# Hochschule Luzern HSLU

29. November 2024

**I.BA_ISM_MM.H2401 - GRUPPE 2**

# «Cobit V und ITIL: Security-Aspekte en Detail, 5 Praxisbeispiele für deren Verwendung»

Egger Etienne
Isenring Alenka
Lopez Manuel
Schmid Christian
Sustic Andrea

# I Arbeitsverteilung

EE = Egger Etienne, IA = Isenring Alenka, LM = Lopez Manuel, CS = Schmid Christian, SA = Sustic Andrea

| Kürzel | Kapitelnummer & Beschreibung | Anzahl Zeichen | Datum |
|---|---|---|---|
| EE | 1. Einführung | 1’740 | 12.10.2024 |
| EE | 5. Evaluation der Praxisbeispiele (Vergleich, Bewertung, Priorisierung) | 3’013 | 29.10.2024 |
| EE | Management Summary | 2’622 | 06.11.2024 |
| EE | 2. Methodik | 1’359 | 11.11.2024 |
| EE | Struktur, Formatierung, Korrektur | - | - |
| Total EE: | | 8’734 | |
| Kürzel | Kapitelnummer & Beschreibung | Anzahl Zeichen | Datum |
| IA | 3.2. COBIT (exkl. COBIT 2019) | 1’742 | 09.10.2024 |
| IA | 3.2.1 Ziele und Nutzen | 1’315 | 14.10.2024 |
| IA | 3.2.2 Die Grundprinzipien von COBIT | 4’546 | 14.10.2024 |
| IA | 3.2.3 Implementierungslebenszyklus | 2’045 | 19.10.2024 |
| IA | 3.2.4 Haupt- und Teilprozesse | 1’536 | 19.10.2024 |
| IA | 3.2.5 Security-Aspekte | 2’309 | 24.10.2024 |
| IA | Struktur, Formatierung, Korrektur, Abkürzungsverzeichnis | - | - |
| Total IA: | | 13’493 | |
| Kürzel | Kapitelnummer & Beschreibung | Anzahl Zeichen | Datum |
| LM | 6. Handlungsempfehlungen für Unternehmen | 6’035 | 19.10.2024 |
| LM | 7. Fazit und Ausblick | 3’008 | 04.11.2024 |
| LM | Struktur, Formatierung, Korrektur | - | - |
| Total LM: | | 9’043 | |
| Kürzel | Kapitelnummer & Beschreibung | Anzahl Zeichen | Datum |
| CS | 4. Praxisbeispiele | 9’437 | 19.10.2024 |
| CS | 3.2 COBIT V (COBIT 2019) | 1’105 | 04.11.2024 |
| CS | Entwurf, Struktur, Formatierung, Korrektur | - | - |
| Total CS: | | 10’542 | |
| Kürzel | Kapitelnummer & Beschreibung | Anzahl Zeichen | Datum |
| SA | 3.1. Überblick | 1’261 | 09.10.2024 |
| SA | 3.3. ITIL | 1’813 | 09.10.2024 |
| SA | 3.3.1. Haupt- und Teilprozesse | 2’807 | 18.10.2024 |
| SA | 3.3.2. Security-Aspekte | 4’391 | 10.11.2024 |
| SA | Struktur, Formatierung, Korrektur | - | - |
| Total SA: | | 10’272 | |
| **Total insgesamt:** | | **52’084** | |
| Einleitung bis Reflexion, ohne Verzeichnisse und evtl. Anhang: | | 49’462 | |

# II Management Summary

Diese Arbeit untersucht die IT-Frameworks COBIT V und ITIL, die für IT-Governance und IT-Service-Management verwendet werden. Beide Frameworks tragen erheblich zur Stärkung der IT-Sicherheit bei. COBIT V fördert durch eine strategische Ausrichtung der IT auf Unternehmensziele die IT-Governance, während ITIL die Effizienz und Qualität des operativen IT-Service-Managements verbessert. Zusammen ermöglichen sie eine umfassende Steuerung und Absicherung der IT-Prozesse.

COBIT V legt den Schwerpunkt auf Sicherheitsrisiken als Teil der IT-Governance und unterstützt ein systematisches Risikomanagement, das eine frühzeitige Identifikation und Bewertung von Bedrohungen erleichtert. ITIL integriert Sicherheitsanforderungen umfassend in die Service-Design- und Betriebsprozesse und gewährleistet so die Vertraulichkeit, Integrität und Verfügbarkeit von IT-Diensten.

Die Praxisbeispiele zeigen, dass in stark regulierten Bereichen wie dem Gesundheitswesen und dem Finanzwesen hilft COBIT V vor allem bei der Compliance und Governance. ITIL hingegen bietet im IT-Service-Management Effizienzgewinne und Qualitätsverbesserungen. Die kombinierte Anwendung beider Frameworks erweist sich als vorteilhaft für Organisationen, die sowohl starke IT-Governance als auch flexible Serviceprozesse benötigen, beispielsweise in der Technologie- und Energiebranche.

**Empfehlungen**

Durch die Analyse der Frameworks und den Praxisbeispielen ergab, dass die folgenden vier Punkte bei der Implementierung empfehlenswert sind:

1. **Governance-Strukturen aufbauen**: Klare Zuständigkeiten und regelmässige Audits tragen dazu bei, Sicherheitsverantwortlichkeiten und Compliance sicherzustellen.
2. **Sicherheitsbewusstsein fördern**: Regelmässige Schulungen für alle Mitarbeitenden sind erforderlich, um das Sicherheitsbewusstsein zu stärken und Risiken durch menschliche Fehler zu reduzieren.
3. **Robustes Incident- und Change-Management implementieren**: ITIL-Prozesse unterstützen eine schnelle Reaktion und Anpassung bei sicherheitsrelevanten Vorfällen.
4. **Systematisches Risikomanagement**: Regelmässige Bedrohungsanalysen und geeignete Überwachungsprozesse helfen, Schwachstellen frühzeitig zu erkennen und zu bewältigen.

Die Weiterentwicklung und Integration von COBIT V und ITIL wird angesichts der zunehmenden Digitalisierung und Cloud-Nutzung zunehmend wichtiger. Automatisierung bieten neue Möglichkeiten, Sicherheitsbedrohungen in Echtzeit zu erkennen und menschliche Fehler noch weiter zu minimieren. Die Kombination von COBIT und ITIL schafft eine fundierte Basis für effektive IT-Governance und IT-Sicherheit in modernen Unternehmen.

# III Inhaltsverzeichnis

# 1 Einführung

Frameworks wie COBIT V und ITIL bieten standardisierte Methoden für die Steuerung und Verwaltung von IT-Services sowie der IT-Governance. Diese standardisierten Methoden ermöglichen es, Cyberbedrohungen präventiv entgegenzutreten und die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu schützen.

Diese Arbeit zielt darauf ab, das Verständnis der Frameworks COBIT V und ITIL zu vertiefen, indem der Fokus auf die Sicherheitskomponenten dieser Ansätze gelegt wird. Es werden die Methoden von COBIT V und ITIL aufgezeigt, die zur Verbesserung der Informationssicherheit beitragen können. Anhand von Praxisbeispielen wird die Anwendung von COBIT V und ITIL veranschaulicht.

**Ziele**

- Analyse der grundlegenden Prinzipien und Konzepte von COBIT V und ITIL.
- Systematische Untersuchung der sicherheitsrelevanten Funktionen beider Frameworks.
- Detaillierte Differenzierung der Prozesse in Haupt- und Teilprozesse zur Identifikation ihrer Beiträge zur IT-Sicherheit.
- Darstellung praxisnaher Umsetzungsbeispiele von COBIT V und ITIL.

**Relevanz und Bedeutung des Projekts**

Die Untersuchung der Frameworks COBIT V und ITIL bieten wertvolle Erkenntnisse für IT-Verantwortliche und Fachpersonen im Bereich der Informationssicherheit. Durch die Analyse der Sicherheitsaspekte in Verbindung mit Praxisbeispielen wird eine Grundlage für eine fundierte Diskussion über die Nutzung von IT-Governance-Frameworks im Bereich der Informationssicherheit geschaffen.

**Disclaimer / Anmerkung zur Arbeit**

Die verwendeten Quellen und Fachwörter sind teilweise auf Englisch. Um die Lesbarkeit zu wahren, wurden die Fachbegriffe ins Deutsche übersetzt. Zur Verdeutlichung sind die englischen Originalbegriffe in Klammern neben der übersetzten Form angegeben.

# 2 Methodik

Zu Beginn dieser Arbeit wurde ein Projektplan erstellt, um die vorliegende Untersuchung in kleinere, befristete Arbeitspakete zu unterteilen. Anschliessend wurde das Dokument strukturiert, wobei die Strukturierung an die Vorlage «Aufbau WIPRO/BAA-Bericht» von Jörg Hofstetter der HSLU angelehnt ist. Kapitel der Vorlage, die nicht zur vorliegenden Arbeit passten, wurden entfernt, während andere hinzugefügt wurden. Nach der Strukturierung des Dokuments wurden die Themenbereiche COBIT, ITIL und Praxisbeispiele grob aufgeteilt. Die Recherche stützt sich auf Fachbücher, Fachartikel und relevante Websites. Die Suche erfolgt hauptsächlich über Google Scholar und die Bibliothek der HSLU.

Um den Fortschritt sicherzustellen, finden wöchentliche Meetings statt, in denen besprochen wird, welche Aufgaben in der vergangenen Woche abgeschlossen wurden und welche in der kommenden Woche anstehen. Dabei wird regelmässig überprüft, ob der Arbeitsfortschritt dem Zeitplan des Projektplans entspricht. Nach Abschluss aller Kapitel beginnt die Korrekturphase, in der das gesamte Dokument detailliert auf grammatikalische, stilistische und sprachliche Fehler geprüft und korrigiert wird.

