Projektbericht
Thema: COBIT

Alexander Wegner, Marius Ciepluch

17. Dezember 2011

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

1.1 Executive Summary

- COBIT steht für „Control Objectives for Information and Related Technology“. Es handelt sich um ein IT Governance Framework, das sich nicht der Art der Umsetzung widmet, sondern definiert welche Objekte umgesetzt werden müssen.
- es ist ein Mittel zum Aufbau von Kontrollstrukturen in Unternehmen, das einen Top Down Steuerungsansatz benutzt. Die Control Objectives sind dazu über 4 Domänen (insgesamt 34 IT Prozesse) verteilt.
- COBIT kann in Unternehmen in Phasen etabliert werden - in verschiedenen Maturity Levels.
- Innerhalb des Einsatzes können die Kontrollstrukturen verbessert werden um die Effizienz von Unternehmensprozessen durch die gewonnen Erkenntnisse zu steigern. Dies geschieht über die Rückkopplung von Erkenntnissen über die verschiedenen Domänen. Um dies zu verdeutlichen wurden im folgenden Bericht die Domänen-Schnittstellen visualisiert.
- COBIT wird benutzt um auf strukturierte Weise Governance in Unternehmen aufzubauen
- es wird COBIT in der aktuellen Version 4.1 (Ende 2011) betrachtet. Version 5 des Frameworks befindet sich noch in aktiver Entwicklung.

1.2 Ersteller des Berichts

Der Bericht wurde durch die in Tabelle 1.2.1 aufgeführten Studentinnen und Studenten erstellt. Jeder bearbeitete hauptverantwortlich zwei Domänen.

Autor	MatrNr	Inhaltliche Verantwortung
Alexander Wegner	123456	PO1 - PO10, A11-A17,
Marius Ciepluch	654321	DS1 - DS13, ME1 - ME4
beide	Gruppe 8	Einleitung, Korrektur, Zusammenfassungen, Koordination

Tabelle 1.2.1: Ersteller des Berichts

Kapitel 2

Allgemeines zu COBIT

Im Folgenden allgemeinen Abschnitt werden diese Fragen beantwortet:

1. Wann sollte man COBIT einsetzen: welche Unternehmen sind Zielgruppe, und welche Personengruppen in Unternehmen
2. Wie ist der Aufbau von COBIT zu verstehen: die Verteilung von IT Prozessen über Domänen
3. Was sind die Maturity Levels: entscheidet man sich COBIT in einem Unternehmen einzusetzen, muss man sich über eine Strategie entscheiden. Woran kann man diese Strategie orientieren
4. Welche Kontrollzyklen und Normen sind zusammen mit COBIT zu betrachten, und die Geschäftsanforderungen umzusetzen?

2.1 Unternehmens- und Personen-Zielgruppen von COBIT

COBIT unterstützt das IT-Management um Risiken abzuwägen und Kontrolle über Investitionen zu behalten (Betriebswirtschaftliche IT). Anwender von IT Diensten sollen beim fachgerechten und gewissenhaften Einsatz der IT unterstützt werden (Produkt IT). Revisoren, Wirtschaftsprüfer oder IT Spezialisten sollen ihre Analysen mit Daten (aus zielgerichtet aufgebauten Informationsquellen und daraus entstandenen Statistiken) belegen (Technische IT). Die Governance, die durch COBIT aufgebaut wird, durchdringt also betriebswirtschaftliche, produkt-technische und rein technische Bereiche der IT.

Das COBIT Framework richtet sich vor allem an Unternehmen, in denen IT durch den Geschäftszweck eine zentrale Bedeutung erlangt hat, und die eine komplexe Unternehmensstruktur aufweisen. Ferner natürlich sind Unternehmen Zielgruppe, die sich von der Rechtsform her zum Aufbau von weitreichenden IT Kontrollstrukturen eignen. Dies wird jedoch im nachfolgenden Bericht nicht vertieft.

