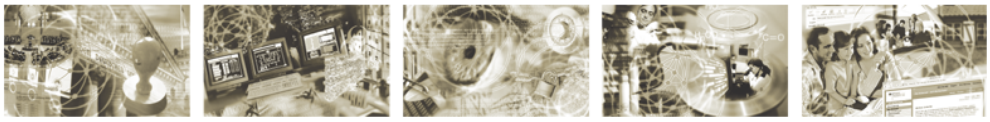
Bundesamt
für Sicherheit in der
Informationstechnik



Band G, Kapitel 1: Einführung

Hochverfügbarkeit eine herausfordernde Aufgabenstellung für ein professionelles IT-Service Management

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: hochverfügbarkeit@bsi.bund.de
Internet: https://www.bsi.bund.de
© Bundesamt für Sicherheit in der Informationstechnik 2013

Inhaltsverzeichnis

1 Einleitung....5
2 Zuordnung zu Standards....7
2.1 Standards mit dem Fokus IT-Governance....8
2.2 Standards mit dem Fokus IT-Sicherheit....8
2.3 Relevante Frameworks....9
3 Zielsetzung....13
3.1 Zielgruppen....15
3.2 Tayloring....15
4 Aufbau des Kompendiums....18
4.1 Grundlagen....18
4.2 Bausteinstruktur....19
4.3 Maßnahmenkatalog....20
4.4 Architekturmodelle und Hilfsmittel....21
5 Messen und Bewerten....22
5.1 Retrospektive Analyse....23
5.2 Prognosen für eine verlässliche Service-Erbringung....24
5.2.1 Prognosen für Prozess-Potentiale....24
5.2.2 Prognosen für Architektur-Potentiale....24
5.2.3 Reifegradmodell zur Bewertung von Verfügbarkeitspotenzialen....25
6. Zuordnung des HV-Kompendiums zu Grundlagenkonzepten für die Bundesverwaltung...29
6.1 BSI-Standards → IT-Grundschutz....29
6.2 Standards und Architekturen für die Bundesverwaltung....31
6.3 IT-Methoden und Methoden zur Prozessmodellierung....33
Anhang: Verzeichnisse....36
Abkürzungen und Akronyme....36
Glossar....36
Literaturverzeichnis....36

Abbildungsverzeichnis

Abbildung 1: Standards als Säulen der Hochverfügbarkeit....7
Abbildung 2: Hierarchie von Standards und Frameworks im Kontext zur Hochverfügbarkeit....12
Abbildung 3: Vorgehen im Kompendium in drei Phasen....18
Abbildung 4: HV-Schichtenmodell....19
Abbildung 5: Messen und Bewerten auf der Zeitachse....22
Abbildung 6: Verfügbarkeitsklassen und Reichweite des IT-Grundschutzes....30
Abbildung 7: Architekturkonzept in SAGA 4.0....32
Abbildung 8: Rahmenarchitektur Bund und Service-Architektur BSI....34

Tabellenverzeichnis

Tabelle 1: Kapitel des ersten Bandes "G: Grundlagen"....19
Tabelle 2: Kapitel des zweiten Bandes "B: Bausteine"....20

Tabelle 3: Kapitel des dritten Bandes "M: Maßnahmen".....21
Tabelle 4: Kapitel des vierten Bandes "AH: Architekturen und Hilfsmittel.....21
Tabelle 5: Typische Verfügbarkeitsklassen und ihre Ausfallzeiten.....23
Tabelle 6: Reifegradstufen.....26
Tabelle 7: Prozess/Architektur-Reifegrade.....27

1 Einleitung

Informationstechnologie (IT) durchdringt heute fast alle Bereiche des privaten oder öffentlichen Lebens. Gerade in Unternehmen und Organisationen haben sich existentielle Abhängigkeiten entwickelt, teilweise haben sie sich schleichend eingestellt und sind damit bisweilen nicht bewusst. Studien belegen regelmäßig, dass bei Ausfall der IT innerhalb weniger Stunden enorme Schäden entstehen[1] und bereits eine Ausfallzeit im Tagesbereich ausreichen kann, um das Überleben von Organisationen zu gefährden. Um die notwendige Handlungsfähigkeit aufrecht zu erhalten, verlangen aus dem gesamten Spektrum der Geschäftsprozesse,vordringlich die kritischen Geschäftsprozesse grundsätzlich einen verlässlichen und nachhaltigen IT-Betrieb. Behörden und Unternehmen stehen damit vor der Herausforderung, die Funktionalität ihrer Geschäftsprozesse kontinuierlich sicherzustellen. Zusätzlich werden IT-Organisationen in Behörden und Unternehmen mit Anforderungen konfrontiert, die sich aus technischen Neuerungen, Marktentwicklungen oder organisatorischen Veränderungen ergeben. Die ständige Anpassung der Systeme an geänderte Anforderungen führt zu Zielkonflikten zwischen Verlässlichkeit und Veränderung. Denn während Verlässlichkeit Beständigkeit verlangt, fordern Veränderungen die Flexibilität. Durch die Verknappung von Ressourcen kann eine weitere Zielkonkurrenz entstehen. Geschäftsprozesse sind die Basis jeder Wertschöpfung. Die Gewährleistung der Kontinuität dieser Prozesse ist zentraler Garant für den Geschäftserfolg und gesetzlich geforderter Gegenstand eines einzurichtenden Risikomanagements. Hohe Qualitätsanforderungen, vornehmlich Anforderungen an die Verlässlichkeit der IT-Services, wie sie im Umfeld kritischer Geschäftsprozesse erwartet werden, erfordern die Ausrichtung der technischen Systeme auf deren Ausfallsicherheit sowie den Aufbau einer klar strukturierten und reibungslos arbeitenden IT-Organisation, die sich an den Anforderungen der Geschäftsprozesse orientiert und die gewünschten Leistungen über definierte IT-Services verlässlich und nachhaltig zur Verfügung stellt. Nachhaltigkeit im Sinne von Kontinuität fordert für kritische Geschäftsprozesse nicht nur verlässliche Ressourcen und ein funktionierendes IT-Service Management sondern verlangt ergänzend ein professionelles Risikomanagement und eine funktionierende Notfallvorsorge, da die Aufrechterhaltung von Geschäftsprozessen in direkter Abhängigkeit zur Sorgfalt der Vorbereitung einer Organisation auf den Eintritt von Geschäftsrisiken steht. Unter dem Stichwort “Compliance” setzen regulatorische Anforderungen die Themen Risiko Management, Business Continuity und Disaster Recovery auf die Agenda jeder Geschäftsleitung. Für die Arbeit von Behörden werden vergleichbare Anforderungen durch die IT-Richtlinie und die IT-Strategie der Bundesverwaltung aufgestellt.

Für die Lösung von Zielkonflikten und für die Nutzung von Synergien bei der Gestaltung der notwendigen Prozesse sind Modelle sinnvoll, die aus Erfahrungen der Praxis entwickelt wurden und ganzheitlich wie durchgängig anwendbar sind. Aus dem Umfeld der Corporate Governance liegen dazu Modelle (z.B. COSO) vor, die eine verantwortliche, professionelle, transparente und auf den langfristigen Erfolg ausgerichtete Steuerung und Führung ermöglichen, und damit positive interne wie externe Effekte erzielen. Interne Effekte stellen Nutzen für die Organisation selbst dar, externe Effekte stellen Kundennutzen oder Nutzen von Interessengruppen dar.

Governance, Compliance und Risk Management werden bisweilen in die alleinige Verantwortung einzelner Organisationsbereiche wie z. B. dem IT-Bereich gelegt. Oder es werden verschiedene Bereiche beauftragt, die isoliert arbeiten. Vergleichbar dem Total-Quality-Management (TQM) ist ein ganzheitlicher Governance, Compliance und Risk Management (GCR) Ansatz zu wählen, der

1 Nach einer aktuellen Studie von Symantec verursacht eine Datenpanne in Unternehmen Kosten von ca. 3,4 Mio. € , sofern der öffentliche Sektor betroffen ist, wird der Schaden pro Datenpanne mit 1,87 Mio. € angegeben http://www.symantec.com/content/de/de/about/downloads/press/2010_annual_study.pdf

alle Verantwortungsbereiche einbezieht. Die Gesamtverantwortung der obersten Leitungsebene wird damit über alle Management-Ebenen heruntergebrochen und an den einheitlichen Zielen ausgerichtet und gemessen.

Die Basis dazu liefern nationale und internationale Initiativen zur Formalisierung und Standardisierung von Steuerung und Kontrolle von Unternehmen sowie der IT als deren Teilbereich. In Anlehnung an den Begriff Corporate Governance wurde der Begriff IT-Governance geprägt, dem in einer Vielzahl von Regelungen in Europa und Deutschland Rechnung getragen wird. Im Bereich der Bundesverwaltung wurde die Notwendigkeit einer ganzheitlichen IT-Steuerung erkannt und durch das Konzept „IT-Steuerung Bund“ einer Umsetzung zugeführt. Im Rahmen dieses Konzeptes werden Strategien, Architekturen und Standards der Bundesverwaltung entwickelt.

Für eine IT-Steuerung bedeutet dies folglich, dass sie auf vorliegenden Standards aufsetzt und sich in den ganzheitlichen Ansatz der Coporate Governance integriert. Die Auswahl eines Steuerungsmodells wird dadurch bestimmt, dass es die Grundgedanken eines ganzheitlichen GCR-Ansatzes aufgreift und auf den IT-Bereich transponiert. Ein IT-Sicherheitsmanagement bedarf demnach Standards, die sich darunter subsumieren. Die Linie der Standards und ihre Einordnung wird nachstehend dargestellt. Für dieses HV-Kompendium ist die Integration der Standards und der ganzheitliche Aspekt des GCR-Ansatzes grundlegende Zielausrichtung.

2 Zuordnung zu Standards

Im Kontext zur **Corporate-** bzw. **IT-Governance** liegen eine Reihe von Standards vor, die zur Bewältigung der beschriebenen Herausforderungen als Orientierung herangezogen werden können. Für den privatwirtschaftlichen Bereich existieren einschlägige Rechtsnormen und Bestimmungen – z.B. das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), für den Bankenbereich Basel II/III oder für internationale Konzerne der Sarbanes-Oxley-Act (SOX/EuroSOX) - welche eine Corporate Governance fordern.

Die Standards zur Coporate Governance gehen von einer strategische Ausrichtung von Managementprozessen an Geschäftszielen aus und sehen Verlässlichkeit und Nachhaltigkeit als Grundlage für den Fortbestand einer Organisation. Damit kommt den Prozessen zur Business Continuity und zum Risikomanagement eine besondere Bedeutung zu. Diese Sichtweisen wurden in die Standards der IT-Governance übernommen. Aus den Standards heraus haben sich eine Reihe von generischen Frameworks (Rahmenwerke) entwickelt, welche Synergien aus "Best Practices" bei der Umsetzung nutzen und in einem Steuerkreis darstellen. Waren diese Frameworks ursprünglich aus Kontroll- und Steuerungsgesichtspunkten heraus entwickelt worden, dienen sie heute zunehmend der Professionalisierung des Prozessmanagements und der IT-Steuerung.

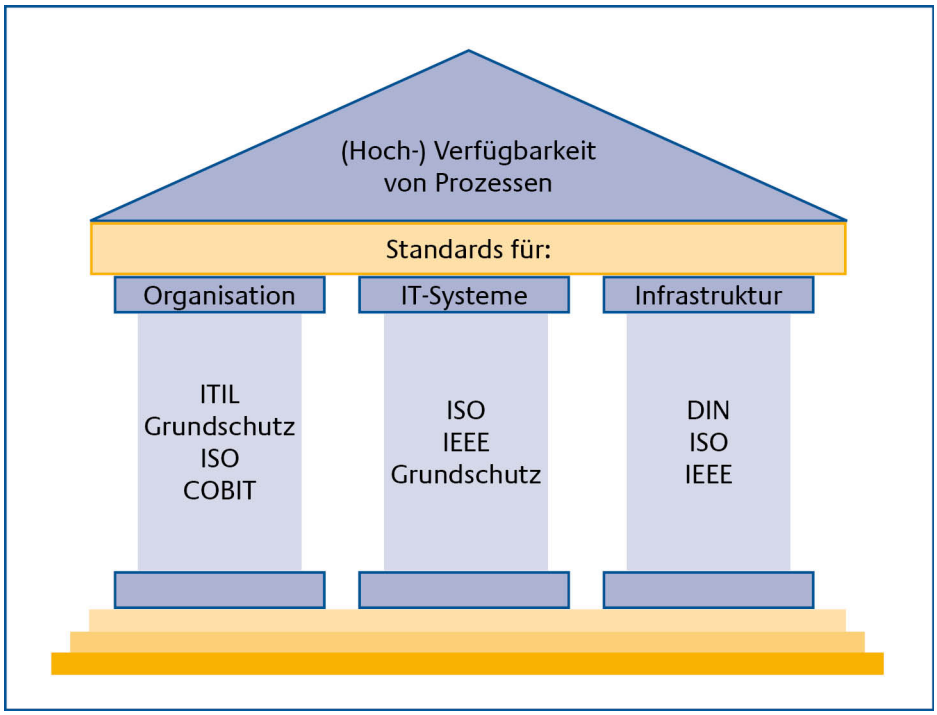


Abbildung 1: Standards als Säulen der Hochverfügbarkeit

Eine Zusammenstellung der relevanten Standards wird für Unternehmen gemeinsam vom BITKOM und DIN unter den Titel "Kompass der IT-Sicherheitsstandards“ [BITKom11] herausgegeben. Für Bundesbehörden wird mit SAGA (Standards und Architekturen für E-Government-Anwendungen) vom Rat der IT-Beauftragten des Bundes eine Sammlung von Standards zur Verfügung gestellt, die Interoperabilität, Wiederverwendbarkeit, Offenheit, Reduzierung von Kosten und Risiken durch Nutzung von Standardisierungen und Skalierbarkeit der Lösungen verfolgen. Nachstehend wird ein zusammenfassender Überblick über die relevanten Standards und Prozessmodelle gegeben.