Mit dieser Methodik sieht sich die Autorenschaft zuversichtlich, die Arbeit den qualitativen Anforderungen einer wissenschaftlichen Untersuchung entsprechend abzuschliessen.

# 3 Literaturarbeit

## 3.1 Überblick

Das vorliegende Kapitel gibt einen Überblick über die Grundlagen und Prinzipien von COBIT V und ITIL. Dabei liegt der Schwerpunkt auf den sicherheitsrelevanten Aspekten. IT-Governance-Frameworks wie COBIT V und ITIL stellen Werkzeuge zur Steuerung und Optimierung von IT-Prozessen in Unternehmen bereit. COBIT V (Control Objectives for Information and Related Technologies) ist ein Framework für das Management und die Governance von IT-Systemen, während ITIL (Information Technology Infrastructure Library) Best Practices für das IT-Service-Management bereitstellt *(Harmer, 2014) (AXELOS, 2019).*

Beide Frameworks zielen darauf ab, IT-Prozesse so zu strukturieren und zu optimieren, dass sie die Geschäftsziele eines Unternehmens bestmöglich unterstützen. Dabei ist ITIL stärker auf das operative Management und COBIT V auf die Governance und Kontrolle ausgerichtet *(Moeller, 2013).*

Die komplementäre Natur von COBIT V und ITIL zeigt sich in ihrer gegenseitigen Ergänzung: COBIT V bietet das strategische Gerüst für die IT-Governance, während ITIL die operativen Details zur Erbringung von IT-Dienstleistungen liefert. Zusammen ermöglichen sie eine umfassende und effiziente Steuerung der IT-Prozesse, insbesondere im Hinblick auf Sicherheitsaspekte.

## 3.2 COBIT V

COBIT steht für „Control Objectives for Information and Related Technology“ und wurde 1996 von der Organisation ISACA (Information Systems Audit and Control Association) als Framework zur Bewertung und Steuerung von internen und externen Audits entwickelt. Im Laufe der Jahre wurde es kontinuierlich weiterentwickelt, um den wachsenden Anforderungen der Informationstechnologie (IT) gerecht zu werden *(Andenmatten, 2018).* Die zweite und dritte Version des COBIT-Frameworks, die in den Jahren 1998 und 2000 veröffentlicht wurden, erweiterten das ursprüngliche Framework durch zusätzliche Kontroll- und Managementrichtlinien *(Andenmatten, 2018).*

Mit der Veröffentlichung von COBIT V im Jahr 2012 wurden das Framework bedeutend überarbeitet und erweitert, um den Anforderungen moderner Unternehmen gerecht zu werden und die neusten Technologien und Geschäftstrends im Bereich Information und Technologie (I&T), wie die Digitalisierung, zu berücksichtigen. COBIT V vereint und integriert verschiedene Frameworks, darunter COBIT 4.1, Val IT 2.0, das Risk IT Framework, das «IT Assurance Framework» (ITAF) und das «Business Model for Information Security» (BMIS). Dadurch entstand ein einheitliches und umfassendes Framework, dass die Steuerung und Verwaltung von IT-Ressourcen unterstützt *(Harmer, 2014, Chapter 4).*

Darüber hinaus wurde COBIT V auf andere bekannte Standards und Frameworks wie ITIL, ISO, PMBOK, PRINCE2 und TOGAF abgestimmt, sodass es sich ohne Probleme integrieren lässt *(IT Governance, n.d.).* Diese Anpassung erleichtert es Unternehmen, Best Practices in ihre bestehenden IT-Prozesse zu implementieren und ihre IT-Ressourcen optimal zu nutzen, um ihre strategischen Unternehmensziele zu erreichen *(Andenmatten, 2018).*

Ende 2018 veröffentlichte ISACA die neuste Version von COBIT unter dem Namen «COBIT 2019». Die aktualisierte Version von COBIT V ist vollständiger und schlüssiger auf die technischen Entwicklungen und Geschäftsanforderungen ausgerichtet. COBIT 2019 bietet ein modularisiertes Design und fokussiert sich auf agile Methoden. Durch neu definierte «Focus Areas» kann das Governance-System an unterschiedliche Bedürfnisse angepasst werden *(Andenmatten, 2018).*

Zusätzlich integriert COBIT 2019 ein neues Designfaktor-Modell, welches das Anwenden des COBIT-Frameworks vereinfacht. Designfaktoren wie Organisationsstrukturen, Compliance-Anforderungen und IT-bezogene Risiken helfen bei der eigentlichen Governance und Managementlösung *(Harisaiprasad, 2020).*

Grundlegend setzt COBIT 2019 auf Flexibilität, Dynamik und eine stärkere Einbindung von Stakeholdern. Best Practices aus anderen bekannten Frameworks (ITIL und ISO 27001) wurden weiter und stärker integriert, um Compliance- und Sicherheitsanforderungen besser abzudecken.

Da sich diese Arbeit auf COBIT V fokussiert, wird die Version 2019 nur kurz erläutert.

### 3.2.1 Ziel und Nutzen

COBIT V erkennt die Bedeutung der IT in modernen Unternehmen und die steigende Abhängigkeit von externen Partnern, wie IT-Dienstleistern und Outsourcing-Anbietern. Das Framework bietet ein Informationsmodell, das Unternehmen unterstützt, die zunehmende Menge an Informationen zu verwalten und relevante Daten für fundierte Geschäftsentscheidungen auszuwählen.

Durch die Implementation von geeigneten Organisationsstrukturen, Richtlinien und einer guten Unternehmenskultur stellt COBIT V sicher, dass IT-Services nicht nur technisch korrekt, sondern auch strategisch auf die Unternehmensziele abgestimmt sind. COBIT V hilft dabei einen Wert zu schaffen, die Benutzer zufriedenzustellen und gesetzliche Vorschriften einzuhalten. Das Framework bietet damit gleichzeitig Prozesse zur Steuerung von IT-Lösungen wie «Bring Your Own Device» (BYOD) oder IT-Outsourcing *(Harmer, 2014, Chapter 4)*.

COBIT V umfasst nicht nur IT-Governance, sondern betrachtet das Unternehmen als ein umfassendes System, das sowohl IT-Funktionalitäten als auch End-to-End-Geschäfts-Funktionen umfasst. Dabei berücksichtigt das Framework die Interessen und Anforderungen sowohl interner als auch externer Stakeholder, um eine umfassende Governance und eine effizientes Management der IT für das gesamte Unternehmen zu gewährleisten *(ISACA, 2012)*.

### 3.2.2 Die Grundprinzipien von COBIT V

COBIT V basiert auf fünf grundlegenden Prinzipien, die sicherstellen, dass das Framework flexibel in Unternehmen angewendet werden kann:

**Prinzip 1: Den Bedürfnissen der Stakeholder gerecht werden**

Die Unternehmensführung muss die Bedürfnisse der Stakeholder verstehen, um erfolgreiche Entscheidungen über Nutzen, Risiken und Ressourcen treffen zu können. COBIT V hilft dabei diese Bedürfnisse systematisch zu erfassen und zu bewerten *(Harmer, 2014, Chapter 4)*. Mit Hilfe der COBIT V Zielkaskade können Unternehmen anhand einer Zuordnungstabelle, die Bedürfnisse ihrer Stakeholder mit den Unternehmenszielen, den IT-bezogenen Zielen und den Enabler-Zielen vergleichen. Die Zielkaskade übersetzt dabei wichtige Unternehmensziele in spezifische IT-Ziele und verknüpft diese mit den entsprechenden Prozessen und Praktiken *(ISACA, 2012, p. 20).*

**Prinzip 2: Das gesamte Unternehmen durchgängig abdecken**

COBIT V verfolgt einen ganzheitlichen Ansatz zur Steuerung und Verwaltung der Unternehmens-IT, indem das Unternehmen als ein Gesamtsystem betrachtet wird. Das Framework deckt alle Funktionen und Prozesse ab, die für die Steuerung und das Management von Informationen und damit verbundenen Technologien erforderlich sind. Dabei wird die IT-Governance nahtlos in die Unternehmenssteuerung integriert, wobei sowohl interne als auch externe IT-Dienste und Geschäftsprozesse berücksichtigt werden. Durch diesen Ansatz unterstützt COBIT V Unternehmen dabei, ihre IT-Strategien an den Geschäftsziele auszurichten und eine einheitliche Sicht auf die Governance und das Management zu entwickeln *(ISACA, 2012, p. 23).*

**Prinzip 3: Anwendungen eines einzigen integrierten Frameworks**

Mit COBIT V wurden verschiedene Standards und Frameworks in eine einheitliche Struktur integriert. Durch die Zusammenführung der verschiedenen Standards und bewährten Praktiken bietet COBIT V umfassende und übersichtliche Anleitungen für verschiedene IT-Aktivitäten, wodurch die Komplexität reduziert wird, da relevante IT-Aktivitäten nahtlos in das System integriert werden können *(ISACA, 2012)*. Dies ermöglicht es Unternehmen, ihre IT-Prozesse effizienter zu steuern, bestehende Frameworks einfach zu integrieren und eine einheitliche Vorgehensweise in ihren IT-Managementprozessen zu implementieren *(Harmer, 2014, Chapter 4)*.

**Prinzip 4: Einen ganzheitlichen Ansatz ermöglichen**

Um eine übergreifende IT- Governance und ein effektives Management zu ermöglichen, definiert COBIT V sieben Enabler, die als Bausteine zur Steuerung, Verwaltung und Erreichung der IT-Unternehmensziele dienen *(Harmer, 2014, Chapter 4)*.