2.2 Aufbau von COBIT in Domänen

COBIT hat vier Hauptdomänen, in denen sich die Prozesse mit ihren Kontroll-Zielen befinden:

- PO steht für Planung und Organisation. Diese Domäne fasst Prozesse zum Managen von Risiken und strategischer Ausrichtung der IT.
- AI steht für Akquisition und Implementierung. Hier geht um die Etablierung neuer Prozesse und Applikationen innerhalb bestehender Infrastruktur.
- DS steht für Delivery und Support. Innerhalb von IT Governance wird hier Service-Level Management, Konfigurations-Management, Kostenmanagement, IT Sicherheit und IT Performance abgedeckt
- ME steht für Monitoring und Überwachung. Dieser Bereich dient der Gewährleistung unabhängiger Revision und der Erhöhung des Vertrauensgrades.

Dabei werden die sieben Informationskriterien berücksichtigt:

- Konformität
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Zuverlässigkeit
- Effektivität
- Einhaltung rechtlicher Erfordernisse (Compliance)

Außerdem werden die fünf Ressourcen berücksichtigt, auf denen Geschäftsprozesse basieren

- Menschen (Human Ressources)
- Gebäude (Facilities)
- Technologieen
- Anwendungssysteme
- Daten

Es gibt keine Aufführung von Management-Instrumenten, keine Verteilung von Verantwortlichkeiten und wenige Rollen- und Berechtigungskonzepte. Funktionstrennung und Schnittstellenüberwachung sind nicht im Framework konkretisiert.

2.2.1 Maturity Levels

Zur Etablierung von COBIT

2.2.2 Kontrollzyklen und Normen

EFQM, CMM/Spice, BSC, Deming Kontrollzyklus, RACI Charts (wichtig!)

2.2.3 Zusammenfassung in Stichpunkten

Die 5 wichtigsten Punkte.

Kapitel 3

Das COBIT Domänen-Modell

3.1 PO - Planung und Organisation

Diese Domäne beschäftigt sich mit der Strategie und der Taktik der IT, um raus zufinden, wie man am besten die Erreichung der Geschäftsziele unterstützt. Die Umsetzung dieser Strategie muss geplant, kommuniziert und durchgeführt werden.

3.1.1 PO1. Definieren eines strategischen Planes

Eine strategische Planung ist für jeden Unternehmensbereich wichtig, da diese den Künftigen Erfolg es Unternehmens sichert, das gilt auch für den IT Bereich.

Strategische Planung dient als Basis für die Lösung bei folgenden Aufgaben: - alle IT-Ressourcen in Übereinstimmung mit Unternehmensstrategie und Prioritäten des Unternehmens zu verwalten und zu steuern. - Bewerten der gegenwärtigen Leistung des Unternehmens - Stütze um den Umfang von notwendigen und zukünftigen Investitionen zu ermitteln. - Aufweisen der Möglichkeiten und Grenzen von IT in einem Unternehmen - Sicherstellen der Zukunft des IT-Bereichs und somit des gesamten Unternehmens

Eine langfristige IT-Strategie ist auf die Unterstützung der Geschäftsziele ausgerichtet und wird aus Geschäftsstrategie entwickelt. Aus Strategie werden Pläne und um diese umsetzbar zu gestallten sind zwei Aspekte zu beachten: Als erstes eine Betrachtung auf dem Markt vorhandenen Technischen Lösungen und zweitens in dem Unternehmen vorhandene Infrastruktur. Im Laufe des Prozesses wird Erfolg der Strategie bewertet und gegebenenfalls angepasst bzw. verändert.

Kontrolle über den IT-Prozess wird erreicht durch: Geschäftsleitung sollte folgende Forraussetzungen erfüllen: Verstehen des derzeitigen IT-Potentials sowie Erstellung eines Schemas für die Priorisierung von Geschäftszielen, das die Geschäftsanforderungen misst. Und die Kontrolle über den IT-Prozess wird 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

3.1.2 PO2. Definieren der Informationsarchitektur

Der Prozess PO1 hat eine IT-Strategie und die taktischen Pläne geliefert, auf deren Grundlage wird dann ein Architekturmodell erstellt. In dem Prozess werden das Datenmodell und die zugehörigen Informationssysteme, die zur Abbildung des Geschäftes notwendig sind, entwickelt. Dies umfasst die Entwicklung eines unternehmensweiten Datenkatalogs, das die Syntaxregeln, ein Datenklassifikationsschema und Sicherheitsstufen festlegt.

