Normen & Standards der IT

Autoren: Lukas Freundensprung, Sebasatian Trostmann, Abd-Sattaar Matitu, Morris Tichy

Inhaltsverzeichnis

1. COBIT

1.1. Kurze Einführung in IT-Governance

IT-Governance umfasst alle Prozesse und Strukturen, die dafür sorgen, dass die IT optimal zur Unterstützung der Unternehmensstrategie beiträgt. Es stellt sicher, dass Verantwortlichkeiten klar geregelt, Leistungen gemessen und regelmäßig überprüft werden.

1.2. Was bringt COBIT?

COBIT (Control Objectives for Information and Related Technologies) ist ein IT-Governance-Framework. Das Framework hilft Unternehmen, ihre IT besser zu organisieren und zu kontrollieren. Es sorgt dafür, dass IT-Maßnahmen mit den Zielen des Unternehmens übereinstimmen. Es unterstützt bei der Identifikation von Risiken und der Verbesserung der Servicequalität. Außerdem sorgt COBIT für Transparenz, indem es klare Richtlinien und Berichte bereitstellt. Durch die Anwendung von COBIT können Unternehmen ihre IT-Investitionen rechtfertigen und langfristig den Geschäftswert steigern. COBIT ist dabei unabhängig von der Unternehmensgröße, der Branche und der Art anwendbar.

1.3. Prinzipien von COBIT

Die Grundlagen von COBIT beruhen auf klar definierten Prinzipien, die den Rahmen für das gesamte Framework bilden:

- **Stakeholder-Orientierung:** COBIT richtet sich nach den Bedürfnissen aller beteiligten Gruppen, wie Führungskräften, IT-Mitarbeitern und Endnutzern. Interessenkonflikte der Stakeholder sollen dabei aufgedeckt und angepasst werden.
- **Abdeckung der gesamten Unternehmens-IT:** Mit COBIT wird die IT in Kombination mit der restlichen Unternehmensführung geführt. Das bedeutet, dass IT kein eigener Teil des Unternehmens mehr ist. Dadurch werden IT-Prozesse und Investitionen übersichtlicher und einfacher zu verwalten.
- **Einziges integriertes Framework:** COBIT ist ein einheitliches integriertes Framework. Das bedeutet, dass es am besten ist, wenn es als alleine als Framework verwendet wird. Es ist an die modernsten Standards angepasst und bietet somit eine einfache Struktur, die eine gute Basis bildet, um Führung und Managment miteinander zu verknüpfen.
- **Ganzheitlicher Ansatz:** Durch COBIT kann ein ganzheitlicher Ansatz ermöglicht werden. Das bedeutet, dass die IT in ihrer Gesamtheit betrachtet wird und die Integration zwischen

einzelnen Bereichen im Unternehmen maximiert wird. Dabei setzt COBIT auf 7 Enabler siehe Abschnitt 1.4.

- **Trennung von Führung und Verwaltung:** bei der Strukturierung unterscheidet COBIT klar zwischen Verwaltung und Führung. Diese beiden haben unterschiedliche Aufgaben, weswegen sie unterschiedliche Strukturen benötigen.
  - Führung: Anforderungen und Rahmenbedingungen leiten den Weg des Unternehmens
  - Verwaltung: Kümmert sich darum, dass die Richtung der Führung durch Unternehmensziele umgesetzt wird.

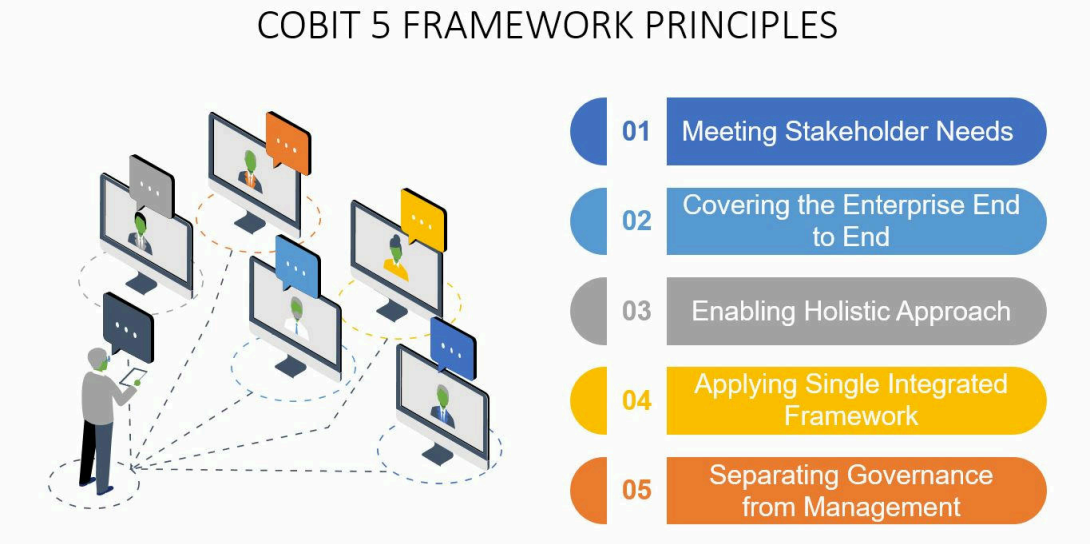

Abbildung 1: Die Prinzipien von COBIT 5 (neuste Version COBIT 2019)

1.4. Die Enabler von COBIT

Die sieben Enabler bieten einen ganzheitlichen Ansatz, um die IT-Governance effektiv zu gestalten und sicherzustellen, dass die IT die Geschäftsziele optimal unterstützt.