2.1 Standards mit dem Fokus IT-Governance

- Die Norm **ISO 31000**[2] **"Risiko Management"** ist die einheitliche Basis für das Management der unterschiedlichen Risiken in einer Organisation. Darin wird ein Risikomanagementsystem nach drei Prinzipien verankert:
  - Risikomanagement ist Führungsaufgabe,
  - Risikomanagement erfolgt Top-Down,
  - Risikomanagement erfolgt nach einheitlichen Kriterien und Vorgehen.
- Die Norm **ISO 38500**[3] **"Corporate Governance in Information Technology"** liefert Richtlinien für das integrierte Management der IT (IT-Governance) zur strategischen Ausrichtung, Steuerung und Überwachung von in Unternehmen eingesetzten Informationstechnologien und Prozessen. COBIT wird darin als Referenz-Modell für Richtlinien und Prozesse empfohlen, welche im Rahmen des IT-Governance Management Systems zu implementieren sind.
- Die Norm **ISO 20000**[4] **"IT-Service Management"** setzt einen Standard für das IT-Service Management, der als Ableger der **ISO 9000** qualitative Mindestanforderungen und weitergehende Empfehlungen für die Umsetzung des IT-Service-, Security- und Relationship-Managements in der IT regelt.

2.2 Standards mit dem Fokus IT-Sicherheit

- Die Normenreihe I**SO 2700x** liefert Standards für Aufbau und Qualitätssicherung des IT-Sicherheitsmanagementsystems. Für die Ausgestaltung und Bewertung der Sicherheitsorganisation haben sich darunter spezifische Standards etabliert, die konkretere Anforderungen auf der technischen und organisatorischen Ebene formulieren.
- Der ISO Standard 27001[5] "Information technology - Security techniques - Information security management systems requirements specification" wurde mit dem **Ziel** entwickelt, ein System bereitzustellen, auf dessen Basis ein **Informations-Sicherheits-Management-System (ISMS)** aufgebaut und betrieben werden kann. Es werden die für das Geschäft notwendigen Informationswerte betrachtet. Der Fokus liegt nicht nur auf IT Sicherheit, sondern auf Informationen. Er ist der direkte Nachfolger des zweiten Teiles des BS 7799 Standards, jedoch wurde der Standard um einen elften Abschnitt erweitert, der sich ausschließlich dem Thema „Information Security Incident Handling“ (Management von Sicherheitsvorfällen) widmet und die ursprünglich in anderen Abschnitten verstreuten Anforderungen und Inhalte zum Umgang mit Sicherheitsvorfällen konsolidiert.
- Mit der internationalen Norm **ISO 27004** liegt ein Entwurf für die Bewertung der Qualität eines IT-Sicherheitsmanagementsystems vor. Die Konkretisierung von Bewertungskriterien und Indikatoren für die Praxis kann dabei auf der Grundlage generischer Prozessmodelle erfolgen, die solche Bewertungskriterien bereitstellen. CobiT liefert für die Bewertung ein Modell zur Bewertung der Potentialreife seiner Prozessgebiete. ITIL schließt darüber hinaus grundsätzliche Anforderungen an die Implementation des Service-Life-Cycle und des Security Managements ein, die auch im ISO 20000 Standard berücksichtigt sind.

2 http://de.wikipedia.org/wiki/Risikomanagement-Standard
3 http://www.38500.org/ IT Governance Standard
4 http://de.wikipedia.org/wiki/ISO/IEC_20000
5 http://de.wikipedia.org/wiki/ISO/IEC_27001

- Im Bereich Informationssicherheitsmanagement ISMS stellt die **ISO 27005** eine genaue Anleitung zur **IT-Risikoanalyse** und zum **Risikomanagement** im IT-Bereich vor. Die ISO 27005 beschreibt einen ganzheitlichen Risikomanagementprozesses und definiert dazu einzelne Merkmale der Risikoanalyse. Für das Risikomanagement wird auf die ISO 27001 referenziert und in den Anhängen der IEC 27005 werden weiterführende Informationen dazu geliefert.
- Die umfassenden Sicherheitsstandards des **BSI 100-1 bis 100-4**[6] bieten auf der Basis der ISO 27001 einerseits bewährte Management-Ansätze, Empfehlungen und Lösungsvorschläge und stellen Hilfsmittel für verbreitete IT-Konfigurationen zur Verfügung, um damit gängigen Gefährdungen wirksam begegnen zu können:
- **BSI-Standard 100-1**: Managementsysteme für Informationssicherheit (ISMS). Der vorliegende BSI-Standard definiert allgemeine Anforderungen an ein ISMS.
- **BSI-Standard 100-2**: IT-Grundschutz-Vorgehensweise. Die IT-Grundschutz Vorgehensweise beschreibt den schrittweisen Aufbau und Betrieb eines IT-Sicherheitsmanagements in der Praxis. Er ist vollständig kompatibel zum ISO Standard 27001 und berücksichtigt weiterhin die Empfehlungen der ISO Standards 13335 und 17799.
- **BSI-Standard 100-3:** Risikoanalyse auf der Basis von IT-Grundschutz.
  Zur Abdeckung von Sicherheitsanforderungen, die über das normale Maß hinausgehen, hat das BSI einen Standard zur Risikoanalyse auf der Basis von IT-Grundschutz erarbeitet. Diese Vorgehensweise ermöglicht den Behörden oder Unternehmen eine zur IT-Grundschutzanalyse ergänzende Risikoanalyse, um die erweiterten Anforderungen zu erfüllen.
- **BSI-Standard 100-4:** Notfallmanagement. Mit diesem Standard wird ein Vorgehen beschrieben, um die Kontinuität des Geschäftsbetriebs sicherzustellen. Dies stellt eine unabdingbare Voraussetzung zur Gewährleistung hoher und höchster Verfügbarkeiten dar.

Dieses Kompendium integriert die bestehenden Standards des IT-Grundschutzes. Es beschreibt ein Vorgehen für die Durchführung von Risikoanalysen nach BSI-Standard 100-3 bzw. ISO 27005 und die Differenzierung des IT-Sicherheits- und Risikomanagements nach BSI-Standard 100-1 für Hochverfügbarkeitslösungen. Die Umsetzung der relevanten Maßnahmen-Emfehlungen aus den IT-Grundschutz-Katalogen des BSI sind notwendige Voraussetzung für das weitere Vorgehen nach diesem Kompendium in Hinblick auf die Hochverfügbarkeit.

2.3 Relevante Frameworks

IT-Governance wird durch eine Reihe von Rahmenwerken (Frameworks) unterstützt, welche Modelle für die Erfüllung der Anforderungen der Corporate Governance bzw. der IT-Governance liefern und die sich in der Praxis bewährt haben. Je nach Hierarchiestufe, welcher der zugehörige Standard angehört, sind die darunterliegenden Standards als Teilmenge davon anzusehen, sodass inhaltliche Überschneidungen möglich sind. Relevante ITG-Frameworks sind:

- das vom Committee of Sponsoring Organizations of the Treadway Commission entwickelte **COSO-Framework**[7], das sich ursprünglich aus Sicht der Finanzkontrolle insbesondere mit der Steuerung und internen Kontrollen in Unternehmen beschäftigt. Mit **COSO ERM (2004)**

6 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html
7 http://de.wikipedia.org/wiki/COSO

wird ergänzend ein Framework für das „Enterprise Risk-Management“ zur Verfügung gestellt,

- die Architekturmethode der Open Group **TOGAF**[8] (The Open Group Architecture Framework) bietet einen umfassenden Ansatz für Entwurf, Planung, Implementierung und Wartung von Unternehmensarchitekturen in den Dimensionen:
  - Geschäftsarchitektur,
  - Informationsarchitektur und
  - Technologiearchitektur.
- die ISACA (Information System Audit and Control Association) veröffentlicht das **CobiT**[9] - Framework, als Werkzeug für die IT-Revision. CobiT definiert 34 IT-Prozesse in den vier Domänen Planung und Organisation, Beschaffung und Einführung, Auslieferung und Unterstützung sowie Überwachung/Steuerung.
- die von der britischen CCTA (Central Computer and Telecommunication Agency) entwickelte **Information Technology Infrastructure Library (ITIL)**[10] die einen Schwerpunkt auf das Service Management legt und den auf *ISO 20000* aufbauenden Qualitätsstandard für IT-Service Management realisiert.
- Kontrollmechanismen, Methoden und Verfahren zur Umsetzung der ISO 2700x, die sich zur Gewährleistung der IT-Sicherheit bewährt haben. Detail-Ausführungen hierzu liefern die **BSI-Standards 100-1 bis 100-4** sowie die **IT-Grundschutzkataloge**[11].
- Das vom Software Engineering Institute bei der Carnegie Mellon University entwickelte **Capability Maturity Model Integration (CMMI)**[12] stellt ein Referenzmodell zur Verfügung, für die Ermittlung der Prozessreife. Die ursprüngliche Ausrichtung auf Produktentwicklung wurde auf den Produkteinkauf und die Softwareentwicklung ausgedehnt, weitere Anwendungsbereiche sind in Arbeit. Das CMMI-Modell liefert eine systematische Darstellung bewährter Praktiken für die Optimierung von Abläufen in einer Organisation.
- Als gemeinsames Qualitätsbewertungsmodell der öffentlichen Verwaltung wurde das Europäische **Common Assessment Framework (CAF)**[13] eingeführt. Basis dieses Ansatzes zum Qualitätsmanagement ist die Normenreihe DIN EN ISO 9000, welche in die Grundphilosophie des **Total Quality Managements (TQM)** in der DIN EN ISO 8402 verfeinert wurde und einen ganzheitlichen methodischen Ansatz zur Planung, Durchführung und Bewertung von Qualitätszielen einführt. „Alle Tätigkeiten des Gesamtmanagements, die im Rahmen eines Qualitätsmanagementsystems die Qualitätspolitik, die Ziele und Verantwortlichkeiten festlegen, sowie diese durch Mittel wie Qualitätsplanung, Qualitätslenkung, Qualitätssicherung und Qualitätsverbesserung verwirklichen", gehören nach der ISO 8402 zum Verantwortungsbereich des Qualitätsmanagements. Zentrale

8 http://de.wikipedia.org/wiki/TOGAF
9 http://www.isaca.org/About-ISACA/Press-room/News-Releases/German/Pages/COBIT-Rahmenwerk-reduziert-IT-Risiken-und-verbessert-Compliance.aspx,; CobiT 5: https://www.isaca.org/COBIT/Pages/Product-Family.aspx
10 http://de.wikipedia.org/wiki/IT_Infrastructure_Library (ITIL)
11 https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/kataloge.html;jsessionid=DEE5ED3ABB123CCF23667DE1E7772BE6.2_cid174
12 http://de.wikipedia.org/wiki/Capability_Maturity_Model_Integration
13 http://www.caf-netzwerk.de/cln_170/nn_376478/sid_3AB36071BBBD84165AFDA180DC5593A0/nsc_true/CAF-Netzwerk/home/home-node.html?__nnn=true

Kriterien der Qualitätsbewertung sind dabei die Kunden-, Prozess-, Mitarbeiter- und Ergebnisorientierung sowie die Etablierung eines kontinuierlichen Verbesserungsprozesses.

Ein Standard oder Framework, der allein die Verfügbarkeit von Prozessen oder (IT)-Infrastrukturen beschreibt, existiert derzeit nicht. Gleichwohl kann der Verfügbarkeitsaspekt aus verschiedenen, sich gegenseitig ergänzenden Standards/Frameworks abgeleitet werden. Die nachstehenden Referenzmodelle wurden bei der Entwicklung dieses HV-Kompendiums herangezogen:

- **ITIL** bündelt Betriebsleistungen der IT-Organisation und der eingesetzten IT-Infrastruktur in IT-Services und stellt Prozesse dar, um diese Services zu steuern und zu überwachen. Dazu werden organisatorische Strukturen für Design und Betrieb von IT-Services auf wohl definierten Service-Leveln und Prozesse für eine Service-Optimierung beschrieben. Für die Beschreibung von Prozessen im Bereich IT-Service Management unter Integration des Security-Managementes orientiert sich dieses Kompendium an diesen Empfehlungen.
- **TOGAF** hat seine Stärke zweifellos im Design von der Unternehmens- und Geschäftsarchitektur. Dazu definiert TOGAF einen Prozess zur Architektur-Entwicklung, die streng orientiert an den Anforderungen den Ist-Zustand in einen Zielzustand überführt. Diese Optimierungsansatz findet sich im Vorgehen in den Phasen S, I und Phase M des HV-Kompendiums wieder.
- **COBIT** sieht die IT als wesentliche Grundlage eines Unternehmens zur Erreichung der Geschäftsziele und fordert, dass die Ziele aus der Geschäftsstrategie in die Ziele der IT einfließen (cascade) und die gelieferten Services den Qualitätsanforderungen der Geschäfts-prozesse genügen. Ebenso wie ITIL setzt COBIT auf zielgerichtete, optimierte IT-Prozesse.
- **CAF** ist geeignet, Stärken und Verbesserungspotenziale zu erkennen und daraus Optimierungspotentiale abzuleiten und folgt dem PDCA-Zyklus. PDCA steht für Plan (planen), Do (umsetzen), Check (überprüfen) und Act (anpassen). Der Bewertungsansatz geht von einer Entwicklung von Organisationen von einfachen Strukturen über mehrere Potenzialstufen hin zu optimierten Strukturen aus und bewertet in einem Prozent-Ranking. Dabei kann festgestellt werden, dass Potenzialstufen und prozentualer Rankingwert hoch mit Reifegradstufen eines Reifegradmodells (z.B. CMMI) korrelieren.

