Projektbericht
Thema: COBIT

Alexander Wegner, Marius Ciepluch

12. Januar 2012

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 es wird eine Struktur 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	Gruppe	**Inhaltliche Verantwortung**
Alexander Wegner	Gruppe 8	PO1 - PO10, A11-A17,
Marius Ciepluch	Gruppe 8	DS1 - DS13, ME1 - ME4
Marius Ciepluch	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 man COBIT einsetzen sollte: welche Unternehmen sind Zielgruppe, und welche Personengruppen in Unternehmen? Welche Unternehmen setzen COBIT ein?
2. Wie der Aufbau von COBIT zu verstehen ist: warum die Verteilung von IT Prozessen über Domänen?
3. Was Maturity Levels sind: 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

Nach Krcmar beinhaltet Informationsmanagement alle „Managementaufgaben, die einerseits auf drei Ebenen (entsprechend den behandelten Objekten) Informationswirtschaft (Gegenstand: Angebot, Nachfrage und Verwendung von Information), Informationssysteme (Gegenstand: Daten, Prozesse, Anwendungslebenszyklus), IuK-Technologie (Gegenstand: Speicherung, Verarbeitung, Kommunikation, Technikbündel), andererseits über die Ebenen hinweg als Führungsaufgaben des Informationsmanagements (Gegenstand: IT-Governance, Strategie, IT-Prozesse, IT-Personal, IT-Controlling) realisiert werden müssen."

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. Damit entspricht es dem Rahmenmodell von Krcmar.

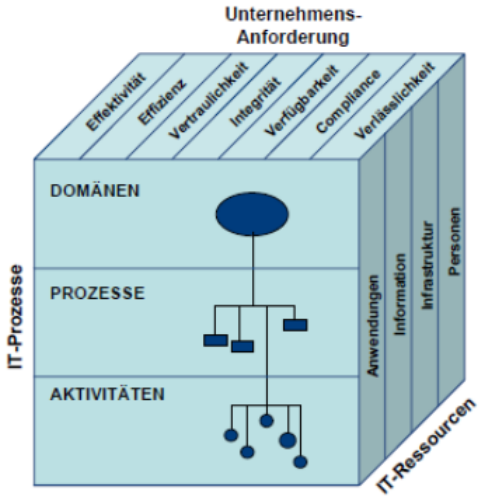
Das COBIT Framework richtet sich vor allem an Unternehmen, in denen IT durch den Geschäftszweck eine zentrale Bedeutung erlangt hat, und die eine komplexe Unternehmensstruktur aufweisen. Ferner natürlich sind Unternehmen Zielgruppe, die sich von der Rechtsform her zum Aufbau von weitreichenden IT Kontrollstrukturen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

Abbildung 2.2.1: COBIT Governance Würfel



Die sieben Informationskriterien sind Unternehmensanforderungen (vertikal), die mit IT Ressourcen erfüllt werden müssen (horizontal). In den COBIT Domänen sind Prozesse modelliert, die sich in Aktivitäten gliedern.

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

- Personen (Human Ressources)
- Infrastruktur (Facilities)
- Anwendungen
- Informationen

Die Realisierung der Aktivitäten ist methodisch offen, d. h. COBIT strukturiert zwar Prozesse thematisch in Domänen, gibt aber keine fixierte Art der Realisierung, was zur Akzeptanzförderung beiträgt. Hilfreiche Modellierungskonzepte, wie man zu notwendigen Kennzahlen kommt für das Unternehmen, sind unter dem Abschnitt Kontrollzyklen und Normen aufgeführt (2.2.2).

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 existieren Reifegrade, die die Tiefe der Etablierung des Frameworks in Unternehmen charakterisieren. Mit diesen Leveln können auch bereits existente Prozesse bewertet werden.

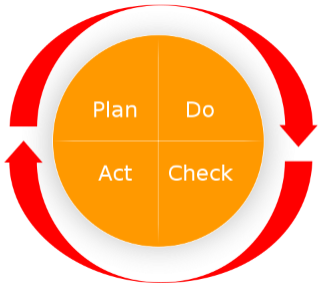
„As the first task and initial scoring, the bank measured the maturity level of current processes.“ (Fallstudie der ISACA, Banco Supervielle S.A.). Die Etablierung von COBIT in vorhandenden Unternehmensstrukturen ist ein umfassender Bereich, der gesonderte Strategien von Unternehmensausrichtung und der Unternehmensarchitektur in Betracht ziehen muss.

2.2.2 Kontrollzyklen und Normen

2.2.2.1 Plan Do Check Act

Mit dem PDCA Zyklus werden allgemein Vorgehensweisen aus dem Management beschrieben.

Abbildung 2.2.2: PDCA Zyklus



Diese Grafik wurde entnommen aus Wikipedia und steht frei zu Dokumentationszwecken unter GPL zur Verfügung.

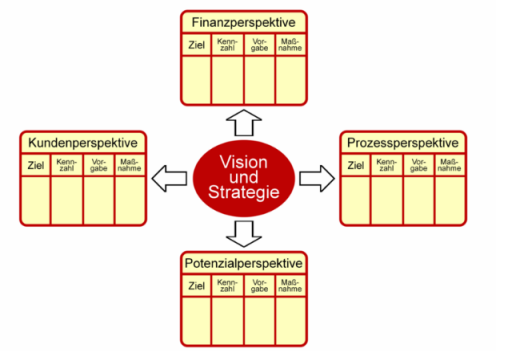
2.2.2.2 Balanced Scorecard

Die Balanced Scorecard (kurz BSC, siehe 2.2.3) stellt ein Konzept zum Messen, Dokumentieren und Steuern der modellierten Prozesse eines Unternehmens dar. Konkret kann im Zusammenhang mit COBIT dieses Konzept beispielsweise hilfreich sein, um nötige vertragliche Vereinbarungen aus DS1 (3.3.1) zu komplettieren, damit sie regelmäßig mit der Realität verglichen werden. So kann über Maßnahmen der Verbesserung entschieden werden, anhand konkret gefasster Kennzahlen im Bezug auf ihre Ziele und Perspektiven für das Unternehmen.

2.2.2.3 EFQM

Das EFQM Modell ist ein Mittel aus dem Qualitätsmanagement, das benutzt wird um umfassende Sichten auf kontinuierliche Weiterentwicklung (nach PDCA, 2.2.2.1) von größeren Managementsystemen zu liefern. Es umfasst drei Säulen (Menschen, Prozesse und Ergebnisse), die miteinander in Beziehung gesetzt werden: Menschen arbeiten in Prozessen (Teile der COBIT Domänen) und erwirtschaften Ergebnisse (möglichst messbar durch Scorecards (2.2.3)), die wiederum Menschen zugute kommen. Hierzu definiert EFQM ein Punktesystem um Metriken anzusetzen.

Abbildung 2.2.3: Balanced Scorecard



Diese Grafik wurde entnommen aus Wikipedia und steht frei zu Dokumentationszwecken unter GPL zur Verfügung.