1. **Grundsätze, Richtlinien und Rahmenbedingungen:** Diese legen die grundlegenden Regeln und Leitlinien für das Verhalten der Organisation fest.
2. **Prozesse:** Beschreiben die Aktivitäten, die zur Erreichung der Unternehmensziele erforderlich sind und helfen bei der Definition von Rollen und Verantwortlichkeiten.
3. **Organisationsstrukturen:** Stellen sicher, dass die Struktur der Organisation die Governance und das Management der IT unterstützt, indem sie klare Berichts- und Kommunikationswege schafft.
4. **Kultur, Ethik und Verhalten:** Fördern ein Arbeitsumfeld, das verantwortungsbewusstes Handeln und ethische Entscheidungsfindung unterstützt.
5. **Auskunft:** Gewährleisten, dass die richtigen Informationen zur richtigen Zeit für die richtigen Personen zur Verfügung stehen, um fundierte Entscheidungen zu treffen.
6. **Dienste, Infrastruktur und Anwendungen**: Beziehen sich auf die technischen Ressourcen, die zur Bereitstellung von IT-Services erforderlich sind, und deren effektive Nutzung.
7. **Menschen, Fähigkeiten und Kompetenzen:** konzentrieren sich auf die Qualifikationen und Kompetenzen der Mitarbeiter, um sicherzustellen, dass das Unternehmen über das notwendige Wissen und die Fähigkeiten verfügt, um seine Ziele zu erreichen.

**Prinzip 5: Trennung von Governance und Management**

COBIT V unterscheidet klar zwischen Governance und Management, da beide Disziplinen unterschiedliche Aktivitäten umfassen, verschiedene Organisationsstrukturen erfordern und unterschiedlichen Zwecken dienen. Governance stellt sicher, dass die Bedürfnisse, Bedingungen und Optionen der Stakeholder bewertet werden, um ausgewogene Unternehmensziele festzulegen. Die Governance gibt die strategische Richtung vor, priorisiert und trifft Entscheidungen, um die Leistung zu überwachen. Im Gegensatz dazu plant, baut, leitet und überwacht das Management die Aktivitäten gemäss den Vorgaben des Leitungsorgans, um die Unternehmensziele zu erreichen *(ISACA, 2012, p. 32)*.

### 3.2.3 Implementationslebenszyklus

Bei der Implementierung von COBIT V handelt es sich um einen fortlaufenden Prozess, der kontinuierlich verbessert werden muss. Dazu bietet COBIT V einen Implementierungslebenszyklus, der Unternehmen hilft die Komplexität und die Herausforderungen, die bei der Implementierung typischerweise auftreten zu bewältigen *(ISACA, 2012, p. 37)*.

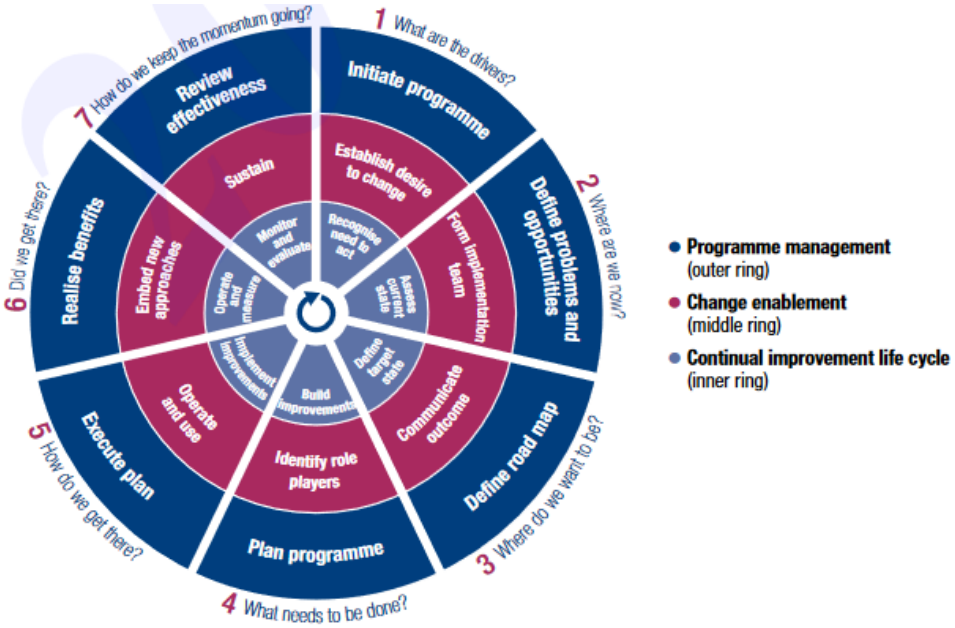


*Abbildung 1: Die sieben Phasen des Implementationslebenszyklus (ISACA, 2012)*

Der Lebenszyklus umfasst sieben Kernphasen (siehe Abbildung 1):

1. **Einführungsphase**: In dieser Phase wird die Notwendigkeit für eine Initiative zur Umsetzung oder Verbesserung der Situation erkannt, sowie die aktuellen Probleme und Auslöser identifiziert.
2. **Definitionsphase**: Der Umfang der Initiative wird mithilfe der COBIT V-Zuordnungstabelle definiert, die Unternehmensziele mit IT-Zielen und zugehörigen IT-Prozessen verknüpft.
3. **Analysephase**: In dieser Phase wird ein Verbesserungsspielraum festgelegt. Mithilfe von COBIT V Leitlinien werden Lücken und mögliche Lösungen identifiziert, wobei Lösungen mit hohem Nutzen und einfacher Umsetzung priorisiert werden.
4. **Planungs- und Projektphase**: Praktische Lösungen werden geplant, indem Projekte definiert werden, die durch nachvollziehbare Business Cases gestützt werden. Ebenso wird ein Änderungsplan für die Implementierung entwickelt.
5. **Implementierungsphase**: Die vorgeschlagenen Lösungen werden in der täglichen Arbeit umgesetzt. Dabei werden Massnahmen anhand der COBIT V-Ziele und Kennzahlen definiert und überwacht, um sicherzustellen das Unternehmensziele erreicht werden können.
6. **Betriebs- und Überwachungsphase**: In dieser Phase wird überprüft, ob die neuen oder verbesserten Enabler nachhaltig betrieben werden und ob die erwarteten Vorteile erreicht werden.
7. **Evaluations- und Verbesserungsphase:** In der letzten Phase wird überprüft, ob die Ziele erreicht wurden. Dabei werden weiter Anforderungen an die Governance oder das Management der IT identifiziert und allenfalls weitere Verbesserungsmassnahmen getroffen *(ISACA, 2012, p. 38)*.

### 3.2.4 Haupt- und Teilprozesse

COBIT V umfasst insgesamt 37 Prozesse, die in fünf Domänen unterteilt sind. Dabei werden die Prozesse in zwei Hauptgruppen unterteilt: die Prozesse für die Governance der Unternehmens-IT und der Prozesse, die Leitlinien für das Management der Unternehmens-IT bereitstellen *(Moeller, 2013, Chapter 5).*

Die Governance-Domäne **Evaluieren, Leiten und Überwachen (EDM)** besteht aus fünf Prozessen, die sicherstellen, dass die IT-Strategien eng mit den Unternehmenszielen verknüpft sind. Diese Prozesse unterstützen die Unternehmensführung dabei, fundierte Entscheidungen zu treffen und den Mehrwert der IT für das Unternehmen zu steigern *(Harmer, 2014, Chapter 6).*

Die vier Managementdomänen umfassen die restlichen 32 Prozesse und sind wie folgt unterteilt:

- **Ausrichten, Planen und Organisieren (APO):** Die Prozesse dieser Domäne stellen sicher, dass die IT-Strategien und -Ressourcen optimal auf die Unternehmensziele abgestimmt sind.
- **Erstellen, Erwerben und Implementieren (BAI):** In dieser Domaine liegt der Fokus auf der Entwicklung und Einführung neuer IT-Lösungen, sowie der Planung und Durchführung von Projekten.
- **Lieferung, Service und Support (DSS):** Dieser Bereich befasst sich mit der Bereitstellung von IT-Diensten und -Support, um die Zufriedenheit der Nutzer zu gewährleisten.
- **Bewerten, leiten und überwachen (MEA):** In diesem Bereich erfolgt die kontinuierliche Bewertung und Überwachung der IT-Leistung, um sicherzustellen, dass die IT-Dienste den Anforderungen entsprechen *(Harmer, 2014, Chapter 6).*

### 3.2.5 Security-Aspekte

COBIT V ist ein umfassendes Framework für die IT-Governance, das grossen Wert auf Sicherheitsaspekte legt. Eines der Grundprinzipien von COBIT V ist die Berücksichtigung der Bedürfnisse aller Stakeholder, einschliesslich ihrer Sicherheitsbedenken. Dabei gehört zu den spezifischen Anforderungen, die COBIT V identifiziert, die Frage, ob alle IT-bezogenen Risiken, wie Sicherheits- und Datenschutzrisiken angemessen adressiert werden *(Moeller, 2013, Chapter 5).*

Ein wichtiger Prozess für die Sicherheit ist „Manage Security“ (DSS7), der darauf abzielt, Sicherheitsstrategien eng mit den Zielen des Unternehmens zu verknüpfen. Dadurch wird nicht nur der Schutz vertraulicher Daten sichergestellt, sondern auch die Integrität und Verfügbarkeit von Informationen, die für den Geschäftsbetrieb entscheidend sind *(Moeller, 2013, Chapter 5).*

Ein weiterer wichtiger Sicherheitsaspekt von COBIT V ist das Risikomanagement. COBIT V empfiehlt ein effektives Risikomanagement einzuführen, das alle Bereiche der IT-Sicherheit abdeckt. Dazu gehören das Identifizieren und Bewerten von Sicherheitsrisiken sowie die Entwicklung geeigneter Kontrollen zur Minderung dieser Risiken. Das Framework empfiehlt, Schulungs- und Sensibilisierungsmassnahmen einzuführen, um sicherzustellen, dass alle Mitarbeiter die Sicherheitsrichtlinien und -verfahren verstehen und befolgen. Zudem betont COBIT V die Notwendigkeit regelmässiger Audits zur Überwachung und Bewertung der Sicherheitsmassnahmen. Diese Audits helfen, Schwachstellen frühzeitig zu identifizieren und erforderliche Anpassungen vorzunehmen, um den dynamischen Bedrohungen in der IT-Welt zu begegnen *(Moeller, 2013, Chapter 5).*