Fazit: CAF ist das universelle, organisationsweite Modell zur Identifikation von Optimeirungspotentialen, während die anderen Modelle den Fokus stärker auf den IT-Bereich legen. CobiT integriert weitgehend relevante Standards, bewertet anhand von Qualitätszielen und Ziel auf die Optimierung von Prozessen. ITIL ist durch Stärken ausgezeichnet, die im Bereich Service- und Ressourcen- Management liegen, insbesondere in der Beschreibung der notwendigen IT-Prozesse für eine Realisierung des IT-Service-Management. Ein weitere Bewertungsschema zur Bewertung von Prozesspotentialen wird mit CMMI geliefert, um Steuerung und Kontrolle im Sinne eines kontinuierlichen Verbesserungsprozesses zu realisieren. CMMI wurde zur qualitativen Bewertung von Entwicklungsprozessen im Umfeld des Software Egineerings entwickelt und diefiniert dazu Reifegrade. In diesem Kompendium werden diese Ansätze auf das Design hochverfügbare Architekturen sowie auf die die Bewertung und Optimierung des Verfügbarkeitspotentials übertragen. Diese Rahmenwerke werden uns daher in diesem Kompendium wiederholt begegnen.

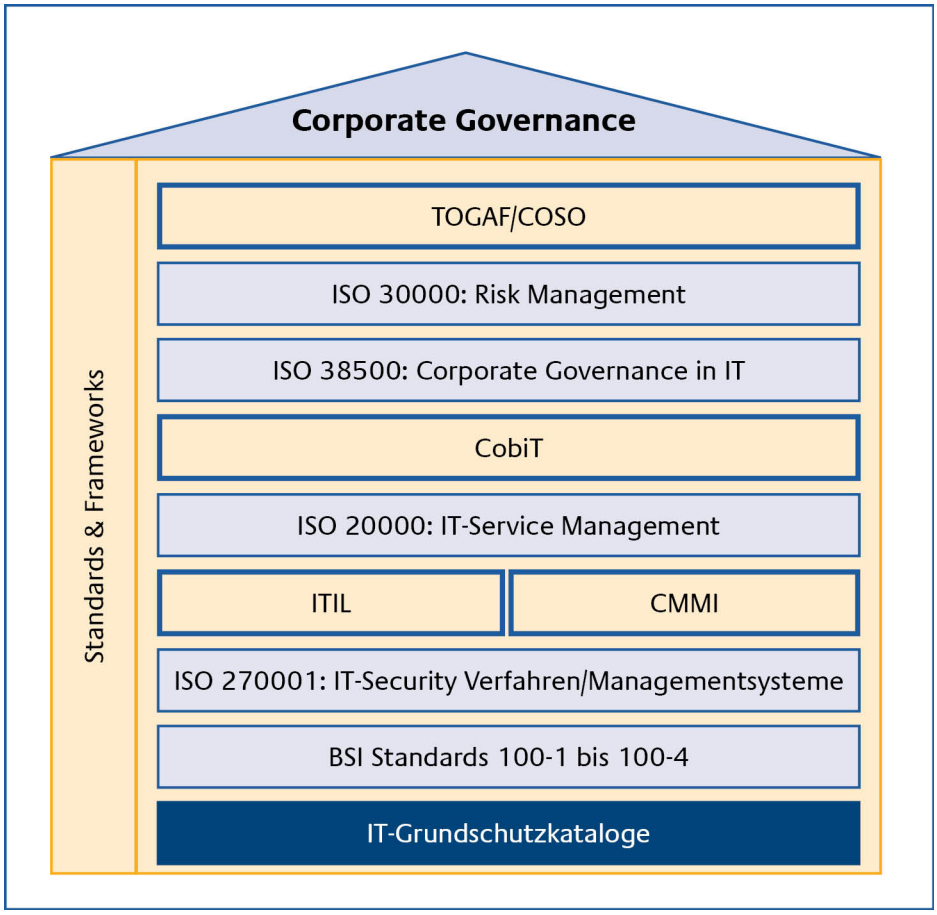


Abbildung 2: Hierarchie von Standards und Frameworks im Kontext zur Hochverfügbarkeit

3 Zielsetzung

Mit diesem Kompendium wird das Ziel verfolgt, den verantwortlichen Managementebenen Hilfestellung zur Wahrnehmung ihrer Verantwortung im Rahmen der IT-Governance anzubieten. Zentrale Zielsetzung des HV-Kompendiums ist Optimierung des Verfügbarkeitspotentials durch die Gestaltung hochverfügbarer Architekturen und damit die **Förderung von Verlässlichkeit und Nachhaltigkeit** von IT-Services. Wie aus den einschlägigen Standards zu schließen ist, greift die rein technische Betrachtung von Architekturen deutlich zu kurz. Nach TOGAF sind Geschäftsarchitektur, Informationsarchitektur und Technologiearchitektur ganzheitlich zu betrachten. Dazu werden in Anlehnung an internationale Standards und Frameworks zur IT-Governance Aktivitäten zur Steuerung und Überwachung beschrieben, die Aktivitäten für ein hinreichendes IT-Risikomanagement einschließen. Aus einem ganzheitlichen Risikomanagement heraus wird in diesem Kompendium auf den verlässlichen und nachhaltigen Einsatz der IT-Ressourcen im Sinne der Verfügbarkeit fokussiert. Insbesondere für kritische Geschäftsprozesse wird damit die Erreichung der Geschäftsziele auch unter einschränkenden Rahmenbedingungen eingeschlossen.

In der Konkretisierung dieser Zielausrichtung liefert dieses Kompendium eine Anleitung für die Analyse der Anforderungen aus den Geschäftsprozessen im Hinblick auf Nachhaltigkeit und Verlässlichkeit. Den daraus resultuierenden Anforderungen für das IT-Service-Management stellt es die Bewertung der gelieferten Service-Qualität gegenüber und betrachtet das Potenzial für die Bewältigung von Risiken aus technischer wie aus organisatorischer Sicht. Mit einer Potential-Analyse werden Schwachstellen und Optimierungspotentiale identifiziert. Bei Unterdeckung der Anforderungen liefert dieses Kompendium mit seinen Architekturmodellen und seinem Maßnahmenkatalog zudem Handreichungen zur Optimierung durch Ableitung und Umsetzung geeigneter Maßnahmen. Die Einrichtung verlässlicher IT-Ressourcen und Anregungen für die Gestaltung von hochverfügbaren IT-Architekturen und effektiver IT-Management-Prozesse werden damit ermöglicht. Mit seinen Anregungen für Nachhaltigkeit und Verlässlichkeit sind die Ansätze auf den langfristigen Erfolg ausgerichtet.

Mit Blick auf Nutzen, Geschäftserfolg und Ressourcen-Einsatz werden die nachstehenden über alle Geschäftsbereiche gemeinsam gültigen Ziele verfolgt:

- **Verlässlichkeit**

  Im Sinne dieses HV-Kompendiums wird Verlässlichkeit wie folgt definiert:
  "Verlässlichkeit beschreibt die Erwartung, dass ein Service die angeforderte Funktion auch hinsichtlich der geforderten Qualität aktuell erfüllt."
  Damit wird in erster Linie der unmittelbare Nutzen durch die Realisierung von Geschäftserfolgen und deren Wertschöpfung adressiert.

- **Nachhaltigkeit**

  Im Sinne dieses HV-Kompendiums wird Nachhaltigkeit wie folgt definiert:
  „Nachhaltigkeit bietet die Gewähr, dass die Funktionalität eines Service in der geforderten Qualität auch künftig zur Verfügung steht, dabei sind auch Umstände zu bewältigen, die besondere Anforderungen an die Kontinuität der IT und des Geschäftserfolges stellen.“
  Diese Sichtweise fokussiert auf die Sicherstellung der Kontinuität der Organisation durch Wahrung bestehender Werte, Schutz von Firmen Know-How, Interessen- & Chancenwahrung.

Verlässlichkeit und Nachhaltigkeit beeinflussen als zentrale Organisationsziele die Bereitstellung von Ressourcen und Organisationsstrukturen sowie die Ausrichtung der IT.

Das HV-Kompendium bietet die Möglichkeit, unter dem Aspekt der Verfügbarkeitsoptimierung in die Professionalisierung des IT-Service Management einzusteigen und eine weitgehende Risikotransparenz als Voraussetzung für ein erfolgreiches IT-Risikomanagement zu schaffen. Die mit den Standards der IT-Governance einhergehenden generischen Frameworks **(TOGAF, CMMI, CobiT und ITIL** (siehe unter 2.3)) liefern praxiserprobte Methoden (Best Practices) der Gestaltung und Steuerung von Prozessen, die bei der Entwicklung des Vorgehens nach diesem Kompendium als Modelle herangezogen wurden.

Risiko Management und IT-Steuerung benötigen eine Beurteilung der in der Organisation vorliegenden Potentiale, die einerseits als Indikatoren für die konkret gegebenen Möglichkeiten einer Risikobewältigung anzusehen sind. Andererseits liefern diese Indikatoren die konkreten Möglichkeiten einer Nutzenoptimierung. Das Vorgehen nach diesem Kompendium berücksichtigt diese Aspekte. Dazu werden in dem später dargestellten Vorgehen die Anforderungen aus Sicht der Geschäftsprozesse im SOLL erhoben und dem ermittelten Potential (IST) der eingesetzten IT-Ressourcen gegenüber gestellt. Im Rahmen der Analyse werden die Service-Potentiale einschließlich des erbrachten Sicherheits- und Verfügbarkeits-IST auf der Basis von Indikatoren an den eingesetzten IT-Ressourcen festgestellt. Die Analyse-Ergebnisse ermöglichen über die Potentialbewertung eine Risikobeurteilung mit der Gefährdungs- und Schadenspotentialen ein Bewältigungspotential gegenüber gestellt werden kann und damit die Eintrittwahrscheinlichkeit an Werten und Geschäftsprozessen bestimmbar gemacht werden kann. Vorgehensweise und Analyse orientieren sich an den durch Standards und Rahmenwerke eingeführten Steuerungsinstrumenten und Bewertungskriterien, die in diesem HV-Kompendium unter den Aspekt Verfügbarkeit, Verlässlichkeit und Nachhaltigkeit verfeinert werden.

Um den Risiken aus kritischen Geschäftsprozessen gerecht zu werden und Hochverfügbarkeit zu erreichen gilt es, auf dem Niveau einer Basisinfrastruktur aufbauend, das Zusammenwirken vieler voneinander abhängiger Bereiche zu betrachten und für eine individuelle Lösung zu gestalten. Die Maßnahmenempfehlungen zur Reduzierung der Risiken schließen den organisatorischen Bereich ein. Jede Lösung wird mit unterschiedlichen Restrisiken verbunden sein, sodass dieses Kompendium auch eine Anleitung geben soll, um im Rahmen einer Restrisikoanalyse die notwendige Risikotransparenz herzustellen.

Was dieses Kompendium nicht kann:

- Man wird von diesem Kompendium keine Rezepte oder pauschale Lösungen „von der Stange“ erwarten können, da die konkrete Gestaltung stark von den Anforderungen der Geschäftsprozesse und dem individuellen organisatorischen Umfeld sowie den konkret vorhandenen IT-Ressourcen und Potentialen einer Behörde oder eines Unternehmens abhängig ist. Dennoch werden zahlreiche Lösungsszenarien prototypisch für die Gestaltung der individuellen IT-Einsatzumgebungen gelten. Dazu stellt dieses Kompendium geeignete Architekturmodelle zur Verfügung, die als Vorlage für eine individuelle Anpassung genutzt werden können.
- Diese Kompendium bietet keine Anleitung für eine Geschäftsprozessanalyse oder deren Modellierung. Im Rahmen der Phase S wird eine Anforderungsanalyse durchgeführt, die spezifisch auf Verfügbarkeit ausgerichtet ist und sich dabei insbesondere auf die Qualitätsaspekte Verlässlichkeit und Nachhaltigkeit konzentriert. Für Analyse und

Modellierung von Geschäftsprozessen in der öffentlichen Verwaltung[14] steht eine entsprechende Arbeitshilfe zur Verfügung.