2.2.2.4 RACI Charts

Mit RACI Charts können Verantwortlichkeiten in Responsible, Accountable, Consulted und Informed unterteilt werden, unter denen Menschen an Prozessen beteiligt sind. Dies wird Form von Tabellen gemacht.

2.2.2.5 Fault Tree Analysis

Bei Fault Tree Analysis geht es um die Erzeugung von Ereignis-Bäumen, die aufeinander folgende Wenn-Dann Situationen hinsichtlich Komponentenausfällen in einer Baum Struktur visualisieren.

2.2.2.6 Normen

Für den Aufbau von Unternehmensstrukturen, Finanzplänen und IT Infrastruktur gibt es Normen, Compliance Richtlinien und Gesetze. Je nach Art und Standort des Unternehmens kann die Erfüllung eines Konformitätsanspruches verpflichtend sein.

2.2.3 Zusammenfassung

Um COBIT anzuwenden ist es hilfreich Modellierungs-Konzepte und Richtlinien für die Organisation und den Betrieb von Unternehmen zu kennen.

Kapitel 3

Das COBIT Domänen-Modell

Im Folgenden werden die einzelnen Domänen von COBIT exemplarisch beschreiben, welche "Plan and Organise", "Acquire and Implement", "Deliver and Support" sowie "Monitor and Evaluate". Zur beispielhaften Verdeutlichung wurde die FH Lübeck und ihre Unternehmensstruktur betrachtet.

3.1 PO Planung und Organisation

Was passiert hier alles, kurz***

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 ebenso für den IT Bereich.

Strategische Planung dient als Basis für die Lösung bei folgenden Aufgaben:

1. Alle IT-Ressourcen in Übereinstimmung mit Unternehmensstrategie und Prioritäten des Unternehmens zu verwalten und zu steuern.
2. Bewerten der gegenwärtigen Leistung des Unternehmens
3. Stütze um den Umfang von notwendigen und zukünftigen Investitionen zu ermitteln
4. Aufweisen der Möglichkeiten und Grenzen von IT in einem Unternehmen
5. Sicherstellen der Zukunft des IT-Bereichs und somit des gesamten Unternehmens

- Kontrolle über den IT-Prozess durch die Konzentration auf Überleitung von Unternehmensanforderungen in IT-Serviceangebote und die Entwicklung von Strategien für die Erbringung dieser Services in transparenter und wirksamer Weise.
- Kontrolle über den IT-Prozess wird erreicht durch:

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

- Kontrolle über den IT-Prozess wird gemessen durch:

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

3.1.2 PO2. Definieren der Informationsarchitektur

Der Prozess PO1 hat eine IT-Strategie und die taktischen Pläne geliefert, auf deren Grundlage ein Architekturmodell erstellt wird. 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, welches die Syntaxregeln, ein Datenklassifikationsschema und Sicherheitsstufen festlegt.

Ziel des Architekturmodels ist:

1. Optimierung des Zusammenspiels aller eingesetzten Informationssysteme und Daten
2. Verbesserung der Qualität der Entscheidungsfindung des Managements (Informationen sind verlässlich und gesichert)
3. Verbesserung der Verantwortungsstruktur für die Integrität und Sicherheit der Daten
4. Verbesserung der Steuerungsmöglichkeit über eine 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, durch die Konzentration auf den Aufbau eines unternehmensweiten Datenmodells, welches ein Datenklassifikationsschema für die Gewährleistung der Integrität und Konsistenz aller Daten beinhaltet.
- Kontrolle über den IT-Prozess, wird erreicht durch:

  1. die Sicherstellung der Genauigkeit der Informationsarchitektur sowie des Datenmodells
  2. die Zuweisung von Datenverantwortlichkeiten
  3. die Klassifikation der Informationen unter Anwendung eines vereinbarten Klassifikationsschemas

- Kontrolle über den IT-Prozess wird gemessen durch:

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

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, durch die Konzentration auf die Festlegung und Implementierung eines technologischen Infrastrukturplans, der Architektur und den Standards, welche technologische Möglichkeiten erkennen und wirksam einsetzen.
- Kontrolle über den IT-Prozess, wird erreicht durch

    1. Aufstellung eines Gremiums, um die Architektur anzuleiten
    2. Erstellung des technischen Infrastrukturplans, welcher Kosten, Risiken und Anforderungen im Gleichgewicht hält.
    3. Festlegung der technischen Infrastrukturstandards, basierend auf den Anforderungen der Informationsarchitektur

- Kontrolle über den IT-Prozess wird gemessen durch

    1. Anzahl und Typ der Abweichungen vom technologischen Infrastrukturplan
    2. Häufigkeit der Aktualisierungen des technologischen Infrastrukturplans
    3. 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:

1. IT-Funktionen
2. IT-Abteilungen

3. IT-Leitung
4. IT-Steuerungsgremien

Eine Beschreiben der Rollen, Aufgaben, Kompetenzen und Verantwortlichkeiten für alle vier Ebenen ist wichtig sowie Beschreibung der Aufgabentrennungen und Überwachungen.

- Kontrolle über den IT-Prozess, durch die Konzentration auf die Erstellung von transparenten, flexiblen und reagierenden IT-Organisationsstrukturen und die Definition sowie Umsetzung von IT-Prozessen mit Rollen und Verantwortlichkeiten, die in die Entscheidungsprozesse des Unternehmens eingebunden sind.
- Kontrolle über den IT-Prozess, wird erreicht durch:
  1. Festlegung eines Frameworks der IT-Prozesse
  2. Aufstellung von angemessenen Organisationseinheiten und -strukturen
  3. Festlegung von Rollen und Verantwortlichkeiten
- Kontrolle über den IT-Prozess wird gemessen durch:
  1. Prozent der Rollen mit dokumentierten Stellenbeschreibungen und Befugnissen
  2. Anzahl der Unternehmenseinheiten/-prozesse, die nicht durch die IT unterstützt werden, die aber gemäß der Strategie unterstützt werden sollten
  3. Anzahl der wesentlichen IT-Aktivitäten außerhalb der IT-Organisation, die nicht genehmigt sind oder die nicht den IT-Organisationsstandards entsprechen *** Abbildung

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.

- Kontrolle über den IT-Prozess, durch die Konzentration auf wirksame und wirtschaftliche Entscheidungen zu IT-Investitionen und Portfolios sowie durch Festlegung und Verfolgung des IT-Budgets im Einklang mit der IT-Strategie und den Investitionsentscheidungen.
- Kontrolle über den IT-Prozess wird erreicht durch:
  1. Planung und Freigabe eines Budgets
  2. Festlegung formaler Investitionskriterien.
  3. Messung des Wertbeitrags und Bewertung gegen die Prognose
- Kontrolle über den IT-Prozess wird gemessen durch:
  1. prozentuelle Reduktion der Stückkosten der erbrachten IT-Services
  2. Prozentanteil der Budgetabweichung verglichen mit dem Gesamtbudget
  3. prozentueller Anteil der IT-Ausgaben, ausgedrückt in Werttreibern des Unternehmens.