Durch die enge Verknüpfung von Governance und Management stellt COBIT V sicher, dass Sicherheitsaspekte nicht isoliert betrachtet werden. Diese einheitliche Governance-Struktur ermöglicht es Unternehmen, klare Verantwortlichkeiten für Sicherheitsfragen festzulegen und sicherzustellen, dass alle Abteilungen zusammenarbeiten, um ein hohes Sicherheitsniveau aufrechtzuerhalten. Auf diese Weise trägt COBIT V nicht nur zur Verbesserung der IT-Sicherheit bei, sondern hilft auch, gesetzliche Anforderungen und Compliance-Vorgaben zu erfüllen, die für Unternehmen in der heutigen Zeit entscheidend sind *(Moeller, 2013, Chapter 5).*

## 3.3 ITIL

ITIL wurde in den 1980er Jahren von der britischen Regierung entwickelt, um die Qualität von IT-gestützten Dienstleistungen und IT-Projekten zu optimieren. Im Jahr 2000 nutzte Microsoft ITIL, um das Microsoft Operations Framework zu entwickeln, und im Jahr 2001 wurde Version 2 von ITIL veröffentlicht. Im Jahr 2007 wurde Version 3 von ITIL veröffentlicht. Diese basiert auf einem Service-Lebenszyklus, der die folgenden Phasen umfasst: Service-Strategie, Service-Design, Service-Übersetzung, Service-Betrieb und kontinuierliche Selbstverbesserung *(Moeller, 2013)*. Die neueste Version von ITIL (ITIL 4) wurde 2019 veröffentlicht und hat sich zu einem wertorientierten Ansatz entwickelt, der mit anderen Managementpraktiken und Arbeitsweisen integriert werden kann *(AXELOS, 2019)*.

Das zentrale Element von ITIL 4 ist das Service Value System (SVS), das beschreibt, wie Organisationen alle Aktivitäten und Ressourcen koordinieren, um Wert für ihre Stakeholder zu schaffen. Das SVS umfasst fünf Kernkomponenten, die eng miteinander vernetzt sind, um eine konsistente und effiziente Bereitstellung von IT-Diensten sicherzustellen *(AXELOS, 2019)*:

1. **Service-Wertschöpfungskette (Service Value Chain)**: Operatives Zentrum des SVS, das alle Aktivitäten zur Erstellung und Bereitstellung von Diensten beschreibt.
2. **Governance**: Steuerung und Kontrolle, die sicherstellt, dass strategische Ziele erreicht werden.
3. **Practices**: Spezifische Methoden und Ressourcen, die zur Umsetzung operativer Aufgaben eingesetzt werden.
4. **Leitprinzipien (Guiding Principles)**: Allgemeine Leitlinien, die für alle Aktivitäten und Entscheidungen der Organisation gelten.
5. **Kontinuierliche Verbesserung (Continual Improvement)**: Durchgängiger Prozess, der Feedback und Analysen nutzt, um Dienstleistungen und Prozesse stetig zu optimieren.

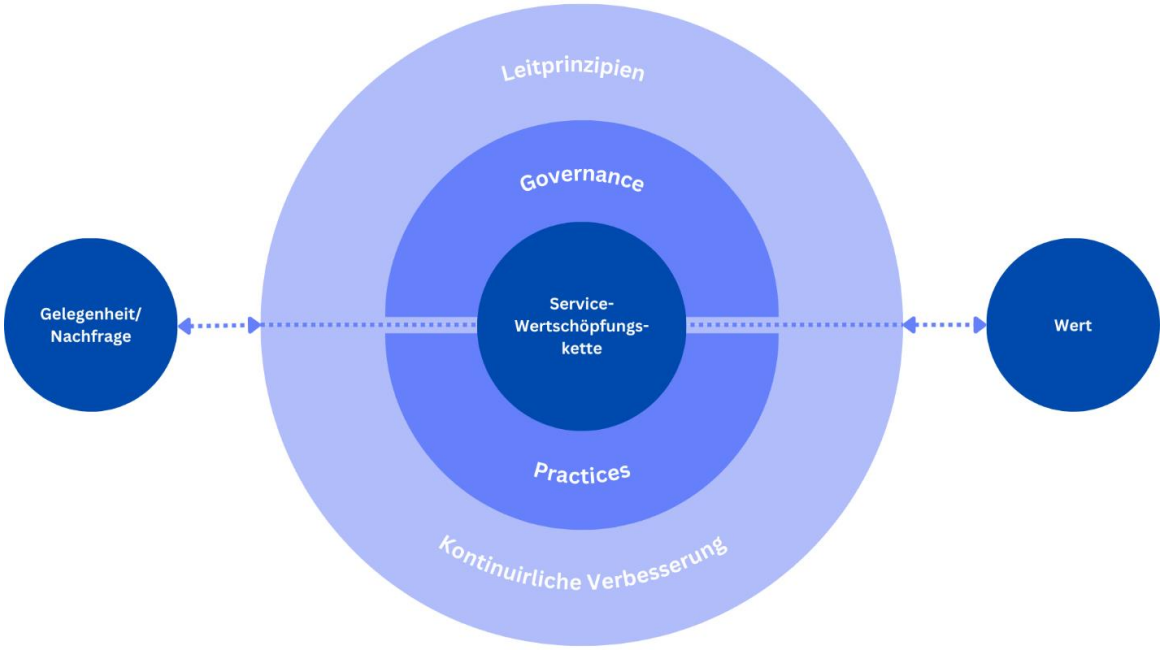


*Abbildung 2: Der Service Value System (Selbstgemacht)*

### 3.3.1 Haupt- und Teilprozesse

**Service-Wertschöpfungskette**

Die Service-Wertschöpfungskette setzt sich aus sechs Hauptaktivitäten zusammen, die in einem dynamischen und nicht-linearen Prozess miteinander verknüpft sind *(AXELOS, 2019)*:

1. **Plan**: Strategische Ausrichtung und langfristige Planung auf Basis der Stakeholder-Bedürfnisse.
2. **Engage**: Einbindung und Berücksichtigung von Stakeholder-Anforderungen.
3. **Design and Transition**: Entwicklung und Übergabe neuer oder geänderter Dienste.
4. **Obtain and Build**: Erwerb und Entwicklung der für die Dienstbereitstellung erforderlichen Ressourcen.
5. **Deliver and Support**: Operative Bereitstellung und laufende Unterstützung von IT-Diensten.
6. **Improve**: Fortlaufende Optimierung auf Basis von Feedback und Analysen.

Diese Aktivitäten stehen in einem dynamischen, nicht-linearen Verhältnis und ermöglichen eine flexible Reaktion auf spezifische Anforderungen. Beispielsweise kann „Engage“ direkt in „Deliver and Support“ übergehen, wenn dies für eine schnelle Reaktion auf Kundenanforderungen erforderlich ist.

**Governance**

Die Governance umfasst zwei zentrale Aufgaben *(AXELOS, 2019)*:

- **Leiten (Direct)**: Strategische Ziele und Richtlinien setzen.
- **Überwachen (Monitor)**: Die Einhaltung dieser Ziele und Richtlinien sicherstellen.

Sicherheitsaspekte und gesetzliche Vorgaben sind integrale Bestandteile dieser Governance.

**Practices**

ITIL definiert 34 Practices, die in drei Kategorien unterteilt sind *(AXELOS, 2019)*:

- **General Management Practices**: Allgemeine Geschäftsaktivitäten wie Risikomanagement oder Finanzmanagement.
- **Service Management Practices**: Direkte Verwaltung von IT-Diensten, wie Incident Management oder Change Control.
- **Technical Management Practices**: Unterstützen technische Umsetzung, wie Deployment Management oder Infrastrukturmanagement.

Practices sind nicht fest an einzelne Aktivitäten der Wertschöpfungskette gebunden, sondern können flexibel integriert werden. Beispielsweise kann „Incident Management“ sowohl in „Deliver and Support“ als auch in „Improve“ verwendet werden, je nach spezifischer Anforderung.

**Leitprinzipien**

Die Leitprinzipien umfassen sieben Kernaussagen, die Organisationen als Grundlage für Entscheidungen und Verhaltensweisen dienen *(AXELOS, 2019)*:

1. Fokus auf den Wert
2. Beginne dort, wo du stehst
3. Schrittweise vorgehen mit Feedback
4. Zusammenarbeit fördern und Transparenz schaffen
5. Ganzheitlich denken und arbeiten
6. Halte es einfach und praktisch
7. Optimieren und automatisieren

**Kontinuierliche Verbesserung**

Die kontinuierliche Verbesserung gewährleistet eine fortlaufende Optimierung von Dienstleistungen und Prozessen. Diese erfolgt auf Basis von Leistungskennzahlen, Rückmeldungen und neuen Anforderungen. Der Prozess ist dabei nicht auf eine spezifische Aktivität beschränkt, sondern integriert sich in alle Bereiche *(AXELOS, 2019)*.

### 3.3.2 Security-Aspekte

Die Integration der Sicherheitsaspekte in die ITIL-Struktur erfolgt umfassend und systematisch, bei dem Sicherheitsaspekte auf allen Ebenen des SVS integriert sind. Ziel ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Systemen sicherzustellen, um sowohl strategische als auch operative Ziele der Organisation zu unterstützen *(AXELOS, 2019)*.

