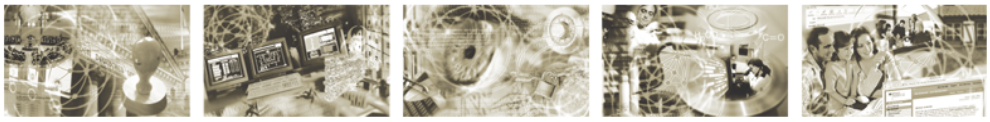
Bundesamt
für Sicherheit in der
Informationstechnik



Band G, Kapitel 6: Phase M (Modellierung)

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

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung Phase M

Die Phase M dient der Modellierung von IT-Services, die ausgerichtet an den Erfordernissen von Geschäftsprozessen bedarfsgerechte Funktionalität und Qualität anbieten. Auf der Basis von HV-Architekturmodellen werden in einem ganzheitlichen methodischen Ansatz qualitativ hochwertige Services zu einer anforderungskonformen IT-Dienstleistung komponiert.

Dabei sind die nachstehenden Eigenschaften tragenden Architekturmerkmale der Architekturmodelle:

- Funktionalität
- Maximierung des Nutzens für die Geschäftsziele
- Konformität
- Beherrschbarkeit der Komplexität
- Kontinuität
- Innovationsfähigkeit und
- Wirtschaftlichkeit

Die Architekturmodelle sollen einen Beitrag zur IT-Steuerung und zum professionellen Service Management liefern, daher werden diese Merkmale abgebildet auf Zielkriterien und messbare Eigenschaften, die sich wie folgt darstellen:

- Funktionalität, Wirtschaftlichkeit und Nutzen der IT
  - in den Zielkriterien: Effektivität und Effizienz
    - gemessen im Rahmen der IT-Steuerung (Kap.4) an den Eigenschaften generisches Ziel (Requirenments Definition), Zielwert (required Prozess Capability), Zielwert Benchmarking, Optimierungspotential
- Konformität als Element Compliance der IT-Governance
  - in den Zielkriterien: Vorgaben, Methoden, Standards
    - gemessen an den Eigenschaften: Prozessorientierung und Prozessreife im Rahmen des HV-Assessments z.B. an der Potentialstufe der IT-Governance;
- Kontinuität als Kontrollziel der IT-Governance
  - in den Zielkriterien: Verlässlichkeit und Nachhaltigkeit
    - gemessen an den Eigenschaften: Organisationspotential als Prozessreife im Continuity Management und Technikpotentiale als Architekturreife
- Beherrschbarkeit der Komplexität
  - in den Zielkriterien: Transparenz, Flexibilität und Robustheit
    - gemessen an den Eigenschaften: hohe Organisationspotentiale als Prozessreife von Service Desk & Incident Management sowie IT-Governance und hohe Technikpotentiale als Architekturreife
- Innovationsfähigkeit
  - in den Zielkriterien: Transparenz, Flexibilität und Robustheit

– gemessen an den Eigenschaften: hohe Organisationspotentiale als Prozessreife und Technikpotentiale als Architekturreife in allen Assessmentbereichen

Mit diesen Eigenschaften und Zielkriterien lassen sich Ziele der IT-Governance auf der Ebene der anzubietenden IT-Dienstleistungen und IT-Services operationalisieren und als Steuerungsgrößen verwenden.

In den vorliegenden Architekturmodellen skaliert die hochwertige Qualität der Eigenschaften z.B. über Verlässlichkeit und Nachhaltigkeit und wird in der konkreten Potentialstufe einer Architektur im Intervall [1;5] bewertet. Die Konformität zu den Anforderungen wird über die in der Phase S ermittelte Kritikalität der Geschäftsprozesse und deren Schutzbedarf hergestellt, die sich in den fünf Stufen der Anforderungsqualität widerspiegeln. Der ganzheitliche methodische Ansatz beschreibt Verfahren für die Analyse der Anforderungsqualität (Phase S) sowie für die Auswahl anforderungskonformer Architekturmodelle. Das Vorgehen leitet sich aus generischen Prozessmodellen der IT-Governance ab und betrachtet technische und organisatorische Architekturpotentiale als Garant für die Zielkonformität der Dienstleistungsarchitektur.

Dieses Kompendium liefert dazu im Band AH für den technischen Bereich Architekturmodelle auf der Basis von auf Verfügbarkeit optimierten Komponenten für die technische Architektursäule und im organisatorischen Bereich Referenzprozessmodelle auf der Basis generischer Prozessmodelle für die organisatorische Architektursäule. Bei den Komponentenmodellen erfolgt die Orchestrierung von Subservices über Ressourcen-Komponenten zu einem technischen IT-Service. Bei den Prozessmodellen stehen organisatorische Abläufe zur Gestaltung und zum Betrieb der IT-Services orientiert an ITIL bzw. CobiT und dem PDCA-Zyklus im Vordergrund. Im Rahmen der Modellierung sind relevante Architekturmodelle auszuwählen, denen jeweils ein Architekturpotential zugeordnet ist. Zielgrößen aus der Phase S bestimmen den empfohlenen Potentialwert des zu wählenden Architekturmodells. Abweichungen der realisierten Architekturen nach unten offenbaren Schwachstellen, die gerade bei kritischen Geschäftsprozessen zu beseitigen sind. Im Rahmen einer vergleichenden Analyse kann eine Verfügbarkeitsoptimierung der IT-Services und die gezielte Ergänzung durch HV-spezifische Maßnahmen erfolgen. Auf der Basis standardisierter aber transparenter Abhängigkeiten sowie der ermittelten Anforderungen erfolgt angesichts der zuvor erhobenen Verfügbarkeits- und Optimierungspotentiale die Analyse weiter bestehender Risiken.

Es fließen daher nicht nur technische Aspekte der IT-Infrastruktur ein, sondern aus einer ganzheitlichen Sicht werden bei der Gestaltung von Architekturen auch personelle und organisatorische Aspekte sowie Umfeldbedingungen berücksichtigt. Der gewählte Ansatz ermöglicht ein anforderungskonformes Service-Design welches neben der Gestaltung von IT-Architekturen auch die Gestaltung von Organisationsstrukturen und –Prozessen auf der Basis einer zuvor durchgeführten Anforderungsanalyse aus Sicht der Geschäftsprozesse zur Ermittlung der Anforderungsqualität umfasst. Das Ergebnis dieses Design-Prozesses wird im Folgenden mit HV-Umgebung bezeichnet und umfasst sieben Schichten des Schichtenmodells nach Abschnitt 2.1.

In der nachstehend beschriebenen Phase M werden unter Verfügbarkeitsaspekt HV-Umgebungen modelliert und gegebenenfalls optimiert. Primäre Zielsetzung ist dabei die Reduzierung bestehender Risiken mit Auswirkung auf den Grundwert Verfügbarkeit und der Vermeidung von Folgeschäden für abhängige Prozesse und damit die Optimierung von Verlässlichkeit und Nachhaltigkeit.

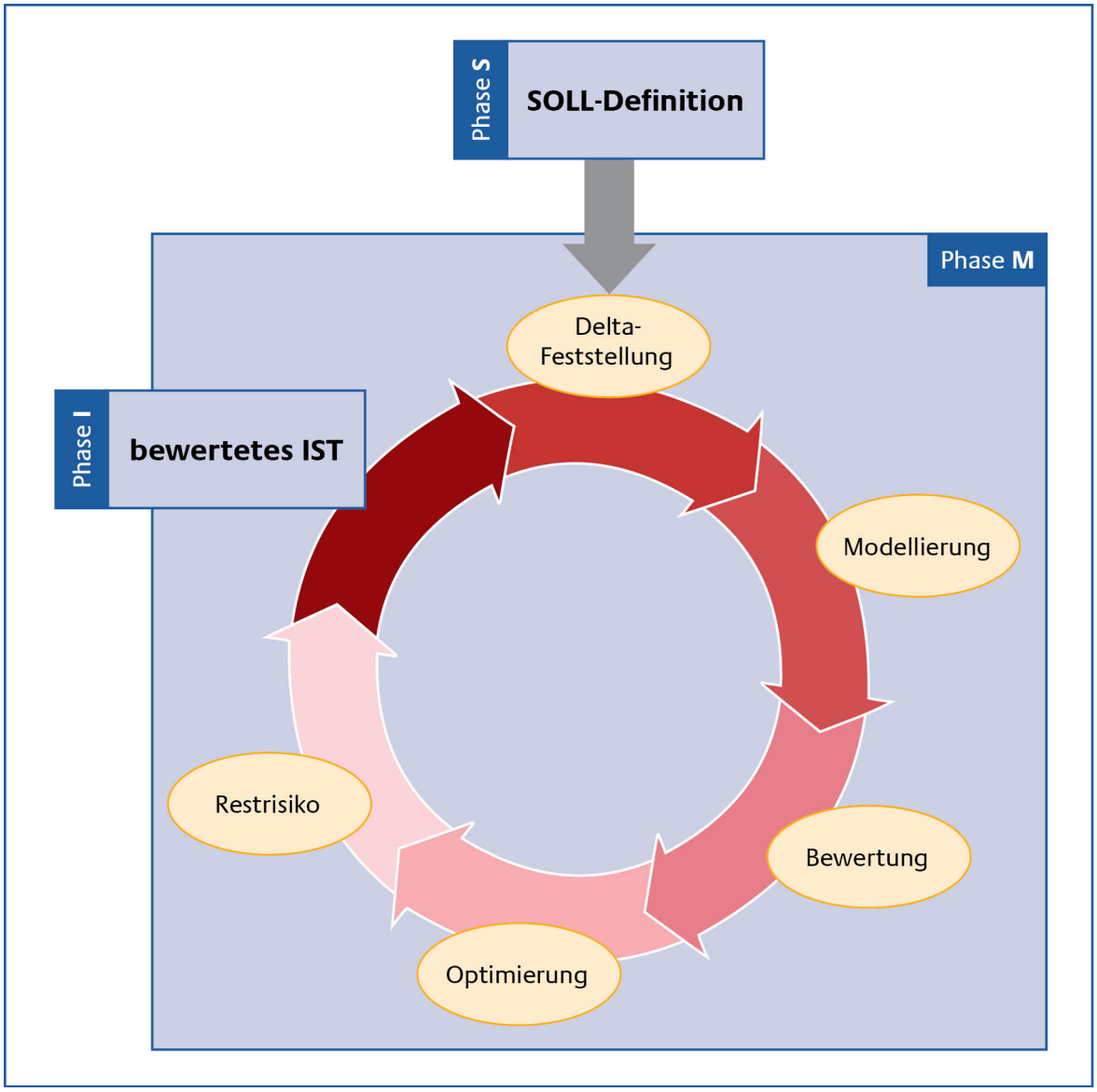


Abbildung 1: Iterativer Prozess in der Phase M

Der Einstieg in die Phase M bildet die Feststellung der Differenz zwischen den Anforderungen im Soll aus Phase S und dem ermittelten Service-Delivery im IST aus Phase I. Mit der Modellierung der HV-Umgebungen durch HV-Bausteine aus sieben Modellierungsschichten wird das Service-Design unter Verfügbarkeitsaspekten beschrieben und das Verfügbarkeits-Delivery über Architekturpotetiale bewertbar gemacht. Die Auswahl der relevanten Bausteine aus den Architekturmodellen sollte sich an den Anforderungen im Soll orientieren. Wird unter diesen Anforderungen geblieben, so verbleiben in der Gesamtarchitektur Restrisiken für den Ausfall des Geschäftsprozesses, die in einem iterativen Prozess, in dem die geforderte Service-Qualität im Hinblick auf den Grundwert Verfügbarkeit optimiert wird, weiter reduziert werden sollten. Die Iteration erfolgt durch Rückkopplung auf den Beitrag 2.3 des Kompendiums „Phase I (Ist-Ermittlung)“, bis das zu erwartende Restrisiko als tragbar erachtet wird.

Voraussetzung für den Einstieg in die Phase M ist das Vorliegen der Qualitäts- und insbesondere der Verfügbarkeitsanforderungen aus Sicht des Geschäftsprozesses als Ergebnis der Phase S. Die Verfügbarkeitsanforderungen im SOLL bilden den Anforderungskatalog für die Phase M. Des Weiteren wird ein vorhandenes oder zu erwartendes Service-Delivery benötigt, um das IST mit dem

Soll vergleichen zu können. Daher ist im weiteren Vorgehen zu unterscheiden, ob eine bestehende HV-Umgebung zu optimieren ist, oder ob sich die HV-Umgebung im Planungsstadium befindet.