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.

- Kontrolle über den IT-Prozess, durch die Konzentration auf die Bereitstellung von richtigen, verständlichen und freigegebenen Richtlinien, Standards und Anleitungen, in ein IT Control Framework eingebetteter Dokumentationen für Stakeholder.
- Kontrolle über den IT-Prozess, wird erreicht durch:
    1. Festlegung eines IT Control Frameworks
    2. Erstellung und Einführung der IT-Richtlinien
    3. Durchsetzung der IT-Richtlinien
- Kontrolle über den IT-Prozess wird gemessen durch:
    1. Anzahl der Geschäftsunterbrechungen aufgrund von Ausfällen von IT-Services
    2. Prozentsatz der Stakeholder, die das IT Control Framework verstehen
    3. Prozentsatz der Stakeholder, welche die Richtlinien nicht einhalten

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.

- Kontrolle über den IT-Prozess, 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 Bewertungsprozesses, das Erstellen von Stellenbeschreibungen, und die Sicherstellung des Bewusstseins für die Abhängigkeit vom jeden Einzelnen.
- Kontrolle über den IT-Prozess, wird erreicht durch:
    1. Bewertung der Mitarbeiter-Performance
    2. Anwerben und Schulung von IT-Personal, um taktische IT-Pläne zu unterstützen
    3. Entschärfen des Risikos einer zu großen Abhängigkeit von Schlüsselressourcen
- Kontrolle über den IT-Prozess wird gemessen durch
    1. Zufriedenheitsgrad der Stakeholder mit den Fähigkeiten und Fachkenntnissen des IT-Personals
    2. Schwankungsrate des IT-Personals
    3. Prozentanteil des IT-Personals, das entsprechend der Erfordernisse der Stelle

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.

- Kontrolle über den IT-Prozess, 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.
- Kontrolle über den IT-Prozess, wird erreicht durch - Festlegung der Qualitätsstandards und -praktiken
    1. Überwachung und Prüfung interner und externer Performance gegen die definierten Qualitätsstandards
    2. kontinuierliche Verbesserung des QMS
- Kontrolle über den IT-Prozess wird gemessen durch
    1. Prozent der mit der IT-Qualität (gewichtet nach Bedeutung) zufriedenen Stakeholder
    2. Prozent der durch die Qualitätssicherung formal und periodisch geprüften ITProzesse, die den Qualitätsvorgaben und Zielen entsprechen
    3. Prozent der Prozesse, die Reviews der Qualitätssicherung (QA) unterliegen

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.

- Kontrolle über den IT-Prozess, 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.
- Kontrolle über den IT-Prozess, wird erreicht durch:
    1. Sicherstellen, dass das Risikomanagement vollständig in die internen und externen Management-Prozesse eingebettet und konstant angewendet wird
    2. Durchführen von Risikobewertungen
    3. Empfehlen und Kommunizieren von Plänen zur Risikominimierung
- Kontrolle über den IT-Prozess wird gemessen durch:
    1. Prozent der kritischen IT-Ziele, die von der Risikobeurteilung abgedeckt sind

2. Prozent der identifizierten kritischen IT-Risiken, für die Maßnahmenpläne entwickelt worden sind
3. Prozent der Risikomanagement-Maßnahmenpläne, die zur Implementierung genehmigt worden sind

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.

- Kontrolle über den IT-Prozess, durch die Konzentration auf einen festgelegten Programm- und Projektmanagementansatz, der auf IT-Projekte angewandt wird. Dies ermöglicht die Beteiligung durch Stakeholder an Überwachung von Projektrisiken und ermöglicht somit den Projektfortschritt.
- Kontrolle über den IT-Prozess, wird erreicht durch:

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

- Kontrolle über den IT-Prozess wird gemessen durch:

  1. Prozent der Projekte, die die Erwartungen der Stakeholder erfüllen
  2. Prozent der Projekte, die Projektmanagement-Standards und -praktiken folgen

3.1.11 Beispiel

Im folgende wird die Domäne Planung und Organisation an einem praktischen Beispiel erläutert. Dieses Beispiel orientiert sich durchgehend an Moodle (Lernraum) Technologie.

In einer FH ist das „Kerngeschäft“ unter anderem Ausbildung von Nachwuchskräften. Um Qualität des Studiums zu verbessern werden folgende strategische Ziele festgelegt:

- Die Betreuung der Studierenden im Studium durch den Einsatz von eLearning zu intensivieren, um dadurch die Studienabbruchquote zu verringern und eine Erhöhung der Absolvierendenzahlen zu erreichen
- Den Studierenden innerhalb und außerhalb der Universität Zugang zu den für das Studium benötigten Ressourcen durch eLearning zu ermöglichen.

Dieses Vorgehen beschreibt ein Teil des Strategischen Planes.

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.

Da an einer FH eine Große menge an Daten für die Benutzer wie z.B. Scripte, Stundenpläne Online durch eLearning 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 die nötigen Sicherheitsstufen festgelegt.

Kommunizieren der Management-Ziele und Strategien an einer FH könnte z.B. so aussehen: Einer von vielen Zielen in der FH-Lübeck ist es eine variable Mischung von Präsenzlehre und virtueller Lehre in vielfältigen Lernszenarien anzubieten. dieses Ziel sollte an die Lehrenden in dieser FH in anwendbaren und praktikablen Anweisungen Kommuniziert werden damit dieses umgesetzt werden kann.

Beispiel für IT-Investitionsmanagements an einer FH: Bevor FH-Lübeck in die Erneuerung und Ausbauung des eLearnings Investiert, wird erstmal eine Kosten/Nutzen Analyse erstellt. Diese Beinhaltet auf der Kostenseite z.B.: Kosten für Seminare um Kompetenzen im Bereich eLearning für Lehrende auszubauen und Kosten für Wartung. Auf der Nutzenseite dagegen: Aktualität und besserer Lernerfolg. Wenn Nutzenseite überwiegt wird Investiert sonst nicht.

Und zuletzt noch ein Beispiel für Qualitätsmanagement: An der FH müssen unter anderem Wartungsrichtlinien für eLearning beachtet werden in denen z.B. vorgeschrieben ist wie oft dieser gewartet werden muss. Diese Wartungen müssen in regelmäßigen Abständen durchgeführt werden.

3.2 AI Akquisition und Implementierung

3.2.1 AI1 Identifizierung automatisierter Lösungen

Es gilt in diesem Fall die Bedürfnisse der Anwender und die Anforderungen durch die Informationsarchitektur und die Kosten zur Deckung zu bringen. Automatisierte und standardisierte Lösungen erfordern bei der Anwendung weniger Aufwand und sind somit zu bevorzugen. Es ist also das Ziel Identifizieren automatisierter Lösungen um einen effektiven Gebrauch sicher zu stellen und somit Zufriedenheit der Anwenderbedürfnisse zu erhöhen und gleichzeitig Kosten zu sparen.