- **Prinzipien, Richtlinien und Frameworks**: Vorgaben und Anweisungen, die sicherstellen, dass alle Beteiligten ein gemeinsames Verständnis der Ziele und Vorgehensweisen haben.
- **Prozesse**: Strukturierte Reihenfolge von Aktivitäteten, die zum Erreichen der Ziele benötigt werden.
- **Organisationsstrukturen**: Hierarchien, Rollen und Verantwortlichkeiten innerhalb des Unternehmens. Fördern effektive Entscheidungsfindung
- **Kultur, Ethik und Verhalten**: Werte, Normen und Verhaltensweisen innehalb des Unternehmens. Eine positive Unternehmenskultur unterstützt die Umsetzung von Richtlinien.

- **Informationen**: Die Qualität, Verfügbarkeit und Sicherheit von Informationen beeinflusst die effektive Entscheidungsfindung und Steuerung innerhalb des Unternehmens.
- **Services, Infrastruktur und Anwendungen**: Damit sind Technische Ressourcen gemeint. Sie ermöglichen die Bereitstellung von IT-Services. Eine gut entwickelte Infrastruktur gewährleistet Statbilität und Flexibilität.
- **Mitarbeiter, Fähigkeiten und Kompetenzen**: Qualifikationen von Mitarbeitern sind entscheidend für die Umsetzungen von Strategien und Prozessen. Um die Qualifikation zu gewährleisten, eignen sich Weiterbildungen und die Anpassungsfähigkeit der Organisation.

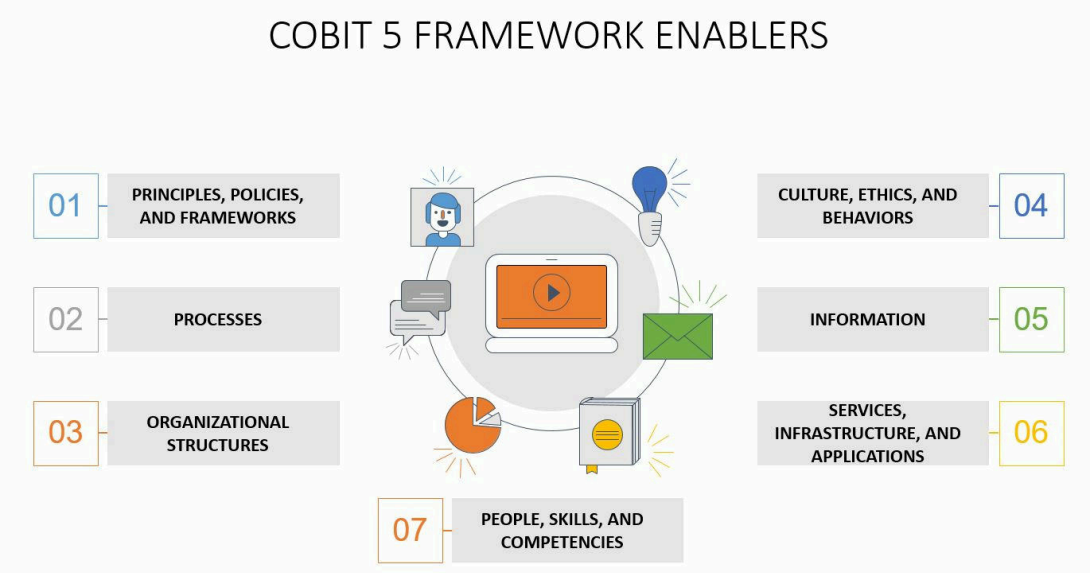

Abbildung 2: Die Enabler von COBIT 5 (neuste Version COBIT 2019)

1.5. Versionen und Entwicklung von COBIT

COBIT wurde in den 1990er Jahren von der ISACA entwickelt, um einen internationalen Standard für IT-Governance zu schaffen. Im Laufe der Zeit wurde das Framework weiterentwickelt:

- **COBIT 4.x:** Diese Version war weit verbreitet, bevor COBIT 5 eingeführt wurde.
- **COBIT 5:** Diese Version integrierte Governance und Management und legte besonderen Wert auf die Bedürfnisse der Stakeholder.
- **COBIT 2019:** Die aktuelle Version bietet mehr Flexibilität und Anpassungsmöglichkeiten, um modernen IT-Herausforderungen gerecht zu werden.

1.6. Wie funktioniert COBIT in der Praxis?

COBIT funktioniert, indem es einen klar strukturierten Rahmen bereitstellt, der alle IT-Aktivitäten eines Unternehmens abdeckt. Das Framework definiert standardisierte Prozesse und Metriken, die in verschiedenen Bereichen – von der strategischen Planung bis zur operativen Umsetzung – angewendet werden. Es ordnet jeder Aktivität spezifische Rollen und Verantwortlichkeiten zu, sodass jederzeit klar ist, wer für welchen Teil der IT-Governance zuständig ist. Durch regelmäßige Überprüfungen und Berichte können Unternehmen ihre IT-Leistung messen, Schwachstellen erkennen und gezielt Verbesserungen vornehmen. Dieser Ansatz sorgt dafür, dass alle IT-Aktivitäten transparent sind und eng mit den übergeordneten Unternehmenszielen verknüpft werden.

COBIT beinhaltet mehr als 40 Governance- und Führungsziele, welche von IT-Managern unterschiedlich priorisiert oder sogar ausgelassen werden können. Diese Ziele können gruppiert werden. Dafür sind die Domänen zuständig. Jede Domäne ist ein Geschäftsprozess wie Planung, Design oder Überwachung. Komponenten (Enabler siehe Abschnitt 1.4) sollen durch das Framework kontinuierlich verbessert werden, da sie die IT beeinflussen. Designfaktoren helfen dabei, Bedürfnisse von Organisationen zu erkennen. Anhand dieser Faktoren werden Entscheidungen über Technologie, Methoden und Outsourcing getroffen.

1.7. Fazit

COBIT ist ein bewährtes und flexibles Framework zur Steuerung und Überwachung der IT. Es hilft dabei, IT-Maßnahmen an den Unternehmenszielen auszurichten, Risiken zu managen und die Einhaltung von Vorschriften zu gewährleisten. Durch seine klaren Prinzipien, die modular aufgebaute Struktur und die kontinuierliche Weiterentwicklung – von COBIT 4.x über COBIT 5 bis zu COBIT 2019 – bietet COBIT eine solide Basis für eine effektive IT-Governance.

