert):
Für Beschaffung und Unterhalt von Anwendungssoftware existiert ein eindeutiger, definierter und generell verstandener Prozess. Dieser Prozess ist auf IT- und Unternehmensstrategie ausgerichtet. Es wird versucht, den dokumentierten Prozess einheitlich für unterschiedliche Anwendungen und Projekte anzuwenden. Die Methodiken sind generell inflexibel und nur schwer für alle Fälle anwendbar, weshalb vermutlich Schritte umgangen werden. Wartungsarbeiten werden inhaltlich und zeitlich geplant und koordiniert.

4 Managed and measurable (gemanaged und messbar):
Es existiert eine formale und wohlverstandene Methodik, die einen Entwurfs- und Spezifikationsprozess, Kriterien für die Beschaffung, einen Prozess zum Testen sowie Anforderungen an die Dokumentation umfasst. Dokumentierte und abgesprochene Abnahmemechanismen existieren, um die Ausführung aller Schritte sowie die Genehmigung von Ausnahmen sicherzustellen. Praktiken und Verfahren wurden so weiterentwickelt, dass sie für das Unternehmen geeignet sind, von allen Mitarbeitern angewandt werden und für die meisten Anwendungsanforderungen anwendbar sind.

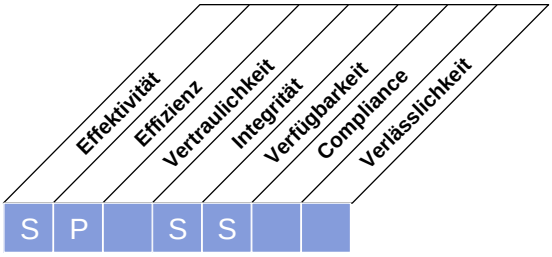
5 Optimised (optimiert):
Die Praktiken für Beschaffung und Unterhalt von Anwendungsprogrammen sind am definierten Prozess ausgerichtet. Der Ansatz basiert auf einzelne Komponenten, wobei vordefinierte, standardisierte Anwendungen auf Unternehmensanforderungen angeglichen werden. Dieser Ansatz wird unternehmensweit eingesetzt. Die Beschaffungs- und Unterhaltsmethodik ist weit entwickelt und erlaubt den schnellen Einsatz von Anwendungen, wodurch eine hohe Reaktionsfähigkeit und Flexibilität bezogen auf Änderungen in den Unternehmensanforderungen ermöglicht wird. Die Methodik für Beschaffung und Unterhalt von Anwendungssoftware wird kontinuierlich verbessert und durch interne und externe Wissensdatenbanken unterstützt, welche Referenzmaterial und Best Practice Verfahren enthalten. Durch die Methodik wird Dokumentation in einer vordefinierten Struktur erzeugt, was den Produktivbetrieb und den Unterhalt wirtschaftlich macht.
.

Diese Seite wurde absichtlich freigelassen

HIGH-LEVEL CONTROL OBJECTIVE

AI3 Acquire and Maintain Technology Infrastructure *(Beschaffe und warte technologische Infrastruktur)*

Organisationen sollten Prozesse für die Beschaffung, Implementierung und Erneuerung der technischen Infrastruktureinrichtungen aufweisen. Dies erfordert eine geplante Vorgehensweise für Beschaffung, Unterhalt und Schutz der Infrastruktur, die mit den vereinbarten technologischen Strategien im Einklang steht, sowie die Bereitstellung von Entwicklungs- und Testumgebungen. Dies stellt sicher, dass ein technischer Support für die Anwendungen permanent zur Verfügung steht.



Kontrolle über den IT-Prozess,

Acquire and maintain technology infrastructure (*Beschaffe und warte technologische Infrastruktur*)

der die Anforderung des Unternehmens an die IT bezüglich

Beschaffung und Unterhalt einer integrierten und standardisierten IT-Infrastruktur

durch die Konzentration auf

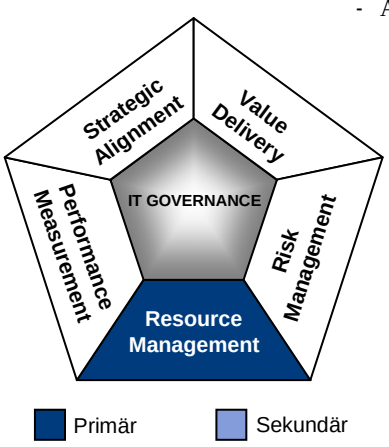
die Bereitstellung geeigneter Plattformen für die AnwendungGeschäftsanwendungen in Übereinstimmung mit der definierten IT-Architektur und den Technologiestandards, *zufrieden stellt*,

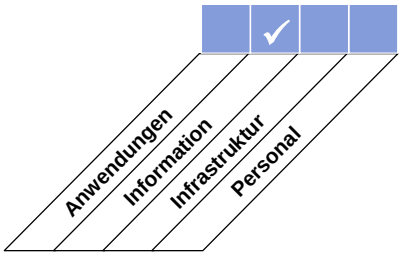
wird erreicht durch

- Entwicklung eines mit dem technologischen Infrastrukturplan konformen Technologiebeschaffungsplans
- Planung der Wartung der Infrastruktur
- Implementierung von Internal Control, Sicherheits- und Prüfmaßnahmen

und gemessen durch

- Prozent der Plattformen, die nicht mit den definierten IT-Architektur- und Technologiestandards konform sind
- Anzahl der kritischer Geschäftsprozesse, die von (sehr bald) obsoleter Infrastruktur unterstützt werden
- Anzahl der Infrastrukturkomponenten, die (bald) nicht mehr unterstützt werden





DETAILLIERTE CONTROL OBJECTIVES

AI3 Acquire and Maintain Technology Infrastructure *(Beschaffe und warte technologische Infrastruktur)*

AI3.1 Technological Infrastructure Acquisition Plan (Beschaffungsplan für technologische Infrastruktur)
Entwickle einen Plan für die Beschaffung, Implementierung und Wartung der technologischen Infrastruktur, der die bestehenden funktionalen Geschäfts- und technischen Anforderungen erfüllt und im Einklang mit der unternehmensweiten technologischen Richtung steht. Der Plan sollte künftige Flexibilität zur Kapazitätserweiterungen, Kosten für den Übergang, technische Risiken und die Gesamtausgaben über den Lebenszyklus von Technologie-Upgrades umfassen. Beurteile bei Einsatz von neueren technischen Möglichkeiten deren Komplexitätskosten und die wirtschaftliche Stabilität des Anbieters und Produktes.

AI3.2 Infrastructure Resource Protection and Availability (Schutz und Verfügbarkeit von Infrastrukturressourcen)
Implementiere Maßnahmen zur Internal Control, Sicherheit und Prüfbarkeit während der Konfiguration, Integration und Wartung von Hardware und Infrastruktur-Software, um Ressourcen zu schützen und Verfügbarkeit und Integrität sicher zu stellen. Die Verantwortung für die Verwendung von empfindlichen Infrastrukturkomponenten sollten klar festgelegt und von denen verstanden werden, die Infrastrukturkomponenten entwickeln und integrieren. Die Verwendung sollte gemonitort und evaluiert werden.

AI3.3 Infrastructure Maintenance (Wartung von Infrastruktur)
Entwickle eine Strategie und einen Plan für die Wartung der Infrastruktur und stelle sicher, dass Changes entsprechend des unternehmensweiten Change-Management-Prozesses gesteuert ablaufen. Berücksichtige regelmäßige Reviews an Hand des Unternehmensbedarfs, Strategien für Patch-Management und Upgrade, Risiken, Verletzbarkeitsanalysen und Sicherheitsanforderungen.

AI3.4 Feasibility Test Environment (Testumgebung)
Etabliere eine Entwicklungs- und Testumgebung, um in frühen Stadien des Beschaffungs- und Entwicklungsprozesses wirksame und wirtschaftliche Machbarkeits- und Integrationstests für Anwendungen und Infrastrukturen zu unterstützen. Berücksichtige Funktionalität, Hard- und Softwarekonfiguration, Integrations- und Performancetests, Migration zwischen den Umgebungen, Versionskontrolle, Werkzeuge und Daten für Tests sowie Sicherheit.

MANAGEMENT GUIDELINES

AI3 Acquire and Maintain Technology Infrastructure *(Beschaffe und warte technologische Infrastruktur)*

Von	Inputs
PO3	Infrastrukturplan der Technologie; Standards und Möglichkeiten; Regelmäßige 'state of technology' Aktualisierungen
PO8	Beschaffungs- und Entwicklungsstandards
PO10	Projektmanagementanleitungen; Detaillierte Projektpläne
AI1	Machbarkeitsstudie bezüglich Unternehmenserfordernisse
AI6	Beschreibung Change-Prozess
DS3	Performance- und Kapatizätsplan (Anforderungen)

Outputs	Nach
Beschaffungsentscheidungen	AI5
Konfiguriertes System, fertig für Test / Installation	AI7
Anforderungen an physische Infrastruktur	DS12
Überarbeitung technologischer Standards	PO3
Anforderungen an Systemmonitoring	DS3
Knowledge über Infrastruktur	AI4
Vorabversionen von OLAs	DS1

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Definiere Beschaffungsverfahren/-prozesse		C		A		C	C	C	R		I
Verhandle die Beschaffung und beschaffe die benötigte Infrastruktur von (akkreditierten) Lieferanten		C/I		A	I	R	C	C	R		I
Definiere eine Strategie und plane die Wartung für Infrastruktur				A		R	R	R	C		
Konfiguriere Infrastrukturkomponenten				A		R	C				I

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele
- Entwicklung eines mit dem technologischen Infrastrukturplan konformen Technologiebeschaffungsplans
- Planung der Wartung von Infrastruktur
- Bereitstellung einer Entwicklungs- und Testumgebungsinfrastruktur
- Implementierung von Internal Control, Sicherheits- und Prüfmaßnahmen

treiben

Prozessziele
- Bereitstellung geeigneter Plattformen für die mit der definierten IT-Architektur und den Technologiestandards abgestimmten Geschäftsanwendungen
- Bereitstellung einer verlässlichen und sicheren IT-Infrastruktur

treiben

IT-Ziele
- Beschaffe und warte integrierte und standardisierte IT-Infrastruktur
- Optimiere IT-Infrastruktur, Ressourcen und Fähigkeiten
- Stelle IT-Agilität her

werden gemessen durch

Key Performance Indicators
- Anzahl und Art der Notfalländerungen an Infrastruktur-Komponenten
- Anzahl offener Beschaffungsanfragen
- Durchschnittliche Zeit zur Konfiguration von Infrastruktur-Komponenten

werden gemessen durch

Key Goal Indicators
- % der nicht mit der definierten IT-Architektur und den Technologiestandards abgestimmten Plattformen
- Anzahl verschiedener Technologieplattformen nach Funktion im gesamten Unternehmen
- % der außerhalb des Beschaffungsprozesses beschafften Infrastrukturkomponenten
- Anzahl der nicht mehr oder bald nicht mehr unterstützten Infrastrukturkomponenten

werden gemessen durch

IT Key Goal Indicators
- Anzahl der von (bald) veralteter Infrastruktur unterstützten kritischen Geschäftsprozesse

MATURITY MODEL

AI3 Acquire and Maintain Technology Infrastructure *(Beschaffe und warte technologische Infrastruktur)*

Die Reife des Management des Prozesses *Acquire and Maintain Technology Infrastructure (Beschaffe und warte technologische Infrastruktur)*, der die Geschäftsanforderungen an die IT erfüllt, eine integrierte und standardisierte IT-Infrastruktur zu beschaffen und zu unterhalten, ist:

0 Non-existent (nicht existent):
Die Verwaltung der IT-Infrastruktur wird nicht als ausreichend wichtiges Thema verstanden, das angegangen werden muss.

1 Initial (initial):
Für jede neue Anwendung werden Changes in der Infrastruktur ohne einen Gesamtplan vorgenommen. Obwohl ein Bewusstsein für die Wichtigkeit der IT-Infrastruktur vorhanden ist, existiert kein Gesamtansatz. Die Unterhaltsaktivitäten richten sich nur nach kurzfristigen Erfordernissen. Die Produktionsumgebung ist die Testumgebung.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Die taktischen Ansätze bei Beschaffung und Unterhalt der IT-Infrastruktur sind konsistent. Beschaffung und Unterhalt der IT-Infrastruktur basiert auf keiner definierten Strategie und beachtet die Anforderungen der zu unterstützenden Geschäftsanwendungen nicht. Ein Verständnis für die Wichtigkeit der IT-Infrastruktur ist vorhanden und wird durch einige formelle Praktiken unterstützt. Unterhalt wird manchmal zeitlich geplant, ist aber nicht vollständig geplant und koordiniert. Für bestimmte Umgebungen bestehen separate Testumgebungen.

3 Defined (definiert):
Ein klarer, definierter und allgemein verstandener Prozess existiert für Beschaffung und Unterhalt der IT-Infrastruktur. Der Prozess unterstützt die Anforderungen kritischer Geschäftsanwendungen und ist auf die IT- und Geschäftsstrategie angepasst, wird aber nicht konsistent angewendet. Unterhalt ist geplant, zeitlich vorgesehen und koordiniert. Verschiedene Umgebungen für Test und Produktion sind vorhanden.

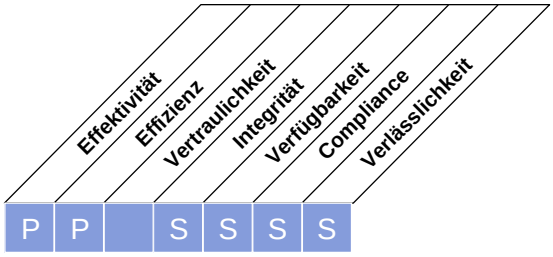
4 Managed and measurable (gemanaged und messbar):
Der Prozess für Beschaffung und Unterhalt der IT-Infrastruktur ist soweit entwickelt, dass er für die meisten Situationen geeignet ist, konsistent befolgt wird und auf Wiederverwendbarkeit ausgerichtet ist. Die IT-Infrastruktur unterstützt die Geschäftsanwendungen angemessen. Der Porzess ist gut organisiert und proaktiv. Die Kosten und die Vorlaufzeit, um den erwarteten Grad an Skalierbarkeit, Flexibilität und Integration zu erreichen, sind teilweise optimiert.

5 Optimised (optimiert):
Der Prozess für Beschaffung und Unterhalt der IT-Infrastruktur ist proaktiv und eng mit den kritischen Geschäftsanwendungen und die IT-Architektur abgestimmt. Good Practices zu Technologie-Lösungen werden befolgt und das Unternehmen kennt die neuesten Plattformentwicklungen und Managementwerkzeuge. Kosten werden durch Rationalisierung und Standardisierung der Infrastrukturkomponenten und durch Automatisierung gesenkt. Ein hohes technisches Bewusstsein kann auf optimale Art und Weise die Performance proaktiv verbessern, inklusive der Beachtung von Outsourcing-Optionen. Die IT-Infrastruktur wird als wesentliche Möglichkeit zur Beeinflussung des Nutzens der IT gesehen.

HIGH-LEVEL CONTROL OBJECTIVE

AI4 Enable Operation and Use (*Ermögliche Betrieb und Verwendung)*

Das Wissen um neue Systeme muss zur Verfügung gestellt werden. Dieser Prozess erfordert die Entwicklung von Dokumenten und Handbüchern für User und die IT und stellt Schulungen zur Verfügung, um die korrekte Verwendung und den Betrieb von Anwendungen und Infrastruktur sicherzustellen.



Kontrolle über den IT-Prozess,

Enable Operation and Use (*Ermögliche Betrieb und Verwendung*)

der die Anforderung des Unternehmens an die IT bezüglich

der Sicherstellung der Zufriedenheit der Enduser mit Serviceangeboten und -levels, und nahtlose Integration der Anwendungen und Techniklösungen in Geschäftsprozesse

durch die Konzentration auf

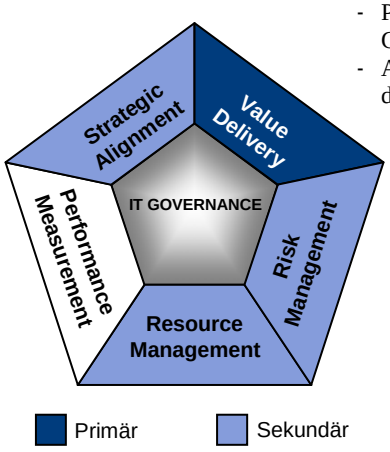
die Bereitstellung wirksamer Anwender- und Betriebshandbücher und Schulungsunterlagen für die Weiterleitung des für den erfolgreichen Betrieb und Anwendung der Systeme notwendigen Wissens , *zufrieden stellt,*

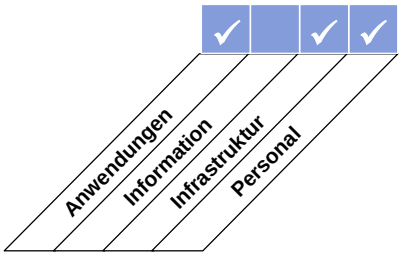
wird erreicht durch

- Entwicklung und Bereitstellung von verfügbaren Dokumenten zum Wissenstransfer
- Kommunikation mit und die Schulung von Usern, Businessmanagement, Support- und Betriebspersonal
- Erstellung von Schulungsunterlagen

und gemessen durch

- Anzahl der Applikationen, deren IT-Verfahren nahtlos in Geschäftsprozesse integriert sind
- Prozent der mit den Anwenderschulungen und den Schulungsunterlagen zufriedenen Geschäftsprozesseigentümer
- Anzahl der Applikationen mit angemessenen Anwenderschulungen und Schulungen des operativen Supports





DETAILLIERTE CONTROL OBJECTIVES

AI4 Enable Operation and Use (*Ermögliche Betrieb und Verwendung)*

AI4.1 Planning for Operational Solutions (Planung für operative Lösungen)
Entwickle einen Plan, um als Ergebnis einer Einführung oder eines Upgrades eines automatisierten Systems oder von Infrastruktur, alle technischen Aspekte, betrieblichen Möglichkeiten und erforderlichen Service Levels zu identifizieren und zu dokumentieren, damit alle Stakeholder frühzeitig die Verantwortung für die Erstellung von Verfahren für das Management, für User und für den Betrieb übernehmen können.

AI4.2 Knowledge Transfer to Business Management (Transfer von Knowledge and den Fachbereich)
Transferiere an das Fachbereichsmanagement Wissen, um ihm zu ermöglichen, die Eigentümerschaft über die Anwendung und Daten zu übernehmen und die Verantwortung für die Leistungserbringung und -qualität, Internal Control und Administrationsprozesse der Anwendung zu übernehmen. Der Wissenstransfer soll Freigaben für den Zugriff, Rechteverwaltung, Funktionstrennung, automatisierte Geschäftskontrollen, Backup und Recovery, physische Sicherheit und Archivierung von Urbelegen umfassen.

AI4.3 Knowledge Transfer to End Users (Transfer von Knowledge and Endbenutzer)
Transferiere an Endbenutzer Wissen und Fertigkeiten, um ihnen die wirksame und wirtschaftliche Verwendung der Anwendung zur Unterstützung der Geschäftsprozesse zu ermöglichen. Der Wissenstransfer sollte die Entwicklung eines Trainingsplan für erstmalige und laufende Schulung und die Entwicklung der Fertigkeiten, Schulungsmaterialien, Benutzerhandbücher, Verfahrenshandbücher, Online-Hilfe, Unterstützung durch den Service Desk, Identifikation von Key-Usern und Evaluation umfassen.

AI4.4 Knowledge Transfer to Operations and Support Staff (Transfer von Knowledge an Betriebs- und Supportmitarbeiter)
Transferiere an den Betrieb und den technischen Supportmitarbeiter Wissen, um ihnen die wirksame und wirtschaftliche Bereitstellung, Unterstützung und Wartung der Anwendung und der korrespondierenden Infrastruktur zu ermöglichen, die den erforderlichen Service Levels entspricht. Der Wissenstransfer soll die Entwicklung eines Trainingsplans für erstmalige und laufende Schulung und die Entwicklung der Fertigkeiten, Schulungsmaterialien, Betriebshandbücher, Verfahrenshandbücher sowie Szenarien für den Service Desk umfassen.

MANAGEMENT GUIDELINES

AI4 Enable Operation and Use (*Ermögliche Betrieb und Verwendung)*

Von	Inputs
PO10	Projektmanagementanleitungen; Detaillierte Projektpläne
AI1	Machbarkeitsstudie bezüglich Unternehmenserfordernisse
AI2	Wissen über Anwendungen und Standardsoftware
AI3	Knowledge über Infrastruktur
AI7	Known Errors
DS7	Erforderliche Updates der Dokumentationen

Outputs	Nach						
Benutzer-, Betriebs-, Support-, technische und administrative Handbücher	AI7	DS4	DS8	DS9	DS11	DS13	
Erforderlicher Knowledge-Transfer für die Umsetzung von Lösungen	DS7						
Schulungsmaterialien	DS7						

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	C'IO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security	Entwicklungsteam	Schulungsabteilung
Entwickle eine Strategie, um Lösung in den Betrieb zu übernehmen				A	A	R		R			I	R	C
Entwickle eine Wissenstransfer-Methodik				C	A							C	R
Entwickle Verfahrenshandbücher für Endbenutzer					A/R			R			C	C	
Entwickle technische Supportdokumentation für Betriebs- und Supportpersonal						A/R		C			C		
Entwickle und halte Schulungen					A	A		R					R
Evaluiere die Resultate von Schulungen und verbessere die Dokumentation, wie erforderlich					A	A						R	R

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Entwicklung und Bereitstellung von verfügbaren Dokumenten zum Wissenstransfer
- Kommunikation mit und Schulung von Benutzern, Businessmanagement, Support- und Betriebspersonal
- Erstellung von Schulungsunterlagen

treiben

Prozessziele

- Stelle effektive Anwender und Betriebshandbücher sowie Schulungsunterlagen für Anwendungen und technische Lösungen Benutzern zur Verfügung
- Leite für den erfolgreichen Systembetrieb notwendiges Wissen weiter

treiben

IT-Ziele

- Stelle die angemessene Verwendung und Performance der Anwendungen und technischen Lösungen sicher
- Stelle die Enduser-Zufriedenheit mit den Serviceangeboten und Service Levels sicher
- Integriere die Anwendungen und Technologielösungen nahtlos in Geschäftsprozesse
- Reduziere Mängel und Nacharbeit bei Lösungen und dem Servicebetrieb

werden gemessen durch

Key Performance Indicators

- Stand der Schulungsteilnahme der Anwender und Betreiber für jede Anwendung
- Zeitspanne zwischen Änderungen und Updates des Schulungs-, Verfahrens- und Dokumentationsunterlagen
- Verfügbarkeit, Vollständigkeit und Korrektheit der Anwender- und Betriebsdokumentation
- Anzahl der Applikationen mit angemessenen Anwenderschulungen und Schulungen des operativen Supports

werden gemessen durch

Key Goal Indicators

- Anzahl der Zwischenfälle, die aufgrund mangelhafter Benutzer- und Betriebshandbücher sowie -schulungen verursacht worden sind
- Anzahl der vom Service Desk behandelten Schulungsanfragen
- Zufriedenheitsgrade für Schulungen und Dokumentation über Benutzer- und Betriebsverfahren
- Verringerte Kosten für die Erstellung/Wartung der Benutzer-dokumentation, Betriebsverfahren und Schulungsunterlagen

werden gemessen durch

IT Key Goal Indicators

- Anzahl der Applikationen, deren IT-Verfahren nahtlos in Geschäftsprozesse integriert sind
- % von mit den Anwenderschulungen und den Schulungsunterlagen zufriedenen Geschäftsprozesseigentümer

MATURITY MODEL

AI4 Enable Operation and Use (*Ermögliche Betrieb und Verwendung)*

Die Reife des Management des Prozesses *Enable Operation and Use (Ermögliche Betrieb und Verwendung)*, der die Geschäftsanforderungen an die IT erfüllt, die Zufriedenheit der Enduser mit Serviceangeboten und -levels und die nahtlose Integration der Anwendungen und Techniklösungen in Geschäftsprozesse sicherzustellen, ist

0 Non-existent (nicht existent):
Ein Prozess für die Erstellung von Anwendungsdokumentationen, Betriebshandbüchern und Schulungsunterlagen existiert nicht. Die einzig vorhandenen Unterlagen sind die zu gekauften Produkten gelieferten.

1 Initial (initial):
Das Bewusstsein für die Notwendigkeit von Prozessdokumentationen ist vorhanden. Die Dokumentationen werden ab und zu erstellt und inkonsequent an wenige Gruppen verteilt. Ein grosser Teil der Dokumentationen und viele Verfahren sind veraltet. Schulungsunterlagen sind in der Regel einmalige Entwürfe von unterschiedlicher Qualität. Eine Integration von Verfahren über verschiedene Systeme und Organisationseinheiten hinweg findet nahezu nicht statt. Von den Organisationseinheiten kommt kein Input für die Gestaltung von Schulungsprogrammen.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Ähnliche Ansätze werden zur Erstellung von Verfahren und Dokumentationen verwendet, aber sie basieren auf keinem strukturierten Ansatz oder Framework. Ein einheitlicher Ansatz zur Entwicklung von Anwender- und Betriebsverfahren ist nicht vorhanden. Die Schulungsunterlagen werden von Einzelnen oder Projektteams erstellt und die Qualität hängt von den involvierten Einzelpersonen ab. Die Verfahren und Qualität der Anwenderunterstützung variiert von schlecht bis sehr gut und die unternehmensweite Einheitlichkeit und Integration ist sehr gering. Schulungsprogramme für den Betrieb und die Anwender werden bereitgestellt oder gefördert, aber ein allgemeiner Plan für die Einführung und Verbreitung von Schulungen existiert nicht.

3 Defined (definiert):
Ein klar definiertes, akzeptiertes und verstandenes Framework zu Anwendungsdokumentationen, Betriebshandbüchern und Schulungsunterlagen ist vorhanden. Die Verfahren werden in einer formellen Bibliothek gespeichert und gepflegt und können von jedem eingesehen werden, der ein berechtigtes Interesse hat. Berichtigungen der Dokumentationen und Verfahren erfolgen reaktiv. Die Verfahren sind offline verfügbar und können im Katastrophenfall eingesehen und gepflegt werden. Ein Prozess ist festgelegt, in dem Verfahrensaktualisierungen und Schulungsmaterialien ein ausdrücklicher Bestandteil des Änderungsprojektes sind. Trotz der Existenz definierter Ansätze, variiert der eigentliche Inhalt, da keine Kontrolle vorhanden ist, welche die Erfüllung von Standards gewährleistet. Die Anwender sind informell in das Verfahren involviert. Automatisierte Werkzeuge werden verstärkt bei der Erstellung und Verbreitung von Verfahren angewendet. Betriebs- und Anwenderschulungen werden vorgesehen und geplant.

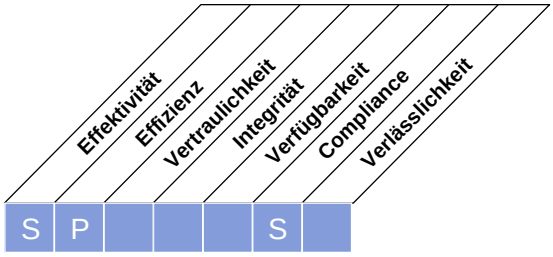
4 Managed and measurable (gemanaged und messbar):
Ein definiertes Framework zur Pflege von Verfahren und Schulungsunterlagen, das vom IT-Management unterstützt wird, ist vorhanden. Der getroffene Ansatz für die Pflege von Verfahrens- und Schulungshandbüchern deckt alle Systeme und alle Organisationseinheiten ab, so dass Prozesse aus Unternehmenssicht betrachtet werden können. Verfahren und die Schulungsunterlagen sind integriert und enthalten auch Abhängigkeiten und Schnittstellen. Controls existieren, die sicherstellen, dass Standards eingehalten werden und Verfahren für alle Prozesse erstellt und gepflegt werden. Die Betriebs- und Anwenderreaktionen auf die Dokumentationen und Schulungen werden gesammelt und im Zuge eines kontinuierlichen Verbesserungsprozesses bewertet. Dokumentationen und Schulungsmaterial sind in der Regel auf einem vorhersagbaren, guten Niveau von Verlässlichkeit und Verfügbarkeit. Erste Prozesse zur Anwendung von automatisierten Verfahrensdokumentation und -verwaltung sind eingeführt. Die automatisierte Entwicklung von Verfahren ist zunehmend in die Anwendungssystementwicklung integriert, so dass die Konsistenz und der Anwenderzugriff erleichtert wird. Betriebs- und Anwenderschulungen sind auf die Anforderungen des Geschäfts ausgerichtet. Das IT-Management erstellt Metriken für die Entwicklung und Verbreitung von Dokumentationen, Schulungsunterlagen und Schulungsprogrammen.

5 Optimised (optimiert):
Der Prozess für Anwendungs- und Betriebsdokumentationen wird kontinuierlich durch Anpassung von neuen Werkzeugen und Methoden verbessert. Die Verfahrens- und Schulungsunterlagen werden als kontinuierlich wachsende Wissensdatenbank gesehen, die elektronisch und durch aktuelle Werkzeuge für Wissensmanagement, Workflow- und Verteilung gepflegt wird, so dass die Informationen zugreifbar und einfach wartbar sind. Die Dokumentationen und Schulungsunterlagen werden aktualisiert, um Unternehmens-, Betriebs- und Softwareänderungen wiederzuspiegeln. Die Entwicklung von Dokumentationen und Schulungsunterlagen und die Verteilung der Schulungsprogramme sind komplett in die Geschäftstätigkeit und in die Geschäftsprozessdefinitionen integriert, so dass unternehmensweite Anforderungen anstatt nur die IT-orientierten Verfahren unterstützt werden.

HIGH-LEVEL CONTROL OBJECTIVE

AI5 Procure IT Resources *(Beschaffe IT-Ressourcen)*

IT-Ressourcen (Personal, Hardware, Software und Dienstleistungen) müssen beschafft werden. Dies erfordert, dass Beschaffungsverfahren für die Auswahl von Anbietern, die Erstellung von vertraglichen Vereinbarungen und die eigentliche Beschaffung festgelegt und durchgesetzt werden. Dadurch wird sicher gestellt, dass der Organisation sämtliche erforderlichen IT-Ressourcen zeitnah und in kostenwirksamer Weise zur Verfügung stehen.



Kontrolle über den IT-Prozess,

Procure IT resources (*Beschaffe IT Ressourcen*)

der die Anforderung des Unternehmens an die IT bezüglich

die Verbesserung der Kosteneffizienz der IT und ihres Beitrags zum Unternehmenserfolg

durch die Konzentration auf

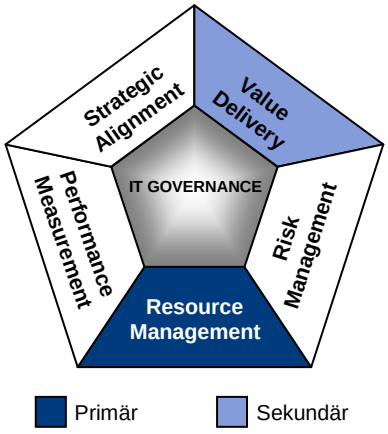
die Beschaffung und Erhaltung von IT-Fertigkeiten, die auf die Unterstützungsstrategie, eine integrierte und standardisierte IT-Infrastruktur und die Reduktion des IT-Beschaffungsrisikos abgestimmt sind , *zufrieden stellt,*

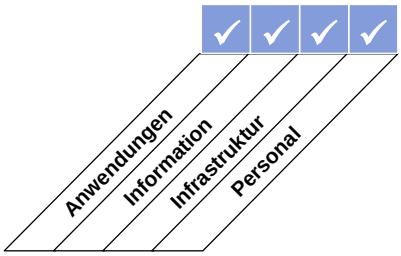
wird erreicht durch

- Bezug professioneller rechtlicher und vertraglicher Beratung
- Festlegung von Beschaffungsverfahren und -standards
- Beschaffung angeforderter Hardware, Software und Services entsprechend der definierten Verfahren

und gemessen durch

- Anzahl der Streitfälle im Zusammenhang mit Beschaffungsverträgen
- Reduzierte Beschaffungskosten
- Prozent der mit den Lieferanten zufriedenen wesentlichen Stakeholder





DETAILLIERTE CONTROL OBJECTIVES

AI5 Procure IT Resources *(Beschaffe IT-Ressourcen)*

AI5.1 Procurement Control (Steuerung der Beschaffung)
Entwickle und befolge Verfahren und Standards, die mit dem unternehmensweit gültigen Einkaufsprozess und der Beschaffungsstrategie übereinstimmen, um sicher zu stellen, dass die Beschaffung von IT-bezogener Infrastruktur, Einrichtungen, Hardware, Software und Dienstleistungen die Unternehmenserfordernisse erfüllt.

AI5.2 Supplier Contract Management (Vertragsmanagement für Lieferanten)
Erstelle ein Verfahren für die Festlegung, Änderung und Beendigung von Verträgen für alle Lieferanten. Das Verfahren sollte im Minimum rechtliche, finanzielle, organisatorische, dokumentarische, Performance-, Sicherheits-, Urheberrechts- und Kündigungsverantwortlichkeiten und Haftung (inklusive Konventionalstrafen) abdecken. Alle Verträge und Vertragsänderungen sollten durch Rechtsberater überprüft werden.

AI5.3 Supplier Selection (Lieferantenauswahl)
Wähle Lieferanten entsprechend einer fairen und formalen Praktik aus, um eine optimale Eignung sicher zu stellen gemäss der Anforderungen, welche auf Basis von Inputs potentieller Lieferanten entwickelt und mit Kunden und Lieferanten vereinbart wurden.

AI5.4 Software Acquisition (Softwarebeschaffung)
Stelle sicher, dass die Interessen der Organisation bei allen vertraglichen Beschaffungsvereinbarungen geschützt sind. Berücksichtige in den Vertragsbedingungen für die Beschaffung der Software die Rechte und Pflichten aller Parteien, die in der Lieferung und der laufenden Verwendung der Software involviert sind und setze diese durch. Diese Rechte und Pflichten können Eigentum und Lizenzierung von geistigem Eigentum, Wartung, Gewährleistung, Schiedsgerichtsverfahren, Bedingungen für Upgrades und die Tauglichkeit zum Gebrauch, wie Sicherheit, Hinterlegung und Recht auf Zugriffe umfassen.

AI5.5 Acquisition of Development Resources (Beschaffung von Entwicklungsressourcen)
Stelle sicher, dass die Interessen der Organisation bei allen vertraglichen Beschaffungsvereinbarungen geschützt sind. Berücksichtige in den Vertragsbedingungen für die Beschaffung von Entwicklungsressourcen die Rechte und Pflichten aller Parteien, die in der Beschaffung von Entwicklungsressourcen involviert sind, und setze diese durch. Diese Rechte und Pflichten können Eigentum und Lizenzierung von geistigem Eigentum, Tauglichkeit zum Gebrauch, wie Entwicklungsmethoden, Sprachen, Test und Qualitätsmanagement-Prozesse inklusive erforderliche Performance-Kriterien, Performance-Review, Zahlungsvereinbarungen, Gewährleistung, Schiedsgerichtsverfahren, Human-Ressource-Management und Einhaltung der Richtlinien der Organisation umfassen.

AI5.6 Acquisition of Infrastructure, Facilities and Related Services (Beschaffung von Infrastruktur, Einrichtungen und entsprechenden Diensten)
Berücksichtige in den Vertragsbedingungen für Beschaffung von Infrastruktur, Einrichtungen und entsprechenden Diensten – einschließlich der Abnahmekriterien – die Rechte und Pflichten aller Parteien und setze diese durch. Diese Rechte und Pflichten können Service Levels, Wartungsverfahren, Zugriffsschutz, Sicherheit, Performance-Review, Zahlungsvereinbarungen und Schiedsgerichtsverfahren umfassen.

MANAGEMENT GUIDELINES

AI5 Procure IT Resources *(Beschaffe IT-Ressourcen)*

Von	Inputs
PO1	IT-Beschaffungsstrategie
PO8	Beschaffungsstandards
PO10	Projektmanagementanleitungen; Detaillierte Projektpläne
AI1	Machbarkeitsstudie bezüglich Unternehmenserfordernissen
AI2-3	Beschaffungsentscheidungen
DS2	Katalog der Lieferanten

Outputs	Nach
Anforderungen für Beziehungsmanagement mit externen Partnern	DS2
Beschaffte Objekte	AI7
Vertragliche Vereinbarungen	DS2

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Entwickle IT-Beschaffungsrichtlinien und -verfahren, die mit Beschaffungsrichtlinien auf der Unternehmensebene übereinstimmen	I	C		A		I	I	I	R		C
Erstelle/unterhalte eine Liste akkreditierter Lieferanten									A/R		
Evaluiere und wähle Lieferanten durch einen Request for Proposal (RFP) Prozess	C	C		A		R		R	R	R	C
Entwickle Verträge, die die Interessen des Unternehmens schützen	R	C		A		R		R	R		C
Beschaffe gemäß der entwickelten Verfahren				A		R		R	R		C

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- ezug professioneller rechtlicher und vertraglicher Beratung
- Festlegung von Beschaffungsverfahren und -standards
- Beschaffung angeforderter Hardware, Software und Services entsprechend der definierten Verfahren

treiben

Prozessziele

- Reduziere IT-Beschaffungsrisiken.
- Erhalte den Wert für das Geld von IT-Beschaffungen

treiben

IT-Ziele

- Beschaffe und warte integrierte und standardisierte Anwendungssysteme und IT-Infrastruktur
- Beschaffe und erhalte IT-Skills, die der IT-Strategie entsprechen
- Verbessere die Kosteneffizienz der IT und ihren Beitrag zum Unternehmenserfolg

werden gemessen durch

Key Performance Indicators

- Zeitspanne zwischen einer Anfrage für die Beschaffung und der Unterzeichnung des Vertrages oder der Beschaffung
- Anzahl der Beschaffungsanfragen, welche durch die Liste bevorzugter Lieferanten erfüllt werden
- Anzahl der RFPs, die aufgrund der Lieferantenreaktionen zu verbessern waren
- Anzahl der zeitgerecht abgeschlossenen Beschaffungsanfragen
- Anzahl der Lieferantenänderungen für die gleiche Art der beschafften Güter oder Services
- Anzahl der auf RFP erhaltenen Antworten

werden gemessen durch

Key Goal Indicators

- % der ursprünglichen Anforderungen, die durch die ausgewählte Lösung erfüllt werden
- % von Beschaffungen gemäß den fest-stehenden Beschaffungsrichtlinien und –verfahren
- Reduzierte Stückkosten der beschafften Güter oder Services

werden gemessen durch

IT Key Goal Indicators

- Anzahl der Streitfälle im Zusammenhang mit Beschaffungsverträgen
- Reduzierte Beschaffungskosten
- % der wesentlichen Stakeholder, die mit den Lieferanten zufrieden sind

MATURITY MODEL

AI5 Procure IT Resources *(Beschaffe IT-Ressourcen)*

Die Reife des Management des Prozesses *Procure IT Resources (Beschaffe IT-Ressourcen)*, der die Geschäftsanforderungen an die IT erfüllt, die Kosteneffizienz der IT und ihren Beitrag zum Unternehmenserfolg zu verbessern, ist:

0 Non-existent (nicht existent):
Ein definierter Prozess zur Beschaffung von IT-Ressourcen existiert nicht. Das Unternehmen erkennt den Bedarf klarer Beschaffungsrichtlinien und -verfahren nicht, damit alle IT-Ressourcen rechtzeitig und kosteneffizient verfügbar sind.

1 Initial (initial):
Das Unternehmen hat die Notwendigkeit dokumentierter Richtlinien und Verfahren erkannt, welche die IT-Beschaffung mit dem unternehmensweiten Beschaffungsprozess verbinden. Verträge für die Beschaffung von IT-Ressourcen werden durch die Projektmanager und andere Einzelpersonen entwickelt und verwaltet, welche ihr sachkundiges Urteil einsetzen, anstatt als Ergebnis formeller Verfahren und Richtlinien. Zwischen den unternehmensweiten Beschaffungs- und Vertragsmanagement-Prozessen und der IT bestehen nur ad hoc-Beziehungen. Beschaffungsverträge werden eher im Rahmen von Projektabschlüssen und weniger auf einer kontinuierlichen Basis verwaltet.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Es besteht im Unternehmen ein Bewusstsein für die Notwendigkeit grundlegender Richtlinien und Verfahren für die Beschaffung von IT-Ressourcen. Die Richtlinien und Verfahren sind teilweise in den unternehmensweiten Beschaffungsprozess integriert. Die Beschaffungsprozesse werden meist für große und sichtbare Projekte verwendet. Aufgaben und Verantwortlichkeiten für das Beschaffungs- und Vertragsmanagement der IT werden durch die individuelle Erfahrung des Vertragsmanagers bestimmt. Die Wichtigkeit von Lieferanten- und Beziehungsmanagement wird zwar erkannt, aber nur aufgrund der Initiative Einzelner angewendet. Vertragsprozesse werden meist für große und sichtbare Projekte verwendet.

3 Defined (definiert):
Das Management hat Richtlinien und Verfahren für die IT-Beschaffung eingeführt. Die Richtlinien und Verfahren werden durch den unternehmensweiten Beschaffungsprozess angeleitet. Die IT-Beschaffung ist größtenteils in die gesamtbetrieblichen Beschaffungssysteme integriert. IT-Standards für die Beschaffung von IT-Ressourcen sind vorhanden. Anbieter von IT-Ressourcen sind aus Sicht des Vertragsmanagements in die Mechanismen des betrieblichen Projektmanagements integriert. Das IT-Management kommuniziert die Notwendigkeit eines geeigneten Beschaffungs- und Vertragsmanagements über die gesamte Informatik.

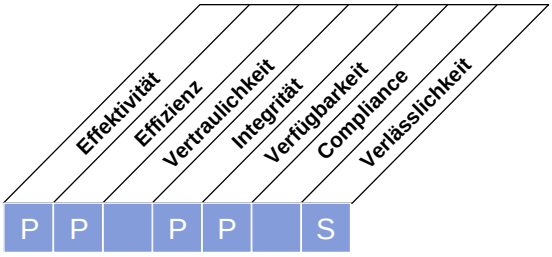
4 Managed and measurable (gemanaged und messbar):
Die Beschaffung von IT-Ressourcen ist vollständig in die unternehmensweiten Beschaffungssysteme integriert. Die IT-Standards für die Beschaffung von IT-Ressourcen werden auf alle Beschaffungen angewendet. Metriken zum Vertrags- und Beschaffungsmanagement werden entsprechend der Business Cases der Beschaffung von IT-Ressourcen eingesetzt. Ein Berichtswesen, das die Geschäftsziele unterstützt, ist verfügbar. Das Management hat üblicherweise Kenntnis von Ausnahmen bei den Richtlinien und Verfahren zur Beschaffung von IT-Ressourcen. Ein strategisches Beziehungsmanagement wird entwickelt. Das IT-Management setzt die Anwendung des Beschaffungs- und Vertragsmanagement-Prozesses für sämtliche Beschaffung mittels Performancemessungen durch.

5 Optimised (optimiert):
Das Management hat wirksame Prozesse für die Beschaffung von IT-Ressourcen institutionalisiert und personell ausgestattet. Das Management setzt die Einhaltung der Richtlinien und Verfahren für die Beschaffung von IT-Ressourcen durch. Metriken zum Vertrags- und Beschaffungsmanagement werden entsprechend der Business Cases der Beschaffung von IT-Ressourcen eingesetzt. Zwischen den Anbietern und Partnern entwickeln sich mit der Zeit gute Beziehungen und die Qualität der Beziehungen wird gemessen und überwacht. Die Beziehungen werden strategisch verwaltet. Die IT-Standards, Richtlinien und Verfahren für die Beschaffung von IT-Ressourcen werden strategisch verwaltet und reagieren auf die Messungen des Prozesses. Das IT-Management kommuniziert die strategische Bedeutung eines geeigneten Beschaffungs- und Vertragsmanagements über die gesamte Informatik.