- Kontrolle über den IT-Prozess, durch die Konzentration auf die Identifizierung technisch machbarer und kosteneffektiver Lösungen.
- Kontrolle über den IT-Prozess, wird erreicht durch:

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

- Kontrolle über den IT-Prozess wird gemessen durch:

    1. Anzahl der Projekte bei denen der prognostizierte Nutzen aufgrund falscher Annahmen in der Machbarkeitsstudie nicht erreicht wurde
    2. Prozent der Machbarkeitsstudien, die vom Geschäftsprozesseigner abgenommen wurden
    3. Prozent der Benutzer/Innen, die mit der gelieferten Funktionalität zufrieden sind

3.2.2 AI2 Erwerb und Pflege von Applikationssoftware

Es gibt einen Konflikt zwischen den qualitativen Anforderungen der Anwender und Anforderungen an die IT Leistungen möglichst kostengünstig zu erbringen. Leistungen sind oft kostengünstiger und effektiver durch Standardapplikationen zu erbringen. Ziel ist es also Applikationssoftware zu erwerben und zu pflegen, um automatisierte Funktionen zur Verfügung zustellen, welche die Geschäftsprozesse effektiv unterstützen.

- Kontrolle über den IT-Prozess, durch die Konzentration auf die Sicherstellung des Vorhandenseins eines zeitgerechten und kostenwirksamen Entwicklungsprozesses.
- Kontrolle über den IT-Prozess, wird erreicht durch:

    1. Überführung von Unternehmenserfordernissen in Entwurfsspezifikationen
    2. Einhaltung von Entwicklungsstandards für alle Modifikationen
    3. Trennung der Tätigkeiten von Entwicklung, Test und Betrieb

- Kontrolle über den IT-Prozess wird gemessen durch:

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

3.2.3 AI3 Erwerb und Pflege der technischen Infrastruktur

Die technische Infrastruktur ist die Basis für alle durch die IT geleistete Prozessunterstützung die auf der automatisierte Lösungen und Applikationen aufsetzen. Fehler in diesem Bereich sind fatal denn diese haben Auswirkungen auf die gesamte Leistungserbringung und sind schwer zu korrigieren. Ziel ist es also technischen Infrastruktur zu Erwerben und zu Pflegen, um eine optimierte Unterstützung für die Geschäftsanwendungen zur Verfügung zu stellen.

- Kontrolle über den IT-Prozess, durch die Konzentration auf die Bereitstellung geeigneter Plattformen für die Geschäftsanwendungen in Übereinstimmung mit der definierten IT-Architektur und Technologiestandards.
- Kontrolle über den IT-Prozess, wird erreicht durch

    1. Entwicklung eines mit dem technologischen Infrastrukturplan konformen Technologiebeschaffungsplans

2. Planung der Wartung der Infrastruktur
3. Implementierung von Sicherheits- und Prüfmaßnahmen

- Kontrolle über den IT-Prozess wird gemessen durch

1. Prozent der Plattformen, die nicht mit den definierten IT-Architektur- und Technologiestandards konform sind
2. Anzahl der kritischer Geschäftsprozesse, die von Infrastruktur unterstützt werden
3. Anzahl der Infrastrukturkomponenten, die nicht mehr unterstützt werden

3.2.4 AI4 Befähigen des Betriebes

Der Gebrauch der IT scheitert oft nicht an den Möglichkeiten, welche die Software bietet, sondern an unzureichenden zu Verfügung gestellten Dokumentationen wie z.B. Gebrauchsanweisungen oder Tipps und Tricks in der Anwendung der Software. Es ist also in diesem Fall das Ziel Entwicklung und Pflege von Anwender- und Betriebshandbüchern Sowie auch Schulungen des Personals.

- Kontrolle über den IT-Prozess, durch die Konzentration auf die Bereitstellung wirksamer Anwender- und Betriebshandbücher sowie Schulungsunterlagen für die Weiterleitung des für den erfolgreichen Betrieb notwendigen Wissens.
- Kontrolle über den IT-Prozess, wird erreicht durch

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

- Kontrolle über den IT-Prozess wird gemessen durch

1. Anzahl der Applikationen, deren IT-Verfahren sehr gut in Geschäftsprozesse integriert sind
2. Prozent der mit den Anwenderschulungen und den Schulungsunterlagen zufriedenen Geschäftsprozesseigentümer
3. Anzahl der Applikationen mit angemessenen Anwenderschulungen und Schulungen der operativen Unterstützung.

3.2.5 AI5 Zur Verfügung stellen von IT-Ressourcen

Mögliche IT-Ressourcen sind z.B. Mitarbeiter, Software, Einrichtungen. Diese müssen kosteneffektiv aber effizient und unter Berücksichtigung der vertraglichen Bedingungen genutzt sowie zur Verfügung gestellt werden. Dabei sind Einkaufsrichtlinien und Lieferantenauswahl wichtige Kriterien. Das Ziel ist es also Diejenigen Ressourcen für den IT-Betrieb kosteneffektiv zur Verfügung zu stellen, die am besten zu dem Geschäft passen und dasunter Reduzierung der Einkaufsrisiken.

- Kontrolle über den IT-Prozess, 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.
- Kontrolle über den IT-Prozess, wird erreicht durch

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

- Kontrolle über den IT-Prozess wird gemessen durch

  1. Anzahl der Streitfälle im Zusammenhang mit Beschaffungsverträgen
  2. Reduzierte Beschaffungskosten
  3. Prozent der mit den Lieferanten zufriedenen Stakeholder

3.2.6 AI6 Änderungsmanagement

In jeder IT-Organisation und in jedem Geschäftsbereich treten Änderungen auf. Diese dürfen nicht zu Störungen oder Beeinträchtigungen der Geschäftsabläufe führen. Eine effektive und effiziente Behandlung und Durchführung solcher Änderungen muss geregelt werden. Ziel ist es also Managen von Änderungen, um die Wahrscheinlichkeit von Serviceunterbrechungen sowie Störungen zu minimieren.

- Kontrolle über den IT-Prozess, durch die Konzentration auf eine geregelte Einschätzung von Auswirkungen der Implementierung aller Änderungen auf die IT-Infrastruktur.
- Kontrolle über den IT-Prozess, wird erreicht durch:

  1. Festlegung und Kommunikation der Verfahren für Änderungen inklusive Notfallsänderungen
  2. Beurteilung, Priorisierung und Autorisierung der Änderungen
  3. Verfolgung des Status der und das Berichten über Änderungen

- Kontrolle über den IT-Prozess wird gemessen durch:

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

3.2.7 AI7 Installieren und Abnehmen von Systemen und Änderungen

Nachdem neue Systeme oder Änderungen entwickelt wurden, müssen diese in den Betrieb überführt werden. Dazu sind Tests sowie Implementierungen notwendig. Diese müssen von dem abschließenden Kontrollverfahren, ob ein Auftrag vollständig und einwandfrei ausgeführt wurde, abgeschlossen werden. Dies stellt sicher, dass die neuen Systeme den Anforderungen und Erwartungen des Betriebes und der Anwender entsprächen. Die Neue oder geänderte Systeme sollen somit nach der Einführung einwandfrei und ohne Probleme arbeiten.