2. SOX

2.1. Einführung in SOX

Der Sarbanes-Oxley Act (SOX) wurde 2002 vom US-Kongress erlassen. Die Gesetzgebung entstand als Reaktion auf große Unternehmensskandale, wie jene um Enron oder WorldCom, und zielt darauf ab, Investoren zu schützen. SOX legt strenge Vorgaben für die Finanzberichterstattung und interne Kontrollen fest, um die Transparenz und Genauigkeit von Unternehmenszahlen zu erhöhen. Obwohl es in den USA gilt, betrifft es auch international tätige Unternehmen, die an US-Börsen notiert sind. SOX führte außerdem zu der Gründung

des Public Company Accounting Oversight Board (PCAOB). PCAOB ist eine gemeinnützige Organisation, die Standards für die Finanzprüfung festlegt. Zusätzlich werden Whistleblower geschützt, indem es illegal ist, Vergeltungsmaßnahmen gegen Mitarbeiter zu ergreifen, die Betrug melden.

2.2. Ziele und Nutzen von SOX Compliance

SOX verlangt, dass Unternehmen effektive interne Kontrollsysteme implementieren, um die Richtigkeit und Zuverlässigkeit von Finanzdaten sicherzustellen. Führungskräfte müssen die Integrität der Finanzberichte persönlich bestätigen. Dadurch wird sichergestellt, dass Risiken frühzeitig erkannt und behoben werden. SOX Compliance verbessert die Unternehmensführung, stärkt das Vertrauen der Investoren und reduziert das Risiko von Betrug und Manipulation in der Finanzberichterstattung.

2.3. Kernanforderungen und Prinzipien

Die Umsetzung von SOX basiert auf klar definierten Anforderungen und Prinzipien:

- **Interne Kontrolle:** Unternehmen sind verpflichtet, wirksame interne Kontrollsysteme zu etablieren, die die Genauigkeit der Finanzdaten gewährleisten.
- **Finanzberichterstattung:** Führungskräfte müssen regelmäßig bestätigen, dass die Finanzberichte korrekt und vollständig sind.
- **Audit und Überwachung:** Regelmäßige interne und externe Audits stellen sicher, dass die Kontrollmechanismen funktionieren und den gesetzlichen Vorgaben entsprechen.
- **Dokumentation:** Alle relevanten Prozesse und Kontrollen müssen dokumentiert und aufbewahrt werden, um eine lückenlose Nachvollziehbarkeit zu gewährleisten.

Durch das SOX-Gesetz sind auch Regeln für Wirtschaftsprüfungsgesellschaften und Analysten entstanden. Sollten diese nicht eingehalten werden, sieht das Gesetz hohe Geldstrafen, sowie strafrechtliche Verurteilungen für betrügerische Aktivitäten vor.

Durchschnittlich geben Unternehmen in den USA mehr als 1 Million US-Dollar für die Einhaltung der SOX-Vorschriften aus.

2.4. SOX im Bezug auf die IT

SOX betrifft nicht nur die Finanzabteilungen, sondern hat auch weitreichende Auswirkungen auf die IT-Infrastruktur eines Unternehmens. Die Absicherung und Integrität von IT-Systemen

ist entscheidend, da sie einen direkten Einfluss auf die Zuverlässigkeit der Finanzdaten haben. Die Einhaltung von SOX ist ein fortlaufender Prozess, der regelmäßige Überprüfungen und Anpassungen erfordert. Unternehmen profitieren von einer verbesserten Unternehmensführung und stärken das Vertrauen von Investoren und anderen Stakeholdern.

2.5. Umsetzung in der Praxis

In der Praxis bedeutet SOX Compliance, dass Unternehmen klare Prozesse und Richtlinien für ihre Finanzberichterstattung entwickeln und umsetzen. IT-Systeme spielen dabei eine zentrale Rolle, da sie die Finanzdaten verarbeiten und absichern. Unternehmen arbeiten häufig mit externen Prüfern zusammen, um die Einhaltung der gesetzlichen Vorgaben zu überprüfen. Regelmäßige Tests und Reviews der internen Kontrollsysteme helfen, Schwachstellen frühzeitig zu erkennen und zu beheben. Dieser kontinuierliche Überwachungsprozess stellt sicher, dass die Systeme und Prozesse immer den aktuellen Anforderungen entsprechen.

2.6. Fazit

SOX ist ein zentrales Regelwerk für börsennotierte Unternehmen, das strenge Anforderungen an die Finanzberichterstattung und interne Kontrollen stellt. Durch die Implementierung von SOX Compliance werden Prozesse zur Sicherstellung der Datenintegrität etabliert, Risiken reduziert und das Vertrauen in die Unternehmensführung gestärkt.

3. ITIL

Die ITIL (Information Technology Infrastructure Library) ist ein Best-Practice-Leitfaden und der De-facto-Standard im Bereich IT-Service-Management. Sie ist in folgenden Umfeld einzuordnen:

- **Prozessmanagement:** Definition und Steuerung der Prozesse eines Unternehmens.
- **IT-Service-Management:** Methoden, die nötig sind, um die bestmögliche Unterstützung von Geschäftsprozessen durch die IT-Organisation zu erreichen. (De-facto-Standard ist ITIL)
- **Business Service Management:** Die Verbindung zwischen Prozessmanagement und ITSM. Es befasst sich mit den wirtschaftlichen Zusammenhängen von IT-Leistungen und Geschäftsprozessen im Unternehmen.