- Für eine bestehende HV-Umgebung ist zunächst Phase I zu durchlaufen, um das Service-Delivery im IST zu bestimmen
- Für eine geplante HV-Umgebung wird im ersten Schritt dieser Phase die Modellierung vorgenommen, um zu einem zu erwartenden Service-Delivery zu kommen

Im Ergebnis steht nun für die Bestimmung des Delta

- eine Anforderung zur Verfügung, die das SOLL festlegt und
- ein ermitteltes Service-Delivery zur Verfügung, welches das IST darstellt

Aus beiden Werten kann ein Delta ermittelt werden, um im anschließenden Vergleich festzustellen, in wie weit, die Anforderungen aus der Phase S abgedeckt sind.

2 Phasenziel

Ziel der Phase M ist das Design geeigneter Architekturen zur Gewährleistung geforderter Verfügbarkeiten, um die geforderte Verlässlichkeit und Nachhaltigkeit und damit eine hinreichende Business-Kontinuität zu gewährleisten und eventuelle Schadensereignisse ohne gravierende Beeinträchtigung der Geschäftsprozesse zu überstehen. Sie dient damit dem übergeordneten Ziel der Erhöhung von Verlässlichkeit und Kontinuität durch Reduzierung der bestehenden Risiken und der konzeptionellen Erarbeitung von alternativen Prozesswegen. Im Rahmen der Konzeption von Hochverfügbarkeits-Lösungen soll ein fundierter Ausgleich zwischen dem finanziell Machbaren und den bestehenden Restrisiken herbeigeführt und das zu tolerierende Restrisiko transparent erarbeitet werden. Dieses Restrisiko ist der verantwortlichen Leitungsebene in Organisationen zu kommunizieren und nach Darstellung des Machbaren von diesen zu akzeptieren.

Als generell geeignete Strategie zur Zielereichung wird die Optimierung angesehen, die sich auf Teilstrategien mit jeweils zugehörigen Teilzielen abstützt:

- Beseitigung von SPoFs
- Vermeidung von Ausfallzeiten
- Verkürzung von Down-Times
- Verwendung standardisierter Architekturmodelle
- Reduzierung von Abhängigkeiten
- Konzeption von Alternativen für besondere Lagen
- Auswahl von HV-Maßnahmen, die höherwertige HV-Prinzipien realisieren

Die Teilstrategien stehen gleichberechtigt nebeneinander und bauen aufeinander auf. Das letztlich tragende Prinzip ist vom angestrebten Verfügbarkeitsniveau abhängig und soll bei höchsten Verfügbarkeitsanforderungen oder disastertoleranten Systemen verstärkt die HV-Prinzipien Fehlertoleranz, Automatismen und Autonomie umfassen, wie sie in den höherwertigen Architekturmodellen berücksichtigt sind. Ein Abweichen von diesen Standards ist gerade bei kritischen Geschäftsprozessen mit hohem und sehr hohem Schutzbedarf im Rahmen der Restrisikoanalyse zu betrachten und mit alternativen Maßnahmen zu begründen.

2.1 Modellierung

Die Modellierung einer HV-Umgebung erfolgt durch die Abbildung der für den Geschäftsprozess notwendigen IT-Dienstleistungen in dem HV-Schichtenmodell (siehe Abbildung 3: Modellierung von HV-Umgebungen). Hierbei ist zu beachten, dass die Komponentenschicht verschiedene Objekt-Cluster enthält, wie z.B. Netzwerkkomponenten, Speichersysteme oder auch IT-Domänen z.B. im Sinne von Server-Architekturen.

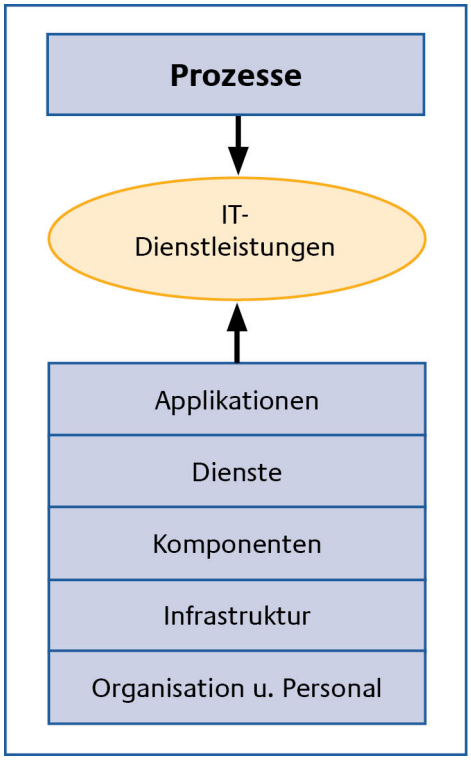


Abbildung 2: HV-Schichten

Auf jeder dieser Schichten bietet das HV-Kompendium Architekturmodelle ergänzt durch Bausteine an, um die Objekte dieser Schicht zu modellieren. Eine konkrete HV-Umgebung besteht aus einer Reihe von physischen und logischen Komponenten, für die im Rahmen der Modellierung geeignete Modelle aus dem Katalog der Architekturmodelle auszuwählen sind. Der Modellkatalog ist eine offene Modellsammlung, weitere Modelle nach den o.a. Zielkriterien zu entwickeln, zu erproben und zu ergänzen sein. Entsprechend der Zielsetzung der Geschäftsprozesse werden im Rahmen der Modellierung in der Meta-Ebene die Anforderungsqualität aus der Phase S und die anforderungskonformen Architekturpotentiale zusammengeführt.

Die Zusammenhänge zwischen den einzelnen Objekten werden von den prozessualen Abhängigkeiten bestimmt. Damit ist für die Modellierung die Frage zu klären, welche Objekte werden benötigt, um den analysierten Geschäftsprozess zu bedienen. Aus dem Schichtenmodell sollte bereits klar werden, dass es übergeordnete und nachgeordnete Abhängigkeiten gibt. So sind Objekte mit übergeordneter Natur solche, die auf praktisch alle anderen Objekte Einfluss haben (z. B. Infrastruktur, Organisation). Objekte mit nachgeordneten Abhängigkeiten müssen in Ihren Bausteinen diese nachrangigen Abhängigkeiten berücksichtigen. In diesem Kompendium werden die nachrangigen Abhängigkeiten in standardisierten Architekturmodellen berücksichtigt, und damit auf generischer Ebene betrachtet. In der Praxis ist daher zu prüfen, inwieweit die standardisierten Abhängigkeiten den tatsächlichen Abhängigkeiten durch die Einbettung der Objekte in den Geschäftsprozess entsprechen.

Bei der Modellierung kommt ein objektorientierter Ansatz zur Anwendung, mit dem (HV-) Eigenschaften an HV-Objekten beschrieben und die auf diese Objekte anzuwendenden Operationen als HV-Maßnahmen dargestellt werden. Die Modellierung erfolgt auf der Grundlage des in Abb. 3 dargestellten Schichtenmodells (siehe unten 1.3.3), wobei die Objekte der inneren Schichten die HV-Eigenschaften der Objekte übergeordneter Schichten erben. Das Vorgehen orientiert sich an der Vorgehensweise des IT-Grundschutzes, die Modellierung erfolgt auf verschiedenen

Abstraktionsschichten unter der Verwendung von HV-Objekten. Die einzelnen Objekte innerhalb der Schichten bilden eine Hierarchie mit steigender Komplexität der Objekte, die sowohl die HV-Eigenschaften der nach- bzw. zugeordneten Objekte erben, als auch um weitere HV-Maßnahmen ergänzt werden können. Grundsätzlich bauen Objekte einer höheren Ebene auf den Eigenschaften bzw. Funktionalitäten eines oder mehrerer Objekte der nachgeordneten Ebene auf. Die Modellierung nach diesem HV-Kompendium erfolgt konkret dadurch, dass für Bausteine jeder Schicht zu entscheiden ist, mit welchen Zusammenhängen ein Baustein auf ein Objekt der HV-Umgebung zutrifft und zur Modellierung der HV-Umgebung herangezogen wird.

Für die Servicemodellierung[1] nach diesem HV-Kompendium wurde eine Synthese aus den Sichtweisen von Komponenten- und Prozessmodellen gebildet.

- in der Prozessschicht, erfolgt die Modellierung aus Sicht notwendiger IT-Prozesse aus den generischen Prozessmodellen der IT-Steuerung angepasst an die Ziele Verlässlichkeit und Nachhaltigkeit. Damit werden auf der mittleren Ebene des Drei -Ebenen-Servicemodell des BSI grundlegende Service-Potentiale geschaffen. Die Prozessschicht spiegelt das Potential des zu modellierenden Services in die Meta-Ebene(s. HV-Kompendium V 1.6 Band B, Kapitel B1“ Meta-Ebene“).
- Die untere Ebene bildet die Komponentenebene, welche die eingesetzten IT-Ressourcen repräsentiert. Hier erfolgt vergleichbar der Modellierung nach IT-Grundschutz, eine Modellierung über die äußeren zu den inneren Schichten.

2.1.1 Modellierung für das Grobkonzept

Für die Gestaltung hochverfügbarer IT-Services werden in diesem Kompendium Modelle und Maßnahmen zur Verfügung gestellt, mit deren Hilfe ein Konzept für Planung, Einsatz und Betrieb von IT-Services auf einen hohen Verfügbarkeitslevel sichergestellt werden kann. Dazu liefert das HV-Kompendium im Band AH eine repräsentative Auswahl standardisierter Architekturmodelle[2]. Diese Architekturmodelle sind auf Verfügbarkeit optimiert, dazu wurden aus den HV-Prinzipien Eigenschaften in den Modellen geschaffen. Aktuell sind dies nachstehende Mechanismen und Prinzipien:

- Toleranz und Transparenz gegenüber Fehlern
- Präventive Build-in-Funktionalitäten
- Proaktives Monitoring und schnelle Fehlererkennung
- Schnelle Wiederherstellungsmechanismen
- Prozessororientierung
- Automatisierte Wiederherstellung ohne administrative Eingriffe
- Kein oder geringer Datenverlust
- Design for Flexibility & Design for Change

Es liegt auf der Hand, dass nicht allein mit einem Modell aus der technischen Architektursäule hohe Verlässlichkeit erreicht werden kann, sondern die Architektur ist immer ganzheitlich zu betrachten, und um die notwendigen Prozesse zu ergänzen, die eine Organisation in einer hochverfügbaren

1 Vgl. dazu Band G, Kapitel 8: "Service-Modell“
2 Vgl. dazu Band AH, Kapitel 2: "HV-Architekturmodelle“

Umgebung prägen. Auch hierzu liegen in der organisatorischen Architektursäule Architekturmodelle vor, die von dem Maßnahmen-Baustein HV-Organisation ergänzt werden.

Für die **Modellierung von HV-Umgebungen** ist zunächst die Stufe der Anforderungsqualität nach Phase S zu ermitteln. Die Stufe der Anforderungsqualität des Geschäftsprozesses gibt den Zielwert für die auszuwählenden Architekturmodelle vor. Sodann werden nach IT-Grundschutz-Vorgehensweise die mit der Strukturanalyse[3] erhobenen Daten bzw. deren Dokumentation (z.B. Netzplan) die wesentlichen Strukturen der bestehenden oder zu schaffenden Architektur ermittelt. Nach IT-Grundschutz sind dies:

1. die im Informationsverbund betriebene Anwendungen und die dadurch gestützten Geschäftsprozesse
2. die organisatorischen und personellen Rahmenbedingungen für den Informationsverbund
3. die im Informationsverbund eingesetzten vernetzten bzw. nicht-vernetzten IT-Systeme
4. die Kommunikationsverbindungen zwischen den IT-Systemen und nach außen
5. die vorhandene Infrastruktur

Die Architekturmodelle aus Band AH, Kapitel 1 liefern die durch das Modell zu erreichende Potentialstufe (siehe Deckblatt „HV-Referenzarchitekturen“). Mit der „Checkliste zur Feststellung der aktuellen Potentialstufe“(siehe Band AH, Kapitel 1, Tabelle 7) und der Zusammenfassung der prägenden Merkmale der beschriebenen Architektur (siehe Band AH, Kapitel 1, Tabelle 9 z.B. Redundanzgrad) kann die Potenzialstufe der in der Praxis vorliegenden Architektur ermittelt werden. Der Architekturkatalog liefert damit die Vorlage für die Auswahl anforderungskonformer Architekturmodelle auf der Basis der dem Zielwert entsprechenden Potenzialstufe.