- Kontrolle über den IT-Prozess, durch die Konzentration auf das Testen, damit Anwendungen und Infrastrukturlösungen dem vorgesehenen Zweck entsprechen und frei von Fehlern sind. Aber auch Konzentration auf die Planung der Inbetriebnahme.
- Kontrolle über den IT-Prozess, wird erreicht durch:
    1. Etablierung der Testmethoden
    2. Evaluierung und Genehmigung der Testergebnisse durch das Businessmanagement
    3. Durchführung des abschließenden Kontrollverfahren, ob ein Auftrag vollständig und einwandfrei ausgeführt wurde (Post-Implementation-Review).
- Kontrolle über den IT-Prozess wird gemessen durch:
    1. Ausfallszeit der Anwendung oder Korrekturen an den Daten, die durch ungeeignetes Testen hervorgerufen sind
    2. Prozent der Systeme die dem erwarteten Nutzen entsprechen
    3. Prozent der Projekte mit einem dokumentierten und genehmigten Testplan

3.2.8 Beispiel

Um die Prozesse der Domäne „Akquisition und Implementierung“ besser zu verstehen kommen wir zu einem Praktischen Beispiel der sich an eLearning Technologie orientiert.

Da in jeder Organisation mit der Zeit Veränderungen auftreten ist Änderungsmanagement ein wichtiger Prozess. Wir nehmen mal an es soll an einer Fachhochschule eine nachhaltigen Implementierung von eLearning-Innovationen gestaltet werden soll. Das Stichwort ist Nachhaltigkeit deswegen soll ein Änderungsmanagement eingeführt werden, der sich auf die nachhaltige Einführung von eLearning als Innovationen in der Hochschullehre bezieht. Dabei ist z.B. die Einschätzung von Auswirkungen der Implementierung aller Änderungen auf die IT-Infrastruktur wichtig.

Viele Fachhochschulen sowie Universitäten bekommen mit der Einführung von eLearning- Technologie neue Möglichkeit wie z.B. online Selbsttests, die Motivation sowie Lernerfolg des Studierenden zu steigern. Diese Methode ist flexibeler als eine Musterlösung. Und man kann anhand automatisierter Testformen Lernfortschritt messen und diese Tests individuell so oft wiederholen, wie man möchte. Diese automatisierte Testform verdeutlicht den Vorgang Identifizierung automatisierter Lösungen.

Bei dem Erwerb und Pflege der technischen Infrastruktur für eLearning Technologie müssen z.B. folgende technische Kriterien berücksichtigt werden: Erweiterbarkeit, Skalierbarkeit, Robustheit, Zuverlässigkeit,

Fehlertoleranz, Ausfallsicherheit, Möglichkeit der Integration vorhandener Lernmaterialien, Integration bestehender Benutzerverwaltungen, Kompatibilität mit anderer und zum Teil bereits vorhandener Komponentensoftware.

Ein Lernraum ist eine komplexe Umgebung und um eine Korrekte Nutzung des eLernraums zu gewährleisten den Lehrenden Umgang mit dieser Technologie zu erleichtern sollten ausreichend Handbücher bereitgestellt werden. Es sollen aber auch Seminarbesuche ermöglicht werden in denen die Lehrenden erforderlichen eLearning-didaktischen und technischen Kompetenzen erwerben können. Dieses Beispiel bezieht sich auf AI4 - Befähigen des Betriebes.

3.3 Delivery und Support

Im Folgenden werden die Teilprozesse der Delivery und Support Domain beschrieben. Die Verbindungen zwischen den Prozessen sind mit Referenzen kenntlich gemacht. Es wurde Wert auf beispielhafte Verdeutlichung aus dem Unternehmensalltag gelegt, und abschließend wurde ein Beispiel aus dem Bereich der FHL betrachtet.

3.3.1 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. Akkurate Mittel dies darzustellen können zum Beispiel Balanced Scorecards sein, da sie die Kundenperspektive über festzusetzende Kennzahlen gegenüber der Prozessperspektive dimensionieren, unter Einbeziehung der Finanz- und Potenzialperspektive (siehe 2.2.3).
Im Bezug auf DS 2 (3.3.3) sind externe Zulieferer „underpinning contractors". Das bedeutet sie sind unter Umständen je nach vertraglicher Bindung und Entwicklung wechselbar.

3.3.2 DS 2: Lieferanten Management

Hier wird die Zulieferung bezüglich der in DS 1 (3.3.1) getroffenen Service Level Absprachen betrachtet. Eine Lieferung stellt ein Risiko dar: Vorkasse, Versicherung, Beschädigung, Pünktlichkeit sind Aspekte die dies im Unternehmensalltag verdeutlichen. Die Rollen der Verantwortlichen müssen klar festgelegt werden. Dies kann über RACI Charts (2.2.2.4) geschehen, oder auch über die Verwendung von Qualitätsmanagement Maßnahmen wie durch den Aufbau auf EFQM (2.2.2.3) basierender Kontrollzyklen, die Menschen, Prozesse und Ergebnisse wiederholt in Beziehung setzen.
Ziel ist in jedem Falle gemäß des PDCA (2.2.2.1) Zyklus eine kontinuierliche Verbesserung im Bezug auf die DS 1 Service Level Absprachen. Zentral ist hier, dass Maßnahmen (Act) getroffen werden können (Plan), wie zum Beispiel die Wahl (Do) eines konkurrierenden Zulieferers (Check).

3.3.3 DS 3: Performance und Kapazitätsmanagement

Die verabredeten DS 1 Kennzahlen (3.3.1) müssen kontrolliert werden, und unter Berücksichtigung der Entwicklung der relevanten Kennzahlen müssen Entscheidungen getroffen werden (3.3.2). Diese können

eine Erhöhung oder Erniedrigung des festgesetzten kapazitären Bedarfs sein, oder eine Veränderung der Performance Kennzahlen (Potenzialperspektive BSC, siehe 2.2.3).

Um dies zu unterstützen definiert man in DS 3 Datenpunkte, die wie in DS 1 erwähnt, Abweichungen von den Kennzahlen registrieren.
Das bedeutet DS 2 betrachtet sowohl Verantwortungen, als auch Leistungsentwicklung bei Zulieferern. Die anforderungs-orientierte Überwachung ist Teil von DS 3.