Ziel des Architekturmodels ist: - Optimiert des Zusammenspiels aller eingesetzten Informationssysteme und Daten - Verbessert die Qualität der Entscheidungsfindung des Managements (Infos sind verlässlich und gesichert) - Verbessert Verantwortung für die Integrität und Sicherheit der Daten - Verbessert Steuerungsmöglichkeit über die gemeinsame Verwendung von Informationen

Die Erstellung eines solchen Modells muss in regelmäßigen Abständen wiederholt werden, weil sich Technologien ständig weiter entwickeln.

Kontrolle über den IT-Prozess 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 Kontrolle über den IT-Prozess wird gemessen durch - den Prozentanteil der doppelten Datenelemente - den Prozentanteil der Applikationen, welche nicht den Anforderungen der Informationsarchitektur genügen

3.1.3 PO3. Festlegen der technischen Ausrichtung

Da Die Technologien sich ständig weiter entwickeln bzw. ändern, müssen vorhandene und Potenzielle Technologien ausgehend von der IT-Strategie in regelmäßigen Abständen auf Verwendbarkeit und Einsatzfähigkeit untersucht und bewertet werden. Das wichtigste Kriterium dabei ist Unterstützung des Geschäftsprozesses. Ziel ist das ausnutzen des Vorteils von Verfügbarkeit neuer Technologien um die Unterstützung und Entwicklung der Geschäftsstrategie zu gewährleisten. Kontrolle über den IT-Prozess, wird erreicht durch - Aufstellung eines Gremiums, um die Architektur anzuleiten und auf Regeltreue zu überprüfen - Erstellung des technischen Infrastrukturplans, welcher Kosten, Risiken und Anforderungen im Gleichgewicht hält - Festlegung der technischen Infrastrukturstandards, basierend auf den Anforderungen der Informationsarchitektur Kontrolle über den IT-Prozess wird gemessen durch - Anzahl und Typ der Abweichungen vom technologischen Infrastrukturplan - Häufigkeit der Aktualisierungen des technologischen Infrastrukturplans - Anzahl der technologischen Plattformen nach Funktion im gesamten Unternehmen

3.1.4 PO4 Definieren der IT-Organisation und ihrer Beziehungen:

Eine IT-Organisation muss unter Berücksichtigung der Anforderungen in transparente, flexiblen und reagierende IT-Organisationseinheiten aufgeteilt werden und es müssen Verantwortlichkeiten und Rollen festgelegt werden. Die Beschreibung einer IT-Organisation sollte die folgenden Elemente umfassen und berücksichtigen: Strukturierung der IT auf vier Ebenen: - IT-Funktionen, IT-Abteilungen, IT-Leitung, IT-Steuerungsgremien. - Beschreiben der Rollen, Aufgaben, Kompetenzen und Verantwortlichkeiten für alle vier Ebenen. - Beschreibung der Aufgabentrennungen und Überwachungen.

Beispiel für Rollenverteilung: IT-Systemadministrator/in, IT-Anwenderin/in, IT-Abteilungsleiter, IT-Systembetreuer.

Kontrolle über den IT-Prozess, 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, 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

3.1.5 PO5 IT-Investitionsmanagement:

Planung und Aufstellung eines Budgets ist für eine Unternehmenseinheit, in diesem Fall IT, erforderlich um Kosten im Überblick zu behalten und um Ausgaben planen zu können und somit eine hohe finanzielle Sicherheit sicher zu stellen. Das hilft dem Kerngeschäft die Kosten für Prozesse genauer zu berechnen, zu planen und damit Erfolg der Gesamtunternehmung zu gewährleisten.

3.1.6 PO6 Kommunizieren der Management-Ziele und Strategien

Die vorhandenen Informationen und vor allem Ziele und Strategien des Unternehmens in diesem Fall des IT-Bereichs sollen den Mitarbeitern mitgeteilt werden. Es ist wichtig, dass diese Informationen in geeigneter Form zu kommunizieren damit diese allen Mitarbeitern bewusst werden. In diesem Fall können sich die Mitarbeiter auf die Ziele und Strategien einstellen und somit qualitativ höhere Leistung erbringen.