Für die Modellierung der IT-Dienstleistung in der vorstehend beschriebenen Abhängigkeitsstruktur nach IT-Grundschutz stehen die nachstehenden Architekturmodelle über jeweils fünf Potentialstufen als Module für die Orchestrierung zur Verfügung:

- Für die im Informationsverbund betriebenen Anwendungen die zu orchestrierende Dienstleistung (siehe vor(1)).
- Für die IT-Systeme (siehe vor(3)) die Architekturmodelle Server und Speicher.
- Für die Kommunikationsverbindungen (siehe vor(4)) die Architekturmodelle Netze.
- Für die Infrastruktur (siehe vor(5)) die Architekturmodelle Infrastruktur, Stromversorgung, Klimatisierung,
- Für Personal und Organisation (siehe vor(2)) die Architekturmodelle Monitoring, IT-Operation, Service-Level Management, IT-Operation, Incident Management, IT-Service Continuity Management.

3 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile, Kapitel 4.2 „Strukturanalyse

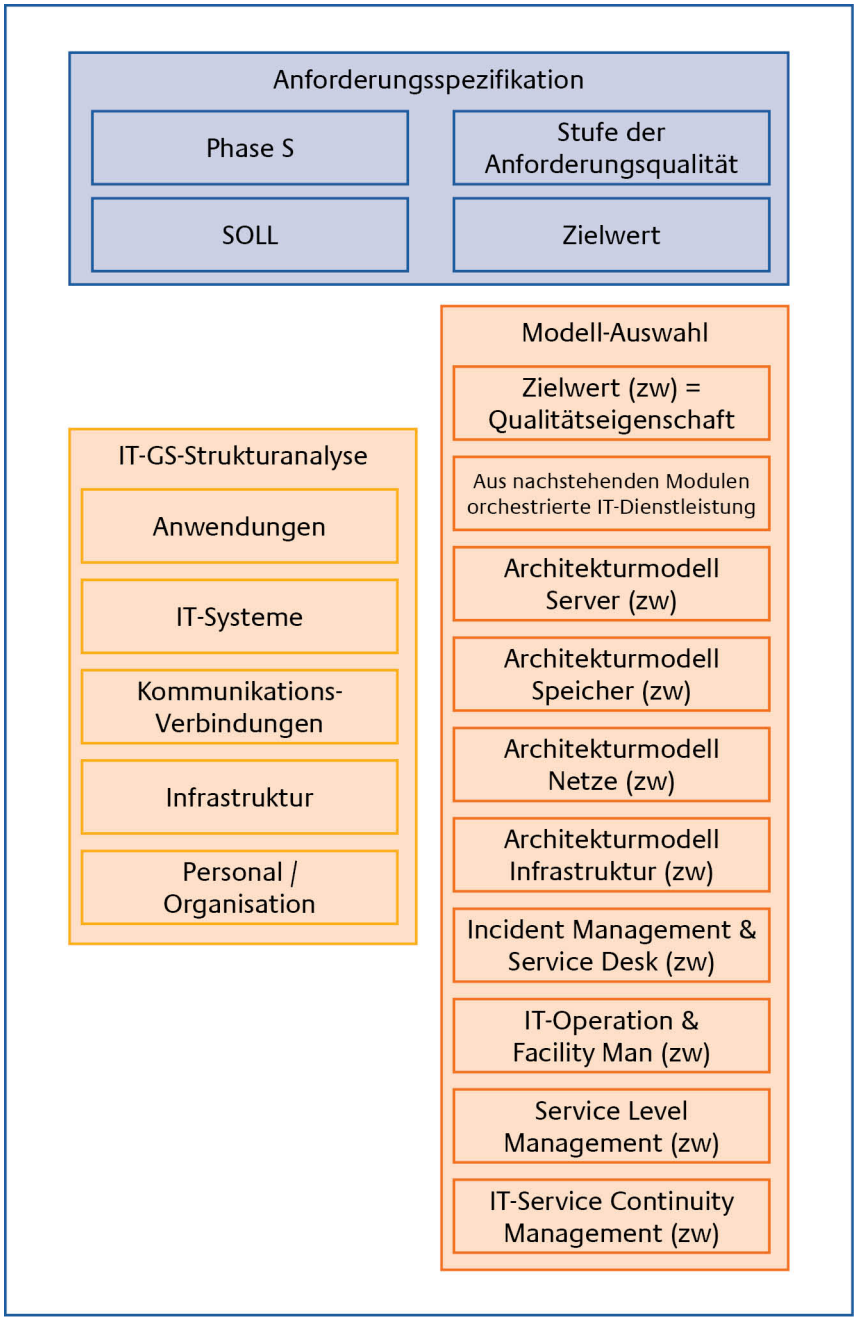


Abbildung 3: Modellierung von HV-Umgebungen

In der Abbildung 3 liefert der blaue Bereich die Anforderungen im Soll, der gelbe Bereich liefert die zu modellierende Struktur bei bestehenden Architekturen, der grüne Bereich umfasst das Modul-Spektrum des Modellkataloges, aus dem IT-Dienstleitungen orchestriert werden können.

Der mit dieser Version 1.6 des Kompendiums vorgelegte Modellkatalog ist noch im Erprobungsstadium (Status „Proof_of_Concept“). Er wird vom BSI auf der Grundlage der Erfahrungen in der Praxis überarbeitet und fortgeschrieben.

Die vorgeschlagenen Methode liefert gleichermaßen Modelle für existierende wie für geplante HV-Anwendungsumgebungen. Für eine existierende Anwendungsumgebung wird ein Leistungsprofil erstellt, der als Prüfplan für die eingesetzten Ressourcen Verwendung finden kann und Ansätze für eine Optimierung der eingesetzten Ressourcen liefert. Für geplante HV-Umgebungen wird ein

Leistungsprofil generiert, welches als konzeptionelle Grundlage für Planung, Umsetzung und Betrieb anzusehen ist.

2.1.2 Modellierung für das Feinkonzept und dessen Umsetzung

Die Modellierung der Phase M auf der Basis der Architekturmodelle liefert im Ergebnis ein Referenzmodell zur Orchestrierung von Services und Komponenten ergänzt durch Maßnahmeempfehlungen. Bei der Umsetzung in das Feinkonzept sind die Architektureigenschaften vorhandenen Komponenten zu berücksichtigen und gegebenenfalls zu optimieren. Möglicherweise wird z.B. die Auswahl robusterer Komponenten erforderlich werden.

Im Rahmen der Modellierung werden mit der Auswahl der Architekturmodelle Maßnahmeempfehlungen zur Verfügung gestellt, welche bei der Feinkonzeption und dessen Umsetzung in die Praxis als essentiell für die Realisierung einer HV-Umgebung anzusehen sind.

Die Architekturmodelle empfehlen:

1. Im Modellierungsbereich bis zur Potentialstufe 2 werden die Bausteine des IT-Grundschutzes relevant, um in der gewählten IT-Infrastruktur einen Basis-Schutz zu realisieren, auf dem die HV-Maßnahmen aufbauen können. Bei der Realisierung der ausgewählten HV-Umgebung ist eine Modellierung des zu betrachtenden IT-Verbundes nach BSI-Standard 100-2 (dort Kap. 4.3.2) vorzunehmen und die relevanten IT-Grundschutzbausteine und -Maßnahmen aus den IT-Grundschutzkatalogen umzusetzen.
2. In den höheren Potentialstufen werden die Maßnahmeempfehlungen des IT-Grundschutzes durch weitere Maßnahmen im jeweiligen HV-Baustein ergänzt, welche den höheren Verfügbarkeitsanforderungen genügen. Dabei können Maßnahmenbündel (z.B. Monitoring) entstehen, die sich auch auf Objekte beziehen, in deren Abhängigkeit das Modellierungsobjekt steht. Diese sind im standardisierten Abhängigkeitsmodell berücksichtigt.
3. Bei Abweichungen von dem Abhängigkeitsmodell in der Realität ist eine wirksame Absicherung der Verfügbarkeit ohne die Betrachtung der real bestehenden Abhängigkeiten nicht erreichbar. Um am Modellierungsobjekt eine effektive Wirksamkeit der Maßnahmen im Hinblick auf die Verfügbarkeit zu erreichen, sind die Verfügbarkeits-Abhängigkeiten dieses Objektes von anderen Objekten zu betrachten und zur ganzheitlichen Absicherung auf die Modelle ergänzender HV-Objekte zurückzugreifen, die an anderer Stelle in diesem Kompendium als HV-Modellierungsobjekte beschrieben sind. Die vorgestellten HV-Szenarien setzen daher eine Strukturanalyse nach Kapitel 4 des BSI-Standards 100-2 voraus.

Zur Absicherung einer HV-Umgebung sind die auf der jeweiligen Potentialstufe des Modells empfohlenen Maßnahmen umzusetzen. Für die Optimierung bestehender Architekturen liefern die Architekturmodelle Maßnahmeempfehlungen, die auf die nächst höhere Potentialstufe führen. Einzelne Maßnahmen oder –Bündel können durch alternative Modelle ersetzt werden, sie sollten in jedem Falle die Charakteristika hochverfügbarer Architekturen besitzen. Bei Abweichungen sind die Folgen für die Verfügbarkeit und andere Sicherheitsziele angesichts der Auswirkungen auf die Restrisiken darzustellen und zu bewerten. Die verbleibenden Restrisiken sind in jedem Fall transparent darzulegen, zu dokumentieren und von den Aufgabenverantwortlichen zu akzeptieren.

2.1.3 Optimierungsansatz auf der Basis von Charakteristika von Hochverfügbarkeitsarchitekturen

Eine IT-Architektur stellt einen strategischen Entwurf für den Einsatz von Technologien und die Weiterentwicklung der IT-Infrastruktur und der IT-Anwendungen zur Verfügung. Die IT-Architektur wird ergänzt durch Standards und Leitlinien, an denen sich Technologieeinsatz sowie Design und Weiterentwicklung von IT-Infrastrukturkomponenten und Anwendungen orientieren. Komponenten der IT-Architektur sind in der Regel die Anwendungs-, Infrastruktur-, Informations- bzw. Datenarchitekturen und Organisations- bzw. Prozessarchitekturen. Um die geforderte Verlässlichkeit zu erreichen, sind die Verfügbarkeits- und Verlässlichkeitspotentiale der eingesetzten Ressourcen aber auch ihre Anordnung in einer Architektur von entscheidender Bedeutung. Ziel der Optimierung ist die Identifikation von Schwachstellen und die Nutzung von Optimierungspotentialen und damit die Nutzung konkreter Verbesserungsvorschläge zur Erhöhung der Verfügbarkeit. Um hochverfügbare Architekturen zu erreichen, sind die Ressourcen und Prozesse so auszurichten dass eine maximale Downtime von 52,2 Minuten pro Jahr erreicht werden kann, um eine Verfügbarkeit von mindestens 99,99 % zu gewährleisten. Auf der Basis der HV-Prinzipien werden zunächst Konzepte verfolgt, die auf Redundanzen aufbauen:

- Clustering (Verfügbarkeitserhöhung durch redundante Komponenten)
- Redundante Internetanbindung
- Redundante Firewall
- Redundante L4/7 Lastballancierung
- Redundante Web-Server
- Redundante Application Server
- Redundante allgemeine Dienste, wie z.B. Stromversorgung.