3.3.4 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. Das bedeutet auch, dass Maßnahmen um den Weiterbetrieb sicher zu stellen, in einem realistischen Finanzrahmen bleiben müssen, und dennoch effiziente Sicherheit für den Weiterbetrieb gewährleisten sollen.
Ein erprobtes Mittel im IT Alltag Continuity Management Maßnahmen zu betrachten ist Fault Tree Analysis (FTA, siehe 2.2.2.5), welche eine Baumstruktur von Folge-Events definiert, um Kettenreaktionen zu modellieren, die den Unternehmensalltag im Bezug auf Continuity Aspekte gefähren können. Mit FTA modelliert man beispielsweise Stromausfälle in sensiblen Industrieanlagen oder Rechenzentren, die vertraglich zu einer hohen Verfügbarkeit verpflichtet sind.

3.3.5 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. Unternehmen, die mit Kredikarten Daten arbeiten, müssen beispielsweise Zertifikate über Complicance Audits erlangen, wie PCI DSS (V2 nach Procedures [2010]). Die Maßnahmen, die in solchen Audits geprüft werden, sind häufig in Jahreskatalogen gelistet. Prinzipiell handelt es sich um Checklisten basierte Tests.
Die Ergebnisse von externen oder internen Tests und Audits müssen betrachtet werden, das heißt es muss ein Internes Report Management geben, welches Security Baselines und Complicance Strategien (können nach DS 1 3.3.1 getroffene Service Level Anforderungen sein, oder Normen (2.2.2)) betrachtet. Je nach Unternehmen muss auf akute Gefährdungen (eventuell sogar nach DS 4 3.3.4) mit geschulten (3.3.7) Incident Response Teams reagiert werden können, oder es müssen präventive Maßnahmen kontrolliert, definiert und evaluiert werden. Solche Maßnahmen können Datenklassifizierung sein, oder Überwachsmaßnahmen.
Die Verbesserung solche Prozesse kann mittels des PDCA Zyklus geschehen, mit speziellen Instrumenten wie Fault Tree Analysis, oder mit IT Risk Management Maßnahmen, die die Evaluierung von Assesments leisten, speziell hinsichtlich unternehmensinterner Kriterien. Diese Kriterien müssen allerdings exportiert werden um eine transparente Risikoevaluation zu gewährleisten und um Verstöße gegen nötige Compliance Richtlinien zu vermeiden, die Bedeutung für den Unternehmensumsatz (DS 6, 3.3.6) haben können.

3.3.6 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 (3.3.1) entstehen unterschiedliche Kostenstrukturen, die an messbaren Ressourcen (3.3.3) identifiziert werden müssen. Unnötig gewordene Ressourcen sollen in eine Kostenüberwachung nach DS 6 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. Die Summe der IT Mittel im Jahresbudget muss die organisatorischen Anforderungen der Firma und die Verrechnungen beim Anwender enthalten.
Die Investitionsplanung nach PO 5 (3.1.5) muss dabei explizit berücksichtigt werden. Das Kostenmanagement steht massiv in verschiedenen Beziehungen mit anderen Prozessen: PO 4 (3.1.4), PO 5 (3.1.5) und PO 10 (3.1.10) wirken auf das Kostenmanagement ein: da PO 4 das Investitionsmanagement leistet, und PO 5 die Kontrolltiefe je nach Unternehmensstruktur und Unternehmensplanung etabliert, ist das Projektmanagement (3.1.10) verantwortlich anhand von Performance Berichten (3.4.1) Service Level nach innen zu überwachen (nach DS 1, 3.3.1). - Und nicht nur gegenüber externen Zulieferern nach DS 2 (3.3.2).

Eine reine Betrachtung nach Kosteneffizienz ist nicht möglich, da die Leistungsfähigkeit der Komponenten häufig in direkter Relation zur Effizienz steht. Trotzdem muss natürlich die Compliance des in PO 4 getroffenen Kostenmodells eingehalten werden, das mit Mitteln der Cooperate Finance etabliert werden muss.

3.3.7 DS 7: 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 (betrifft DS 5, 3.3.5) . 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 Schulungsplan fungiert. Hierbei jedoch sind die Schulungsmethoden zu evaluieren, da es sich um den Einkauf zusätzlicher externer Leistungen handeln kann, oder um ein eigens entwickeltes Trainingssystem.
Mittel für DS 7 in Unternehmens liegen oft im Verantwortungsbereich von Human Ressources, welches auch eine Schnittstelle zur Internalisierung erworbenen Wissens definieren kann, hinsichtlich DS 8.

3.3.8 DS 8: Anwenderunterstützung

Betreffend DS 7 stellt DS 8 die Unterstützung für den Gebrauch der vorhandenen Systeme in den Vordergrund. Mitarbeiter müssen die IT Systeme auch praktisch bedienen können, und oft ergeben sich beim Einsatz trotz Schulungen offene Fragen.
Dies trifft ins besonders dann zu, wenn im Rahmen des Konfigurationsmanagements (siehe 3.3.9) Anpassungen vorgenommen werden müssen (nach A16, 3.2.6) um Service Requests gerecht zu werden gemäß DS 10 (siehe 3.3.10), da Anwenderzufriedenheit erheblichen Einfluss auf die potenziell mögliche Leistung des Unternehmens haben kann. - Was auch in der Betrachtung von Balanced Scorecards reflektierbar ist, wenn Performance Berichte nach ME 1 (siehe 3.4.1) nach Einführung eines neuen IT Systems negative

statt positive Entwicklung aufweisen, und erwünschte Kennzahlen damit nicht erreicht werden.
Weiterhin spielen A 14, A 15 und A 16 (3.2.4 bis 3.2.6) eine erhebliche Rolle, da Betriebsbefähigung hinreichende Bedingung für operativen Betrieb ist. So können zudem teure Fehler vermieden werden, die Zeit- und Ressourcen-intensives Nachbearbeiten nötig machen.

3.3.9 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, also Benutzerordnungen) und Strategien (Schnittstellen-Verabredungen zur Interoperabilität) entwickelt, um eine Zusammenarbeit von Prozessen zu ermöglichen. Dies können einfache Passwort Richtlinien sein, oder komplexe Setup Regeln für IT Services.
Konfigurationsmanagement kann bedeutsam für die Sicherheit in Unternehmen sein, nach DS 5 (3.3.5), da manche Complicance Richtlinien beispielsweise Passwortsicherheit mit Mindestlängen definieren. Rückwirkend betrifft Konfigurationsmanagement natürlich auch DS 7 und DS 8, da Benutzer ein erwartungskonform konfiguriertes System erwarten.

Weiterhin sollte aus Gründen der Wartbarkeit Homogenität bei IT Systemen angestrebt werden, um eine Kostenexplosion hinsichtlich nötigen Personalaufwands bei Wartungsarbeiten zu verhindern. Erfahrungen und Techniken (Daten, Konfigurationsformate, Systembackups etc.) mit der IT in Unternehmen sollten übertragbar bleiben. Es sollte also zudem Langzeitsupport von Soft- und Hardware angestrebt werden, was unter Umständen höhere Anschaffungskosten nach DS 6 (3.3.6) erzeugt.

3.3.10 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. Beispielsweise aus dem Security Management nach DS 5, welches den Aufbau Security Incident Response Teams definieren kann.