**Service-Wertschöpfungskette**

Die Service-Wertschöpfungskette integriert Sicherheitsaspekte in alle Aktivitäten zur Bereitstellung von Dienstleistungen:

- **Plan**: Sicherheitsanforderungen werden definiert und strategisch auf die Organisationsziele abgestimmt. Dazu gehören Richtlinien wie Zugriffskontrollen, Datensicherung und Notfallpläne, die die Grundlage für weitere Aktivitäten bilden *(AXELOS, 2019)*.
- **Engage**: Stakeholder werden aktiv in die Sicherheitsplanung eingebunden, um ihre Anforderungen und potenziellen Risiken frühzeitig zu berücksichtigen *(AXELOS, 2019)*.
- **Design and Transition**: Sicherheitsmassnahmen werden in den Designprozess integriert, unterstützt durch Richtlinien und Standards, die sicherstellen, dass neue Dienste den Anforderungen entsprechen *(Moeller, 2013)*.
- **Obtain/Build**: Sicherheitskontrollen sind Teil von Entwicklungs- und Beschaffungsprozessen. Beispielsweise wird geprüft, ob neue Software die Sicherheitsanforderungen erfüllt oder ob sichere Codierungspraktiken bei der Entwicklung genutzt werden *(AXELOS, 2019)*.
- **Deliver and Support**: Sicherheitsstandards werden überwacht, und das Incident Management sorgt für frühzeitige Erkennung, Klassifizierung und Behebung von Sicherheitsvorfällen *(Moeller, 2013)*.
- **Improve**: Erkenntnisse aus Vorfällen, Audits und kontinuierlicher Überwachung fliessen in die Optimierung von Sicherheitsmassnahmen ein, etwa durch verbesserte Prozesse oder neue Werkzeuge *(AXELOS, 2019)*.

**Governance**

Definiert die strategischen Sicherheitsrichtlinien der Organisation, überwacht deren Umsetzung und stellt sicher, dass alle Aktivitäten den strategischen Zielen und gesetzlichen Vorgaben entsprechen. Ein Beispiel hierfür ist die Integration von Sicherheitsanforderungen in die Richtlinien für Servicebereitstellung und -support, die es ermöglichen, Risiken proaktiv zu minimieren *(AXELOS, 2019)*.

**Practices**

Die ITIL-Practices bieten operative Methoden zur Umsetzung der Sicherheitsziele:

- **Informationssicherheitsmanagement (Information Security Management):** Systematische Planung, Umsetzung und Überwachung von Sicherheitsmassnahmen *(AXELOS, 2019)*.
- **Verfügbarkeitsmanagement (Availability Management):** Sicherstellung der System- und Dienstverfügbarkeit, auch bei Sicherheitsvorfällen. Beispielsweise durch Redundanz oder Backups *(Moeller, 2013)*.
- **Kontinuitätsmanagement (Continuity Management):** Planung und Test von Massnahmen zur Wiederherstellung der IT-Services nach Vorfällen *(Moeller, 2013)*.
- **Vorfallmanagement (Incident Management):** Schnelle Erkennung, Klassifizierung und Behebung von Sicherheitsvorfällen zur Schadensminimierung *(Moeller, 2013)*.
- **Problem Management:** Analyse von Ursachen und Entwicklung von Massnahmen zur Vermeidung zukünftiger Sicherheitsvorfälle *(AXELOS, 2019)*.
- **Change Control:** Prüfung von Änderungen auf potenzielle Sicherheitsrisiken vor Genehmigung und Umsetzung *(AXELOS, 2019)*.
- **Zugriffsmanagement (Access Management):** Sicherstellung, dass nur autorisierte Personen Zugang zu Systemen und Informationen haben *(AXELOS, 2019)*.

Die prozessübergreifende Sicherheitsintegration verringert Risiken, gewährleistet die Einhaltung von Vorschriften und schützt Unternehmensressourcen sowie Kundendaten.

**Leitprinzipien**

Fordert, dass Sicherheit als zentraler Wert alle Prozesse und Aktivitäten durchdringt. Prinzipien wie „Fokus auf den Wert“ und „Zusammenarbeit fördern“ unterstreichen, dass Sicherheitsaspekte nicht als getrennte Aufgaben betrachtet werden dürfen. Alle Abteilungen und Stakeholder, einschliesslich IT und Management, müssen gemeinsam Sicherheitsziele verfolgen und eine Kultur schaffen, in der jeder seine Verantwortung wahrnimmt *(AXELOS, 2019).*

**Kontinuierliche Verbesserung**

Das Feedback aus Sicherheitsvorfällen, Audits und (externen) Bedrohungsanalysen dient der Identifikation von Schwachstellen und der Anpassung von Sicherheitsmassnahmen. Beispielsweise kann ein Vorfallbericht zur Verbesserung der Authentifizierungsprozesse oder zur Einführung zusätzlicher Massnahmen gegen Datenlecks führen *(AXELOS, 2019).*

# 4 Praxisbeispiele

Die Anwendungen von COBIT V und ILIT können in verschiedenen Branchen und Organisationen je nach spezifischen An- und Herausforderungen variieren. Während COBIT V hauptsächlich als Framework für IT-Governance eingesetzt wird, wird ITIL für die Optimierung des IT-Service-Managements verwendet. Dies ist auch in verschiedensten Praxisbeispielen ersichtlich. Unternehmen, welche ausschliesslich COBIT V implementieren, fokussieren sich auf Überwachung von Kontrollmechanismen und Ressourcenoptimierung *(ISACA, 2012)*. Unternehmen, welche ITIL implementieren, steuern eher auf bessere Servicequalität durch effizientere IT-Prozesse zu *(AXELOS, 2019)*.

In den folgenden Kapiteln werden fünf reale Praxisbeispiele analysiert. Es wird Wert daraufgelegt Beispiele rauszusuchen, welche rein COBIT V, rein ITIL oder eine Kombination aus Beidem nutzen und implementieren. Aus Vertraulichkeits- und Datenschutzgründen nutzen einige Unternehmen Non-Disclosure Agreements (NDAs), um ihre Kunden zu schützen.

## 4.1 Beispiel 1: Governance im Gesundheitswesen

**Beschreibung der Organisation/Branche**

Die Organisation ist ein führender Akteur im Gesundheitswesen, welcher sich wachsenden Herausforderungen in IT-Governance und Compliance stellen muss. Dank steigenden Anforderungen und schnelllebiger Technologie, werden Bedrohungen und Risiken im Bereich Datenschutz und IT-Sicherheit immer grösser. Eines der Governance-Herausforderungen war der Anstieg von Prüfungsmängel um 25%, welches unter anderem auf inkonsistente Dokumentation zurückzuführen ist *(Flevy, n.d.)*.

**Umsetzung von COBIT V**

Das Unternehmen entschied sich für die Implementation eines COBIT V-Frameworks, um IT-Prozesse zu optimieren. Dabei waren die IT-Ziele an Geschäftszielen auszurichten ein entscheidender Faktor bei der Auswahl des COBIT V-Frameworks. Die Organisation folgte einem strukturierten Ansatz, welcher Schulungen, Change-Management und ein Leistungsüberwachungsprogramm beinhielten. Möglichkeiten wie Workshops, Online-Kurse und Zertifizierungsprogramme wurden angeboten, um jeden Mitarbeiter korrekt zu schulen. Ein frisches Change-Management-Framework förderte klare Kommunikation zwischen Stakeholder und Geschäftsleitung. Führungskräfte betonten ausdrücklich die Wichtigkeit der neuen Governance-Richtlinien *(Flevy, n.d.)*.

**Ergebnisse und Nutzen**

Durch die Implementierung sah das Unternehmen eine deutliche Erhöhung der Audit-Scores und bessere Einhaltungsraten von Rechtsvorschriften. Die Organisation nutzte Key Performance Indicators (KPIs) und Analysetools, um Anpassungen von bis zu 25% vorzunehmen und die Mängel erfolgreich zu mindern *(Flevy, n.d.)*.

## 4.2 Beispiel 2: Finanzinstitute in Georgia

**Beschreibung der Organisation/Branche**

Die Organisation ist ein regionaler, kommerzieller Bankbetrieb in Georgien, welcher den Anforderungen der Nationalbank Georgiens (NBG) auf IT- und Cybersicherheitsmanagement gerecht werden muss. Die Bank ist ein Teil eines grösseren Netzwerkes, welches von einer Muttergesellschaft im Ausland betrieben wird. Dadurch werden spezifische Herausforderungen im Bereich IT-Governance und -Management verlangt. COBIT V integriert verschiedenste Standards wie NIST CSF, ISO 27001 und ISO 27002. Aus diesem Grund fiel die Wahl für das IT-Audit auf das COBIT V-Framework *(Shavgulidze, 2022)*.

**Umsetzung von COBIT**

Die Umsetzung startete mit den Schwerpunkten aus der Governance-Domain «Evaluate, Direct and Monitor» (EDM) und der Management-Domain «Deliver, Service and Support» (DSS). Die Bank verwendete vor der Implementierung kein Framework, daher wurden spezifische Fähigkeitsniveaus festgelegt, um den aktuellen Stand der IT-Prozesse zu bewerten. Die Bewertung basierte auf den COBIT V-Zielen. Sie bestand aus einer Analyse von bestehenden IT-Prozessen und konkreter Ziele, um Governance-Strukturen zu verbessern *(Shavgulidze, 2022)*.

**Ergebnisse und Nutzen**

Die Ergebnisse sind visuell durch Balkendiagramme veranschaulicht worden (Siehe Abbildungen 3 & 4). Sie zeigten, wie die Bank im Vergleich zu den festgelegten Zielen abschneidet. Durch die Darstellungsweise fiel es dem Management leichter, den Fortschritt zu erkennen und gezielte Entscheidungen zu treffen. Eines der ersten Bewertungen konzentrierte sich auf die Bereiche der EDM und DSS. Sie legten damit den Grundstein für eine verbesserte Unternehmensgovernance und eine effizientere IT-Nutzung *(Shavgulidze, 2022)*.