Beispiel: In dem Studiengang Informatik/Softwaretechnik soll die Fähigkeit im Team zu arbeiten gefördert werden, dieses Ziel sollte an die Lehrenden in dieser FH in anwendbaren und praktikablen Anweisungen Kommuniziert werden damit diese Ziele umgesetzt werden können.

3.1.7 PO7 Personalführungsmanagement

Der Erfolg einer Organisation ist von der Einstellungen und Fähigkeiten der Menschen die in dieser Organisation tätig sind sehr stark abhängig. Ziel des IT Bereichs ist fähige Mitarbeiter einzustellen und diese dann langfristig zu binden sowie auch die Motivation dieser Mitarbeiter aufrecht zu erhalten.

3.1.8 PO8 Qualitätsmanagement

Kunden erwarten eine immer höhere Qualität bei gleichzeitiger Kostensenkung. Um diese Anforderung zu erfüllen ist Qualitätsmanagement erforderlich. Dieser muss eine Organisation an jeder Stelle durchdringen und von jedem Mitarbeiter in jedem System gespürt werden auf der anderen Seite müssen die Kosten gering gehalten werden.

3.1.9 PO9 Risikomanagement

Risiken sind bei dem Ansatz von Menschen sowie Technologien immer vorhanden. Es gibt Externe Risiken wie z.B. Erdbeben und interne Risiken die eher Wahrscheinlich sind und auf diese Risiken sollte man vorbereitet sein. Das Ziel ist Ermitteln der Risiken um auf diese reagieren zu können.

3.1.10 PO10 Projektmanagement

Zur Durchführung der IT Aufgaben werden in einer IT-Organisation verschiedene Projekte was die Art und die Größe angeht durchgeführt. Die wichtigsten drei Faktoren an denen ein Projekt oft scheitert sind: Zeit, Qualität, Kosten. Ein professionell durchgeführtes Projektmanagement kann die Risiken, die mit dem Projekt verbunden sind deutlich senken. Das in PO9 erläuterte Risikomanagement sollte sich daher auch auf die Risiken im Projekt erstrecken.

3.2 Beispiel

In einer FH ist das „Kerngeschäft“ unter anderem Ausbildung von Nachwuchskräften. Um den Nachhaltigen integrierten Technikeinsatz zu gewährleisten der diese Aufgabe unterstützt, werden basiert auf einer Bestandsaufnahme die notwendigen Ausbaustuffen für die IT-Ausstattung entwickelt. Dieses Vorgehen beschreibt ein Teil des Strategischen Planes. Da an einer FH eine Große menge an Daten für die Benutzer wie z.B. Scripte, Stundenpläne Online bereitgestellt werden, muss z.B. folgende Frage beantwortet werden: „Wie werden Inhalte für bestimmte Zielgruppen bereitgestellt“? Die Antwort auf diese Frage werden also bei der Erstellung der Informationsarchitektur berücksichtigt und z.B. die nötigen Sicherheitsstufen festgelegt. Festlegen der technischen Ausrichtung an einer FH könnte man sich an dem folgenden Beispiel veranschaulichen: Als sich z.B. in der Mitte der 1990 der Trend für Internetgestütztes lernen auszeichnete, bewertet viele Hochschulen diese Entwicklung mit dem Ziel diese neue Möglichkeit zu etablieren um qualitativ höhere Gestaltung der Lehre zu ermöglichen. In der Fachhochschule Lübeck z.B. wird Moodle (Lernraum) seit 2007 produktiv eingesetzt. Einsatz dieser Technologie würde Vorteile den Hochschulen gegenüber verschaffen die diese Technologie nicht einsetzen. Beispiel für IT-Investitionsmanagements an einer FH: Bevor FH-Lübeck in die Erneuerung der Ausstattung eines Labors Investiert, wird erstmal eine Kosten/Nutzen Analyse erstellt. Diese Beinhaltet z.B. auf der Kostenseite: Kosten für Hard- und Software, Kosten für Trainer und auf Nutzenseite: Aktualität, besserer Lernerfolg wenn Nutzenseite überwiegt wird Investiert sonst nicht. Kommunizieren der Management-Ziele und Strategien an einer FH könnte z.B. so aussehen: In dem Studiengang Informatik/Softwaretechnik soll die Fähigkeit im Team zu arbeiten gefördert werden, dieses Ziel sollte an die Lehrenden in dieser FH in anwendbaren und praktikablen Anweisungen Kommuniziert werden damit diese Ziele umgesetzt werden können. Um einen Qualifizierenden Lehrenden jedoch langfristig an der FH behalten zu können kommt Personalführungsmanagement ins Spiel. Es sind unter anderem folgende Faktoren die in dem Zusammenhang eine Rolle spielen: Aufstiegsmöglichkeiten, Vergütung. Beispiel für Qualitätsmanagement sowie Risikomanagement: An der FH müssen Einkaufs- und Wartungsrichtlinien für PCs beachtet werden in denen z.B. vorgeschrieben ist wie oft die PCs gewartet werden. Risikomanagement verhindert unter anderem, dass ein Virus das FH Netzwerk infiltriert und diesen schädigt dafür wird jeder Rechner mit dem einem Anti-Virus Programm ausgestattet. Das Virusprogramm wird auch jedem studierenden kostenlos angeboten.