Wichtig ist hier auch im Zusammenhang mit dem Konfigurationsmanagement (nach DS9, 3.3.9) eine sachgerechte Änderungsverfolgung zu gewährleisten, sodass Ursachen von Incidents gefunden werden können, und in die interne Knowledge Base Richtlinien zur Vermeidung einfließen können (nach A16 bzw. DS9 3.2.6, 3.3.9). Dies kann nachhaltig Performance Berichte (ME 1, 3.4.1) verbessern.

3.3.11 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. Dennoch gibt es eine steigende Tendenz, dass Unternehmen zunehmen kritische Daten verlieren (nach Baker et al. [2011]).

Speichersysteme müssen gemanaget werden, Kapazitäten geschaffen (DS 3, betrifft Underpinned Cotractors im Falle von Cloud Computing), Backups geplant (DS 5, Secruity Management), und Integrität muss überprüft werden (um zum Beispiel alte Backups mit neuen Systemen noch verwenden zu können).

Data Management ist Kernbereich von IT Administration in Unternehmen, da Fehler im Falle von mangelhaften Continuity Management (siehe DS4, 3.3.4) hohe Kosten verursachen können. Zum anderen muss klar sein, welche Daten notwendigerweise vorgehalten werden, da beispielsweise das Speichern von kritischen Informationen wie Kreditkartendaten rechtlichen Einschränkungen unterliegt, spezielles Security Management (DS 5) nach sich zieht, und in vielen Fällen nicht nötig ist. Data Management kann ein zentraler Kostenträger sein (siehe DS 6, 3.3.6 Kostenmanagement), denn zwar ist Speicherhardware relativ günstig, aber versicherter Speicher - wenn beispielsweise ein Storage Anbieter benutzt wird - ist mit teuren Verträgen verbunden, je nach angestrebten Service Leveln (DS 1). Hierbei muss auch aus juristischer und versicherungstechnischer Sicht eine Definition der Erwartungshaltung des Unternehmens folgen, ins besonders nach Erwägungen aus DS 4, da eventuell günstige Cloud Computing Anbieter keine Haftung für Datenverlust übernehmen, und ein Outsourceing damit eine Entscheidung des Risk Managements (Teil von DS 5) wird.

3.3.12 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.

Dies betrifft das Unternehmen gesamt: betrachtet man DS 5 (3.3.5), das Security Management, muss neben IT technischen Erwägungen auch der physischer Zugang zu Speicherhardware durch geeignete Maßnahmen beschränkt werden. Data Management (DS 11, 3.3.11) wird schwieriger, wenn regelmäßig Probleme mit der Infrastruktur vor Ort auftreten. Dies kann erhebliche Kosten verursachen, nach DS 6 (3.3.6), bzw. DS 9 (3.3.9) bei notwendiger Neuanschaffung, wenn sie eine Systemumstellung impliziert. Manche IT Systeme haben eine unersetzliche Bedeutung in Unternehmen.
Unter Facility Management fällt ebenso die Planung von handwerklichen Arbeiten, die Lärmbelästigung erzeugen können. Es sollte erwogen werden ob dadurch negative Effekte nach ME 1 auftreten. Außerdem überprüft werden muss die geeignete Bereithaltung notwendiger Schlüssel, die im Rahmen der Einflüsse von DS 5 hinsichtlich DS 11 bei unautorisiertem physischen Zugang zu Datenverlust führen können. Viele „Schlösser“ sind heutzutage digital (RFID basiert, Zugangskarten, Codes, Alarmanlagen), weshalb eine Koordination mit anderen Bereichen von zunehmender Bedeutung ist.

Bereiche wie Reinigung, Gebäudesicherheit oder auch Klimatisierung sind zum Beispiel entschiedene Bereiche des Facility Managements, die auch im Rahmen des Continuity Managements (DS 4, 3.3.4) von Bedeutung sein können.

3.3.13 Beispiel

Es soll an einem Beispiel von der FH Lübeck konkretisiert werden, die die einzelnen Prozesse der Delivery und Support Domäne von COBIT betrachtet werden können.

Im Rahmen des Praktikums einer Lehrveranstaltung „Signale und Systeme“ des Fachbereichs Elektrotechnik und Informatik ist die Arbeit mit einer speziell zu fertigenden Platine geplant. Die Studenten sollen mit der Platine digitale Signalverarbeitung erforschen. Die Platine muss bei einem externen Anbieter gefertigt werden, da es viele Lötstellen durch-kontaktiert werden müssen. Es wird eine Stückzahl von 32 Platinen bestellt, zum Preis von 20 Euro für 4 Platinen auf einer Euro-Platine. Die Platine soll danach selbstständig bestückt, und im Labor verwendet werden. Im Labor soll Software für das Zusammenspiel mit der Platine entwickelt werden. Die Ergebnisse sollen abschließend zur Bewertung vorgestellt werden.

Im Folgenden ein RACI Chart für diesen Prozess:

Tabelle 3.3.1: RACI Chart - DS 1 - 12 Beispiel zur Definition von Service Level Agreements

	Professor	Student	Hersteller	Sekretariat	Post	WiMi	Hausmeister
Liefertermin vereinbaren	R	I	A	I		I	
Lieferung annehmen				R		I	
Lieferung aushändigen	I		A		R		
Platine entwerfen	R		I			A	
Platine testen	R	I				A	
Platine bestücken	I	R				C	
Programmierung	I	R				C	
Platine bezahlen	R			A		A	
Abrechnung verwalten	I			R		I	
Bestückung bestellen		R	I			C	
Arbeit bewerten	R	I				C	
Bewertung speichern	R			A			
Bewertung ausstellen	R	I		I		A	
Praktikum durchführen	R	I				C	
Laborraum	A	I				C	R

Nach der Bestellung ist automatisch eine Vorstellung des Service Levels entstanden (DS 1), welches erwartet wird. Das Material und der Lieferzeitpunkt sind verabredet. Das Praktikum findet halbjährlich statt, was bedeutet, dass ein Hersteller, der sich einmal bewährt hat, behalten werden kann (DS 2). Die Anzahl der zu bestellenden Platinen ist abhängig von der Semestergröße (DS 3), weshalb die Kapazität der Bestellung sich ändern kann. Die Platine wird nicht in den Unternehmensalltag der FH registriert, also nur von Kunden (Studenten) benutzt. Interferiert ihre Benutzung aber beispielsweise mit dem WLAN, ist entsprechende Anwenderschulung wichtig (DS 7 und DS 8), damit dieser Teilprozess den Betrieb nicht gefährdet. Falls aber die Platine nicht geliefert wird, sollte es eine Alternative geben, um das Praktikum dennoch durchzuführen (DS 4).

Die zu entwickelnde Software, die im Labor funktionieren soll, muss trotz eventueller Sicherheits-Richtlinien lauffähig sein (DS 5). Ebenso sollten kritische Daten wie die Bewertungsdetails, Matrikelnummern etc. nach DS 11 gemanaget sein.