Dies allein reicht nicht aus, um hohe Kontinuität für den Geschäftsprozess sicherzustellen. Proaktives Monitoring, schnelle Fehlererkennung und Beseitigung muss in Prozesse überführt werden, die einem ganzheitlichen Managementkonzept folgen, welches ein Business Continuity Management einschließen. Solche Managementkonzepte werden mit dem IT-Governance-Ansatz eingeführt, es ist bei einer Optimierung zur Erreichung hoher und höchster Verfügbarkeiten unumgänglich, dass derartigen Standards und den dazugehörigen Prozessmodellen gefolgt wird. Für die Optimierung liefern die generischen Prozessmodelle CobiT und ITIL geeignete Ansätze. Wesentlich dabei ist, dass ein IT-Service-Management auf der Basis messbarer Indikatoren eingeführt wird, die eine IT-Steuerung ermöglichen. Für die Bewertung der Verfügbarkeitseigenschaften von Architekturen und für die Steuerung von Services wurden hier weiterführende Reifegrad- bzw. Potentialmodelle entwickelt. Diese sind die Grundlage für das Management der Prozesse und die Identifikation von Optimierungspotentialen. Dabei sei an dieser Stelle auch darauf hingewiesen, dass die etablierten Prozessmodelle die Potential-Sicht als qualitative Indikation für die Steuerung von IT-Services bislang nur begrenzt nutzen. Die Aspekte Verlässlichkeit und Nachhaltigkeit werden von den vorliegenden Prozessmodellen grundsätzlich gesehen, eine explizite Indikation dazu fehlt bislang. Die Potentialbetrachtung nach dem HV-Kompendium kann problemlos als Indikatoren in die Prozessgebiete Monitor, Evaluate an Assess (MEA nach CobiT) bzw. Continous Service Improvement (CSI nach ITIL) integriert werden.

Der mit der Orientierung an den generischen Prozessmodellen einzuführende Prozessansatz sollte bei eine Modellierung von Services auf dem Service- oder Availability Management aufsetzen, da hier die Anforderungen aus Sicht der Geschäftsprozesse den Zielwert für ein SLA liefern. Im

Service Design sollten die Architekturmodelle berücksichtigt werden, wobei auch IT-Organisation als Objektgruppe im HV-Umfeld zu betrachten ist. Damit umfasst jeder Service eine Kette von HV-Objekten und Prozessen mit jeweils zugeordneten Bündeln von HV-Maßnahmen und Abläufen aus dem HV-Bausteinen, welche jeder Schicht der Kette HV-Eigenschaften in einer bestimmten Qualität verleihen. Diese HV-Eigenschaften stellen Eigenschaften der Architektur dar und ergeben sich aus dem Verfügbarkeits-Delivery der einzelnen Objekte in der jeweiligen Schicht und deren architektonischen Zusammenwirken mit Objekten anderer Schichten. Der Optimierungsansatz setzt bei der Analyse eines realen IT-Sevices mit der Feststellung der Abweichung des Service Delivery (Ist) von der geforderten Anforderungsqualität (Soll). Zunächst wird die Abweichung durch das Ergebnis des HV-Assessments in der Phase I festgestellt und deren Auswirkungen über die Risikoindikation analysiert. Dabei ist eine differenzierte Betrachtung des Services dort vorzunehmen, wo die Abweichungen von den Anforderungen besonders hoch sind. Beim Vergleich mit dem Architekturmodell lassen sich Engpässe und Schwachstellen identifizieren. Dabei wird die Zielsetzung verfolgt solche Objekte und Prozesse auszumachen, die den ungünstigsten Beitrag zum angestrebten Verfügbarkeitslevel liefern. Dort sind die zu erwartenden Optimierungspotentiale am größten.

Der Assessment-Ansatz bietet sich für die Analyse an, um in einer bestehenden Umgebung den gegebenen Verfügbarkeitsstatus festzustellen und zu optimieren. Die service- und prozessbezogene Betrachtungsweise im Assessment bietet den Vorteil der Konzentration auf die zentralen Objekte.

Für das Design von hochverfügbaren Architekturen eignet sich der Schichten-Ansatz besser, um das Zusammenspiel aller Services zu einer IT-Dienstleistung zu orchestrieren. Aus den Schichten der Abbildung 3 sollten die relevanten Architekturmodelle ausgewählt werden, welch die geforderte Funktionalität am ehesten liefern. Dies sollte bei neu zu konzipierenden HV-Umgebungen über alle Schichten durchgezogen werden. Da übergeordnete (Meta-)Maßnahmen nicht ausschließlich durch Vererbung den Objekten auf den „unteren“ HV-Schichten zugeordnet werden können, wird für die Modellierung eine weitere Meta-Schicht eingeführt, welche die Service Strategie abbildet. Hier werden auf der Ebene der Service Strategie Maßnahmen beschrieben, welche Design- oder Architekturaspekte beinhalten, die auf alle anderen Schichten Auswirkungen haben (z. B. „Implementierung fehlertoleranter Architekturen“). Übergeordnete Maßnahmen müssen nach diesem Modell nun nicht zwangsläufig durch eine Modellierung über alle Schichten hinweg hergeleitet werden, sondern können direkt über die Verknüpfung mit der Meta-Ebene, den Objekten auf der betrachteten Schicht zugeordnet werden. Die Meta-Schicht umschließt alle bisher betrachteten HV-Schichten (siehe Abbildung 4).

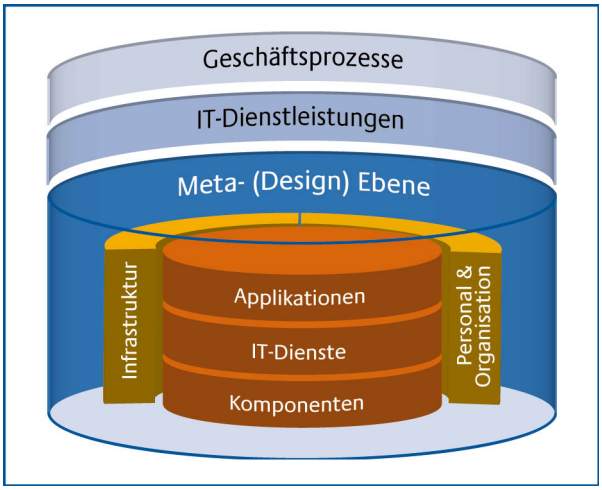


Abbildung 4: Modellierung der Schichten für das Design von HV-Architekturen

2.2 Schichten, HV-Bausteine, HV-Objekte und Architekturmodelle

Auf den einzelnen Schichten des HV-Schichtenmodells werden Objekt-Cluster unterschieden, welche durch die Verkettung unterschiedlicher Objekte oder Komponenten für die genutzten IT-Dienstleistungen funktionale Services in unterschiedlicher Qualität anbieten. Objekte oder Architekturmodelle werden nach funktionalen Eigenschaften in Clustern zusammengefasst, so dienen z.B. Objekte des Clusters Netze der Kommunikation nach innen oder außen. Sobald ein Objekt-Cluster sich in der Praxis bewährt hat (Best Practices), wird es zu einem standardisierten HV-Architekturmodell. Sie sind damit essenzieller Bestandteil des Service Designs und leisten im hier behandelten Kontext unterschiedliche Verfügbarkeitsbeiträge. Anhand der Architekturmodelle oder Objekt-Cluster können Bausteine zur Modellierung relevanter HV-Objekte identifiziert werden. Die Liste der Cluster, Bausteine, Architekturmodelle und auch der Objekte wird in den nachstehenden Beiträgen des HV-Kompendiums differenziert beschrieben. Sie ist als offene Liste anzusehen, die aufgrund der Vielfältigkeit möglicher HV-Lösungen und der technischen Entwicklung regelmäßig in neuen Clustern bzw. Modellen fortzuschreiben ist. Die Anpassung an aktuelle Entwicklungen soll im Dialog mit der Praxis erfolgen, um eine bedarfsgerechte Weiterentwicklung des HV-Kompendiums zu erreichen. Die notwendige Skalierbarkeit ist durch die skalierbaren Qualitätseigenschaften und den modularen Aufbau des Kompendiums gegeben.

Die Schicht „Organisation / Personal“ wird in einer optimalen HV-Umgebung durch an Standards orientierten Best Practices in Form von definierten IT-Managementprozessen realisiert.

Die Schicht „Infrastruktur“ beinhaltet die HV-Objekte der technischen Infrastruktur und beschreibt Maßnahmen für allgemeine und grundlegende Dienste der Gebäudeinfrastruktur, in den Objekt-Clustern Energieversorgung, Klimatisierung oder Beschaffenheit der Gebäude sowie der Versorgungs- und Netzwerkverkabelung.

Die Schicht „Komponenten“ umfasst IT-technische Objekte mit direkten Abhängigkeiten:

- im Bereich Systeme sind die technischen Basiskomponenten einer HV-Umgebung angesiedelt, die zur Erbringung von Diensten erforderlich sind, wie Server, Betriebssysteme, oder Clients
- dem Bereich Netzwerke sind HV-Objekte zugeordnet, die sich auf die logischen und organisatorischen Aspekte des Netzwerkes sowie grundlegende Netzdienste beziehen
- Die Schicht „Dienste“ dient der Darstellung und Modellierung von übergeordneten IT-Diensten. Bei IT-Diensten handelt es sich um Module, die den Applikationen komplexe Basisfunktionalitäten zur

Verfügung stellen. In der Regel setzt sich ein solcher Dienst aus mehreren Softwarekomponenten (Betriebssoftware) und mehreren IT-Komponenten zusammen

- Die Schicht „Applikationen“ stellt HV-Objekte dar, die den Anwendern als Schnittstelle zu den Geschäftsprozessen definierte Services mit einer gewünschten Verfügbarkeit zur Verfügung stellen (z. B. Web-Applikation)

2.2.1 HV-Bausteine und HV Objekte

Die Bausteine dieses Kompendiums gehen von Gefährdungen aus, die sich vornehmlich auf die Verfügbarkeit auswirken. Jeder HV-Baustein beschreibt Maßnahmeempfehlungen, welche insbesondere darauf ausgelegt sind, eine hohe Verfügbarkeit zu gewährleisten. Dazu werden ergänzende und abhängige Maßnahmen oder Maßnahmen zur Erreichung von Redundanzen in den Bausteinen beschrieben. Je nach zugeordneter Schicht umfassen die Beschreibungen im Baustein zum Beispiel organisatorische Rahmenbedingungen und Regelungen, Einsatzumgebungen, Sicherheitsdienste oder technische Detail-Lösungen, welche die Verfügbarkeit erhöhen. Im Folgenden wird von der Definition ausgegangen, dass ein HV-Baustein ein Maßnahmenbündel an einem HV-Objekt beschreibt, unabhängig davon, ob sich die Beschreibung auf ein Architekturmodell, ein konkretes Objekt, eine logische oder physische Komponente oder auf allgemeine Rahmenbedingungen bezieht. HV-Objekte können somit auch Verfahren und deren Dokumentation sein.

Das Maßnahmenbündel für ein HV-Objekt umfasst:

- die grundlegenden Maßnahmen für eine Basissicherung durch eine Modellierung nach IT-Grundschutz
- Verweise auf ergänzende HV-Objekte oder ergänzende Maßnahmen an diesen
- Maßnahmen zur Erhöhung der Verfügbarkeit am Objekt selbst

Die Bausteine des HV-Kompendiums sind nach dem HV-Schichtenmodell gegliedert.

2.2.2 Architekturmodelle

HV-Architekturmodelle sind auf Verfügbarkeitseigenschaften optimierte HV-Objekte für zentrale Funktions- oder Servicebereiche. Diese orientieren sich an den in diesem HV-Kompendium definierten HV-Prinzipien. In der Praxis stellt sich die Ausgangslage in komplexen HV-Architekturen dar, die sich in den Schichten Infrastruktur, Organisation & Personal, Komponenten und Dienste konkretisieren. Die Komplexität spiegelt sich in der Struktur- oder Abhängigkeitsanalyse wieder, wo schon die Auflösung der Architekturen in Komponenten oft an die Grenze des Machbaren stößt. Durch die Beschreibung von Referenzarchitekturen auf Schichtenebene als Cluster technischer Komponenten und organisatorischen Prozessen und deren Aufgabenstellung (Netze, Server, Speicher, Monitoring) soll der Komplexitätsgrad für die Analyse und Bewertung verringert und die Transparenz für das Design hochverfügbarer Architekturen durch Modellarchitekturen vergrößert werden.

HV-Architekturmodelle sind Referenzarchitekturen, deren Komponenten- oder Prozess-Struktur eine standardisierte Vorlage zum Design verlässlicher IT-Architekturen liefert. Auf der anderen Seite werden durch die Zuordnung von Verfügbarkeitseigenschaften und -potentialen Ansätze zur Bewertung des IT-Architekturpotentials geschaffen. Sie erfüllen daher zwei zentrale Use Cases:

1. Die Modellarchitektur beschreibt ein Komponenten- oder Prozessmodell mit bestimmten Verfügbarkeitseigenschaften durch spezifische Architekturmerkmale, die auf den HV-Prinzipien

beruhen. Auf der Basis von verbreitet eingesetzter Komponenten oder standardisierter Prozesse kann ein anforderungskonformes Design von Services orientiert an einem Standard erfolgen. Der Service liefert ein über die Verfügbarkeitseigenschaften bestimmbares Architekturpotential. Für das Design werden aus dem Architekturkatalog (HV-Kompendium V1.6, Band AH, Kap. AH 2) jene Modelle ausgewählt, die das erforderliche Potential liefern (siehe dazu Abschnitt 1.3.1 "Modellierung").