3.3 AI

3.3.1 Beispiel

3.4 Delivery und Support

3.4.1 DS1

Es muss der Bedarf des geforderten Services zwischen Kunden, IT-Organisationen und Zulieferern ermittelt werden. Dies bezeichnet man als Defintion von "Service Leveln". Der Kunde hat einen Grundbedarf an Service, der im Service Level als Leistungskriterium für Qualität und Quantität formalisiert dargestellt wird. Dazu trifft man Vereinbarungen, die vertraglich festgehalten werden. Die festgehaltenen Service Level werden regelmäßig mit der Realität verglichen, um Maßnahmen zur Verbesserung festzulegen

Beispiel: An der FH werden Getränkeautomaten betrieben, die von den Kunden (Studierende, Mitarbeiter) genutzt werden. Die verschiedenen Getränke sollten alle verfügbar sein, an jedem Automat, in ausreichender Anzahl, in entsprechender Qualität (Haltbarkeit, Marke). Hierzu ist es nötig zu definieren was die FH Lübeck erwartet. Der externe Zulieferer wird als "underpinning contracter" bezeichnet (DS 2)

3.4.2 DS 2: Lieferanten Management

Hier wird die Zulieferung bezüglich der in DS 1 getroffenen Service Level Absprachen betrachtet. Eine Lieferung stellt ein Risiko dar: Vorkasse, Versicherung, Beschädigung, Pünktlichkeit sind Aspekte die dies verdeutlichen. Die Rollen der Verantwortlichen müssen klar festgelegt werden.

Beispiel: Die Abhängigkeit des Getränkeverkaufes (interne Anforderung) von der Lieferung (externe Anforderung) macht es nötig Kontrolle auf den Prozess auszuüben. Wenn die an der FH bestellten Getränke mit DHL*** kommen, aber keiner den Schlüssel für den Getränkeautomaten hat, kann trotzdem nicht an den Automaten verkauft werden. Daher muss die Rolle klar sein, ob jemand in der FH den Automaten befüllt, oder ob es einen Lieferservice gibt, der die Bestückung ebenso übernimmt.

3.4.3 DS 3: Performance und Kapazitätsmanagement

Die Anforderungen an die Systeme werden überwacht.

Beispiel: wie oft wird ein Getränkeautomat frequentiert (benutzt). Werden alle Getränkeautomaten im Flur genutzt oder nur die neben dem warmen Rechenzentrum. - Müssen daher alle gleichermaßen bestückt und betrieben werden. Muss der Getränkeautomat im obersten Flur (der nachts abgeschlossen ist) auch nachts kühlen?

***

3.4.4 DS 4: Continuity Management

Im Falle einer Störung muss der Weiterbetrieb gewährleistet werden. Hierbei werden allerdings nicht nur größere Störungen betrachtet, sondern auch kleinere Alltagsstörungen, die den Betrieb trotzdem empfindlich gefährden können. Die Auswirkungen auf das Geschäft sollen minimiert werden.