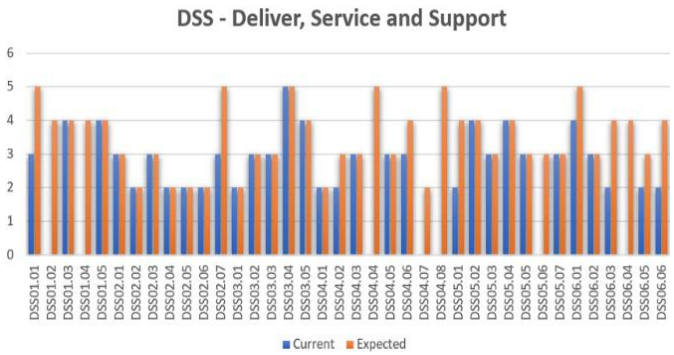


*Abbildung 3: Bankbetrieb in Georgien - Beispiel von den DSS-Ergebnissen (nicht wirkliche Daten)*

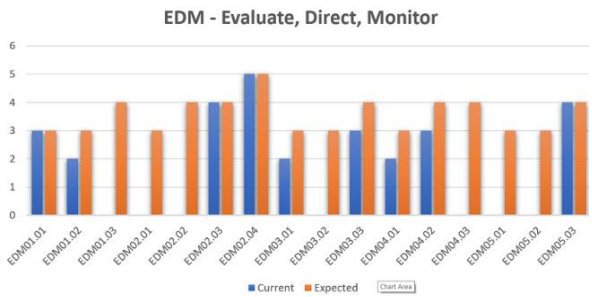


*Abbildung 4: Bankbetrieb in Georgien - Beispiel von den EDM-Ergebnissen (nicht wirkliche Daten)*

## 4.3 Beispiel 3: The Walt Disney Company

**Beschreibung der Organisation/Branche**

The Walt Disney Company (TWDC) ist ein weltweit führendes Unterhaltungsunternehmen mit fünf Bereichen: Studios, Konsumgüter, Mediennetzwerke, interaktive Medien und Theme-Parks & Resorts. Davon sind die Themenparks & Resorts einer der grössten Bereiche und macht ~30% des Umsatzes. Mit über 100‘000 Mitarbeitern und rund 118 Millionen Besuchern jährlich muss Zuverlässigkeit und Effizienz an erster Stelle sein *(AXELOS, 2011)*.

**Umsetzung von ITIL**

Bereits in den 2000er Jahre begann TWDC mit der Einführung von ITIL-Best Practices. Bereits 2008 wurde ein erfahrener ITIL-Experte eingestellt, um die Implementierung von ITIL voranzutreiben. Das Service-Level und ein produktiveres IT-Management war das Ziel der Implementierung. Ein breites Bildungsprogramm mit Schulungen wurde erstellt, um ITIL in die Organisation zu integrieren. Durch selbsternannte «ITIL-Champions» und das Stärken des Bewusstseins der Mitarbeiter entstand ein vollfunktionsfähiges ITIL-Framework in der TWDC *(AXELOS, 2011)*.

**Ergebnisse und Nutzen**

Es gab deutliche Verbesserungen des IT-Servicemanagements. Durch Schulung von über 250 Mitarbeitern in ITIL und die Ernennung von 20 ITIL-Champions konnte das ITIL-Framework überall implementiert werden. Die IT-Abteilung konnte stärker in die Geschäftsziele eingebunden werden und steigerte damit die Effizienz und die Betriebskosten *(AXELOS, 2011)*.

## 4.4 Beispiel 4: FinTech Unternehmen

**Beschreibung der Organisation/Branche**

Finanztechnologiebranche (FinTech) sind Unternehmen, welche technologische Innovationen benutzen, um Finanzdienstleistungen zu verbessern. Dies umfasst beispielsweise Zahlungs-abwicklungen, Kreditvergabe, Vermögensverwaltung und Blockchain-basierte Lösungen. Dank eines Projektes einer führenden FinTech-Organisation konnte der Einsatz von beiden Frameworks (COBIT V und ITIL) erforscht werden. Als FinTech-Organisation wird vorausgesetzt, dass strenge Anforderungen und effizientes IT-Management betrieben werden können *(Mehta, 2019)*.

**Umsetzung von COBIT V und ITIL**

Das Projekt verfolgte drei zentrale Ziele:

1. Identifikation aller IT-Funktionen
2. Zuordnung dieser Funktionen zu den ITIL v3-Prozessen und Richtlinien
3. Ableitung von Kontrollzielen basierend auf den COBIT V-Praktiken

In der folgenden Tabelle (siehe Abbildung 5) sind die priorisierten IT-bezogenen Ziele basierend auf der COBIT V Zielkaskade dargestellt, welche im Projekt besonders wichtig waren.

Da beide Frameworks unterschiedliche Bereiche abdecken, konnten diese gut als Kombination fungieren. In der Praxis wurde gezeigt, dass COBIT V-Prozesse (Änderungsmanagement BAI06 & Konfigurationsmanagement BAI10) mit ITIL-Prozessen korrelieren *(Mehta, 2019)*.

**Ergebnisse und Nutzen**

Die Kombination von COBIT V und ITIL brachte der FinTech Organisation mehrere Vorteile:

- Optimierte IT-Governance und klare Strategieumsetzung durch COBIT V
- Flexibilität bei der Implementierung durch COBIT V
- Effektiveres Risikomanagement durch ITIL
- Verbesserte Servicequalität durch ITIL

Durch beide Frameworks konnte das FinTech-Unternehmen die Anforderungen erfüllen und den IT-Bereich effizienter kontrollieren *(Mehta, 2019)*.

| | | | Enterprise Goal | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Stakeholder value of business investments | Portfolio of competitive products and services | Managed business risk (safeguarding of assets) | Compliance with external laws and regulations | Financial transparency | Customer-oriented service culture | Business service continuity and availability | Agile responses to a changing business environment | Information-based strategic decision making | Optimisation of service delivery costs | Optimisation of business process functionality | Optimisation of business process costs | Managed business change programmes | Operational and staff productivity | Compliance with internal policies | Skilled and motivated people | Product and business innovation culture |
| | | | 1. | 2. | 3. | 4. | 5. | 6. | 7. | 8. | 9. | 10. | 11. | 12. | 13. | 14. | 15. | 16. | 17. |
| IT-related Goal | | | Financial | | | | | Customer | | | | | Internal | | | | | Learning and Growth | |
| Financial | 01 | Alignment of IT and business strategy | P | P | S | | | P | S | P | P | S | P | S | P | | | S | S |
| | 02 | IT compliance and support for business compliance with external laws and regulations | | | S | P | | | | | | | | | | | P | | |
| | 03 | Commitment of executive management for making IT-related decisions | P | S | S | | | | | S | S | | S | | P | | | S | S |
| | 04 | Managed IT-related business risk | | | P | S | | | P | S | | P | | | S | | S | S | |
| | 05 | Realised benefits from IT-enabled investments and services portfolio | P | P | | | | S | | S | | S | S | P | | S | | | S |
| | 06 | Transparency of IT costs, benefits and risk | S | | S | | P | | | | S | P | | P | | | | | |
| Customer | 07 | Delivery of IT services in line with business requirements | P | P | S | S | | P | S | P | S | | P | S | S | | | S | S |
| | 08 | Adequate use of applications, information and technology solutions | S | S | S | | | S | S | | S | S | P | S | | P | | S | S |
| Internal | 09 | IT agility | S | P | S | | | S | | P | | | P | | S | S | | S | P |
| | 10 | Security of information, processing infrastructure and applications | | | P | P | | | P | | | | | | | | P | | |
| | 11 | Optimisation of IT assets, resources and capabilities | P | S | | | | | | S | | P | S | P | S | S | | | S |
| | 12 | Enablement and support of business processes by integrating applications and technology into business processes | S | P | S | | | S | | S | | S | P | S | S | S | | | S |
| | 13 | Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards | P | S | S | | | S | | | | S | | S | P | | | | |
| | 14 | Availability of reliable and useful information for decision making | S | S | S | S | | | P | | P | | S | | | | | | |
| | 15 | IT compliance with internal policies | | | S | S | | | | | | | | | | | P | | |
| Learning and Growth | 16 | Competent and motivated business and IT personnel | S | S | P | | | S | | S | | | | | | P | | P | S |
| | 17 | Knowledge, expertise and initiatives for business innovation | S | P | | | | S | | P | S | | S | | S | | | S | P |

*Abbildung 5: FinTech-Unternehmen - Priorisierte IT-bezogene Ziele (Mehta, 2019)*

## 4.5 Beispiel 5: Multinationales Ölunternehmen

**Beschreibung der Organisation/Branche**

Das letzte Beispiel beschreibt eine multinationale Öl-Organisation aus den Vereinigten Arabischen Staaten, welche eine automatische Implementation von COBIT V und ITIL verwendete. Die Organisation hat einen Jahresumsatz von 14,7 Milliarden US-Dollar und circa 6'500 Mitarbeiter. Die Organisation hat vier Geschäftsbereiche: Lieferung, Handel und Verarbeitung, Terminals und Marketing & Einzelhandel. Durch die Grösse, besitzt die IT-Abteilung 89 Mitarbeiter für den IT-Service und nutzt 165 physische sowie 200 virtuelle Server *(Nicho et al., 2017)*.

**Umsetzung von COBIT V und ITIL**

Um die Servicequalität zu verbessern, wurde die Implementierung von ITIL geplant. Dabei wurde 2009 ein neuer CIO ernannt, welcher den Fokus auf Prozessautomatisierung und Shared Services Centers (SSC) legte. COBIT V wurde für die Organisation der IT- und Geschäftsziele geplant. Nach der Ernennung des CIOs wurden Helpdesk-Prozesse optimiert, gefolgt von Incident-, Change- und Release-Management. Später kam die Einführung einer Configuration Management Database (CMDB) hinzu *('Wikipedia, CMDB', 2024)*. Schritt für Schritt sind beide Frameworks implementiert worden *(Nicho et al., 2017)*.