2. Das Architekturmodell liefert einen Beitrag für die qualitative Bewertung einer konkreten Ist-Architektur über den Referenzwert. Zur Einschätzung des Verfügbarkeitspotentials wird dem Referenzmodell ein Referenzwert zugeordnet, der entsprechend der Anforderungsqualität über fünf Stufen skaliert. Der zugeordnete Referenzwert beschreibt das zu erwartende Verfügbarkeitspotential und korreliert hoch mit dem zu erwartenden Verfügbarkeitsdelivery. Modellarchitekturen liefern mit jedem Modell einen Beitrag für das Design hochverfügbarer Architekturen, deren Verfügbarkeitsdelivery auf der Ebene der IT-Dienstleistung sich aus der Gesamtsicht aller beteiligten Modelle ergibt. Dabei bestimmt das schwächste Glied der Kette das Architekturpotential der IT-Dienstleistung.

Die Potenzialbewertung eröffnet wiederum zwei Anwendungsbereiche.

- für das Service Management werden Indikatoren für die Bewertung, Steuerung und Optimierung der Servicequalität geliefert;
- für die IT-Steuerung werden Aussagen zur Servicequalität und zu Optimierungspotentialen der IT sowie zu Risikopotentialen für die Geschäftsprozesse getroffen.

Ohne die ergänzende Einführung von Instrumenten für das Service Management und eine gezielte Steuerung bleiben zentrale Potentiale der Architekturmodelle ungenutzt. Das Erkennen von Fehlentwicklungen und Schwachstellen sowie die frühzeitige Korrektur von Abweichungen erfordert Zielwerte für eine transparente Bewertung des aktuellen Potentials und Optimierung des Status Quo. Die Instrumente bedürfen einer generischen Basis für eine standardisierbare, ganzheitliche Verfügbarkeitsbewertung wie sie dieses HV-Kompendium liefert. Die Entwicklung der entsprechenden Tools für die Steuerung der IT und für das Service Management ist vom BSI initiiert, erste Ergebnisse und Prototypen dazu liegen vor.

2.3 Restrisikoanalyse

Zielsetzung der Restrisikoanalyse in der Phase M ist die Ermittlung der Auswirkungen des bestehenden Delta auf die Geschäftsprozesse. Aus dem möglichen Risikoportfolio gehen jene Risiken in die Restrisikoanalyse ein, die besonders auf die kritischen Geschäftsprozesse wirken. Die Restrisikoanalyse betrachtet auch die bestehenden oder geplanten Ausweichmöglichkeiten oder alternativen Prozesswege, welche die verbleibenden potentiellen Schäden nicht allein am System, sondern aus Sicht des Geschäftsprozesses - wenn auch bei eingeschränkter Prozess-Qualität beleuchten. Ziel der Restrisikoanalyse ist die Reduzierung der am Geschäftsprozess verbleibenden Risiken auf ein tragbares Maß.

Voraussetzung für eine Restrisikoanalyse sind:

- das Vorliegen der Service-Anforderungen aus der Phase S: Soll-Anforderungen,
- das Vorliegen der Ergebnisse aus Phase I: Service-Delivery im IST,
- die Begutachtung des Delta aus dem HV-Assessement,

– eine Auswahl von Architekturmodellen für die Optimierung und das Vorliegen von Konzepten über Ausweichmöglichkeiten oder alternative Prozesswege für den Geschäftsprozess.

Die konzeptionelle Erarbeitung von Alternativen kann im Rahmen der Rekursion der Phase M unter Einbeziehung der Verantwortlichen für das GPM geleistet werden. Die Restrisikoanalyse hat zunächst den Grad des Erreichens oder die Einhaltung der zuvor als relevant angesehenen Ziel-Kriterien festzustellen. Aus dem Ergebnis der Phase S gilt es daher zunächst, die relevanten Zielkriterien zu extrahieren und mit den dazugehörigen Soll-Anforderungen für den Einstieg in die Restrisiko-Analyse zur Verfügung zu stellen. Diese liegen im Datenblatt „Verlässlichkeitsanforderungen“ vor. Die Zielkriterien mit den entsprechenden Soll-Anforderungen stellen die zu erreichenden Sicherheitsziele dar.

Für die Analyse des Restrisiko sind die Kritikalität und die Auswirkugen auf den Geschäftsprozess (Business-Impact) steuernde Zielkriterien, die letztlich die Dauer der Verzichtbarkeit und alternative Verfahrensmöglichkeiten bestimmen. Die Konsolidierung der Zielkriterien zu Sicherheitszielen kann verbal oder mittels der nachstehenden Tabelle erfolgen. Diese ist gegebenenfalls individuell anzupassen. Sofern mit dem Ergebnis einer Schutzbedarfsfeststellung nach IT-Grundschutz in die HV-Analyse und -Konzeption eingestiegen wurde, wird empfohlen, den nachstehenden Kriterienkatalog gemeinsam mit den Geschäftsprozessverantwortlichen abzuarbeiten.

Geschäftsprozess			
Kritikalität	Kernprozess 1.4.1.1 Lagerelevanz Tolerierbare Ausfallzeit (tA)	Business-Impact (Auswirkung auf GP)	Schadenshöhe bei Ausfall (Lt. Schutzbedarfs-feststellung)
Prozess-Qualität			
Maximale Bearbeitungszeit/Reaktionszeit			[ ]Min
Hinnehmbare Integritätseinschränkung			[ ]Nein
Hinnehmbare Vertraulichkeitseinschränkung			[ ]Nein
Rahmenbedingungen für Lage, auf jeden Fall verfügbar			[ ]Ja
Dauer der Verfügbarkeit			
Besondere Risiken:			
Abhängigkeiten			
Portierbarkeit			[ ]Nein
Alternativen			[ ]Nein
Grad interner Abhängigkeiten			[ ]hoch
Abhängige Geschäftsprozesse/Prozesskette			

Tabelle 1: Kriterienkatalog für die Beurteilung des Restrisikos

Die komplexen Anforderungen an die Verfügbarkeit sollten aus Sicht der Praxis eher wie folgende beispielhafte Sicherheitsziele formuliert sein:

- die Dienstleistung muss werktags von 08:00 bis 18:00 Uhr zur Verfügung stehen,
- die Dauer eines Ausfalls darf 1h auf keinen Fall überschreiten und

– mehr als 2 Ausfälle pro Monat sind nicht tolerabel, die Dauer eines Ausfalls darf 10 Minuten nicht überschreiten.

Angesichts der konsolidierten Sicherheitsziele ist die Frage zu beantworten, inwieweit durch den Lösungsvorschlag oder das angestrebte Service Level die vorgegebenen Sicherheitsziele erreicht werden oder auch nicht. Bei der Begutachtung des Lösungsvorschlages werden die Objekte wiederum entlang der prozessualen Kette mit ihren Abhängigkeiten betrachtet und mögliche Auswirkungen auf den Geschäftsprozess und davon abhängige Geschäftsprozesse geprüft.

Sind die Auswirkungen auf den Prozess durch die ausgewählten Maßnahmenbündel soweit abgefangen, dass der Prozess trotz Beeinträchtigungen aufrecht erhalten werden kann, können die Sicherheitsziele als eingehalten angesehen werden und das geplante Sicherheitsniveau erscheint ausreichend. Das verbleibende Restrisiko ist damit tragbar.

Werden die Ziele nicht erreicht, so kann das verbleibende Restrisiko weiter reduziert werden.

– Indem höherwertige HV-Architekturmodelle in die Modellierung des Service einbezogen werden. Diese genügen höherwertigen Verfügbarkeitsprinzipien und können das Restrisiko möglicherweise weiter reduzieren. Hier wird häufig die Frage der Machbarkeit oder Finanzierbarkeit gestellt. Mit einer Wirtschaftlichkeitsbetrachtung nach dem Modellierungsschritt wird eine Rekursion empfohlen, um die Anforderungsqualität des Geschäftsprozess mit der technisch oder organisatorisch geänderten Modell-Umgebung erneut der Restrisikoanalyse zuzuführen.

– Verfolgen der Kontinuitätsstrategie für kritische Geschäftsprozesse

  Umstrukturierung, d. h.. der Geschäftsprozess wird im Schadensfall auf alternative Ressourcen und Hilfsmittel verlagert. Dies setzt die Portierbarkeit der Prozesse voraus. Dabei ist davon auszugehen dass, das zu vereinbarende Service-Delivery im Normalfall ausreicht, um den Prozess mit hinreichender Qualität und Verfügbarkeit durchzuführen. Alternativen oder Umstrukturierungen werden nur in besonderen Ausnahme-Situationen wirksam, um in dieser Situation den Prozess aufrechterhalten zu können.

– Kontinuitätsstrategie(2):
  Inanspruchnahme ergänzender oder alternativer IT-Ressourcen oder Services interner oder externer Lieferanten über OLAs oder UPCs um bei auftretenden Engpässen den Prozess aufrechterhalten zu können. Ein vollständiger Risiko-Transfer oder die Risiko-Übernahme wird gerade bei kritischen Geschäftsprozessen regelmäßig als Alternative zur Bewältigung des Restrisikos nicht in Frage kommen. Die Absicherung des Service-Delivery z. B. durch eine Pönale wird häufig als probates Mittel bei einem Risikotransfer angesehen. Es muss in diesem Zusammenhang jedoch auch klar festgelegt sein, dass der Service-Anbieter z. B. bei einem durch höhere Gewalt verursachten Ereignis in der Lage ist, das vereinbarte Service Level anzubieten. Gerade in solchen Situationen kann die Verfügbarkeit kritischer Geschäftsprozesse zwingend erforderlich sein. Rechtlich kann der Anbieter allerdings objektiv nicht in der Lage sein, den notwendigen Service zu liefern, da höhere Gewalt als Exkulpationsgrund vorliegen kann.

In die Restrisikoanalyse sind die Verantwortlichen für die Geschäftsprozesse einzubeziehen. Sie wird durch Betrachtung ausgewählter Schadensszenarien erleichtert, bei denen von großflächigen oder schwerwiegenden Schäden und besonderen Lagen auszugehen ist. Insbesondere bei Entscheidungen über Umstrukturierungen oder die Inanspruchnahme alternativer Ressourcen liefern derartige Szenarien häufig die Begründung für besondere Investitionen. Die beschriebenen Maßnahmen und Alternativen orientieren sich an HV-Prinzipien wie Redundanz oder Autonomie, sodass die Realisierung einer höherwertigen HV-Umgebung regelmäßig mit höheren Kosten

verbunden sein wird. Wir befinden uns bei der Konzeption und Umsetzung in einer Art magischem Viereck zwischen Verfügarkeits-Delivery, Komplexität, Kosten und Restrisiko. Es wird voraussichtlich Alternativen geben, die bei einem geringeren Qualitäts-Delivery zwar geringere Kosten verursachen jedoch bei möglicherweise gleichbleibender Komplexität mit einem höheren Restrisiko verbunden sind. Die mit der Konsolidierung der Sicherheitsanforderungen erhobenen Verfügbarkeitsanforderungen sind daher dem Verfügbarkeits-Delivery gegenüberzustellen und der Nutzen z.B. aus geringeren Kosten gegenüber dem verbleibenden Restrisiken abzuwägen. Die verursachten Kosten erscheinen bisweilen nicht tragbar, hier sind individuelle Alternativen zu entwickeln, mit ihren Restrisiken zu bewerten und in Ihrer Wirkung mit den vorher entwickelten Modelle zu vergleichen. Die Entscheidung für eine Alternative kann immer nur vor dem Hintergrund der von den Aufgabenverantwortlichen zu übernehmenden Restrisiken getroffen werden.