HIGH-LEVEL CONTROL OBJECTIVE

AI6 Manage Changes *(Manage Changes)*

Alle Changes an der Infrastruktur und den Anwendungen in der produktiven Umgebung, inklusive Notfalls-Changes und Patches, müssen formell auf eine gesteuerte Art und Weise vorgenommen werden. Jeder Change (inklusive an Verfahren, Prozesse, Systemen und Service-Parametern) müssen vor der Implementierung aufgezeichnet, bewertet und autorisiert sowie nach der Implementierung an Hand der geplanten Ergebnisse überprüft werden. Dies stellt die Verminderung von Risiken sicher, die sich negativ auf die Stabilität und Integrität der Produktivumgebung auswirken.



Kontrolle über den IT-Prozess,

Manage Changes (*Manage Changes*)

der die Anforderung des Unternehmens an die IT bezüglich

der Reaktion auf Geschäftsanforderungen in Übereinstimmung mit der Unternehmensstrategie, während der Reduktion der Mängel und Nacharbeit bei Lösungen und dem Servicebetrieb

durch die Konzentration auf

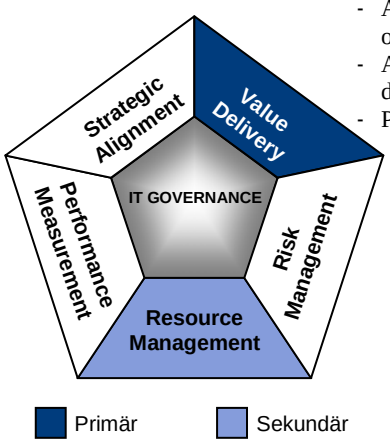
eine geregelte Einschätzung von Auswirkungen, der Autorisierung und der Implementierung aller Änderungen auf die IT-Infrastruktur, Anwendungen und technischen Lösungen, die Minimierung der Fehler aufgrund unvollständiger Anfragespezifikationen und Abbruch der unautorisierten , *zufrieden stellt,*

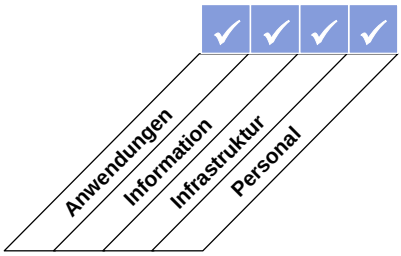
wird erreicht durch

- Festlegung und Kommunikation der Verfahren für Änderungen inklusive Notfallsänderungen
- Beurteilung, Priorisierung und Autorisierung der Änderungen
- Verfolgung des Status der und das Berichten über Änderungen

und gemessen durch

- Anzahl der Unterbrechungen oder Datenfehler, die durch ungenaue Spezifikation oder unvollständige Beurteilung der Auswirkungen hervorgerufen sind
- Applikations- oder Infrastruktur-Nacharbeit, die durch mangelhafte Spezifikation der Änderungenhervorgerufen ist
- Prozent der Änderungen, die formale Prozesse zur Steuerung von Changes befolgen





DETAILLIERTE CONTROL OBJECTIVES

AI6 Manage Changes *(Manage Changes)*

AI6.1 Change Standards and Procedures (Standards und Verfahren für Changes)
Erstelle formelle Change-Management-Verfahren, um in geregelter Weise alle Anfragen (inklusive Wartung und Patches) für Changes an Anwendungen, Verfahren, Prozessen, System- oder Serviceparametern sowie an Basisplattformen zu behandeln.

AI6.2 Impact Assessment, Prioritisation and Authorisation (Bewertung von Auswirkungen, Priorisierung und Freigabe)
Stelle sicher, dass alle Anfragen für Changes in einer strukturierten Art und Weise auf deren Auswirkungen auf die operativen Systeme und deren Funktionalität hin beurteilt werden. Diese Beurteilung sollte eine Kategorisierung und Priorisierung der Changes umfassen. Vor der Migration in die Produktion werden Changes durch die jeweiligen Stakeholder genehmigt.

AI6.3 Emergency Changes (Notfalls-Changes)
Erstelle eine Prozess für die Definition, Aufnahme, Beurteilung und Genehmigung von Notfalls-Changes, die nicht dem bestehenden Change-Prozess folgen. Dokumentation und Tests sollten durchgeführt werden, auch nach der Implementierung des Notfalls-Changes.

AI6.4 Change Status Tracking and Reporting (Statusverfolgung und Berichterstattung)
Erstelle ein Nachverfolgungs- und Reportingsystem, um Anfordernde und die entsprechenden Stakeholder über den Status der Änderung an Anwendungen, Verfahren, Prozessen, System- oder Serviceparametern sowie an den Basisplattformen informiert zu halten.

AI6.5 Change Closure and Documentation (Abschluss und Dokumentation von Changes)
Sobald System-Changes umgesetzt sind, aktualisiere die betreffende System- und Benutzerdokumentation sowie die Verfahren entsprechend. Erstelle einen Review-Prozess, um die vollständige Umsetzung der Changes sicher zu stellen.

MANAGEMENT GUIDELINES

AI6 Manage Changes *(Manage Changes)*

Von	Inputs
PO1	IT-Projektportfolio
PO8	Aktivitäten zur Qualitätsverbesserung
PO9	IT-bezogene Risikominderungs-Pläne
PO10	Projektmanagementvorgaben und detaillierte Projektpläne
DS3	Erforderliche Änderungen
DS5	Erforderliche Security-Änderungen
DS8	Service-Requests/Request for Change
DS9-10	Request for Change (wo und wie den Fix anwenden)
DS10	Problem-Aufzeichnungen

Outputs	Nach						
Beschreibung Change-Prozess	AI1	AI2	AI3				
Statusreports von Changes	ME1						
Freigabe von Änderungen	AI7	DS10	DS8				

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Entwickle und implementiere einen Prozess für konsistente Aufzeichnung, Bewertung und Priorisierung der Change-Requests				A	I	R	C	R	C	C	C
Bewerte die Auswirkungen und priorisiere Changes, die auf geschäftlichen Bedürfnissen basieren				I	R	A/R	C	R	C	R	C
Stelle sicher, dass jeder Notfall und jede kritische Änderung den Genehmigungsprozess durchläuft				I	I	A/R		R			C
Autorisiere Changes				I	C	A/R	I	R			
Manage und leite die für Änderungen relevante Information weiter				A	I	R		R	I	R	C

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Festlegung und Kommunikation der Verfahren für Changes inklusive Notfalländerungen und -patches
- Beurteilung, Priorisierung und Genehmigung der Changes
- Planung von Änderungen
- Status-Verfolgung und Berichterstattung über Changes

treiben

Prozessziele

- Führe genehmigte Änderungen an der IT-Infrastruktur und Anwendungen durch
- Bewerte die Auswirkungen der Changes auf die IT-Infrastruktur, Anwendungen und technischen Lösungen
- Verfolge und berichte den Change-Status den wichtigsten Stakeholder
- Minimiere Fehler, die durch unvollständige Anfrage-Spezifikation hervorgerufen sind.

treiben

IT-Ziele

- Reagiere auf Geschäftsanforderungen in Übereinstimmung mit der Unternehmensstrategie
- Reduziere Mängel und Nacharbeit bei Lösungen und dem Servicebetrieb
- Stelle sicher, dass der Einfluss einer IT-Service-Störung oder -Änderung auf das Geschäft minimiert ist
- Definiere, wie funktionale geschäftliche und Steuerungsanforderungen in wirksame und wirtschaftliche automatisierte Lösungen überführt werden.
- Erhalte die Integrität der Informationen und die diese Informationen verarbeitende Infrastruktur

werden gemessen durch

Key Performance Indicators

- % der aufgezeichneten und mit automatisierten Tools verfolgten Änderungen
- % der Änderungen, die formale Änderungskontrollprozesse befolgen
- Verhältnis der akzeptierten zu abgelehnten Änderungsanfragen
- Anzahl der unterschiedlichen Versionen jeder Geschäftsanwendungen oder Infrastruktur, die gewartet werden
- Anzahl und Art der Notfalländerungen an Infrastrukturkomponenten
- Anzahl und Art der Patches an den Infrastrukturkomponenten

werden gemessen durch

Key Goal Indicators

- Nacharbeit an Anwendungen, die durch mangelhafte Spezifikation der Änderungen hervorgerufen ist
- Reduzierte Zeit und reduzierter Aufwand, um Änderungen durchführen zu können
- % der gesamten Änderungen, die Notfallsfixes sind
- % der nicht erfolgreichen Änderungen der Infrastruktur, die durch ungeeignete Änderungsspezifikationen hervorgerufen sind
- Anzahl der Änderungen, die nicht formal verfolgt oder berichtet oder nicht genehmigt sind

werden gemessen durch

IT Key Goal Indicators

- Anzahl der Unterbrechungen oder Datenfehler, die durch ungenaue Spezifikation oder unvollständige Beurteilung der Auswirkungen hervorgerufen ist

MATURITY MODEL

AI6 Manage Changes *(Manage Changes)*

Die Reife des Management des Prozesses *Manage Changes (Manage Changes)*, der die Geschäftsanforderungen an die IT erfüllt, auf Geschäfsanforderungen in Übereinstimmung mit der Unternehmensstrategie und unter Reduktion der Mängel und Nacharbeit bei Lösungen und dem Servicebetrieb reagieren zu können, ist:

0 Non-existent (nicht existent):
Ein definierter Prozess für Change-Management existiert nicht und Changes können nahezu ohne jede Kontrolle durchgeführt werden. Es besteht kein Bewusstsein, dass Changes für den IT- und Geschäftsbetrieb unterbrechend sein könen, und kein Bewusststein für die Vorzüge eines guten Change-Managements.

1 Initial (initial):
Es ist erkannt, dass Changes verwaltet und gesteuert werden sollten. Die Praktiken variieren und es ist wahrscheinlich, dass nicht genehmigte Changes durchgeführt werden. Dokumentationen zu Changes sind schlecht oder existieren nicht und die Dokumentation zu Konfigurationen ist unvollständig und unzuverlässig. Fehler treten voraussichtlich im Zusammenhang mit Störungen der Produktionsumgebung auf, die durch ein schlechtes Change-Management ausgelöst werden.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Ein informeller Change-Management-Prozess ist vorhanden und bei den meisten Changes wird dieser Ansatz verfolgt; auch wenn er nicht strukturiert, rudimentär und fehleranfällig ist. Die Dokumentationsgenauigkeit von Konfigurationen ist inkonsistent und nur begrenzte Planung und Auswirkungseinschätzungen findet statt vor Changes.

3 Defined (definiert):
Ein definierter formeller Change-Management-Prozess mit steigender Einhaltung ist vorhanden, inklusive Kategorisierung, Priorisierung, Notfallverfahren, Change-Autorisierung und Release-Management. Provisorische Lösungen werden entwickelt und Prozesse werden oft umgangen. Fehler treten weiterhin auf und unautorisierte Changes werden ab und zu durchgeführt. Die Analyse der Auswirkungen von IT- Changes auf betriebliche Abläufe wird so langsam formalisiert, um geplante Einführungen von neuen Anwendungen und Technologien zu unterstützen.

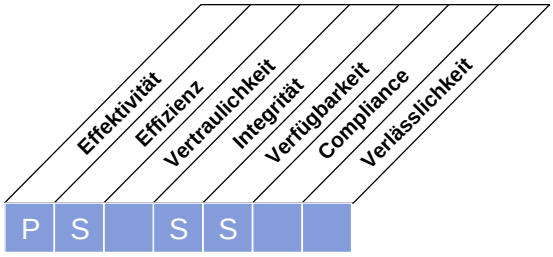
4 Managed and measurable (gemanaged und messbar):
Der Change-Management-Prozess ist gut entwickelt und wird für alle Changes konsistent befolgt, und das Management ist überzeugt, dass es wenige Ausnahmen gibt. Der Prozess ist wirtschaftlich und wirksam, ist aber auf erhebliche manuelle Maßnahmen und Kontrollen angewiesen, um die Qualität zu gewährleisten. Alle Changes unterliegen sorgfältiger Planungen und Auswirkungseinschätzungen, um die Wahrscheinlichkeit von Problemen bei der Nachbearbeitung zu minimieren. Ein Genehmigungsverfahren für Changes ist vorhanden. Die Dokumentation zum Change-Management ist aktuell und korrekt, und die Changes werden formell nachverfolgt. Die Dokumentation von Konfigurationen ist im Allgemeinen fehlerfrei. Die Planung und Implementierung des IT-Change-Managements werden immer mehr in Änderungen von Geschäftsprozessen integriert, um sicherzustellen, dass die Bereiche Schulung, organisatorische Änderungen und Geschäftskontinuitätsfragen berücksichtigt werden. Es besteht eine verstärkte Koordination zwischen dem IT-Change-Management-Prozess und dem Business-Process-Redesign. Ein konsistenter Prozess für die Überwachung der Qualität und Leistung des Change-Management-Prozesses existiert.

5 Optimised (optimiert):
Der Change-Management-Prozess wird einem regelmäßigen Review unterzogen und aktualisiert, um mit den Good Practices in Einklang zu bleiben. Der Reviewprozess spiegelt das Ergebnis der Überwachung wider. Die Informationen zur Konfigurationen liegen elektronisch vor und unterstützen die Versionskontrolle. Die Verfolgung von Changes ist fortschrittlich und beinhaltet Werkzeuge, um unautorisierte und unlizenzierte Software zu erkennen. Das IT- Change-Management ist in das Geschäftsänderungsmanagement integriert, um sicherzustellen, dass die IT eine erhöhte Produktivität fördert und neue Geschäfsmöglichkeiten für das Unternehmen erzeugt.

HIGH-LEVEL CONTROL OBJECTIVE

AI7 Install and Accredit Solutions and Changes *(Installiere und akkreditiere Lösungen und Changes)*

Nachdem die Entwicklung abgeschlossen ist, müssen neue Systemein Betrieb genommen werden. Dies erfordert sorgfältige Tests mit relevanten Testdaten in einer dedizierten Umgebung, Festlegung von Rollout- und Migrationsanweisungen, eine Release-Planung, die eigentliche Inbetriebnahme sowie ein Post-Implementation Review. Dies stellt sicher, dass operativ eingesetzte Systeme den vereinbarten Erwartungen und Ergebnissen entsprechen.



Kontrolle über den IT-Prozess,

Install and Accredit Solutions and Changes (*Installiere und akkreditiere Lösungen und Änderungen*)

der die Anforderung des Unternehmens an die IT bezüglich

der neuen oder geänderten Systeme, die nach der Installation ohne bedeutende Probleme arbeiten

durch die Konzentration auf

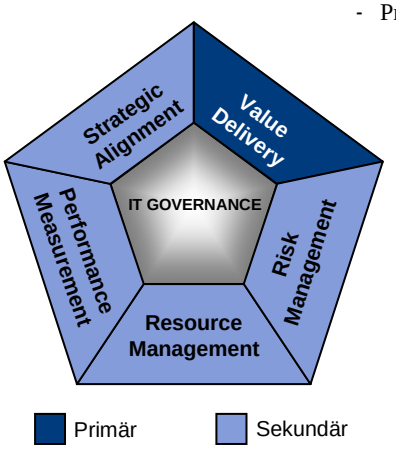
das Testen, damit Anwendungen und Infrastrukturlösungen dem vorgesehenen Zweck entsprechen und frei von Fehlern sind, und die Planung der Inbetriebnahme, *zufrieden stellt,*

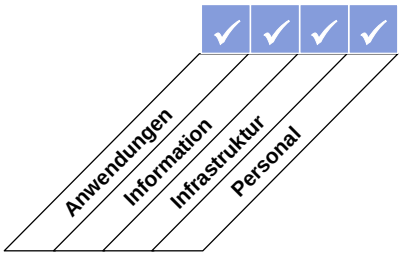
wird erreicht durch

- Etablierung der Testmethoden
- Durchführung der Releaseplanung
- Evaluierung und Genehmigung der Testergebnisse durch das Businessmanagement
- Durchführung der Post-Implementation Reviews

und gemessen durch

- Ausfallszeit der Anwendung oder Korrekturen an den Daten, die durch ungeeignetes Testen hervorgerufen sind
- Prozent der Systeme die dem erwarteten Nutzen entsprechen, wie im Post-Implementation Review gemessen wurde
- Prozent der Projekte mit einem dokumentierten und genehmigten Testplan





DETAILLIERTE CONTROL OBJECTIVES

AI7 Install and Accredit Solutions and Changes *(Installiere und akkreditiere Lösungen und Changes)*

AI7.1 Training (Schulung)
Schule – als Teil jedes Entwicklungs-, Implementierungs- oder Änderungsprojektes – Mitarbeiter der betroffenen Abteilungen und das Betriebspersonal der IT in Einklang mit den festgelegten Schulungs- und Implementierungsplänen und den entsprechenden Unterlagen.

AI7.2 Test Plan (Testplan)
Erstelle einen Testplan und hole das Einverständnis der relevanten Parteien ein. Der Testplan basiert auf unternehmensweiten Standards und definiert Rollen, Verantwortlichkeiten und Erfolgskriterien. Der Plan berücksichtigt die Testvorbereitung (inklusive Vorbereitung notwendiger Räumlichkeiten), Schulungserfordernisse, Installation oder Update einer definierten Testumgebung, der Planung, Umsetzung, Dokumentation und Aufbewahrung von Testfällen, Fehlerbehandlung und -korrektur sowie formelle Abnahme. Basierend auf der Beurteilung des Risikos von Systemfehlern oder Störungen bei der Implementierung, sollte der Plan die Erfordernis für Leistungs-, Stress-, Usability-, Pilot- und Sicherheitstests umfassen.

AI7.3 Implementation Plan (Implementierungsplan)
Erstelle einen Implementierungsplan und hole das Einverständnis von den relevanten Parteien ein. Der Plan definiert das Release-Design, den Aufbau von Release-Paketen, Verfahren für Roll-out/Installation, Umgang mit Ereignissen, Steuerung der Verteilung (inklusive Werkzeuge), Speicherung von Software, Review des Release und die Dokumentation von Changes. Der Plan sollte auch Vorkehrungen für eine Rücksetzung (engl.: *fallback/backout*) enthalten.

AI7.4 Test Environment (Testumgebung)
Erstelle eine separate Testumgebung für Tests. Diese Umgebung sollte der künftigen Betriebsumgebung entsprechen (zB ähnliche Sicherheit, Internal Controls und Workloads), um sinnvolles Testen zu ermöglichen. Verfahren sollen vorhanden sein, um sicher zu stellen, dass die in der Testumgebung verwendeten Daten den später in der Produktivumgebung verwendeten Daten entsprechen und, wo nötig, anonymisiert sind. Ergreife angemessene Maßnahmen, um die Veröffentlichung sensitiver Testdaten zu verhindern. Das dokumentierte Testergebnis sollte aufbewahrt werden.

AI7.5 System and Data Conversion (System- und Datenkonvertierung)
Stelle sicher, dass die Entwicklungsmethoden der Organisation für alle Entwicklungs-, Implementierungs- oder Änderungsprojekte alle notwendigen Bestandteile, wie Hardware, Software, Transaktionsdaten, Stammdaten, Backups und Archive, Schnittstellen mit anderen Systemen, Verfahren, Systemdokumentation etc vom Altsystem in das Neusystem entsprechend eines vorher entwickelten Plans überführt werden. Eine Prüfspur von Ergebnissen vor und nach der Konvertierung sollte entwickelt und aufbewahrt werden. Eine detaillierte Verifikation der ersten Verarbeitung des neuen Systems sollte durch die Systemeigner durchgeführt werden, um die erfolgreiche Überführung zu bestätigen.

AI7.6 Testing of Changes (Test von Changes)
Stelle sicher, dass Changes entsprechend der definierten Abnahmepläne getestet werden, die auf einer Beurteilung von Auswirkungen und Ressourcenbedarf basieren. Diese Beurteilung berücksichtigt die Bestimmung der notwendigen Performance in einer separaten Testumgebung durch eine (von Entwicklern) unabhängige Testgruppe, bevor eine Verwendung in der Normalbetriebsumgebung erfolgt. Die Sicherheitsmaßnahmen sollten vor der Auslieferung getestet werden, so dass die Wirksamkeit der Sicherheit zertifiziert werden kann. Pläne für eine Rücksetzung (engl.: *fallback/backout plan*) sollten vor der Umsetzung des Change in die Produktion entwickelt und getestet werden.

AI7.7 Final Acceptance Test (Abschließender Akzeptanztest)
Stelle sicher, dass Verfahren, als Teil der Abnahme oder abschließenden Qualitätssicherung neuer oder modifizierter Informationssysteme, eine formale Evaluierung und Freigabe der Testergebnisse durch das Management der betroffenen User-Abteilung(en) und der IT vorsehen. Die Tests sollten alle Komponenten des Informationssystems (zB Anwendungssoftware, Einrichtungen, Technologie und User-Verfahren) umfassen und sicherstellen, dass die Anforderungen an die Informationssicherheit durch alle Komponenten eingehalten werden. Die Testdaten sollten als Prüfspur und für künftige Tests aufbewahrt werden.

AI7.8 Promotion to Production (Produktivstellung)
Erstelle formale und dem Umsetzungsplan entsprechende Verfahren zur Steuerung der Übergabe des Systems von der Entwicklung zum Test und dann in die Produktion. Das Management sollte verlangen, dass das Einverständnis des Systemeigners eingeholt wird, bevor eine neue Anwendung in die Produktion verschoben wird, und dass das neue System erfolgreich die Tages-, Monats-, Quartals- und Jahresendverarbeitung durchgeführt hat, bevor das Altsystem außer Betrieb genommen wird.

AI7.9 Software Release (Release von Software)
Stelle sicher, dass der Release von Software durch formelle Verfahren geregelt wird, die eine Freigabe, Erstellung von Paketen, Regressionstest, Verteilung, Übergabe, Statusverfolgung, Pläne für eine Rücksetzung und Benachrichtigung von Usern gewährleisten.

AI7.10 System Distribution (Systemverteilung)
Entwickle Steuerungsverfahren, um zeitgerechte und korrekte Verteilung und Updates von freigegebenen Configuration Items sicher zu stellen. Dies umfasst Integritätskontrollen, Funktionstrennung zwischen den Personen, die erstellen, testen und betreiben und angemessene Prüfspuren aller Aktivitäten.

AI7.11 Recording and Tracking of Changes (Aufzeichnung und Verfolgung von Changes)
Automatisiere das System, das für das Monitoring von Changes an Anwendungen eingesetzt werden, um die Aufzeichnung und Verfolgung von Changes an Anwendungen, Verfahren, Prozessen, Systemen und Service-Parametern und der Basisplattform zu unterstützen.

AI7.12 Post-implementation Review (Post-Implementation Review)
Entwickle, in Übereinstimmung mit dem unternehmensweiten Entwicklungs- und Change-Standards, Verfahren, die einen Post Implementation Review der operativen Systeme verlangen, um zu bewerten und zu berichten, ob der Change auf die kostenwirksamste Art die Kundenanforderungen erfüllt und den vorgesehenen Nutzen erbracht hat.

MANAGEMENT GUIDELINES

AI7 Install and Accredit Solutions and Changes *(Installiere und akkreditiere Lösungen und Changes)*

Von	Inputs
PO3	Technologiestandards
PO4	Dokumentierte Systemeigner
PO8	Entwicklungsstandards
PO10	Projektmanagementanleitungen; Detaillierte Projektpläne
AI3	Konfiguriertes System, fertig für Test / Installation
AI4	Benutzer-, Betriebs-, Support-, technische und administrative Handbücher
AI5	Beschaffte Objekte
AI6	Freigabe von Änderungen

Outputs	Nach						
Configuration Items (Released)	DS8	DS9					
Bekannte und akzeptierte Fehler	AI4						
Freigabe zum Produktiveinsatz	DS13						
Known Errors	AI4						
Software-Release und -Verteilungsplan	DS13						
Post-Implementation-Review	PO2	PO5	PO10				

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Erstelle und reviewe Implementierungspläne			C	A	I	C	C	R		C	C
Definiere und reviewe eine Teststrategie (Eingangs- und Ausgangskriterien) und eine Planungsmethode für die Testdurchführung			C	A	C	C	C	R		C	C
Erstelle und unterhalte ein Repository von unternehmens- und technisch orientierten Anforderungen und Testfällen für akkreditierte Systeme				A				R			
Führe Übernahme- und Integrationstests in der Testumgebung durch			I	I	R	C	C	A/R		I	C
Wende eine Testumgebung an und führe Abnahmetests durch			I	I	R	A	C	A/R		I	C
Empfehle die Produktivstellung basierend auf vereinbarten Abnahmekriterien			I	R	A	R	C	C		I	C

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Festlegung der Testmethodik, die ausreichende Akzeptanztests vor der Inbetriebnahme sicherstellt
- Verfolge Änderungen aller Configuration Items
- Durchführung der Releaseplanung
- Durchführung der Post-Implementation Reviews
- Evaluierung und Genehmigung der Testergebnisse durch das Businessmanagement

treiben

Prozessziele

- Verifiziere und bestätige, dass Anwendungen und technische Lösungen fit für den vorgesehenen Zweck sind
- Release und verteile freigegebene Applikationen und technische Lösungen in angemessener Form
- Bereite Business User und den Betrieb für die zu nutzenden Anwendungen und technischen Lösungen vor
- Stelle sicher, dass neue Business Anwendungen und Änderungen in exisiterenden Anwendungen frei von Fehlern sind

treiben

IT-Ziele

- Stelle sicher, dass automatischen Transaktionen und Informationsaustausch vertraut werden kann
- Reduziere Mängel und Nacharbeit bei Lösungen und dem Servicebetrieb
- Reagiere auf Geschäftsanforderungen in Übereinstimmung mit der Unternehmensstrategie
- Integriere die Anwendungen und Technologielösungen nahtlos in Geschäftsprozesse
- Stelle sicher, dass IT-Services und Infrastruktur Ausfällen auf Grund von Fehlern, bewussten Angriffen oder Katastrophen standhalten können und ihre Wiederherstellung gewährleistet ist
- Stelle die angemessene Verwendung und Performance der Anwendungen und technischen Lösungen sicher

werden gemessen durch

Key Performance Indicators

- Grad der Involvierung der Stakeholder in den Installations- und Akkreditierungsprozess
- % der Projekte mit einem dokumentierten und genehmigten Testplan
- Anzahl der durch den Post-Implementation Review gelernten Fakten
- % der Fehler, die während dem Qualitätssicherheitsreview der Installations- und Akkreditierungsfunktionen gefunden wurden
- Anzahl der umgesetzten Änderungen ohne der erforderlichen Freigabe durch das Management

werden gemessen durch

Key Goal Indicators

- % der die Installation und Akkreditierungs-prozess betreffenden Fehler, die während interner oder externer Audits gefunden wurden
- Nacharbeit nach Implementierung, die auf unzureichende Akzeptanztests zurück-zuführen ist
- Service Desk Anrufe von User, die auf unzureichendes Training zurückzuführen sind
- Ausfallszeit der Anwendung oder Korrekturen an den Daten, die durch ungeeignete Tests hervorgerufen wurden

werden gemessen durch

IT Key Goal Indicators

- % der Stakeholder, die mit der Datenintegrität der neuen Systeme zufrieden sind
- % der Systeme, die den erwarteten Nutzen erbringen, wie im Post-Implementation Review gemessen wurde

MATURITY MODEL

AI7 Install and Accredit Solutions and Changes *(Installiere und akkreditiere Lösungen und Changes)*

Die Reife des Management des Prozesses *Install and Accredit Solutions and Changes (Installiere und akkreditiere Lösungen und Changes)*, der die Geschäftsanforderungen an die IT erfüllt, dass die neuen oder geänderten Systeme nach dder Installation ohne bedeutende Probleme arbeiten, ist:

0 Non-existent (nicht existent):
Formelle Prozesse für Installationen oder Akkreditierung fehlen vollständig und weder das Senior-Management noch die IT-Mitarbeiter erkennen die Notwendigkeit der Verifikation, ob Lösungen für den geplanten Zweck geeignet sind.

1 Initial (initial):
Es besteht ein Bewusstsein für die Notwendigkeit der Verifikation und Bestätigung, dass implementierte Lösungen den vorgesehenen Zweck erfüllen. Tests werden für einige Projekte durchgeführt, die Initiative für die Tests bleibt jedoch bei den einzelnen Projektteams und die verwendeten Ansätze variieren. Formelle Akkreditierungen und Abnahmen sind selten oder inexistent.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Die Test- und Genehmigungsprozesse sind teilweise konsistent, basieren aber im Allgemeinen auf keiner Methodik. Die einzelnen Entwicklungsteams entscheiden üblicherweise über den Testansatz und Integrationstests werden normalerweise nicht durchgeführt. Ein informeller Abnahmeprozess existiert.

3 Defined (definiert):
Für die Installation, die Migration, die Konvertierung und die Abnahme existiert eine formelle Methodik. Die IT-Installations und Akkreditierungsprozesse sind in den System-Lebenszyklus integriert und zu einem gewissen Grad automatisiert. Schulungen, Tests und Übergaben in die Produktion sowie Akkreditierungen weichen, je nach der Entscheidung Einzelner, vom definierten Prozess ab. Die Qualität der Systeme bei der Übergabe in Produktion ist unterschiedlich, wobei neue Systeme oft ein signifikantes Maß an Probleme zur Nachbearbeitung verursachen.

4 Managed and measurable (gemanaged und messbar):
Die Verfahren sind formalisiert, gut entwickelt und praktikabel mit definierten Testumgebungen und Akkreditierungsverfahren. In der Praxis folgen alle wesentliche Changes an Systemen diesem formellen Ansatz. Die Evaluation, ob die Anforderungen der Anwender erfüllt werden, ist standardisiert und messbar, indem Metriken erzeugt werden, die durch das Management wirksam überprüft und analysiert werden können. Die Qualität von Systemen bei der Übergabe in Produktion ist trotz eines zumutbaren Maßes an Problemen zur Nachbearbeitung für das Management zufrieden stellend. Die Automatisierung des Prozesses findet ad hoc statt und ist projektabhängig. Das Management ist trotz der fehlenden Beurteilung nach der Implementation mit dem aktuellen Effizienz-Level zufrieden. Das Testsystem spiegelt die Live-Umgebung angemessen wider. Belastungstests für neue Systeme und Regressionstests für existierende Systeme werden für die grossen Projekte durchgeführt.

5 Optimised (optimiert):
Die Prozesse zur Installation und Akkreditierung befinden sich auf einem Level von Good Practice, basierend auf den Ergebnissen andauernder Verbesserung und Verfeinerung. Prozesse für die IT-Installation und –akkreditierung sind komplett in den System Lebenszyklus integriert und – wo sinnvoll – automatisiert, um die effizientesten Schulungen, Tests und Produktionsübernahmen neuer Systeme zu unterstützen. Gut entwickelte Testumgebungen, Problemverzeichnisse und Prozesse zur Fehlerbereinigung gewährleisten effiziente und wirksame Übergaben in die Produktionsumgebung. Die Akkreditierungen erfolgen üblicherweise ohne Nachbearbeitungen und Probleme nach der Implementierung sind normalerweise auf kleinere Korrekturen beschränkt. Die Reviews der Nach-Implementierung sind standardisiert, wobei Erfahrungsberichte an den Prozess zurück geleitet werden, um eine kontinuierliche Qualitätsverbesserung zu gewährleisten. Belastungstests neuer Systeme und Regressionstests für geänderte Systeme werden konsistent durchgeführt.

Diese Seite wurde absichtlich freigelassen

DELIVER AND SUPPORT

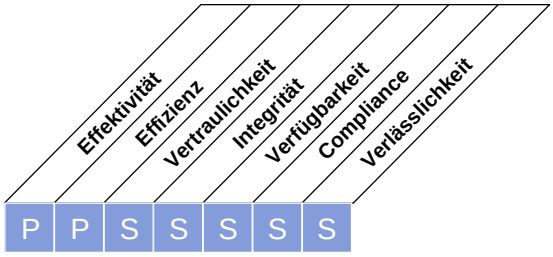
DS1 Define and Manage Service Levels
(Definiere und manage Service Levels)
DS2 Manage Third-party Services
(Manage Leistungen von Dritten)
DS3 Manage Performance and Capacity
(Manage Performance und Kapazität)
DS4 Ensure Continuous Service
(Stelle den kontinuierlichen Betrieb sicher)
DS5 Ensure Systems Security
(Stelle Security von Systemen sicher)
DS6 Identify and Allocate Costs
(Identifiziere und verrechne Kosten)
DS7 Educate and Train Users
(Schule und trainiere User)
DS8 Manage Service Desk and Incidents
(Manage den Service Desk und Incidents)
DS9 Manage the Configuration
(Manage die Konfiguration)
DS10 Manage Problems
(Manage Probleme)
DS11 Manage Data
(Manage Daten)
DS12 Manage the Physical Environment
(Manage die physische Umgebung)
DS13 Manage Operations
(Manage den Betrieb)

Diese Seite wurde absichtlich freigelassen

HIGH-LEVEL CONTROL OBJECTIVE

DS1 Define and Manage Service Levels *(Definiere und manage Service Levels)*

Eine effektive Kommunikation zwischen dem IT-Management und den Kunden im Unternehmen über die erforderlichen Services wird durch die dokumentierte Ausgestaltung und Vereinbarung von IT-Services und Service Levels ermöglicht. Dieser Prozess enthält ebenso die Überwachung und die zeitnahe Berichterstattung an die Interessensvertreter über die Erreichung von Service Levels. Der Prozess erlaubt die Angleichung zwischen IT-Services und den entsprechenden Unternehmenserfordernissen.



Kontrolle über den IT-Prozess,

Define and Manage Service Levels (*Definiere und manage Service Levels*)

der die Anforderung des Unternehmens an die IT bezüglich

der Angleichung zwischen den wesentlichen IT-Services und der Geschäftsstrategie gewährleistet

durch die Konzentration auf

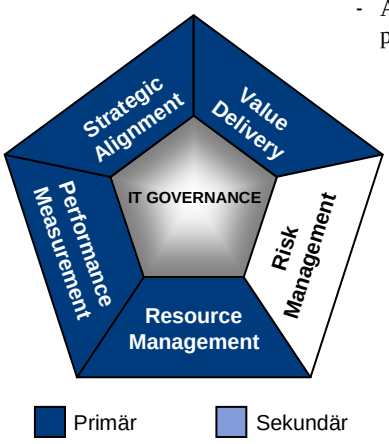
die Identifizierung der Serviceanforderungen, die Vereinbarung der Service Levels und die Überwachung der Einhaltung der Service Levels, *zufrieden stellt,*

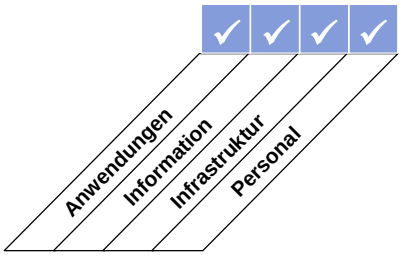
wird erreicht durch

- Formalisierung interner und externer Vereinbarungen gemäß den Anforderungen und Leistungsvermögen
- Berichterstattung über die Einhaltung der Service Levels (Berichte und Meetings)
- Identifizierung und Kommunikation neuer und aktualisierter Serviceanforderungen an die strategische Planung

und gemessen durch

- Prozent der Stakeholder, die zufrieden sind, dass die Dienstleistungserbringung die vereinbarten Service Levels erreichen
- Anzahl der geleisteten Services, die nicht im Service Katalog enthalten sind
- Anzahl der formellen SLA Review Meetings mit dem Unternehmensmanagement pro Jahr





DETAILLIERTE CONTROL OBJECTIVES

DS1 Define and Manage Service Levels *(Definiere und manage Service Levels)*

DS1.1 Service Level Management Framework (Service Level Management Framework)
Definiere ein Framework, das einen formalisierten Service Level Management-Prozess zwischen Kunden und dem Dienstleistungsanbieter zur Verfügung stellt. Das Framework erhält die laufende Anpassung mit den Unternehmenserfordernissen und -prioritäten aufrecht und unterstützt das gemeinsame Verständnis von Kunden und Dienstleister(n). Das Framework umfasst Prozesse für die Erstellung von Anforderungen an Services, Definition von Services, Service Level Agreements (SLAs), Operating Level Agreements (OLAs) und Finanzierungsmittel. Diese Attribute sind in einem Service-Katalog gesammelt. Das Framework definiert die organisatorische Struktur für das Service Level Management, die aus Rollen, Aufgaben und Verantwortlichkeiten von internen und externen Leistungsanbietern sowie von Kunden besteht.

DS1.2 Definition of Services (Definition von Services)
Stütze die Definition von IT-Services auf die Charakteristika der Services und die Unternehmensanforderungen, die zentral durch die Anwendung eines Service-Katalogs oder Service-Portfolios verwaltet und gespeichert sind.

DS1.3 Service Level Agreements (Service Level Agreements)
Definiere und vereinbare, basierend auf Kundenanforderungen und Fähigkeiten der IT, Service Level Agreements für alle entscheidenden IT-Services. Diese decken Kundenverpflichtungen, Unterstützungsanforderungen, quantitative und qualitative Messgrößen zur Messung des mit den Stakeholdern vereinbarten Service, finanzielle und wirtschaftliche Vereinbarungen (falls anwendbar) sowie Rollen und Verantwortlichkeiten, inklusive Beaufsichtigung des SLA. Zu berücksichtigende Einzelheiten sind Rahmenbedingungen für Verfügbarkeit, Verlässlichkeit, Performance, Wachstumsfähigkeiten, Support-Levels, Kontinuitätsplanung, Sicherheit und Nachfrage.

DS1.4 Operating Level Agreements (Operating Level Agreements)
Stelle sicher, dass Operating Level Agreements beschreiben, wie die Services technisch bereitgestellt werden, um die SLA(s) optimal zu unterstützen. Die OLAs spezifizieren die technischen Prozesse in einer für den Anbieter verständlichen Weise und können mehrere SLAs unterstützen.

DS1.5 Monitoring and Reporting of Service Level Achievements (Monitoring und Berichterstattung der Erreichung von Service Levels)
Monitore kontinuierlich festgelegte Kriterien der Service Levels Performance. Berichte über die Erreichung der Service Levels werden in einem für Stakeholder verständlichen Format erstellt. Die Überwachungsstatistiken werden analysiert und verfolgt, um negative und positive Trends für einzelne Services sowie die gesamten Services zu identifizieren.

DS1.6 Review of Service Level Agreements and Contracts (Review von Service Level Agreements und Underpinning Contracts)
Reviewe regelmäßig Service Level Agreements und Underpinning Contracts mit internen und externen Leistungsanbietenden, um sicherzustellen, dass diese wirksam und aktuell sind und dass Änderungen der Anforderungen berücksichtigt wurden.

MANAGEMENT GUIDELINES

DS1 Define and Manage Service Levels *(Definiere und manage Service Levels)*

Von	Inputs
PO1	Strategische und taktische IT-Pläne; IT-Serviceportfolio
PO2	Klassifizierte Daten
PO5	Aktualisiertes IT-Service Portfolio
AI2	Vorabversionen von SLAs
AI3	Vorabversionen von OLAs
DS4	Service-Anforderung für Notfälle (inkl. Rollen und Verantwortlichkeiten)
ME1	Performance Inputs für die IT-Planung

Outputs	Nach						
Report über Vertragsreview	DS2						
Berichte über Prozessperformance	ME1						
Neue / überarbeitete Anforderungen für Services	PO1						
SLAs	AI1	DS2	DS3	DS4	DS6	DS8	DS13
OLAs	DS4	DS5	DS6	DS7	DS8	DS11	
Aktualisiertes IT-Service Portfolio	PO1						

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security	Service Manager
Erzeuge ein Framework für die Festlegung von IT-Services			C	A	C	C	I	C	C	I	C	C
Erstelle einen IT Service-Katalog			I	A	C	C	I	C	C	I	I	R
Definiere Service Level Agreements (SLAs) für kritische IT Services		I	I	C	C	R	I	R	R	C	C	A/R
Definiere Operational Level Agreements (OLAs) entsprechend den SLAs				I	C	R	I	R	R	C	C	A/R
Überwache und berichte über die end-to-end Service Level Performance				I	I	R		I	I		I	A/R
Reviewe SLAs und Underpinning Contracts (externe Verträge)		I		I	C	R		R	R		C	A/R
Reviewe und aktualisiere den IT-Service-Katalog			I	A	C	C	I	C	C	I	I	R
Erstelle einen Verbesserungsplan für Services			I	A	I	R	I	R	C	C	I	R

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

Aktivitätsziele

- Festlegung der Services
- Formalisierung interner und externer Vereinbarungen gemäß den Anforderungen und Lieferfähigkeiten
- Berichterstattung über die Erreichung von Service Levels (Berichte und Meetings)
- Sicherstellung, dass Berichte auf die Zielgruppe der Empfänger zugeschnitten sind
- Feedback neuer und aktualisierter Service Anforderungen an die strategische Planung

treiben

Prozessziele

- Baue ein gemeinsames Verständnis über die Levels des benötigten Services auf
- Formalisiere und überwache Service Level Agreements und Leistungskriterien.
- Passe die zu erbringenden Services an die vereinbarten Service Levels an
- Erstelle einen up-to-date Service-Katalog, der an die Unternehmensziele angepasst ist

treiben

IT-Ziele

- Stelle die Enduser-Zufriedenheit mit den Serviceangeboten und Service Levels sicher
- Reagiere auf Geschäftsanforderungen in Übereinstimmung mit der Unternehmens-strategie
- Stelle Transparenz und Verständnis von IT-Kosten, Nutzen, Strategie, Richtlinien und Service Levels sicher

werden gemessen durch

Key Performance Indicators

- Anzahl der formellen SLA Review Meetings mit den Geschäftsbereichen pro Jahr
- % der berichteten Service Levels
- % der automatisch berichteten Service Levels
- Anzahl der verstrichenen Arbeitstage zwischen der Vereinbarung des Service Level Agreements mit dem Kunden und der Anpassung eines Service Levels

werden gemessen durch

Key Goal Indicators

- Anzahl der erbrachten Services, die nicht im Katalog enthalten sind
- % der Services, die den Service Levels entsprechen
- % der gemessenen Service Levels

werden gemessen durch

IT Key Goal Indicators

- % der Stakeholder, die zufrieden sind, dass die Dienstleistungserbringung die vereinbarten Service Levels erreichen
- % der Benutzer, die zufrieden sind, dass die Dienstleistungserbringung die vereinbarten Service Levels erreichen

MATURITY MODEL

DS1 Define and Manage Service Levels *(Definiere und manage Service Levels)*

Die Reife des Management des Prozesses *Define and Manage Service Levels (Definiere und manage Service Levels)*, der den Geschäftsanforderungen an die IT abdeckt der Angleichung zwischen den wesentlichen IT-Services und der Geschäftsstrategie, ist:

0 Non-existent (nicht existent):
Das Management hat die Notwendigkeit für einen Prozess zur Festlegung von Service Levels nicht erkannt. Zur Überwachung dieser Service Levels sind keine Aufgaben und Verantwortlichkeiten festgelegt.

1 Initial (initial):
Das Bewusstsein für die Notwendigkeit der Verwaltung von Service Levels ist vorhanden, der Prozess ist jedoch informell und reaktiv. Die Aufgaben und Verantwortlichkeiten für die Festlegung und Verwaltung von Service Levels sind nicht festgelegt. Wenn Performance-Messungen existieren, sind diese ausschließlich qualitativ und mit ungenau definierten Zielen. Die Berichterstattung ist informell, unregelmäßig und inkonsistent.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Vereinbarte Service Levels sind vorhanden, sie sind jedoch informell und werden keinem Review unterzogen. Die Berichterstattung über Service Levels ist lückenhaft und könnte für die Kunden irrelevant oder irreführend sein. Die Berichterstattung über Service Levels hängt von den Fähigkeiten und Bemühungen einzelner Manager ab. Ein Koordinator für die Service Levels mit definierten Verantwortlichkeiten aber begrenzten Kompetenzen wird eingesetzt. Falls ein Prozess für die Einhaltung von Service Level Agreements existiert, ist es freiwillig und wird nicht durchgesetzt.