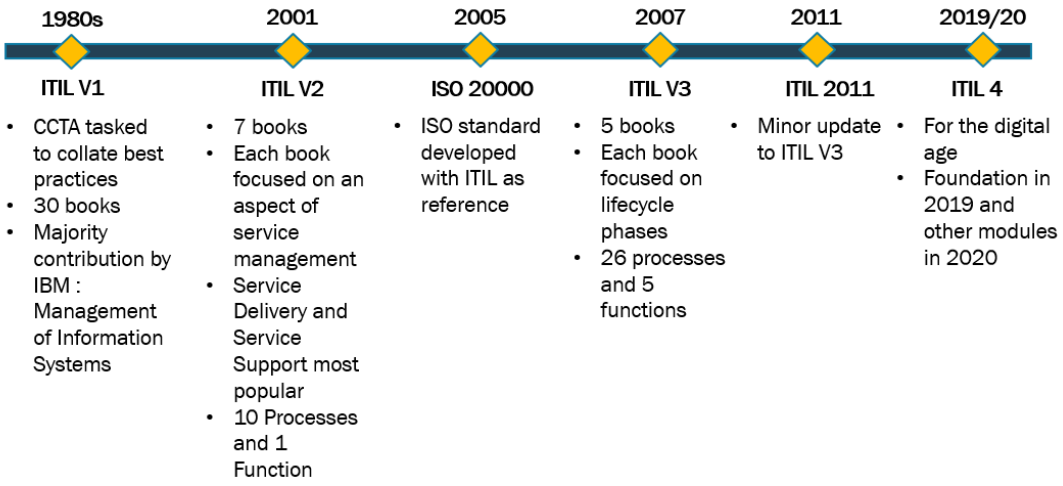

Abbildung 3: Geschichte und Entwicklung der ITIL

3.1. ITIL v4

ITIL 4 bringt neue Gedanken ein und entwickelt bestehende Inhalte von ITIL v3 weiter. ITIL 4 nennt zwei Schlüsselelemente:

3.1.1. Service Value System

Das ITIL Service Value System (SVS) beschreibt, wie alle Komponenten und Aktivitäten einer Organisation zusammenwirken, um durch Services nachhaltigen Wert für Kunden und Stakeholder zu schaffen.

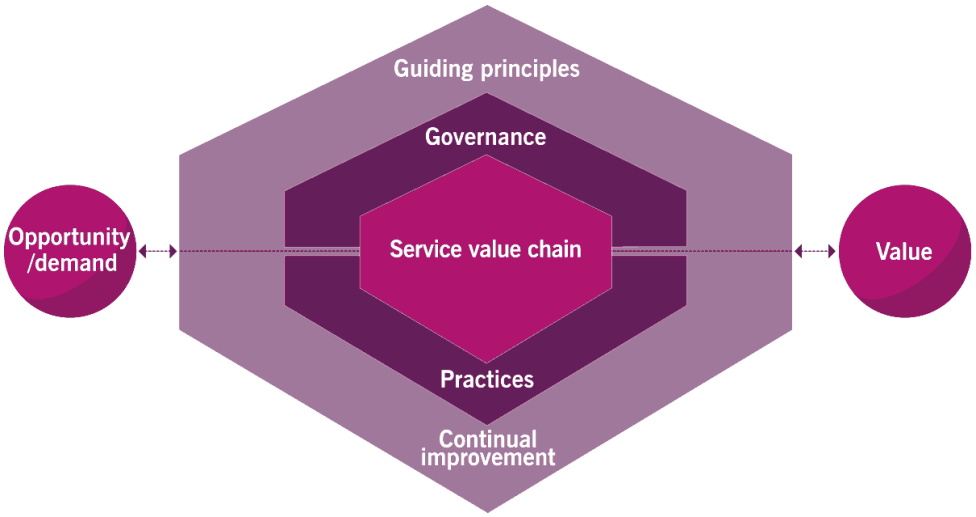

Abbildung 4: ITIL SVS

3.1.1.1. ITIL-Service-Wertschöpfungskette

Zentrales Modell für die Erstellung, Bereitstellung und kontinuierliche Verbesserung von Services, darunter sind:

- Planung
- Verbesserung
- Engagement
- Design & Transition
- Erhalten/erstellen
- Bereitstellung & Support

3.1.1.2. ITIL-Grundprinzipien

Die ITIL-Grundprinzipien stammen aus dem Servicemanagement und finden sich auch in Rahmenwerken, Normen oder Methoden wie DevOps, COBIT oder PRINCE2 wieder.