- Diese Kompendium bietet keine Anleitung für die Ableitung von Funktionen aus einem geschäftlichen Modell zur Entwicklung eines funktionalen Dienstekataloges. Hierzu liegt der Leitfaden Rahmenarchitektur[15] der CIO des Bundes vor. Natürlich gibt es Schnittstellen zu diesem Leitfaden *(siehe unten: 6. Zuordnung des HV-Kompendiums zu Grundlagenkonzepten für die Bundesverwaltung).* Während die o.a. Empfehlung zur Entwicklung und deren Orchestrierung in einer Dienstearchitektur aus Sicht der Geschäftsprozesse vorgeht, werden in der Phase M dieses Kompendiums anforderungskonforme IT-Services geschaffen und in IT-Dienstleistungen orchestriert. Beide Ansätze treffen sich auf der Ebene der konkreten Dienste, die in den Dienstekatalog eingehen.

3.1 Zielgruppen

Das HV-Kompendium beschreibt Vorgehensweisen für alle Organisationen, die Anforderungen aus Sicht der Geschäftsstrategie oder der Geschäftsprozesse identifizieren wollen und diese als Grundlage für die Ausrichtung der geforderten Service-Qualität und der eingesetzten IT-Ressourcen nutzen, wollen. Insofern werden Verantwortliche für Geschäftsprozesse sowie Verantwortliche für IT-Services gleichermaßen angesprochen. Da die Verantwortung für die Definition und die Kontrolle der Erreichung von Geschäftszielen Aufgabe des Managements darstellt, sollte von oberster Ebene der notwendige Analyse- und Gestaltungsprozess angestoßen, gesteuert und überwacht werden und über die Ergebnisse informiert sein. Dies wird insbesondere dann dringlich, wenn die Potentialanalysen Handlungsbedarf signalisieren.

Als Zielgruppe im engeren Sinne werden Verantwortliche gesehen, die in nachstehenden Bereichen engagiert sind:

1. für Geschäftsprozesse (Prozess-Owner), insbesondere für kritische Geschäftsprozesse,
2. für IT-Betrieb und IT-Prozesse (CIO),
3. als IT-Service-Manager,
4. als Manager für Service Design, Service Support, Service Delivery,
5. als Manager für Application Management, insbesondere Anforderungsmanagement und
6. als Manager für IT-Governance, IT-Steuerung und Überwachung der Compliance sowie
7. für IT-Sicherheitsmanagement.

3.2 Tayloring

- Dieses Kompendium geht den Aufgabenkomplex “Verfügbarkeit” umfassend an. Bisweilen sind einzelne Verantwortliche lediglich an Teilaspekten interessiert, diesen wird durch den modularen Aufbau des Kompendiums Rechnung getragen. Durch eine Auswahl geeigneter Module wird ein Gerüst für die Gestaltung der jeweiligen Teilprozesse an die Hand gegeben. Die Auswahl ist abhängig von der Zielstellung als Teilaspekt einer delegierten

14 http://www.cio.bund.de/DE/Standards/Modellierung/modellierung_node.html
15 http://www.cio.bund.de/DE/Standards/Architekturmanagement/architekturmanagement_node.html

Verantwortlichkeit. Nachstehend wird eine Auswahl für folgende Zielstellungen vorgenommen:

- Selektion "**Anforderungsanalyse**" für die Ermittlung der Anforderungen aus der Sicht der Geschäftsprozesse durch GP-Verantwortliche oder Vertreter von Fachabteilungen mit der Lektüre dieser Einführung, sowie des Kapitels 3 "IT-Steuerung" und Abarbeiten der Empfehlungen für „Phase S" nach Kapitel 4 des Bandes „G";
- Selektion "**Architektur-Design**" für das Design höher verfügbarer HV-Umgebungen und -Architekturen durch Verantwortliche für die Auswahl und den Betrieb von IT-Verbünden mit der Lektüre dieser Einführung, dem Kapitel des Kapitels 3 "IT-Steuerung ", Orientierung an den in Band G unter Kapitel 6 beschriebenen HV-Prinzipien, Orientierung an den unter Band B Kapitel 1 „Meta-Ebene" beschriebenen Anforderungskriterien und Vergleich der bestehenden Architektur mit den Architekturmodellen aus Band „AH" Kapitel 1 „Architekturmodelle" ergänzt um die spezifischen Regelungen der relevanten Bausteine zur Realisierung hoher Verfügbarkeit aus Band B dieses Kompendiums;
- Selektion "**Restrisikobewertung**" für die Bewertung des Restrisikos durch GP-Verantwortliche oder Vertreter von Fachabteilungen gemeinsam mit IT-Verantwortlichen im Rahmen der präventiven Abwehr von Gefahren. Mit der Lektüre dieser Einführung sowie dem Kapitel 3 "IT-Steuerung/HV-Analyse" und Abarbeiten der Phasen S und I nach den Kapiteln 4 und 5, sowie Abarbeiten der Empfehlungen für die Restrisiko-Betrachtung in Kapitel 6 des Bandes G wird den Verantwortlichen eine Hilfe zur Abarbeitung und die Hand gegeben. Für kritische Geschäftsprozesse wird empfohlen, den BSI Standard 100-4 zur Umsetzung der Business-Kontinuität heranzuziehen;
- Selektion "**Identifikation von Optimierungspotential**" ist ein Optimierungsansatz auf kurzem Weg, der ohne Rücksicht auf notwendige Aktivitäten zum Service-Management und zur -Steuerung. Um Optimierungspotentiale für bestimmte Architekturen zu identifizieren, lassen sich die Architekturmodelle des Bandes AH Kapitel 1 durcharbeiten. Ergänzend wird empfohlen, die Kapitel 3, 5 und 6 des Bandes G heranzuziehen. Die zum angestrebten Architekturmodell relevanten Bausteine und Maßnahmenempfehlungen sind bei der Umsetzung zu beachten.
- Selektion "**Service-Management**" für das Design anforderungsgerechter IT-Services für kritische Geschäftsprozesse. Service-Manager können auf dieser Basis den von ihnen verantworteten Service-Bereich unter Verfügbarkeits-, Kapazitäts- und Sicherheitsaspekt managen, steuern, kontrollieren und optimieren. Aus Band G Lektüre dieser Einführung, dem Kapitel 3 "IT-Steuerung/HV-Analyse", Mitwirkung an der Anforderungsanalyse (Phase S), Orientierung an den in Kapitel 7 beschriebenen HV-Prinzipien und Abarbeiten der für den Service relevanten Bausteine zur Realisierung hoher Verfügbarkeit unter Orientierung an den Anforderungskriterien in den Ausführungen zur „Meta-Ebene" aus Kapitel 1, Band B dieses Kompendiums. Für die Überwachung der Service-Qualität wird das Vorgehen nach dem Kapitel 2 "Assessment/Benchmark" des Bnades AH empfohlen.
- Selektion "**IT-Steuerung**" beschreibt wesentliche Elemente der Qualitätssicherung für die IT-Steuerung und das IT- Service-Management als wesentliche Voraussetzung für die Umsetzung von IT-Governance. Die Grundlagen hierzu sind in Band G, Kapitel 3 "IT-Steuerung/HV-Analyse" beschrieben, die Beschreibung der Steuerungsinstrumente sind unter

Band 3 Kapitel 5 "Phase I" sowie in Band AH, Kapitel 2 "Assessment/Benchmark" zu finden.

Mit diesen Selektionen bietet das HV-Kompendium die Möglichkeit eines skalierbaren Einstiegs in einen kontinuierlichen Verbesserungsprozess, der den Weg in ein professionelles IT-Service Management eröffnet. Über die Potentialbewertung begleitet dieses Kompendium Organisationen in der Entwicklung einer IT-Steuerung, die nicht nur Optimierungspotentiale identifiziert, sondern IT-Services in einen kontinuierlichen Verbesserungsprozess (Continuos Service Improvement) überführt. Damit liefert dieses Kompendium Instrumente für den Einstieg in die IT-Governance (GRC[16]) und gleichfalls Anregungen und Empfehlungen für das professionelle IT-Service Management. Die mit diesem Kompendium eingeführten Instrumente zur Bewertung und Steuerung sind damit nicht nur für den Überblick auf der Leitungsebene geeignet, sondern insbesondere für die ständige Nutzung durch die jeweiligen Service-Manager gedacht.

Die Einführung von Mechanismen für die Steuerung und Kontrolle von Prozessen und Services ist keine Angelegenheit, die den IT-Bereich alleine betrifft. Der ganzheitliche Ansatz, eine prozessorientierte Betrachtung sowie eine Kultur der kontinuierlichen Verbesserung erfordern Sichtweisen von Kunden, Aufgabenverantwortlichen, IT-Verantwortlichen sowie der Leitungsebene; damit ist nur eine Teilmenge(Enabler) jener Voraussetzungen nach CobiT genannt . Jeder dieser Sichtweisen ist mindestens ein Verantwortlicher in den Projekten zur Optimierung der Leistungserbringung zuzuordnen, die nicht nur ihre Sichtweise vertreten, sondern dafür Sorge tragen, dass sich in der gesamten Organisation und an ihren Schnittstellen diese Kultur entwickeln und nachhaltig wirksam werden kann. Diesen vielfältigen Sichtweisen trägt die Orientierung an dem CAF-Modell Rechnung.

16 Governace, Risk, Compliance

4 Aufbau des Kompendiums

In der Version 1.6 liegt das HV-Kompendium als vierbändiges Werk vor. Die einzelnen Bände des HV-Kompendiums werden folgend mit ihrer Gliederung dargestellt und ihr Inhalt kurz beschrieben.

4.1 Grundlagen

Band 1 („G: Grundlagen“) Einführung und methodische Grundlagen

Die Einführung beschreibt die Zielsetzung des HV-Kompendiums und ordnet das Vorgehen in vorliegende Standards ein. Für einzelne Zielgruppen wird ein Tayloring vorgenommen welches einzelne Modulen der jeweiligen Zielgruppe zuordnet. Ergänzend erfolgt eine Einordnung des beschriebenen Vorgehens in die vorliegenden relevanten Standards. Im Kapitel ″IT-Steuerung" werden die Instrumente für die Potentialbewertung und die Steuerungsinstrumente für die IT-Steuerung und Optimierung der IT-Services vorgestellt. Für das Vorgehen wird ein Phasen-Modell eingeführt, welches den Einstieg über die Feststellung der strategischen Ziele vorsieht und sodann aus Sicht der Geschäftsprozesse die Anforderungen im Soll ermittelt (Phase S). Nicht zuletzt wird mit dem Service-Modell des BSI die Grundlage für Design und Bereitstellung von hochverfügbaren IT-Services geschaffen.

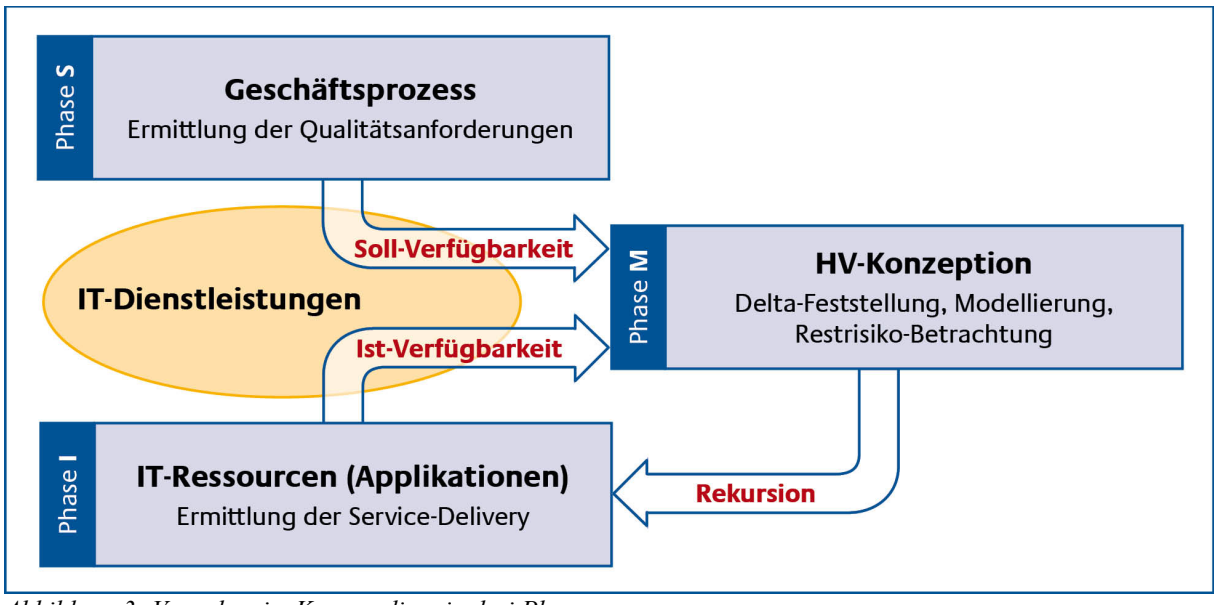


Abbildung 3: Vorgehen im Kompendium in drei Phasen

Die nachstehende Tabelle beschreibt die im **„Band G“** enthaltenen Kapitel:

Kapitel	*Kapitelbezeichnung*
Band G Kapitel 1	Einführung
Band G Kapitel 2	Definition
Band G Kapitel 3	IT-Steuerung (HV-Analyse)
Band G Kapitel 4	Phase S
Band G Kapitel 5	Phase I
Band G Kapitel 6	Phase M
Band G Kapitel 7	HV-Prinzipien
Band G Kapitel 8	Service-Modell

Tabelle 1: Kapitel des ersten Bandes "G: Grundlagen"

4.2 Bausteinstruktur

Band 2 („B: Bausteine“) Bausteine für die nachhaltige und kontinuierliche Service-Bereitstellung

Im Rahmen der Phase M erfolgt eine Modellierung von HV-Umgebungen anhand der HV-Bausteine aus Modellierungsschichten. Band 2 stellt die Bausteine der einzelnen Modellierungsschichten vor. Mit der Auswahl einzelner Bausteine werden Objekte mit spezifischen HV-Eigenschaften zu HV-Architekturen und hochverfügbaren IT-Dienstleistungen komponiert. Dabei erben die Objekte der inneren Schichten die Eigenschaften aus übergeordneten Schichten. Über die Schichten hinweg werden Hierarchien mit steigender Komplexität der Objekte aufgebaut, die letztlich auf einer Meta-Ebene Design- oder Architekturprinzipien realisieren, die eine besonders fördernde Wirkung im Hinblick auf die Verfügbarkeit besitzen.