Möglicherweise liegen aus der Phase S bereits Ergebnisse aus der Szenarien-Analyse vor, auf deren Dokumentation an dieser Stelle zurückgegriffen werden kann. Die Szenario-Technik ist bereits für die Phase S beschrieben. Für die Bewertung der Restrisiken wird die folgende Bewertungsmatrix vorgeschlagen, die künftig für die Toolgestütze Risikobetrachtung Verwendung finden sollte:

Ausprägung des Restrisikos	*Wert*
Sicherheitsziele werden eingehalten	1
Sicherheitsziele werden in tolerierbaren Grenzen verletzt	2
Sicherheitsziele werden verletzt, es kann zur Überschreitung gesetzter Grenzen kommen, (Grenzüberschreitungen beschreiben)	3
Sicherheitsziele werden verletzt, gesetzte Grenzen können nicht garantiert weden	4
Sicherheitsziele sind nicht einzuhalten, das geforderte Sicherheitsniveau kann nicht erreicht werden	5

Tabelle 2: Ausprägung des Restrisikos

Im Hinblick auf Transparenz und Beurteilung des Restrisikos ist für die Leitungsebene das Szenario zu benennen und die Grenzverletzungen zu beschreiben. Als Entscheidungshilfe sollten die geprüften Alternativen dokumentiert werden. Das Ergebnis der Restrisikoanalyse ist in einem Managementreport zusammenzufassen und an die Leitungsebene zu adressieren. Bei bemerkenswerten Ausprägungen des Restrisikos sollte immer eine Leitungsentscheidung über den Umgang mit dem Restrisiko herbeigeführt werden.

2.4 Wirtschaftlichkeitsbetrachtung

Die Herausforderung für IT-Verantwortliche liegt darin, die gestellten Anforderungen mit begrenzten Mitteln umzusetzen. ITIL sieht dazu bereits im Service Strategy Prozess die Entscheidung über den verfügbaren Finanzrahmen vor. Vor dem Hintergrund der identifizierten Restrisiken eines realisierbaren Qualitäts- und Sicherheitsniveaus bedarf es einer fundierten Begründung, welche dieser Anforderungen zu welchem Grad umgesetzt werden können, welche Anforderungen den Rahmen der Möglichkeiten übersteigen und mit welchem Restrisiko zu rechnen

ist. Die Frage nach dem zu tolerierenden und damit tragbaren Restrisiko bedarf daher einer Abwägung wirtschaftlicher Gesichtspunkte. Kosten und Nutzen sollen schließlich in einem angemessenen Verhältnis zueinander stehen. Angesichts der Größenordnung der IT-Maßnahmen (Begriffsverwendung nach ITWiBe) zur Gewährleistung hoher oder höchster Verfügbarkeitsanforderungen wird eine formal fundierte Wirtschaftlichkeitsbetrachtung regelmäßig erforderlich sein. Die Durchführung von Wirtschaftlichkeitsbetrachtungen richtet sich in der Bundesverwaltung nach den Vorschriften des § 7 der Bundeshaushaltsordnung (BHO) sowie ergänzenden Verwaltungsvorschriften. Für die Durchführung wird hier auf die IT-WiBe [ITSt07] der IT-Steuerung des Bundes verwiesen.

Auf der einen Seite der Wirtschaftlichkeitsbetrachtung stehen die mit dem Lösungsvorschlag verbundenen Kosten, also monetär quantifizierbare Kosten, denen als Nutzen ein vermindertes Risiko gegenübersteht. Soll auch der Nutzen quantifiziert werden, wird empfohlen, über die ersparten Kosten durch verhinderte Schäden zu argumentieren.

Die Betrachtung der Auswirkung von Ausfällen eines Services auf den Geschäftsprozess des Unternehmens oder der Behörde wird an einem Beispiel in der nachstehenden Tabelle verdeutlicht:

Kosten =	***Kosten pro Einheit***	***Einheiten***
Produktivität der Benutzer	Stundensatz der betroffenen Benutzer	Dauer der Unterbrechung
Produktivität der IT	Stundensatz der betroffenen IT-Mitarbeiter	Dauer der Unterbrechung
Finanzielle Schäden	entgangene Einnahmen/ Schadenersatzforderungen Dritter	Dauer der Unterbrechung
Schäden an dem Prozess/der Aufgabe	Gefährdung strategischer Ziele/ Gefährdung operativer Schäden Schäden für Umwelt oder Gemeinwohl Schadenersatzforderungen Dritter	Beurteilung der Schäden als Qualitätseinbußen oder Verlust von Qualitäten z. B.: Imagebeeinträchtigung oder -verlust Je Unterbrechung
Verletzung von Gesetzen	Strafen durch Gesetzesverstoß, Verfahrenskosten	Anzahl der Verstöße
Weitere Verluste	Instandsetzen, Nachholen/Mehrarbeit, Verbrauchsmaterialien	Dauer der Unterbrechung
Einfluss auf Leistungserbringung gegenüber Kunden	Vertragsverletzungen SLA-Vereinbarungen (Konventionalstrafen, Schadensersatz)	Dauer der Unterbrechung
Summe:		

Tabelle 3: Beispielrechnung für die Kosten einer Unterbrechung

Gerade für kritische Geschäftsprozesse wird ein vermindertes Risiko eher als Qualität anzusehen sein. Für die Betrachtung qualitativer Aspekte wird die Durchführung einer Nutzwertanalyse empfohlen. Die Risikominimierung besitzt für kritische Geschäftsprozesse eine herausragende

Bedeutung, die an der Kritikalität der Prozesse zu messen ist. Unter dem Aspekt der Wirtschaftlichkeit ist das verminderte Risiko mit einer besonderen Gewichtung zu versehen. Den mit dem konzipierten Lösungsvorschlag verbundenen Kosten stehen daher in der Wirtschaftlichkeitsbetrachtung qualitative Aspekte gegenüber, die eine qualitativ strategische Bedeutung besitzen oder durch gegebene Abhängigkeiten möglicherweise externe Effekte erzeugen. Für die Betrachtung dieser Wirkungsdimensionen wird dringend empfohlen, die IT-Wibe heranzuziehen.

2.5 Vorgehen in der Phase M

Am Anfang der Phase M liegt die Delta-Feststellung.

2.5.1 Schritt M 1 Delta-Feststellung

Die Delta-Feststellung setzt voraus, dass

- in der Phase S die Anforderungsqualität ermittelt wurde, welche als Anforderungsprofil im Sinne des Kriterienkatalogs für die Beurteilung des Restrisikos (S. Tabelle 1) differenziert darzustellen ist;
- bei bestehenden Architekturen ein Ergebnis aus dem HV-Assessement der Phase I vorliegt, mit dem das Delta zwischen Anforderungsqualität und Servicequalität bestimmt werden kann;
- für neue HV-Umgebungen auf der Basis der Anforderungen aus der Phase S in die Modellierung eingestiegen wurde.

Ist das Anforderungsprofil lediglich aus der Schutzbedarfsfeiststellung abgeleitet, so ist es um die Kriterien des Kriterienkatalogs aus Sicht des Geschäftsprozesses für die Beurteilung des Restrisikos zu ergänzen. Ein bewertetes Ist wird bei bestehenden HV-Umgebungen durch die Phase I geliefert. Bei einer geplanten HV-Umgebung ist zunächst ein erstes Grobkonzept für die geplante HV-Umgebung zu entwickeln und eine Modellierung vorzunehmen, um für den abzuwickelnden Geschäftsprozess eine geeignete Dienstleistungsumgebung zu designen. Die Entwicklung des Grobkonzeptes kann sich dabei an vorliegenden HV-Modellen orientieren, die vergleichbare Funktionalität und Qualität anbieten. Wichtig ist dabei in jedem Fall, alle Schichten im Rahmen der Grobkonzeption abzuarbeiten und anforderungskonforme Architekturmodelle auszuwählen.

Bei der Bestimmung des Delta sollte im Idealfall das Ist dem Soll entsprechen, d. h. die Anforderungen aus Sicht der Geschäftsprozesse werden durch die HV-Umgebung und die verfügbaren IT-Dienstleistungen erfüllt. Sollte eine Unterversorgung der Geschäftsprozesse festzustellen sein, ist das bestehende Restrisiko zu analysieren und zu beschreiben. Solange das Restrisiko von den Verantwortlichen als nicht tragbar angesehen wird, ist durch Auswahl ergänzender oder alternativer Modelle der HV-Verbund zu optimieren. Der vom Financial Management vorgegebene Rahmen setzt dabei zu verhandelnde Grenzen und muss bei nicht akzeptablen Restrisiken zu einem Überdenken der Kontinuitätsstrategie führen.

2.5.2 Schritt M 2.1 :Modellierung

Im Rahmen der Modellierung wird eine HV-Umgebung aus den vorliegenden Architekturmodellen gebildet, um für den Geschäftsprozess IT-Dienstleistungen in ausreichender Qualität zur Verfügung

stellen zu können. Die Orientierung an dem Schichtenmodell gewährleistet dabei eine ganzheitliche Betrachtung der vom Geschäftsprozess geforderten Service-Qualität mit all seinen Abhängigkeiten. Die Modellierung teilt sich in einen Schritt M 2.1, welcher der eigentlichen Modellierung dient, und einen Schritt M 2.2, welcher die Basisanforderungen bei der Modellierung berücksichtigt und eine Qualitätssicherung anbietet.

Die dargestellte Methodik verfolgt einen objektorientierten Ansatz durch die Modellierung von HV-Objekten anhand ihrer (HV-) Eigenschaften und den, auf diese anzuwendenden Operationen (HV-Maßnahmen). Grundlage der Modellierung ist der Architekturkatalog ergänzt durch den Maßnahmenkatalog, der jedem zu modellierenden HV-Objekte ein Bündel von HV-Maßnahmen zuordnet, welche dem Architekturmodell HV-Eigenschaften (prägende Merkmale der Architektur) in verschiedenen Qualitäten (Potentialstufen) verleiht.

Mehrere HV-Objekte mit (im Sinne der HV-Architektur) gleichartigen Eigenschaften werden Modellierungsbereichen zugeordnet. In der Weiterverfolgung des objektorientierten Ansatzes bilden diese Bereiche wiederum HV-Objekte höherer Komplexität, die sowohl die (HV-) Eigenschaften der untergeordneten Objekte erben, als auch um weitere Eigenschaften (HV-Maßnahmen) ergänzt werden können.

In Schritt 2.1 Modellierung wird jede Schicht auf das Vorliegen geeigneter Bausteine und Modelle geprüft und bei gegebener Eignung der Baustein mit den dort beschriebenen Objekten und Maßnahmen herangezogen. Ein geeignetes Modell liegt dann vor, wenn das Modell der geforderten Klasse der Anforderungsqualität so nah als möglich kommt. Beim ersten Modellierungszyklus wird zugelassen, gemessen an den Anforderungen des Geschäftsprozesses, das Modell mit dem Optimum an Verfügbarkeit auszuwählen. Im Rahmen von Wirtschaftlichkeitsbetrachtung und Restrisikoanalyse wird zu entscheiden sein, ob nicht alternative Lösungen, die weniger Kosten verursachen, zu tragbaren Restrisiken führen. In einem weiteren Modellierungszyklus sollen dann solche Modelle bevorzugt betrachtet werden, die sich am Redundanzprinzip orientieren und die redundante Auslegung von Objekten beschreiben. Dies wird von der Erfahrung getragen, dass High-End-Produkte regelmäßig bei sehr hohen Verfügbarkeitsanforderungen zum Tragen kommen. Bei hohen Verfügbarkeitsanforderungen reichen hinreichend verlässliche redundante Komponenten meistens aus, wenn die organisatorischen Prozesse die Verlässlichkeit sicherstellen.

Modelle werden über alle Schichten nach der Strukturanalyse in standardisierten Abhängigkeiten abgearbeitet. Übergeordnete Abhängigkeiten - Objekte mit übergeordneter Wirkung auf praktisch alle anderen Objekte - können dabei im Schichten-Ansatz vorweg abgearbeitet werden. Wird auf einer übergeordneten Schicht ein geeignetes Objekt identifiziert, so ist auch sicherzustellen, dass die nachgeordneten abhängigen Bausteine und Objekte in das Modell mit eingehen. Architekturkatalog und Maßnahmenkatalog dieses Kompendiums liefern standardisierte Abhängigkeitsmodelle.