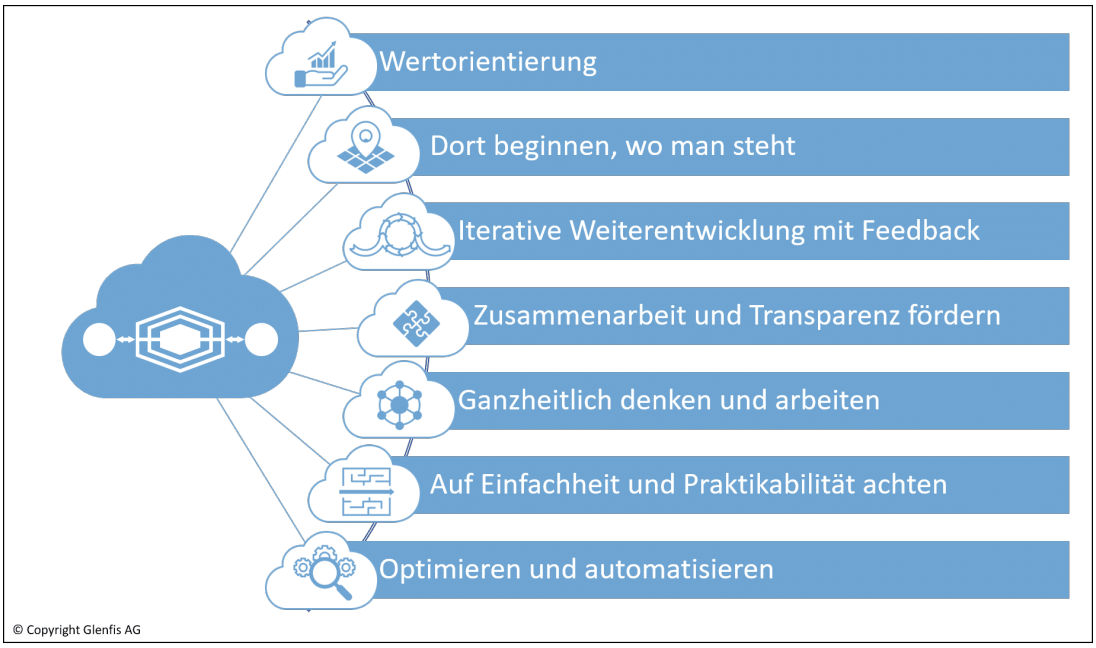

Abbildung 5: Grundprinzipien des ITIL

3.1.1.3. Governance

Governance als System, das die gesamte Organisation steuert und eine Richtung vorgibt.

3.1.1.4. ITIL-Practices

Methoden und Ressourcen zur effektiven Umsetzung von ITSM (z.B. Incident Management, Change Enablement).

3.1.1.5. Continual Improvement

Dauerhafte Optimierung aller Elemente des SVS.

3.1.2. Modell der vier Dimensionen

Das Modell der vier Dimensionen beschreibt die zentralen Bereiche, die bei jeder Komponente des SVS berücksichtigt werden müssen, um Services wirksam zu gestalten.

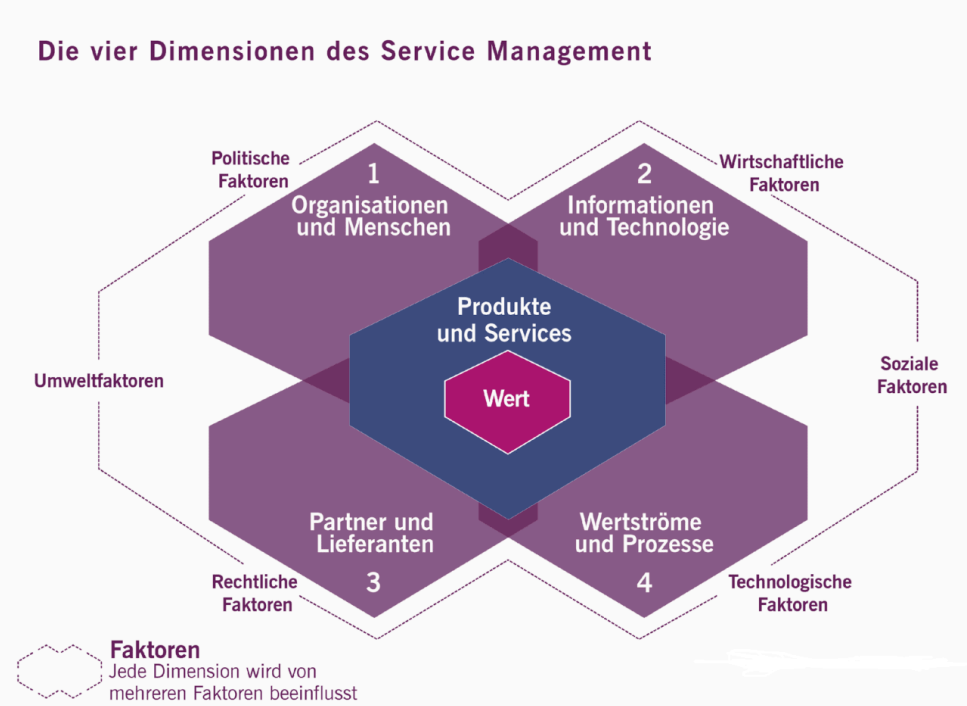

Abbildung 6: ITIL vier Dimensionenmodell

3.2. Zertifizierungsprozess

Der Zertifizierungsprozess ist in 5 Phasen unterteilt und wird seit 2018 von PeopleCert geführt. Die Zertifizierung muss alle 3 Jahre erneuert werden und die Kosten für eine ITIL Master belaufen sich auf bis zu 12.000 US-Dollar in einem gesamt Paket (ITIL Foundation Prüfung ca. 150-400€ und mit Kurs 500-1500€).