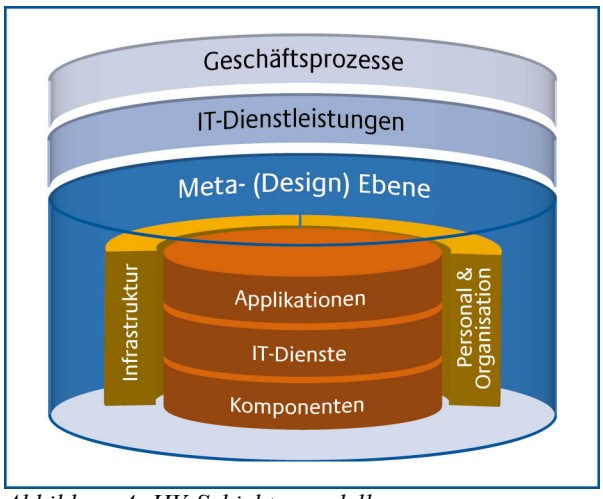


Abbildung 4: HV-Schichtenmodell

Band "B" repräsentiert den Bausteinkatalog und stellt Modelle für eine Modellierung zur Verfügung. Während in den unteren HV-Klassen die vorgeschlagenen Modelle als Standard-Lösung für eine Verfügbarkeitsoptimierung direkt übernommen werden können, wird man spätestens mit der Gewährleistung sehr hoher Verfügbarkeitsanforderungen auf einen

iterativen kontinuierlichen Verbesserungsprozess nicht verzichten können, der sich sinnvoll mit einem professionellen IT-Service Management und Continual Service Improvement der Rahmenwerke ergänzt.

Die nachstehende Tabelle beschreibt die im **„Band B“** enthaltenen Kapitel:

Nummerierung	*Kapitelbezeichnung*
Band B Kapitel 1	Meta-Ebene
Band B Kapitel 2	IT-Organisation
Band B Kapitel 3	Netzwerk
Band B Kapitel 4	Cluster
Band B Kapitel 5	Server
Band B Kapitel 6	Speicher
Band B Kapitel 7	IT-Dienste
Band B Kapitel 8	Datenbanken
Band B Kapitel 9	Software
Band B Kapitel 10	Überwachung
Band B Kapitel 11	Infrastruktur

Tabelle 2: Kapitel des zweiten Bandes "B: Bausteine"

4.3 Maßnahmenkatalog

Band 3 („M: Maßnahmen“) Maßnahmenkataloge zur Realisierung nachhaltiger und kontinuierlicher Services

Zur Realisierung und Optimierung von IT-Architekturen mit Anforderungen an die Hochverfügbarkeit stellt das HV-Kompendium Maßnahmenkataloge zur Verfügung, in denen Maßnahmen und Konzepte in konzentrierter Form dargestellt sind. Die Maßnahmen in den Katalogen leiten sich aus den einzelnen Kapiteln des Bandes B ab. Sie stellen die Anwendung der grundlegenden HV-Prinzipien auf die Modellierungsschichten sicher.

Die nachstehende Tabelle beschreibt die im **„Band M“** enthaltenen Kapitel:

Nummerierung	*Kapitelbezeichnung*
Band M, Kapitel VM 1	Meta-Ebene
Band M, Kapitel VM 2	IT-Organisation
Band M, Kapitel VM 3	Netzwerk
Band M, Kapitel VM 4	Cluster
Band M, Kapitel VM 5	Server
Band M, Kapitel VM 6	Speicher
Band M, Kapitel VM 7	IT-Dienste
Band M, Kapitel VM 8	Datenbanken
Band M, Kapitel VM 9	Software
Band M, Kapitel VM 10	Überwachung
Band M, Kapitel VM 11	Infrastruktur

Tabelle 3: Kapitel des dritten Bandes "M: Maßnahmen"

4.4 Architekturmodelle und Hilfsmittel

Band 4 („AH: Architekturmodelle und Hilfsmittel“) Architekturmodelle Steuerungsinstrumente und weitere Hilfsmittel

Zentrale Inhalte des vierten **Bandes "AH"** stellen die Architekturmodelle und für die Verfügbarkeitsoptimierung präzisierten Steuerungsinstrumente dar. HV-Architekturmodelle stellen Referenzarchitekturen für scalierte Verfügbarkeitsanforderungen zur Verfügung. Sie orchestrieren Ressourcen in Komponenten-Modellen unter Integration geeigneter Prozessmodelle zu hochverfügbaren IT-Services. Der Band AH stellt weitere zielführende Hilfsmittel zur Verfügung.

Die nachstehende Tabelle beschreibt die im **„Band AH“** enthaltenen Kapitel:

Nummerierung	*Kapitelbezeichnung*
Band AH Kapitel 1	Architekturmodelle
Band AH Kapitel 2	Assessment/Benchmarking
Band AH Kapitel 3	Muster, Beispiele, Formulare, Datenblätter
Band AH Kapitel 4	Tools
Band AH Kapitel 5	Abkürzungsverzeichnis
Band AH Kapitel 6	Glossar
Band AH Kapitel 7	Literaturverzeichnis

Tabelle 4: Kapitel des vierten Bandes "AH: Architekturen und Hilfsmittel

5 Messen und Bewerten

IT-Governance führt für die Steuerung der IT messbare Ziele ein, die sich im IT-Service Management als zentraler Ansatz für das Steuern von IT-Services wiederfinden. Zur Bewertung der Verfügbarkeit führt dieses HV-Kompendium Kriterien ein, die mit den Verfügbarkeitszielen Verlässlichkeit und Nachhaltigkeit korrelieren, und benutzt Instrumente, wie sie in den generischen Prozessmodellen als standardisierte Lösung vorgeschlagen werden. Es liefert damit die Grundlage für den Einstieg in ein professionelles IT-Service-Management und bereitet den Weg für eine umfassende IT-Steuerung.

Risikomanagement macht Messen und Bewerten erforderlich, um

- einen Status quo beurteilen und dokumentieren zu können,
- Abweichungen von einem Zielwert rechtzeitig erkennen zu können,
- Entscheidungshilfen für die Priorisierung von Handlungsbedarfen liefern zu können und
- Prognosen treffen zu können.

Messen und Bewerten erfordert damit drei Blickrichtungen, um zu den o.a. Aussagen gelangen zu können, den Blick in die Vergangenheit, den Blick auf den Status quo und den Blick in die Zukunft.

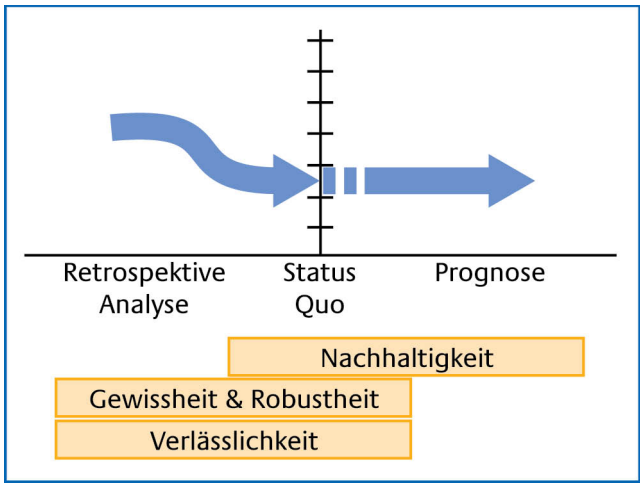


Abbildung 5: Messen und Bewerten auf der Zeitachse

Wird ein Service geliefert, so sind für dessen Vergütung der Nutzen für den Kunden (im Sinne von Nutzbarkeit) sowie die Beurteilung der Service-Qualität ausschlaggebende Merkmale. Nur wenn die gelieferte Qualität den vereinbarten Qualitätskriterien entspricht, wird ein Kunde bereit sein, die geforderte Gegenleistung zu erbringen. Um die Verlässlichkeit eines Service zu beurteilen, sind daher Kriterien zu definieren und ständig zu überwachen, damit Abweichungen frühzeitig erkannt und gegengesteuert werden kann. Wir stehen damit an der Schwelle zur Einführung eines professionellen Service-Management. Im Rahmen des Vorgehens nach diesem Kompendium werden Kriterien und Potentiale identifiziert und bewertet, die sich auf Verlässlichkeit und Nachhaltigkeit und damit besonders auf die Verfügbarkeit auswirken.

5.1 Retrospektive Analyse

Der klassische Ansatz zur Bewertung der Verfügbarkeit liegt in der Betrachtung von Verfügbarkeits- bzw. Ausfallzeiten in der Vergangenheit. Rückblickend werden Zeiten der Verfügbarkeit bzw. Nichtverfügbarkeit dokumentiert und als Ergebnis des Service-Delivery dargelegt. Ergänzend dazu sind Verfügbarkeitsklassen festgelegt worden, denen Aussagen im Hinblick auf Ausfallzeiten zugeordnet wurden. Mit Blick auf die Erfahrungen aus der Vergangenheit werden Systeme und Komponenten in ein derartiges Schema eingeordnet. Es wird auch dazu verwendet, Systeme einzuordnen, für die statistische Aussagen bezüglich mittlerer Verfügbarkeitsdauer (MTBF) oder Ausfalldauer (MTTR) im eigenen Betrieb nicht vorliegen. Aus Sicht der Geschäftsprozesse werden häufig deren Anforderungen an einem derartigen Klassifikationsschema (siehe Tabelle 5: Typische Verfügbarkeitsklassen und ihre Ausfallzeiten) abgebildet, da es zumindest für Ausfallzeiten Anhaltspunkte liefert.

Verfügbarkeitsklasse	***Bezeichnung***	***Minimale Verfügbarkeit***	***Nichtverfügbarkeit***	***Ausfallzeit pro Monat***	***Ausfallzeit pro Jahr***
VK 0	Standard-IT-System ohne Anforderungen an die Verfügbarkeit	~95%	~5%	1 Tag	Mehrere Tage
VK 1	Standard-Sicherheit nach IT-Grundschutz bei normalem Verfügbarkeitsbedarf	99,0%	1%	< 8 h	< 88 h
VK 2	Standard-Sicherheit nach IT-Grundschutz bei erhöhtem Verfügbarkeitsbedarf	99,9%	0,1%	< 44 min	< 9 h
VK 3	Hochverfügbar nach IT-Grundschutz für spezifische IT-Ressourcen; BSI-Standard 100-3	99,99%	0,01%	< 5 min	< 53 min
VK 4	Höchstverfügbar	99,999%	0,001%	< 26 s	< 6 min
VK 5	Desaster-Tolerant	max. Verfügbarkeit	0	0	0

Tabelle 5: Typische Verfügbarkeitsklassen und ihre Ausfallzeiten

Aus der Zuordnung der Anforderungen zu den Verfügbarkeitsklassen lassen sich Anempfehlungen für den verlässlichen IT-Einsatz ableiten, die bis zur Verfügbarkeitskalsse 2 aus den IT-Grundschutzkatalogen abgeleitet werden können. Ab der Verfügbarkeitsklasse 3 reicht eine Realisierung nach IT-Grundschutz alleine nicht mehr aus. Die ergänzende Risikoanalyse nach BSI-Standard 100-3 kann auf der Basis dieses Kompendiums erfolgen, für die Umsetzung sind die Maßnahmenempfehlungen dieses HV-Kompendiums heranzuziehen. Bei den Verfügbarkeitsklassen 3, 4 und 5 kommen damit verstärkt solche Maßnahmen zum Einsatz, die in diesem Kompendium beschrieben werden. Sie sind auf Erhöhung von Redundanz, Fehlertoleranz bzw. Robustheit ausgreichtet und fördern damit die Verlässlichkeit von Services.

Nachhaltigkeit fordert die Gewähr, dass Selbstheilungsmechanismen und Redundanzen hinreichende Robustheit gewährleisten können. Dies kann erst durch Integration von Bewertungs- und Steuerungsmechanisamen in einen kontinuierlichen Verbesserungsprozess erreicht werden. Zumindest die Verfügbarkeitsklassen 4 und 5 erfordern damit weitergehende Kriterien zur Indikation der Verfügbarkeit und Gewährleistung der Nachhaltigkeit.