**Ergebnisse und Nutzen**

Durch die Implementierung wurden die IT- und Geschäftsziele besser aufeinander abgestimmt, was eine effizientere Ressourcennutzung bedeutete. IT-Kosten wurden transparenter gestaltet und Kundenanforderungen wurden schneller umgesetzt. Durch die eingesetzten ITSM-Tools beider Frameworks wurden die IT-Prozesse kontinuierlich verbessert und die Servicequalität für die Kunden deutlich gesteigert *(Nicho et al., 2017)*.

In der Abbildung 6 wird die Ausrichtung zwischen IT- und Geschäftsprozessen veranschaulicht. Sie zeigt die Verbindung der IT- und Geschäfts-Ziele mit den IT-Service-Prozessen der Organisation:

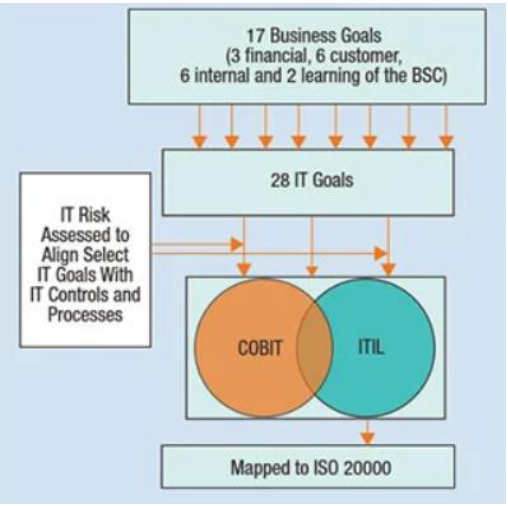


*Abbildung 6: Verbindung der IT- und Geschäftsziele mit den IT-Service-Prozessen (Nicho et al., 2017)*

# 5 Evaluation der Praxisbeispiele (Vergleich, Bewertung, Priorisierung)

**Beispiel 1 - Gesundheitswesen:** Die Implementierung des COBIT V-Frameworks führte zu deutlichen Fortschritten in der Compliance und IT-Governance. Mithilfe von KPIs und eines strukturierten Change-Managements wurden Audit-Scores verbessert und Prüfungsmängel erfolgreich reduziert. Die beschriebene Fokussierung auf die Governance zeigt, wie COBIT V gezielt zur Verbesserung der IT-Sicherheit eingesetzt werden kann.

**Beispiel 2 - Finanzinstitute in Georgia**: Durch die Einbindung des COBIT V-Frameworks konnte das Finanzinstitut grundlegende IT-Governance-Strukturen entwickeln und vorhandene Prozesse optimieren. Die Visualisierung der Ergebnisse ermöglichte es dem Management, die Fortschritte nachvollziehbar zu bewerten. Die Implementierung von «Evaluate, Direct and Monitor» (EDM) und «Deliver, Service and Support» (DSS) bewies ihre Effektivität in einem regulierten Umfeld.

**Beispiel 3 - The Walt Disney Company:** Die langjährige Nutzung von ITIL verhalf TWDC zu deutlichen Verbesserungen im IT-Servicemanagement. Die Einführung von «ITIL-Champions» und eine weitreichende Schulungsinitiative führten zu höherer Effizienz und besseren Betriebskosten. Der Fokus auf Servicemanagement und die Etablierung einer serviceorientierten IT-Umgebung veranschaulichen die Stärke von ITIL in der Unterstützung betrieblicher Ziele.

**Beispiel 4 - FinTech:** Die Kombination von COBIT V und ITIL ermöglichte, der FinTech-Organisation, welche den Einsatz der beiden Frameworks erforschte, eine umfassende Lösung, die sowohl IT-Governance als auch Flexibilität gewährleistet. Durch gezielte Prozessanpassungen konnte das Unternehmen sein IT-Management verbessern und Risiken effektiver managen. Die klare Zuordnung von ITIL-Prozessen zu COBIT V-Zielen stärkte die Servicequalität und optimierte die IT-Governance.

**Beispiel 5 - Multinationales Ölunternehmen:** Das Ölunternehmen kombinierte ITIL und COBIT V für eine strukturierte und automatisierte IT-Governance. Durch die Schaffung eines Shared Service Centers und einer Configuration Management Database konnten Prozesse kontinuierlich verbessert und IT-Kosten transparent gestaltet werden. Die Verknüpfung von IT- und Geschäftsprozessen führte zu einer gesteigerten Servicequalität und besseren Ressourcenverwaltung.

**Vergleich und Bewertung**

In hochregulierten Branchen wie dem Gesundheitswesen und der Finanzwirtschaft zeigt sich COBIT V als äusserst effektiv für Governance- und Compliance-Ziele. ITIL hingegen unterstützt besonders im Bereich des IT-Servicemanagements, wie das Beispiel Disney verdeutlicht. Die Kombination beider Frameworks, wie in den FinTech- und Ölunternehmen, bietet eine Lösung für Organisationen, die sowohl eine starke IT-Governance als auch flexible Servicemanagement-Lösungen benötigen. Insgesamt sind die Frameworks komplementär einsetzbar und in spezifischen Kontexten besonders effektiv. Die Effektivität und der Frameworks ist von den branchenspezifischen Anforderungen abhängig.

# 6 Handlungsempfehlungen für Unternehmen

Unternehmen, die COBIT V und ITIL einführen möchten, sollten den Fokus auf klare Kommunikation legen, da diese entscheidend für den Erfolg ist, wie das Beispiel von Disney zeigt. Disney erkannte bei der Einführung von ITIL, dass eine unterschätzte Kommunikation den Fortschritt hemmen kann. Bestehende Tools und Dokumente sollten genutzt werden, um unnötige Arbeit zu vermeiden. Dabei ist es wichtig, praktische und realistische Ansätze zu verfolgen, um zu verhindern, dass Prozesse unnötig kompliziert werden. IT-Governance und Service-Management müssen mit gesundem Menschenverstand implementiert werden, um einen nachhaltigen Nutzen zu erzielen *(AXELOS, 2011, Chapter Glen's advice for organizations adopting ITIL)*.

## 6.1 Governance-Strukturen etablieren

Unternehmen sollten Governance-Strukturen aufbauen, um IT-Sicherheitsverantwortlichkeiten klar zu definieren. Konkret bedeutet dies, einen CISO zu benennen, ein Sicherheitskomitee einzurichten und die Sicherheitslage regelmässig zu bewerten.

COBIT V bietet hierfür ein geeignetes Framework. Unternehmen sollten Rollen und Verantwortlichkeiten dokumentieren und Governance-Frameworks wie COBIT V in ihre Organisationsstrukturen integrieren. COBIT V unterscheidet klar zwischen Governance (Bewertet Stakeholder Bedürfnisse, legt Unternehmensziele fest, priorisiert Entscheidungen und überwacht Einhaltung der Ziele; Verwaltungsrat) und Management (Planen, Bauen, Ausführen und Überwachen der Unternehmensziele; Geschäftsleitung) *(ISACA, 2012, p. 31)*.

## 6.2 Risikomanagement priorisieren

Um ein effektives Risikomanagement zu etablieren, müssen Unternehmen Bedrohungen und Schwachstellen systematisch identifizieren und bewerten. Dies erfordert den Einsatz geeigneter Tools und die Implementierung spezifischer Prozesse zur Risikobewältigung.

COBIT V unterstützt dabei, Risiken im Verhältnis zu den Geschäftszielen zu bewerten, indem beispielsweise Risk Heat Maps oder Risikoanalyse-Software genutzt werden. Zudem sollten Unternehmen Risikomanagementprozesse wie Risikoakzeptanz, Risikominderung und Risikotransfer implementieren und regelmässig überprüfen.

## 6.3 Sicherheitsrichtlinien standardisieren

Unternehmen sollten Sicherheitsrichtlinien entwickeln, die Standards wie COBIT V und ITIL berücksichtigen. Diese Richtlinien sollten in einem zentralen, leicht zugänglichen Dokument festgehalten und regelmässig aktualisiert werden. Schulungen stellen sicher, dass alle Mitarbeiter die Richtlinien verstehen und einhalten.

## 6.4 Zugriffskontrollen implementieren

Unternehmen sollten strikte Zugriffskontrollsysteme implementieren, um den unbefugten Zugriff auf sensible Daten zu verhindern. Es empfiehlt sich, Multifaktor-Authentifizierung (MFA) einzuführen und rollenbasierte Zugriffskontrollen (Role-Based Access Control, RBAC) anzuwenden. Regelmässige Überprüfungen der Zugriffsrechte sind unerlässlich, um unberechtigten Zugang zu vermeiden. Tools wie Identity and Access Management (IAM) können dabei unterstützen, diese Prozesse effizient zu steuern.

## 6.5 Incident-Management verbessern

Um ein robustes Incident-Management aufzubauen, sollten Unternehmen klare Prozesse und Eskalationspfade festlegen. Dies kann durch die Einführung eines Ticketing-Systems und die Schulung von Response-Teams unterstützt werden. Simulationen, wie Cyberangriffe, verbessern die Reaktionsfähigkeit, und ITIL bietet nützliche organisatorische Leitlinien, insbesondere im Bereich des Incident- und Problem-Managements.

## 6.6 Kontinuierliche Überwachung einführen

Unternehmen sollten Überwachungssysteme implementieren, die kontinuierlich die IT-Infrastruktur überwachen und Sicherheitsanomalien erkennen. Dazu sollten Werkzeuge zur Netzwerkanalyse und Bedrohungserkennung, wie beispielsweise SIEM (Security Information and Event Management), eingesetzt werden. Unternehmen müssen ausserdem sicherstellen, dass regelmässige Audits und Sicherheitsbewertungen stattfinden. COBIT V bietet Leitlinien zur Definition von KPIs sowie zur regelmässigen Überprüfung der Wirksamkeit von Überwachungsmechanismen.