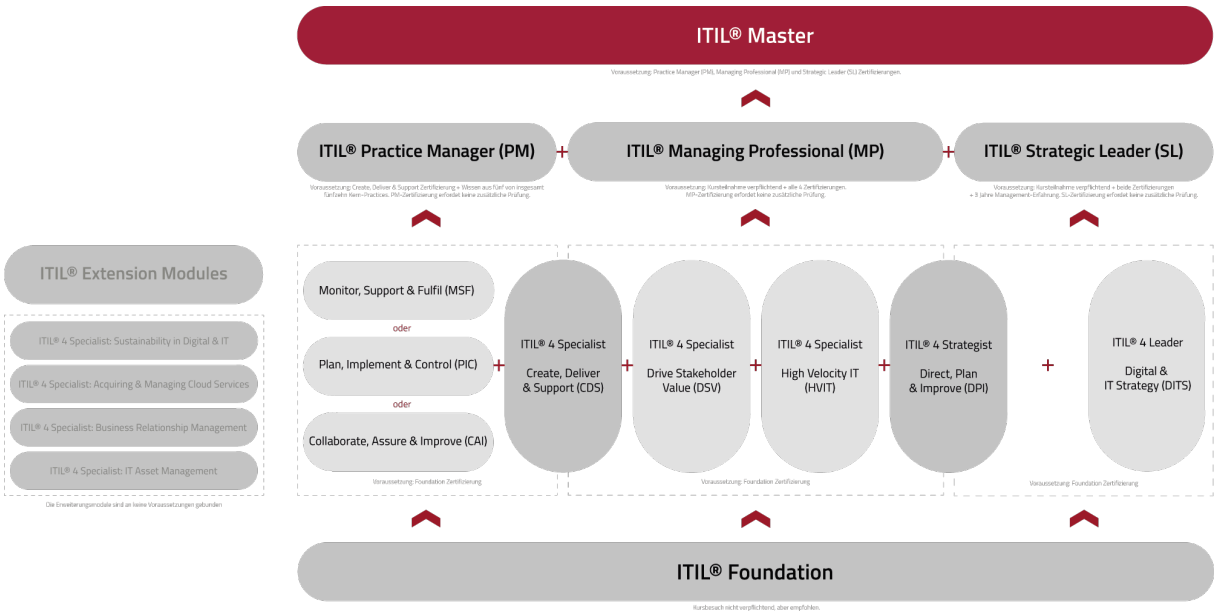

Abbildung 7: Zertifizierungsprozess des ITIL

3.3. Kritik

Laut einer Studie, in der über 300 mittelständische Unternehmen befragt wurden, hielten die Unternehmen die ITIL äußerst hilfreichh, aber für Mittel- und Kleinunternehmen zu komplex. Die Prozesse seien nicht für kleinere Unternehmen angelegt, da sie zu methodisch und zu langwierig sind. (Light Version für KMUs)

4. NIS 1 & NIS 2

Hinweis: Dieses Thema wurde bereits von Stefan ausführlich behandelt und wird daher in diesem Kapitel nur kurz zusammengefasst.

Die EU-Richtlinien NIS 1 (2016) und NIS 2 (2022) sollen die Cybersicherheit in kritischen Sektoren verbessern und die Zusammenarbeit der Mitgliedsstaaten stärken.

4.1. NIS 1 (2016)

- **Ziel:** Schutz kritischer Infrastrukturen (z.B. Energie, Verkehr, Gesundheit) und Steigerung der Cybersicherheitsfähigkeiten.
- **Pflichten:** Unternehmen müssen ein Risikomanagement implementieren, Sicherheitsvorfälle melden und mit nationalen Behörden kooperieren.

- **Auswirkungen:** Betroffene Sektoren umfassen unter anderem Finanzwesen und digitale Infrastruktur; Verstöße führen zu Sanktionen und erhöhter Haftung.

4.2. NIS 2 (2022)

- **Erweiterter Geltungsbereich:** Bezieht zusätzliche Sektoren wie Postdienste, Lebensmittelversorgung und Forschung ein.
- **Strengere Anforderungen:** Erfordert ein noch strikteres Risikomanagement, verpflichtende Cybersicherheitsstrategien sowie eine schnellere (innerhalb von 24 Stunden) Meldung von Sicherheitsvorfällen.
- **Konsequenzen für Unternehmen:**
  - Höhere Kosten für die Umsetzung der neuen Maßnahmen
  - Höhere Strafen (bis zu 10 Mio. Euro oder 2% des Jahresumsatzes)
  - verstärkte Aufsicht
  - Größeres Reputationsrisiko und erhöhter organisatorischer Aufwand zur Sicherstellung der Compliance.

4.3. Umsetzung in Österreich (NISG)

Die NIS-Richtlinien werden in Österreich über das Netzwerk- und Informationssicherheitsgesetz (NISG) umgesetzt, wobei das BMI als zentrale Aufsichtsbehörde fungiert.

5. CISSP

Der Certified Information System Security Professional ist eine Zertifizierung, die von der International Information Systems Security Certification Consortium (ISC)² angeboten wird. Sie gilt als eine der angesehensten Zertifizierungen auf dem Markt für Informationssicherheit. Die meisten Unternehmen verlangen oder bevorzugen diese Zertifizierung bei der Einstellung von Mitarbeiter/innen.

Das breite Spektrum der Themen, die im CISSP-Wissenkorpus enthalten sind, soll sicherstellen, dass Kandidaten/Innen in der Lage sind, Risikominderungsstrategien zu entwickeln, Sicherheitsrichtlinien zu erstellen und Sicherheitslösungen zu implementieren.

5.1. Voraussetzungen für die CISSP-Zertifizierung

Kandidaten/innen müssen mindestens 5 Jahre Berufserfahrung in 2 der 8 CISSP-Domänen haben. Ein Universitätsabschluss oder eine andere anerkannte Zertifizierung kann 1 Jahr Berufserfahrung ersetzen. Sollte die Berufserfahrung nicht vorhanden sein, kann die Person dennoch die CISSP-Zertifizierung machen und Mitglied von (ISC)² werden. Danach hat die Person 6 Jahre Zeit, um die Berufserfahrung zu sammeln.

5.2. CISSP-Domänen

Die 8 Kompetenzbereiche der CISSP-Zertifizierung sind:

1. Sicherheit und Risikomanagement
   - Verstehen und Anwenden von Sicherheitskonzepten
   - Verstehen und Anwenden von Risikomanagementkonzepten

2. Asset Sicherheit
   - Assets und Informationsklassifizierung
   - Festlegen der Anforderungen für den Umgang mit Informationen und Assets

3. Sicherheitsarchitektur und Ingenieurtechnik
   - Sicherheitsfunktionen von Informationssystemen verstehen
   - Bewerten und entschärfen der Schwachstellen von Sicherheitsarchitekturen
   - Auswahl und Festlegen von kryptographischen Lösungen

4. Kommunikations- und Netzwerksicherheit
   - Anwendung sicherer Entwurfsprinzipien in Netzwerkarchitekturen
   - Sichern von Netzwerkkomponenten
   - Implementierung von sicheren Kommunikationskanälen gemäß dem Entwurf

5. Identitäts- und Zugriffsmanagement (IAM)
   - physichen und logische Zugriffssteuerung von Assets
   - Implementierung von Authentifizierungssystemen

6. Sicherheitsbewertung und -tests
   - Durchführung von Sicherheitskontrolltests
   - Sammlung von Sicherheitsprozessdaten (z. B. technische und administrative)

