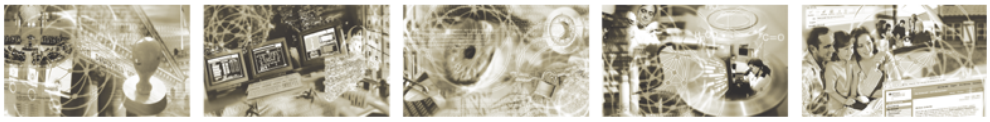
Bundesamt
für Sicherheit in der
Informationstechnik



Band B, Kapitel 2: IT-Organisation

Im Umfeld der Hochverfügbarkeit

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 Einleitung

IT-Verantwortliche in Behörden und Unternehmen stehen heute besonders vor der Herausforderung, die wachsenden Anforderungen an Sicherheit, Stabilität und Wirtschaftlichkeit der IT-Services zu gewährleisten und dies kontinuierlich sicherzustellen. Galt es bislang vielfach als Aufgabe des IT-Bereichs, die Nutzeranforderungen zu bedienen, wurden in Zeiten voller Kassen die Anforderungen selten hinterfragt, was man sich leisten konnte wurde umgesetzt. Dieses Vorgehen war eine wesentliche Ursache für die unkontrollierte Steigerung von Komplexität und Kosten der IT. Vor diesem Hintergrund hat sich heute IT-Management mehr denn je mit den Forderungen der IT-Governance auseinanderzusetzen und für die strategische Ausrichtung der IT sowie für Transparenz und Kontrolle zu sorgen. Zur Realisierung hoher und höchster Verfügbarkeiten wird auf redundante Technik gesetzt, verbunden mit Investitionen in rechnergestützte weitgehend automatisierte Umgebungen. Die Sicherstellung von Kontinuität und Nachhaltigkeit erfordert ergänzend steuernde Aktivitäten, mit denen Systeme und Prozesse überwacht und gesteuert werden können. Besonders im Umfeld kritischer Geschäftsprozesse sind diese Anforderungen nur zu gewährleisten, wenn sich IT-Organisation an den generischen Prozessmodellen der IT-Governance orientiert. Um die gewünschten Leistungen über definierte und bewertbare IT-Services bereitzustellen, ist eine klar strukturierte und reibungslos arbeitende IT-Organisation, die sich an den Erfordernissen der Geschäftsprozesse orientiert (Business Alignment) aufzubauen. Weiter setzen die Forderungen nach Steigerung von Effizienz und Effektivität strikt zielgerichtete IT-Prozesse voraus, die durch einen kontinuierlichen Verbesserungsprozess begleitet werden. In HV-Umgebungen bietet sich damit die Chance zu einer Optimierung der Verfügbarkeit. Die prozessualen Ansätze der IT-Governance zur Erbringung, Bewertung, Steuerung und kontinuierlichen Verbesserung der Qualität von IT-Services sind in idealer Weise geeignet, Prozesse zur Risikoprävention und Gewährleistung höchster Verfügbarkeit zu etablieren.

Die bewährten Praktiken für die Prozessgestaltung werden mit ITIL und die notwendige Geschäftssicht mit CobiT geliefert. In diesem Beitrag werden die für die Zielerreichung, Kontinuität des Geschäftsbetriebes, wichtige Prozessgebiete identifiziert, relevante Aktivitäten und Rollen herausgestellt und ein Bewertungsansatz mittels spezifischen Kennwerten und Reifegradmodellen für die IT-Organisation geschaffen. Die Bewertung hinsichtlich der Prozessreife bzw. des Organisationspotenzials wird im Rahmen des HV-Assessments durchgeführt (siehe HV-Kompendium, Band AH, Kapitel 2 „HV-Assessment und Benchmarking“).

Im vorliegenden Beitrag werden analog zur Ausgestaltung der technischen Betrachtungsfelder, wie Netzwerk oder Infrastruktur, die Gestaltungsmöglichkeiten im Hinblick auf die IT-Organisation dargestellt. Den Ausführungen in den nachfolgenden Abschnitten liegt die Frage zugrunde: Wie können/müssen die IT-Prozesse ausgerichtet sein, um die notwendigen IT-Services in der geforderten Qualität liefern zu können?

ITIL verfolgt das Ziel der Standardisierung von Abläufen, um so Qualität, Sicherheit und Wirtschaftlichkeit von IT-Prozessen nachhaltig zu sichern und zu verbessern. Diese Zieldefinition ist weitestgehend deckungsgleich mit denen der Rahmenarchitektur Steuerung Bund (siehe http://www.cio.bund.de/SharedDocs/Publikationen/DE/Standards_und_Architekturen/rahmenarchitektur_itsteuerung_bund_grundlagen_download.pdf?__blob=publicationFile) und den Zielsetzungen des HV-Kompendiums für die Gestaltung hochverfügbarer IT-Architekturen (siehe HV-Kompendium, Band G, Kapitel 1 „Einführung“).