3 Defined (definiert):
Die Aufgaben sind klar definiert, aber mit willkürlichen Kompetenzen. Ein Prozess für die Entwicklung von Service Level Agreements mit Kontrollpunkten für die Neueinschätzung von Service Levels und der Kundenzufriedenheit wird eingesetzt. Die Service Levels sind festgelegt, dokumentiert und vereinbart, indem ein Standardprozess angewendet wird. Die Unterschreitungen von Service Levels werden identifiziert, die Verfahren für den Umgang mit Unterschreitungen sind jedoch informell. Eine klare Verbindung zwischen der erwarteten Erreichung von Service Levels und der Finanzierung wurde erstellt. Den Service Levels wird zugestimmt, sie decken jedoch nicht unbedingt die Geschäftsanforderungen ab.

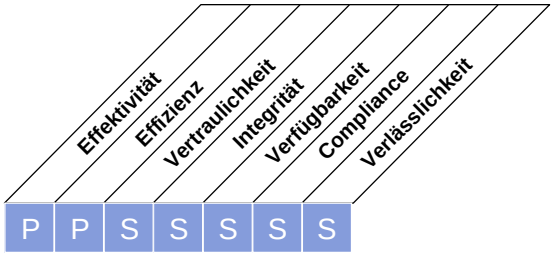
4 Managed and measurable (gemanaged und messbar):
Service Levels werden vermehrt in der Phase der Definition von betrieblichen Anforderungen festgelegt und im Design der Anwendungen oder betrieblichen Umgebungen berücksichtigt. Die Kundenzufriedenheit wird routinemäßig gemessen und beurteilt. Die Performance-Messungen spiegeln vermehrt die Anforderungen der Kunden und weniger die IT-Ziele wider. Die Messungen für die Einschätzung der Service Level Agreements werden standardisiert und widerspiegeln Industrienormen. Die Kriterien für die Festlegung von Service Levels basieren auf der betrieblichen Kritikalität und beinhalten Verfügbarkeit, Verlässlichkeit, Performance, Wachstumskapazität, Anwenderunterstützung, Kontinuitätsplanung und Sicherheitsüberlegungen. Die Analyse von Grundursachen wird routinemäßig durchgeführt, wenn die Service Levels nicht eingehalten werden. Der Prozess für die Berichterstattung über die Überwachung von Service Levels wird zunehmend automatisiert. Operationelle und finanzielle Risiken verbunden mit der Verfehlung von vereinbarten Service Levels werden genau bestimmt und verstanden. Eine formelle Anordnung für die Messung von KPIs und KGIs wurde institutionalisiert und wird unterhalten.

5 Optimised (optimiert):
Service Levels werden kontinuierlich neu überprüft, um die Ausrichtung auf IT- und Unternehmensziele zu gewährleisten, wobei die Vorteile von Methoden wie dem Gewinnkoeffizienten (engl.: *cost-benefit ratio*) wahrgenommen werden. Alle Prozesse zur Verwaltung von Service Levels werden fortlaufend verbessert. Der Grad der Kundenzufriedenheit wird kontinuierlich überwacht und verwaltet. Die erwarteten Service Levels spiegeln die strategischen Ziele der Organisationseinheiten wider und werden mit Industrienormen verglichen. Das IT-Management besitzt die zur Erreichung der Service Level Ziele notwendigen Ressourcen und Kompetenzen – und die (finanziellen) Entschädigungen sind so strukturiert, dass sie einen Anreiz für die Erfüllung dieser Ziele schaffen. Das Senior-Management überwacht die KPIs und KGIs im Rahmen eines kontinuierlichen Verbesserungsprozesses.

HIGH-LEVEL CONTROL OBJECTIVE

DS2 Manage Third-party Services *(Manage Leistungen von Dritten)*

Das Erfordernis sicherzustellen, dass die von Dritten erbrachten Leistungen den Unternehmenserfordernissen entsprechen, setzt einen wirksamen Prozess voraus. Dieser Prozess wird zustande gebracht, indem klare Rollen, Aufgaben und Erwartungen in den Vereinbarungen mit Dritten festgehalten werden und und auch diese Vereinbarungen auf Wirksamkeit und Compliance überprüft und überwacht werden. Ein wirksames Management der Leistungen von Dritten reduziert Unternehmensrisiken, die auf notleidenden Lieferanten beruhen.



Kontrolle über den IT-Prozess,

Manage Third-party Services (*Manage Leistungen von Dritten*)

der die Anforderung des Unternehmens an die IT bezüglich

der zufriedenstellenden Erbringung von Leistungen Dritter unter Wahrung der Transparenz über Nutzen, Kosten und Risiken

durch die Konzentration auf

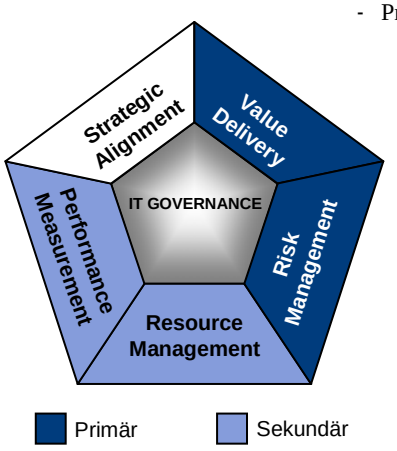
den Aufbau von Beziehungen und bilateraler Verantwortung mit qualifizierten, externen Leistungsanbietern und die Überwachung der Service Delivery, um die Einhaltung der Vereinbarungen zu verifizieren und zu garantieren, *zufrieden stellt,*

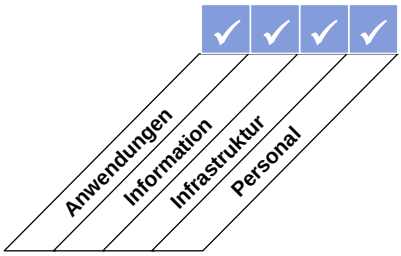
wird erreicht durch

- Identifizierung und Kategorisierung der Leistungen von Lieferanten
- Identifizierung und Reduktion der lieferantenbezogenen Risiken
- Überwachung und Messung der Performance von Lieferanten

und gemessen durch

- Anzahl der Anwenderbeschwerden hinsichtlich der vereinbarten Services
- Prozent der Hauptlieferanten, welche die klar definierten Anforderungen und Service Levels erfüllen
- Prozent der wichtigsten Lieferanten, die gemonitort werden





DETAILLIERTE CONTROL OBJECTIVES

DS2 Manage Third-party Services *(Manage Leistungen von Dritten)*

DS2.1 Identification of All Supplier Relationships (Identifikation aller Beziehungen mit Lieferanten)
Identifiziere alle Leistungen von Lieferanten und kategorisiere sie entsprechend Lieferantentyp, Bedeutung und Kritikalität. Unterhalte formelle Dokumentation technischer und organisatorischer Beziehungen mit Rollen und Verantwortlichkeiten, Zielen, erwarteten Leistungen und Empfehlungsschreiben von Beauftragten dieser Lieferanten.

DS2.2 Supplier Relationship Management (Lieferanten-Beziehungsmanagement)
Formalisiere den Prozess des Beziehungsmanagements für alle Lieferanten. Der Beziehungsverantwortliche muss eine Verbindung zwischen Kunde und Lieferant herstellen und sicherstellen, dass die Beziehung auf Vertrauen und Transparenz basiert (zB durch Service Level Agreements).

DS2.3 Supplier Risk Management (Lieferanten-Risikomanagement)
Identifiziere und behandle Risiken bezüglich der Fähigkeit des Lieferanten, weiterhin wirksam Leistungen in einer sicheren und wirtschaftlichen Weise auf einer konstanten Basis zu erbringen. Stelle sicher, dass Verträge sich nach den allgemeingültigen Unternehmensstandards richten und in Übereinstimmung stehen mit rechtlichen und regulativen Anforderungen. Das Risikomanagement sollte auch Geheimhaltungsvereinbarungen (engl.: *non-disclosure agreements (NDAs)*), Hinterlegungsverträge, andauernde Überlebensfähigkeit des Anbieters, Konformität mit Sicherheitserfordernissen, alternative Lieferanten, Konventionalstrafen und Boni, etc berücksichtigen.

DS2.4 Supplier Performance Monitoring (Monitoring der Performance von Lieferanten)
Etabliere einen Prozess, um die Leistungserbringung zu überwachen, um sicherzustellen, dass der Lieferant die bestehenden Unternehmenserfordernisse erfüllt und weiterhin das Vertragswerk und die Service Level Agreements einhält und dass die Leistungen konkurrenzfähig sind mit alternativen Anbietern und den Marktverhältnissen sind.

MANAGEMENT GUIDELINES

DS2 Manage Third-party Services *(Manage Leistungen von Dritten)*

Von	Inputs
PO1	IT-Sourcing-Strategie
PO8	Beschaffungsstandards
AI5	Vertragliche Vereinbarungen; Anforderungen für Beziehungsmanagement mit externen Partnern
DS1	SLAs; Report über Vertragsreview
DS4	Service-Anforderung für Notfälle (inkl. Rollen und Verantwortlichkeiten)

Outputs	Nach
Berichte über Prozessperformance	ME1
Katalog der Lieferanten	AI5
Lieferanten-Risiken	PO9

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Identifiziere und kategorisiere Beziehungen zu Leistungen der Dritten				I	C	R	C	R	A/C	C	C
Definiere und dokumentiere die Prozesse des Lieferantenmanagements		C		A	I	R	I	R	R	C	C
Führe Richtlinien und Verfahren für die Beurteilung und Auswahl von Lieferanten ein		C		A	C	C		C	R	C	C
Identifiziere, bewerte und reduziere lieferantenbezogene Risiken		I		A		R		R	R	C	C
Überwache die Service Delivery der Lieferanten				R	A	R		R	R	C	C
Evaluiere langfristige Ziele hinsichtlich der Lieferanten-Beziehungen für alle Stakeholder	C	C	C	A/R	C	C	C	C	R	C	C

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Identifikation und Kategorisierung der Leistungen von Lieferanten
- Identifikation und Reduktion der lieferantenbezogenen Risiken
- Überwachung und Messung der Performance von Lieferanten

treiben

Prozessziele

- Baue Beziehungen und bilaterale Verantwortung mit qualifizierten, externen Leistungsanbietern auf
- Überwache die Service Delivery und verifiziere die Einhaltung der Vereinbarungen
- Stelle sicher, dass der Lieferant den relevanten internen und externen Standards entspricht
- Beobachte das Interesse des Lieferanten an der Weiterführung der Geschäftsbeziehung

treiben

IT-Ziele

- Stelle die gegenseitig zufriedenstellenden Lieferantenbeziehungen sicher
- Stelle die Enduser-Zufriedenheit mit den Serviceangeboten und Service Levels sicher
- Stelle Transparenz und Verständnis von IT-Kosten, Nutzen, Strategie, Richtlinien und Service Levels sicher

werden gemessen durch

Key Performance Indicators

- % der wichtigsten Lieferanten, die klar festgelegten Anforderungen und Service Levels unterliegen
- % der wichtigsten Lieferanten, die gemonitort werden
- Zufriedenheitsgrad der Geschäftsbereiche mit der Wirksamkeit der Kommunikation des Lieferanten
- Zufriedenheitsgrad des Lieferanten mit der Wirksamkeit der Kommunikation des Unternehmens
- Anzahl der wesentlichen Ereignisse der Non-Compliance des Lieferanten

werden gemessen durch

Key Goal Indicators

- % der Hauptlieferanten, welche die klar definierten Anforderungen und Service Levels erfüllen
- Anzahl der formellen Streitfälle mit Lieferanten
- % der bemängelten Lieferantenrechnungen

werden gemessen durch

IT Key Goal Indicators

- Anzahl der Anwenderbeschwerden hinsichtlich der vereinbarten Services
- % der Ankäufe, die einer konkurrenzbetonten Beschaffung unterstanden

MATURITY MODEL

DS2 Manage Third-party Services *(Manage Leistungen von Dritten)*

Die Reife des Management des Prozesses *Manage Third-party Services (Manage Leistungen von Dritten)*, der die Geschäftsanforderungen an die IT erfüllt der zufriedenstellenden Erbringung von Leistungen Dritter unter Wahrung der Transparenz über Nutzen, Kosten und Risiken, ist:

0 Non-existent (nicht existent):
Aufgaben und Verantwortlichkeiten sind nicht definiert. Formelle Richtlinien und Verfahren für die Vertragsschließung mit Dritten sind nicht vorhanden. Die Leistungen von Dritten werden durch das Management weder bewilligt noch einem Review unterzogen. Messungen und Berichterstattung durch Dritte existieren nicht. Auf Grund des Mangels an der vertraglichen Verpflichtung für die Berichterstattung ist sich das Management über die Qualität der erbrachten Leistungen nicht bewusst.

1 Initial (initial):
Dem Management ist die Notwendigkeit dokumentierter Richtlinien und Verfahren für das Management der Drittparteien, inklusive unterschriebener Verträge bewusst. Standardisierte Bedingungen für die Übereinkommen mit Dritten sind nicht vorhanden. Die Messung der erbrachten Leistungen ist informell und reaktiv. Die Praktiken hängen von den Erfahrungen einzelner Personen und dem Leistungserbringer ab (zB on demand).

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Der Prozess zur Überwachung externer Leistungsanbieter, damit verbundener Risiken und der Leistungserbringung ist informell. Ein unterzeichneter pro forma Vertrag mit standardisierten Lieferantenbedingungen und -Konditionen (zB die Beschreibung der zu erbringenden Leistungen) wird verwendet. Berichte über die erbrachten Leistungen sind verfügbar, unterstützen die betrieblichen Ziele jedoch nicht.

3 Defined (definiert):
Gut dokumentierte Verfahren sind vorhanden, um die Leistungen Dritter mittels klarer Prozesse für Sicherheitsüberprüfungen und Verhandlungen mit Lieferanten zu lenken. Wenn eine Übereinkunft für die Erbringung von Leistungen getroffen wird, besteht nur eine Beziehung zum Leistungserbringer auf vertraglicher Ebene. Die Art der zu erbringenden Leistung ist im Vertrag genau beschrieben und enthält Gesetzes-, Betriebs- und Kontrollanforderungen. Die Verantwortlichkeit für die Aufsicht über die Leistungserbringung Dritter ist festgelegt. Vertragliche Bedingungen basieren auf standardisierten Vorlagen. Das mit den Leistungen Dritter verbundene betriebliche Risiko wird beurteilt und gemeldet.

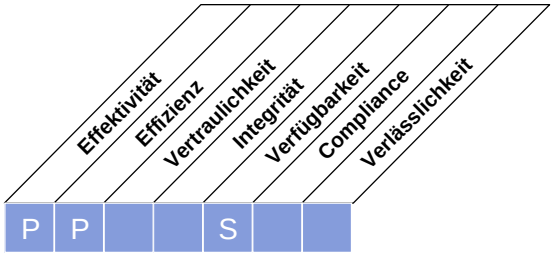
4 Managed and measurable (gemanaged und messbar):
Formelle und standardisierte Kriterien für die Festlegung der Bestimmungen der Beauftragung, inklusive dem Arbeitsbereich, der zu erbringenden Leistungen/Lieferungen, der Annahmen, der Zeitpläne, der Kosten, der Abrechnungsvereinbarungen und der Verantwortlichkeiten werden erstellt. Die Verantwortlichkeiten für das Vertrags- und Lieferanten-Management sind zugewiesen. Die Qualifikationen, Risiken und Fähigkeiten der Lieferanten werden kontinuierlich verifiziert. Die Leistungsanforderungen werden festgehalten und mit den betrieblichen Zielen verbunden. Ein Prozess zur Überprüfung der Performance der erbrachten Leistungen gegenüber den vertraglichen Bedingungen ist vorhanden, welcher den Input für die Beurteilung der aktuellen und zukünftigen Leistungen Dritter liefert. Modelle zur Festsetzung des Verrechnungspreises werden im Beschaffungsprozess angewandt. Alle involvierten Parteien sind sich der erwarteten Leistungen, Kosten und Meilensteine bewusst. Den KPIs und KGIs für die Beaufsichtigung der Leistungserbringer wurde zugestimmt.

5 Optimised (optimiert):
Die mit Drittparteien abgeschlossenen Verträge werden periodisch in vordefinierten Intervallen überprüft. Die Verantwortlichkeiten für das Management der Lieferanten und der Qualität der erbrachten Leistungen sind zugewiesen. Der Nachweis für die Vertragseinhaltung bezüglich der Betriebs-, Gesetzes- und Kontrollvorkehrungen wird überwacht und korrektive Handlungen werden durchgesetzt. Der Drittanbieter wird einem unabhängigen periodischen Review unterzogen und Feedback über die Performance wird bereitgestellt und zur Verbesserung der Leistungserbringung genutzt. Die Messtechniken variieren als Antwort auf sich verändernde Geschäftsbedingungen. Die Messungen unterstützen die frühzeitige Erkennung von potentiellen Problemen mit den Leistungen Dritter. Die umfassende, definierte Berichterstattung der Erreichung von Service Levels ist mit den Entschädigungen der Drittanbieter verbunden. Das Management gleicht den Prozess für den Erwerb und die Überwachung der Leistungen Dritter ab, basierend auf dem Ergebnis der KPIs und KGIs.

HIGH-LEVEL CONTROL OBJECTIVE

DS3 Manage Performance and Capacity (*Manage Performance und Kapazität)*

Das Erfordernis, die Performance und Kapazität der IT-Ressourcen zu managen, bedingt einen Prozess, mit dem periodisch die aktuelle Performance und Kapazität der IT-Ressourcen beurteilt wird. Dieser Prozess berücksichtigt die Prognose künftiger Bedürfnisse, basierend auf den Anforderungen an die Arbeitslast, den Speicher und an die Sicherstellung des störungsfreien Betriebs (engl.: *contingency*). Dieser Prozess bietet die Bestätigung, dass die Unternehmenserfordernisse unterstützende Informations-Ressourcen kontinuierlich zur Verfügung stehen.



Kontrolle über den IT-Prozess,

Manage Performance and Capacity (*Manage Performance und Kapazität*)

der die Anforderung des Unternehmens an die IT bezüglich

der Performanceoptimierung der IT-Infrastruktur, Ressourcen und Fähigkeiten in Einklang mit den Unternehmenserfordernissen

durch die Konzentration auf

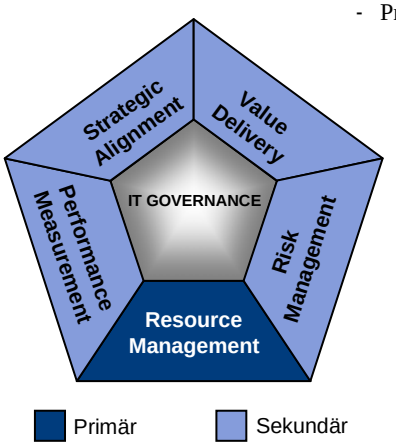
die Einhaltung der in den Service Level Agreements festgelegten Antwortzeiten, Minimierung der Ausfallszeiten und kontinuierliche Verbesserung der IT-Performance und Kapazität mittels Überwachung und Messung, *zufrieden stellt,*

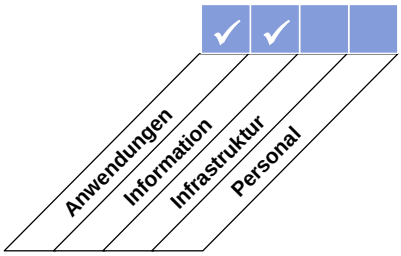
wird erreicht durch

- Planung und Bereitstellung von Systemkapazität und -verfügbarkeit
- Überwachung der und Berichterstattung über Systemperformance
- Modellierung und Vorhersage der Systemperformance

und gemessen durch

- Anzahl der verlorenen Stunden pro User und Monat aufgrund unzureichender Kapazitätenplanung
- Prozent der Spitzenlastzeiten, in denen die Zielauslastung übertroffen worden ist
- Prozent der Antwortzeiten, die den SLAs nicht entsprechen





DETAILLIERTE CONTROL OBJECTIVES

DS3 Manage Performance and Capacity (*Manage Performance und Kapazität)*

DS3.1 Performance and Capacity Planning (Planung von Performance und Kapazität)
Richte einen Planungsprozess zur Überprüfung der Performance und Kapazität von IT-Ressourcen ein, um sicherzustellen, dass kostenmäßig begründbare Kapazität und Performance verfügbar ist, um den in den Service Level Agreements festgelegten Workload zu bewältigen. Kapazitäts- und Performance-Pläne sollten geeignete Modellierungstechniken anwenden, um ein Modell der derzeitigen und künftigen Performance, Kapazität und Durchsatz der IT-Ressourcen zu erhalten.

DS3.2 Current Capacity and Performance (Gegenwärtige Kapazität und Performance)
Überprüfe die derzeitige Kapazität und Performance der IT-Ressourcen, um zu bestimmen, ob ausreichende Kapazität und Performance vorhanden ist, um die Leistungen entsprechend der Service Level Agreements zu erbringen.

DS3.3 Future Capacity and Performance (Künftige Kapazität und Performance)
Erstelle in regelmäßigen Abständen Vorhersagen der Performance und Kapazität von IT-Ressourcen, um das Risiko einer Serviceunterbrechung auf Grund ungenügender Kapazität oder einer Performanceverschlechterung zu minimieren. Identifiziere auch überschüssige Kapazitäten für mögliche andere Einsätze. Identifiziere Auslastungstrends und erstelle Prognosen als Input für Performance- und Kapazitätspläne.

DS3.4 IT Resources Availability (Verfügbarkeit der IT-Ressourcen)
Stelle die benötigte Kapazität und Performance bereit unter Berücksichtigung von Aspekten wie normale Auslastung, Notfälle, Speicheranforderungen und Lebenszyklus von IT-Ressourcen. Vorkehrungen wie Priorisierung von Aufgaben, Fehlertoleranzmechanismen und Ressourcenverteilungspraktiken sollten getroffen werden, falls die Performance und Kapazität nicht dem erforderlichen Niveau entspricht. Das Management sollte sicherstellen, dass Kontinuitätspläne die Verfügbarkeit, Kapazität und Performance der einzelnen IT-Ressourcen angemessen berücksichtigen.

DS3.5 Monitoring and Reporting (Monitoring und Reporting)
Monitore laufend die Performance und Kapazität von IT-Ressourcen. Die gesammelten Daten dienen den beiden Zwecken:

- Die derzeitige Performance innerhalb der IT aufrecht zu erhalten und zu tunen, wobei Ausfallssicherheit, Zwischenfälle, derzeitige und künftige Auslastung, Speicherpläne und Beschaffung von Ressourcen behandelt werden.
- Über Verfügbarkeit der erbrachten Services an die Geschäftsbereiche zu berichten, wie dies in SLAs festgehalten ist. Mit allen Ausnahmeberichten werden entsprechende Empfehlungen für korrektive Handlungen abgegeben.

MANAGEMENT GUIDELINES

DS3 Manage Performance and Capacity (*Manage Performance und Kapazität)*

Von	Inputs
AI2	Verfügbarkeits-, Kontinuitäts- und Recovery-Spezifikation
AI3	Anforderungen an Systemmonitoring
DS1	SLAs

Outputs	Nach						
Performance- und Kapazitätsinformation	PO2	PO3					
Performance- und Kapazitätsplan (Anforderungen)	PO5	AI1	AI3	ME1			
Erforderliche Änderungen	AI6						
Report der Prozessperformance	ME1						

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Richte einen Planungsprozess für das Review der Performance und Kapazität von IT-Ressourcen ein				A		R	C	C	C	C	
Reviewe aktuelle Performance und Kapazitäten der IT-Ressourcen				C	I	A/R		C	C	C	
Führe Prognosen zur Performance und Kapazität von IT-Ressourcen durch				C	C	A/R	C	C	C	C	
Führe Gap-Analysen zur Identifikation inkompatibler IT-Ressourcen durch				C	I	A/R		R	C	C	I
Führe eine Notfallplanung für die mögliche Nichtverfügbarkeit der IT-Ressourcen durch				C	I	A/R		C	C	I	C
Überwache und berichte laufend über die Verfügbarkeit, Performance und Kapazität der IT-Ressourcen				I	I	A/R		I	I	I	I

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Planung und Gewährleistung von Systemkapazität und -verfügbarkeit
- Überwachung und Berichterstattung der Systemperformance
- Modellierung und Prognose der Systemperformance

werden gemessen durch

Key Performance Indicators

- Häufigkeit von Performance- und Kapazitätsprognosen
- % der Anlagen, die in Kapazitätenreviews enthalten sind
- % der Anlagen die durch zentralisierte Tools überwacht werden

treiben

Prozessziele

- Überwache und messe die Lastspitzen (engl. peak load) und die Antwortzeiten von Transaktionen
- Halte die in den SLAs festgelegten Antwortzeiten ein
- Minimiere die Transaktionsversagen
- Minimiere die Ausfallszeit
- Optimiere die Auslastung der IT-Ressourcen

werden gemessen durch

Key Goal Indicators

- Lastspitzen und Gesamtauslastungsrate
- % der Spitzenlastzeiten, in denen die Zielauslastung übertroffen wird
- Prozent der Antwortzeiten, die den SLAs nicht entsprechen
- Versagensrate von Transaktionen

treiben

IT-Ziele

- Reagiere auf Geschäftsanforderungen in Übereinstimmung mit der Unternehmensstrategie
- Stelle die Verfügbarkeit der IT-Services gemäß den Anforderungen sicher
- Optimiere IT-Infrastruktur, Ressourcen und Fähigkeiten

werden gemessen durch

IT Key Goal Indicators

- Anzahl der verlorenen Stunden pro User und Monat auf Grund unzureichender Kapazitätsplanung
- Anzahl der kritischen Geschäftsprozesse, die nicht von einem definierten Service Availability Plan gedeckt werden

MATURITY MODEL

DS3 Manage Performance and Capacity (*Manage Performance und Kapazität)*

Die Reife des Management des Prozesses *Manage Performance and Capacity (Manage Performance und Kapazität)*, der die Geschäftsanforderungen an die IT abdeckt der Performanceoptimierung der IT-Infrastruktur, Ressourcen und Fähigkeiten in Einklang mit den Unternehmenserfordernissen, ist:

0 Non-existent (nicht existent):
Das Management hat nicht erkannt, dass wesentliche Geschäftsprozesse einen hohen Grad an Performance von der IT benötigen oder dass die allgemeinen betrieblichen Anforderungen für IT-Leistungen die Kapazität überschreiten könnten. Ein Verfahren für Kapazitätsplanung ist nicht vorhanden.

1 Initial (initial):
Die Anwender müssen oft provisorische Lösungen wegen der Performance- und Kapazitätseinschränkungen entwickeln. Die Verantwortlichen („Owner“) der Geschäftsprozesse haben wenig Verständnis für die Notwendigkeit der Planung von Kapazität und Performance. Die Bemühungen zur Verwaltung von Performance und Kapazität sind üblicherweise reaktiv. Der Prozess zur Kapazitäts- und Performanceplanung ist informell. Das Verständnis für die aktuelle und zukünftige Kapazität und Performance der IT-Ressourcen ist begrenzt.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Das Geschäfts- und IT-Management sind sich der Auswirkungen eines fehlenden Performance- und Kapazitäts-Managements bewusst. Die Anforderungen zur Performance werden im Allgemeinen erfüllt, basierend auf Beurteilungen von einzelnen Systemen und dem Wissen der Support- und Projektteams. Manche einzelne Werkzeuge werden verwendet, um Probleme bei der Performance und Kapazität zu diagnostizieren, aber die Konsistenz der Ergebnisse hängt von den Fachkenntnissen einzelner Schlüsselpersonen ab. Eine allgemeine Einschätzung der Leistungsfähigkeit der IT-Performance oder eine Abwägung der Situation bei Spitzen- und Worst-Case-Belastung ist nicht vorhanden. Verfügbarkeitsprobleme treten unvorhergesehen und zufällig auf und benötigen erhebliche Zeit, um diagnostiziert und korrigiert zu werden. Jede Art der Performance-Messung basiert hauptsächlich auf den Anforderungen der IT und nicht auf denen der Kunden.

3 Defined (definiert):
Die Performance- und Kapazitätsanforderungen sind über den gesamten System-Lebenszyklus festgelegt. Definierte Anforderungen zu den Service Levels und Metriken zur Messung der betrieblichen Performance sind vorhanden. Zukünftige Performance- und Kapazitätsanforderungen werden nach einem definierten Prozess modelliert. Berichte mit Performance-Statistiken werden erstellt. Performance- und Kapazitätsprobleme treten immer noch auf und sind zeitaufwändig zu berichtigen. Trotz der Veröffentlichung von Service Levels sind die Anwender und Kunden über die Leistungsfähigkeit skeptisch.

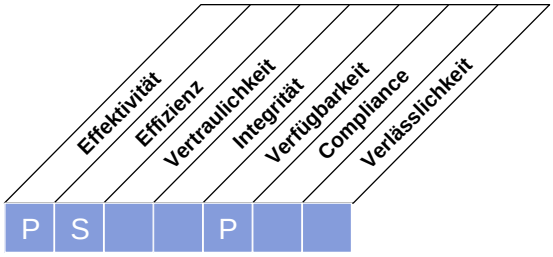
4 Managed and measurable (gemanaged und messbar):
Prozesse und Werkzeuge für die Messung der Systembenutzung, Performance und Kapazität sind verfügbar und die Ergebnisse werden mit festgelegten Zielen abgeglichen. Aktuelle Informationen sind verfügbar; sie ermöglichen standardisierte Performancestatistiken und alarmierende Störfälle, die durch unzureichende Performance und Kapazität hervorgerufen werden. Fragen mangelhafter Performance und Kapazität werden gemäss definierten und standardisierten Verfahren behandelt. Automatisierte Werkzeuge werden für die Überwachung besonderer Ressourcen, wie der Laufwerkskapazität, Netzwerken, Servern und Netzwerk-Gateways eingesetzt. Performance- und Kapazitätsstatistiken werden in einer für Kerngeschäftsverantwortliche verständlichen Form berichtet, damit die Anwender und Kunden die IT-Service Levels verstehen. Die Anwender sind im Allgemeinen zufrieden mit der aktuellen Leistungserbringung und dürfen neue und verbesserte Verfügbarkeitslevel fordern. KGIs und KPIs für die Messung der IT-Performance und -Kapazität wurden vereinbart, werden aber nur sporadisch und inkonsistent angewendet.

5 Optimised (optimiert):
Die Planung der Performance und Kapazität ist vollständig mit den betrieblichen Bedarfsvorhersagen abgestimmt. Die IT-Infrastruktur und der betriebliche Bedarf werden regelmäßigen einem Review unterzogen, um sicherzustellen, dass die optimale Kapazität zu den geringsten Kosten erreicht wird. Die Werkzeuge für die Überwachung kritischer IT-Ressourcen wurden standardisiert und werden über alle Plattformen eingesetzt und mit einem unternehmensweiten Incident-Management-System verbunden. Die Überwachungswerkzeuge können Performance- und Kapazitätsprobleme erkennen und automatisch korrigieren. Trendanalysen werden ausgeführt und zeigen drohende Performanceprobleme auf, die durch steigende Geschäftsvolumina verursacht werden; sie ermöglichen die Planung und Vermeidung unerwarteter Vorfälle. Die Metriken für die Messung der IT-Performance und -Kapazität wurden fein abgestimmt zu KGIs und KPIs für alle kritischen Geschäftsprozesse und werden konsistent gemessen. Das Management richtet die Planung der Performance und Kapazität nach der Analyse der KGIs und KPIs aus.

HIGH-LEVEL CONTROL OBJECTIVE

DS4 Ensure Continuous Service *(Stelle den kontinuierlichen Betrieb sicher)*

Die Notwendigkeit, IT-Services kontinuierlich anzubieten, erfordert die Entwicklung, Aufrechterhaltung und den Test von IT-Kontinuitätsplänen, ausgelagerte Aufbewahrung von Backup und das regelmäßige Training des Notfallvorsorgeplans. Ein wirksamer Prozess für kontinuierliche Services minimiert die Wahrscheinlichkeit von bedeutenden Unterbrechungen von IT-Services und deren Auswirkung auf wesentliche Unternehmensfunktionen und -prozesse.



Kontrolle über den IT-Prozess,

Ensure Continuous Service (*Stelle den kontinuierlichen Betrieb sicher*)

der die Anforderung des Unternehmens an die IT bezüglich

der Sicherstellung einer minimalen Auswirkung auf die Geschäftstätigkeit im Falle einer Unterbrechung der IT-Services

durch die Konzentration auf

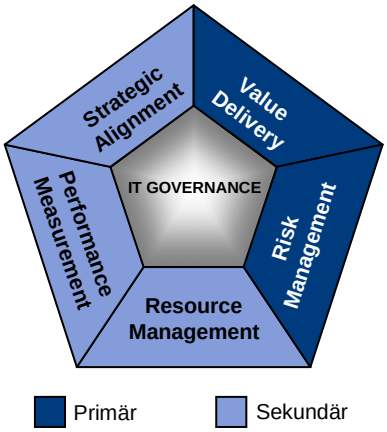
die Integration von Ausfallssicherheit in automatisierte Lösungen und die Entwicklung, Wartung und das Testen von IT-Kontinuitätsplänen, *zufrieden stellt,*

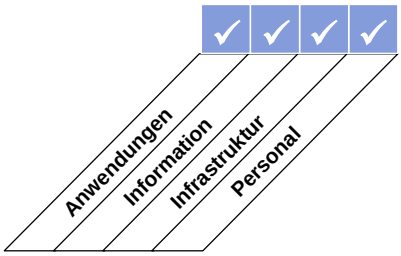
wird erreicht durch

- Entwicklung und Wartung (Verbesserung) einer IT-Notfallplanung
- Schulungen über und Tests von IT-Notfallplänen
- Aufbewahrung von Kopien der Notfallpläne und Daten an einem entfernten Standort

und gemessen durch

- Anzahl verlorener Stunden pro User und Monat aufgrund von ungeplanten Ausfällen
- Anzahl von geschäftskritischen, auf die IT angewiesenen Prozessen, die durch die IT-Notfallplanung nicht abgedeckt werden





DETAILLIERTE CONTROL OBJECTIVES

DS4 Ensure Continuous Service *(Stelle den kontinuierlichen Betrieb sicher)*

DS4.1 IT Continuity Framework (Framework für IT-Kontinuität)
Entwickle ein Framework für IT-Kontinuität zur Unterstützung eines unternehmensweiten Management der Geschäftskontinuität durch einen konsistenten Prozess. Das Ziel des Frameworks ist die Unterstützung bei der Bestimmung der notwendigen Ausfallssicherheit der Infrastruktur und das Vorantreiben der Entwicklung von Wiederanlauf- und IT-Kontinuitätsplänen (engl.: *disaster recovery and IT contingency plans*). Das Framework sollte die Organisationsstruktur für Kontinuitätsmanagement behandeln, mit den Rollen, Aufgaben und Verantwortlichkeiten von internen und externen Dienstleistern, ihrem Management und ihren Kunden, und die Rollen und Strukturen für Dokumentation, Test und Ausführung der Wiederanlauf- und IT-Kontinuitätsplänen. Der Plan sollte Einzelheiten wie die Identifikation kritischer Ressourcen, das Monitoring und Reporting der Verfügbarkeit kritischer Ressourcen, alternative Verarbeitung und die Grundprinzipien für Backup und Wiederherstellung umfassen.

DS4.2 IT Continuity Plans (IT-Kontinuitätspläne)
Entwickle basierend auf dem Framework IT-Kontinuitätspläne, die auf die Reduktion der Auswirkungen einer wesentlichen Unterbrechung auf die Schlüssel-Geschäftsfunktionen und -Prozesse ausgelegt sind. Die Pläne sollten die Anforderungen für Ausfallsicherheit, alternative Verarbeitung und Wiederherstellungstauglichkeit für alle kritischen IT-Services behandeln. Sie sollten auch Gebrauchsanleitungen, Rollen und Verantwortlichkeiten, Verfahren, Kommunikationsprozesse und das Testvorgehen abdecken.

DS4.3 Critical IT Resources (Kritische IT-Ressourcen)
Lenke die Aufmerksamkeit auf die im IT-Kontinuitätsplan als am kritischsten definierten Elemente, um Ausfallsicherheit einzubauen und um Prioritäten für den Wiederanlauf festzulegen. Vermeide die Ablenkung der Wiederherstellung weniger kritischer Elemente und stelle Reaktion und Wiederanlauf entsprechend den priorisierten Unternehmensbedürfnissen sicher, unter Wahrung der Kosten auf einem akzeptablen Niveau gehalten werden und der Einhaltung regulatorischer und vertraglicher Anforderungen. Beachte Anforderungen für Ausfallsicherheit, Reaktion und Wiederherstellung für verschiedene Abstufungen, zB eine bis vier Stunden, vier bis 24 Stunden, mehr als 24 Stunden und kritische geschäftliche Betriebszeiten.

DS4.4 Maintenance of the IT Continuity Plan (Wartung des IT-Kontinuitätsplans)
Unterstütze das IT-Management bei der Festlegung und Anwendung von Verfahren zur Steuerunv von Changes, um sicherzustellen, dass der IT-Kontinuitätsplan aktuell gehalten wird und fortwährend die aktuellen Geschäftsanforderungen widerspiegelt. Es ist wichtig, dass Veränderungen der Verfahren und Verantwortlichkeiten klar und rechtzeitig kommuniziert werden.

DS4.5 Testing of the IT Continuity Plan (Test des IT-Kontinuitätsplans)
Teste den IT-Kontinuitätsplan regelmäßig, um sicherzustellen, dass alle IT-Systeme wirksam wiederhergestellt werden können, Mängel behandelt werden und die Pläne zweckmäßig bleiben. Dies verlangt eine sorgfältige Vorbereitung, Dokumentation, Berichterstattung über Testergebnisse und – abhängig von den Ergebnissen – die Umsetzung einer Maßnahmenplanung. Erwäge den Umfang für Wiederherstellungstests von einzelnen Anwendungen, integrierten Test-Szenarios bis hin zu durchgehenden Tests und integrierten Anbieter-Tests.

DS4.6 IT Continuity Plan Training (Schulung des IT-Kontinuitätsplans)
Stelle sicher, dass alle betroffenen Parteien regelmäßig Schulungen für die im Ereignis- oder Katastrophenfall anzuwendenden Verfahren sowie ihrer Rollen und Verantwortlichkeiten erhalten. Verifiziere und erweitere Trainings entsprechend den Ergebnissen von Kontinuitätstests.

DS4.7 Distribution of the IT Continuity Plan (Verteilung des IT-Kontinuitätsplans)
Stelle sicher, dass eine festgelegte und gesteuerte Verteilungsstrategie besteht, um sicherzustellen, dass die Pläne genau und sicher an geeignete, autorisierte Interessensgruppen verteilt werden und diesen bei Bedarf – zeitlich und örtlich – zur Verfügung stehen. Es sollte darauf geachtet werden, dass die Pläne für alle Katastrophenszenarien verfügbar gemacht werden.

DS4.8 IT-Services Recovery and Resumption (Wiederherstellung und Wiederanlauf von IT-Services)
Plane die Aktionen für den Zeitraum, während die IT wiederhergestellt und die Services wieder aufgenommen werden. Dies kann die Aktivierung von Ausweichsstandorten, die Inbetriebnahme der alternativen Verarbeitung, die Kommunikation mit Kunden und Stakeholdern, Wiederanlaufverfahren etc beinhalten. Stelle sicher, dass die Fachbereiche die IT-Wiederherstellungszeiten und die notwendigen technologischen Investitionen zur Unterstützung der geschäftlichen Bedürfnisse hinsichtlich Wiederherstellung und Wiederanlauf verstehen.

DS4.9 Offsite Backup Storage (Auslagerung von Backup)
Lagere alle kritischen Backup-Medien, Dokumentationen und andere IT-Ressourcen, welche für den IT-Wiederanlauf und die Geschäftskontinuitätspläne notwendig sind, an einem entfernten Standort aus. Der Inhalt der Backup-Aufbewahrung sollte in

Zusammenarbeit zwischen Geschäftsprozesseignern und den IT-Mitarbeiter bestimmt werden. Die Verwaltung der externen Lagereinrichtung sollte dem Datenklassifikationsschema und Unternehmenspraktiken für Medienlagerung folgen. Das IT-Management sollte sicherstellen, dass die Vorkehrungen für Auslagerung periodisch (mindestens jährlich) nach ihrem Inhalt, dem umgebungsbezogenen Schutz und der Sicherheit beurteilt werden. Stelle die Kompatibilität von Hardware und Software sicher, um die archivierten Daten wiederherzustellen, periodisch zu testen und archivierte Daten aufzufrischen.

DS4.10 Post-resumption Review (Review nach dem Wiederanlauf)
Bestimme nach erfolgreichem Wiederanlauf der IT-Funktionen nach einem Unglück, ob das IT-Management Verfahren für die Beurteilung der Angemessenheit der Pläne und für deren dementsprechende Überarbeitung etabliert hat.

MANAGEMENT GUIDELINES

DS4 Ensure Continuous Service *(Stelle den kontinuierlichen Betrieb sicher)*

Von	Inputs
PO2	Klassifizierte Daten
PO9	Risikobewertung
AI2	Verfügbarkeits-, Kontinuitäts- und Recovery-Spezifikation
AI4	Benutzer-, Betriebs-, Support-, technische und administrative Handbücher
DS1	SLAs und OLAs

Outputs	Nach						
Ergebnisse Contingency-Tests	PO9						
Incident- und Katastrophen-Schwellwerte	DS8						
Kritikalität von IT-Configuration Items	DS9						
Plan zur Lagerung und Schutz von Backups	DS11	DS13					
Service-Anforderung für Notfälle (inkl. Rollen und Verantwortlichkeiten)	DS1	DS2					

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Entwickle ein Framework für die IT-Kontinuität		C	C	A	C	R	R	R	C	C	R
Führe eine Business-Impact-Analyse und eine Risikobeurteilung durch		C	C	C	C	A/R	C	C	C	C	C
Entwickle und unterhalte IT-Kontinuitätspläne	I	C	C			A/R	C	C	C	C	C
Identifiziere und kategorisiere IT-Ressourcen nach deren Wiederherstellungszielen				C		A/R		C	I	C	I
Definiere und wende Änderungskontrollverfahren an, um sicherzustellen, dass der IT-Kontinuitätsplan auf dem neuesten Stand ist				I		A/R		R	R	R	I
Teste regelmäßig den IT-Kontinuitätsplan				I	I	A/R		C	C	I	I
Entwickle einen Folgeplan basierend auf den Testergebnissen				C	I	A/R	C	R	R	R	I
Plane und führe Trainings für den IT-Wiederanlauf durch				I	R	A/R		C	R	I	I
Plane die Wiederherstellung und den Wiederanlauf von IT-Services		I	I	C	C	A/R	C	R	R	R	C
Plane und implementiere Backup-Archivierung und -Sicherung				I		A/R		C	C	I	I
Führe Verfahren für die Durchführung der Reviews nach dem Wiederanlauf ein				C	I	A/R		C	C		C

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Entwicklung und Aufrechterhaltung (Verbesserung) einer IT-Notfallplanung
- Schulungen über und Tests von IT-Kontinuitätsplänen
- Aufbewahrung von Kopien der Notfallpläne und Daten an entfernten Standorten

werden gemessen durch

Key Performance Indicators

- Zeitspanne zwischen den Tests von jeglichen Bestandteilen des IT-Kontinuitätsplans
- Schulungsstunden über die IT-Kontinuität pro Jahr und betroffenem IT-Mitarbeiter
- % der kritischen Infrastrukturkomponenten mit automatisierter Verfügbarkeits-überwachung
- Häufigkeit von Reviews des IT-Kontinuitätsplans

treiben

Prozessziele

- Führe einen IT-Kontinuitätsplan ein, der die Kontinuitätspläne der Geschäftsbereiche unterstützt
- Entwickle durchführbare IT-Kontinuitäts-pläne, die getestet und gewartet werden
- Minimiere die Wahrscheinlichkeit einer IT-Service-Unterbrechung

werden gemessen durch

Key Goal Indicators

- % der Verfügbarkeiten, die die SLAs erfüllen
- Anzahl von geschäftskritischen, auf IT angewiesene Prozessen, die durch die IT-Notfallplanung nicht abgedeckt wurde
- % der Tests, die die Zielsetzungen bezüglich Wiederherstellung erreichen
- Häufigkeit der Service-Unterbrechungen bei kritischen Systemen

treiben

IT-Ziele

- Stelle die Verfügbarkeit der IT-Services gemäß den Anforderungen sicher
- Stelle sicher, dass der Einfluss einer IT-Service-Störung oder -Änderung auf das Geschäft minimiert ist
- Stelle sicher, dass IT-Services und Infrastruktur Ausfälle auf Grund von Fehlern, bewussten Angriffen oder Katastrophen standhalten können und ihre Wiederherstellung gewährleistet ist

werden gemessen durch

IT Key Goal Indicators

- Anzahl der verlorenen Stunden pro User und Monat auf Grund von ungeplanten Ausfällen

MATURITY MODEL

DS4 Ensure Continuous Service *(Stelle den kontinuierlichen Betrieb sicher)*

Die Reife des Management des Prozesses *Ensure Continuous Service (Stelle den kontinuierlichen Betrieb sicher)*, der die Geschäftsanforderungen an die IT der Sicherstellung einer minimalen Auswirkung auf die Geschäftstätigkeit im Falle einer Unterbrechung der IT-Services, ist:

0 Non-existent (nicht existent):
Es besteht kein Verständnis für die Risiken, Verletzbarkeiten und Bedrohungen für den IT-Betrieb oder die Auswirkungen eines Ausfalls der IT-Services auf das Unternehmen. Service-Kontinuität wird nicht betrachtet, Aufmerksamkeit des Management zu benötigen.