5.2 Prognosen für eine verlässliche Service-Erbringung

IT-Governance richtet Riskoanalysen und Risikomanagement auf Kontinuität und Nachhaltigkeit aus und braucht dazu verlässliche Prognosen auf der Basis validierter Prozesse. Für eine fundierte Risikoanalyse ist der transparente Nachweis erforderlich, dass die servicetragenden Ressourcen und Prozesse mit einer hohen Verlässlichkeit auch künftig in der Lage sind, notwendige Dienstleistungen zeitgerecht in der geforderten Qualität zur Verfügung zu stellen. Dabei beschreibt Verlässlichkeit ein hohes Maß an Robustheit verbunden mit der Gewissheit, dass die erwarteten Ergebnisse bei der Service-Erbringung auch im Hinblick auf ihre Qualität eintreten. Ist dieses hohe Maß an Robustheit und Gewissheit nicht gegeben, so steigen die Risiken für Ausfälle oder Qualitätseinbußen der erwarteten Dienstleistungen. Sind von diesen Dienstleistungen kritische Geschäftsprozesse abhängig, so muss dieses hohe Maß an Robustheit und Gewissheit hergestellt werden, damit lediglich ein tragbares Maß an Restrisiken bestehen bleibt. Dieses HV-Kompendium beschreibt dazu Potentiale die als Kritierien zur Indikation herangezogen werden: Verfügbarkeits-Potentiale, Organisations-Potentiale, Architektur-Potentiale und Optimierungspotentiale.

Ein Instrumentarium, mit dem Potentiale bewertet werden können, stellen Reifegradmodelle dar, wie sie mit generischen Prozessmodellen (CMMI, Spice) zur Verfügung gestellt werden.

5.2.1 Prognosen für Prozess-Potentiale

Die o.a. Reifegradmodelle beschreiben zunächst die Potentiale organisatorischer Prozesse über Entwicklungsstadien von Aktivitäten zur Steuerung und Kontrolle der Prozesse. Der aktuelle Zustand eines konkreten Prozesses wird unter Nutzung spezifischer Attribute der Reife in einem Reifegrad dokumentiert. Über diese Attribute werden Anforderungen an einzelne Prozesse beschrieben, die hinsichtlich Management und Steuerung auf Entwicklungsstufen abstellen. Bei der Skalierung wird dabei davon ausgegangen, dass sich Prozesse von einer initialen Ausgangslage zu einem optimierten Potential entwickeln. Durch die Auswahl geeigneter Attribute lassen sich IT-Prozesse damit hinsichtlich ihres Potentials beschreiben. Bezüglich der Ausprägung des Potentials zur Bestimmung der Reife von Prozessen definiert dieses Kompendium Attribute der Reife, die an den Kriterien der Verfügbarkeit ausgerichtet sind, wozu z.B. Robustheit und Transparenz gehören. Die Definition von unterstützenden IT-Prozessen, deren Zielsetzung und die Bewertung über Attribute ist Voraussetzung dazu, um auf den höheren Reifegradstufen die Steuerung von Prozessen über Indikatoren leisten und damit managen zu können.

5.2.2 Prognosen für Architektur-Potentiale

Aus dem TOGAF-Ansatz wurde der Grundgedanke übernommen, dass sich Informations-architektur und Technologiearchitektur in die Unternehmensarchitektur zu integrieren und an

gemeinsamen Zielen zu entwickeln haben. Wenn denn Nachhaltigkeit ein gemeinhin akzeptiertes Unternehmensziel ist, muss sich auch eine Informationsarchitektur oder Technologiearchitektur von einer initialen Ausgangslage zu einem optimierten Potential entwickeln. Die Definition von Reifegraden über Technik- bzw. Architekturpotentiale war daher im Rahmen der Entwicklung des Vorgehens für dieses Kompendium die folgerichtige Konsequenz und hebt darauf ab, Technik und Prozesse soweit zu integrieren, dass ein optimiertes Potential erreicht werden kann.

Für die Ermittlung der Architektur (Technik) -Reifegrade werden die in Kapitel G7 „Prinzipien“ dargestellten HV-Prinzipien der Verfügbarkeit um weitere Attribute ergänzt:

- HV-Prinzipien
- Architektureigenschaften
  - Basis Redundanz
  - Robustheit
  - Software-Integration
  - Höhere Stufen (Automatismen&Organisations-Integration)
- Zeitaspekte (z. B. Stillstand, Aktivierungszeit, Zugriffszeit etc.)
- Integration (Technik/Prozess)

Das technische Potential ist ableitbar aus dem Zusammenspiel der eingesetzten Ressourcen über alle Schichten des HV-Schichtenmodells hinweg. Neben den rein technischen Betrachtungsebenen spielen Integrationsaspekte eine entscheidende Rolle. Eine geeignete HV-Architektur integriert nicht nur Software zur Ergänzung von Basis-Technologien, sondern insbesondere Zielvorgaben aus der Organisationsschicht und unterstützt die auf dieser Schicht laufenden Prozesse.

5.2.3 Reifegradmodell zur Bewertung von Verfügbarkeitspotenzialen

In Anlehnung an das generische Reifegradmodell von CMMI wurde zur Bewertung der Qualität von Verfügbarkeitspotenzialen das nachstehende IT-Service Quality Management Maturity Modell eingeführt, welches Prozessreife über fünf Reifegradstufen beschreibt:

Reifegrad-Stufe	*Bezeichnung*	*Beschreibung*
1	Initial (initial)	Der Handlungsbedarf ist den Verantwortlichen bekannt. Es wird situationsbezogen gehandelt bzw. individuell reagiert. Der Service wird „irgendwie“ erbracht, wobei sich das Know-how dazu in den Köpfen Einzelner befindet.
2	Wiederholbar (repeatable)	Die Ausführung der Prozesse hat durch festgelegte Ablauf-Muster ein gewisses Maß an Robustheit erreicht. Eine Zielsetzung ist vorhanden, Konsens wurde jedoch nicht herbeigeführt. Die Ausführung basiert immer noch auf dem Wissen von Einzelpersonen. Durch das festgelegte Ablaufmuster werden Prozesse wiederholbar.
3	Definiert/Standardisiert (defined)	Prozesse sind definiert und orientieren sich an einem Standard, entweder als formales Abbild bestehender Praktiken oder auf der Basis etablierter Standards (z. B. ITIL). Für Prozesse sind Ziele im Konsens entwickelt und operationalisiert. Die Definition erfolgt durch Festlegung von Abläufen und Verantwortlichkeiten und das Wissen dazu ist dokumentiert und wird weitergegeben.
4	Gesteuert (managed)	Für Prozesse ist ein Management eingeführt, welches zur Steuerung der Abläufe auf die operationalisierten Ziele zurückgreift. Die Wirksamkeit der Prozesse wird an bewertbaren Indikatoren gemessen. Der Prozess wird an den Soll-Vorgaben überwacht und in seiner Zielerreichung gesteuert (Soll-/Ist-Vergleich).
5	Optimiert (optimized)	IT-Management und Service Qualität werden ständig verbessert. Die Effektivität des Prozesses wird über Stellgrößen optimiert. Alle Prozesse folgen einem kontinuierlichen Verbesserungsprozess.

Tabelle 6: Reifegradstufen

Der Skalenwert Null wurde absichtlich weggelassen, da dieser Wert einen Zustand beschreibt, in dem die Organisation weder den Bedarf erkannt, noch im Sinne des Qualitätsmanagements zielgerichtet handelt. Aus dem allgemeinen IT-Service Quality Management Maturity Modell wurden spezifischen Bewertungsmodelle für die Bewertung von Architekturpotentialen entwickelt. Die vorgenannten Überlegungen führen zu Reifegradmodellen für die Bewertung von Potentialstufen. Über Attribute der Reife für Prozesse und Architekturen lassen sich Organisationsreife und Prozesspotenziale sowie Architekturpotentiale ableiten:

Reife-grad	*1*	*2*	*3*	*4*	*5*
	Initial	**Wiederholbar**	**Standardisiert /Definiert**	**Gemanagt**	**Optimiert**
Prinzip	*Redundanz*	*Robustheit*	*Skalierbarkeit/ Transparenz*	*Priorisierung Virtualisierung Separation*	*Autonomie*
Prozesse	Prozesse sind ereignis-getrieben und intuitiv	Prozesse folgen einem festgelegten, robusten Muster	Prozesse sind standardisiert, dokumentiert und kommuniziert	Prozesse werden an Zielvorgaben gemessen und überwacht	Prozesse werden kontinuierlich optimiert
Architektur-eigenschaften	Redundanz als Basis-Technologie	Zusammen-wirken von robusten Komponenten (z. B. Durch Software-Integration)	Technik folgt einem Architekturstandard unter Integration organisatorischer Aspekte	Prozess-Integration/ Steuert Technik (Überwachung der Soll-Werte/ Soll-Ist-Vergleich)	Autonome Reaktion unter KVP-Integration
Zeit-aspekt	Stillstand	Manuelle Reaktion	Meldung der Überschreitung Soll-Vorgabe	Automatische Reaktion vor Überschreitung Soll-Vorgabe	Anstoß aller abhängigen Prozesse

Tabelle 7: Prozess/Architektur-Reifegrade

Die Umsetzung und Anwendung des Ansatzes zur Bewertung von Architekturpotentialen erfolgt in diesem Kompendium an den Stellen:

- Kapitel G3 „IT-Steuerung“
- Kapitel G4 „Phase I“
- Kapitel G5 „Phase M“
- Kapitel B1 „Meta-Ebene“
- Kapitel B2 „HV-Organisation“
- Kapitel AH1 „HV-Architekturmodelle“
- Kapitel AH2 „HV-Assessment und Benchmark“

Zur Umsetzung beschreibt diese Kompendium Referenzarchitekturen für häufig auftretende Problemstellungen mit unterschiedlichen Varianten und spezifischen Attributen auf den jeweiligen Potenzialstufen. Sie setzen sich zusammen aus einzelnen Komponenten die alle relevanten Schichten des HV-Schichtenmodells repräsentieren und berücksichtigen technische und organisatorische Prozess-Aspekte der Architekturen. Für die unterschiedlichen Potentialstufen wurden spezifische Attribute der Reife entwickelt, die sich an den Kriterien

der Verfügbarkeit orientieren. Die Referenzarchitekturen können für die Bewertung von existierenden Architekturen im IST verwendet werden, durch Zuordnung der realen Architektur zu einer Potentialstufe auf der Basis von vergleichbaren Attributen. Durch Feststellung der Abweichungen der real existierenden Architektur vom Architekturmodell der ausgewählten bzw. nächsthöheren Potentialstufe lassen sich Optimierungspotentiale identifizieren. Durch Referenzen auf den Maßnahmenkatalog des HV-Kompendiums können die Möglichkeiten der Optimierung konkretisiert werden. Die Kenntnis der Potentiale der eingesetzten Architekturen sind für Risikoanalysen insofern von Bedeutung, als sie Schwächen in der Technik bzw. Organisation offenbaren und ein Maß für die Bewältigung von besonderen Lagen liefern. Unter Berücksichtigung der für die Organisation relevanten Risikoszenarien offenbaren sie Handlungsbedarfe zur Sicherung der Geschäfts- und IT-Kontinuität.

Für das Design von Prozessen und Architekturen können die Architekturmodelle gleichfalls herangezogen werden. Ausgehend von den Anforderungen der primären Geschäftsprozesse kommen jene Architekturen in Betracht, deren Potential der Kritikalität der Anforderungen am ehesten gerecht werden. Welche Architekturen und Prozesse mit welcher Priorität zu realisieren sind, hängt primär von dem Status quo also dem **Risikobewältigungspotential** innerhalb der bestehenden Organisation ab. Die Empfehlungen dieses Kompendiums beziehen sich primär auf die Prozesse, die sich besonders förderlich auf die Erhöhung der Verfügbarkeit auswirken, da die primäre Zielsetzung des HV-Kompendiums die Verfügbarkeitsoptimierung ist und der Status quo vor Ort festzustellen ist. Kritische Geschäftsprozesse begründen regelmäßig hohe Anforderungen an die Performance von IT-Services, sodass hinsichtlich der Unterstützung der Zielerreichung mit dem Empfehlungen der Architekturmodelle Entscheidungshilfen geliefert werden.

6. Zuordnung des HV-Kompendiums zu Grundlagenkonzepten für die Bundesverwaltung

Die nachstehenden Grundlagenwerke gehen von der Betrachtung von Geschäftsprozessen aus Behördensicht aus, die grundlegenden Standards und Strukturen sind jedoch generischer Natur, also auf keinen spezifischen Untersuchungs- oder Branchenbereich fokussiert. Bei den Anwendungsszenarien ist eine sinngemäße Übertragung auf die Sichtweise von Unternehmen nach geeigneter Anpassung der Fragestellungen durchaus möglich. Der IT-Grundschutz des BSI ist ohnehin auf den Einsatz in Wirtschaft und Verwaltung ausgelegt.