Nicht immer ist es möglich und notwendig eine umfassende Prozessstruktur zu implementieren, wie sie für das IT-Service-Management in ITIL v3 dargestellt ist. Die Herausforderung für die

Verantwortlichen besteht darin, dass einerseits mit den gegebenen Ressourcen der Service-Lebenszyklus funktional abgebildet wird und andererseits entsprechend der gewichteten Anforderungen an die IT-Services entsprechende Akzente für Kernbereiche der Prozesslandschaft gesetzt werden. Eine adäquate Konzentration auf Kernbereiche bei vorausgesetzt hohen Anforderungen an die Verfügbarkeit erfolgt im nächsten Kapitel.

2 Zentrale Standards zur Förderung und Optimierung der Verfügbarkeit

Für die Bestimmung der Verfügbarkeit fördernden Indikatoren wurden zunächst zentrale Prozessgebiete und Aktivitäten zur Optimierung der Verfügbarkeit aus dem Spektrum vorliegender Standards (CobiT/ITIL/BSI-Standards) identifiziert und bewertet. Dabei sind unbestreitbar die BSI-Standards 100-1 bis 100-4 durchgängig anzuwenden. Für die Bedeutung einzelner Prozessgebiete nach CobiT bzw. ITIL für einen verlässlichen und nachhaltigen IT-Betrieb wurde ein Potentialwert je Prozessgebiet ermittelt und in ein Ranking im Sinne einer Optimierung des Verfügbarkeitspotentials überführt. Dabei wurden die nachstehenden Prozessgebiete identifiziert, die sich besonders förderlich auf die Verfügbarkeit auswirken. Unter Berücksichtigung des ITIL/CobiT-Mappings fasst die folgende Tabelle das Ergebnis zusammen:

Rang	*Potential-wert*	*CobiT/ITIL-Prozessgebiete*
1	38,5	Assess & Manage IT-Risks
2	37,85	Service Desk&Incident Management
3	31	Manage Continuity
4	29,81	Manage Operations & Facility Management
5	28,5	Manage Service Agreements

Tabelle 1: Prozessgebiete CobiT/ITIL mit zentraler Bedeutung für die Verfügbarkeitsoptimierung

Zur Komposition von Architektur-Modellen in der IT-Organisationssäule sind aus dieser Basis Prozessgebiete i.S. von Vorgehensweisen und Aktivitäten abzuleiten, und bewertbare Indikatoren dazu zu bestimmen. Mit der getroffenen Auswahl wird im organisatorischen Bereich Priorität auf Prozesse gesetzt, von denen eine besondere Förderung des Verfügbarkeitspotentials zu erwarten ist. Die hier relevanten IT-Prozesse werden unter dem Begriff **IT-Operation** als Bestandteil von Architektur-Modellen in der IT-Organisationsarchitektur nachstehend beschrieben.

3 Umsetzung und Bewertung der relevanten Prozessgebiete

In diesem Absatz werden die im 2. Kapitel identifizierten Prozessgebiete einer genaueren Betrachtung unterzogen. Aus dem vorigen Abschnitt ergibt sich das folgende Bild für die Prozessgebiete, die für die Förderung der Verfügbarkeit die höchste Relevanz besitzen:

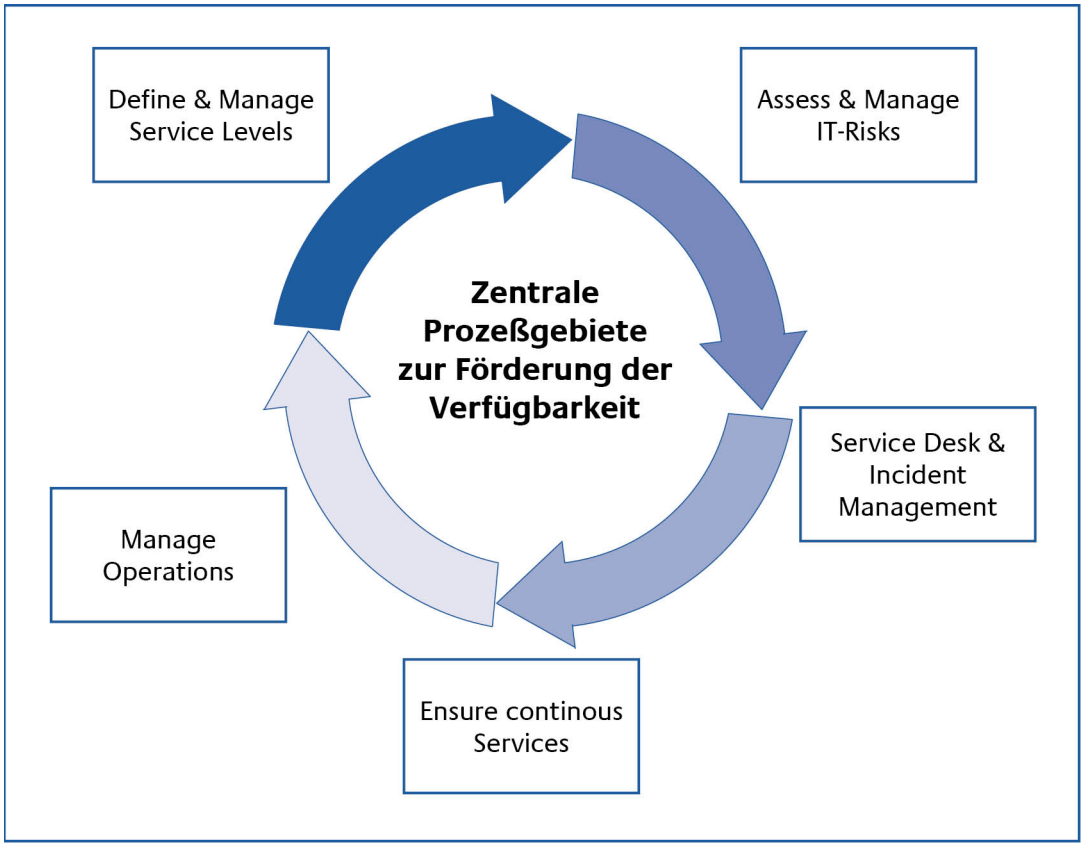


Abbildung 1: Przessgebiete mit hoher Relevanz für die Verfügbarkeit

Die Prozessgebiete werden nachstehend in der Reihenfolge ihres Einflusses auf die Verfügbarkeit dargestellt. Um eine Potentialbewertung zu ermöglichen, werden diese Prozessgebiete der Organisationsarchitektur über Entwicklungsstadien und Aktivitäten zur Steuerung und Kontrolle der Prozesse skaliert. Bei der Skalierung wird davon ausgegangen, dass sich Prozesse von einer initialen Ausgangslage zu einem optimierten Potenzial entwickeln. Zur Bestimmung der Organisationspotentiale wird die Prozessreife über Reifegrade analog CMMI[1] skaliert. Damit wird ein relativ einfaches, nachvollziehbares und aussagefähiges Werkzeug zur Bestimmung des IST-Zustandes geliefert. Der aktuelle Zustand eines konkreten Prozesses wird unter Nutzung spezifischer Attribute der Reife in einer Potenzialstufe dokumentiert.

1 CMMI(Capability Maturity Model Integration): http://de.wikipedia.org/wiki/Capability_Maturity_Model_Integration

3.1 Assess&Manage Risks

3.1.1 IT-Sicherheitsmanagement

Für das IT-Sicherheitsmanagement liegen mit den BSI-Standards 100-1 bis 100-3 ausführliche Beschreibungen vor. Standards der IT-Governance liefern ergänzende Beiträge z. B. durch die Beschreibung entsprechender Prozess-Gebiete (CobiT APO13, DSS04). Hier stehen die Steuerungs- und Managementaspekte im Vordergrund, während die BSI-Standards stärkeres Gewicht auf die Ausgestaltung legen. Für die Analyse und qualitative Bewertung der Organisationspotentiale werden an dieser Stelle der Entwicklungsstand des Security-Managements und die Integration vorliegender Standards als Indikatoren verwendet. Für die Bewertung wird vom Schutzbedarf als gesetzte Zielgröße ausgegangen. Danach ergibt sich nachstehendes Bewertungsschema für die Organisationspotentiale im Bereich IT-Security Management:

Gegenstand		*IT-Sicherheitsmanagement (ITSM)*				*Verweise*		
		Berücksichtigung der BSI-Standards 100-1, 100-2, 100-3, 100-4				Standards der IT-Governance		
Schutzbedarf				Normal	Hoch	Sehr hoch	Höchste Verfügbarkeit	Desaster tolerant
Potential-Stufe			1	2	3	4	5	
Reifegrad		0	1	2	3	4	5	
1	Sicherheits-Konzeption		100-1	100-2	Risikoanalyse nach 100-3	Notfallmanagement nach 100-4		
2	Ergänzende Standards				Vorgehen nach HV-Kompendium	Umsetzung der Steuerungsprinzipien nach CobiT/ITIL	Umsetzung der Optimierungsprinzipien nach CobiT/ITIL	
Verfügbarkeitsklasse			VK0	VK1	VK2	VK3	VK4	VK5