Beispiel: Ein Stromausfall im Cluster, der komplexe Berechnungen zur Schwarmtheorie leistet, kann zu einem kompletten Systemverlust führen wenn die Integrität beschädigt wird. Um vor Stromausfällen zu schützen kann man USVs einsetzen. Der Einsatz von anderen Maßnahmen zur Sicherung der Ergebnisse oder Fortführung des Betriebes wird in Fault-Trees modelliert.

3.4.5 DS 5: Security Management

Sicherheit in Unternehmen muss effizient sein, sollte jedoch idealerweise die Arbeitsprozesse nicht zu behindern. Dennoch haben die Anforderungen an Sicherheit heutzutage eine hohe Dynamik.

Beispiel: Es gibt gesetzliche Auflagen nach denen in Bereichen, in denen sensible Daten in der IT gehandhabt werden, ein Level an Compliance nachzuweisen ist, das ein Mindestmaß an IT Sicherheit darstellt. An der FH Lübeck betrifft das beispielsweise den Netzzugang, der speziell überwacht werden muss, damit keine Spam EMail oder ähnliches aus dem FH Netz ins WAN vordringt.

3.4.6 DS 6: Kostenmanagement

Um die Kosten eines Service im Griff zu halten ist es nötig Kostentreiber im Unternehmen zu identifizieren, sodass die Kostenentwicklung in Betracht gezogen werden kann. Auf die Kostentreiber kann eingewirkt werden um Kosten zu senken. Je nach Service Level entstehen unterschiedliche Kostenstrukturen, die an messbaren Ressourcen identifiziert werden müssen. Unnötige Ressourcen sollen in eine Kostenüberwachung fließen. Durch exakte Zuweisung können die Kosten mit externen Anbietern verglichen werden - für den Vergleich müssen jedoch die entsprechenden Kenntnisse vorhanden sein, d. h. Kostentreiber identifiziert und exakt berechnet sein. Andernfalls besteht die Gefahr unzulässige Vergleiche anzustellen. Mit der Verrechnung der Kosten sind Mittel vorhanden, die die Refinanzierung der IT Infrastruktur ermöglichen. IT Mittel im Jahresbudget muss die organisatorischen Anforderungen der Firma und die Verrechnungen beim Anwender enthalten. PO 5 - Investitionsplanung - muss dabei explizit berücksichtigt werden.

Das Kostenmanagement steht in verschiedenen Beziehungen mit anderen Prozessen:

PO4, PO5, PO10, DS1 -> Kostenmanagement (IT Finanzen PO5 , Prozess, Performance-Berichte ME1)

(Abbildung folgt - Nachbearbeitung - Tool Absprache)

Eine reine Betrachtung nach Kosteneffizienz ist nicht möglich, da die Leistungsfähigkeit der Komponenten in direkter Relation zur Effizienz steht.

offene Fragen: Was ist Compliance bei einem Kostenmodell?

Beispiel: Die für die Studententerminals nötigen Anwendungsprogramme sind veraltet und es müssen neue angeschafft werden, um mit dem Fortschritt schritt zu halten und neue Systeme zu unterstützen. Speziell bei einigen PC Systemen fällt allerdings auf, dass sie nicht mehr kompatibel sind, da die entsprechende Software explosionsartig höhere Systemanforderungen stellt. Entsprechend muss diese Software als Kostentreiber identifiziert werden und ihr Bedarf muss evaluiert werden hinsichtlich der Notwendigkeit um das für die Studenten nötige Service Level zu erbringen. Es kann nicht lediglich auf den Preis geachtet werden, denn wenn die Software für die Fortführung eines Studienganges von essentieller Bedeutung ist, wäre der Service an sich gefährdet. Allerdings kann ein externer Anbieter, beispielsweise ein "Cloud Service", der per Remote Service jene Software zu einem Festpreis zur Verfügung stellt, günstiger sein, als alle lokalen Clients zu updaten. Sofern der Service gleichwertig ist, und die Verfügbarkeit zu den Ballungszeiten gewährleistet ist (Praktikum, alle Studentzen nutzen den Client gleichzeitig um sich zu verbinden).