1 Initial (initial):
Die Verantwortlichkeiten für kontinuierliche Services sind informell und die Kompetenz, die Pflichten auszuüben, ist begrenzt. Das Management erkennt das Risiko bei und die Notwendigkeit für kontinuierliche Services. Der Fokus der Aufmerksamkeit des Managements in Bezug auf kontinuierliche Services liegt auf Infrastruktur-Ressourcen und weniger auf IT-Services. Die Anwender setzen provisorische Lösungen als Reaktion auf Service-Incidents ein. Die Reaktionen der IT auf größere Unterbrechungen sind reaktiv und unvorbereitet. Vorgesehene Ausfälle werden eingeplant, um die IT-Anforderungen zu erfüllen, berücksichtigen jedoch keine betrieblichen Anforderungen.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Die Verantwortlichkeit für die Gewährleistung kontinuierlicher Services ist zugewiesen. Die Ansätze für die Gewährleistung der Servicekontinuität sind bruchstückhaft. Die Berichterstattung über die Systemverfügbarkeit ist sporadisch, kann unvollständig sein und berücksichtigt die geschäftlichen Auswirkungen nicht. Es besteht kein dokumentierter IT-Kontinuitätsplan, obwohl Verpflichtungen für die kontinuierliche Verfügbarkeit von Services vorhanden sind und die wesentlichen Grundprinzipien bekannt sind. Ein Verzeichnis kritischer Systeme und Komponenten ist vorhanden, ist jedoch nicht unbedingt zuverlässig. Praktiken zur Servicekontinuität entstehen, aber ihr Erfolg hängt von einzelnen Personen ab.

3 Defined (definiert):
Die Verantwortlichkeiten für die Verwaltung der Servicekontinuität sind eindeutig. Die Aufgaben für die Planung und das Testen der Servicekontinuität sind klar festgelegt und zugewiesen. Der IT-Kontinuitätsplan ist dokumentiert und basiert auf der Kritikalität der Systeme und den betrieblichen Auswirkungen. Eine periodische Berichterstattung über Tests der Servicekontinuität ist vorhanden. Einzelne Personen ergreifen die Initiative, um Standards zu befolgen und Schulungen über den Umgang mit bedeutenden Ereignissen oder Katastrophen zu erhalten. Das Management kommuniziert konsistent die Notwendigkeit der Planung für die Gewährleistung kontinuierlicher Services. Hoch-verfügbare Komponenten und System-Redundanz werden eingesetzt. Ein Verzeichnis kritischer Systeme und Komponenten wird gepflegt.

4 Managed and measurable (gemanaged und messbar):
Die Verantwortlichkeiten und Standards für kontinuierliche Services werden durchgesetzt. Die Verantwortung für die Pflege des Servicekontinuitätplans ist festgelegt. Die Pflegeaktivitäten basieren auf den Ergebnissen der Tests der Servicekontinuität, internen Good Practices und den Veränderungen der IT- und Betriebsumgebung. Strukturierte Daten über die Servicekontinuität werden gesammelt, analysiert, gemeldet und danach gehandelt. Formelle und vorgeschriebene Schulungen über die Prozesse für die Servicekontinuität werden bereitgestellt. Good Practices der Systemverfügbarkeit werden konsistent genutzt. Die Praktiken für die Verfügbarkeit und die Planung der Servicekontinuität beeinflussen einander gegenseitig. Unterbrechungen werden klassifiziert und der jeweilige Eskalationspfad ist allen involvierten Personen gut bekannt. Die KGIs und KPIs für die Servicekontinuität wurden entwickelt und vereinbart, werden aber teilweise inkonsistent gemessen.

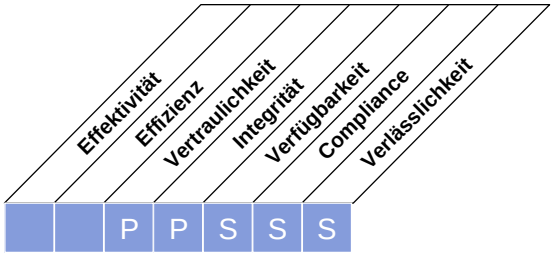
5 Optimised (optimiert):
Integrierte Prozesse für die Servicekontinuität berücksichtigen Benchmarking und die besten externen Praktiken. Der IT-Kontinuitätsplan ist in die betrieblichen Kontinuitätspläne integriert und wird routinemäßig gepflegt. Die Anforderungen für die Gewährleistung der Servicekontinuität werden durch die Anbieter und wesentlichen Zulieferer gesichert. Globale Tests für die IT-Kontinuitätsplanung werden ausgeführt und die Testergebnisse werden als Eingabe für die Aktualisierung des Plans verwendet. Die Erfassung und Analyse von Daten werden für die kontinuierliche Verbesserung des Prozesses verwendet. Die Verfügbarkeitspraktiken und die Planung der Servicekontinuität sind vollständig abgestimmt. Das Management gewährleistet, dass keine Katastrophe oder ein größeres Ereignis auf Grund eines Single Point of Failure auftritt. Die Praktiken zur Eskalation werden verstanden und uneingeschränkt durchgesetzt. Die KGIs und KPIs für die Erreichung kontinuierlicher Services werden systematisch gemessen. Das Management richtet die Planung der Servicekontinuität in Reaktion auf die KGIs und KPIs aus.

Diese Seite wurde absichtlich freigelassen

HIGH-LEVEL CONTROL OBJECTIVE

DS5 Ensure Systems Security *(Stelle Security von Systemen sicher)*

Die Notwendigkeit, die Integrität von Informationen zu erhalten sowie die IT-bezogenen Vermögenswerte zu schützen, erfordert einen Security Management-Prozess. Dieser Prozess umfasst die Erstellung und Aufrechterhaltung von Rollen, Verantwortlichkeiten, Richtlinien, Standards und Verfahren für die IT-Sicherheit. Security Management umfasst ebenfalls die Überwachung und den periodischen Test sowie die Umsetzung korrektiver Maßnahmen für erkannte Schwachstellen oder Vorfälle. Wirksames Security Management schützt alle IT-bezogenen Vermögenswerte, um die Auswirkungen auf das Kerngeschäft durch Schwachstellen oder Vorfälle zu minimieren.



Kontrolle über den IT-Prozess,

Ensure Systems Security (*Stelle Security von Systemen sicher*)

der die Anforderung des Unternehmens an die IT bezüglich

der Aufrechterhaltung der Integrität von Informationen und der Infrastruktur der Informationsverarbeitung und der Minimierung der Auswirkungen von Sicherheitsschwachstellen und Incidents

durch die Konzentration auf

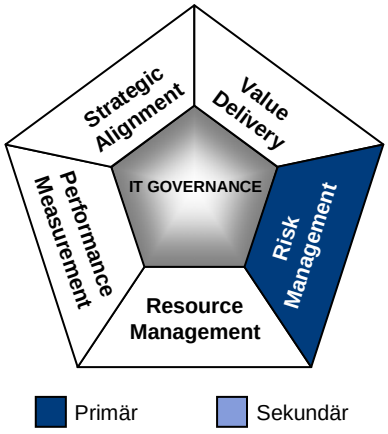
die Festlegung von IT-Sicherheitsrichtlinien, Verfahren und Standards sowie die Überwachung, Erkennung, Berichterstattung und Lösung von Sicherheitsschwachstellen und -Incidents, *zufrieden stellt,*

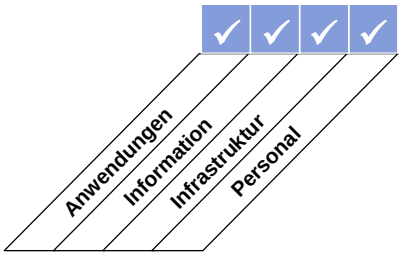
wird erreicht durch

- Verstehen der Sicherheitsanforderungen, -schwachstellen und -Incidents
- Management von Benutzerkennungen und -berechtigungen in standardisierter Art
- Regelmäßiges Testen der Sicherheit

und gemessen durch

- Anzahl der Vorfälle die dem Ruf des Unternehmens in der Öffentlichkeit schaden
- Anzahl der Systeme, die den Sicherheitsanforderungen nicht entsprechen
- Anzahl der Verstöße gegen die Funktionstrennung





DETAILLIERTE CONTROL OBJECTIVES

DS5 Ensure Systems Security *(Stelle Security von Systemen sicher)*

DS5.1 Management of IT Security (Management der IT-Sicherheit)
Manage die IT-Sicherheit auf der höchstmöglichen organisatorischen Ebene, so dass das Management von sicherheitsrelevanten Aktivitäten in Einklang steht mit den Unternehmensanforderungen.

DS5.2 IT Security Plan (IT-Security Plan)
Überführe den Informationsbedarf des Unternehmens, die IT-Konfiguration, Maßnahmenpläne für informationsbezogene Risiken und die Kultur der Informationssicherheit in einen umfassenden IT-Security Plan. Der Plan ist implementiert in Sicherheitsrichtlinien und -verfahren zusammen mit angemessenen Investitionen in Services, Personal, Software und Hardware. Sicherheitsrichtlinien und -verfahren werden an Stakeholder und Benutzer kommuniziert.

DS5.3 Identity Management (Identitätsmanagement)
Alle (internen, externen, temporären) Benutzer und ihre Aktivitäten auf IT-Systemen (Geschäftsanwendungen, Systembetrieb, Entwicklung und Wartung) sollten eindeutig identifizierbar sein. Benutzerberechtigungen für die Systeme und Daten sollten mit festgelegten und dokumentierten Geschäftsbedürfnissen und Arbeitsplatzanforderungen übereinstimmen. Benutzerberechtigungen werden durch das Management des Fachbereichs angefordert, durch die Systemeigner bewilligt und durch die sicherheitsverantwortliche Person implementiert. Benutzerkennungen und Zugriffsberechtigungen werden in einer zentralen Datenbank geführt. Kostengünstige technische und organisatorische Maßnahmen werden eingesetzt und aktuell gehalten, um die Benutzeridentifikation zu ermitteln, die Authentisierung einzurichten und Zugriffsrechte durchzusetzen.

DS5.4 User Account Management (Management von Benutzerkonten)
Stelle sicher, dass Antrag, Einrichtung, Ausstellung, Aufhebung, Änderung und Schließung von Benutzerkonten und zugehörige Benutzerberechtigungen durch die Benutzerkontenverwaltung behandelt werden. Ein Freigabeverfahren sollte darin enthalten sein, dass den Daten- oder Systemeigner behandelt, der die Zugriffsberechtigungen bewilligt. Diese Verfahren sollten für sämtliche Benutzer, einschließlich Administratoren (privilegierte Benutzer), interne und externe Benutzer, für normale und für Notfalls-Changes Gültigkeit haben. Rechte und Pflichten in Zusammenhang mit dem Zugriff auf Unternehmenssysteme und -informationen sollten vertraglich für alle Arten von Benutzer festgelegt werden. Führe regelmäßig Management-Reviews aller Benutzerkonten und entsprechenden Berechtigungen durch.

DS5.5 Security Testing, Surveillance and Monitoring (Testen, Beobachtung und Überwachung der Sicherheit)
Stelle sicher, dass die Umsetzungen der IT-Sicherheit getestet und proaktiv überwacht wird. Die IT-Sicherheit sollte periodisch neu zertifiziert werden, um sicherzustellen, dass der genehmigte Sicherheitsgrad beibehalten wird. Eine Protokollierungs- und Monitoringfunktion ermöglicht die frühzeitige Erkennung von ungewöhnlichen oder abnormalen Aktivitäten, die eventuell behandelt werden müssen. Der Zugriff zur Protokollierungsinformation steht bezüglich Zugriffsrechten und Aufbewahrungsvorschriften in Einklang mit den Geschäftsanforderungen.

DS5.6 Security Incident Definition (Definition von Security Incidents)
Stelle sicher, dass die Charakteristika von möglichen Security Incidents klar definiert und kommuniziert werden, so dass Sicherheitsvorfälle korrekt durch den Incident oder Problem-Management-Prozess behandelt werden können. Die Charakteristika umfassen eine Beschreibung dessen, was als Security Incident verstanden wird und dem Grad der Auswirkungen. Eine begrenzte Anzahl von Auswirkungsniveaus sind definiert und für alle sind die spezifisch erforderlichen Aktivitäten und die zu benachrichtigenden Personen identifiziert.

DS5.7 Protection of Security Technology (Schutz von Sicherheitseinrichtungen)
Stelle sicher, dass wichtige Sicherheitstechnologie gegen Sabotage abgesichert wird und dass Sicherheitsdokumentation nicht unnötigerweise veröffentlicht wird, was bedeutet, dass sie nicht auffällt. Mache jedoch die Sicherheit von Systemen nicht von der Geheimhaltung der Sicherheitsspezifikationen abhängig.

DS5.8 Cryptographic Key Management (Verwaltung kryptographischer Schlüssel)
Stelle sicher, dass Richtlinien und Verfahren etabliert sind für die Erzeugung, Änderung, Widerrufung, Zerstörung, Verteilung, Zertifizierung, Speicherung, Eingabe, Verwendung und Archivierung von kryptographischen Schlüsseln, um den Schutz der Schlüssel gegen Veränderung und unberechtigte Aufdeckung sicherzustellen.

DS5.9 Malicious Software Prevention, Detection and Correction (Schutz vor, Erkennung und Korrektur von bösartiger Software)
Stelle sicher, dass präventive, detektive und korrektive Maßnahmen (speziell aktuelle Sicherheits-Patches und Virenschutz) in der gesamten Organisation vorhanden sind, um Informationssysteme und die Technologie vor bösartigem Code (Viren, Würmer, Spionage-Software (engl.: *spyware*), Spam, intern entwickelte betrügerische Software etc) zu schützen.

DS5.10 Network Security (Netzwerk-Sicherheit)
Stelle sicher, dass technische Sicherheitsmaßnahmen und zugehörige Managementverfahren (zB Firewall, Sicherheits-Appliances, Netzwerksegmentierung und Intrusionserkennung) verwendet werden, um den Zugriff zu Netzwerken zu bewilligen und den Informationsfluss von und zu Netzwerken zu steuern.

DS5.11 Exchange of Sensitive Data (Austausch sensitiver Daten)
Stelle sicher, dass sensitive Transaktionsdaten nur über einen vertrauenswürdigen Pfad oder ein Medium ausgetauscht werden mit (den notwendigen) Maßnahmen, um die Authentizität des Inhalts, den Beweis der Aufgabe und des Empfangs und Nichtabstreitbarkeit der Quelle zu bieten.

MANAGEMENT GUIDELINES

DS5 Ensure Systems Security *(Stelle Security von Systemen sicher)*

Von	Inputs
PO2	Informationsarchitektur; Klassifizierte Daten
PO3	Technologiestandards
PO9	Risikobewertung
AI2	Spezifikation der anwendungsspezifischen Sicherheitsmaßnahmen
DS1	OLAs

Outputs	Nach
Definition Security Incidents	DS8
Spezifische Schulungserfordernisse für Sicherheitsbewusstsein	DS7
Berichte der Prozessperformance	ME1
Erforderliche Security-Änderungen	AI6
Security-Bedrohungen und Schwachstellen	PO9

RACI-CHART*

Aktivitäten / Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Definiere und unterhalte einen IT-Sicherheitsplan	I	C	C	A	C	C	C	C	I	I	R
Definiere, erstelle und führe einen Identity- (Benutzerkonten-) managementprozess aus			I	A	C	R	R	I			C
Überwache mögliche und wirkliche Security Incidents				A	I	R	C	C			R
Reviewe und bestätige Benutzerzugriffsberechtigungen und -privilegien periodisch				I	A	C					R
Erstelle und unterhalte Verfahren für die Wartung und den Schutz von kryptographischen Schlüsseln				A		R		I			C
Implementiere und unterhalte technische Maßnahmen und Verfahren zum Schutz des Informationsflusses in Netzen				A	C	C	R	R			C
Führe regelmäßig Verletzbarkeitsanalysen durch		I		A	I	C	C	C			R

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Verstehen der Sicherheitsanforderungen, -schwachstellen und -bedrohungen
- Management von Benutzerkennungen und -berechtigungen in standardisierter Art
- Definition von Security Incidents
- Regelmäßiges Testen der Sicherheit

treiben

Prozessziele

- Gestatte nur autorisierten Usern Zugang zu kritischen und sensiblen Daten
- Identifiziere, überwache und melde Sicherheitsschwachstellen und -Incidents
- Erkenne und kläre unberechtigten Zugang zu Informationen, Anwendungen und Infrastruktur auf
- Minimiere die Auswirkungen von Sicherheitsschwachstellen und -Incidents

treiben

IT-Ziele

- Stelle den Schutz von kritischen und vertraulichen Informationen vor unberechtigtem Zugriff sicher
- Stelle sicher, dass automatischen Transaktionen und Informationaustausch vertraut werden kann
- Erhalte die Integrität der Informationen und die diese verarbeitende Infrastruktur
- Übernimm die Verantwortung für und schütze alle IT-Anlagen
- Stelle sicher, dass IT-Services und Infrastruktur Ausfällen auf Grund von Fehlern, bewussten Angriffen oder Katastrophen standhalten können und ihre Wiederherstellung gewährleistet ist

werden gemessen durch

Key Performance Indicators

- Häufigkeit und Review der Art der Security-Incidents, die überwacht werden sollen
- Anzahl und Art von veralteten Benutzerkonten
- Anzahl der nicht autorisierten IP-Adressen und Ports sowie der Typen des zurückgewiesenen Netzwerkverkehrs
- Prozent der kompromittierten und widerrufenen kryptografischen Schlüssel
- Anzahl der Zugriffsberechtigungen, die autorisiert, widerrufen, gelöscht oder verändert wurden

werden gemessen durch

Key Goal Indicators

- Anzahl und Art der vermuteten und wirklichen Zugangsverstöße
- Anzahl der Verstöße gegen die Funktionstrennung
- % der User, welche die Passwort-Standards nicht einhalten
- Anzahl und Art von verhinderten bösartigen Codes

werden gemessen durch

IT Key Goal Indicators

- Anzahl der Erreignisse mit Auswirkungen auf das Unternehmen
- Anzahl der Systeme, die den Sicherheits-anforderungen nicht entsprechen
- Dauer für die Bewilligung, Veränderung und Löschung von Zugangsberechtigungen

MATURITY MODEL

DS5 Ensure Systems Security *(Stelle Security von Systemen sicher)*

Die Reife des Management des Prozesses *Ensure Systems Security (Stelle Security von Systemen sicher)*, der die Geschäftsanforderungen an die IT abdeckt der Aufrechterhaltung der Integrität von Informationen und der Infrastruktur der Informationsverarbeitung und der Minimierung der Auswirkungen von Sicherheitsschwachstellen und -vorfällen, ist:

0 Non-existent (nicht existent):
Das Unternehmen erkennt die Notwendigkeit für IT-Sicherheit nicht. Aufgaben und Verantwortlichkeiten für die Gewährleistung der Sicherheit sind nicht festgelegt. Metriken, die das Management der IT-Sicherheit unterstützen, werden nicht eingesetzt. Eine Berichterstattung zur IT-Sicherheit und ein Reaktionsverfahren für IT-Sicherheitsverstöße sind nicht vorhanden. Ein erkennbares Administrationsverfahren der Systemsicherheit fehlt vollständig.

1 Initial (initial):
Das Unternehmen erkennt die Notwendigkeit der IT-Sicherheit. Das Bewusstsein für die Notwendigkeit der Sicherheit hängt hauptsächlich von der Einzelperson ab. Die IT-Sicherheit ist reaktiv ausgerichtet. IT-Sicherheit wird nicht gemessen. Erkannte IT-Sicherheitsverstöße provozieren die Suche nach Schuldigen, da die Verantwortlichkeiten unklar sind. Die Reaktion auf Verstöße gegen die IT-Sicherheit ist unvorhersehbar.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Die Aufgaben und Verantwortlichkeiten für die IT-Sicherheit werden einem IT-Sicherheits-Koordinator zugeordnet, obwohl die Managementautorität des Koordinators begrenzt ist. Das Bewusstsein für die Notwendigkeit der Sicherheit ist fragmentiert und limitiet. Obwohl sicherheitsrelevante Informationen durch die Systeme erzeugt werden, werden diese nicht analysiert. Die Leistungen Dritter decken nicht unbedingt die konkreten Sicherheitsanforderungen des Unternehmens ab. Sicherheitsrichtlinien werden entwickelt, jedoch sind die Fähigkeiten und Werkzeuge unzureichend. Die Berichterstattung zur IT-Sicherheit ist unvollständig, irreführend oder nicht sachdienlich. Sicherheitsschulungen sind verfügbar, werden jedoch nur auf Grund der Initiative von Einzelpersonen durchgeführt. Die IT-Sicherheit wird hauptsächlich als Verantwortungsbereich und Arbeitsgebiet der IT angesehen und die Fachbereiche sehen die IT-Sicherheit nicht in ihrem Aufgabenbereich.

3 Defined (definiert):
Ein Sicherheitsbewusstsein ist vorhanden und wird durch das Management gefördert. Die IT-Sicherheitsverfahren sind festgelegt und mit der IT-Sicherheitspolitik abgeglichen. Verantwortlichkeiten für die IT-Sicherheit sind festgelegt und werden verstanden, werden jedoch nicht konsistent durchgesetzt. Eine Planung der IT-Sicherheit und Sicherheitslösungen ist, durch Risikoanalysen angetrieben, vorhanden. Die Berichterstattung über Sicherheit beinhaltet keinen klaren betrieblichen Fokus. *Ad hoc* Sicherheitstests (z. B. Testen von unberechtigten Eingriffen („intrusion testing“)) werden durchgeführt. Sicherheitsschulungen sind für die IT und die Fachbereiche verfügbar, werden aber nur informell geplant und verwaltet.

4 Managed and measurable (gemanaged und messbar):
Die Verantwortlichkeiten für die IT-Sicherheit sind klar zugewiesen, verwaltet und durchgesetzt. Die Analysen der IT-Sicherheitsrisiken und Auswirkungen werden konsistent durchgeführt. Sicherheitsrichtlinien und -verfahren werden durch konkrete Mindeststandards für Sicherheit vervollständigt. Die Aussetzung mit Methoden für die Förderung des Sicherheitsbewusstseins ist verbindlich. Die Anwenderidentifikation, Authentifikation und Autorisierung ist standardisiert. Sicherheitszertifizierung wird für Mitarbeiter, die verantwortlich für die Prüfung und Verwaltung der Sicherheit sind, verfolgt. Sicherheitstests werden mit Hilfe standardisierter und formeller Prozesse durchgeführt, die zur Verbesserung der Sicherheit führen. Die IT-Sicherheitsprozesse werden durch eine unternehmensweite Sicherheitsfunktion koordiniert. Die Berichterstattung zur IT-Sicherheit ist mit den betrieblichen Zielen verknüpft. Die IT-Sicherheitsschulungen werden sowohl in den Fachbereichen als auch in der IT durchgeführt. Die IT-Sicherheitsschulungen sind derart geplant und verwaltet, dass die auf betriebliche Anforderungen und definierte IT-Sicherheits-/Risikoprofile reagieren. Die KGIs und KPIs für das Sicherheitsmanagement wurden definiert, werden bis jetzt aber noch nicht gemessen.

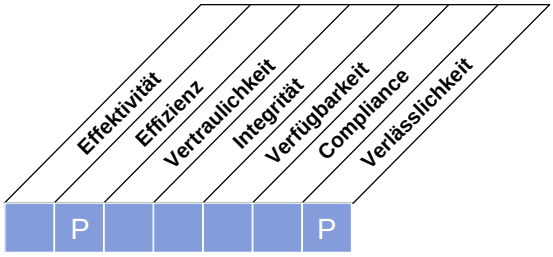
5 Optimised (optimiert):
Die IT-Sicherheit liegt im gemeinsamen Verantwortungsbereich der Fachbereiche und der IT und ist in die betrieblichen Sicherheitsziele integriert. Die IT-Sicherheitsanforderungen sind klar festgehalten, optimiert und in einem genehmigten Sicherheitsplan enthalten. Die Anwender und Kunden sind vermehrt verantwortlich für die Festlegung von Sicherheitsanforderungen und Sicherheitsfunktionen werden in die Anwendungen in der Entwurfsphase integriert. Auf Security Incidents wird umgehend mit formellen Verfahren und unterstützt durch automatisierte Werkzeuge reagiert. Periodische Sicherheitseinschätzungen werden durchgeführt, um die Wirksamkeit der Ausführung der Sicherheitsplanung auszuwerten. Die Informationen zu Bedrohungen und Verwundbarkeiten werden systematisch gesammelt und analysiert. Angemessene Controls zur Risikoverminderung werden sofort kommuniziert und implementiert. Die Sicherheitstests, die Ursachenanalyse der Security Incidents und die proaktive Identifikation von Risiken werden für kontinuierliche Prozessverbesserungen verwendet. Die Security Incidents und -technologien werden unternehmensweit eingegliedert. Die KGIs und KPIs für das Sicherheitsmanagement werden gesammelt und kommuniziert. Das Management verwendet die KGIs und KPIs, um die Sicherheitsplanung in einem kontinuierlichen Verbesserungsprozess anzugleichen.

Diese Seite wurde absichtlich freigelassen

HIGH-LEVEL CONTROL OBJECTIVE

DS6 Identify and Allocate Costs *(Identifiziere und verrechne Kosten)*

Die Notwendigkeit eines fairen und ausgeglichenen Systems zur Zuordnung von IT-Kosten an das Business erfordert die genaue Erhebung von IT-Kosten und eine Vereinbarung mit den Kerngeschäftsverantwortlichen über die faire Verrechnung. Dieser Prozess enthält den Aufbau und Betrieb eines Systems, mit dem IT-Kosten aufgezeichnet, zugeordnet und dem Nutzer der Dienstleistung berichtet werden. Ein faires System der Zuordnung ermöglicht dem Business, sachkundigere Entscheidungen zum Einsatz von IT-Services zu treffen.



Kontrolle über den IT-Prozess,

Identify and Allocate Costs (*Identifiziere und verrechne Kosten*)

der die Anforderung des Unternehmens an die IT bezüglich

der Transparenz und des Verstehens von IT-Kosten und der Verbesserung der Kosteneffizienz durch gut unterrichtete Verwendung von IT-Services

durch die Konzentration auf

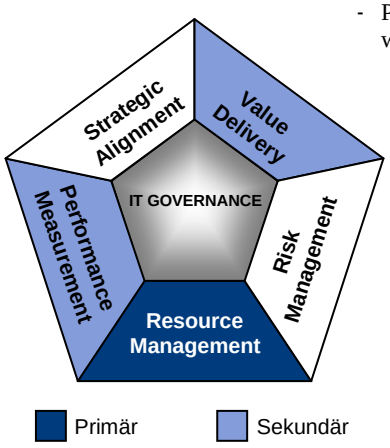
die vollständige und genaue Erfassung der IT-Kosten, ein mit den Kerngeschäftsverantwortlichen vereinbartes, faires Verrechnungssystem und ein System für die rechtzeitige Berichterstattung der IT-Nutzung und -Kosten zufrieden stellt,

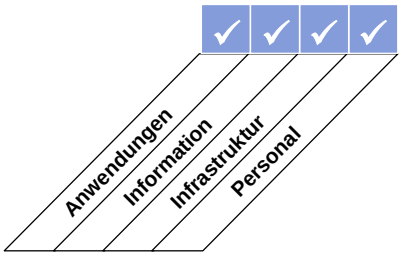
wird erreicht durch

- Anpassung der Belastungen an die Qualität und Quantität der angebotenen Services Gestaltung und Vereinbarung eines vollständigen Kostenmodells
- Implementierung der Belastungen gemäß der vereinbarten Policy

und gemessen durch

- Prozent der von der Geschäftsführung akzeptierten/bezahlten IT-Service Rechnungen
- Prozent der Abweichung zwischen Budget, prognostizierten und aktuellen Kosten
- Prozent der IT-Gesamtkosten, die nach den vereinbarten Kostenmodellen verrechnet werden





DETAILLIERTE CONTROL OBJECTIVES

DS6 Identify and Allocate Costs *(Identifiziere und verrechne Kosten)*

DS6.1 Definition of services (Definition von Services)
Identifiziere alle IT-Kosten und lege sie auf die IT-Services um, um ein transparentes Kostenmodell zu unterstützen. IT-Services sollten mit Geschäftsprozessen verbunden werden, so dass das Kerngeschäft die jeweiligen Service-Rechnungsgrössen genau bestimmen kann.

DS6.2 IT accounting (IT-Rechnungswesen)
Zeichne die Istkosten auf und weise diese entsprechend dem definierten Kostenmodell zu. Abweichungen zwischen Plan- und Istkosten sollten, entsprechend den unternehmensweiten Systemen zur Messung von Finanzzahlen, analysiert und berichtet werden.

DS6.3 Cost modelling and charging (Kostenmodellierung und -verrechnung)
Lege – basierend auf den definierten Services – ein Kostenmodell fest, das direkte, indirekte und Gemeinkosten (engl.: *overhead*) für Services berücksichtigt und das die Berechnung von Verrechnungssätzen je Service unterstützt. Das Kostenmodell sollte mit den unternehmensweiten Kostenrechnungsverfahren übereinstimmen. Das IT-Kostenmodell sollte sicherstellen, dass die Verrechnung von Services für User nachvollziehbar, messbar und vorhersehbar ist, um einen angemessenen Gebrauch der Ressourcen zu unterstützen. Das Fachbereichsmanagement sollte in der Lage sein, die tatsächliche Verwendung und Verrechnung der Services zu verifizieren.

DS6.4 Cost Model Maintenance (Wartung des Kostenmodells)
Überprüfe und benchmarke die Angemessenheit des Kosten(verrechnungs)modells regelmäßig, um dessen Sachlichkeit und Angemessenheit entsprechend der sich entwickelnden Unternehmens- und IT-Aktivitäten zu erhalten.

MANAGEMENT GUIDELINES

DS6 Identify and Allocate Costs *(Identifiziere und verrechne Kosten)*

Von	Inputs
PO4	Dokumentierte Systemeigner
PO5	Kosten-/Nutzenberichte; IT-Budgets
PO10	Detaillierte Projektpläne
DS1	SLAs und OLAs

Outputs	Nach
IT-Finanzen	PO5
Berichte über Prozessperformance	ME1

RACI-CHART*

Aktivitäten / Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Mappe die IT-Infrastruktur auf die bereitgestellten Services/unterstützten Geschäftsprozesse		C	C	A	C	C	C	C	R	C	
Identifiziere alle IT-Kosten (Personen, Technologie, etc.) und bilde sie auf die IT-Services auf Basis der Stückkosten ab		C		A		C	C	C	R	C	
Etabliere und unterhalte einen IT-Rechnungswesen- und -Kostenkontrollprozess		C	C	A	C	C	C	C	R	C	
Etabliere und unterhalte Kosten-Policies und -Verfahren		C	C	A	C	C	C	C	R	C	

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Review der verrechneten Kosten durch die Geschäftsführung
- Anpassung der Kosten an die Qualität der bereitgestellten Services
- Gestaltung und Vereinbarung eines vollständigen Kostenmodells
- Implementierung der Kosten, wie in der Policy vereinbart
- Regelmäßiges Benchmarking der Kosten

treiben

Prozessziele

- Entwickle eine faire und ausgeglichene Definition von IT-Kosten und Services
- Erfasse die Kosten von IT-Services genau
- Verrechne den Nutzern die IT-Kosten von IT-Services fair und ausgeglichen

treiben

IT-Ziele

- Stelle Transparenz der und Verständnis von IT-Kosten, Nutzen, Strategie, Richtlinien und Service Levels sicher
- Verbessere die Kosteneffizienz der IT und ihren Beitrag zum Unternehmenserfolg
- Stelle sicher, dass die IT kosteneffiziente Servicequalität, eine kontinuierliche Verbesserung und Bereitschaft für zukünftige Veränderungen zeigt

werden gemessen durch

Key Performance Indicators

- % der Kerngeschäftverantwortlichen, die in die Bestimmung des Kostenmodells involviert waren
- Häufigkeit der Überprüfung des Kostenverrechnungsmodells
- % der Kosten, die automatisch/manuell verrechnet wurden

werden gemessen durch

Key Goal Indicators

- % der Abweichung zwischen Budget, prognostizierten und aktuellen Kosten
- % der IT-Gesamtkosten, die nach dem vereinbarten Kostenmodell verrechnet wurden
- % der vom Fachbereich bestrittenen Kosten

werden gemessen durch

IT Key Goal Indicators

- % der von der Geschäftsführung akzeptierten/bezahlten IT-Service-Rechnungen
- Zeitliche Entwicklung der Stückkosten pro Service
- Zufriedenheit im Unternehmen (Umfrage) mit dem IT-Services-Kostenmodell

MATURITY MODEL

DS6 Identify and Allocate Costs *(Identifiziere und verrechne Kosten)*

Die Reife des Management des Prozesses *Identify and Allocate Costs (Identifiziere und verrechne Kosten)* der die Geschäftsanforderungen an die IT erfüllt der Transparenz und des Verstehens von IT-Kosten und der Verbesserung der Kosteneffizienz durch gut unterrichtete Verwendung von IT-Services ist:

0 Non-existent (nicht existent):
Ein erkennbarer Prozess zur Identifikation und Zuordnung der Kosten für erbrachte Informationsdienste fehlt vollständig. Das Unternehmen hat noch nicht einmal erkannt, dass im Zusammenhang mit dem betrieblichen Rechnungswesen eine Problemstellung existiert, und eine Kommunikation darüber ist nicht vorhanden.

1 Initial (initial):
Ein allgemeines Verständnis für die gesamten Kosten der Informationsdienste existiert, aber eine Aufteilung nach Anwender, Kunde, Abteilung, Anwendergruppe, Betriebsfunktion, Projekt oder gelieferten Ergebnissen ist nicht vorhanden. Es erfolgt praktisch keine Kostenüberwachung und nur mit einer zusammenfassenden Management-Berichterstattung. IT-Kosten werden als betriebliche Gemeinkosten zugewiesen. Der Geschäftsbereich erhält keinerlei Informationen über Kosten oder Nutzen der Leistungserbringung

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Es besteht ein grundlegendes Bewusstsein für den Bedarf der Identifikation und Zuordnung von Kosten. Die Kostenzuordnung basiert auf informellen und rudimentären Kostenannahmen, z.B. Hardware-Kosten, und eine Verbindung zu Werttreibern ist nahezu nicht vorhanden. Die Prozesse für die Kostenzuordnung sind wiederholbar. Formelle Schulungen oder Kommunikation über Standardverfahren zur Kostenidentifikation und -zuordnung sind nicht vorhanden. Die Verantwortlichkeiten für die Erfassung oder Zuordnung von Kosten sind nicht festgelegt.

3 Defined (definiert):
Ein definiertes und dokumentiertes Kostenmodell für Informationsdienste ist vorhanden. Ein Prozess für die Zuordnung von IT-Kosten zu den für die Anwender erbrachten Diensten wurde festgelegt. Ein angemessener Kenntnisstand für die den Informationsdiensten zurechenbaren Kosten existiert. Die Fachbereiche werden mit rudimentären Informationen über die Kosten versorgt.

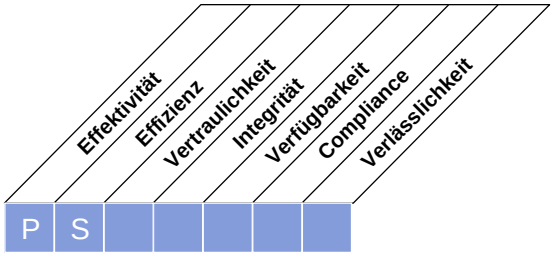
4 Managed and measurable (gemanaged und messbar):
Die Aufgaben und Verantwortlichkeiten für das Kostenmanagement für Informationsdienste sind definiert, werden auf allen Ebenen vollständig verstanden und werden durch formelle Schulungen unterstützt. Direkte und indirekte Kosten werden identifiziert sowie rechtzeitig und automatisiert an das Management, die Geschäftsprozesseigner und die Anwender berichtet. Im Allgemeinen existieren Kostenüberwachung und -überprüfung, und Maßnahmen werden ergriffen, wenn Kostenabweichungen erkannt werden. Die Berichterstattung zu den Kosten der Informationsdienste ist mit den betrieblichen Zielen und den Service Level Agreements eng verbunden und wird durch die Geschäftsprozesseigner überwacht. Die Angemessenheit des Prozesses zur Kostenzuordnung wird durch einen Finanzbereich überprüft. Ein automatisiertes System zur betrieblichen Rechnungslegung ist zwar vorhanden, fokussiert jedoch eher den Funktionsbereich für Informationsdienste und weniger die Geschäftsprozesse. Die KPIs und KGIs für Kostenmessungen wurden festgelegt, werden aber inkonsistent gemessen.

5 Optimised (optimiert):
Die Kosten der bereitgestellten Dienste werden identifiziert, gesammelt, zusammengefasst und an das Management sowie die Geschäftsprozesseigner und Anwender berichtet. Die Kosten werden als anrechenbare Buchungsposten identifiziert und könnten ein Ausgleichsbuchungssystem unterstützen, welches den Anwendern die erbrachten Leistungen, basierend auf der Auslastung, angemessen in Rechnung stellt. Die Kostendetails unterstützen die Service Level Agreements. Die Überwachung und Bewertung der Kosten für Leistungen werden für die Optimierung der Kosten von IT-Ressourcen verwendet. Die erhaltenen Kostenkennzahlen werden zur Verifikation der Realisierung des Nutzens eingesetzt und in den Budgetierungsprozess des Unternehmens einbezogen. Die Berichterstattung zu den Kosten für Informationsdienste liefert durch intelligente Berichterstattungs-Systeme frühzeitige Warnungen für sich ändernde betriebliche Anforderungen. Ein variables Kostenmodell wird eingesetzt, welches aus den verarbeiteten Volumen jeder erbrachten Leistung abgeleitet wird. Das Kostenmanagement wurde auf das Level der Industriepraktiken verfeinert, basierend auf dem Ergebnis kontinuierlicher Verbesserung und dem Leistungsvergleich mit anderen Unternehmen. Die Optimierung von Kosten ist ein permanenter Prozess. Das Management überprüft die KPIs und KGIs im Rahmen eines laufenden Verbesserungsprozesses bei der Umgestaltung der Systeme zur Kostenmessung.

HIGH-LEVEL CONTROL OBJECTIVE

DS7 Educate and Train Users *(Schule und trainiere User)*

Die wirksame Schulung aller Benutzer von IT-Systemen, inklusive jenen innerhalb der IT, erfordert die Identifikation des Schulungsbedarfs für jede Benutzergruppe. Zusätzlich umfasst dieser Prozess die Festlegung und Umsetzung einer Strategie für wirksame Schulungen und die Messung der Ergebnisse. Ein wirksames Ausbildungsprogramm verbessert die wirkungsvolle Nutzung von Technologie durch die Reduktion von Anwenderfehlern, die Erhöhung der Produktivität und eine erhöhte Compliance mit wesentlichen Controls, wie benutzerbezogene Sicherheitsmaßnahmen.



Kontrolle über den IT-Prozess,

Educate and Train Users (*Schule und trainiere User*)

der die Anforderung des Unternehmens an die IT bezüglich

einer wirksamen und wirtschaftlichen Verwendung von Anwendungen und Technologielösungen und der Einhaltung der Richtlinien und Verfahren durch die Benutzer

durch die Konzentration auf

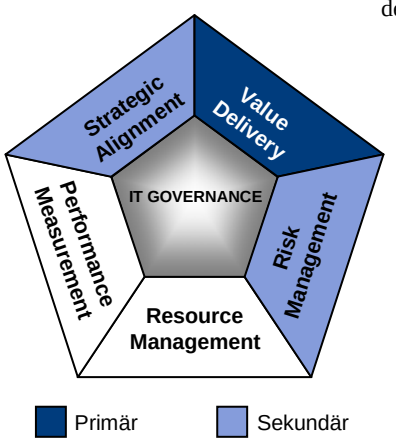
ein klares Verständnis in Bezug auf den Schulungsbedarf von IT-Benutzern, die Anwendung einer wirksamen Schulungsstrategie und das Messen der Ergebnisse zufrieden stellt,

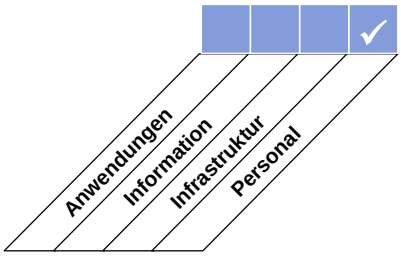
wird erreicht durch

- Erstellung eines Schulungsplans
- Organisation von Schulungen
  Abhalten von Schulungen
- Überwachung der und Berichterstattung über die Wirksamkeit der Schulungen

und gemessen durch

- Anzahl der Service Desk Calls aufgrund fehlender Benutzerschulung
- Prozent der Zufriedenheit der Stakeholder mit den angebotenen Schulungen
- Zeitspanne zwischen der Identifikation eines Schulungsbedarfs und dem Abhalten der Schulung





DETAILLIERTE CONTROL OBJECTIVES

DS7 Educate and Train Users *(Schule und trainiere User)*

DS7.1 Identification of education and training needs (Identifikation von Schulungs- und Trainingsbedarf)
Entwickle und aktualisiere regelmäßig ein Curriculum für alle Zielgruppen von Mitarbeiter unter Berücksichtigung von:

- Derzeitige und künftige Unternehmenserfordernisse und -strategie
- Unternehmensweite Werte (ethische Werte, Control, Sicherheitskultur, etc)
- Einführung neuer IT-Infrastruktur und Software (Pakete und Anwendungen)
- Derzeitige Fertigkeiten, Kompetenzprofile, Bedarf an Zertifizierung und/oder Berechtigungsnachweisen
- Schulungsmethoden (zB Klassenraum, Web-basierend), Größe der Zielgruppe, Erreichbarkeit und Zeitvorgaben

DS7.2 Delivery of training and education (Abhaltung von Trainings und Schulungen)
Identifiziere, basierend auf dem festgestellten Schulungs- und Trainingsbedarf, Zielgruppen und deren Mitglieder, wirksame Schulungsmethoden, Lehrkräfte, Trainer und Mentoren. Ernenne Trainer und organisiere zeitgerecht Schulungseinheiten. Anmeldung (inklusive Voraussetzungen), Teilnahme und Leistungsbewertungen sollten festgehalten werden.

DS7.3 Evaluation of training received (Evaluierung von besuchten Trainings)
Beurteile die Vermittlung der Schulungs- und Trainingsinhalte nach dem Abschluss hinsichtlich Relevanz, Qualität, Wirksamkeit, Erfassen und Behalten des Wissens, Kosten und Nutzen. Die Ergebnisse dieser Beurteilung sollten als Input für die künftige Festlegung von Curricula und Trainingseinheiten dienen.