Tabelle 2: (IT-SM) Potential der IT-Security-Management-Prozesse

Die gelb hinterlegten Bereiche 1 und 2 beschreiben die Indikatoren für die Bewertung des Potentials der IT-Security-Management-Prozesse. Der Bereich 1 findet sich bei der Bewertung des Potentials des Risikomanagements wieder (siehe Tabelle 4). Der Bereich 2 ist ab Schutzbedarf hoch als Ergänzung bzw. Alternative anzusehen.

3.1.2 Identifikation der kritischen Geschäftsprozesse und Potentialabgleich

Kritische Geschäftsprozesse liefern die Anforderungen für die bereit zu stellende Service Qualität und das Risk Management. Die dazu notwendigen Erhebungen erfolgen im Vorgehensmodell des HV-Kompendiums in der Phase S. Die Professionalität der Anforderungserhebung und des Requirements Management muss den Anforderungen der Geschäftsprozesse entsprechen. Für die Bewertung des Organisationspotentials wird an dieser Stelle die Prozessreife der Erhebung und Bewertung der Anforderungen kritischer Geschäftsprozesse als Indikator benutzt.

Damit kann eine Bewertung der vorliegenden Potentiale für das Anforderungsmanagement über nachstehendes Reifegradmodell verwenden. An den höheren Potentialstufen ist zu erkennen, dass eine Verifikation der erhobenen Anforderungen stattfinden muss und eine Überführung in einen kontinuierlichen Verbesserungsprozess unumgänglich wird, um Verlässlichkeit und Nachhaltigkeit zu gewährleisten.

Anforderungsmanagement (AM)					
Bedarfserhebung durch Identifikation bedeutender Geschäftsprozesse nach Phase S1					
0 Non-existend	1 Bedarf informell bekannt	2 Bedarf systematisch erhoben	3 Potential der Architektur über Assessment erhoben & Bedarf dokumentiert und vereinbart	4 Potential nach Standard (HV-Assessment) bewertet & über Benchmark analysiert/ Bedarf als Anforderungen differenziert nach Utility und Warranty bewertet	5 Nachfrage-& Potentialanalyse als kontinuierlicher Prozess zur Steuerung & Optimierung von Core Services und Service Level Packages auf der Basis bewertbarer Indikatoren (IT-Service-Management)

Tabelle 3: (AM) Bewertung des Potentials des Anforderungsmanagements

Im Bewertungs-Modell wird Bedarf als konkretisierte Anforderungen an das Serviceportfolio verstanden. Der Reifegrad 1 entspricht z.B. einem angenommenen Bedarf, bei dem die Eignung des Serviceportfolios unterstellt wurde. Dies beschreibt typischerweise die Situation in Organisationen, in denen IT-Organisation dem Geschäftsbetrieb die zu nutzenden Services diktiert.

3.1.3 Risikomanagement

Der zentralen Bedeutung von Risiko-Management wird durch den BSI-Standard 100-3 Rechnung getragen. Für die Bewertung der im HV-Umfeld notwendigen Prozesse und Aktivitäten wurde in Phase I ein Reifegradmodell nach CobiT eingeführt. In CobiT findet man die entsprechenden Abschnitte in P09 (in der CobiT Version 5.0 im Abschnitt AP012[2]).

Die in ITIL präferierte Methode zu Durchführung der Risikobetrachtung ist Management of Risk (M_o_R) [MoR]. Die hier beschriebenen Aktivitäten wurden nach M_o_R entwickelt und an entsprechenden Stellen durch Aktivitäten weiterer Methoden und Standards ergänzt.

3.1.3.1 Festlegung des Risikokontext

Zunächst sollte festgelegt werden, für wen und für was das Risiko-Management Anwendung finden soll. Das Spektrum erstreckt sich von einem einzelnen Fachverfahren mit einer entsprechenden IT-Anwendung bis hin zu einer vollständigen Organisation mit Geschäftsprozessen und IT-Infrastruktur. Die Festlegung des Risikokontextes ist keine explizite Aktivität der Methode M_o_R. Der Kontext ist im Rahmen der ITIL-Umsetzung bereits durch Management-Prozesse aus dem Bereich Service Strategie und Service Design festgelegt.