Das HV-Kompendium folgt den offenen Architekturstandards, wie sie mit TOGAF oder SOA definiert und in SAGA zusammenfassend dargestellt sind. Diese Standards unterstützen Mehrschichtarchitekturen und eine strukturierte Entwicklung sowie Umsetzung der Architekturen. Den Anforderungen an eine offene Architektur trägt der modularer Aufbau Rechnung, der eine Anpassung auf projekt- und zielgruppenspezifische Bedürfnisse (Tayloring) ermöglicht. Als offenes Grundlagenwerk des BSI wird dieses ständig insbesondere in den Bereichen HV-Maßnahmen und Architekturmodelle fortgeschrieben. Die Orientierung an den IT-Governance-Prinzipien bilden die Basis für die Definition von IT-Services und Prozessen und deren Optimierung. Insbesondere Anforderungen an Skalierbarkeit, Performance, Fehlertoleranz und Wartbarkeit sind Kriterien für Verlässlichkeit und Nachhaltigkeit und damit Teilaspekte der Verfügbarkeit. Verlässlichkeit und Nachhaltigkeit spiegeln sich in fundamentalen HV-Prinzipien und gelten als durchgängige Ziele für die strategische Ausrichtung der Geschäftsprozesse und der IT. Die Grundprinzipien offener Architekturmodelle sind damit für die Realisierung hochverfügbarer Lösungen übertragbar. Unter dem Aspekt IT-Governance beschreibt das HV-Kompendium geeignete Steuerungsinstrumente für die IT-Steuerung und die Steuerung einzelner IT-Services.

6.1 BSI-Standards → IT-Grundschutz

Während Vertraulichkeits- und Integritätsaspekte in dem vorliegenden BSI-Standard 100-2 sowie den ergänzenden IT-Grundschutzkatalogen hinreichend Berücksichtigung finden, konzentriert sich die Sichtweise im Rahmen dieses Kompendiums auf Verfügbarkeitsaspekte. Grundlage für die IT-Sicherheitskonzeption ist das Vorgehen nach IT-Grundschutz und die Orientierung an den BSI-Standards 100-1 und 100-2 [BSI11]. Damit wird eine für normale Verfügbarkeitsanforderungen ausreichende Basis geschaffen. Die Maßnahmen des IT-Grundschutzes bilden damit gleichzeitig Grundlage und Voraussetzung für die Realisierung hochverfügbarer IT-Umgebungen.

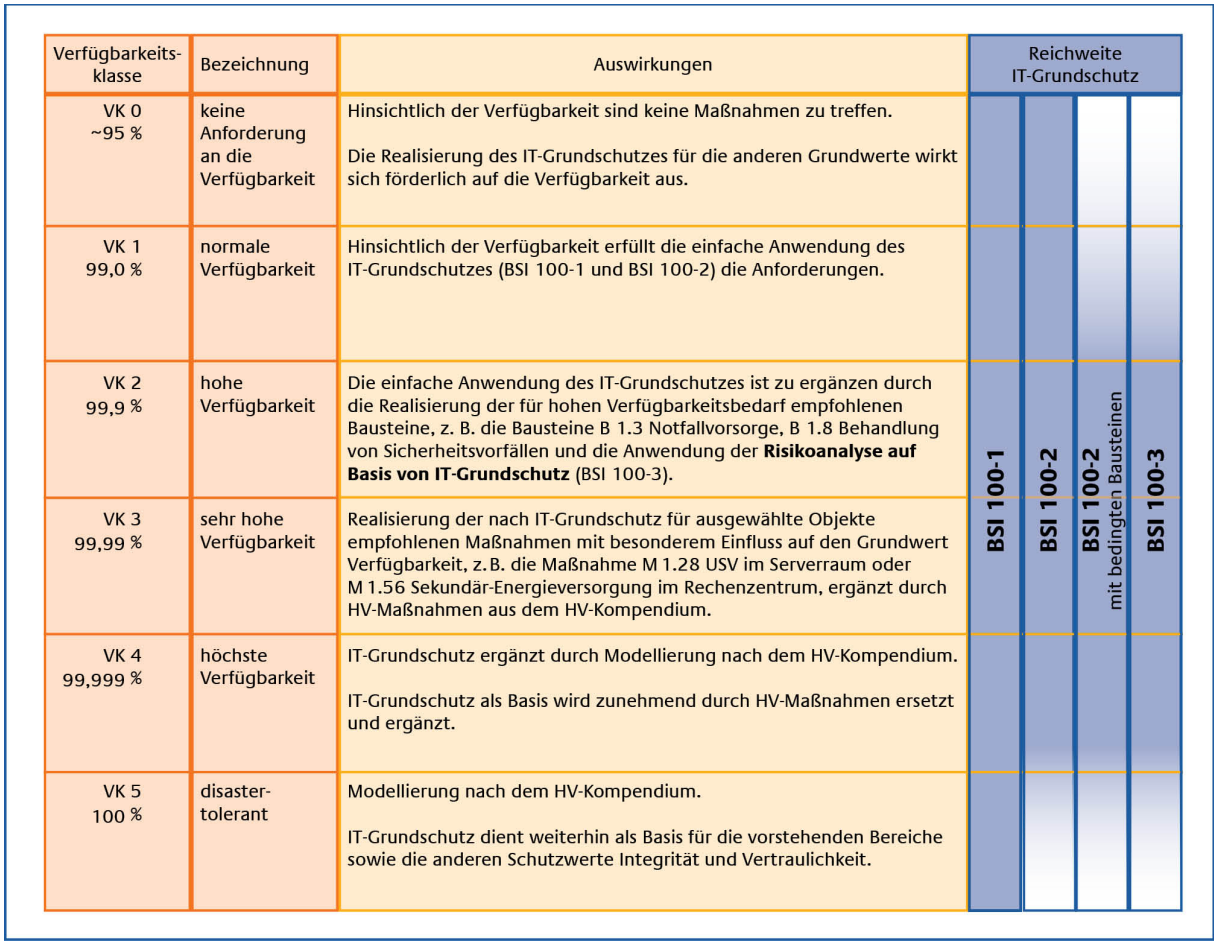


Abbildung 6: Verfügbarkeitsklassen und Reichweite des IT-Grundschutzes

Mit der Schutzbedarfsfeststellung nach IT-Grundschutz wird festgestellt, welches Vorgehen zur Abdeckung des Schutzbedarfes angebracht ist. Aus der Zuordnung der Anforderungen zu den Verfügbarkeitsklassen lassen sich Anempfehlungen für den verlässlichen IT-Einsatz ableiten. Bei den Schutzbedarfskategorien hoch und sehr hoch im Hinblick auf Verfügbarkeitsanforderungen kommt dieses HV-Kompendium zum Einsatz. Für das weitere Vorgehen gelten die nachstehenden Regeln:

- Die Verfügbarkeitsklasse 0 bedarf keiner besonderen Maßnahmen zur Gewährleistung der Verfügbarkeit, ein ordnungsmäßiger Geschäftsbetrieb wird durch Ausfälle nur unwesentlich beeinträchtigt.
- Die Verfügbarkeitsklasse 1 wird bei normalem Schutzbedarf im Rahmen der Modellierung des IT-Verbundes nach IT-Grundschutz erreicht durch Modellierung des IT-Verbundes und Realisierung der empfohlenen Maßnahmen.
- Die Verfügbarkeitsklasse 2 wird bei einem erhöhten Schutzbedarf einzelner IT-Systeme im Bereich der Verfügbarkeit erreicht durch Realisierung der nach IT-Grundschutz für hohen Verfügbarkeitsbedarf empfohlenen Bausteine.
- Die Verfügbarkeitsklasse 3 wird erreicht durch Realisierung der nach IT-Grundschutz für jene IT-Komponenten mit wesentlichem Einfluss auf den Grundwert Verfügbarkeit

empfohlenen Maßnahmenkataloge[17]. Für die ergänzende Risikoanalyse nach BSI-Standard 100-3 ist dieses Kompendiums als Basis heranzuziehen. Es liefert gleichzeitig die Maßnahme-Empfehlungen für den hohen Schutzbedarf kritischer Geschäftsprozesse.

- Bei den Verfügbarkeitsklassen 3, 4 und 5 müssen verstärkt solche Maßnahmen zum Einsatz kommen, die in diesem Kompendium nachstehend beschrieben werden. Sie sind gezielt auf Fehlertoleranz und Robustheit ausgerichtet. Ab der Verfügbarkeitsklasse 4 muss für kritische Geschäftsprozesse ein Notfallmanagement nach BSI-Standard 100-4 auf der Basis dieses Kompendiums erfolgen.

6.2 Standards und Architekturen für die Bundesverwaltung[18]

Im Rahmen des Designprozesses (Phase M) werden nachhaltige und verlässliche HV-Umgebungen entwickelt. Diese orientieren sich grundsätzlich an der IT-Strategie des Bundes und den Empfehlungen für eine IT-Gesamtarchitektur des Bundes, wie sie in den Standards und Architekturen für E-Government-Anwendungen (SAGA) für die Bundesverwaltung [SAGA11] beschrieben werden. Aus den dort genannten Anforderungskriterien, welche die Interoperabilität und Skalierbarkeit der verschiedenen IT-Systeme und die Wiederverwendbarkeit ihrer Dienste und Komponenten sichern, stehen insbesondere jene Prinzipien im Fokus der hier anzustellenden Betrachtungen, welche hoch mit dem Verfügbarkeitsaspekt korrelieren. Vor diesem Hintergrund besitzen primär jene Anforderungen Relevanz, die sich auf Fähigkeiten beziehen, mit denen Dienste oder Ressourcen bedarfs- und zeitgerecht zur Verfügung gestellt werden. Aus diesem Grunde werden die Anforderungskriterien des Architekturkonzeptes aus Sicht des Grundwertes Verfügbarkeit priorisiert und im Architektur-Design wie folgt berücksichtigt:

- Verfügbarkeit (1)
- Performanz (1)
- Wartbarkeit (1)
- Sicherheit (1)
- Skalierbarkeit (2)
- Offenheit (2)
- Interoperabilität (3)
- Flexibilität (3)
- Erweiterbarkeit (3)
- Wiederverwendbarkeit (3)

Die ermittelten Anforderungen aus Sicht von Geschäftsprozessen (Phase S), führen im Architektur-Design einer HV-Lösung zu einer am Verfügbarkeitsbedarf angepassten Service- und Betriebsinfrastruktur. Im Rahmen der Modellierung (Phase M) wird ein angemessener Ausgleich zwischen Verfügbarkeits-SOLL und -IST angestrebt, sodass im Phasenabschluss

17 z. B. M 1.28 USV im Serverraum od. M1.56 Sekundär-Energieversorgung eines RZ, B 2.9 Rechenzentrum

18 http://www.cio.bund.de/DE/Standards/standards_node.html;jsessionid=D411DDA532E10FEF534CFF62323B340F.2_cid155

ein verfügbarkeitsoptimierter Architekturentwurf auf der Ebene der Grobkonzeption vorliegt. Dieser ist in weiteren Projektphasen in die Feinkonzeption für das IT-Design zu überführen. Im Rahmen der Feinkonzeption werden ausgehend von der vorgegebenen IT-Strategie und Geschäftsarchitektur unter Beibehaltung der grundlegenden Architekturprinzipien Objektorientierung, Komponentenbasierung und Diensteorientierung flexible Lösungen realisierbar, welche die Interoperabilität und Skalierbarkeit der verschiedenen IT-Systeme und die Wiederverwendbarkeit ihrer Dienste und Komponenten sichern. Anregungen hierzu liefern die HV-Architekturmodelle in Kapitel „AH1“.

Damit gliedert sich das methodische Vorgehen von diesem Kompendium vollständig in die IT-Strategie des Bundes ein, berücksichtigt die Empfehlungen des Architekturkonzeptes und leistet einen entscheidenden Beitrag zur Nachhaltigkeit, Innovationsfähigkeit und zum effizienten und flexiblen Einsatz von Ressourcen.