2.5.3 Schritt M 2.2: Berücksichtigung von Basis Anforderungen bei der Modellierung

Die Modellierung nach diesem Kompendium verfolgt das primäre Ziel einer Verfügbarkeits-optimierung. Damit stehen beim Design von Lösungen jene Prinzipien im Vordergrund, die auf eine Qualitätssteigerung insbesondere unter Verfügbarkeitsaspekt zielen. An der Modellierung einschließlich dieser Prüfung sollten die nach ITIL für das Service Design Verantwortlichen beteiligt werden, da an dieser Stelle eine wesentliche Grundlage geschaffen wird für den Abschluss geeigneter Service Level Agreements. Diese Beteiligung setzt implizit voraus, dass die Verantwortlichkeiten für ITIL-Prozessgebiete definiert sind. Im Kontext der Hochverfügbarkeit ist

dies insbesondere für das IT-Service Continuity Management, Service Level Management und Incident Management zu fordern.

Um auf der Ebene der Grobkonzeption sicherzustellen, dass die ausgewählten HV-Modelle die funktionalen Anforderungen sowie Qualitätsanforderungen erfüllen, wird empfohlen im ersten Entwurf bereits die Basisanforderungen zu berücksichtigen und diese anhand der ausgewählten Modelle zu verifizieren:

- Welche Anforderungen an die Performanz stellt der Geschäftsprozess?
- Welche Anforderungen an die Kapazität stellt der Geschäftsprozess?
- Angesichts künftiger Entwicklungen ist Skalierbarkeit in welchem Rahmen gefordert?
- Sind die Availability Anforderungen nach ITIL in den Kriterien
  - Reliability (Zuverlässigkeit)
  - Maintainability (Wartbarkeit)
  - Serviceability (Servicefähigkeit)
  - Security (Sicherheit)

  erfüllt?

Aus dem Bereich der Sicherheitsanforderungen sollte an dieser Stelle insbesondere hinterfragt werden:

- Sind die Anforderungen an Integrität und Vertraulichkeit durch die ausgewählten Objekte erfüllt?
- Beim Einsatz ergänzender Sicherheitskomponenten (z. B. Kryptokomponenten) sind diese Basisanforderungen auch von diesen zu erfüllen?

Im Ergebnis liefert Schritt M2 eine Architekturauswahl mit Objekt- und Maßnahmenkette für Gestaltung hochverfügbarer IT-Ressourcen über alle Schichten unter Berücksichtigung funktionaler und qualitativer Anforderungen. Im nächsten Schritt gilt es, die angebotene Qualität zu bewerten. In wie Weit die Anforderungen an die Verfügbarkeit von den eingesetzten Objekten erfüllt werden können, ist Gegenstand der folgend beschriebenen Bewertung.

2.5.4 Schritt M 3: Bewertung

In diesem Schritt wird das erwartete Service-Delivery der modellierten HV-Umgebung für den Geschäftsprozess festgestellt. Dabei ergibt sich die Verfügbarkeit des Service Delivery aus dem Minimum der mit den verschiedenen Architekturmodellen erreichten Verfügbarkeit. Für jede Schicht ist daher zunächst einzeln die Verfügbarkeit festzustellen. Für die Bewertung wird in diesem Kompendium das HV-Assessment zur Verfügung gestellt. Diese lässt für jede Schicht den die Ermittlung des Verfügbarkeitspotenziales zu.

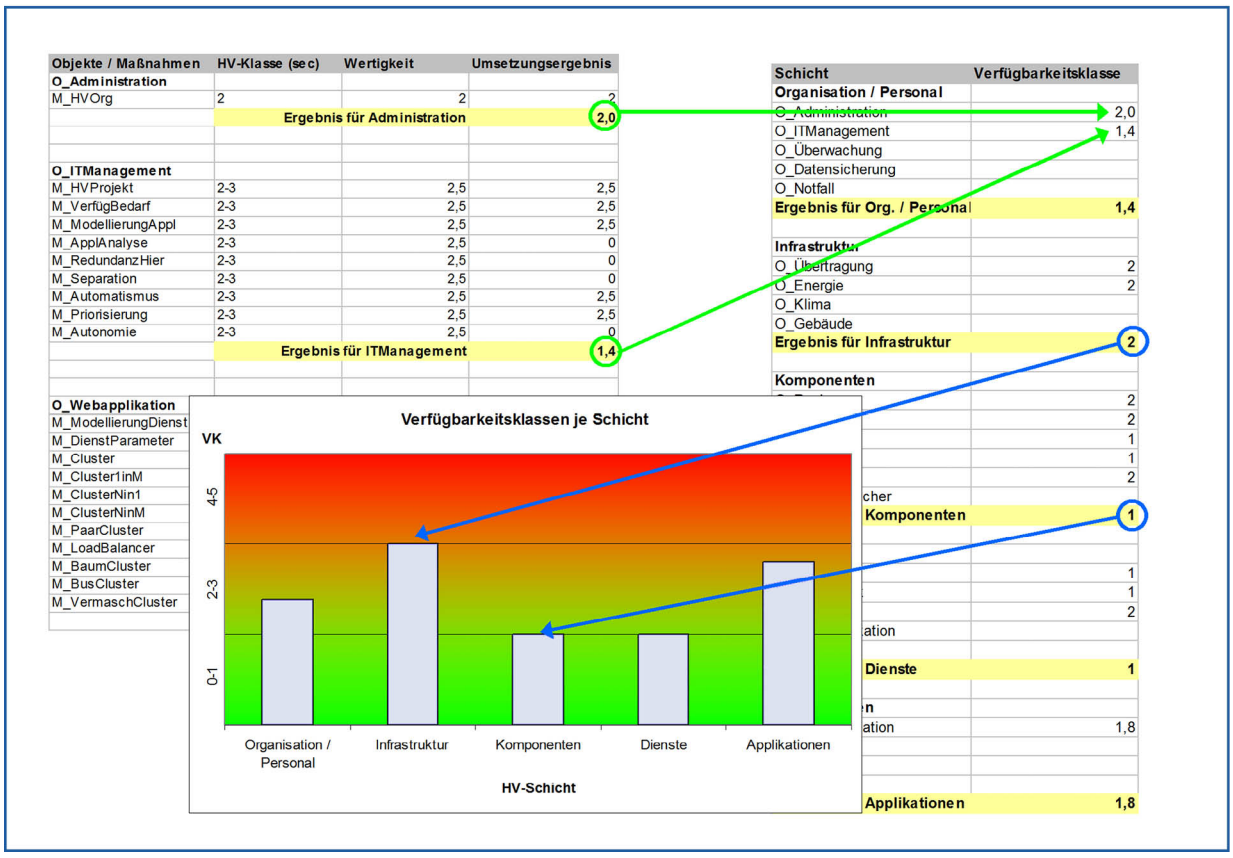


Abbildung 5: Bewertung der HV-Schichten nach umgesetzten Maßnahmen

Sind Architekturen zu bewerten für die keine HV-Architekturmodelle vorliegen oder die nicht dem standardisierten Abhängigkeitsmodell folgen, so ist auf der Baiss der Maßnahmenkataloge über die Schichten zu bewerten. In der Abbildung 5 werden die notwendigen Schritte zur Verfügbarkeitsbewertung der einzelnen HV-Schichten auf der Basis von HV-Maßnahmen illustriert. Zunächst müssen die HV-Maßnahmen, die an einem Objekt umgesetzt wurden bewertet werden. In der linken Tabelle der Abbildung 5 sind exemplarisch die Maßnahmenbündel für die Objekte „Administration“, „IT-Management“ und „Webapplikation“ aufgelistet. Alle Maßnahmen zu diesen und weiteren Objekten sind als HV-Bausteine im Kapitel „HV-Maßnahmen“ zusammengestellt. Die Einteilung der Maßnahmen in Verfügbarkeitsklassen, wie sie im Maßnahmenkatalog des Kapitels „HV-Maßnahmen“ vorgenommen wurde, bildet hier die Basis für die Bewertung. Wird eine Maßnahme nicht einer Verfügbarkeitsklasse, sondern einem Bereich zugeordnet, so wird zur Bewertung der Mittelwert für die Wertigkeit dieser Maßnahme angenommen. Die Wertigkeit der Maßnahme wird schließlich auch für das Umsetzungsergebnis einer Maßnahme herangezogen, wenn diese entsprechend der Maßnahmenbeschreibung umgesetzt wurde. Wurde die Maßnahme nicht oder nicht vollständig umgesetzt, so ist als Umsetzungsergebnis der Wert „Null“ einzutragen. Ist die vorgeschlagene Maßnahme für das betrachtete Objekt nicht relevant, weil beispielsweise eine alternative Maßnahme zum gleichen Verfügbarkeitseffekt führt, so ist für diese kein Wert anzugeben. Durch Mittelwertbildung der einzelnen Umsetzungsergebnisse wird die Verfügbarkeitsklasse eines Objektes ermittelt (in der linken Tabelle derAbbildung 5 gelb markiert).In einem weiteren Schritt werden alle Objekte einer HV-Schicht mit den zuvor ermittelten Verfügbarkeitsklassen in eine Tabelle übertragen (siehe rechte Tabelle in Abbildung 5). Alle Objekte, die den Gesamtprozess stützen, müssen bei der Verfügbarkeitsbewertung berücksichtigt werden. Die Verfügbarkeitsklasse für die gesamte Schicht wird nach dem Minimum-Prinzip

ermittelt. Demnach ergibt sich der Verfügbarkeitswert der jeweiligen Schicht aus dem niedrigsten Verfügbarkeitswert aller Objekte dieser Schicht.

Die Verfügbarkeitswerte der einzelnen HV-Schichten können in einem Säulendiagramm grafisch aufbereitet und mit dem SOLL-Profil aus der Phase S verglichen werden (siehe Abbildung 7).

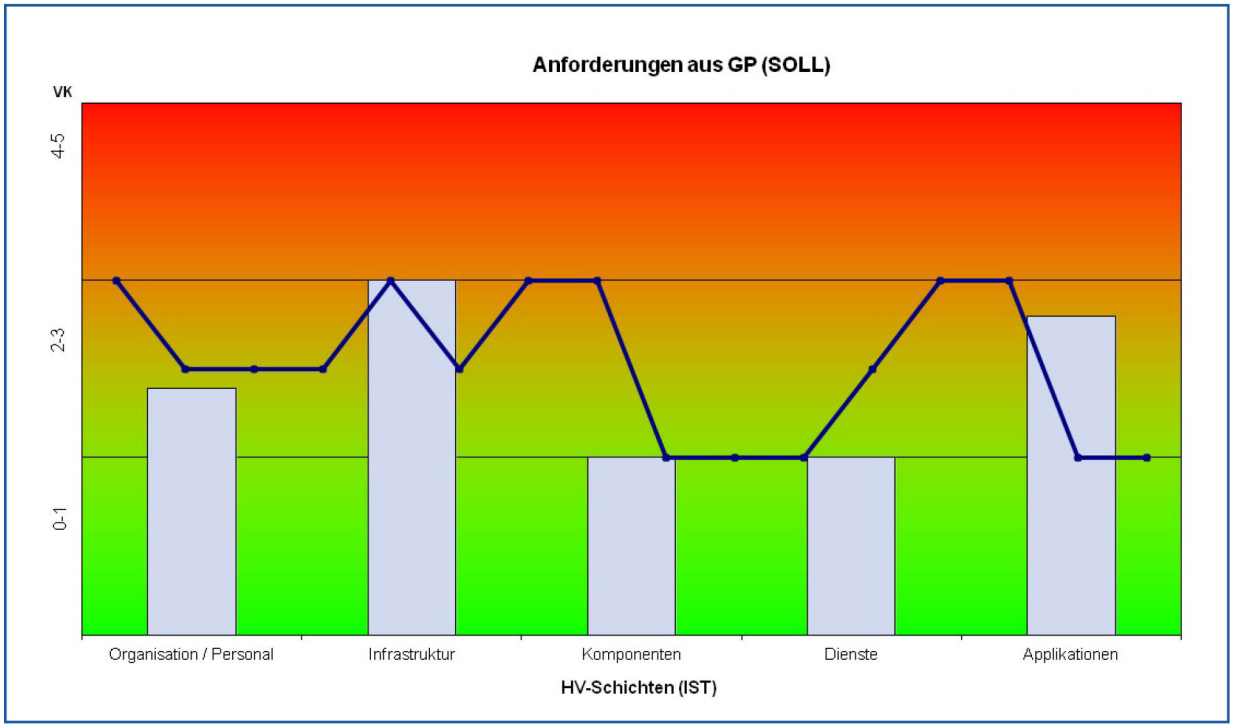


Abbildung 6: Grafischer Soll-Ist-Vergleich

2.5.5 Schritt M 4: Rekursion auf Delta Feststellung (Soll-IstVergleich für erarbeitetes Modell)

Wird dem standardisierten Abhängigkeitsmodell gefolgt, so liefert das HV-Assessement diese Auswertungen im Kiviat-Diagramm. Die Auswertung kann sowohl für einzelne Teilbereiche (Schichten) als auch für die gesamte Dinstleistung gemacht werden. Dem BSI liegt der Prototyp für ein Assessement&Benchmarking-Tool vor (Siehe dazu Band AH, Kapitel 1„HV-Assessement&Benchmarking“). Sollen Verfügbarkeitspotentiale in RZ-spezifischen Bereichen bestimmt werden, so bietet sich das Tool VAIR „Verfügbarkeitsanalyse in Rechenzentren an, welches im Auftrag des BSI entwickelt wurde. Für den Einsatz beider Tools kann im Bereich der Bundesverwaltung über „Sicherheitsberatung@bsi.bund.de“ nachgefragt werden.