7. Sicherheitsoperationen
   - Durchführung von Konfigurationsmanagement (CM) (z. B. Provisioning, Baselining, Automatisierung)
   - Durchführung von Protokollierungs- und Überwachungsaktivitäten

8. Software-Entwicklungs-Sicherheit
   - Bewertung der Wirksamkeit der Softwaresicherheit
   - Verstehen und Integrieren von Sicherheit in den Software Development Life Cycle (SDLC)

6. IT-Audit

IT-Audits werden von Unternehmen durchgeführt, um Sicherheitsrisiken in einem Unternehmen zu identifizieren und zu verstehen. Audits sind deshalb wichtig, weil Unternehmen viel Geld in Systeme ausgeben und um sicherzugehen, dass die Systeme und deren Outputs ordnungsgemäß funktionieren. Systeme zu inspizieren, Schadensmessungen und Reports zu Fußnissen zu erstellen, das ist Sinn und Zweck von IT-Audits.

IT-Auditer konzentrieren sich stark auf die Cybersicherheit, da Datenpannen und Cyberangriffe zunehmen. Sie prüfen dabei Zugangskontrollen, Netzwerkschutz und Reaktionspläne, um Schwachstellen zu finden.

6.1. Arten von IT-Audits

1. General Control Audits: Beurteilen die gesamte Effektivität der IT-Infrastruktur eines Unternehmens, mit Fokus auf Access-Controls, Management-Änderungen sowie Betriebs- und physischer Sicherheit.
2. Application-Control-Audits: Evaluieren die spezifischen IT-Systeme und deren Applikationen.

6.2. Prozess eines IT-Audits

Der Prozess beginnt mit der Planung, wo Ziele und Ausmaße definiert und Ressourcen bestimmt werden. Gefolgt von der Untersuchung vor Ort, wo ein IT-Auditor Beweise sammelt und Kontrollen vor Ort evaluiert. Anschließend werden die Beweise analysiert und die Ergebnisse in einem Auditbericht zusammengefasst. Der Bericht wird dann dem Management präsentiert und gegebenenfalls werden Empfehlungen ausgesprochen. Der letzte Schritt ist

die Nachverfolgung, bei der überprüft wird, ob die Empfehlungen umgesetzt wurden und ob die Kontrollen weiterhin effektiv sind.

7. ISO 27001

In modernen Unternehmen werden Geschäftsprozesse zunehmend digitalisiert und Daten elektronisch verarbeitet sowie gespeichert. Die Daten- und Informationssicherheit ist daher ein essenzieller Aspekt, wenn es um die IT-Sicherheit geht. Informationen müssen den Mitarbeitern einerseits zuverlässig zur Verfügung stehen, andererseits müssen sie vor nicht autorisierten Zugriffen und Manipulationen geschützt werden.

7.1. ISMS

Hierbei hilft ein **Information Security Management System (ISMS)**. Dieses legt den Grundstein für entsprechende Sicherheitsmaßnahmen. In ihm werden Sicherheitsziele, Richtlinien sowie Prozesse (und ihre Umsetzung) definiert, mit denen die Informationssicherheit kontrolliert, gesteuert und gesteigert werden kann.

Dadurch können mögliche Sicherheitsrisiken identifiziert sowie transparent gemacht werden und das Sicherheitsniveau eines Unternehmens wird effektiv angehoben.

7.1.1. Unterschiedliche Schritte

1. **Zieldefinition:** In dieser Phase wird ein Sicherheitskonzept erstellt, das die Sicherheitsziele des Unternehmens definiert. Das Sicherheitskonzept sollte die Sicherheitsanforderungen des Unternehmens berücksichtigen und die Ziele klar definieren.

2. **Analyse der Risiken**: In dieser Phase werden die Risiken für die Informationssicherheit des Unternehmens analysiert. Dazu gehört die Identifizierung von Bedrohungen, Schwachstellen und potenziellen Auswirkungen auf die Informationssicherheit.

3. **Auswahl und Umsetzung**: Auf Basis der Risikoanalyse werden im dritten Schritt Maßnahmen entwickelt, um Sicherheitsbedrohungen zu minimieren und gezielt reagieren zu können. Diese betreffen nicht nur die IT, sondern alle Bereiche des Unternehmens – inklusive physischer Sicherheitsaspekte.

4. **Die Instandhaltung und Wartung des ISMS**: In dieser Phase wird das ISMS kontinuierlich überwacht und gewartet. Dazu gehört die Überprüfung der Sicherheitsmaßnahmen,

die Schulung der Mitarbeiter und die Anpassung des Sicherheitskonzepts an neue Bedrohungen.

7.2. ISO 27001

Die **internationale Norm ISO 27001** definiert die Anforderungen an ein **Information Security Management System (ISMS)**. Auf Basis international erprobter „Best Practices" definiert die Norm mögliche Risikobereiche und legt fest, ab wann ein solches System ausreichende Informationssicherheit gewährleistet. Betriebe und Institutionen können sich gemäß dieser Norm zertifizieren lassen, um intern Risiken zu minimieren und extern Kundenvertrauen zu maximiere

Bei ISO 27001 handelt es sich um eine von der **Internationalen Organisation für Normung (ISO)** sowie der **Internationalen Elektrotechnischen Kommission (IEC)** herausgegebene Norm. Aus diesem Grund wird sie alternativ auch als IEC 27001 bezeichnet.

Die Zertifizierung bietet Unternehmen einen international anerkannten Leitfaden zur Einführung eines effektiven Informationssicherheits-Managementsystems (ISMS). **Intern** sorgt sie für regelmäßig geprüfte und angepasste Prozesse, klare Zielvorgaben und spart durch bewährte Methoden Zeit und Kosten. Eine Zertifizierung zeigt, dass Sicherheitsmaßnahmen wirksam umgesetzt wurden.