3.4.7 DS7: Anwendungsschulung und Training

Ein neues IT System allein bildet ohne entsprechende Anwenderkompetenz keinen Mehrwert für das Unternehmen. Die Anwenderkompetenz kann durch Mitarbeiter-Schulungen und Training gesteigert werden. Diese Kompetenz umfasst ebenso Risikobewusstsein bei den Verantwortlichkeiten im Einsatz. Für neue Mitarbeiter können spezielle Security Trainings verpflichtend sein, oder für Security Management oder Administration. Die Durchführung der Schulungen ist in einem Curriculum festzuhalten, das als Schuldungsplan fungiert. Hierbei jedoch sind die Schulungsmethoden zu evaluieren, da es sich um den Einkauf zusätzlicher externe Leistungen handeln kann, oder um ein eigens entwickeltes Trainingssystem.

Beispiel: Mitarbeiter aus dem Bereich Elektrotechnik, die in der Digitalen Signalverarbeitung tätig sind, müssen in der Lage sein mit dem angeschafften Spectrum Analyzer oder dem Oszilloskop umzugehen. Reicht es eine interne Einweisung zu bekommen, oder ist das System derart komplex, dass ein Dienstleister eine Schulung leisten muss.

3.4.8 DS 8: Anwenderunterstützung

Betreffend DS 7 stellt DS 8 die Unterstützung für den Gebrauch der Systeme. Mitarbeiter müssen die IT Systeme auch praktisch bedienen können, und oft ergeben sich beim Einsatz trotz Schulungen offene Fragen.

A14-17, DS1, DS4, DS5, DS9, DS10, DS 13 -> Anwenderunterstützung Service Requests - > A16 Vorfalls-Berichte -> DS 10 Anwenderzufriedenheit -> DS 7, ME 1 Prozess, Performance Berichte -> ME 1

Beispiel: Für die Laborgeräte im Labor gibt es Support-Hotlines, die angerufen werden können, bei speziellen Fragen zu Einsatz.

3.4.9 DS 9: Konfigurationsmanagement

Konfigurationsmanagement ist eine der Kernaufgaben der IT, da unautorisierte Veränderungen verhindert werden müssen, physische Existenz nachzuweisen ist, und damit Veränderungen zu managen sind. Hierzu werden Vorschriften (Policies) und Strategieen (Schnittstellen-Verabredungen z. B.) entwickelt, um eine Zusammenarbeit von Prozessen zu ermöglichen.

Beispiel: die Studenten arbeiten zwar als normale unprivilegierte User auf ihren Systemen, aber für spezielle Aufgaben sind Applikationen so eingestellt, dass Super-User Rechte gewährt werden. Beispielsweise Wireshark im Rechnernetze Praktikum. Der Prozess der Durchführung dieses Praktikums benötigt diese Ausnahme, die im Rahmen der Policy, die Useraktivitäten auf den Systemen restriktiviert, festgehalten ist.

3.4.10 DS 10: Problem Management

Ziel ist es aus immanent auftretenden Problemen und Störungen zu lernen. Incidents werden als Ereignisse definiert, die einen Service stören, und zu Problemen führen können. Probleme in diesem Zusammenhang sind solche Störungen mit erheblichen Auswirkungen auf den Service, oder solche Fehler, deren Ursache

nicht bekannt ist. Die Probleme und Incidents müssen gelöst werden. Daher ist ein Problem Management zu entwickeln, dass den Geschäftsprozess nicht stört. Beispielsweise können Probleme mit Checklisten vermieden werden, oder für Incidents müssen entsprechende Maßnahmen autorisierbar sein.