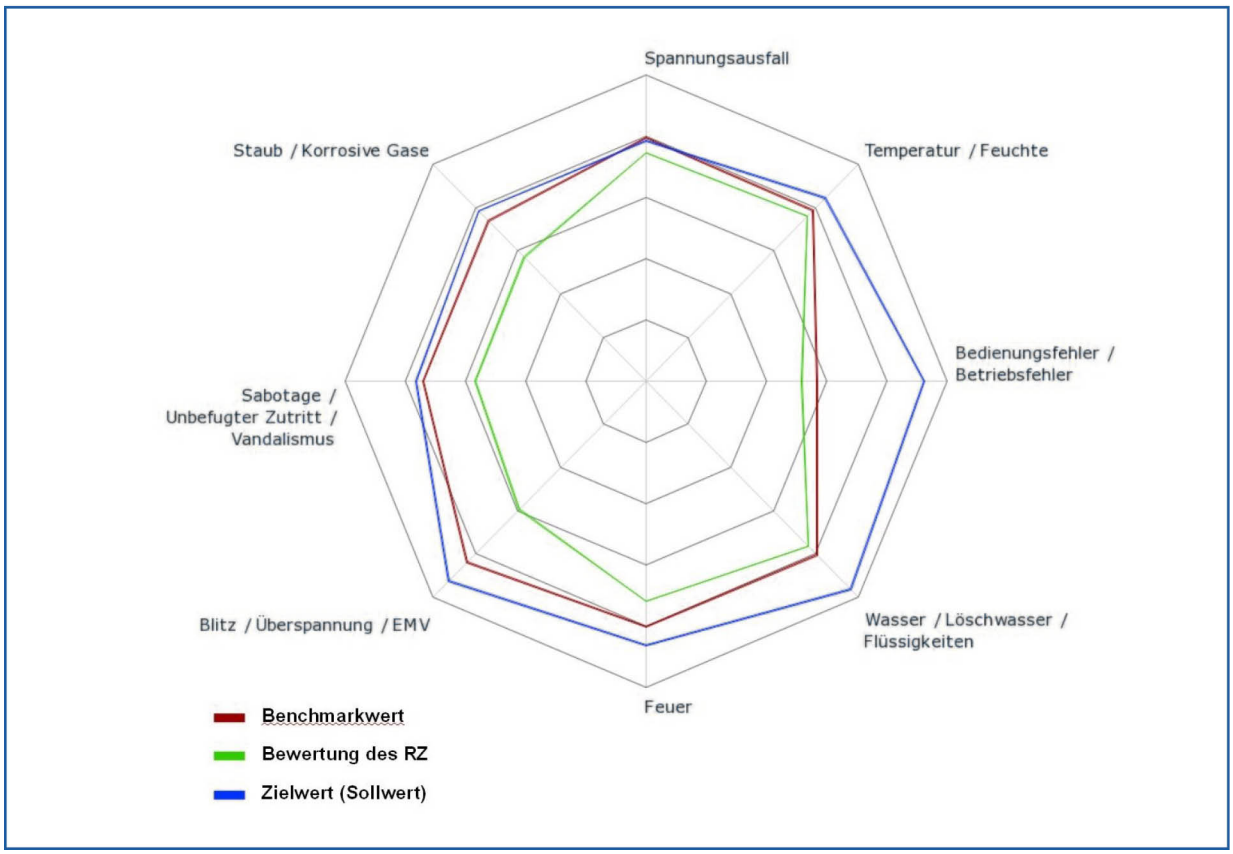


Abbildung 7: VAIR Verfügbarkeitsanalyse in Rechenzentren: Ergebnis in der Schicht Infrastruktur

Der Soll-Ist-Vergleich aus der Beispielanwendung "VAIR"(Abb.: 7) zeigt im Kiviat-Diagramm, dass die vorliegende Service-Qualität unterhalb der Anforderungen liegt und damit Opzimierungspotentiale aufweist.

Das Ergebnis des Soll-Ist-Vergleiches ist Voraussetzung für die anstehende Restrisiko-Analyse. Das erarbeitete Ergebnis ist Basis für die Optimierung des Service Delivery. Wird eine augenscheinlich erhebliche Abweichung festgestellt, so ist davon auszugehen, dass ein Engpass oder Schwachstelle für die Verfügbarkeit vorliegt. Bei augenscheinlich erheblichen Abweichungen werden die potentiellen Schäden regelmäßig ohne weitere Analyse zu beschreiben sein. In diesen Fällen ist eine Rekursion in den Modellierungsschritt vorzunehmen, um ein Architekturmodell der nächst höheren Potentialstufe in die HV-Umgebung aufzunehmen. Sprünge über mehrere Potentialstufen sind dabei nicht zulässig, weil die Architekturmodelle Entwicklungen über Potentialstufen bescheiben. Die Auswahl der Modelle sollte über die Stufen und Schichten erfolgen und sich an der Frage orientieren, ob in der betrachteten Schicht Modelle im gleichen Objekt-Cluster vorliegen, die einen höheren Verfügbarkeitsbeitrag liefern. Wird kein entsprechendes Modell gefunden, so wird empfohlen, aus dem Bausteinkatalog solche Objekte und Maßnahmeempfehlungen auszuwählen, die ein höheres Prinzip aus der Prinzipien-Hierarchie verfolgen. Nach der Auswahl neuer Objekte ist erneut in die Restrisikoanalyse einzusteigen.

2.5.6 Schritt M 5: Restrisikoanalyse

Für die eigentliche Restrisiko-Analyse ist auf die Kriterien zurückzugreifen, die im Rahmen der Phase S (Band G, Kapitel 4 des HV-Kompendiums) für die Ermittlung von Sicherheitsanforderungen als wesentlich angesehen wurden. Gerade bei kritischen

Geschäftsprozessen ist deren Bedeutung für die öffentliche Sicherheit, das Gemeinwohl oder die Bewältigung von Lagen besonders Rechnung zu tragen. Risikoszenarien, die vom Ausfall der IT über einen mehrtägigen Zeitraum gehen, sind in die Restrisikobetrachtung einzubeziehen und mit der Kontinuitätsstrategie zu bewältigen. Inhaltlich orientiert sich die Analyse der Restrisiken auf die Prüfung der Auswirkung nicht zu beseitigender Schwachstellen und nicht weiter zu optimierender IT-Ressourcen.

Für die Akzeptanz des Restrisikos sind – auch wenn augenscheinlich keine erheblichen Abweichungen Ist-Soll vorliegen- im Rahmen der Restrisiko-Analyse Auswirkungen von potentiellen Schadensereignissen in einer differenzierten Analyse angesichts der Kontinuitätsstrategie und des vorhandenen Bewältigungspotentials zu betrachten, um festzustellen, ob die gewählten alternativen Wege zur Aufrechterhaltung kritischer Geschäftsprozesse in besondern Lagen tragen.

2.5.7 Schritt M 6: Wirtschaftlichkeitsbetrachtung

Es wird auf die Ausführungen unter Kapitel 2.4 Wirtschaftlichkeitsbetrachtung verwiesen

2.5.8 Phasenabschluss

Der Phasenabschluss dient dazu, die in diesem Kompendium beschriebenen Aktivitäten und erarbeiteten Ergebnisse in einen geschlossenen Managementzyklus, wie er mit ISO 27001 beschrieben ist, zu überführen. Während die hier beschriebene Aktivitäten zur Konzeption von HV-Umgebungen überwiegend dem Aktivitätsbereich „PLAN“ zuzuordnen sind, soll für die Aktivitätsbereiche „DO“, „CHECK“ und „ACT“ wiederum auf etablierte Standards zurückgegriffen werden. Die Phase M ist abzuschließen, wenn ein tragbares Restrisiko erreicht wurde. Der Phasenabschluss steht im Zeichen der Integration der HV-Konzeption in das bestehende IT-Prozess- und IT-Sicherheitsmanagement-System. Es wird hier davon ausgegangen, dass das IT-Sicherheitsmanagement sich am BSI-Standard 100-1 orientiert. Fernerer wird die Integration in ein IT-Governance-Modelle bzw. in ein ITIL-oder CobiT-konformes IT-Prozess-Management angenommen.

2.6 Integration in das bestehende IT-Sicherheitsmanagement System

Im Ansatz der IT-Governance ist die Optimierung der Service-Potentiale Aufgabe des Service Level Management. Eine Trennung von IT-Aspekten und IT-Sicherheitsaspekten ist in den Prozessmodellen der IT-Governance nicht vorgesehen. Bereits die Anforderungsanalyse ist elementarer Bestandteil des Service Design und wird geprägt von der strategischen Ausrichtung der IT und an den Erfordernissen der Geschäftsprozesse.

Wird vom IT-Grundschutz-Ansatz ausgegangen, so ist die Schutzbedarfsfeststellung Aufgabe des IT-Sicherheitsmanagements. Die im Rahmen der Modellierung herausgearbeiteten Maßnahmenbündel sind dann für die Umsetzung in den laufenden IT-Sicherheitsprozess [BSI05] zu integrieren. Somit wird die Verantwortung für die Umsetzung und Erfüllung der Anforderungen zwischen IT-Service Management und IT-Sicherheitsmanagement geteilt.

Die Umsetzung wird eingeleitet mit der Wirtschaftlichkeitsbetrachtung im Rahmen der Restrisiko-Analyse und umfasst im Phasenabschluss die Einleitung der Feinkonzeption in Zusammenarbeit mit dem Change-Management sowie später die Initiierung der Beschaffungsvorgänge in Zusammenarbeit mit dem Financial-Management. Die behandelten Alternativen, Entscheidungen

und Ergebnisse der Restrisikoanalyse sind zu dokumentieren, dazu kann auf die Vorlagen des BSI-Standards 100-3 zurückgegriffen werden.

Die Bausteine dieses Kompendiums beschreiben Maßnahmenbündel für HV-Objekte unter Integration des IT-Grundschutz. Grundschutzmaßnahmen sind in den Bausteinen bereits berücksichtigt, Überschneidungen sollten damit ausgeschlossen sein. Zur weiteren Konsolidierung des IT-Sicherheitskonzeptes wird auf das Vorgehen nach Kapitel 7 des BSI-Standards 100-3 verwiesen. Für die Umsetzung und den Betrieb erfolgt gleichermaßen der Verweis auf die Rückführung in den IT-Sicherheitsprozess in Kapitel 8 des BSI-Standards 100-3.

2.7 Ergebnisse der Phase M

Die nachstehenden Artefakte dokumentieren den Entscheidungshintergrund für die zu realisierende HV-Umgebung:

Ein Service-Design-Entwurf mit

- einer aus standardisierten Architekturmodellen orchestrierten IT-Dienstleistung als Entwurf für zu realisierende HV-Architekturen (Grob-Konzeption)
- einem IT-Sicherheitskonzept unter HV-Aspekt
- Bausteinen und Maßnahmenbündeln für HV-Objekte
- Beschreibung der konsolidierten IT-Sicherheitsziele
- Beschreibung des Restrisikos
- Dokumentation der Entscheidungshilfen für die Akzeptanz des Restrisikos
- eine Wirtschaftlichkeitsbetrachtung
- ein von der Leitungsebene akzeptiertes Restrisiko.

Anhang: Verzeichnisse

Abkürzungen und Akronyme

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

Glossar

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

Literaturverzeichnis

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