MANAGEMENT GUIDELINES

DS7 Educate and Train Users *(Schule und trainiere User)*

Von	Inputs
PO7	Skills und Fertigkeiten von Benutzern, inkl. individuellem Training; Spezifische Trainingsanforderungen
AI4	Schulungsmaterialien; Erforderlicher Knowledge-Transfer für die Umsetzung von Lösungen
DS1	OLAs
DS5	Spezifische Schulungserfordernisse für Sicherheitsbewusstsein
DS8	Berichte über Benutzerzufriedenheit

Outputs	Nach
Berichte über Prozessperformance	ME1
Erforderliche Updates der Dokumentationen	AI4

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security	Training Department
Identifiziere und charakterisiere den Schulungsbedarf der BenutzerInnen			C	A	R	C	C	C	C	C	C	C
Erstelle ein Schulungsprogramm			C	A	R	C	I	C	C	C	I	R
Führe Awareness-, Ausbildungs- und Schulungsaktivitäten durch			I	A	C	C	I	C	C	C	I	R
Führe eine Schulungsevaluation durch			I	A	R	C	I	C	C	C	I	R
Identifiziere und evaluiere die besten Schulungsmethoden und -werkzeuge			I	A/R	R	C	C	C	C	C	C	R

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Erstellung eines Schulungsplans
- Organisation von Schulungen
- Abhalten von Schulungen
- Überwachung von und Berichterstattung über die Wirksamkeit von Schulungen

treiben

Prozessziele

- Erstelle ein Schulungsprogramm für die Benutzer aller Ebenen unter Verwendung der kostenwirksamsten Methode
- Übertrage Wissen an die Benutzer der Anwendungen und Technologielösungen
- Erhöhe das Bewusstsein für Risiken und Verantwortlichkeiten in Zusammenhang mit der Verwendung von Anwendungen und Technologielösungen

treiben

IT-Ziele

- Stelle die Enduser-Zufriedenheit mit den Serviceangeboten und Service Levels sicher
- Stelle die angemessene Verwendung und Performance der Anwendungen und technischen Lösungen sicher
- Optimiere IT-Infrastruktur, Ressourcen und Fähigkeiten

werden gemessen durch

Key Performance Indicators

- Häufigkeit der Aktualisierungen des Schulungsplans
- Zeitspanne zwischen der Identifikation eines Schulungsbedarfs und dem Abhalten der Schulung

werden gemessen durch

Key Goal Indicators

- Anzahl der Service Desk Calls für Schulungen oder zur Beantwortung von Fragen
- % der Zufriedenheit der Interessensvertreter mit den angebotenen Schulungen
- % der geschulten Mitarbeiter

werden gemessen durch

IT Key Goal Indicators

- Gemessene Verbesserung der Mitarbeiterproduktivität als Ergebnis eines besseren Verständnisses der Systeme
- Erhöhte Benutzerzufriedenheit mit der Einführung von Services, Systemen oder neuen Technologien

MATURITY MODEL

DS7 Educate and Train Users *(Schule und trainiere User)*

Die Reife des Management des Prozesses *Educate and Train Users (Schule und trainiere User)*, der die Geschäftsanforderungen an die IT erfüllt einer wirksamen und wirtschaftlichen Verwendungen von Anwendungen und Technologielösungen und der Einhaltung der Richtlinien und Verfahren durch die Benutzer, ist:

0 Non-existent (nicht existent):
Ausbildungs- und Schulungsprogramme fehlen vollständig. Das Unternehmen hat noch nicht einmal erkannt, dass im Zusammenhang mit Schulungen eine Problemstellung existiert, und eine Kommunikation darüber ist nicht vorhanden.

1 Initial (initial):
Anzeichen, dass das Unternehmen die Notwendigkeit für Ausbildungs- und Schulungsprogramme erkannt hat, sind vorhanden, aber standardisierte Prozesse existieren nicht. Auf Grund des Fehlens an organisierten Programmen haben die Mitarber die Schulungen eigenmächtig ermittelt und an ihnen teilgenommen. Einige dieser Schulungen bezogen sich auf ethisches Verhalten, Bewusstsein zur Systemsicherheit und Sicherheitspraktiken. Dem allgemeinen Managementansatz fehlt jeglicher Zusammenhang und nur sporadische und inkonsistente Kommunikation über Fragen und Ansätze zu Ausbildungen und Schulungen ist vorhanden.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Es besteht innerhalb des Unternehmens ein Bewusstsein für die Notwendigkeit von Ausbildungs- und Schulungsprogrammen und für die damit verbundenen Prozesse. Die Schulungen werden vermehrt in den individuellen Performanceplanungen der Mitarber identifiziert. Die Prozesse wurden auf eine Stufe entwickelt, wo informelle Ausbildungs- und Schulungseinheiten durch unterschiedliche Referenten unterrichtet werden, welche denselben Lehrstoff durch verschiedene Ansätzen abdecken. Einige dieser Schulungen beziehen sich auf ethisches Verhalten sowie das Bewusstsein und die Praktiken der Systemsicherheit. Das Vertrauen in das Wissen von Einzelpersonen ist hoch. Allerdings existiert eine widerspruchsfreie Kommunikation über die allgemeinen Fragen und die Notwendigkeit, diese anzugehen.

3 Defined (definiert):
Das Ausbildungs- und Schulungsprogramm wurde institutionalisiert und kommuniziert und die Mitarber und Manager identifizieren und dokumentieren den Schulungsbedarf. Die Ausbildungs- und Schulungsprozesse wurden standardisiert und dokumentiert. Die Budgets, Ressourcen, Einrichtungen und Referenten wurden festgelegt, um das Ausbildungs- und Schulungsprogramm zu unterstützen. Formelle Schulungseinheiten über ethisches Verhalten sowie Bewusstsein und Praktiken zur Systemsicherheit werden den Mitarber vermittelt. Die meisten Ausbildungs- und Schulungsverfahren werden überwacht, aber wahrscheinlich werden nicht alle Abweichungen vom Management entdeckt. Analysen von Ausbildungs- und Schulungsproblemen werden nur gelegentlich durchgeführt.

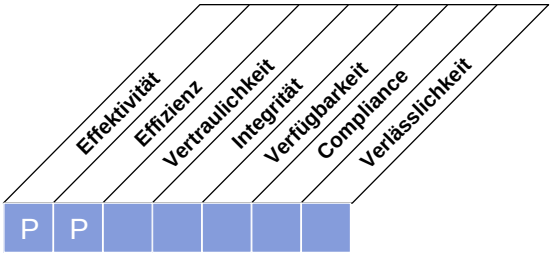
4 Managed and measurable (gemanaged und messbar):
Ein umfassendes Ausbildungs- und Schulungsprogramm, das messbare Ergebnisse liefert, ist vorhanden. Die Verantwortlichkeiten sind klar und die Prozesseigentümerschaft wurde festgelegt. Ausbildung und Schulung sind Bestandteile der beruflichen Laufbahn der Mitarbeiter. Das Management unterstützt und besucht Ausbildungs- und Schulungsveranstaltungen. Alle Mitarber erhalten Schulungen in ethischem Verhalten und Sicherheitsbewusstsein. Alle Mitarber erhalten das geeignete Maß an Schulungen über Systemsicherheitspraktiken für den Schutz vor Schäden durch Ausfälle, welche die Verfügbarkeit, Vertraulichkeit oder Integrität beeinträchtigen. Das Management überwacht die Einhaltung durch konstante Überprüfung und Aktualisierung der Ausbildungs- und Schulungsprogramme und -prozesse. Prozesse werden optimiert und erzwingen beste interne Praktiken.

5 Optimised (optimiert):
Die Ausbildungen und Schulungen verbessern die individuellen Leistungen. Die Ausbildungen und Schulungen sind entscheidende Komponenten der beruflichen Laufbahn der Mitarbeiter. Ausreichende Budgets, Ressourcen, Einrichtungen und Referenten werden für die Ausbildungs- und Schulungsprogramme bereitgestellt. Prozesse wurden verfeinert und werden kontinuierlich verbessert, indem die Vorteile der besten externen Praktiken und der Reifegrade-Modellierung mit anderen Unternehmen genutzt werden. Alle Probleme und Abweichungen werden nach ihrer Grundursache analysiert und wirksame Maßnahmen werden zweckdienlich identifiziert und getroffen. Eine positive Einstellung zu ethischem Verhalten und Grundsätzen der Systemsicherheit ist vorhanden. Die IT wird umfangreich, integriert und optimiert eingesetzt, um Werkzeuge für die Ausbildungs- und Schulungsprogramme zu automatisieren und bereitzustellen. Externe Trainingsexperten werden zum Vorteil eingesetzt und Benchmarks zur Anleitung verwendet.

HIGH-LEVEL CONTROL OBJECTIVE

DS8 Manage Service Desk and Incidents *(Manage den Service Desk und Incidents)*

Die rechtzeitige und wirksame Beantwortung von Anfragen und Problemen von IT-Anwendern erfordert einen gut konzipierten und umgesetzten Service Desk- sowie Incident-Management-Prozess. Dieser Prozess umfasst die Etablierung einer Service Desk-Funktion mit Entgegennahme, Incident-Eskalation, Trend- und Ursachenanalyse sowie Lösung. Der Nutzen für das Kerngeschäft beinhaltet eine erhöhte Produktivität durch die rasche Lösung von Benutzeranfragen. Darüber hinaus kann das Business die Grundursachen (zB dürftige Benutzerschulungen) durch eine wirksame Berichterstattung angehen.



Kontrolle über den IT-Prozess,

Manage Service Desk and Incidents (*Manage den Service Desk und Incidents*)

der die Anforderung des Unternehmens an die IT bezüglich

der Ermöglichung einer wirksamen Verwendung der IT-Systeme durch die Sicherstellung der Lösung und Analyse von Endbenutzer-Anfragen, Fragen und Incidents

durch die Konzentration auf

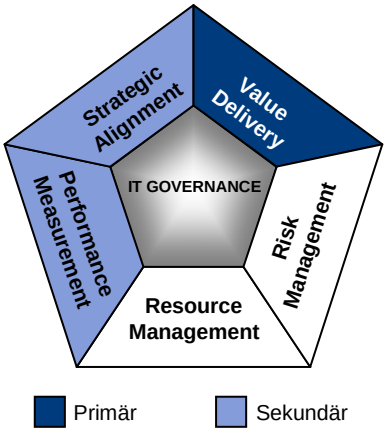
e eine professionelle Service Desk-Funktion mit rascher Reaktion, klaren Eskalationsverfahren und Lösungs- und Trendanalysen zufrieden stellt,

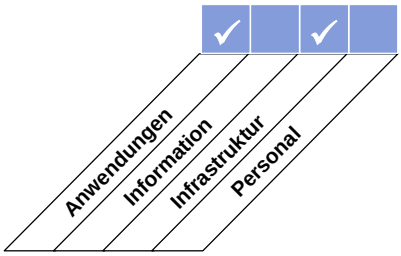
wird erreicht durch

- Installation und Betrieb eines Service Desks
- Überwachung und Berichterstattung von Trends
- Festlegung klarer Eskalationskriterien und -verfahren

und gemessen durch

- Benutzerzufriedenheit mit dem ersten Support(kontakt)
- Prozent der innerhalb der vereinbarten/akzeptablen Zeitspanne gelösten Ereignisse
- Anteil der abgebrochenen Calls





DETAILLIERTE CONTROL OBJECTIVES

DS8 Manage Service Desk and Incidents *(Manage den Service Desk und Incidents)*

DS8.1 Service Desk (Service Desk)
Richte eine Service Desk-Funktion als Schnittstelle von Usern zur IT, zur Aufnahme, Kommunikation, Weitergabe und Analyse aller Anrufe, gemeldeten Incidents, Service- und Informationsanfragen ein. Basierend auf den vereinbarten Service Levels gemäß dem geeigneten SLA sollten Verfahren für die Überwachung und die Eskalation umgesetzt werden, welche die Klassifikation und Priorisierung aller gemeldeten Vorfälle als Incident, Serviceanfrage oder Informationsanfrage erlauben. Messe die Zufriedenheit des Endbenutzers mit der Qualität des Service Desk und der IT-Services.

DS8.2 Registration of customer queries (Registrierung von Kundenanfragen)
Etabliere eine Funktion und ein System zur Aufzeichnung und Verfolgung von Anrufen, Incidents, Serviceanfragen und Informationsbedürfnissen. Es sollte in Prozesse wie Incident-Management, Problem-Management, Change-Management, Kapazitäts- und Verfügbarkeitsmanagement eng eingebunden sein. Incidentssollten entsprechend einer Geschäfts- und Service-Priorität klassifiziert und dem geeigneten Team zur Problembehandlung übergeben werden und die Kunden sollten über den Status ihrer Anfragen informiert bleiben.

DS8.3 Incident escalation (Eskalation von Incidents)
Erstelle Verfahren für den Service Desk, so dass nicht sofort lösbare Incidentsangemessen, entsprechend den in den SLAs definierten Grenzen eskaliert, und – wo anwendbar – entsprechende Workarounds angeboten werden. Stelle sicher, dass die Eigentümerschaft von Incidentsund deren Überwachung während des gesamten Lebenszyklus der durch Benutzer initiierten Incidentsbeim Service Desk verbleibt, unabhängig davon, welche Gruppe der IT an der Lösung arbeitet.

DS8.4 Incident closure (Schließen von Incidents)
Erstelle Verfahren für das zeitnahe Monitoring der Erledigung von Kundenanfragen. Wenn ein Incidentgelöst wird, sollte der Service Desk die zugrunde liegende Ursache (falls bekannt) aufzeichnen und bestätigen, dass die getroffene Handlung vom Kunden akzeptiert wurde.

DS8.5 Trend analysis (Trendanalyse)
Erstelle Berichte der Aktivitäten des Service Desks, um dem Management zu ermöglichen, die Leistungserbringung und Antwortzeiten zu messen und Trends oder wiederkehrende Probleme zu identifizieren, so dass das Service kontinuierlich verbessert werden kann.

MANAGEMENT GUIDELINES

DS8 Manage Service Desk and Incidents *(Manage den Service Desk und Incidents)*

Von	Inputs
AI4	Benutzer-, Betriebs-, Support-, technische und administrative Handbücher
AI6	Freigabe von Changes
AI7	Configuration Items (Released)
DS1	SLAs und OLAs
DS4	Incident- und Katastrophen-Schwellwerte
DS5	Definition Security Incidents
DS9	Details zur IT-Konfiguration / Assets
DS10	Known Problems, Known Errors und Workarounds
DS13	Incident-Tickets

Outputs	Nach						
Service-Requests/Request for Change	AI6						
Berichte über Incidents	DS10						
Berichte über Prozessperformance	ME1						
Berichte über Benutzerzufriedenheit	DS7	ME1					

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security	Service Desk / Incident Manager
Erstelle Klassifikations- (Schweregrad und Auswirkung) und Eskalationsverfahren (funktional und hierarchisch)				C	C	C	C	C	C		C	A/R
Erkenne und erfasse Incidents / Serviceanfragen / Informationsanfragen												A/R
Klassifiziere, ermittle und diagnostiziere Anfragen				I		C	C	C			I	A/R
Behebe, löse und schließe Incidents					I	R	R	R			C	A/R
Informiere Benutzer (zB Statusaktualisierungen)				I	I							A/R
Erstelle Managementauswertungen	I			I	I	I			I		I	A/R

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Installation und Betrieb eines Service Desk
- Überwachung und Berichterstattung von Trends
- Abstimmung der Lösungsprioritäten von Ereignisse mit den Bedürfnissen der Geschäftstätigkeit
- Festlegung klarer Eskalationskriterien und -verfahren

treiben

Prozessziele

- Analysiere, dokumentiere und eskaliere Incidentszeitgerecht
- Reagiere auf Anfragen exakt und zeitgerecht
- Führe regelmäßig Trendanalysen der Incidentsund Anfragen durch

treiben

IT-Ziele

- Stelle die Enduser-Zufriedenheit mit Serviceangeboten und Service Levels sicher
- Stelle die angemessene Verwendung und Performance der Anwendungen und technischen Lösungen sicher
- Stelle die Verfügbarkeit der IT-Services gemäß den Anforderungen sicher

werden gemessen durch

Key Performance Indicators

- % der Ereignisse und Serviceanfragen, die reportet und mittels automatisierter Tools protokolliert wurden
- Anzahl der Schulungstage pro Service Desk MitarberInnen pro Jahr
- Anzahl der pro Service Desk MitarbeiterIn pro Stunde bearbeiteten Anrufe
- % der Ereignisse, die einen Vor-Ort-Support benötigen (Field Support, persönlicher Besuch)
- Rückstand nicht gelöster Anfragen

werden gemessen durch

Key Goal Indicators

- % der direkten Lösungen basierend auf der Gesamtzahl der Anfragen
- % der erneut geöffneten Incidents
- Anteil der abgebrochenen Calls
- Durchschnittliche Dauer der Incidentsnach Schweregrad
- Durchschnittliche Reaktionszeit auf Telefon- und E-Mail-/Web-Anfragen

werden gemessen durch

IT Key Goal Indicators

- Benutzerzufriedenheit mit dem Erst-Support (Service Desk oder Knowledge Base)
- % der innerhalb einer vereinbarten/akzeptablen Zeitspanne gelösten Incidents

MATURITY MODEL

DS8 Manage Service Desk and Incidents *(Manage den Service Desk und Incidents)*

Die Reife des Management des Prozesses *Manage Service Desk and Incidents (Manage den Service Desk und Incidents)*, der die Geschäftsanforderungen an die IT erfüllt der Ermöglichung einer wirksamen Verwendung der IT-Systeme durch die Sicherstellung der Lösung und Analyse von Endbenutzer-Anfragen, Fragen und Incident, ist:

0 Non-existent (nicht existent):
Es gibt keinen Support zur Lösung von Benutzerfragen und -problemen. Ein Prozess zum Incident-Management fehlt vollständig. Das Unternehmen hat nicht erkannt, dass ein Handlungsbedarf besteht.

1 Initial (initial):
Das Management erkennt, dass es eines durch Hilfsmittel und Personal unterstützten Prozesses bedarf, um auf Benutzeranfragen reagieren und die Incident-Lösung bewältigen zu können. Es gibt jedoch keinen standardisierten Prozess und ausschließlich ein reaktiver Support wird geboten. Es findet keine Überwachung von Benutzeranfragen, Incidentsoder Trends durch das Management statt. Es gibt keinen Eskalationsprozess, um die Lösung von Problemen sicherzustellen.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Das Unternehmen ist sich der Notwendigkeit einer Benutzerunterstützung und eines Incident-Management-Prozesses bewusst. Es wird eine formlose Unterstützung durch ein Netzwerk qualifizierter Mitarber bereitgestellt. Diese Mitarber verfügen über einige gängige Hilfsmittel zur Incident-Behebung. Es finden keine formalen Schulungen bzw keine Kommunikation bezüglich Standardverfahren statt und die Verantwortung liegt beim einzelnen Mitarbeiter.

3 Defined (definiert):
Die Notwendigkeit einer Benutzerunterstützung und eines Incident- Management-Prozesses wird anerkannt und akzeptiert. Verfahren wurden standardisiert und dokumentiert, und es findet eine formlose Schulung statt. Es bleibt jedoch dem Einzelnen überlassen, an Schulungen teilzunehmen und die Standards einzuhalten. Es wurden häufig gestellte Fragen (engl.: *FAQs*) und Benutzerrichtlinien aufgestellt, aber der einzelne Mitarber muss diese finden und ist nicht gezwungen, sie einzuhalten. Anfragen und Incidentswerden manuell nachverfolgt und individuell überwacht, aber es gibt keine formale Berichterstattung. Die rechtzeitige Reaktion auf Anfragen und Incidentswird nicht gemessen und es kann sein, dass Incidents ungelöst bleiben. Die Benutzer haben klare Anweisungen erhalten, wohin und wie Probleme und Incidentszu melden sind.

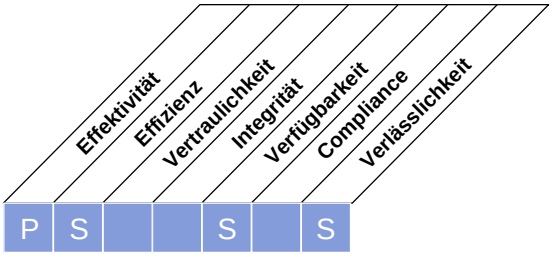
4 Managed and measurable (gemanaged und messbar):
Es besteht ein umfassendes Verständnis über den Nutzen eines Incident-Managment-Prozesses auf allen Ebenen des Unternehmens und die Benutzerunterstützung wurde in dafür geeigneten Unternehmenseinheiten eingerichtet. Werkzeuge und Techniken wurden mittels einer zentralisierten Wissensdatenbank automatisiert. Die Mitarbeiter des User-Support arbeiten eng mit den Mitarbeiter des Problemmeldewesens zusammen. Die Zuständigkeiten sind klar und die Wirksamkeit wird überwacht. Es wurden Verfahren zur Kommunikation, Eskalation und Lösung von Incidentsaufgestellt und kommuniziert. Die Mitarber der Benutzerunterstützung sind geschult und die Prozesse werden durch den Einsatz aufgabenspezifischer Software verbessert. Das Management hat KPIs und KGIs für die Leistung der Benutzerunterstützung entwickelt.

5 Optimised (optimiert):
Der Incident-Management-Prozess und der Service Desk sind eingeführt und gut organisiert und insofern auf den Kundenservice ausgerichtet, als sie über entsprechendes Know-how verfügen, kundenorientiert arbeiten und Hilfestellung leisten. KPIs und KGIs werden systematisch gemessen und weitergemeldet. Ausführliche, umfassende häufig gestellte Fragen (engl.: FAQs) sind integraler Bestandteil der Wissensdatenbank. Hilfsmittel ermöglichen Benutzer eine Selbstdiagnose und Incident-Lösung. Es wird eine konsistente Hilfe bereitgestellt und Incidentwerden im Rahmen eines strukturierten Eskalationsprozesses rasch gelöst. Das Management nutzt ein integriertes Tool für die Leistungsstatistik des Incident-Management-Prozesses und des Service Desks. Die Prozesse wurden auf das Niveau von gängigen Industrie-Praktiken entwickelt und basieren auf den Ergebnissen der Analysen von KPIs und KGIs, der kontinuierlichen Verbesserung und dem Vergleich mit anderen Unternehmen.

HIGH-LEVEL CONTROL OBJECTIVE

DS9 Manage the Configuration *(Manage die Konfiguration)*

Um die Integrität der Hard- und Softwarekonfiguration sicherzustellen, ist die Entwicklung und der Unterhalt eines Repository mit richtigen und vollständigen Konfigurationsinformationen erforderlich. Dieser Prozess umfasst die initiale Sammlung von Konfigurationsinformationen, die Erstellung einer Basis-/Referenzkonfiguration (engl.: *baseline*), die Verifikation und Überprüfung der Konfigurationsinformation sowie die Aktualisierung des Repository der Konfigurationsdaten bei Bedarf. Ein effektives Konfigurationsmanagement unterstützt eine höhere Systemverfügbarkeit, minimiert Fehler in der Produktion und löst Fragen (engl.: *issues*) schneller.



Kontrolle über den IT-Prozess,

Manage the Configuration (*Manage die Konfiguration*)

der die Anforderung des Unternehmens an die IT bezüglich

der Optimierung der IT-Infrastruktur, der Ressourcen und des Leistungspotentials und des Nachweises der IT Anlagen erfüllt

durch die Konzentration auf

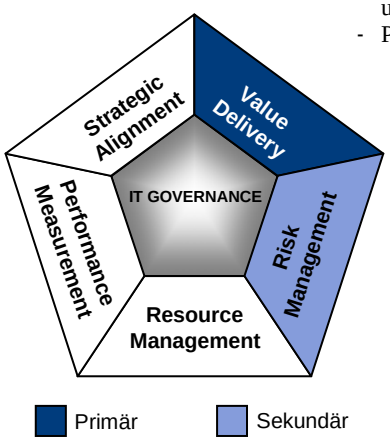
die Erstellung und den Unterhalt eines exakten und kompletten Repository der Konfigurationsattribute der Anlagen und Referenzversionen (engl.: *baselines*) und den Vergleich zur tatsächlichen Anlagenkonfiguration zufrieden stellt,

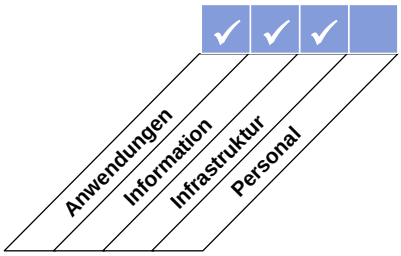
wird erreicht durch

- Erstellung eines zentralen Repository aller Configuration Items
- Identifikation und Unterhalt von Configuration Items
- Review der Integrität der Konfigurationsdaten

und gemessen durch

- Anzahl der Geschäfts-Compliance-Probleme, die durch nicht korrekte Konfiguration von Anlagen verursacht wurden
- Anzahl der festgestellten Abweichungen zwischen dem Konfigurations-Repository und den tatsächlichen Asset Konfigurationen
- Prozent der gekauften und im Repository nicht ausgewiesenen Lizenzen





DETAILLIERTE CONTROL OBJECTIVES

DS9 Manage the Configuration *(Manage die Konfiguration)*

DS9.1 Configuration repository and baseline (Konfigurationsinformation und Referenzversionen)
Erstelle eine zentrale Sammlung (engl.: *repository*) aller relevanten Informationen über Configuration Items. Dieses Repository umfasst Hardware, Anwendungssoftware, Middleware, Parameter, Dokumentation, Verfahren und Werkzeuge für Betrieb, Zugriff und Verwendung der Systeme und Services. Berücksichtigt werden sollten Informationen wie Benennung, Versionsnummern und Lizenzierungsdetails. Eine Referenzversion der Configuration Items sollte für jedes System und alle Services aufbewahrt werden, um nach Changes wieder dazu zurückkehren zu können.

DS9.2 Identification and maintenance of configuration items (Identifikation und Wartung von Configuration Items)
Erstelle Verfahren für:

- Identifikation von Configuration Items und deren Attribute
- Aufzeichnung neuer, modifizierter und gelöschter Configuration Items
- Identifikation und Wartung der Beziehungen zwischen Configuration Items im Configuration Repository
- Update bestehender Configuration Items im Konfigurations-Repository
- Verhinderung der Berücksichtigung nichtautorisierter Software

Diese Verfahren sollten eine angemessene Autorisierung und Aufzeichnung aller Aktionen am Konfigurations-Repository ermöglichen und in die Verfahren des Change-Management und Problem-Management integriert sein.

DS9.3 Configuration integrity review (Review der Integrität der Konfiguration)
Überprüfe und verifiziere regelmäßig, wo notwendig unter Verwendung von entsprechenden Werkzeugen, den Status der Configuration Items, um die Integrität der derzeitigen und historischen Konfigurationsdaten zu bestätigen und mit der effektiven Situation zu vergleichen. Überprüfe periodisch anhand der Policy für die Verwendung von Software die Existenz von privater oder nichtlizenzierter Software oder anderer Software, die gültigen Lizenzvereinbarungen widerspricht. Fehler und Abweichungen sollten berichtet, verfolgt und korrigiert werden.

MANAGEMENT GUIDELINES

DS9 Manage the Configuration *(Manage die Konfiguration)*

Von	Inputs
AI4	Benutzer-, Betriebs-, Support-, technische und administrative Handbücher
AI7	Configuration Items (Released)
DS4	Kritikalität von IT-Configuration Items

Outputs	Nach						
Details zur IT-Konfiguration / Assets	DS10	DS13	DS8				
Request for Change (wo und wie den Fix anwenden)	AI6						
Berichte über Prozessperformance	ME1						

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security	Configuration Manager
Entwickle Verfahren zur Planung des Konfigurationsmanagements					C	A	C	I	C		C	R
Sammle erste Konfigurationsinformationen und erstelle Referenzkonfigurationen						C	C	C			I	A/R
Verifiziere und prüfe Konfigurationsinformationen (einschließlich Nachweis von unerlaubter Software)						A			I		I	A/R
Aktualisiere das Konfigurations-Repository						R	R	R			I	A/R

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele
- Erstellung eines zentralen Repositorys aller Configuration Items
- Identifikation und Unterhalt von Configuration Items
- Review der Integrität der Konfigurationsdaten

werden gemessen durch

Key Performance Indicators
- Durchschnittliche Zeitspanne (Verzögerung) zwischen Identifikation einer Abweichung und deren Richtigstellung
- Anzahl der Abweichungen in Bezug auf unvollständige oder fehlende Konfigurationsinformation
- % der Configuration Items in Einklang mit den Service Levels für Performance, Sicherheit und Verfügbarkeit

treiben

Prozessziele
- Erstelle ein Repository aller Anlagen, Konfigurationsattribute und Referenz-konfigurationen
- Warte die Integrität des Konfigurations-Repository
- Überprüfe die tatsächlichen Anlagen-Konfigurationen hinsichtlich der Übereinstimmung mit den Referenzkonfigurationen im Repository

werden gemessen durch

Key Goal Indicators
- Anzahl der festgestellten Abweichungen zwischen dem Konfigurations-Repository und der tatsächlichen Anlagen-Konfiguration
- % der gekauften und im Repository nicht ausgewiesenen Lizenzen

treiben

IT-Ziele
- Optimiere IT-Infrastruktur, Ressourcen und Fähigkeiten
- Übernimm die Verantwortung für und schütze alle IT-Anlagen

werden gemessen durch

IT Key Goal Indicators
- Anzahl der Business Compliance Probleme verursacht durch nicht korrekte Konfiguration von Anlagen

MATURITY MODEL

DS9 Manage the Configuration *(Manage die Konfiguration)*

Die Reife des Management des Prozesses *Manage the Configuration (Manage die Konfiguration)*, der die Geschäftsanforderungen an die IT erfüllt der Optimierung der IT-Infrastruktur, der Ressourcen und Leistungspotentials und des Nachweises der IT-Anlagen ist:

0 Non-existent (nicht existent):
Das Management sieht weder bei Hardware- noch bei Software-Konfigurationen den Nutzen eines Prozesses zur Berichterstattung und zum Management der IT-Infrastruktur.

1 Initial (initial):
Die Notwendigkeit eines Konfigurationsmanagement wird anerkannt. Grundlegende Konfigurationsmanagement-Aufgaben wie die Pflege von Hardware- und Softwarebeständen werden auf einer individuellen Basis durchgeführt. Standardpraktiken sind nicht festgelegt.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Das Management ist sich der Notwendigkeit einer Kontrolle der IT-Konfiguration bewusst und versteht die Vorteile von präzisen und vollständigen Konfigurationsinformationen, aber man verlässt sich stillschweigend auf das Know-how und das Fachwissen des technischen Personals. Es werden zu einem gewissen Grad Konfigurationsmanagement-Hilfsmittel eingesetzt, die jedoch von Plattform zu Plattform unterschiedlich sind. Außerdem wurden keine Standard-Arbeitspraktiken festgelegt. Die Konfigurationsdaten-Inhalte sind begrenzt und werden nicht in verbundenen Prozessen wie dem Changes-Management und dem Incident-Management genutzt.

3 Defined (definiert):
Die Verfahren und Arbeitspraktiken wurden dokumentiert, standardisiert und kommuniziert, aber die Schulung und die Anwendung der Standards bleiben dem Einzelnen überlassen. Zusätzlich werden ähnliche Konfigurationsmanagement-Hilfsmittel plattformübergreifend implementiert. Verfahrensabweichungen werden in der Regel nicht entdeckt, und physische Überprüfungen werden nicht konsistent durchgeführt. Ein gewisser Grad an Automation dient der Nachverfolgung von Changes an der Ausstattung und der Software. Die Konfigurationsdaten werden in verbundenen Prozessen genutzt.

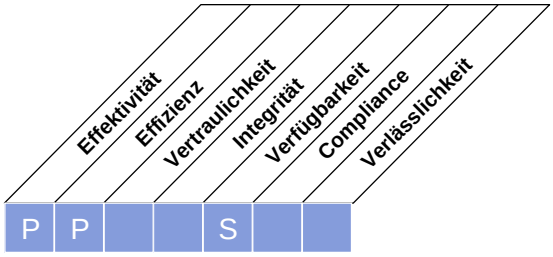
4 Managed and measurable (gemanaged und messbar):
Die Notwendigkeit des Konfigurationsmanagement wird auf allen Unternehmensebenen erkannt und es werden immer mehr gängige Praktiken entwickelt. Verfahren und Standards werden kommuniziert und in die Schulung einbezogen. Abweichungen werden überwacht, verfolgt und in Berichten festgehalten. Es werden automatisierte Hilfsmittel wie die automatische Informationsweitergabe (engl.: *push technology*) angewandt, um Standards durchzusetzen und die Stabilität zu verbessern. Die Konfigurationsmanagementsysteme decken einen Großteil der IT-Anlagen ab und ermöglichen eine korrekte Versionsverwaltung und Verteilungskontrolle. Die Analyse von Aussnahmen sowie physische Überprüfungen, werden einheitlich durchgeführt und ihre Grundursachen untersucht.

5 Optimised (optimiert):
Alle IT-Anlagen werden innerhalb eines zentralen Konfigurationsmanagementsystems verwaltet, das alle nötigen Informationen über Komponenten, ihre gegenseitigen Abhängigkeiten und Ereignisse enthält. Die Konfigurationsdaten stimmen mit den Herstellerangaben überein. Es gibt eine vollständige Integration der in gegenseitiger Beziehung stehenden Prozesse und diese nutzen und aktualisieren die Konfigurationsdaten automatisch. Referenzkonfigurations-Revisionsberichte stellen grundlegende Hardware- und Software-Daten zu Instandsetzung, Service, Garantie, Aktualisierung und technischer Beurteilung für jede einzelne Einheit bereit. Regeln zur Begrenzung der Installation nicht freigegebener Software werden umgesetzt. Das Management erstellt auf der Grundlage von Analyseberichten Instandsetzungs- und Aktualisierungsprognosen und stellt vorgesehene Upgrades und Kapazitäten zur technologischen Überarbeitung bereit. Die Aufzeichnung von Anlagen und die Überwachung einzelner IT-Anlagen schützen diese und beugen Diebstahl, unsachgemäßer Verwendung und Missbrauch vor.

HIGH-LEVEL CONTROL OBJECTIVE

DS10 Manage Problems *(Manage Probleme)*

Ein wirksames Problemm-Management erfordert die Identifikation und Klassifikation von Problemen, die Grundursachenanalyse (engl.: *root cause analysis*) und die Lösung von Problemen. Der Problem-Management-Prozess umfasst außerdem die Identifikation von Verbesserungsempfehlungen, die Verwaltung der Problemaufzeichnungen und die Überprüfung des Status von korrigierenden Maßnahmen. Ein wirksamer Problem-Management Prozess verbessert Service Levels, reduziert Kosten und verbessert den Komfort und die Zufriedenheit der Benutzer.



Kontrolle über den IT-Prozess,

Manage Problems (*Manage Probleme*)

der die Anforderung des Unternehmens an die IT bezüglich

der Sicherstellung der Zufriedenheit der Endbenutzer mit den Serviceangeboten und Service Levels, Reduktion der Mängel bei der Erbringung von Lösungen und Services und Reduktion der Nacharbeiten

durch die Konzentration auf

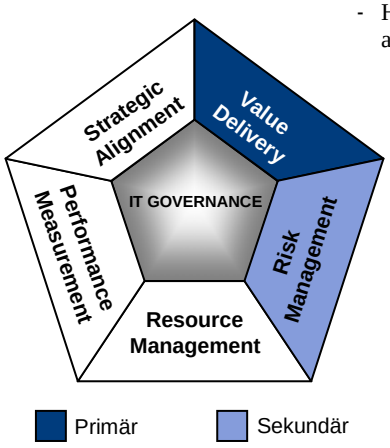
Aufzeichnung, Nachverfolgung und Lösung betrieblicher Probleme, Ermitteln der zugrunde liegenden Ursachen für alle signifikanten Probleme und Festlegung von Lösungen für identifizierte betriebliche Probleme zufrieden stellt,

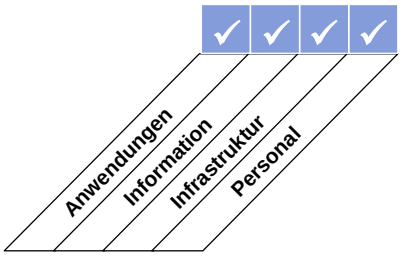
wird erreicht durch

- Durchführen von Analysen der Grundursachen für berichteten Probleme
- Trendanalysen
- Übernahme der Eigentümerschaft für Probleme und Vorantreiben der Lösung von Problemen

und gemessen durch

- Anzahl der wiederkehrenden Probleme mit Einfluss auf die Geschäftstätigkeit
- Prozentsatz der Probleme, die innerhalb des geforderten Zeitraums gelöst werden
- Häufigkeit der Berichte oder Aktualisierungen über laufende Probleme, basierend auf der Schwere der Probleme





DETAILLIERTE CONTROL OBJECTIVES

DS10 Manage Problems *(Manage Probleme)*

DS10.1 Identification and classification of problems (Identifikation und Klassifikation von Problemen)
Erstelle Prozesse zur Meldung und Klassifikation von Problemen, welche als Teil des Incident-Management identifiziert wurden. Die Schritte einer Problemklassifizierung sind ähnlich zu den Schritten für die Klassifizierung von Incidents; sie sollten Kategorie, Auswirkungen, Dringlichkeit und Priorität bestimmen. Probleme sollten sinnvoll in zusammenhängende Gruppen oder Domänen kategorisiert werden (zB Hardware, Software, unterstützende Software). Diese Gruppen können den organisatorischen Verantwortlichkeiten, dem User- oder dem Kundenkreis entsprechen und sind die Grundlage für die Zuweisung von Problemen an Support-Personal.

DS10.2 Problem tracking and resolution (Problemverfolgung und -lösung)
Das Problemmanagementsystem sollte angemessene Prüfspur-Aufzeichnungen bieten, welche die Nachverfolgung, Analyse und Bestimmung der zugrunde liegenden Ursache (engl.: *root cause*) aller gemeldeten Probleme ermöglichen, unter Beachtung von

- allen verbundenen Konfigurationselementen
- ungelösten Problemen und Ereignissen
- bekannten und vermuteten Fehlern

Identifiziere und initialisiere anhaltende Lösungen, welche die zu Grunde liegende Ursache angehen und Change-Requests an den etablierten Change-Management-Prozess stellen. Während des gesamten Lösungsprozesses sollte das Problem-Management regelmäßig vom Change-Management Berichte über den Fortschritt in der Lösung von Problemen und Fehlern erhalten. Das Problem-Management sollte die andauernden Auswirkungen von Problemen und bekannten Fehlern (engl.: *known errors*) auf die User Services erhalten. Für den Fall, dass die Auswirkungen wesentlich werden, sollte das Problem-Management das Problem eskalieren, allenfalls an ein entsprechendes Gremium verweisen, um die Priorität der Änderungsanfrage (engl.: *request for change = RFC*) zu erhöhen oder um – falls notwendig – einen dringenden Change zu implementieren. Der Fortschritt der Problemlösung sollte gegen das SLA gemonitort werden.

DS10.3 Problem closure (DS10.3 Abschluss von Problemen)
Setze ein Verfahren ein zum Abschluss von Problemaufzeichnungen entweder nach der Bestätigung einer erfolgreichen Beseitigung des bekannten Fehlers oder nach einer Übereinkunft mit dem Fachbereich, wie man das Problem alternativ lösen könnte.

DS10.4 Integration of change, configuration and problem management (Integration von Change-, Configuration- und Problem-Management)
Um ein wirksames Management von Problemen und Incidents sicherzustellen, integriere die in Beziehung stehenden Prozesse Change-, Configuration- und Problem-Management. Verfolge wie viel Aufwand in notfallartige Korrekturen an Stelle von Maßnahmen zur Verbesserung des Kerngeschäfts gesteckt wird, und verbessere diese Prozesse, um Probleme zu minimieren.

MANAGEMENT GUIDELINES

DS10 Manage Problems *(Manage Probleme)*

Von	Inputs
AI6	Freigabe von Changes
DS8	Berichte über Incidents
DS9	Details zur IT-Konfiguration / Assets
DS13	Fehler-Protokolle

Outputs	Nach
Request for Change	AI6
Problem-Aufzeichnungen	AI6
Berichte über Prozessperformance	ME1
Known Problems, Known Errors und Workarounds	DS8

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security	Problem Manager
Identifiziere und klassifiziere Probleme			I	I	C	A	C	C			I	R
Führe Analysen zur Ermittlung der zu Grunde liegenden Ursachen durch						C		C				A/R
Löse Probleme					C	A	R	R		R	C	C
Verfolge den Status von Problemen			I	I	C	A/R	C	C		C	C	R
Erarbeite Verbesserungsvorschläge und erstelle entsprechende Change Requests					I	A	I	I		I		R
Führe Aufzeichnungen über Probleme					I	I		I			I	A/R

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Ausstatten der Problem-Manager mit ausreichender Autorität
- Durchführen von Analysen zur Ermittelung der zugrunde liegenden Ursachen für alle berichteten Probleme
- Trendanalysen
- Übernahme der Eigentümerschaft für Probleme und Vorantreiben der Lösung von Problemen

werden gemessen durch

Key Performance Indicators

- Durchschnittliche Dauer zwischen der Erfassung eines Problems und der Identifizierung der zugrunde liegenden Ursache
- Prozentsatz der Probleme, für die eine Analyse der zugrunde liegenden Ursache gemacht wurde
- Häufigkeit der Berichte oder Aktualisierungen über laufende Probleme, basierend auf der Schwere der Probleme

treiben

Prozessziele

- Aufzeichnung und Nachverfolgung betrieblicher Probleme bis zur Lösung
- Ermittlung der zugrunde liegenden Ursachen für alle signifikanten Probleme
- Definition von Lösungen für identifizierte betriebliche Probleme

werden gemessen durch

Key Goal Indicators

- % der aufgezeichneten und nachverfolgten Probleme
- % der wiederkehrenden Probleme (innerhalb eines Zeitraums), geordnet nach deren Schwere
- % der Probleme, die innerhalb des geforderten Zeitraums gelöst werden
- Anzahl der offenen/neuen/geschlossenen Probleme, geordnet nach deren Schwere
- Mittelwert und Standardabweichung der Zeitspanne zwischen Identifizierung und Lösung von Problemen
- Mittelwert und Standardabweichung der Zeitspanne zwischen Lösung und Schließen von Problemen

treiben

IT-Ziele

- Stelle die Enduser-Zufriedenheit mit Serviceangeboten und Service Levels sicher
- Reduziere Mängel und Nacharbeit bei Lösungen und dem Servicebetrieb
- Schütze die Erreichung der IT-Ziele

werden gemessen durch

IT Key Goal Indicators

- Anzahl der wiederkehrenden Probleme mit Einfluss auf die Geschäftstätigkeit
- Anzahl der durch betriebliche Probleme hervorgerufenen Unterbrechungen der Geschäftstätigkeit

MATURITY MODEL

DS10 Manage Problems *(Manage Probleme)*

Die Reife des Management des Prozesses *Manage Problems (Manage Probleme)*, der die Geschäftsanforderungen an die IT erfüllt der Sicherstellung der Zufriedenheit der Endbenutzer mit den Serviceangeboten und Service Levels, Reduktion der Mänger bei der Erbringung von Lösungen und Services und Reduktion der Nacharbeiten ist:

0 Non-existent (nicht existent):
Es besteht kein Bewusstsein für die Notwendigkeit eines Problem-Managements, da zwischen Problemen und Ereignissen nicht unterschieden wird. Deshalb wird nicht versucht, die Grundursachen von Zwischenfällen zu identifizieren.

1 Initial (initial):
Einzelne Personen haben die Notwendigkeit zum Management von Problemen und der Klärung zugrunde liegender Ursachen erkannt. Qualifizierte Schlüssel-Mitarber bieten eine gewisse Unterstützung bei in ihr Fachgebiet fallenden Problemen an, aber die Verantwortlichkeit für das Problem-Management ist nicht zugewiesen. Informationen werden nicht weitergegeben, was zu zusätzlichen Problemen und einem Verlust an produktiver Zeit führt, während nach Antworten gesucht wird.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Sowohl die Geschäftseinheiten als auch die IT-Abteilung sind sich der Notwendigkeit und der Vorteile des Management von IT-bezogenen Problemen bewusst. Der Problemlösungsprozess wurde soweit entwickelt, dass einige Schlüssel-Mitarber für die Identifikation und Lösung von Problemen zuständig sind. Die Informationen werden formlos und reaktiv unter den Mitarber weitergegeben. Der Dienstleistungsgrad für die Benutzer variiert und wird dadurch gehemmt, dass dem zuständigen Problem-Manager nur unzureichend strukturiertes Wissen zur Verfügung steht.