Extern stärkt die Zertifizierung das Vertrauen von Kunden, Partnern und Auftraggebern. Sie signalisiert professionelles Risikomanagement und kann bei Kooperationen oder öffentlichen Ausschreibungen ein entscheidender Vorteil oder sogar eine Voraussetzung sein.

7.3. Zertifizierungsprozess

Die Zertifizierung eines ISMS gemäß ISO 27001 wird von einem unabhängigen Auditor übernommen. Das können beispielsweise Einzelpersonen sein, die ihrerseits beispielsweise durch Stellen wie das Bundesamt für Sicherheit in der Informationstechnik zertifiziert worden sind. Typischerweise geschieht die Zertifizierung jedoch durch geprüfte Zertifizierungsstellen wie dem TÜV. Die Standardisierungsorganisationen ISO, IEC und DIN führen selbst keine Zertifizierungen aus.

7.3.1. Ablauf

1. **Informationsgespräch**

Unverbindliches Gespräch über Voraussetzungen, Nutzen, Geltungsbereich und Anforderungen der Zertifizierung.

2. **Beauftragung**

Nach Angebotsannahme wird die Zertifizierungsstelle offiziell beauftragt.

3. **Voraudit (optional)**

Vorabprüfung zur Feststellung von Schwachstellen und zur Einschätzung der Zertifizierungsfähigkeit.

4. **Zertifizierungsaudit Stufe 1**

Prüfung der Dokumentation, Konformität und Umsetzungsstatus des Managementsystems.

5. **Zertifizierungsaudit Stufe 2**

Praktische Überprüfung der Wirksamkeit des Systems im Unternehmen anhand von Stichproben.

6. **Zertifikatserteilung**

Nach positivem Audit wird das Zertifikat ausgestellt (gültig für 3 Jahre), inklusive jährlicher Überwachung.

7. **Überwachungsaudits**

Jährliche Prüfungen zur Kontrolle und Aufrechterhaltung des Managementsystems.

8. **Re-Zertifizierungsaudit**

Nach drei Jahren erneute, verkürzte Prüfung zur Verlängerung des Zertifikats.

8. IT Grundschutz

Die BSI IT-Grundschutz-Standards sind Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu bewährten Methoden und Maßnahmen der Informations- und IT-Sicherheit. Sie richten sich an Behörden und Unternehmen und basieren auf national sowie international anerkannten Vorgehensweisen.

Aktuell verfügbare Standards:

BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS) ⟶ Definiert allgemeine Anforderungen an ein ISMS, kompatibel mit ISO/IEC 27001.

BSI-Standard 200-2: IT-Grundschutz-Methodik ⟶ Beschreibt, wie ein ISMS praktisch aufgebaut und betrieben wird.

BSI-Standard 200-3: Risikomanagement ⟶ Erklärt die Durchführung von Risikoanalysen nach der Grundschutz-Methodik.

BSI-Standard 200-4: Business Continuity Management (BCMS) ⟶ Leitfaden zum Aufbau eines Notfallmanagementsystems in der eigenen Organisation.

8.1. Vorteile

Kostenfrei & öffentlich zugänglich: Der IT-Grundschutz ist kostenlos und sehr detailliert dokumentiert – ideal als Orientierungshilfe oder Best Practice.

Detaillierte Maßnahmen: Besonders hilfreich für Organisationen, die konkrete Sicherheitsmaßnahmen suchen und nicht bei null anfangen wollen.

Gute Ergänzung zu ISO 27001: Man kann den IT-Grundschutz auch als Werkzeug nutzen, um ISO-27001-Anforderungen umzusetzen – gerade für technische und organisatorische Maßnahmen (TOMs).

Verwendbar in jeder Organisation – auch außerhalb Deutschlands.

Man muss jedoch beachten, dass der IT Grundschutz für die deutschen Behörden und Unternehmen entwickelt wurde. Manche Anforderungen sind daher nicht auf andere Länder übertragbar.

8.2. Unterschied zu ISO/IEC 27001

Ein Zertifikat nach ISO 27001 bescheinigt nur das korrekt eingerichtete ISMS. Nach IT-Grundschutz wird zusätzlich bezeugt, dass ein ausreichendes IT-Sicherheitsniveau erreicht wurde; neben dem funktionierenden Prozess wird also auch dessen tatsächliches Ergebnis bescheinigt.

ISO 27001: international anerkannt, flexibel, risikobasiert – gut für Organisationen, die ihre Sicherheitsstrategie individuell gestalten wollen.

BSI IT-Grundschutz: sehr detailliert, standardisiert, besonders gut für Organisationen in Deutschland mit klaren Vorgaben oder wenig Erfahrung im ISMS-Bereich.

9. Quellen

COBIT & IT-Governance Überblick: https://www.computerweekly.com/de/definition/COBIT COBIT Grundsätze: https://www.agile-heroes.com/de/magazine/cobit/; COBIT ISACA: https://www.isaca.org/resources/cobit#1; Weitere Informationen zu COBIT von Fortinet: https://www.fortinet.com/de/resources/cyberglossary/what-is-cobit; Praktisch um der COBIT Geschichte nachzugehen: https://de.wikipedia.org/wiki/COBIT

Genaue Erklärung von SOX: https://www.ibm.com/de-de/topics/sox-compliance; SOX im Bezug auf Security: https://www.fortinet.com/de/resources/cyberglossary/sox-sarbanes-oxley-act; weiterer Artikel zu SOX-Compliance: https://www.cloudflare.com/de-de/learning/privacy/what-is-sox-compliance/

ISMS:https://enginsight.com/de/glossar/information-security-management-system-isms/
ISOAblauf: https://www.tuv.at/informationssicherheits-zertifizierung-iso-27001/

CISSP:https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/exam-outlines/CISSP-Exam-Outline-May-2021-German.pdf
CISSP:https://www.youtube.com/watch?v=0XKLR19_Ths

Audit:https://www.auditboard.com/blog/it-audit/