Die Laborräume sollten zur Zeit des Praktikums verfügbar sein, und voll funktionsfähig (DS 12). Allerdings sollte nachts das Licht ausgemacht werden, und abgeschlossen werden.

3.4 Monitoring und Evaluation

In dieser Domain befinden sich Prozesse des Bereichs Monitoring und Evaluation. COBITs Top Down Steuerungsansatz bezieht einen Großteil seiner Dynamik aus den durch diese Prozesse gewonnen Daten, die entsprechen quantitativ und qualitativ zum Erfolg der Etablierung des Frameworks im Unternehmen beitragen. Es werden nicht nur Datenaufkommen von Applikationen gemessen, sondern auch Nutzungsverhalten. Letzte können ins besonders Aufschluss über die produktiven Kapazitäten geben, die in der IT durch ihre Benutzer aufgebaut sind.

3.4.1 ME 1: Überwachen und Evaluieren der IT Performance

Die Service Ziele der IT (interne Service Level) müssen in den Prozessen der Domänen an der richtigen Stelle überwacht werden. Die Datenerhebung muss sich stetig verbessern, indem sie die wesentlichen Testpunkte betrachtet, angemessen in Bezug auf Aufwand: die primär nötigen Daten müssen geliefert werden. Dies muss auf eine Weise geschehen, die es ermöglicht, Schlussfolgerunden zur Anpassung des jeweiligen Teilprozesses der Domäne vorzunehmen. Beispielsweise kann dies durch entsprechende Visualisierung, geeignete statistische Evaluationsmethoden (Umfragen von Mitarbeitern) oder entwickelte Verfahren zum gezielten Logmanagement (Anwendungsüberwachung) geschenen.
Erst 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 (von ME 4, 3.4.4) zu gewährleisten.

3.4.2 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: wurde an der richtigen Stelle gemessen oder umgefragt? Kann das Kontrollziel erreicht werden, oder ist es durch Outsourcing gar nicht mehr möglich die entsprechenden statistischen Aussagen zu treffen, da ein externer Anbieter den Zugriff auf die benötigten Daten verwehrt? Diese Fragen können für ME 2 von zentraler Wichtigkeit sein.

Es ist sowohl wichtig den Überblick über die Art der Kontrollen zu behalten, hinsichtlich Frequenz und damit verbunden, Angemessenheit. Aber auch die Wahl der Instrumente ist wichtig: fortgeschrittene Logmanagement und Datamining Applikationen können die Begutachtung der Daten aus ME 1 (3.4.1) zwar vereinfachen, jedoch gibt es zur Auswertung lokale rechtliche Grenzen. Ist das Kontrollziel beispielsweise die der Ermittlung der Zahl der eingehenden eMails pro Mitarbeiter, spielt ME 3 eine zentrale Rolle, denn ME 2 hält sich an die rechtlichen Regelungen zum Erreichen des Kontrollziels.

3.4.3 ME 3: Sicherstellung der Einhaltung gesetzlicher Vorschriften

Die Angemessenheit der Kontrollmechanismen und Kontrollziele ist ein wichtiger Punkt bei der Erhebung von Statistiken. Wird im persönlichen eMail Verkehr der Mitarbeiter gemessen, ist unter Umständen darauf

zu achten, dass die Inhalte selbst nicht mitevaluiert werden, und dass damit notwendige Datenschutzrichtlinien eingehalten werden. Mitarbeiter müssen über den Hergang solcher Maßnahmen regelmäßig informiert werden. Zudem ist es oft notwendig Daten zu anonymisieren, sofern sie dem Board (3.4.4) als Statistik vorgelegt werden sollen. Maßnahmen aus ME 3 sollen nicht zur Überführung und Diskriminierung von Personal beitragen können.

Zwar kann es nötig sein einen globalen Spam Filter zu installieren (auch hinsichtlich DS 5, 3.3.5), um die Anzahl unbenötigter eingehender eMails zu senken, aber von Löschungen muss dann abgesehen werden, wenn die entsprechenden Daten digitales Eigentum des Mitarbeiters sind. Viele Maßnahmen können über entsprechende interne Policies durchgesetzt werden, wenn klar definiert ist, an welchen Stellen die Mittel aus ME 2 eingesetzt werden, sodass Mitarbeiter als informiert betrachtet werden können. Dies kann auch positive Auswirkungen auf die Produktivität haben.

3.4.4 ME 4: Sorgen für IT Governance

Um Policies in Unternehmen durchzusetzen benötigt man eine soziale Strategie. Es reicht nicht aus umfangreiche Regelwerke zur Benutzung von Systemen zu definieren (z. B. nach DS 5,3.3.5, DS 7 3.3.7 und DS 8, 3.3.8), die Systeme und die Systemnutzung zu kontrollieren (nach ME 2, 3.4.2). Ohne Executive Support können solche Richtlinien häufig ignoriert werden, und trotz bekannter und eventuell sogar notwendiger Maßnahmen, die sich mit relevanten statistischen Aussagen begründen lassen, wird der Unternehmenskörper nicht folgen.
Eine soziale Strategie kann die Bildung eines festen Management Boards sein, mit konkret definierten Verantwortungen in der Unternehmens-IT. Die Nicht-Einhaltung von Policies aus beispielsweise DS 5 (3.3.5) wird in der Regel anders betrachtet, wenn es einen entsprechenden Chief Security Officer (CSO) mit Personalkompetenz gibt. Die Einhaltung von Datenschutzrichtlinien wird zentraler gesehen, wenn es einen mit ausreichenden Kompetenzen ausgestatteten Datenschutzbeauftragten im Unternehmen gibt.

3.4.5 Beispiel

Der eMail Verkehr der FHL soll ausgewertet werden. Die Kontrollziele sind die Feststellung der Anzahl der Spam Mails jedes registrierten Nutzers, da vermehrt Cliet-seitige Malware Infektionen im eigenen Netzwerk registriert werden. Gemäß ME 1 ist das Kontrollziel zwar sehr schnell festgesetzt, jedoch stößt die Idee an konkrete rechtliche Grenzen (ME 3). Daher werden unternehmensweite Informationsmails vom Präsidium (Executive Buy-In nach ME 4) der FHL versandt, in dem die Maßnahmen umfassend begründet werden, da es für das interne Netz der Institution eine gesetzliche Sicherheitsverantwortung gibt.

Abschließend wird, um das neue automatisierte Verfahren mitzuevaluieren, eine Umfrage hinsichtlich der Spam-Frequenz gestartet, und hinsichtlich der False-Positives (ME 2).

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

Wade Baker, Alexander Hutton, C David Hylender, Joseph Pamula, D Ph, Marc Spitler, Mark Goudie, Christopher Novak, Mike Rosen, Peter Tippett, D Ph, Calvin Chang, and Jason Fisher. 2011 Data Breach Investigations Report. 2011.

Security Assessment Procedures. Payment Card Industry (PCI) Data Security Standard. *October*, (October), 2010.