3 Defined (definiert):
Die Notwendigkeit eines wirksamen integrierten Problemmeldewesens wird akzeptiert, was sich an der Bereitstellung entsprechender Managementunterstützung und Budgets für Personal und Schulung zeigt. Die Problemlösungs- und -eskalationsprozesse wurden standardisiert. Die Aufzeichnung und Nachverfolgung von Problemen und ihrer Lösungen erfolgen bruchstückhaft innerhalb des Problembearbeitungsteams, das die verfügbaren Hilfsmittel ohne Zentralisierung verwendet. Abweichungen von aufgestellten Normen oder Standards bleiben in der Regel unentdeckt. Die Informationen werden proaktiv und formell unter den Mitarber weitergegeben. Die Überprüfung der Zwischenfälle und der Analysen zur Problemidentifikation und -beseitigung durch die Führungskräfte ist begrenzt und formlos.

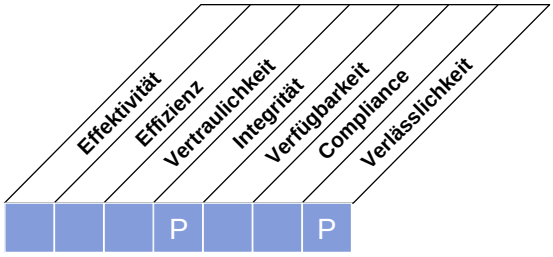
4 Managed and measurable (gemanaged und messbar):
Der Problem-Management-Prozess wird auf allen Unternehmensebenen verstanden. Die Aufgaben und Kompetenzen sind klar und zugewiesen. Methoden und Verfahren sind dokumentiert, kommuniziert und auf ihre Wirksamkeit hin gemessen. Die Mehrzahl der Probleme werden ermittelt, aufgezeichnet, in einem Bericht festgehalten und Lösungen sind initiiert. Know-how und Fachwissen werden gepflegt, aufrecht erhalten und weiterentwickelt, da diese Funktion als wertvoller und wichtiger Faktor zur Erreichung von IT-Zielen und Verbesserung der IT-Dienste betrachtet wird. Das Problem-Management ist gut in die zusammenhängenden Prozesse wie Incident-, Change-, Availability-und Configuration-Management integriert und unterstützt die Kunden bei der Verwaltung von Daten, Einrichtungen und Betriebsprozessen. KPIs und KGIs wurden für den Prozess der Problemmeldung vereinbart.

5 Optimised (optimiert):
Der Problem-Management-Prozess hat sich zu einem zukunftsweisenden und proaktiven Prozess entwickelt, der einen Beitrag zur Realisierung der IT-Ziele leistet. Probleme werden vorweggenommen und vermieden. Das Know-how bezüglich Muster bereits aufgetretener und künftiger Probleme wird durch regelmäßige Kontakte zu Anbietern und Experten aufrecht erhalten. Die Aufzeichnung, Berichterstattung über und Analyse von Problemen und deren Lösung erfolgt automatisch und unter vollständiger Integration in das Konfigurationsdaten-Management. KPIs und KGIs werden konsistent gemessen. Die meisten Systeme wurden mit automatischen Erkennungs- und Warnmechanismen ausgestattet, die kontinuierlich verfolgt und bewertet werden. Der Problem-Management-Prozess wird analysiert in Hinblick einer kontinuierlichen Verbesserung auf Grundlage der Analyse von KPIs und KGIs und wird den betroffenen Stakeholdern gemeldet.

HIGH-LEVEL CONTROL OBJECTIVE

DS11 Manage Data *(Manage Daten)*

Ein wirksames Datenmanagement erfordert die Identifikation der Anforderungen an die Daten. Der Datenmanagement-Prozess umfasst auch die Entwicklung wirksamer Verfahren zum Management der Medien-Bibliothek, der Sicherung und Wiederherstellung von Daten sowie die sorgsame Vernichtung von Medien. Eine wirksames Datenmanagement hilft, die Qualität, Aktualität und Verfügbarkeit von Geschäftsdaten zu gewährleisten.



Kontrolle über den IT-Prozess,

Manage Data (*Manage Daten*)

der die Anforderung des Unternehmens an die IT bezüglich

der Optimierung der Verwendung von Informationen und Sicherstellung der geforderten Verfügbarkeit von Informationen

durch die Konzentration auf

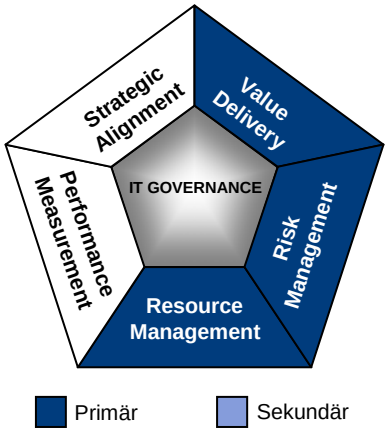
die Aufrechterhaltung der Vollständigkeit, Genauigkeit, Verfügbarkeit und Schutz von Daten zufrieden stellt,

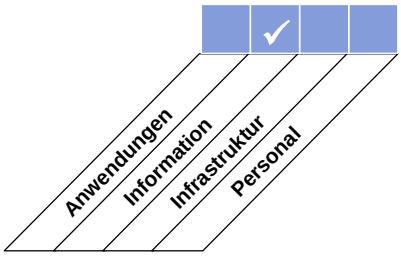
wird erreicht durch

- Sicherung und Testen der Wiederherstellung von Daten
- Managen der vor Ort und extern aufbewahrten Datenspeicherung
- Sichere Entsorgung von Daten und Geräten

und gemessen durch

- Benutzerzufriedenheit mit der Verfügbarkeit von Daten
- % der erfolgreichen Wiederherstellung von Daten
- Anzahl von Vorfällen, wo sensitive Daten von bereits entsorgten Medien wiederhergestellt wurden





DETAILLIERTE CONTROL OBJECTIVES

DS11 Manage Data *(Manage Daten)*

DS11.1 Business requirements for data management (Unternehmensanforderungen an Datenmanagement)
Erstelle Vorkehrungen, um sicherzustellen, dass vom Kerngeschäft erwartete Quelldokumente erhalten werden, alle vom Kerngeschäft erhaltene Daten verarbeitet werden, der gesamte vom Kerngeschäft benötigte Output vorbereitet und abgeliefert wird und dass Anforderungen für Wiederanlauf und nochmalige Verarbeitung unterstützt werden.

DS11.2 Storage and retention arrangements (Speicherungs- und Aufbewahrungsvorkehrungen)
Definiere und setze Verfahren für die Datenspeicherung und -archivierung ein, dass Daten im Zugriff und verwendbar bleiben. Die Verfahren sollten Anforderungen hinsichtlich Wiederauffindung, Kostengünstigkeit, kontinuierliche Integrität und Sicherheit berücksichtigen. Entwickle Speicherungs- und Aufbewahrungsvorkehrungen, um gesetzliche, regulatorische und Unternehmenserfordernisse für Dokumente, Daten, Archive, Programme, Berichte und (eingehende und ausgehende) Meldungen sowie die für deren Verschlüsselung und Authentifikation verwendeten Daten einzuhalten.

DS11.3 Media library management system (Medien-Bibliotheksmanagementsystem)
Definiere und setze Verfahren zum Unterhalt eines Inventars von lokal vorhandenen Datenträgern ein, und stelle deren Verwendbarkeit und Integrität sicher. Verfahren sollten für ein zeitgerechtes Review und Abklärung aller gefundenen Differenzen sorgen.

DS11.4 Disposal (Entsorgung)
Definiere und setze Verfahren ein, die den Zugriff auf sensitive Informationen und Software von Geräten oder Datenträgern verhindern, wenn diese entsorgt oder einem anderen Zweck übertragen werden. Solche Verfahren sollten sicherstellen, dass als gelöscht markierte oder zur Entsorgung bestimmte Daten nicht wiedergewonnen werden können.

DS11.5 Backup and restoration (Backup und Wiederherstellung)
Definiere und setze Verfahren für Sicherung und Wiederherstellung von Anwendungen, Daten und Dokumentation in Übereinstimmung mit den Geschäftsanforderungen und dem Kontinuitätsplan ein. Verifiziere die Einhaltung von Backupverfahren, die Fähigkeit zu sowie die notwendige Zeit für eine erfolgreiche und komplette Wiederherstellung. Teste Backup-Medien und den Wiederherstellungsprozess.

DS11.6 Security requirements for data management (Sicherheitsanforderungen für Management der Daten)
Entwickle Vorkehrungen, um Sicherheitsanforderungen in Bezug auf Empfang, Verarbeitung, physischer Speicherung und Ausgabe von Daten und sensitiven Meldungen zu identifizieren und umzusetzen. Dies umfasst physische Aufzeichnungen, Datenübermittlung und alle ausgelagerte Datenspeicherung.

MANAGEMENT GUIDELINES

DS11 Manage Data *(Manage Daten)*

Von	Inputs
PO2	Data dictionary; klassifizierte Daten
AI4	Benutzer-, Betriebs-, Support-, technische und administrative Handbücher
DS1	OLAs
DS4	Plan zur Lagerung und Schutz von Backups

Outputs	Nach
Berichte über Prozessperformance	ME1
Anweisungen für Operatoren zum Datenmanagement	DS13

RACI-CHART*

Aktivitäten / Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Übertrage Anforderungen bezüglich Datenspeicherung und -aufbewahrung in Verfahren				A	I	C	R				C
Definiere, unterhalte und implementiere Verfahren zum Management von Medienbibliotheken				A		R	C		I		C
Definiere, unterhalte und implementiere Verfahren zur sicheren Entsorgung von Datenträgern und Geräten				A	C	R			I		C
Sichere Daten gemäß dem Schema				A		R					
Definiere, unterhalte und implementiere Verfahren zur Wiederherstellung von Daten				A	C	R	C				I

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Sicherung von Daten und Testen der Wiederherstellung
- Managen der vor Ort und externe aufbewahrten Datenspeicherung
- Sichere Entsorgung von Daten und Geräten

treiben

Prozessziele

- Aufrechterhaltung der Vollständigkeit, Genauigkeit, Gültigkeit und Zugänglichkeit von gespeicherten Daten
- Datensicherheit während der Entsorgung von Medien
- Effizientes Management der Speichermedien

treiben

IT-Ziele

- Optimiere die Verwendung von Informationen
- Stelle den Schutz von kritischen und vertraulichen Informationen vor unberechtigtem Zugriff sicher
- Stelle die IT-Compliance mit Gesetzen und Vorschriften sicher

werden gemessen durch

Key Performance Indicators

- Frequenz der Überprüfung von Sicherungsmedien
- Durchschnittliche Zeit für die Wiederherstellung von Daten

werden gemessen durch

Key Goal Indicators

- % der erfolgreichen Wiederherstellung von Daten
- Anzahl von Vorfällen, wo sensitive Daten wiederhergestellt wurden, nachdem die Medien bereits entsorgt worden sind
- Anzahl von Betriebsunterbrechungen oder Vorfällen bezüglich Datenintegrität, die durch unzureichende Speicherkapazitäten hervorgerufen worden sind

werden gemessen durch

IT Key Goal Indicators

- Vorkommnoisse des Unvermögens der Wiederherstellung von Daten, die für Geschäftsprozesse kritisch sind
- Benutzerzufriedenheit mit der Verfügbarkeit von Daten
- Vorfälle der Nichteinhaltung von Gesetzen auf Grund von Fällen mit dem Speicherungs-Management

MATURITY MODEL

DS11 Manage Data *(Manage Daten)*

Die Reife des Management des Prozesses *Manage Data (Manage Daten)*, der die Geschäftsanforderungen an die IT erfüllt der Optimierung der Verwendung von Informationen und Sicherstellung der geforderten Verfügbarkeit von Informationen, ist:

0 Non-existent (nicht existent):
Daten werden nicht als Unternehmens-Ressourcen und -werte angesehen. Es besteht keine zugewiesene Dateneigentümerschaft oder individuelle Verantwortlichkeiten für Datenmanagement. Qualität und Sicherheit der Daten sind schwach oder nicht-existent.

1 Initial (initial):
Das Unternehmen erkennt die Notwendigkeit für ein fehlerfreies Datenmanagement. Ein *ad hoc* Ansatz für die Spezifikation von Sicherheitsanforderungen für Datenmanagement ist vorhanden, aber keine formelle Verfahren für die Kommunikation sind etabliert. Spezifische Schulungen für Datenmanagement werden nicht durchgeführt. Die Verantwortung für Datenmanagement ist unklar. Verfahren für Backup/Wiederherstellung und Vernichtung sind vorhanden.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Das Bewusstsein für die Notwendigkeit eines korrekten Datenmanagement ist unternehmensweit vorhanden. Erste Dateneigentümerschaft auf hoher (grober) Ebene findet statt. Sicherheitsanforderungen für Datenmanagement werden durch Schlüsselpersonen dokumentiert. Einige Überwachungsaktivitäten bei den wesentlichen Aufgaben des Datenmanagement werden innerhalb der IT durchgeführt (Backup, Wiederherstellung, Vernichtung). Die Verantwortlichkeiten für Datenmanagement sind informell für die IT-Schlüsselpersonen festgelegt.

3 Defined (definiert):
Die Notwendigkeit für Datenmanagement innerhalb der IT und im ganzen Unternehmen wird verstanden und akzeptiert. Die Verantwortung für Datenmanagement ist festgelegt. Dateneigentümerschaft ist der verantwortlichen Gruppe zugewiesen, welche die Integrität und Sicherheit kontrolliert. Dateneigentümerschaft ist zugewiesen und die Integrität und Sicherheit werden durch die verantwortliche Partei kontrolliert. Datenmanagement-Verfahren sind innerhalb der IT formalisiert und einige Werkzeuge für Backup/ Wiederherstellung und Vernichtung von Ausrüstung werden verwendet. Einige Überwachungstätigkeiten über Datenmanagement werden durchgeführt. Grundlegende Performance-Metriken sind festgelegt. Schulungen für die Mitarber des Datenmanagement entstehen.

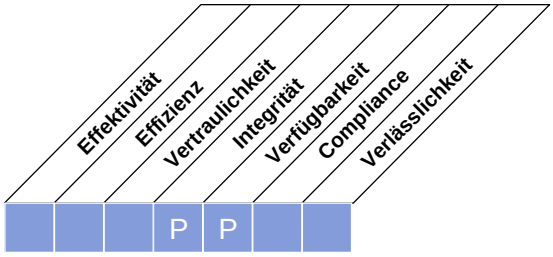
4 Managed and measurable (gemanaged und messbar):
Die Notwendigkeit für das Datenmanagement wird verstanden und die nötigen Maßnahmen werden innerhalb des Unternehmens akzeptiert. Die Verantwortung für Dateneigentümerschaft und Datenmanagement sind klar definiert, zugewiesen und innerhalb des Unternehmens kommuniziert. Die Verfahren sind formalisiert und weitherum bekannt, und das Wissen wird geteilt. Die Verwendung von aktuellen Werkzeugen kommt auf. Die KGIs und KPIs sind mit den Kunden vereinbart und werden durch einen klar definierten Prozess überwacht. Formelle Schulungen für die Mitarber des Datenmanagement sind vorhanden.

5 Optimised (optimiert):
Die Notwendigkeit für das Datenmanagement und das Verständnis für alle nötigen Maßnahmen werden unternehmensweit verstanden und akzeptiert. Der zukünftige Bedarf und Anforderungen werden proaktiv ermittelt. Die Verantwortlichkeiten für Dateneigentümerschaft und Datenmanagement sind eindeutig festgelegt, innerhalb des ganzen Unternehmens bekannt und werden rasch aktualisiert. Die Verfahren sind formalisiert und weitherum bekannt und die Teilung von Wissen ist die übliche Praxis. Weit entwickelte Werkzeuge mit höchster Automatisierung des Datenmanagement werden verwendet. Die KGIs und KPIs werden mit den Kunden vereinbart, mit den Geschäftszielen verknüpft und und durch ein klar definiertes Verfahren konsistent überwacht. Die Gelegenheiten für die Verbesserung werden fortlaufend erweitert. Die Schulungen für die Mitarber des Datenmanagement sind institutionalisiert.

HIGH-LEVEL CONTROL OBJECTIVE

DS12 Manage the Physical Environment *(Manage die physische Umgebung)*

Der Schutz von Computer-Ausrüstung und Personal erfordert eine gut konzipierte und verwaltete physische Einrichtungen. Der Prozess für das Management der physischen Umgebung umfasst die Festlegung der Anforderungen an den physischen Standort, die Auswahl geeigneter Einrichtungen und das Design wirksamer Prozesse zur Überwachung von Umweltfaktoren und des Management des physischen Zutritts. Ein wirksames Management der physischen Umgebung reduziert Unterbrechungen der Kerngeschäftsprozesse durch Schäden an Computer-Ausrüstung und Personal.



Kontrolle über den IT-Prozess,

Manage the Physical Environment (*Manage die physische Umgebung*)

der die Anforderung des Unternehmens an die IT bezüglich

des Schutzes von Computeranlagen und Geschäftsdaten und Minimierens des Risikos von Unterbrechungen der Geschäftstätigkeit

durch die Konzentration auf

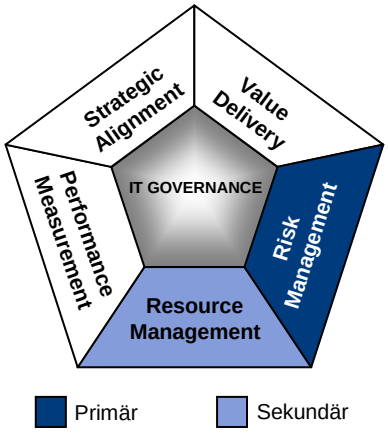
die Bereitstellung und den Unterhalt einer geeigneten physischen Umgebung, um die IT-Anlagen vor Zugriff, Beschädigung oder Diebstahl zu schützen, zufrieden stellt

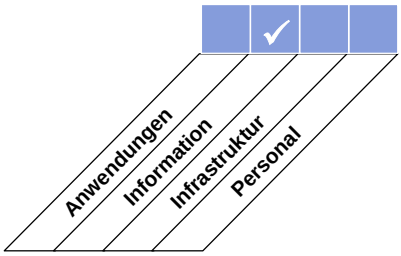
wird erreicht durch

- Implementierung von physischen Sicherheitsmaßnahmen
- Auswahl und Management von Gebäuden und Einrichtungen

und gemessen durch

- Stillstandszeiten aufgrund von Vorfällen bezüglich der physischen Umgebung
- Anzahl der Vorfälle aufgrund von Verletzungen oder Ausfällen der physischen Sicherheit
- Frequenz von physischen Risikobewertungen und -überprüfungen





DETAILLIERTE CONTROL OBJECTIVES

DS12 Manage the Physical Environment *(Manage die physische Umgebung)*

DS12.1 Site selection and layout (Standortwahl und Layout von Einrichtungen)
Definiere und wähle die physischen Standorte für IT-Ausrüstungen aus, um die mit der Unternehmensstrategie verbundene Technologiestrategie zu unterstützen. Auswahl und Entwurf des Layout eines Standortes sollten die Risiken von natürlichen und durch Menschen hervorgerufene Katastrophen einbeziehen und relevante Gesetze und Bestimmungen wie für Betriebsgesundheit und Safetybestimmungen berücksichtigen.

DS12.2 Physical security measures (Physische Sicherheitsmaßnahmen)
Definiere und implementiere den Unternehmenserfordernissen entsprechende Maßnahmen zur physischen Sicherheit. Maßnahmen sollten unter anderem Layout und Perimeter des Sicherheitsbereichs, Sicherheitszonen, Standort kritischer Ausrüstung sowie Versand- und Anlieferungszonen umfassen. Halte insbesondere ein unaufälliges Profil bezüglich der Präsenz des kritischen IT-Betriebs. Verantwortlichkeiten für die Überwachung und Verfahren für Berichterstattung und Lösung von Incidents der physischen Sicherheit müssen aufgestellt werden.

DS12.3 Physical access (Physischer Zugang)
Entwickle und implementiere Verfahren für die dem Unternehmensbedarf inklusive Notfällen entsprechende Erteilung, Einschränkung und Zurücknahme von Zutritt zu Gelände, Gebäuden und Arbeitsbereichen. Der Zugang zu Gelände, Gebäuden und Arbeitsbereichen sollte begründet, genehmigt, protokolliert und überwacht werden. Dies gilt für alle Personen, die das Gelände betreten, inklusive Personal, temporäres Personal, Kunden, Lieferanten, Besucher oder andere Drittparteien.

DS12.4 Protection against environmental factors (Schutz gegen Umwelteinflüsse)
Entwickle und implementiere Maßnahmen zum Schutz gegen Umweltfaktoren. Spezielle Ausrüstung und Geräte zur Überwachung und Steuerung der Umwelt sollten installiert sein.

DS12.5 Physical facilities management (Management von physischen Einrichtungen)
Manage Einrichtungen, inklusive Strom- und Kommunikationsausrüstung entsprechend Gesetzen und Bestimmungen, technischen und Unternehmenserfordernissen, Spezifikationen von Anbietern und Gesundheits- und Safetyrichtlinien.

MANAGEMENT GUIDELINES

DS12 Manage the Physical Environment *(Manage die physische Umgebung)*

Von	Inputs
PO2	Klassifizierte Daten
PO9	Risikobewertung
AI3	Anforderungen an physische Infrastruktur

Outputs	Nach
Berichte über Prozessperformance	ME1

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Definiere das erforderliche Niveau des physischen Schutzes					C	A/R	C				C
Wähle und kommissioniere den Standort (Rechenzentrum, Büro, etc)	I	C	C	C	C	A/R	C		C	C	C
Implementiere physische Schutzmaßnahmen					I	A/R	I	I			C
Manage die physische Umgebung (inklusive Wartung, Überwachung und Berichterstattung)						A/R	C				
Definiere und implementiere Verfahren für Autorisierung und Unterhalt des physischen Zutritts				C	I	A/R	I	I	I		C

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Implementierung von physischen Schutzmaßnahmen
- Rigorose Auswahl und Management von Einrichtungen

Prozessziele

- Bereitstellung und Unterhalt einer geeigneten physischen Umgebung für die IT-Infrastruktur und Ressourcen
- Verhinderung des Zugangs zur physischen Umgebung für diejenigen, welche keinen Zugang benötigen

IT-Ziele

- Stelle sicher, dass IT-Services und Infrastruktur Ausfällen auf Grund von Fehlern, bewussten Angriffen oder Katastrophen standhalten können und ihre Wiederherstellung gewährleistet ist
- Stelle den Schutz von kritischen und vertraulichen Informationen vor unberechtigtem Zugriff sicher
- Stelle sicher, dass der Einfluss einer IT-Service-Störung oder -Änderung auf das Geschäft minimiert ist
- Übernimm die Verantwortung für und schütze alle IT-Anlagen

treiben

treiben

werden gemessen durch

Key Performance Indicators

- Frequenz der Schulung des Personals in Maßnahmen bezüglich Safety, Sicherheit und der Einrichtungen
- % des Personals, das in Maßnahmen bezüglich Safety, Sicherheit und der Einrichtungen geschult ist
- Anzahl von Risiko mindernden Überprüfungen, die im letzten Jahr durchgeführt worden sind
- Frequenz von physischen Risikobewertungen und -überprüfungen

werden gemessen durch

Key Goal Indicators

- Anzahl der durch Verletzungen oder Ausfälle der physischen Sicherheit hervorgerufenen Vorfälle
- Anzahl der Vorfälle mit autorisiertem Zugang zu Computereinrichtungen

werden gemessen durch

IT Key Goal Indicators

- Stillstandzeit aufgrund von Vorfällen bezüglich der physischen Umgebung
- Anzahl der durch die physische Umgebung verursachten Verletzungen
- Durch Vorfälle bezüglich der physischen Umgebung entstandene Sicherheitsgefährdung

MATURITY MODEL

DS12 Manage the Physical Environment (Manage die phyische Umgebung)

Die Reife des Management des Prozesses *Manage the Physical Environment (Manage die physische Umgebung)*, der die Geschäftsanforderungen an die IT abdeckt des Schutzes von Computeranlagen und Geschäftsdaten und Minimierens des Risikos von Unterbrechungen der Geschäftstätigkeit, ist:

0 Non-existent (nicht existent):
Es besteht kein Bewusstsein für die Notwendigkeit, Einrichtungen oder Investitionen in IT-Ressourcen zu schützen. Umgebungsbezogene Einflussfaktoren wie Brandschutz, Staub, Strom, exzessive Hitze oder Feuchtigkeit werden weder überwacht noch gesteuert.

1 Initial (initial):
Das Unternehmen hat die Unternehmensanforderung erkannt, eine geeignete physische Umgebung zu schaffen, welche die Ressourcen und das Personal gegen menschlich verursachte und natürliche Gefahren schützt. Das Management von Einrichtungen und Ausrüstung ist vom Können und den Fähigkeiten einzelner Schlüsselpersonen abhängig. Das Personal kann sich innerhalb der Einrichtungen ohne Einschränkungen bewegen. Das Management überwacht die umgebungsspezifischen Controls der Einrichtungen sowie die Bewegungen des Personals nicht.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Umgebungsspezifische Sicherheitsmaßnahmen sind implementiert und werden durch das Betriebspersonal überwacht. Physische Sicherheit ist ein informeller Prozess, welcher von einer kleinen Mitarbeitergruppe mit einem hohen Maß an Sorge für die Sicherung von physischen Einrichtungen betrieben wird. Die Verfahren zur Wartung der Einrichtungen sind nicht gut dokumentiert und beruhen auf bewährten Praktiken weniger Einzelpersonen. Die Ziele physischer Sicherheit basieren nicht auf irgendwelchen formellen Standards und das Management stellt nicht sicher, dass diese Sicherheitsziele erreicht werden.

3 Defined (definiert):
Die Notwendigkeit zum Unterhalt einer kontrollierten IT-Umgebung ist verstanden und im Unternehmen akzeptiert. Die umgebungsspezifischen Sicherheitsmaßnahmen, präventive Wartung und physische Sicherheit sind Budgetpositionen, die vom Management freigegeben und verfolgt werden. Zugangsbeschränkungen sind im Einsatz, die nur autorisiertem Personal Zugang zu den Rechnereinrichtungen gewähren. Besucher werden registriert und abhängig von der Einzelperson eskortiert. Die physischen Einrichtungen sind unauffällig und nicht einfach zu erkennen. Zivile Behörden überwachen die Einhaltung von gesetzlichen Gesundheits- und Safetyvorschriften. Die Risiken sind versichert, mit minimalem Bestreben, die Versicherungskosten zu optimieren.

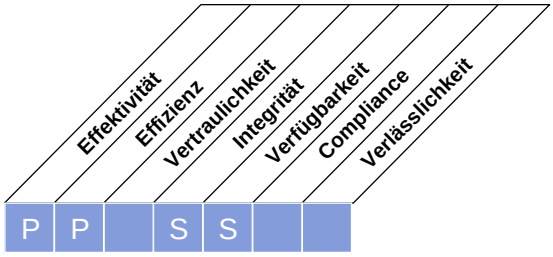
4 Managed and measurable (gemanaged und messbar):
Die Notwendigkeit zum Unterhalt einer kontrollierten IT-Umgebung ist vollständig verstanden, wie Organisationsstruktur und Budgetzuteilungen beweisen. Anforderungen umgebungsspezifischer und physischer Sicherheit sind dokumentiert; der Zugang wird strikt kontrolliert und überwacht. Verantwortlichkeiten und Eigentümerschaft wurden etabliert und kommuniziert. Das in den Einrichtungen tätige Personal ist vollständig in Notsituationen geschult, ebenso wie in Gesundheits- und Safetypraktiken. Standardisierte Kontrollmechanismen sind im Einsatz, um den Zugang zu Einrichtungen zu beschränken sowie die Einflussfaktoren auf Umgebung und Safety zu adressieren. Das Management überwacht die Wirksamkeit der Sicherheitsmaßnahmen und die Einhaltung etablierter Standards. Das Management hat KPIs und KGIs zur Messung der Verwaltung der IT-Umgebung etabliert. Die Wiederherstellbarkeit der IT-Ressourcen ist in einen organisatorischen Risikomanagement-Prozess eingegliedert. Die integrierten Informationen werden zur Optimierung des Versicherungsschutzes sowie der damit verbundenen Kosten verwendet.

5 Optimised (optimiert):
Ein vereinbarter langfristiger Plan ist vorhanden für Einrichtungen, welche die IT-Umgebung des Unternehmens unterstützen. Standards sind für sämtliche Einrichtungen festgelegt und umfassen die Standortwahl, Bauwerke, Bewachung, Safety, mechanische und elektrische Systeme, Schutz gegen umweltspezifische Einflussfaktoren (zB Brand, Blitzschlag, Überflutung). Sämtliche Einrichtungen sind inventarisiert und gemäß dem laufenden Risikomanagement-Prozess des Unternehmens klassifiziert. Der Zugang wird auf einer Job-Bedarf-Basis strikt kontrolliert und kontinuierlich überwacht und sämtliche Besucher werden jederzeit eskortiert. Die Umgebung wird durch eine spezielle Ausrüstung überwacht und kontrolliert. In Ausrüstungsräumen halten sich keine Personen mehr auf. KPIs und KGIs werden konsistent gemessen. Präventive Wartungsprogramme erzwingen eine strikte Beachtung von Ablaufplänen und sensitive Ausrüstung wird regelmäßig getestet. Die für die Einrichtungen definierten Strategien und Standards sind ausgerichtet an den Verfügbarkeitszielen der IT-Dienste und integriert in die Business Continuity-Planung und das Krisenmanagement. Das Management überprüft und optimiert die Einrichtungen durch den Einsatz von KPIs und KGIs kontinuierlich, und nutzt die Gelegenheiten, deren Geschäftsbeitrag zu verbessern.

HIGH-LEVEL CONTROL OBJECTIVE

DS13 Manage Operations *(Manage den Betrieb)*

Die vollständige und richtige Verarbeitung von Daten erfordert ein effektives Management der Datenverarbeitung und Wartung von Hardware. Dieser Prozess umfasst die Festlegung von Betriebsanweisungen sowie Verfahren zum wirksamen Management der zeitgesteuerten Verarbeitung, den Schutz von sensitivem Output, die Überwachung der Infrastruktur und vorbeugende Wartung von Hardware. Ein wirksames Betriebsmanagement hilft, die Datenintegrität zu erhalten, und reduziert Verzögerungen der Abläufe und operative IT-Betriebskosten.



Kontrolle über den IT-Prozess,

Manage Operations (*Manage den Betrieb*)

der die Anforderung des Unternehmens an die IT bezüglich

der Aufrechterhaltung der Datenintegrität und der Sicherstellung, dass die IT-Infrastruktur Fehlern und Störfällen standhalten kann und ihre Wiederherstellung gewährleistet ist

durch die Konzentration auf

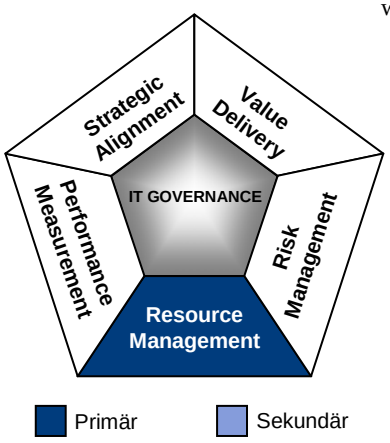
das Erreichen operativer Service Levels für zeitgesteuerte Datenverarbeitung, den Schutz von sensitivem Output und die Überwachung und den Unterhalt der Infrastruktur zufrieden stellt,

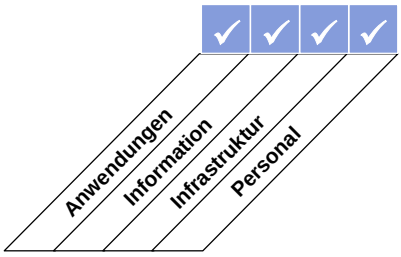
wird erreicht durch

- Betrieb der IT-Landschaft in Übereinstimmung mit vereinbarten Service Levels und definierten Anleitungen
- Unterhalt der IT-Infrastruktur

und gemessen durch

- Anzahl der betriebsbedingten Incidents mit Einfluss auf Service Levels
- Anzahl der Stunden nicht geplanter Ausfallszeiten auf Grund betriebsbedingter Incidents
- Prozent der Hardwarekomponenten, die in präventive Wartungspläne aufgenommen wurden





DETAILLIERTE CONTROL OBJECTIVES

DS13 Manage Operations *(Manage den Betrieb)*

DS13.1 Operations procedures and instructions (Operative Verfahren und Anweisungen)
Definiere, implementiere und unterhalte standardisierte Verfahren für den IT-Betrieb und stelle sicher, dass das Betriebspersonal mit allen für sie relevanten Betriebsaufgaben vertraut sind. Operative Verfahren sollten Schichtübergaben (formale Übergaben von Aktivitäten, Status-Aktualisierungen, operativen Problemen, Eskalationsverfahren und Berichte über derzeitige Verantwortungen) abdecken, um einen kontinuierlichen Betrieb sicherzustellen.

DS13.2 Job scheduling (Job-Planung)
Organisiere und plane Jobs, Prozesse und Aufgaben in der wirtschaftlichsten Reihenfolge, maximiere den Durchsatz und die Verwendung, um die Unternehmenserfordernisse zu erfüllen. Die erstmalige Planung sowie Änderungen dieser Pläne sollten autorisiert werden. Verfahren sollten vorhanden sein, um Abweichungen von normalen Job-Plänen zu erkennen, abzuklären und freizugeben.

DS13.3 IT infrastructure monitoring (Monitoring der IT-Infrastruktur)
Definiere und implementiere Verfahren zur Überwachung der IT-Infrastruktur und der damit in Zusammenhang stehenden Vorkommnisse. Stelle sicher, dass ausreichend chronologische Informationen in Betriebsprotokollen gespeichert sind, um Wiederherstellung, Review und die Untersuchung der zeitlichen Abfolge von Betriebs- und anderen Aktivitäten im Umfeld oder zur Unterstützung des Betriebs zu ermöglichen.

DS13.4 Sensitive documents and output devices (Sensitive Dokumente und Ausgabegeräte)
Etabliere geeignete physische Absicherungen, Verrechnungs- und Inventurpraktiken für sensitive IT-Anlagen wie Spezialformulare, verwertbare Einrichtungen, Spezialdrucker oder Security-Token.

DS13.5 Preventive maintenance for hardware (Präventive Hardware-Wartung)
Definiere und implementiere Verfahren zur Sicherstellung einer zeitgerechten Wartung der Infrastruktur, um die Häufigkeit und Auswirkungen von Fehlern oder Leistungsabfall zu reduzieren.

MANAGEMENT GUIDELINES

DS13 Manage Operations *(Manage den Betrieb)*

Von	Inputs
AI4	Benutzer-, Betriebs-, Support-, technische und administrative Handbücher
AI7	Freigabe zum Produktiveinsatz; Software-Release und -Verteilungsplan
DS1	SLAs und OLAs
DS4	Plan zur Lagerung und Schutz von Backups
DS9	Details zur IT-Konfiguration / Assets
DS11	Anweisungen für Operatoren zum Datenmanagement

Outputs	Nach
Incident-Tickets	DS8
Fehler-Protokolle	DS10
Berichte über Prozessperformance	ME1

RACI-CHART*

Aktivitäten / Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Erstelle/modifiziere Verfahren des Betriebs (inkl. Handbücher, Checklisten, Schichtpläne, Übergabedokumentation, Eskalationsverfahren, etc.)						A/R					I
Plane Workload und Batch Jobs					C	A/R	C	C			
Überwache die Infrastruktur und die Verarbeitung und löse Probleme						A/R					I
Manage and schütze physischen Output (Papier, Medien, etc.)						A/R					C
Implementiere Fixes und Changes am Zeitplan und an der Infrastruktur					C	A/R	C	C			C
Implementiere/erstelle einen Prozess zur Absicherung der Authentifizierungsanlagen gegen Beeinflussung, Verlust und Diebstahl				A		R			I		C
Plane und führe präventive Wartung durch						A/R					

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Betrieb der IT-Landschaft in Übereinstimmung mit vereinbarten Service Levels, definierten Anleitungen und enger Überwachung
- Präventive Wartung und Überwachung der IT-Infrastruktur

werden gemessen durch

Key Performance Indicators

- Anzahl der Schulungstage pro BetriebsmitarberIn pro Jahr
- % der Hardwareanlagen, die in präventive Wartungspläne aufgenommen wurden
- % der Arbeitspläne, die automatisiert sind
- Häufigkeit der Aktualisierung von Betriebsverfahren

treiben

Prozessziele

- Definiere operative Verfahren und gleiche diese mit den vereinbarten Service Levels an
- Erledige vorab und nach Bedarf geplante Arbeiten innerhalb der vereinbarten Service Levels
- Schütze sensitive Informationen physisch

werden gemessen durch

Key Goal Indicators

- Anzahl der Stillstände und Verzögerungen, die durch Abweichung von Betriebsverfahren verursacht wurden
- % der geplanten Arbeiten und Anfragen, die nicht zeitgerecht fertig gestellt wurden
- Anzahl der Stillstände und Verzögerungen, die durch mangelhafte Verfahren verursacht wurden

treiben

IT-Ziele

- Stelle sicher, dass IT-Services und Infrastruktur Ausfällen auf Grund von Fehlern, bewussten Angriffen oder Katastrophen standhalten können und ihre Wiederherstellung gewährleistet ist
- Stelle die Enduser-Zufriedenheit mit den Serviceangeboten und Service Levels sicher
- Stelle die Verfügbarkeit der IT-Services gemäß den Anforderungen sicher

werden gemessen durch

IT Key Goal Indicators

- Anzahl der betriebsbedingten Incidents mit Einfluss auf Service Levels
- Anzahl der Stunden ungeplanter Betriebsunterbrechungen auf Grund betriebsbedingter Störungen

MATURITY MODEL

DS13 Manage Operations *(Manage den Betrieb)*

Die Reife des Management des Prozesses *Manage Operations (Manage den Betrieb)*, der die Geschäftsanforderungen an die IT erfüllt der Aufrechterhaltung der Datenintegrität und der Sicherstellung, dass die IT-Infrastruktur Fehlern und Störfällen standhalten kann und ihre Wiederherstellung gewährleistet ist, ist:

0 Non-existent (nicht existent):
Das Unternehmen wendet weder Zeit noch Ressourcen für die Etablierung von elementaren Aktivitäten des IT-Supports und des IT-Betriebs auf.

1 Initial (initial):
Das Unternehmen ist sich der Notwendigkeit für die Strukturierung der IT-Support-Funktionen bewusst. Wenige Standardverfahren sind etabliert und die Aktivitäten des Betriebs sind reaktiv. Die Mehrzahl der Betriebsprozesse sind informell terminiert und Verarbeitungsanfragen werden ohne vorherige Validierung akzeptiert. Computer, Systeme und Anwendungen, welche die Geschäftsprozesse unterstützen, werden häufig unterbrochen, verzögert oder sind nicht verfügbar. Während Mitarber auf Ressourcen warten, geht Zeit verloren. Ausgabemedien tauchen manchmal an unerwarteten Orten oder überhaupt nicht mehr auf.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Das Unternehmen ist sich der Tatsache bewusst, dass Aktivitäten des IT-Betriebs eine Schlüsselrolle bei der Erbringung von IT-Support-Funktionen spielen. Budgets für Werkzeuge werden fallbezogen zugeteilt. Der IT-Support wird informell und intuitiv betrieben. Eine hohe Abhängigkeit vom Können und den Fähigkeiten einzelner Personen besteht. Instruktionen, was, wann und in welcher Reihenfolge zu tun ist, sind nicht dokumentiert. Einige Schulungen für Bediener (engl.: *operator*) sind ebenso vorhanden wie einige formelle Standards für den Betrieb.

3 Defined (definiert):
Die Notwendigkeit eines Management des Computerbetriebs wird innerhalb des Unternehmens verstanden und akzeptiert. Ressourcen sind zugewiesen worden und Ausbildung am Arbeitsplatz findet teilweise statt. Wiederholbare Tätigkeiten sind formell festgehalten, standardisiert, dokumentiert und kommuniziert. Die Ereignisse und Ergebnisse abgeschlossener Aufgaben werden aufgezeichnet und eingeschränkt an das Management berichtet. Eine automatische Ablaufsteuerung und andere Werkzeuge werden eingeführt, um das Eingreifen der Operator zu beschränken. Für den Einsatz von neuen Jobs im laufenden Betrieb werden Controls eingeführt. Eine formelle Richtlinie zur Reduzierung der Anzahl unplanmäßiger Ereignisse ist entwickelt. Wartungs- und Service-Vereinbarungen mit Lieferanten sind bisher informeller Art.

4 Managed and measurable (gemanaged und messbar):
Die Verantwortlichkeiten für den Betrieb und den Support sind klar definiert und Eigentümerschaft ist zugewiesen. Der Betrieb wird durch einen Etat für finanzielle und personelle Ressourcen unterstützt. Schulungen sind formalisiert und erfolgen laufend. Ablaufpläne und Aufgaben sind dokumentiert und sowohl intern an die IT-Funktion als auch an die Auftraggeber im Geschäftsbereich kommuniziert. Mit Hilfe von standardisierten Performance Agreements und etablierten Service Levels ist eine Messung und Überwachung der täglichen Aktivitäten möglich. Jegliche Abweichungen von den etablierten Normen werden zeitnah adressiert und korrigiert. Das Management überwacht die Nutzung der Computer-Ressourcen sowie fertiggestellte Arbeiten oder übertragene Aufgaben. Ein ständiges Bestreben besteht, den Grad der Prozessautomatisierung als Mittel kontinuierlicher Verbesserung zu erhöhen. Formelle Wartung und Service Agreements mit Lieferanten sind etabliert. Es besteht vollständiger Einklang mit den Verfahren des Problem-, Kapazitäts- und Verfügbarkeitsmanagement, welche durch Ursachenanalysen von Fehlern und Ausfällen unterstützt werden.

5 Optimised (optimiert):
Der Betrieb des IT-Support ist wirksam, wirtschaftlich und ausreichend flexibel, um Service Level-Bedürfnissen mit minimalem Produktivitätsverlust nachzukommen. Die operativen Verfahren des IT-Management sind standardisiert, innerhalb einer Wissenbasis dokumentiert und unterliegen kontinuierlicher Verbesserung. Automatisierte Prozesse zur Unterstützung von Systemen funktionieren reibungslos und tragen zu einer stabilen Umgebung bei. Sämtliche Probleme und Fehler werden analysiert, um die Grundursache zu ermitteln. Regelmäßige Meetings mit Verantwortlichen des Change-Management stellen eine zeitliche Eingliederung von Changes in die produktiven Abläufpläne sicher. In Kooperation mit den Lieferanten wird die Ausrüstung auf Alter und Anzeichen von Fehlfunktionen untersucht. Die Wartung erfolgt vorwiegend präventiv.

MONITOR AND EVALUATE

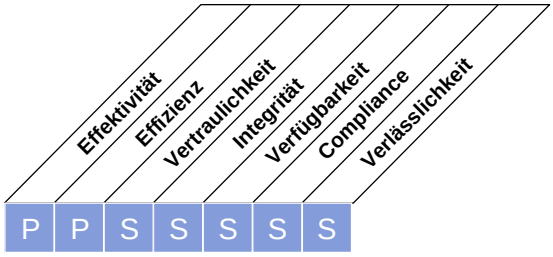
ME1 Monitor and Evaluate IT-Performance
(Monitore und evaluiere IT-Performance)
ME2 Monitor and Evaluate Internal Control
(Monitore und evaluiere Internal Controls)
ME3 Ensure Regulatory Compliance
(Stelle Compliance mit Vorgaben sicher)
ME4 Provide IT-Governance
(Sorge für IT-Governance)

Diese Seite wurde absichtlich freigelassen

HIGH-LEVEL CONTROL OBJECTIVE

ME1 Monitor and Evaluate IT-Performance *(Monitore und evaluiere IT-Performance)*

Ein wirksames Management der IT-Performance erfordert einen Überwachungsprozess. Dieser Prozess umfasst die Festlegung von relevanten Performance-Indicators, eine systematische und zeitnahe Berichterstattung der Performance und promptes Handeln im Fall von Abweichungen. Eine Überwachung ist erforderlich, um sicherzustellen, dass die richtigen Aufgaben entsprechend der vereinbarten Ausrichtung und Richtlinien wahrgenommen werden.