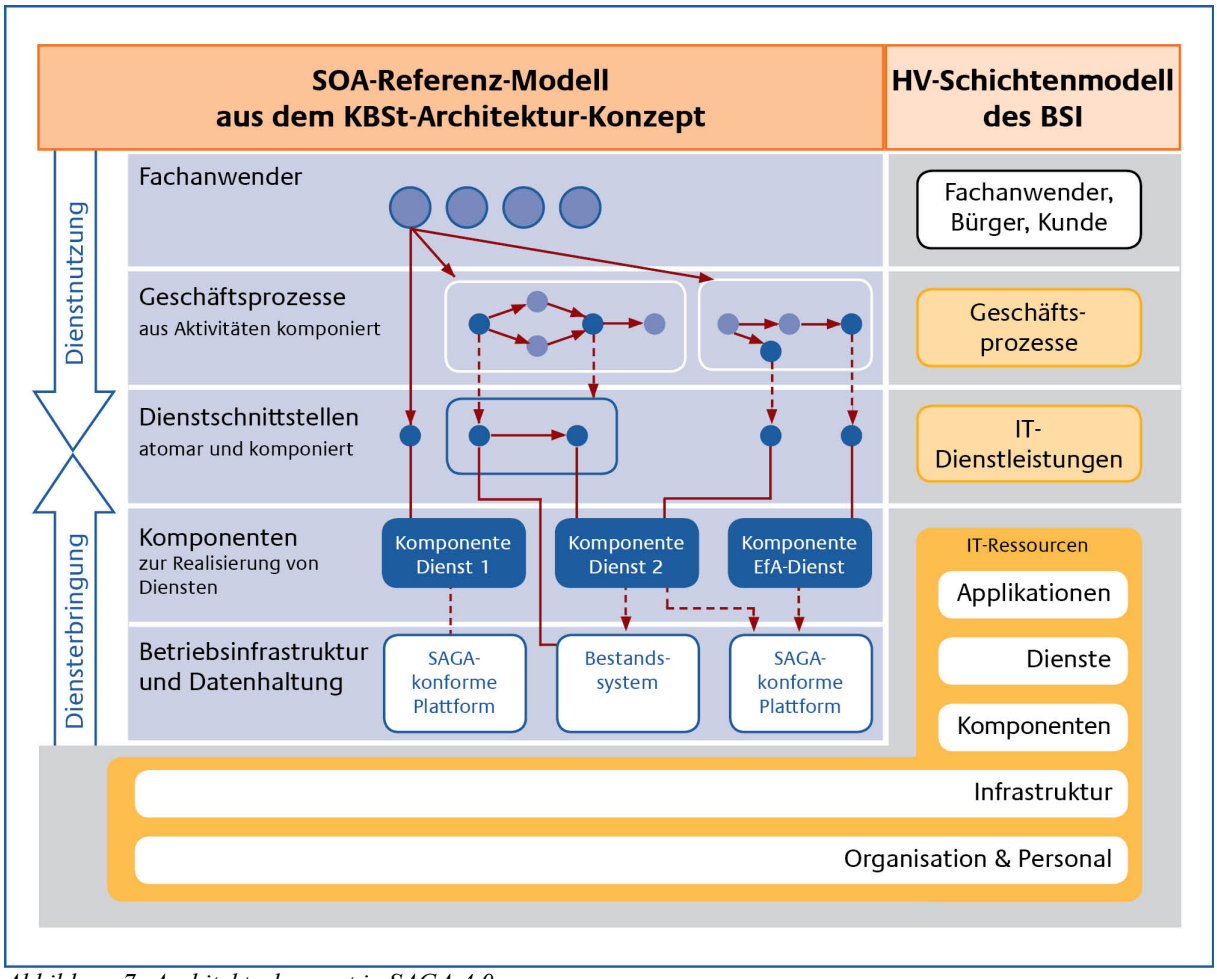


Abbildung 7: Architekturkonzept in SAGA 4.0

Das HV-Kompendium folgt der IT-Strategie des Bundes durch Integration des Architekturkonzepts nach SAGA und ergänzt den methodischen Ansatz zur HV-Analyse durch ein Instrument der IT-Steuerung.

6.3 IT-Methoden[19] und Methoden zur Prozessmodellierung[20]

Geschäftsprozesse werden durchgängig als Ausgangspunkt für Analysen und Modellierungen betrachtet. Um zu geeigneten Aussagen über einen Geschäftsprozess zu kommen, ist die reine IT-Sicht im Einstieg eher ungeeignet. Es wird eine ganzheitliche Betrachtung erforderlich, mit der Abhängigkeiten und Wechselwirkungen zu anderen Geschäftsprozessen und über Organisationsgrenzen hinweg transparent gemacht werden können. Die im Rahmen der Geschäftsprozessanalyse und Modellierung anzustellenden Betrachtungen werden in diesem Kompendium nicht behandelt, sondern es wird dazu auf die Leitfäden der Beauftragten der Bundesregierung für die Informationstechnik verwiesen. Insbesondere der „**Leitfaden für Entwickler von Prozess- und Datenmodellen**“ dieser Quelle wird wegen vorhandener Schnittstellen zur Phase S dieses Kompendiums von Interesse sein. Im Rahmen der Anforderungsanalyse wird ein Datenblattkonzept eingeführt, welches in der Phase S für das Vorgehen der HV-Analyse weiter differenziert wird.

Die kontinuierliche Analyse und Verbesserung der Qualität und Effizienz öffentlicher Leistungserstellung ist Zielsetzung des **Common Assessment Framework** [CAF10], das gemeinsame Qualitätsbewertungsmodell der öffentlichen Verwaltung Europas. CAF liefert Instrumentarien, um die Stärken und Verbesserungspotenziale öffentlicher Services zu erkennen sind und Optimierungspotentiale zu identifizieren. CAF strebt die Einführung von den Prinzipien des Total Quality Management (umfassendes Qualitätsmanagement) in der öffentlichen Verwaltung an und führt den PDCA-Zyklus in der Verwaltungspraxis ein. Prozessorientierung kontinuierliche Verbesserung sind Sichtweisen die aus CAF übernommen werden. Die Ergebnisse aus einer Bewertung mittels CAF-Modell können für die Bewertung von Organisationspotenzialen für die HV-Analyse verwendet werden.

Auf der Basis des Konzeptes "IT-Steuerung Bund" werden für das Architekturmanagement in der Bundesverwaltung neben den o.a. Empfehlungen zu IT-Architekturen auch Empfehlungen für ein aktives Architekturmanagement entwickelt. Dazu gehören Planungsinstrumente für die Fortentwicklung zentral gesteuerter IT-Dienste, sowie Prozesse für Definition, Fortschreibung, Umsetzung und Erfolgskontrolle der IT. Beginnend bei der Geschäftsprozessebene werden Konzepte und Instrumente zur integrierten Steuerung entwickelt, die für das Management aller Bereiche der Organisation anwendbar sind. Assessment und Benchmark sind Instrumente, die gleichfalls in diesem Kompendium zum Einsatz kommen. Der Einsatzbereich dieser Instrumente wurde auf die Anwendung zur Steuerung und Bewertung von IT-Services angepasst und basiert auf der Potentialanalyse und -Bewertung über Reifegradstufen, der auch im CAF-Modell als Ansatz zum Tragen kommt. Details hierzu finden Sie im Kapitel G3 „IT-Steuerung“. Die Schnittstelle zwischen Geschäftsprozessen und IT-Services bildet nach dem IT-Service-Modell des BSI (siehe Kapitel G 8 „ Service-Modell“) auf der obersten Ebene die IT-Dienstleistungen (Business Prozess Services BPS). In dieser Schnittstelle zwischen Geschäftsprozessen und IT-Diensten werden IT-Services angeboten, die die erforderliche Funktionalität in der angeforderten Qualität liefern. In der Schnittstelle treffen sich Anforderungen der Geschäftsprozesse und strategische Ausrichtung der IT-Services. Zielvorgaben und -Kriterien auf der Ebene der IT-Dienstleistung sind Basis für die Service-Steuerung. An dieser Stelle sei auf den „**Leitfaden zur Rahmenarchitektur IT-Steuerung Bund"** verwiesen, der die Ableitung von Diensten

19 http://www.cio.bund.de/DE/IT-Methoden/it-methoden_node.html
20 http://www.cio.bund.de/DE/Standards/Modellierung/modellierung_node.html

aus Geschäftsprozessen beschreibt. Orientiert an einem Zielemodell wird ein geschäftliches Modell entwickelt. Das Zielemodell stellt die Ziel aus geschäftlicher und IT-Sicht strukturiert dar und liefert Indikatoren und Zielwerte für die Steuerung und Kontrolle. Im Rahmen dieses Kompendiums werden Indikatoren und Zielwerte im Hinblick auf die Ziele Verfügbarkeit, Verlässlichkeit und Nachhaltigkeit konkretisiert. Aufgaben und Ziele des geschäftlichen Modells konkretisieren die Nachfrage in funktionalen wie in qualitativen Anforderungen an die IT-Dienstleistungen. Im Dienstemodell werden die nachgefragten Funktionen als Fach-, Querschnitts- oder Basisdienst als inhaltliches Angebot in einem Service-Katalog dargestellt. Das Angebot des Dienstemodells wird auf ein technisches und ein Informations-Modell heruntergebrochen. Auf der Ebene des Dienstemodells treffen sich beide Ansätze. Fach- und Querschnittsdienste werden im HV-Kompendium als IT-Dienstleistung (Business Prozess Services) bezeichnet, weil sie unmittelbar eine funktionale Anforderung eines Geschäftsprozesses erfüllen. Diese Services (vgl.: Kapitel G8 „Service-Modell“) an der Schnittstelle zu den Geschäftsprozessen sind „Business Enabling Services“ oder „Business Prozess Services“ (IT-Dienstleistungen), weil sie Geschäftsprozesse ermöglichen oder unterstützen (Nutzen-Aspekt). IT-Dienstleistungen bilden die abrechnungsrelevante Transferebene zwischen den beiden Betrachtungsebenen „Geschäftsprozess“ und „IT-Ressourcen“, die sich in Service Level Agreements konkretisieren.

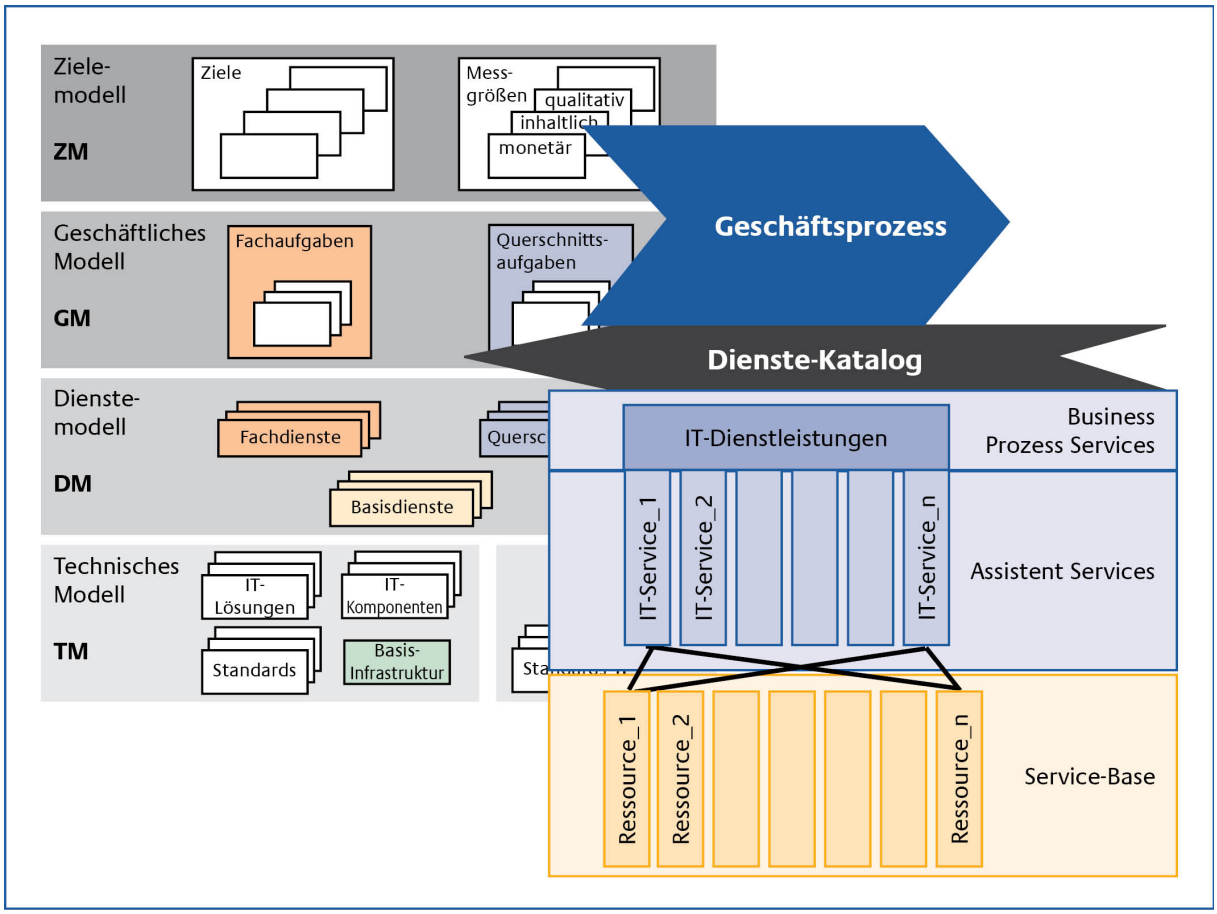


Abbildung 8: Rahmenarchitektur Bund und Service-Architektur BSI

Basis-Dienste sind keine direkten Business Prozess Services sondern unterstützen die IT-Dienstleistungen auf der nächst höheren Ebene. Das HV-Kompendium betrachtet an dieser Stelle weniger systemnahe Services (Basisdienste) wie z.B. den Print-Service, sondern

vielmehr solche unterstützenden Services (Assisstent Services), die im Rahmen Verfügbarkeitssicherung oder der IT-Steuerung (z.B. Service Level Management) notwendigerweise anzubieten, sind. Grundlage der Service-Erbringung sind auf der Ebenen der Service-Base konkrete IT-Lösungen, Komponenten und weitere Ressourcen, die zur Sicherstellung der Verfügbarkeit erforderlich sind (z.B. Personal). Die Schnittstelle zwischen der Geschäftssicht und der IT-Sicht wird durch den **Dienstekatalog** realisiert. Das HV-Kompendium beschreibt dazu das Vorgehen, wie verlässliche Dienste mit hohen Anforderungen an die Verfügbarkeit realisiert und nachhaltig betrieben werden können.

Anhang: Verzeichnisse

Abkürzungen und Akronyme

Ein komplettes Verzeichnis hierzu findet sich im Band AH, Kapitel 5

Glossar

Ein komplettes Verzeichnis hierzu findet sich im Band AH, Kapitel 6

Literaturverzeichnis

Ein komplettes Verzeichnis hierzu findet sich im Band AH, Kapitel 7