A16, DS 9. DS 10, DS 13 - > Problem Management Änderungsverfolgung -> A 16 Aufgezeichnete Probleme Bekannte Probleme, Workarounds -> DS 8 Prozess, Performance Berichte -> ME 1

Beispiel: Studenten möchten einen Leistungsnachweis haben über die erbrachten Prüfungsleistungen. Dieser Nachweis ist zu jedem Zeitpunkt des Studiums auszustellen, und die Fachhochschule hat die Pflicht die Korrektheit zu gewährleisten. Störungen oder Umstellungen bei den dazu bereit gestellten Terminals dürfen den Service für die Studierenden nicht betreffen, und müssen bekannt sein. Änderungen an den Leistungen sind zu betrachten. ***

3.4.11 DS 11: Data Management

In Unternehmen sind heutzutage Daten wertvoll. - Sie müssen sorgfältig behandelt werden, da der Verlust von Daten erhebliche Auswirkungen auf alle Services haben kann. Speichersysteme müssen gemanaget werden, Kapazitäten geschaffen, Backups geplant, und Integrität muss überprüft werden.

Beispiel: Ein Verlust sämtlicher Prüfungsleistungen aus der Datenbank der Fachhochschule würde den Fortbestand der Studiengänge gefährden. Entsprechend ist der Stand regelmäßig zu backuppen, und die Integrität der Backups und die Fähigkeit der Wiederherstellung zu überprüfen.

3.4.12 DS 12: Facility Management

Die Gebäudestruktur und Einrichtung muss betrachtet werden, da sie essentielle Auswirkungen auf den Betriebsalltag hat. Geeignete physikalische Umgebung ist zu schaffen und zu warten.

Beispiel: Die Ausbreitung von WLAN über den Universitätscampus benötigt spezielle Räume für die Access Points, Strom, Uplink, Kühlung, und spezielle Masten und Antennen. Diese müssen so geschaffen werden, dass sie eine 100%ige Signalabdeckung in allen Räumen erreichen. DS 13: Operationsmanagement Ziel ist es zu planen, welche Aktivitäten zu welchem Zeitpunkt ausgeführt werden. Bereiche müssen zwar prioretisiert werden, aber kein Bereich darf übermäßig vernachlässigt werden.

Beispiel: Die Baustellen vor dem Gebäude sollten nicht zur Zeit der Durchführung von Klausuren oder mündlichen Prüfung fortgeführt werden. Entsprechend ist eine Erweiterung des Parkplatzes beispielsweise in den Semesterferien vorzunehmen.

3.4.13 Beispiel

TODO

3.5 ME

3.5.1 ME 1: Überwachen und Evaluieren der IT Performance

Die Service Ziele der IT müssen über Prozesse an der richtigen Stelle überwacht werden. Diese Prozesse müssen sich stetig verbessern, indem sie die wesentlichen Testpunkte betrachten, angemessen in Bezug

auf Aufwand: die primär nötigen Daten müssen geliefert werden. Durch die notwendigen Daten können die IT Prozesse an die Anforderungen des Kunden angepasst werden, unter Einhaltung der Richtlinien (Policies) und Standards. Ziel ist es Einblick in IT Kosten, Nutzen und Strategie in Übereinstimmung mit den Goverance Anforderungen zu gewährleisten. -> Berichterstattung: Reporting Strukturen Beispiel: Frequentierung der Seite: von Wo, Wann? Zufriedenheit über die Performance bei den Studenten im Moofle abfragen (Umfrage)

TODO: Balanced Sourcecard

3.5.2 ME 2: Überwachung und Begutachtung der internen Kontrollen

Die nötigen Daten für ME 1 müssen auf Korrektheit überprüft werden. Dabei muss sichergestellt werden, dass die Kontrollpunkte der Prozesse so gewählt sind, dass fundierte Aussagen möglich sind. Zudem stellt ME 2 die Einhaltung gesetzlicher Regelungen hierbei sicher, hinsichtlich der Angemessenheit der Kontrollmechanismen und Kontrollziele.

3.5.2.1 ME 3: Sicherstellung der Einhaltung gesetzlicher Vorschriften

3.5.2.2 ME 4: Sorgen für IT Governance TODO

3.5.3 Beispiel

Kapitel 4

Zusammenfassung

Detailliertere Zusammenfassung der dargestellten Sachverhalte als das Executive Summary in Abschnitt 1.1.

Kernaussagen mit Verweisen auf Ihre Abschnitte zusammenführend und den Gesamtkontext berücksichtigend auf den Punkt bringen.

Literaturverzeichnis