Kontrolle über den IT-Prozess,

Monitor and evaluate IT performance (*Monitoring und Evaluierung von IT-Performance*)

der die Anforderung des Unternehmens an die IT bezüglich

Transparenz und Verständnis für IT-Kosten, Nutzen, Strategie, Richtlinien und Service Levels in Übereinstimmung mit Anforderungen der Governance

durch die Konzentration auf

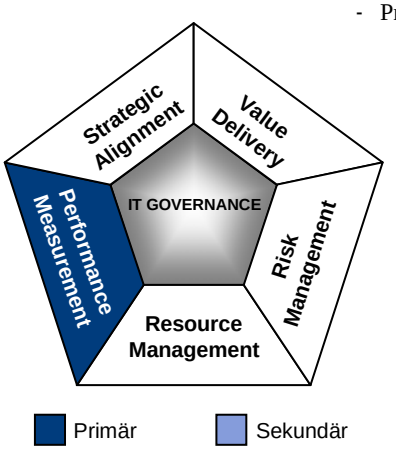
Monitoring und Berichterstattung von Prozessmetriken und Identifikation sowie Umsetzung von Maßnahmen zur Leistungsverbesserung , *zufrieden stellt,*

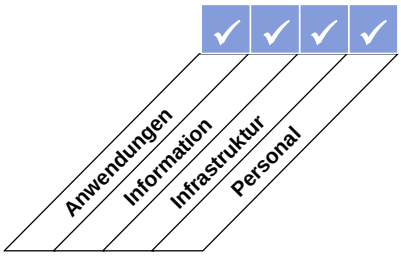
wird erreicht durch

- Zuordnung und Überführung von Berichten der Prozessperformance in Managementberichte
- Abgleich von Performance mit vereinbarten Zielen und Initiierung notwendiger Korrektur-Maßnahmen

und gemessen durch

- Zufriedenheit des Managements und der Governance-Organisationseinheit mit der Performance-Berichterstattung
- Anzahl der Verbesserungsmaßnahmen, die durch Monitoring getrieben werden
- Prozent der kritischen Prozesse mit Monitoring





DETAILLIERTE CONTROL OBJECTIVES

ME1 Monitor and Evaluate IT-Performance *(Monitore und evaluiere IT-Performance)*

ME1.1 Monitoring Approach (Ansatz für das Monitoring)
Stelle sicher, dass das Management ein Framework und einen Ansatz für ein generelles Monitoring aufstellt, welche den Scope, die Methoden und anzuwendenden Prozesse festlegen, die befolgt werden müssen, um den Beitrag der IT zu den Portfoliomanagement- und Programmmanagement-Prozessen sowie jene Prozesse zu überwachen, die spezifisch sind für die Erbringung des Potential und der Services der IT. Das Framework sollte in das unternehmensweite System zum Performance-Monitoring integriert sein.

ME1.2 Definition and Collection of Monitoring Data (Definition und Sammlung von Monitoring-Daten)
Stelle sicher, dass das IT-Management in Zusammenarbeit mit dem Kerngeschäft ein ausgewogenes Maß an Vorgaben, Messgrößen, Zielen und Benchmarks für Performance definiert und dass diese auch durch Kerngeschäftsverantwortliche und andere, relevante Stakeholder freigegeben werden. Messgrößen für Performance sollten die folgenden enthalten:

- Beitrag zum Kerngeschäft, der auch, aber nicht nur finanzorientierte Zahlen enthält
- Perfomance im Vergleich zum strategischen Geschäfts- und IT-Plan
- Risiken aus und Einhaltung von Regulativen
- Zufriedenheit interner und externer User
- Wesentliche IT-Prozesse, inklusive Entwicklung und Service Delivery
- Zukunftsorientierte Aktivitäten (zB neu entstehende Technologien, wieder verwendbare Infrastruktureinrichtungen, Fertigkeiten von Geschäfsbereichs- und IT-Personal).

Prozesse sollten erstellt werden, um zeitnahe und richtige Daten zu sammeln und um über den Zielerreichungsgrad berichten zu können.

ME1.3 Monitoring Method (Methode des Monitoring)
Stelle sicher, dass der Monitoring-Prozess eine Methode einsetzt (zB Balanced Scorecard), die eine prägnante, umfassende Übersicht über die Performance der IT ermöglicht und die zum unternehmensweiten Monitoring System passt.

ME1.4 Performance Assessment (Beurteilung der Performance)
Vergleiche in regelmäßigen Abständen die Performance mit den Zielen, führe Ursachenanalysen (engl.: *root cause analysis*) durch und ergreife Maßnahmen, die die zugrunde liegenden Ursachen in Angriff zu nehmen.

ME1.5 Board and Executive Reporting (Berichte an geschäftsführende Gremien)
Erstelle Management-Berichte für den Review des Fortschritts der Organisation durch die Geschäftsführung hinsichtlich der identifizierten Ziele – speziell in Bezug auf die Performance des Unternehmensportfolios von IT-gestützten Investitionsprogrammen, auf die Service Levels individueller Programme und auf den Beitrag der IT zu dieser Performance. Statusberichte sollten das Ausmaß aufzeigen, wie geplante Ziele erreicht, Ergebnisse fertig gestellt, Performance-Ziele erreicht und Risiken vermindert wurden. Nach dem Review sollten sämtliche Abweichungen von der erwarteten Performance identifiziert, geeignete Management-Aktivitäten initiiert und darüber berichtet werden.

ME1.6 Remedial Actions (Verbesserungsmaßnahmen)
Identifiziere und initiiere Verbesserungsmaßnahmen, welche basieren auf dem Monitoring, der Beurteilung und der Berichterstattung über die Performance. Dies umfasst die Nachverfolgung aller Überwachungen, Berichterstattung und Beurteilungen durch

- Review, Verhandlung und Herbeiführung von Reaktionen des Managements
- Zuweisung von Verantwortlichkeiten für die Verbesserung
- Verfolgung der Ergebnisse der eingeleiteten Maßnahmen

MANAGEMENT GUIDELINES

ME1 Monitor and Evaluate IT-Performance *(Monitore und evaluiere IT-Performance)*

Von	Inputs
PO5	Kosten-/Nutzenbericht
PO10	Report der Projektperformance
AI6	Statusreports von Changes
DS1-DS13	Berichte über Prozessperformance
DS8	Berichte über Benutzerzufriedenheit
ME2	Report zur Wirksamkeit von IT-Controls
ME3	Bericht zur Compliance von IT-Aktivitäten mit externen rechtlichen und regulatorischen Anforderungen
ME4	Bericht zum Status der IT-Governance

Outputs	Nach						
Performance Inputs für die IT-Planung	PO1	PO2	DS1				
Plan der Verbesserungsmaßnahmen	PO4	PO8					
Historische Risiken (Trends und Ereignisse)	PO9						
Berichte über Prozessperformance	ME2						

RACI-CHART*

Aktivitäten \ Funktionen	Board	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Entwickle den Monitoring Ansatz		A	R	C	R	I	C	I	C	I		C
Identifiziere und sammle messbare Ziele, die Unternehmensziele unterstützen		C	C	C	A	R	R		R			
Erstelle Scorecards												
Beurteile Performance			I	I	A	R	R	C	R	C		
Reporte Performance	I	I	I	A	A	R	R	C	R	C		I
Identifiziere und monitore Maßnahmen zur Verbesserung der Performance					A	R	R	C	R	C		C

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Aufzeichnung, Zuordnung und Überführung von Reports der Prozessperformance in Management-Reports
- Abgleich von Performance mit vereinbarten Zielen und Initiierung notwendiger Verbesserungsmaßnahmen

werden gemessen durch

Key Performance Indicators

- Zeitverzögerung zwischen dem Bericht der Abweichung und dem Beginn der Handlung
- Verzögerung in der Aktualisierung der Messung, um die wirklichen Performanceziele, -messung, -zielwerte und Benchmarks widerzuspiegeln
- Anzahl der Metriken (pro Prozess)
- Anzahl der identifizierten und in das Monitoring integrierten Ursachen/Wirkungszusammenhänge
- Erforderlicher Aufwand für die Sammlung der Messdaten
- Anzahl von Problemen, die nicht durch den Messprozess identifiziert wurden

treiben

Prozessziele

- Lege messbare Vorgaben, KGIs und KPIs für IT- und Schlüsselprozesse fest
- Messe, monitore und berichte Prozess-Metriken
- Identifiziere und implementiere Performanceverbesserungsmaßnahmen

werden gemessen durch

Key Goal Indicators

- Zufriedenheit der Stakeholder mit dem Bewertungsprozess
- % kritischer Prozesse, die überwacht werden
- Anzahl von Verbesserungsmaßnahmen, die durch Monitoring-Aktivitäten getrieben werden
- Anzahl der erreichten Performanceziele (erreichte Indikatoren)

treiben

IT-Ziele

- Reagiere auf Anforderungen der Governance entsprechend den Geschäftsführungs-vorgaben
- Reagiere auf Geschäftsanforderungen in Übereinstimmung mit der Unternehmensstrategie
- Stelle sicher, dass die ITeine kosteneffiziente Servicequalität, eine kontinuierliche Verbesserung und Bereitschaft für zukünftige Veränderungen zeigt
- Stelle Transparenz und Verständnis von IT - Kosten, Nutzen, Strategie, Richtlinien und Service Levels sicher

werden gemessen durch

IT Key Goal Indicators

- Anzahl der Änderung von Zielen für die Wirksamkeits- und Wirtschaftlichkeits-indikatoren der IT-Prozesse
- Zufriedenheit des Managements und des Governance-Gremiums mit der Performance-Berichterstattung
- Reduktion in der Anzahl von ungelösten Prozess-Unzulänglichkeiten

MATURITY MODEL

ME1 Monitor and Evaluate IT-Performance *(Monitore und evaluiere IT-Performance)*

Die Reife des Management des Prozesses *Monitor and Evaluate IT-Performance (Monitore und evaluiere IT-Performance)*, der die Geschäfsanforderungen an die IT abdeckt der Transparenz und Verständnis für IT-Kosten, Nutzen, Strategie, Richtlinien und Service Levels in Übereinstimmung mit Anforderungen der Governance, ist:

0 Non-existent (nicht existent):
Die Organisation hat keinen Monitoring-Prozess implementiert. IT führt kein unabhängiges Monitoring von Projekten oder Prozessen durch. Sinnvolle, rechtzeitige und genaue Berichte sind nicht vorhanden. Der Bedarf für klar verstandene Prozessziele ist nicht erkannt.

1 Initial (initial):
Das Management hat den Bedarf erkannt, Informationen über Monitoring-Prozesse zu sammeln und zu beurteilen. Standardisierte Prozesse zur Sammlung und Beurteilung wurden nicht identifiziert. Monitoring und Messgrößen werden fallweise entsprechend dem Bedarf einzelner IT-Projekte und -Prozesse umgesetzt resp. ausgewählt. Monitoring wird im allgemeinen als Reaktion auf einen Incident implementiert, der Verlust oder Aufsehen verursacht hat. Das Rechnungswesen überwacht grundlegende Finanzkennzahlen für die IT.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Grundlegende, zu überwachende Messgrößen wurden festgelegt. Methoden und Techniken zur Sammlung und Beurteilung existieren, aber die Prozesse wurden nicht in der gesamten Organisation übernommen. Die Interpretation der Überwachungsergebnisse basiert auf der Expertise von Schlüsselpersonen. Werkzeuge mit begrenztem Leistungsumfang werden ausgewählt und zur Informationssammlung eingesetzt, jedoch basiert diese nicht auf einem geplanten Ansatz.

3 Defined (definiert):
Das Management hat standardisierte Überwachungsprozesse kommuniziert und institutionalisiert. Informations- und Ausbildungsprogramme für Monitoring wurden umgesetzt. Eine formale Wissensbasis für historische Performanceinformationen wurde entwickelt. Die Beurteilung wird noch immer auf Basis einzelner IT-Prozesse und -Projekte durchgeführt und ist nicht über alle Prozesse integriert. Werkzeuge für die Überwachung von IT-Prozessen und Service Levels wurden festgelegt. Messungen für den Beitrag der IT zur Unternehmensperformance wurden definiert, die herkömmliche Finanz- und operative Kriterien verwenden. IT-spezifische Performance Messungen, nicht finanzbezogene Messungen, strategische Messungen, Messungen von Kundenzufriedenheit und Service Levels sind festgelegt. Ein Framework zur Messung der Performance wurde definiert.

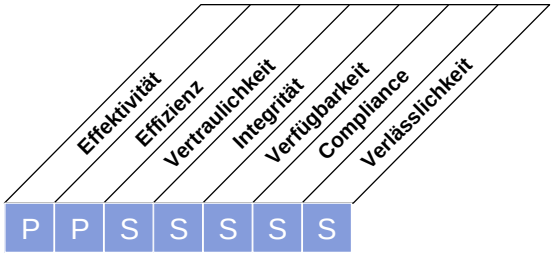
4 Managed and measurable (gemanaged und messbar):
Das Management hat Toleranzgrenzen festgelegt, innerhalb derer IT-Prozesse laufen müssen. Die Berichterstattung der Monitoring-Ergebnisse wurde standardisiert und normalisiert. Es besteht eine Integration der Metriken über alle IT-Projekte und -Prozesse. Die Systeme zum Management-Reporting der IT sind formalisiert. Automatisierte Tools sind integriert und organisationsweit harmonisiert, um betriebliche Informationen zu Anwendungen, Systemen und Prozessen zu sammeln. Das Management kann die Performance auf Basis vereinbarter, durch die Stakeholder genehmigte Kriterien evaluieren. Die Messung der IT ist mit organisationsweiten Zielen in Einklang.

5 Optimised (optimiert):
Ein Prozess zur kontinuierlichen Qualitätsverbesserung wurde entwickelt, um die unternehmensweiten Standards und Richtlinien für Monitoring zu verbessern und um Best-Practices der Industrie umzusetzen. Alle Überwachungsprozesse sind optimiert und unterstützen unternehmensweite Ziele. Vom Kerngeschäft getriebene Metriken werden üblicherweise verwendet, um ie Performance zu messen und sind in strategische Beurteilungsframeworks wie die IT Balanced Scorecard integriert. Monitoring und laufendes Redesign von Prozessen sind in Einklang mit den unternehmensweiten Verbesserungsplänen für Geschäftsprozesse. Benchmarking mit Vergleichswerten der Industrie und wesentlichen Mitbewerbern wurde auf Basis gut verstandener Vergleichskriterien formalisiert.

HIGH-LEVEL CONTROL OBJECTIVE

ME2 Monitor and Evaluate Internal Control *(Monitore und evaluiere Internal Controls)*

Die Einrichtung eines wirksamen Internal Control Programms für die IT erfordert einen wohl-definierten Überwachungsprozess. Dieser Prozess umfasst die Überwachung von Abweichungen bei Controls, Ergebnissen von Self-Assessments und externen Reviews sowie die Berichterstattung. Ein wesentlicher Nutzen der Überwachung von Internal Controls ist, eine Bestätigung über den wirksamen und wirtschaftlichen Betrieb und die Einhaltung der entsprechenden Gesetze und Vorschriften zu erhalten.



Kontrolle über den IT-Prozess,

Monitor and Evaluate Internal Control (*Monitore und evaluiere Internal Controls*)

der die Anforderung des Unternehmens an die IT bezüglich

der Absicherung für das Erreichen der IT-Ziele und der Einhaltung von IT-bezogenen Gesetzen und Vorschriften

durch die Konzentration auf

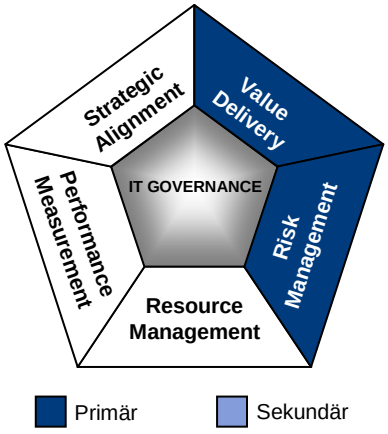
die Überwachung der internen Kontrollprozesse für IT-bezogene Aktivitäten und die Identifikation von Verbesserungsmaßnahmen , *zufrieden stellt,*

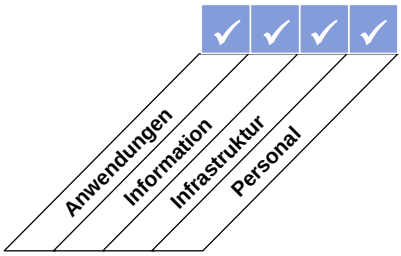
wird erreicht durch

- Festlegung eines in das IT-Prozess-Framework eingebetteten Systems von Internal Controls
- Überwachung und Reporten der Wirksamkeit der Internal Controls über die IT
- Berichterstattung über Control-Abweichungen an das Management zur Behandlung

und gemessen durch

- Anzahl wesentlicher Verstöße gegen Internal Controls
- Anzahl der Verbesserungsinitiativen für Controls
- Anzahl und Umfang der Control Self-Assessments





DETAILLIERTE CONTROL OBJECTIVES

ME2 Monitor and Evaluate Internal Control *(Monitore und evaluiere Internal Controls)*

ME2.1 Monitoring of internal control framework (Monitoring des Control Frameworks)
Monitore laufend das IT Control-Umfeld und das Control Framework. Eine Bewertung unter Anwendung von Best Practices der Industrie und Benchmarks sollte verwendet werden, um die IT-Control Umgebung und das Control Framework zu verbessern.

ME2.2 Supervisory review (Übergeordneter Review)
Monitore die Wirksamkeit der Internal Controls über die IT durch einen übergeordneten Review und berichte darüber – unter Einbezug von zB Einhaltung von Richtlinien und Normen, Informationssicherheit, Steuerung von Changes und in Service Level Agreements aufgeführte Controls.

ME2.3 Control exceptions (Ausnahmebehandlung für Controls)
Zeichne Informationen für alle Ausnahmen von Controls auf und stelle sicher, dass diese für die Analyse der grundlegenden Ursachen und für Verbesserungsmaßnahmen verwendet werden. Das Management sollte entscheiden, welche Ausnahmen an die funktional verantwortliche Person kommuniziert werden und welche Ausnahmen eskaliert werden sollten. Das Management ist auch für die Information der betroffenen Parteien verantwortlich.

ME2.4 Control self-assessment (Selbstbeurteilung der Steuerung)
Evaluiere durch ein ständiges Programm zur Selbsteinschätzung die Vollständigkeit und Wirksamkeit der Internal Control des Managements über die IT-Prozesse, -Richtlinien und -Verträge.

ME2.5 Assurance of internal control (Bestätigung der Internal Controls)
Hole, wo notwendig, weitere Bestätigungen für die Vollständigkeit und Wirksamkeit der Internal Controls durch Reviews von Dritten ein. Solche Reviews können durch die Compliance-Funktion des Unternehmens oder – auf Anfrage des Managements – durch Internal Audit oder durch extern beauftragte Prüfer, Berater oder Zertifizierungsstellen durchgeführt werden. Die Qualifikation der Personen, die diese Audits durchführen, muss sichergestellt sein, zB durch Zertifizierung als Certified Information Systems Auditor™ (CISA®).

ME2.6 Internal control at third parties (Internal Controls bei Dritten)
Bewerte den Status der Internal Controls von sämtlichen externen Dienstleistern. Bestätige, dass externe Dienstleister rechtliche und regulatorische Anforderungen sowie vertragliche Verpflichtungen einhalten. Dies kann durch einen Audit durch Dritte erfolgen oder durch ein Review der internen Audit-Funktion des Managements und den Ergebnissen der Prüfungen.

ME2.7 Remedial actions (Verbesserungsmaßnahmen)
Identifiziere auf Basis von Berichten und Beurteilungen von Controls Verbesserungsmaßnahmen und initiiere diese. Dies umfasst eine Nachbearbeitung aller Beurteilungen und Berichte durch:

- Review, Verhandlung und Umsetzung von Reaktionen des Management
- Zuweisung von Verantwortung für die Verbesserung (kann auch die Risikoakzeptanz umfassen)
- Verfolgung der Ergebnisse der vereinbarten Aktivitäten.

MANAGEMENT GUIDELINES

ME2 Monitor and Evaluate Internal Control *(Monitore und evaluiere Internal Controls)*

Von	Inputs
ME1	Report der Prozessperformance

Outputs	Nach						
Report zur Wirksamkeit von IT-Controls	PO4	PO6	ME1	ME4			

RACI-CHART*

Aktivitäten \ Funktionen	Board	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Monitore und steuere IT Internal Control-Aktivitäten					A		R		R	R		A/I
Monitore den Selbstbeurteilungsprozess				I	A		R		R	R		C
Monitore die Leistungen unabhängiger Reviews, Audits und Prüfungen				I	A		R		R	R		C
Monitore den Prozess zur Erlangung einer Bestätigung der von Dritten ausgeführten Controls		I	I	I	A		R		R	R		C
Monitore den Prozess zur Identifikation und Beurteilung der Control-Ausnahmen		I	I	I	A	I	R		R	R		C
Monitore den Prozess zur Identifikation und Beseitigung von Control-Ausnahmen		I	I	I	A	I	R		R	R		C
Berichte den wesentlichen Stakeholdern	I	I	I		A/R							I

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Definition eines in das IT-Prozess-Framework eingebetteten Systems von Internal Controls
- Überwachung und Berichterstattung über die Wirksamkeit der Internal Controls über die IT
- Berichterstattung über Control-Ausnahmen an das Management zur Behandlung

treiben

Prozessziele

- Überwache das Erreichen der für die IT-Prozesse gesetzten Internal Control Zielen
- Identifiziere Verbesserungsmaßnahmen für Internal Controls

treiben

IT-Ziele

- Stelle sicher, dass IT-Services und Infrastruktur Ausfällen auf Grund von Fehlern, bewussten Angriffen oder Katastrophen standhalten können und ihre Wiederherstellung gewährleistet ist
- Schütze die Erreichung der IT-Ziele
- Stelle die IT-Compliance mit Gesetzen und Vorschriften sicher
- Übernimm die Verantwortung für und schütze alle IT-Anlagen

werden gemessen durch

Key Performance Indicators

- Anzahl und Abdeckung der Control Self-Assessments
- Anzahl und Abdeckung der Internal Controls, die einem übergeordneten Review unterliegen
- Zeitspanne zwischen dem Auftreten einer Schwäche der Internal Control und deren Meldung
- Anzahl, Häufigkeit und Abdeckung der Internal Compliance Berichte

werden gemessen durch

Key Goal Indicators

- Häufigkeit von Fehlern im Internal Control
- Anzahl der von externen Qualifizierungs- und Zertifizierungsberichten identifizierten Schwachstellen
- Anzahl der Verbesserungsinitiativen für Controls
- Anzahl der Vorfälle aufgrund der Nichtbefolgung von Vorschriften oder Gesetzen
- Anzahl der zeitgerechten Handlungen auf Internal Control Ereignisse

werden gemessen durch

IT Key Goal Indicators

- Grad der Zufriedenheit des Senior Managements mit der Berichterstattung des Internal Control Monitoring
- Anzahl der bedeutenden Verstöße gegen Internal Controls

MATURITY MODEL

ME2 Monitor and Evaluate Internal Control *(Monitore und evaluiere Internal Controls)*

Die Reife des Management des Prozesses *Monitor and Evaluate Internal Control (Monitore und evaluiere Internal Controls)*, der die Geschäftsanforderungen an die IT abdeckt der Absicherung der Erreichung der IT-Ziele und der Einhaltung von IT-bezogenen Gesetzen und Vorschriften, ist:

0 Non-existent (nicht existent):
Im Unternehmen fehlen Verfahren zur Überwachung der Wirksamkeit der Internal Controls. Es fehlen Methoden zur Management-Berichterstattung über die Internal Controls. Es fehlt ein allgemeines Bewusstsein für eine Bestätigung der operationellen Sicherheit der IT sowie der Internal Controls. Management und Mitarber lassen jegliches Bewusstsein für Internal Controls vermissen.

1 Initial (initial):
Das Management ist sich der Notwendigkeit einer regelmäßigen Bestätigung des IT-Managements bzw. der IT-Controls bewusst. Individuelle Expertise wird bei der Bewertung der Angemessenheit von Internal Controls auf *ad hoc*-Basis angewandt. Das IT-Management hat nicht formell die Verantwortlichkeiten für die Überwachung der Wirksamkeit der Internal Controls zugeteilt. Die Bewertung der IT Internal Controls wird im Rahmen von Abschlussprüfungen (financial audits) vorgenommen, ohne dass die Methodiken und Qualifikationen den Bedürfnissen der Informatikfunktion gerecht werden.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Das Unternehmen verwendet informelle Control-Berichte, um Initiativen mit korrigierenden Maßnahmen einzuleiten. Die Bewertung der Internal Controls ist abhängig von den Qualifikationen von Schlüsselpersonen. Das Unternehmen verfügt über ein erhöhtes Bewusstsein für die Überwachung der Internal Controls. Das Informatik-Management führt regelmäßig eine Überwachung der Wirksamkeit derjenigen Internal Controls durch, die es als kritisch ansieht. Methodiken und Werkzeuge zur Überwachung der Internal Controls werden eingeführt, jedoch nicht auf der Grundlage eines Plans. Die spezifischen Risikofaktoren im IT-Umfeld werden auf der Grundlage der Fähigkeiten Einzelner identifiziert.

3 Defined (definiert):
Das Management unterstützt die Überwachung der Internal Controls und hat diese institutionalisiert. Richtlinien und Verfahren wurden entwickelt für die Bewertung und Berichterstattung über Überwachungsaktivitäten im Zusammenhang mit Internal Controls. Ein Ausbildungs- und Schulungsprogramm für die Überwachung der Internal Controls ist festgelegt worden. Ein Prozess für Self-Assessments und Bestätigungs-Reviews der Internal Controls ist mit Rollen für die verantwortlichen Business- und IT-Manager definiert worden. Werkzeuge werden verwendet, sind jedoch nicht notwendigerweise in sämtliche Prozesse integriert. Richtlinien für die Bewertung von IT-Prozessrisiken werden innerhalb von Control-Rahmenwerken eingesetzt, welche speziell für die IT-Organisation entwickelt wurden. Prozessspezifische Risiken und Risikominderungsrichtlinien sind festgelegt.

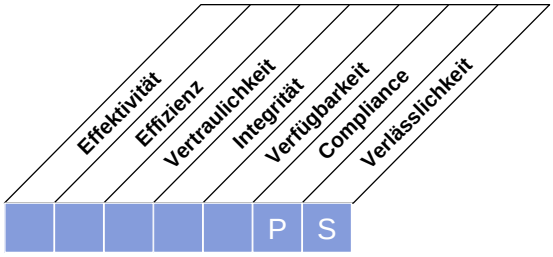
4 Managed and measurable (gemanaged und messbar):
Das Management hat ein Rahmenwerk zur Überwachung der IT Internal Controls implementiert. Das Unternehmen hat für den Überwachungsprozess der Internal Controls Toleranzgrenzen etabliert. Werkzeuge zur Standardisierung von Bewertungen und zur automatischen Erkennung von Kontrollabweichungen wurden implementiert. Eine formelle IT Internal Control-Funktion mit spezialisierten und zertifizierten Fachkräften, welche ein vom Senior Management freigegebenes formelles Control-Rahmenwerk einsetzen, ist etabliert. Fähige IT-Mitarber nehmen routinegemäß an der Bewertung von Internal Controls teil. Eine Metriken-Wissensbasis mit historischen Informationen über die Überwachung von Internal Controls ist etabliert worden. Überprüfungen der Überwachung der Internal Controls durch Experten wurden eingerichtet.

5 Optimised (optimiert):
Das Management hat ein unternehmensweites, kontinuierliches Verbesserungsprogramm etabliert, welches Erfahrungsberichte und Industry Best Practices zur Überwachung von Internal Controls berücksichtigt. Soweit angemessen, setzt das Unternehmen integrierte und aktualisierte Werkzeuge ein, welche eine wirksame Bewertung von kritischen IT-Controls sowie eine zeitnahe Erkennung von Vorfällen im Rahmen der Überwachung der IT-Controls erlauben. Die gemeinsame Nutzung des spezifischen Wissens der Informatikfunktion ist formell implementiert. Benchmarking gegen Industriestandards und Best Practices ist formalisiert.

HIGH-LEVEL CONTROL OBJECTIVE

ME3 Ensure Regulatory Compliance *(Stelle Compliance mit Vorgaben sicher)*

Eine wirksame Aufsicht erfordert die Einrichtung eines unabhängigen Review-Prozesses, um die Einhaltung von Gesetzen und Vorschriften sicherzustellen. Dieser Prozess umfasst die Definition einer Audit Charter, die Unabhängigkeit des Auditors, berufsbezogene ethische Grundlagen und Standards sowie die Planung, Durchführung, Berichterstattung und Nachverfolgung von Prüfungsaktivitäten. Das Ziel dieses Prozesses ist, in Bezug auf die IT eine positive Bestätigung der Einhaltung von Gesetzen und Vorschriften zu erhalten.



Kontrolle über den IT-Prozess,

Ensure Regulatory Compliance (*Stelle Compliance sicher*)

der die Anforderung des Unternehmens an die IT bezüglich

der Einhaltung von Gesetzen und Vorschriften

durch die Konzentration auf

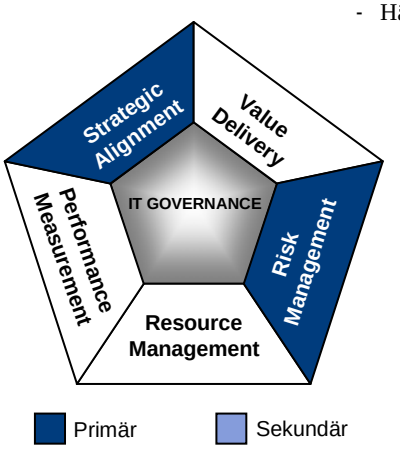
die Identifikation aller maßgeblichen Gesetze und Vorschriften und der entsprechenden Levels der IT Compliance und die Optimierung von IT Prozessen, um das Risiko der Non-Compliance zu reduzieren, *zufrieden stellt,*

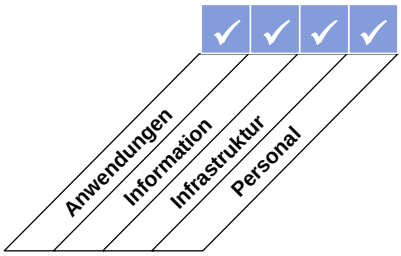
wird erreicht durch

- Identifikation von gesetzlichen und regulatorischen Anforderungen in Bezug auf die IT
- Beurteilung der Auswirkungen von regulatorischen Anforderungen
- Überwachung und Berichterstattung über die Einhaltung von regulatorischen Anforderungen

und gemessen durch

- Kosten der IT Non-Compliance, einschließlich Vergleichen und Strafen
- Durchschnittliche Zeitspanne zwischen Identifikation externer Compliance–Problemen und deren Lösung
- Häufigkeit der Compliance-Reviews





DETAILLIERTE CONTROL OBJECTIVES

ME3 Ensure Regulatory Compliance *(Stelle Compliance mit Vorgaben sicher)*

ME3.1 Identification of laws and regulations having potential impact on IT (Identifikation von Gesetzen und Regulativen mit einer potentiellen Auswirkung auf die IT)
Definiere und implementiere einen Prozess, um die zeitnahe Identifikation von lokalen und internationalen, durch Recht, Verträge, Richtlinien oder Regulative begründeten Anforderungen an Informationen, Informationserbringung (inklusive der Leistungen von Dritten) und die IT-Organisation, Prozesse und Infrastruktur, sicherzustellen. Beachte Gesetze und Vorschriften des elektronischen Handelns, Datenfluss, Datenschutz, Internal Controls, Finanzberichterstattung, industriespezifische Vorschriften, geistiges Eigentum und Urheberrecht sowie Gesundheit und Arbeitnehmersicherheit (engl.: Safety).

ME3.2 Optimisation of response to regulatory requirements (Optimierung der Reaktion auf regulatorische Anforderungen)
Reviewe und optimiere IT-Richtlinien, -Standards und -Verfahren, um sicherzustellen, dass rechtliche und regulatorische Anforderungen in wirtschaftlicher Weise abgedeckt sind.

ME3.3 Evaluation of compliance with regulatory requirements (Evaluierung der Compliance mit regulatorischen Anforderungen)
Evaluiere in wirtschaftlicher Weise – basierend auf der Governance-Übersicht und des Betriebs der Internal Controls des Unternehmens- und IT-Managements – die Einhaltung von IT-Richtlinien, Standards und Verfahren, inklusive rechtlicher und regulativer Anforderungen.

ME3.4 Positive assurance of compliance (Positive Bestätigung der Compliance)
Definiere und implementiere Verfahren, um eine positive Bestätigung der Compliance zu erhalten und darüber zu berichten – und, wo notwendig, über die rechtzeitige Einleitung von Verbesserungsmaßnahmen durch die verantwortlichen Prozesseigner zur Behandlung von Compliance-Lücken. Integriere die IT-Berichterstattung über den Fortschritt der Compliance und deren Status mit ähnlichen Ergebnissen anderer Unternehmensfunktionen.

ME3.5 Integrated reporting (Integrierte Berichterstattung)
Integriere die IT-Berichterstattung bezüglich regulativer Anforderungen mit ähnlichen Ergebnissen anderer Unternehmensfunktionen.

MANAGEMENT GUIDELINES

ME3 Ensure Regulatory Compliance *(Stelle Compliance mit Vorgaben sicher)*

Von	Inputs
*	Rechtliche und regulative Compliance-Anforderungen

* Input außerhalb COBIT

Outputs	Nach						
Katalog rechtlicher und regulatorischer Anforderungen in Bezug auf die IT-Service-Delivery	PO4	ME4					
Bericht zur Compliance der IT-Aktivitäten mit externen rechtlichen und regulatorischen Anforderungen	ME1						

RACI-CHART*

Aktivitäten \ Funktionen	Board	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Definiere einen Prozess zur Identifikation von Anforderungen aus Gesetzen, Verträgen, Richtlinien und sonstigen Regulativen und führe diesen aus					A/R	C	I	I	I	C	I	R
Evaluiere Compliance der IT-Aktivitäten mit IT-Richtlinien, Standards und Verfahren	I	I	I	I	A/R	I	R	R	R	R	R	R
Berichte die eindeutige Zusicherung, dass die IT-Aktivitäten mit IT-Richtlinien, Standards und Verfahren übereinstimmen					A/R	C	C	C	C	C	C	R
Liefere Input zum Angleichen der IT-Richtlinien, Standards und Verfahren in Reaktion auf Compliance-Erfordernisse					A/R	C	C	C	C	C		R
Integriere die IT-Berichterstattung über regulative Anforderungen mit ähnlichem Output von anderen Bereichen					A/R		I	I	I	R	I	R

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Identifikation von rechtlichen und regulatorischen Anforderungen mit Bezug auf die IT
- Training von IT-Mitarbeitern bezüglicher ihrer Verantwortung für Compliance
- Beurteilung der Auswirkungen von regulativen Anforderungen
- Überwachung und Berichterstattung über die Einhaltung der regulativen Anforderungen

treiben

Prozessziele

- Identifiziere alle maßgeblichen Gesetze und Vorschriften und identifiziere den Grad der IT-Compliance
- Sorge für das Angleichen der IT-Richtlinien, Standards und Verfahren ein, um die Risiken der Non-Compliance effizient zu managen
- Minimiere die Geschäftsauswirkung von identifizierten Compliance-Problemen innerhalb der IT

treiben

IT-Ziele

- Stelle die IT-Compliance mit Gesetzen und Vorschriften sicher

werden gemessen durch

Key Performance Indicators

- Durchschnittliche Zeitspanne zwischen Identifikation externer Compliance –Themen und deren Lösung
- Durchschnittliche Zeitspanne zwischen der Veröffentlichung eines neuen Gesetzes oder einer neuen Vorschrift und der Einleitung eines Compliance-Reviews
- Schulungstage pro IT-MitarberIn pro Jahr in Bezug auf Compliance

werden gemessen durch

Key Goal Indicators

- Anzahl der pro Jahr identifizierten, kritischen Non-Compliance Fälle
- Häufigkeit der Compliance Reviews

werden gemessen durch

IT Key Goal Indicators

- Kosten der IT Non-Compliance, einschließlich Vergleichen und Strafen
- Anzahl der Non-Compliance Fälle, die an die Geschäftsführung berichtet oder die öffentliches Aufsehen und Reaktionen hervorgerufen haben

MATURITY MODEL

ME3 Ensure Regulatory Compliance *(Stelle Compliance mit Vorgaben sicher)*

Die Reife des Management des Prozesses *Ensure Regulatory Compliance (Stelle Compliance mit Vorgaben sicher)*, der die Geschäftsanforderungen an die IT abdeckt der Einhaltung von Gesetzen und Vorschriften, ist:

0 Non-existent (nicht existent):
Es ist nur ein geringes Bewusstsein vorhanden für externe Anforderungen, welche die IT beeinflussen, und kein Prozess zur Einhaltung von regulatorischen, rechtlichen und vertraglichen Anforderungen.

1 Initial (initial):
Ein Bewusstsein für regulatorische, vertragliche und rechtliche Compliance-Anforderungen mit Einfluss auf das Unternehmen ist vorhanden. Informelle Prozesse zur Aufrechterhaltung der Compliance werden befolgt – jedoch nur dann, wenn sich die Notwendigkeit innerhalb neuer Projekte oder als Folge von Audits oder Reviews ergibt.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Ein Verständnis ist vorhanden für die Notwendigkeit, externe Anforderungen zu erfüllen; die Notwendigkeit ist kommuniziert. In Bereichen, in denen Compliance eine periodisch wiederkehrende Anforderung darstellt – wie finanz- oder datenschutzrechtliche Gesetzgebung –, wurden individuelle Compliance-Verfahren entwickelt, welche auf jährlicher Basis befolgt werden. Ein standardisierter Ansatz besteht jedoch nicht. Man verlässt sich in hohem Maße auf das Wissen und die Verantwortung von Einzelpersonen, und Fehler sind wahrscheinlich. Schulungen bezüglich externer Anforderungen und Compliance-Themen werden informell durchgeführt.

3 Defined (definiert):
Richtlinien, Verfahren und Prozesse sind entwickelt, dokumentiert und kommuniziert worden, um die Einhaltung von Richtlinien, vertraglichen oder rechtlichen Verpflichtungen sicherzustellen; aber einige werden nicht immer befolgt, andere können veraltet oder nicht praktikabel implementierbar sein. Eine Überwachung wird nur in geringem Umfang betrieben; teilweise bestehen Compliance-Anforderungen, welche nicht adressiert wurden. Schulungen in externen rechtlichen und regulatorischen Anforderungen mit Einfluss auf das Unternehmen und die definierten Compliance-Prozesse werden angeboten. Standard- (*pro forma-)* Verträge und Rechtswege zur Minimierung von Risiken, welche sich aus vertraglichen Haftungspflichten ergeben, sind vorhanden.

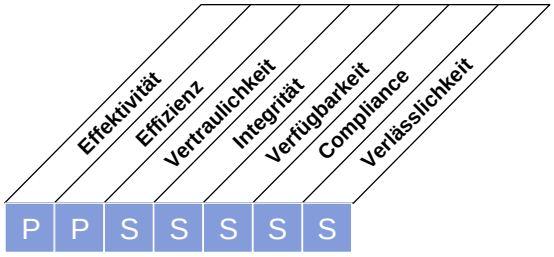
4 Managed and measurable (gemanaged und messbar):
Auf allen Ebenen besteht in umfassendes Verständnis für Sachverhalte und Gefahren in Zusammenhang mit externen Anforderungen sowie für die Notwendigkeit, Compliance sicherzustellen. Durch ein formelles Schulungsprogramm wird sichergestellt, dass sich sämtliche Mitarber ihrer Compliance-Verpflichtungen bewusst sind. Verantwortlichkeiten sind klar; Prozessverantwortlichkeiten sind verstanden. Der Prozess beinhaltet einen Review des Umfelds, um externe Anforderungen und laufende Veränderungen zu identifizieren. Mechanismen zur Überwachung der Non-Compliance mit externen Anforderungen sind im Einsatz, welche interne Praktiken sowie die Implementierung korrigierende Handlungen erzwingen. Die Ursachen von Non-Compliance-Sachverhalten werden mit dem Ziel, nachhaltige Lösungen zu identifizieren, in standardisierter Weise analysiert. Standardisierte interne Good Practices werden für spezielle Bedürfnisse wie laufende Regulierungen und wiederkehrende Serviceverträge angewendet.

5 Optimised (optimiert):
Ein wohl-organisierter, effizienter und erzwungener Prozess zur Einhaltung externer Anforderungen ist vorhanden und basiert auf einer einzelnen zentralen Funktion, die dem gesamten Unternehmen Anleitung und Koordination zur Verfügung stellt. Ausgeprägtes Wissen über anzuwendende externe Anforderungen inklusive zukünftiger Trends und antizipierter Veränderungen ist vorhanden und dem Bedarf für neue Lösungen besteht. Das Unternehmen beteiligt sich an externen Diskussionen mit Aufsichts- und Industrieverbänden, um auf das Unternehmen einwirkende externe Anforderungen zu verstehen und diese zu beeinflussen. Best Practices, welche eine effiziente Compliance mit externen Anforderungen sicherstellen, sind mit dem Ergebnis entwickelt worden, dass nur in sehr wenigen Fällen keine Compliance besteht. Ein zentrales, unternehmensweites System zur Nachverfolgung besteht, welches dem Management die Dokumentation des Workflows sowie die Messung und Verbesserung von Qualität und Wirksamkeit des Compliance-Überwachungsprozesses erlaubt. Ein Self-Assessment-Prozess in Zusammenhang mit externen Anforderungen ist implementiert und wurde bis zu einen Level von Good Practices verfeinert. Stil und Kultur des Unternehmensmanagements sind in ausreichendem Maße ausgeprägt, und die Prozesse sind so weit entwickelt, dass Schulungen auf neues Personal oder auf Fälle signifikanter Veränderungen beschränkt werden können.

HIGH-LEVEL CONTROL OBJECTIVE

ME4 Provide IT-Governance *(Sorge für IT-Governance)*

Die Einrichtung eines wirksamen Governance-Frameworks umfasst die Festlegung von Organisationsstrukturen, Prozessen, Führung, Rollen und Verantwortlichkeiten, um sicherzustellen, dass IT-Investitionen der Unternehmen an den Unternehmensstrategien und -zielen ausgerichtet sind und umgesetzt werden.