## 6.7 Sicherheitsbewusstsein schärfen

Unternehmen können durch Schulungsprogramme das Sicherheitsbewusstsein stärken. Dazu zählen E-Learning-Module, Phishing-Simulationen und interne Kampagnen. ITIL unterstützt die Integration dieser Schulungen in den Arbeitsalltag durch klare Sicherheitsrollen und Verantwortlichkeiten. Es ist wichtig, dass das Management dieses Sicherheitsbewusstsein ebenfalls vorlebt.

## 6.8 Datenintegrität sicherstellen

Unternehmen sollten Backup- und Wiederherstellungsprozesse einrichten, um die Integrität und Verfügbarkeit von Daten zu gewährleisten. Automatisierte, regelmässig getestete Backups sowie Disaster-Recovery-Pläne sind essenziell. COBIT V und ITIL bieten Ansätze zur Integration der Datenintegrität in Geschäftsprozesse, indem sie Richtlinien für das Backup-Management, Tests und Wiederherstellungsverfahren festlegen.

## 6.9 Change-Management-Prozesse absichern

Unternehmen sollten sicherstellen, dass Änderungen in der IT-Infrastruktur stets sicher und kontrolliert erfolgen. ITIL-konforme Change-Management-Prozesse, wie formelle Änderungsanfragen (RFCs), sollten dabei genutzt werden, und jede Änderung muss auf potenzielle Sicherheitsrisiken hin geprüft werden. IT-Service-Management-Systeme (ITSM) können verwendet werden, um Änderungen zu planen, zu dokumentieren und nachzuverfolgen. Regelmässige Change-Management-Meetings helfen, Risiken zu bewerten und zu minimieren.

## 6.10 Compliance sicherstellen

Um die Einhaltung gesetzlicher Vorschriften und interner Sicherheitsanforderungen zu gewährleisten, sollten Unternehmen Compliance-Programme implementieren. Regelmässige Audits und die Dokumentation aller Sicherheitsmassnahmen sind dabei essenziell (siehe auch «6.6 Kontinuierliche Überwachung einführen»). COBIT V bietet einen Rahmen, um Compliance-Richtlinien systematisch zu überwachen und deren Einhaltung sicherzustellen. Automatisierte Tools zur Compliance-Überwachung unterstützen dabei, Verstösse frühzeitig zu erkennen und zu beheben.

# 7 Fazit und Ausblick

Zukünftige Entwicklungen und Trends im Bereich von COBIT V und ITIL, insbesondere im Hinblick auf Sicherheitsaspekte, deuten auf eine wachsende Bedeutung von Automatisierung, Künstlicher Intelligenz (KI) und maschinellem Lernen hin. Diese Technologien ermöglichen eine proaktive Erkennung und Reaktion auf Bedrohungen in Echtzeit und helfen, menschliche Fehler zu minimieren. Zudem etabliert sich ein stärker risikobasierter Ansatz, der es Organisationen erlaubt, Sicherheitsmassnahmen gezielt auf ihre spezifischen Bedrohungsprofile auszurichten. Dadurch lassen sich Sicherheitsressourcen effizienter nutzen und potenzielle Schwachstellen dynamisch beheben.

Wie beschrieben im Praxisbeispiel 4 (FinTech Unternehmen), ist die zunehmende Integration von COBIT- und ITIL-Frameworks, die eine nahtlose Verbindung zwischen Governance- und Sicherheitsanforderungen schafft, ein weiterer Trend. Durch diese Kombination können Sicherheitsrichtlinien effizienter gesteuert und fest in IT-Prozesse eingebettet werden. Dies verbessert nicht nur die Wirksamkeit der Sicherheitsmassnahmen, sondern fördert auch die Einhaltung regulatorischer Anforderungen.

Mit der vermehrten Nutzung von Cloud-Umgebungen rückt zudem die Entwicklung spezifischer Cloud-Sicherheitsstrategien in den Vordergrund, um hybride und Multi-Cloud-Strukturen zu schützen *(Taleb & Mohamed, 2020)*. Organisationen stehen hier vor der Herausforderung, Sicherheitsaspekte wie Netzwerk- und Datenverkehr, Datenintegrität, Zugriffskontrollen und die Überwachung von Cloud-Services im Einklang mit den Standards von COBIT V und ITIL zu gestalten.

Zusätzlich nimmt die Bedeutung von Schulungen und einem hohen Sicherheitsbewusstsein innerhalb der Organisation stetig zu. Angesichts der steigenden Anzahl an Bedrohungen und der Compliance-Anforderungen ist es entscheidend, dass alle Mitarbeitenden regelmässig in Sicherheitsfragen geschult werden und ein tiefes Sicherheitsbewusstsein entwickeln. Interaktive Lernsysteme oder gamifizierte Ansätze können hierbei die Wirksamkeit der Schulungsmassnahmen erhöhen.

Zusammengefasst zeigen die zentralen Erkenntnisse, dass die Kombination von COBIT V und ITIL eine tiefere Integration von Sicherheitspraktiken und -protokollen ermöglicht. Anhand der fünf Praxisbeispiele wird deutlich, dass durch den Einsatz strukturierter Sicherheitsprotokolle Risiken verringert und Reaktionszeiten bei Vorfällen verkürzt werden. Die Beispiele verdeutlichen auch, wie COBIT V und ITIL in unterschiedlichen Branchen zur Optimierung von IT-Governance und IT-Service-Management beitragen. Die Implementierung variiert je nach branchenspezifischen Anforderungen. Insgesamt belegen die Praxisbeispiele, dass die Wahl und Kombination von COBIT V und ITIL stark von den jeweiligen Anforderungen der Branche abhängt. Während COBIT V besonders in regulierten Umfeldern die Einhaltung gesetzlicher Vorschriften und die IT-Governance unterstützt, bietet ITIL vor allem im Bereich des Service-Managements Effizienzgewinne.

# 8 Abbildungsverzeichnis

# 9 Glossar

| Abkürzung | Bedeutung |
|---|---|
| APO | Align, Plan and Organise |
| BAI | Build, Acquire and Implement |
| BMIS | Business Model for Information Security |
| CISO | Chief Information Security Officer |
| CMDB | Configuration Management Database |
| COBIT | Control Objectives for Information and Related Technologies |
| CSI | Continual Service Improvements |
| DSS | Deliver, Service and Support |
| EDM | Evaluate, Direct and Monitor |
| FinTech | Finanztechnologiebranche |
| IAM | Identity and Access Management |
| ISACA | Information Systems Audit and Control Association |
| IT | Informationstechnik |
| I&T | Information und Technologie |
| ITAF | IT Assurance Framework |
| ITSM | IT-Service-Management-Systeme |
| KI | Künstlicher Intelligenz |
| KPIs | Key Performance Indicators |
| MEA | Monitor, Evaluate and Assess |
| MFA | Multifaktor-Authentifizierung |
| NBG | Nationalbank Georgiens |
| NDAs | Non-Disclosure Agreements |
| RBAC | Role-Based Access Control |
| RFCs | Requests for Comments |
| SIP | Service Improvement Plan |
| SLAs | Service Level Agreements |
| SLM | Service Level Management |
| SSC | Shared Services Centers |
| SVS | Service Value System |
| TWDC | The Walt Disney Company |

# 10 Literaturverzeichnis

Andenmatten, M. (2018, November 26). *COBIT 2019 – Das neue Enterprise Governance Modell für Informationen und Technologien*. Disruptive agile Service Management. https://blog.itil.org/2018/11/cobit-2019-das-neue-enterprise-governance-modell-fuer-informationen-und-technologien/

AXELOS. (2011, Oktober). *Disney's ITIL & Journey*. https://www.axelos.com/resource-hub/case-study/disneys-itil-journey-case-study

AXELOS. (2019). *ITIL foundation: ITIL 4 edition* (First edition). TSO (The Stationery Office).

Configuration management database. (2024). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Configuration_management_database&oldid=1249812684

Flevy. (n.d.). *Transforming Governance: COBIT Strategy in Health Care and Social Assistance - COBIT Case Study*. Retrieved 9 October 2024, from https://flevy.com/topic/cobit/case-transforming-governance-cobit-strategy-health-care-social-assistance

Harisaiprasad, K. (2020, April 27). *COBIT 2019 and COBIT 5 Comparison*. ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison

Harmer, G. (2014). *Governance of Enterprise IT based on COBIT®5*. IT Governance Publishing. https://learning.oreilly.com/library/view/governance-of-enterprise/9781849285193/xhtml/chapter06.html

ISACA (Ed.). (2012). *COBIT 5: A business framework for the governance and management of enterprise IT: an ISACA® framework*. ISACA.

IT Governance. (n.d.). *What is COBIT 5? Definition & Explanation*. Retrieved 10 October 2024, from https://itgovernance.co.uk/cobit

Mehta. (2019, June 24). *Lessons Learned While Combining COBIT 5 and ITIL*. ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2019/lessons-learned-while-combining-cobit-5-and-itil

Moeller. (2013). *Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL*. Wiley. https://learning.oreilly.com/library/view/executives-guide-to/9781118238936/

Nicho, M., Khan, S., & Mohan, R. (2017, July 1). *Challenges and Lessons Learned Implementing ITIL, Part 1: Realizing Value Through Business IT Alignment*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/challenges-and-lessons-learned-implementing-itil-part-1-realizing-value-through-business-it-alignmen

Shavgulidze, D. (2022, October 12). *Financial Institutions in Georgia*. ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/a-cobit-2019-use-case-financial-institutions-in-georgia

Taleb, N., & Mohamed, E. A. (2020). Cloud Computing Trends: A Literature Review. *Academic Journal of Interdisciplinary Studies*, *9*(1), 91. https://doi.org/10.36941/ajis-2020-0008