Kontrolle über den IT-Prozess,

Provide IT-Governance (*Sorge für IT-Governance*)

der die Anforderung des Unternehmens an die IT bezüglich

der Integration von IT-Governance in Corporate Governance Ziele und der Einhaltung von Gesetzen und Vorschriften

durch die Konzentration auf

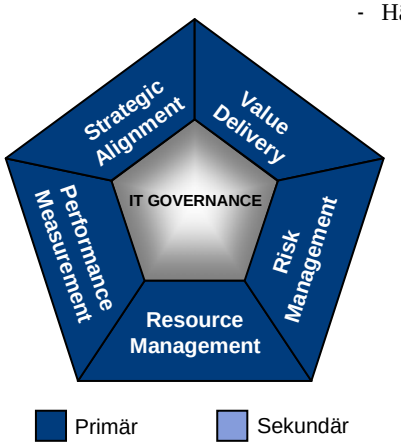
die Ausarbeitung von Geschäftsführungsreports über IT-Strategie, Performance und Risiken und das Reagieren auf Governance-Anforderungen in Übereinstimmung mit den Vorgaben der Geschäftsführung, *zufrieden stellt,*

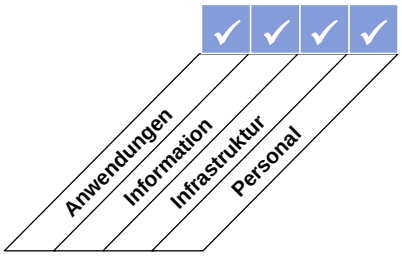
wird erreicht durch

- Erstellung eines in die Corporate Governance integrierten IT-Governance Frameworks
- Erlangung einer unabhängigen Bestätigung über den Status der IT-Governance

und gemessen durch

- Häufigkeit der Berichterstattung der Geschäftsführung an Stakeholder über die IT (einschließlich deren Reife)
- Häufigkeit der Berichterstattung von der IT an die Geschäftsführung (einschließlich deren Reife)
- Häufigkeit von unabhängigen Reviews der IT-Compliance





DETAILLIERTE CONTROL OBJECTIVES

ME4 Provide IT-Governance *(Sorge für IT-Governance)*

ME4.1 Establishment of an IT governance framework (Einführung eines IT-Governance-Frameworks)
Arbeite mit der Geschäftsleitung, um ein IT-Governance Framework festzulegen und einzurichten, das Führung, Prozesse, Rollen und Verantwortlichkeiten, Informationsbedarf und Organisationsstrukturen umfasst, um sicherzustellen, dass die IT-gestützten Investitionsprogramme des Unternehmens an den Unternehmensstrategien und -zielen ausgerichtet sind und entsprechend diesen arbeiten. Das Framework sollte eine klare Verbindung herstellen zwischen der Unternehmensstrategie, dem Portfolio von IT-gestützten Investitionsprogrammen, welche die Strategie umsetzen, den individuellen Investitionsvorhaben und den Unternehmens- und IT-Projekten, die die Programme darstellen. Das Framework sollte unmissverständliche Zuständigkeiten und Praktiken unterstützen, um einen Zusammenbruch der Internal Controls und der Aufsicht zu vermeiden. Das Framework sollte mit der unternehmensweiten Control Umgebung und allgemein akzeptierten Grundsätzen für Control konsistent sein und auf dem Framework für IT-Prozesse und Control basieren.

ME4.2 Strategic alignment (Strategische Ausrichtung)
Ermögliche der Geschäftsführung, die strategischen IT-Belange wie die Rolle der IT, technologische Einblicke und Möglichkeiten zu verstehen. Stelle sicher, dass ein gemeinsames Verständnis zwischen dem Geschäftsbereich und der IT über den potentiellen Beitrag der IT zur Unternehmensstrategie besteht. Stelle sicher, dass ein klares Verständnis darüber besteht, dass nur Wertbeitrag durch IT erzielt wird, wenn durch IT-gestützte Investitionen als ein Portfolio von Programmen gemanagt werden, das den vollen Umfang der Changes berücksichtigt, die das Unternehmen umzusetzen hat, um den Wertbeitrag für die Umsetzung der Strategie durch Potentiale der IT zu optimieren. Arbeite mit der Geschäftsleitung, um Governance-Gremien, wie einen IT-Strategieausschuss festzulegen und zu implementieren, um strategische Vorgaben an das Management in Relation zur IT zu erstellen, womit sichergestellt wird, dass die Strategie und Ziele in die Unternehmenseinheiten und die IT-Funktionen herunter gebrochen werden und dass Zuversicht und Vertrauen zwischen dem Kerngeschäft und der IT aufgebaut wird. Ermögliche die Ausrichtung der IT am Kerngeschäft in strategischer und operativer Hinsicht durch die gemeinsame Verantwortung von Kerngeschäft und IT für das Treffen strategischer Entscheidungen und dem Erzielen von Nutzen aus IT-gestützten Investitionen.

ME4.3 Value delivery (Schaffen von Werten/Nutzen)
Manage IT-gestützte Investitionsprogramme und andere Werte und Services der IT, um sicherzustellen, dass diese den höchstmöglichen Nutzen zur Unterstützung der Unternehmensstrategie und -ziele erbringen. Stelle sicher, dass der erwartete Unternehmenserfolg von IT-gestützten Investitionsprogrammen und der gesamte Umfang des Aufwands, der für die Erreichung dieses Erfolgs notwendig ist, verstanden wird, dass umfassende und konsistente Business-Cases und von Stakeholdern erstellt und freigegeben werden, dass Vermögenswerte und Investitionen über ihren gesamten wirtschaftlichen Lebenszyklus verwaltet werden und dass ein aktives Management der Realisierung des Nutzens vorhanden ist, wie zB der Wertbeitrag für neue Services, Steigerung der Wirtschaftlichkeit und verbesserte Reaktion auf Kundenanfragen. Setze einen disziplinierten Ansatz für Portfolio-, Programm- und Projektmanagement durch, bestehe darauf, dass vom Kerngeschäft die Eigentümerschaft aller IT-gestützten Investitionen übernommen wird und dass die IT eine Optimierung der Kosten für die Bereitstellung von IT-Potentialen und Services sicherstellt. Stelle sicher, dass Technologie-Investitionen so weit wie möglich standardisiert sind, um erhöhte Kosten und Komplexität eines Wildwuchses technischer Lösungen zu verhindern.

ME4.4 Resource management (Ressourcenmanagement)
Optimiere die Investitionen in IT-Vermögenswerte, deren Verwendung und Belegung durch regelmäßige Beurteilungen, die sicherstellen, dass die IT ausreichende, kompetente und fähige Ressourcen hat, um die derzeitigen und künftigen strategischen Ziele umzusetzen und mit dem Unternehmensbedarf mitzuhalten. Das Management sollte klare, konsistente und durchgesetzte Human-Ressource- und Beschaffungs-Richtlinien einsetzen, um sicherzustellen, dass Ressourcenanforderungen wirksam und entsprechend den Architektur-Richtlinien und Standards erfüllt werden. Die IT-Infrastruktur sollte in periodischen Abständen beurteilt werden, um sicherzustellen, dass sie, wo immer möglich, standardisiert ist und dass eine Interoperabilität, wo gefordert, besteht.

ME4.5 Risk management (Risikomanagement)
Arbeite mit der Geschäftsführung, um die Risikobereitschaft des Unternehmens für IT-Risiken festzulegen. Kommuniziere die IT-Risikobereitschaft im Unternehmen und vereinbare einen Plan zum IT-Risikomanagement. Bette die Verantwortlichkeiten für Risikomanagement in die Organisation ein, um sicherzustellen, dass das Unternehmen und die IT regelmäßig die IT-bezogenen Risiken und deren Auswirkungen auf das Geschäft beurteilt und darüber berichtet. Stelle sicher, dass das IT-Management drohende Risiko-Gefährdungen behandelt und eine besondere Aufmerksamkeit auf das Versagen von IT-Controls und Schwachstellen in Internal Controls und die Beaufsichtigung legt sowie auf deren tatsächliche und potentielle Auswirkungen auf die Geschäftstätigkeit. Die Haltung des Unternehmens bezüglich IT-Risiken sollte für alle Stakeholder transparent sein.

ME4.6 Performance measurement (Messung der Performance)
Berichte dem Aufsichtsrat und der Geschäftsleitung rechtzeitig und genau über relevante Portfolios, Programme und die IT-Performance. Die Managementberichte sollten für den Review der Entwicklung des Unternehmens hinsichtlich der festgelegten

Ziele durch die Geschäftsführung erstellt werden. Statusberichte sollten den Grad der Erreichung von Zielen, erstellte Ergebnisse, erreichte Performancezahlen und verminderte Risiken umfassen. Integriere die Berichterstattung mit ähnlichen Ergebnissen anderer Unternehmensfunktionen. Die Performance-Messung sollte durch die wichtigsten Stakeholder freigegeben werden. Der Aufsichtsrat und die Geschäftsleitung sollte diese Performance-Berichte hinterfragen und dem IT-Management sollte die Gelegenheit geboten werden, Abweichungen und Performance-Probleme zu erklären. Nach dem Review sollten geeignete Management-Maßnahmen initiiert und gesteuert werden.

ME4.7 Independent assurance (Unabhängige Bestätigung)
Stelle sicher, dass die Organisation eine kompetente und personell angemessen ausgestattete Funktion etabliert und betreibt und/oder sich externer Prüfungsleistungen bedient, um dem Aufsichtsrat – wahrscheinlich über ein Audit-Committee – eine zeitgerechte, unabhängige Bestätigung der Compliance der IT mit ihren Richtlinien, Standards und Verfahren sowie mit allgemein anerkannten Praktiken zu liefern.

MANAGEMENT GUIDELINES

ME4 Provide IT-Governance *(Sorge für IT-Governance)*

Von	Inputs
PO4	IT-Prozess-Framework
PO5	Kosten-/Nutzenbericht
PO9	Risikobeurteilung und –berichterstattung
ME2	Report zur Wirksamkeit von IT-Controls
ME3	Katalog rechtlicher und regulatorischer Anforderungen in Bezug auf die IT-Service-Delivery

Outputs	Nach					
Verbesserungen des Prozess-Frameworks	PO4					
Bericht zum Status der IT-Governance	PO1	ME1				
Erwarteter Wertbeitrag von IT-unterstützten Investitionen im Kerngeschäft	PO5					
Strategische Vorgaben des Unternehmens für die IT	PO1					
Unternehmensweite Risikofreudigkeit bezüglich IT-Risiken	PO9					

RACI-CHART*

Aktivitäten \ Funktionen	Geschäftsführung	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Ermögliche der Geschäftsführung die Beaufsichtigung und Erleichterung von Aktivitäten der IT	A	R	C	C	C							C
Reviewe, befürworte, koordiniere und kommuniziere IT-Performance, IT-Strategie, Ressourcen und Risikomanagement im Einklang mit der Unternehmensstrategie	A	R	I	I	R							C
Hole periodisch unabhängige Beurteilung von Performance und Compliance mit Richtlinien, Standards und Verfahren ein	A	R	C	I	C		I	I	I	I	I	R
Löse Feststellungen von unabhängigen Beurteilungen und stelle die Umsetzung des Managements vereinbarter Maßnahmen sicher	A	R	C	I	C		I	I	I	I	I	R
Erstelle einen IT Governance Report	A	C	C	C	R	C	I	I	I	I	I	C

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Erstellung eines in die Corporate Governance integrierten IT-Governance-Frameworks
- Einholung einer unabhängigen Bestätigung über den IT-Governance Status

treiben

Prozessziele

- Integriere IT-Governance in Corporate Governance-Ziele
- Erarbeite vollständige und zeitgerechte Vorstandsberichte zu IT-Strategie, Performance und Risiken
- Reagiere auf Anliegen und Anfragen des Vorstands zu IT-Strategie, Performance und Risiken
- Sorge für eine unabhängige Bestätigung in Bezug auf die Compliance mit IT-Richtlinien, Standards und Verfahren

treiben

IT-Ziele

- Reagiere auf Anforderungen der Governance entsprechend den Geschäftsführungs-vorgaben
- Stelle Transparenz und Verständnis von IT-Kosten, Nutzen, Strategie, Richtlinien und Service Levels sicher
- Stelle die IT-Compliance mit Gesetzen und Vorschriften sicher
- Stelle sicher, dass die IT eine kosteneffiziente Servicequalität, eine kontinuierliche Verbesserung und Bereitschaft für zukünftige Veränderung zeigt

werden gemessen durch

Key Performance Indicators

- % des Personals, das in Governance (zB Verhaltenskodex) geschult wurde
- Anzahl der Ethical Officers pro Abteilung
- Häufigkeit von IT-Governance als Tagesordnungspunkt in IT-Lenkungsausschuss/Strategie-Meetings
- % der Vorstandsmitglieder, die in IT-Governance geschult sind oder damit Erfahrung haben
- Altersanalyse der vereinbarten Empfehlungen
- Häufigkeit der Berichterstattung an den Vorstand über Erhebungen zur Stakeholder-Zufriedenheit

werden gemessen durch

Key Goal Indicators

- Häufigkeit der Berichterstattung der IT an den Vorstand (einschließlich deren Reife)
- Anzahl der Governance-Verstöße
- Häufigkeit von unabhängigen Reviews der IT-Compliance

werden gemessen durch

IT Key Goal Indicators

- Häufigkeit, dass IT proaktiv auf der Tagesordnung einer Vorstandssitzung steht
- Häufigkeit der Vorstandsberichterstattung über die IT an Stakeholders (einschließlich Reifegrad)
- Anzahl wiederkehrender IT Themen auf der Tagesordnung von Vorstandssitzungen

MATURITY MODEL

ME4 Provide IT-Governance *(Sorge für IT-Governance)*

Die Reife des Management des Prozesses *Provide IT-Governance (Sorge für IT-Governance)*, der die Geschäftsanforderungen an die IT erfüllt der Integration von IT-Governance in Corporate Governance Ziele und der Einhaltung von Gesetzen und Vorschriften, ist:

0 Non-existent (nicht existent):
Es besteht kein einziger erkennbarer IT-Governance-Prozess. Das Unternehmen hat nicht einmal erkannt, dass man sich um dieses Thema kümmern sollte; daher wird dieser Sachverhalt nicht kommuniziert.

1 Initial (initial):
Es wurde erkannt, dass IT-Governance-Sachverhalte existieren und zu adressieren sind. *Ad hoc*-Ansätze kommen individuell oder fallbezogen zur Anwendung. Der Ansatz des Managements ist reaktiv – und es besteht lediglich eine sporadische, inkonsistente Kommunikation über solche Sachverhalte und Ansätze zu ihrer Adressierung. Das Management besitzt lediglich ungefähre Vorstellungen darüber, welchen Beitrag die IT zur Performance des Unternehmens leistet. Das Management reagiert lediglich rückwirkend auf Vorfälle, die Verlust oder Aufsehen für das Unternehmen verursachten.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Ein Bewusstsein für IT-Governance-Sachverhalte ist vorhanden. Indikatoren für IT-Governance-Aktivitäten und -Performance, welche Prozesse der IT-Planung, -Verteilung und -Überwachung abdecken, befinden sich in der Entwicklung. Ausgewählte IT-Prozesse sind auf der Grundlage von Einzelentscheidungen als verbesserungswürdig identifiziert worden. Das Management hat elementare Methoden und Techniken zur Messung und Bewertung von IT-Governance identiziert; dieser Prozess wurde nicht unternehmensweit adaptiert. Die Kommunikation über Standards und Verantwortlichkeiten für Governance obliegt einzelnen Personen. Einzelpersonen betreiben Governance-Prozesse innerhalb verschiedener IT-Projekte und -Prozesse. Auf Grund fehlender Expertise über deren Funktionalität sind die Prozesse, Werkzeuge und Metriken zur Messung von IT-Governance nur beschränkt und können nicht in vollem Umfang eingesetzt werden.

3 Defined (definiert):
Die Wichtigkeit und Notwendigkeit von IT-Governance werden vom Management verstanden und innerhalb des Unternehmens kommuniziert. Ein Grundlagengerüst von IT-Governance-Indikatoren ist entwickelt; Verknüpfungen zwischen Ergebnismaßen und Performance-Treibern sind festgehalten und dokumentiert. Die Verfahren wurden standardisiert und dokumentiert. Das Management hat die standardisierten Verfahren kommuniziert; Schulungen sind etabliert. Werkzeuge zur Unterstützung der Beaufsichtigung von IT-Governance wurden identifiziert. Dashboards wurden als Teil der IT-Balanced-Business-Scorecard definiert. Jedoch sind die Teilnahme an Schulungen sowie die Einhaltung und Anwendung von Standards dem Einzelnen überlassen. Prozesse werden vielleicht überwacht. Es ist jedoch unwahrscheinlich, dass Abweichungen – obwohl darauf in der Regel aufgrund einzelner Initiativen gehandelt wird – durch das Management entdeckt werden.

4 Managed and measurable (gemanaged und messbar):
Auf allen Ebenen besteht ein umfassendes Verständnis für IT-Governance-Sachverhalte. Es besteht ein klares Verständnis, wer der Kunde ist, und Verantwortlichkeiten sind festgehalten und werden im Rahmen von Service Level Agreements überwacht. Verantwortlichkeiten sind klar; Prozess-Ownership ist etabliert. IT-Prozesse und IT-Governance sind ausgerichtet an und integriert in die Geschäfts- bzw die IT-Strategie. Verbesserungen innerhalb der IT-Prozesse basieren primär auf einem quantitativen Verständnis und es ist möglich, Compliance mit Hilfe von Verfahrens- und Prozessmetriken zu überwachen und zu messen. Sämtliche Stakeholder von Prozessen sind sich der Risiken, der Wichtigkeit der IT und der Möglichkeiten, welche sich daraus bieten, bewusst. Das Management hat Toleranzgrenzen festgelegt, innerhalb denen die Prozesse zu betreiben sind. Der Technologie-Einsatz ist primär taktisch, beschränkt und basiert auf ausgereiften Techniken und erzwungenen Standardwerkzeugen. IT-Governance ist in die strategischen und operativen Planungs- und Überwachungsprozesse integriert worden. Performance Indicators werden für alle IT-Governance-Aktivitäten aufgezeichnet und verfolgt und führen zu unternehmensweiten Verbesserungen. Die Gesamtverantwortung für die Key Process Performance ist klar; das Management wird auf der Grundlage von Key-Performance-Maßen entschädigt.

5 Optimised (optimiert):
Ein fortschrittliches und zukunftsgerichtetes Verständnis für IT-Governance-Sachverhalte und -Lösungen ist vorhanden. Schulung und Kommunikation werden durch erstklassige Konzepte und Techniken unterstützt. Auf der Grundlage der Ergebnisse kontinuierlicher Verbesserung und Maturity Modelling mit anderen Unternehmen wurden die vorhandenen Prozesse auf das Niveau von Industry Best Practice verfeinert. Die Implementierung von IT-Richtlinien hat dazu geführt, dass Organisation, Mitarber und Prozesse in der Lage sind, neue IT-Governance-Vorgaben zeitnah zu adaptieren und diese vollständig zu unterstützen. Bei sämtlichen Problemen und Abweichungen werden Analysen der grundlegenden Ursachen durchgeführt und effiziente Maßnahmen zweckdienlich identifiziert und eingeleitet. Die IT wird in umfassender, integrierter und optimierter Weise zur Automatisierung des Workflows eingesetzt und stellt Werkzeuge zur Verbesserung der Qualität und Wirksamkeit zur Verfügung. Die Risiken und Erträge der IT-Prozesse werden unternehmensübergreifend festgelegt, abgestimmt und kommuniziert. Externe Experten werden wirksam eingesetzt und Benchmarks zur Lenkung verwendet. Überwachung, Self-Assessment und Kommunikation über Governance-Erwartungen haben das Unternehmen durchdrungen; Technologien werden optimal eingesetzt zur Unterstützung von Messungen, Analysen, Kommunikation und Schulung. Corporate Governance und IT-

Governance sind strategisch verknüpft, um durch einen wirksamen Einsatz der technologischen, personellen und finanziellen Ressourcen die Wettbewerbsvorteile des Unternehmens zu steigern. IT-Governance-Aktivitäten sind in den Governance-Prozess des Unternehmens integriert.

ANHANG I

VERBINDUNG VON UNTERNEHMENSZIELEN IT-ZIELEN

Dieser Anhang bietet eine Übersicht, wie generische Unternehmensziele mit IT-Zielen, IT-Prozessen und Information Criteria in Verbindung stehen. Er besteht aus drei Tabellen:

1. Die erste Tabelle verbindet Unternehmensziele, die entsprechend einer Balanced-Scorecard gruppiert sind, mit den IT-Zielen und den Information Criteria. Dies hilft, um für ein vorgegebenes, generisches Unternehmensziel jene IT-Ziele, die normalerweise dieses Ziel unterstützen, und die COBIT Information Criteria, die mit diesem Unternehmensziel verbunden sind, darzustellen.
2. Die zweite Tabelle verbindet IT-Ziele mit den COBIT IT-Prozessen und den Information Criteria, auf denen das (jeweilige) Ziel basiert.
3. Die dritte Tabelle zeigt für alle IT-Prozesse als umgekehrte Verbindung die unterstützten IT-Ziele.

Die Tabellen helfen, den Umfang von COBIT und die gesamthafte, unternehmensorientierte Beziehung zwischen COBIT und den Treibern des Unternehmens aufzuzeigen, in dem typische Unternehmensziele über IT-Ziele mit den IT-Prozessen, die zu ihrer Unterstützung nötig sind, verbunden werden. Die Tabellen basieren auf generischen Zielen und sollten demzufolge als eine Anleitung verwendet und an das jeweilige Unternehmen angepasst werden.

Um mit älteren Versionen der in COBIT 3rd Edition für die Geschäftsanforderungen verwendeten Information Criteria abwärtskompatibel zu sein, enthalten die Tabellen auch Hinweise zu den wichtigsten Information Criteria, welche durch die Unternehmens- und IT-Ziele unterstützt werden.

Anmerkungen:
Die Information Criteria der Tabelle mit den Unternehmenszielen basieren auf einer Zusammenfassung der Kriterien der zugehörigen IT-Ziele und einer subjektiven Beurteilung der Kriterien, die für die Unternehmensziele am relevantesten sind. Es wurde keine Unterscheidung in primäre oder sekundäre Zusammenhänge getroffen. Die Zusammenhänge haben einen rein indikativen Charakter und Anwender sollten einen analogen Prozess zur Beurteilung der eigenen Unternehmensziele wählen.
2. Die primären und sekundären Zusammenhänge der Information Criteria der Tabelle IT-Ziele basieren auf einer Zusammenfassung der Kriterien für jeden IT-Prozess und einer subjektiven Beurteilung, was für das IT-Ziel primär und sekundär ist – da manche Prozesse mehr Auswirkungen auf die IT-Ziele haben als andere. Sie besitzen folglich rein indikativen Charakter und Anwender sollten einen analogen Prozess zur Beurteilung der eigenen IT-Ziele wählen.

VERBINDUNG VON UNTERNEHMENSZIELEN UND IT ZIELEN

		Unternehmensziele	IT Ziele								Effektivität	Effizienz	Vertraulichkeit	Integrität	Verfügbarkeit	Compliance	Verlässlichkeit
Finanz-perspektive	1	Marktanteil erhöhen	25	28							✓	✓					
	2	Erträge erhöhen	25	25							✓	✓					
	3	Rendite	24									✓					
	4	Kapitalverwertung optimieren	14								✓	✓					
	5	Geschäftsrisiken managen	2	14	17	18	19	20	21	22			✓	✓	✓		
Kunden-perspektive	6	Kunden- und Serviceorientierung erhöhen	3	23							✓						
	7	Kostengünstige Produkte und Services anbieten	5	24							✓	✓					
	8	Verfügbarkeit von Services	10	16	22	23					✓				✓		
	9	Agilität bei Reaktion auf sich ändernde Geschäftsanforderungen (time to market)	1	5	25						✓	✓					
	10	Kostenoptimierung bei Serviceerbringung	7	8	10	24						✓					
Interne Perspektive	11	Automatisierung und Integration der Wertschöpfungskette	6	7	8	11					✓	✓					
	12	Geschäftsprozess überarbeiten und verbessern	6	7	8	11					✓	✓					
	13	Prozesskosten reduzieren	7	8	13	15	24					✓					
	14	Compliance mit Gesetzen und Regulativen	2	19	20	21	22	26	27				✓			✓	
	15	Transparenz	2	18													✓
	16	Compliance mit internen Regelungen	2	13									✓			✓	
	17	Betriebliche- und Mitarbeiterproduktivität steigern	7	8	11	13					✓	✓					
Lern- und Wachstums-perspektive	18	Produkt-/Geschäftsinovation	5	25	28						✓	✓					
	19	Verlässliche und nützliche Informationen für strategische Entscheidungen erlangen	2	4	12	20	26				✓			✓			✓
	20	Qualifizierte und motivierte MitarbeiterInnen einstellen und entwickeln	9								✓	✓					

VERBINDUNG VON IT ZIELEN UND IT PROZESSEN

IT Ziele		Prozesse										Effektivität	Effizienz	Vertraulichkeit	Integrität	Verfügbarkeit	Compliance	Verlässlichkeit
1	Reagiere auf Geschäftsanforderungen in Übereinstimmung mit der Unternehmensstrategie	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1	P	P		S	S		
2	Reagiere auf Anforderungen der Governance entsprechend der Geschäftsführungs-vorgaben	PO1	PO4	PO10	ME1	ME3						P	P					
3	Stelle die Enduser-Zufriedenheit mit den Serviceangeboten und Service Levels sicher	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13			P	P		S	S		
4	Optimiere die Verwendung von Information	PO2	DS11										S		P			S
5	Stelle IT-Agilität her	PO2	PO4	PO7	AI3							P	P		S			
6	Definiere, wie funktionale geschäftliche und Steuerungsanforderungen in wirksame und wirtschaftliche automatisierte Lösungen überführt werden.	AI1	AI2	AI6								P	P				S	
7	Beschaffe und unterhalte integrierte und standardisierte Anwendungssysteme	PO3	AI2	AI5								P	P				S	
8	Beschaffe und warte integrierte und standardisierte IT-Infrastruktur	AI3	AI5									S	P					
9	Beschaffe und erhalte IT-Skills, die der IT-Strategie entsprechen	PO7	AI5									P	P					
10	Stelle die gegenseitig zufriedenstellenden Lieferantenbeziehungen sicher	DS2										P	P	S	S	S	S	S
11	Integriere die Anwendungen und Technologielösungen nahtlos in Geschäftsprozesse	PO2	AI4	AI7								P	P		S	S		
12	Stelle Transparenz und Verständnis von IT -Kosten, Nutzen, Strategie, Richtlinien und Service Levels sicher	PO5	PO6	DS1	DS2	DS6	ME1	ME4				P	P				S	S
13	Stelle die angemessene Verwendung und Performance der Anwendungen und technischen Lösungen sicher	PO6	AI4	AI6	AI7	DS7	DS8					P	S					
14	Übernimm die Verantwortung für und schütze alle IT-Anlagen	PO9	DS5	DS9	DS12	ME2						S	S	P	P	P	S	S
15	Optimiere IT-Infrastruktur, Ressourcen und Fähigkeiten	PO3	AI3	DS3	DS7	DS9						S	P					
16	Reduziere Mängel und Nacharbeit bei Lösungen und dem Servicebetrieb	PO8	AI4	AI6	AI7	DS10						P	P		S	S		
17	Schütze die Erreichung der IT-Ziele	PO9	DS10	ME2								P	P	S	S	S	S	S
18	Schaffe Klarheit über die Geschäftsauswirkungen der Risiken von IT-Zielen und -Ressourcen	PO9										S	S	P	P	P	S	S
19	Stelle den Schutz von kritischen und vertraulichen Informationen vor unberechtigtem Zugriff sicher	PO6	DS5	DS11	DS12									P	P	S	S	S
20	Stelle sicher, dass automatischen Transaktionen und Informationsaustausch vertraut werden kann	PO6	AI7	DS5								P			P	S	S	
21	Stelle sicher, dass IT-Services und Infrastruktur Ausfällen auf Grund von Fehlern, bewussten Angriffen oder Katastrophen standhalten können und ihre Wiederherstellung gewährleistet ist	PO6	AI7	DS4	DS5	DS12	DS13	ME2				P	S		S	P		
22	Stelle sicher, dass der Einfluss einer IT-Service-Störung oder -Änderung auf das Geschäft minimiert ist	PO6	AI6	DS4	DS12							P	S		S	P		
23	Stelle die Verfügbarkeit der IT-Services gemäß den Anforderungen sicher	DS3	DS4	DS8	DS13							P	P			P		
24	Verbessere die Kosteneffizienz der IT und ihren Beitrag zum Unternehmenserfolg	PO5	AI5	DS6								S	P					S
25	Setze Projekte pünktlich und im Budgetrahmen und unter Einhaltung der Qualitätsstandards um	PO8	PO10									P	P		S			S
26	Erhalte die Integrität der Informationen und die diese Informationen verarbeitende Infrastruktur	AI6	DS5									P	P		P	P		S
27	Stelle die IT-Compliance mit Gesetzen und Vorschriften sicher	DS11	ME2	ME3	ME4										S		P	S
28	Stelle sicher, dass die IT eine kosteneffiziente Servicequalität, eine kontinuierliche Verbesserung und Bereitschaft für zukünftige Veränderung zeigt	PO5	DS6	ME1	ME3							P	P					P

IT PROZESSE UND IT ZIELE

IT Ziele	1 Reagiere auf Geschäftsanforderungen in Übereinstimmung mit der Unternehmensstrategie	2 Reagiere auf Anforderungen der Governance entsprechend der Geschäftsführungsvorgaben	3 Stelle die Enduser-Zufriedenheit mit den Serviceangeboten und Service Levels sicher	4 Optimiere die Verwendung von Information	5 Stelle IT-Agilität her	6 Definiere, wie funktionale plezifische und Steuerungsanforderungen in wirksame und wirtschaftliche automatisierte Lösungen überführt werden	7 Beschaffe und warte integriere und standardisiere Anwendungssysteme	8 Beschaffe und warte integriere und standardisierte IT-Infrastruktur	9 Beschaffe und erhalte IT-Skills, die der IT-Strategie entsprechen	10 Stelle die gegenseitig zufriedenstellenden Lieferantenbeziehungen sicher	11 Integriere die Anwendungen und Technologielösungen nahtlos in Geschäftsprozesse	12 Stelle Transparenz und Verständnis von IT -Kosten, Nutzen, Strategie, Risiken und Service Levels	13 Stelle die angemessene Verwendung und Performance der Anwendungen und technischen Lösungen sicher	14 Überprüfe die Verwaltung für und Schütze alle IT-Anlagen	15 Optimiere IT-Infrastruktur, Ressourcen und Fähigkeiten	16 Reduziere Mängel und Nachahbel bei Lösungen und dem Serviceteam	17 Schütze die Erreichung der IT-Ziele	18 Schaffe Klarheit über die Geschäftsauswirkungen der Risiken von IT-Zielen und -Ressourcen	19 Stelle den Schutz von kritischen und vertraulichen Informationen vor unberechtigtem Zugriff sicher	20 Stelle sicher, dass automatischen Transaktionen und Informationsaustausch vertraut werden kann	21 Stelle sicher, dass IT-Services und Infrastruktur Ausfällen auf Grund von Fehlern bewussten Angriffen oder Katastrophen standhalten können und ihre Wiederherstellung gewährleistet ist	22 Stelle sicher, dass bei Eintritt einer IT-Service-Störung oder Änderung auf das Geschäft minimiert ist	23 Stelle die Verfügbarkeit der IT-Services gemäß den Anforderungen sicher	24 Verbessere die Kosteneffizienz der IT und ihren Beitrag zum Unternehmenserfolg	25 Setze Projekte priorisiert und im Budgetrahmen und unter Einhaltung der Qualitätsstandards um	26 Erhalte die Integrität der Informationen und die diese Informationen verarbeitende Infrastruktur	27 Stelle die IT-Compliance mit Gesetzen und Vorschriften sicher	28 Stelle sicher, dass die IT eine kosteneffiziente Servicequalität, eine kontinuierliche Verbesserung und Benutzerzufriedenheit mit zukünftiger Vereinbarung regt
PO1 Define a Strategic IT Plan (Definiere einen strategischen IT Plan)	✔	✔																									
PO2 Define the Information Architecture (Definiere die Informationsarchitektur)	✔			✔	✔						✔																
PO3 Determine Technological Direction (Bestimme die technologische Richtung)							✔							✔													
PO4 Define the IT Processes, Organisation and Relationships (Definiere die IT Prozesse, Organisation und Beziehungen)	✔	✔																									
PO5 Manage the IT Investment (Manage IT Investitionen)											✔											✔					✔
PO6 Communicate Management Aims and Direction (Kommuniziere Ziele und Richtung des Managements)											✔	✔						✔	✔	✔	✔						
PO7 Manage IT Human Resources (Manage die IT-Human-Ressourcen)					✔			✔																			
PO8 Manage Quality (Manage Qualität)			✔												✔									✔			
PO9 Assess and Manage IT Risks (Beurteile und Manage IT Risiken)													✔			✔	✔										
PO10 Manage Projects (Manage Projekte)	✔	✔																						✔			
AI1 Identify Automated Solutions (Identifiziere automatisierte Lösungen)	✔					✔	✔																				
AI2 Acquire and Maintain Application Software (Beschaffe und warte Anwendungssoftware)						✔																					
AI3 Acquire and Maintain Technology Infrastructure (Beschaffe und warte technologische Infrastruktur)					✔			✔						✔													
AI4 Enable Operation and Use (Ermögliche Betrieb und Verwendung)			✔							✔		✔			✔												
AI5 Procure IT Resources (Beschaffe IT Ressourcen)							✔	✔	✔															✔			
AI6 Manage Changes (Manage Changes)	✔					✔						✔			✔										✔		
AI7 Install and Accredit Solutions and Changes (Installiere und akkreditiere Solutions und Changes)	✔									✔		✔			✔					✔	✔	✔					
DS1 Define and Manage Service Levels (Definiere und manage Service Levels)	✔		✔								✔																
DS2 Manage Third-party Services (Manage Leistungen von Dritten)			✔						✔		✔																
DS3 Manage Performance and Capacity (Manage Performance und Kapazität)	✔													✔									✔				
DS4 Ensure Continuous Service (Stelle den kontinuierlichen Betrieb sicher)																			✔	✔	✔	✔	✔				
DS5 Ensure Systems Security (Stelle Security von Systemen sicher)													✔					✔	✔						✔		
DS6 Identify and Allocate Costs (Identifiziere und verrechne Kosten)											✔												✔				✔
DS7 Educate and Train Users (Schule und trainiere User)			✔									✔		✔													
DS8 Manage Service Desk and Incidents (Manage den Service Desk und Incidents)			✔									✔											✔				
DS9 Manage the Configuration (Manage die Konfiguration)													✔	✔													
DS10 Manage Problems (Manage Probleme)			✔													✔	✔										
DS11 Manage Data (Manage Daten)				✔														✔								✔	
DS12 Manage the Physical Environment (Manage die physische Umgebung)													✔					✔	✔	✔	✔						
DS13 Manage Operations (Manage den Betrieb)			✔																✔			✔					
ME1 Monitor and Evaluate IT Performance (Monitore und evaluiere IT Performance)	✔	✔									✔																✔
ME2 Monitor and Evaluate Internal Control (Monitore und evaluiere Internal Controls)													✔			✔			✔							✔	
ME3 Ensure Regulatory Compliance (Stelle Compliance sicher)		✔									✔															✔	✔
ME4 Provide IT Governance (Sorge für IT Governance)																										✔	

Anhang II

Mapping von IT-Prozessen zu den Kernbereichen der IT-Goverannce, COSO, CobiT IT-Ressourcen und CobiT Information Criteria

Dieser Anhang umfasst ein Mapping zwischen den CobiT IT-Prozessen und den fünf Kernbereichen der IT-Governance, den Komponenten von COSO, IT-Ressourcen und den Information Criteria. Die Tabelle zeigt auch die relative Bedeutung der Prozesse (hoch, mittel, gering), die auf einem Benchmarking über CobiT Online-basiert. Diese Matrix zeigt auf einer Seite und auf hoher Abstraktionsebene, wie das CobiT-Framework Anforderungen an IT-Governance und von COSO adressiert und zeigt die Verknüpfung zwischen den IT-Prozessen, IT-Ressourcen und den Information Criteria. P wird verwendet, wenn es eine starke Beziehung, und S, wenn es eine schwache Beziehung gibt. Kein P und kein S bedeutet nicht, dass keinerlei Beziehung besteht, sondern dass sie weniger wichtig oder marginal ist. Die Bedeutungs-Werte basieren auf einer Befragung und auf Expertenmeinung uns sollten nur als Hinweis verstanden werden. Anwender der Tabellen sollten überlegen, welche Prozesse in der eigenen Organisation wichtig sind.

MAPPING VON IT PROZESSEN ZU DEN KERNBEREICHEN DER IT GOVERNANCE, COSO, COBIT IT RESSOURCEN UND INFORMATION CRITERIA

		IT Governance Kernbereiche					COSO					COBIT IT Ressourcen				CobiT Information Criteria						
	Bedeutung	Strategic Alignment	Value Delivery	Resource Management	Risk Management	Performance Measurement	Personal	Value Delivery	Resource Management	Risk Management	Performance Measurement	Personal	Information	Anwendungen	Infrastruktur	Effektivität	Effizienz	Vertraulichkeit	Integrität	Verfügbarkeit	Compliance	Verlässlichkeit
Plan and Organise (Plane und organisiere)																						
PO1 Define a Strategic IT Plan (Definiere einen strategischen IT Plan)	K	P		S	S			P		S	S	✓	✓	✓	✓	P	S					
PO2 Define the Information Architecture (Definiere die Informationsarchitektur)	G	P	S	P	S				P	P			✓	✓		S	P	S	P			
PO3 Determine Technological Direction (Bestimme die technologische Richtung)	M	S	S	P	S			S	P	S				✓	✓	P	P					
PO4 Define the IT Processes, Organisation and Relationships (Definiere die IT Prozesse, Organisation und Beziehungen)	G	S		P	P		P			S	S	✓				P	P					
PO5 Manage the IT Investment (Manage IT Investitionen)	M	S	P	S		S		S	P			✓		✓	✓	P	P					S
PO6 Communicate Management Aims and Direction (Kommuniziere Ziele und Richtung des Managements)	M	P			P		P		P			✓	✓			P					S	
PO7 Manage IT Human Resources (Manage die IT-Human-Ressources)	G	P		P	SS	S	P		S			✓				P	P					
PO8 Manage Quality (Manage Qualität)	M	P	S		S		P		P	S	P	✓	✓	✓	✓	P	P		S			S
PO9 Assess and Manage IT Risks (Beurteile und Manage IT Risiken)	H	P			P			P				✓	✓	✓	✓	S	S	P	P	S	S	S
PO10 Manage Projects (Manage Projekte)	H	P	S	S	S	S	S	S	P		S	✓		✓	✓	P	P					
Acquire and Implement (Beschaffe und Implementiere)																						
AI1 Identify Automated Solutions (Identifiziere automatisierte Lösungen)	M	P	P	S	S				P					✓	✓	P	S					
AI2 Acquire and Maintain Application Software (Beschaffe und warte Anwendungssoftware)	M	P	P		S				P					✓		P	P		S		S	
AI3 Acquire and Maintain Technology Infrastructure (Beschaffe und warte technologische Infrastruktur)	G			P					P						✓	S	P		S	S		
AI4 Enable Operation and Use (Ermögliche Betrieb und Verwendung)	G	S	P	S	S				P	S		✓		✓	✓	P	P		S	S	S	S
AI5 Procure IT Resources (Beschaffe IT Ressourcen)	M		S	P					P			✓	✓	✓	✓	S	P				S	
AI6 Manage Changes (Manage Changes)	H		P	S				S	P		S	✓	✓	✓	✓	P	P		P	P		S
AI7 Install and Accredit Solutions and Changes (Installiere und akkreditiere Solutions und Changes)	M	S	P	S	S	S			P	S	S	✓	✓	✓	✓	P	S		S	S		
Deliver and Support (Erbringe und Unterstütze)																						
DS1 Define and Manage Service Levels (Definiere und manage Service Levels)	M	P	P	P		P	S		P	S	S	✓	✓	✓	✓	P	P	S	S	S	S	S
DS2 Manage Third-party Services (Manage Leistungen von Dritten)	G		P	S	P	S	P	S	P		S	✓	✓	✓	✓	P	P	S	S	S	S	S
DS3 Manage Performance and Capacity (Manage Performance und Kapazität)	G	S	S	P	S	S			P		S			✓	✓	P	P			S		
DS4 Ensure Continuous Service (Stelle den kontinuierlichen Betrieb sicher)	M	S	P	S	P	S	S		P	S		✓	✓	✓	✓	P	S			P		
DS5 Ensure Systems Security (Stelle Security von Systemen sicher)	H				P				P	S	S	✓	✓	✓	✓			P	P	S	S	S
DS6 Identify and Allocate Costs (Identifiziere und verrechne Kosten)	G		S	P		S			P			✓	✓	✓	✓		P					P
DS7 Educate and Train Users (Schule und trainiere User)	G	S	P		S		P			S		✓				P	S					
DS8 Manage Service Desk and Incidents (Manage den Service Desk und Incidents)	G	S	P			S	S			P	P	✓		✓		P	P					
DS9 Manage the Configuration (Manage die Konfiguration)	M		P		S				P				✓	✓	✓	P	S			S		S
DS10 Manage Problems (Manage Probleme)	M		P		S				P	S	S	✓	✓	✓	✓	P	P			S		
DS11 Manage Data (Manage Daten)	H		P	P	P				P				✓						P			P
DS12 Manage the Physical Environment (Manage die physische Umgebung)	G			S	P			S	P						✓				P	P		
DS13 Manage Operations (Manage den Betrieb)	G			P					P	S		✓	✓	✓	✓	P	P		S	S		
Monitor and Evaluate (Monitore und evaluiere)																						
ME1 Monitor and Evaluate IT Performance (Monitore und evaluiere IT Performance)	H					P				S	P	✓	✓	✓	✓	P	P	S	S	S	S	S
ME2 Monitor and Evaluate Internal Control (Monitore und evaluiere Internal Controls)	M		P		P						P	✓	✓	✓	✓	P	P	S	S	S	S	S
ME3 Ensure Regulatory Compliance (Stelle Compliance sicher)	H	P			P				P	S	S	✓	✓	✓	✓						P	S
ME4 Provide IT Governance (Sorge für IT Governance)	H	P	P	P	P	P	P	S		S	P	✓	✓	✓	✓	P	P	S	S	S	S	S

Anmerkung: Das Mapping zu COSO basiert auf dem originalen Framework von COSO. Es ist aber ebenso für das später erschienene COSO Enterprise Risk Management-Integrated Framework anwendbar, welches sich auf Internal Control bezieht und eine stabilere und umfangreichere Diskussion des weiten Themenbereichs des ERM enthält. Nachdem es weder das originale Framework ersetzt, noch eine derartige Absicht besteht, sondern eher das Internal Control Framework erweitert, können Anwender von CobiT wählen, ob sie dieses ERM framework verwenden wollen, um sowohl die Erfordernisse für Internal Control, als auch die künftige Behandlung von Risk-Management-Prozessen zu gewährleisten.

ANHANG III

REIFEGRADMODELL FÜR INTERNAL CONTROL

Dieses Reifegeradmodell wurde nicht übersetzt, da dieses derzeit vom ITGI überarbeitet wird. Weitere Informationen finden Sie unter
www.isaca.org

Anhang IV

Hauptsächliche Quellen, die für CobiT 4.0 verwendet wurden

CobiT Anhang IV

Für frühere Entwicklungen und Erweiterungen von CobiT wurde eine breite Basis von mehr als 40 internationalen detaillierten IT-Standards, Frameworks, Guidelines und Best Practices verwendet, um die Vollständigkeit von CobiT sicherzustellen,alle Bereiche von IT-Governance und Steuerung zu berücksichtigen.

Nachdem sich CobiT darauf konzentriert, WAS erforderlich ist, um angemessenes Management und Steuerung der IT zu erreichen, ist es auf hoher Ebene positioniert. Die detaillierteren IT-Standards und Best Practices sind weniger detailliert und beschreiben, WIE spezifische Aspekte der IT gemanagt und gesteuert werden. CobiT agiert als der Integrator dieser unterschiedlichen Wegleitungs-Materialen, in dem es die wichtigsten Ziele unter einem übergeordneten Framework zusammenfasst, das auch auf die Geschäfts- und Governance-Anforderungen verweist.

Für das Update von CobiT (CobiT 4.0) wurde auf sechs wesentliche, weltweite IT-Standards, Frameworks und Practices fokussiert, die als die wichtigsten Basisreferenzen verwendet wurden, um eine geeignete Abdeckung, Konsistenz und Ausrichtung sicherzustellen. Diese sind:

- Committee of Sponsoring Organisations of the Treadway Commission (COSO):
  - *Internal Control—Integrated Framework*, 1994
  - *Enterprise Risk Mangement—Integrated Framework*, 2004
- Office of Government Commerce (OGC®):
  - *IT Infrastructure Library® (ITIL®), 1999-2004*
- International Organisation for Standardisation:
  - *ISO/IEC 17799:2005, Code of Practice for Information Security Management*
- Software Engineering Institute (SEI®):
  - *SEI Capability Maturity Model (CMM®), 1993*
  - *SEI Capability Maturity Model Integration (CMMI®), 2000*
- Project Management Institute (PMI®):
  - Project Management Body of Knowledge (PMBOK®), 2000
- Information Security Forum (ISF):
  - The Standard of Good Practice for Information Security, 2003