Bei der Anwendung des BSI Standards 100-3 ist der Kontext bereits festgelegt. Da BSI 100-3 als konsequente Fortführung der Standards BSI 100-1 [BSI100-1] und BSI 100-2 [BSI100-2] betrachtet

2 In diesem Kompendium ist CobiT 4 berücksichtigt; inzwischen gibt es CobiT in der Version 5.0

werden muss, ist Kontext durch die Umsetzung von BSI 100-1 (Aufbau und Betrieb eines ISMS) bereits festgelegt. Die **Basiskriterien zur Risikobewertung** beinhalten den Standard 100-3 [BSI100-3] selbst. Im Zusammenhang mit Risiken, welche sich auf die Verfügbarkeit auswirken, sind insbesondere die elementaren Gefährdungen relevant.

Nach M_o_R beinhaltet diese Aktivität, Bedrohungen und Chancen im Zusammenhang mit einer Aktivität identifizieren, die Auswirkungen auf das von ihr angestrebte Ziel haben können.

Gemäß der ISO 27005 stellt diese Aktivität den ersten Teil der Risikoanalyse dar und umfasst die folgenden Punkte:

- Identifikation der Assets
- Identifikation von Bedrohungen und relevanten Gefährdungen
- Identifikation bereits realisierter Maßnahmen
- Identifikation von Schwachstellen
- Identifikation von Schadensauswirkungen

Bei der Erstellung eines IT-Sicherheitskonzeptes nach IT-Grundschutz (BSI 100-2) werden die Assets (IT-Strukturanalyse), Bedrohungen und bereits realisierte Maßnahmen (Modellierung und Basissicherheitscheck) und Schadensauswirkungen (Schutzbedarfsfeststellung) bereits im Vorfeld identifiziert. Die Risikobetrachtung erfolgt im Rahmen der Vorgehensweise der Risikoanalyse nach BSI 100-3. Wie bereits erwähnt sind hier die elementaren Gefährdungen besonders relevant, da diese vornehmliche Risiken für das Sicherheitsziel Verfügbarkeit verursachen. Für die Risiko-Betrachtung in diesem Kontext kann auf die Empfehlungen zu „Risikoanalysen mittels elementarer Gefährdungen“ zurückgegriffen werden, welche als Ergänzungen zum BSI-Standard 1[3]00-3 erschienen sind.

3.1.3.2 Bewerten

M_o_R führt eine Bewertung der identifizierten Bedrohungen im Vergleich zu den Chancen einer Aktivität durch und erstellt damit ein Risikoprofil, welches akzeptable und nicht akzeptable Risikoniveaus aufzeigt. Risiken, die das akzeptable Risikoniveau überschreiten, erfordern eine Risikoreaktion.

Auch die anderen Methoden und Standards führen eine Risikobewertung durch, um nicht akzeptable Risiken, die einer Behandlung bedürfen, zu ermitteln.

Häufig wird zu Beginn in der ersten Iteration des Prozesses eine qualitative Bewertung des Risikos durchgeführt und das Risiko in Form von linguistischen Skalen wie z. B. von „kein“ über „geringes“ bis hin zu „sehr hohem“ Risiko beschrieben. In späteren Iterationen werden meist quantitative Bewertungen durchgeführt. Sie beschreiben das Risiko als Multiplikation der Schadensauswirkungen mit den Eintrittswahrscheinlichkeiten. Wenn sich die Schadensauswirkungen noch relativ leicht beziffern lassen (z. B. im Rahmen einer BIA), so ist die Ermittlung der Wahrscheinlichkeiten nicht trivial und beruht dabei auf Zahlen aus der Vergangenheit. Im IT-Bereich ist aufgrund des sich schnell ändernden Umfeldes eine gewisse Unsicherheit mit der Extrapolation der Daten aus der Vergangenheit in die Zukunft verbunden. Diese Unsicherheit wird im HV-Umfeld häufig dadurch umgangen, dass der Eintrittswahrscheinlichkeit keine hohe Gewichtung zukommt und man eher davon ausgeht, dass die Bedrohung wirkt (und nicht nur wirken kann) und man entsprechend gewappnet sein will.

3 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

Zur Abschätzung des Risikoniveaus oder -Levels werden in den Standards verschiedene Methoden vorgeschlagen und angewendet. Die häufigst verwendeten Methoden sind:

- Szenario-Analysen
- Business Impact Analysis (BIA)
- Ursachenanalyse – Root Cause Analysis (RCA)
- Fehler- und Ereignisbaumanalysen - Fault Tree Analysis (FTA) und Event Tree Analysis (ETA)
- Ursache-Wirkungsanalyse
- Bow Tie Methode
- Brainstorming
- Checklisten

Der BSI-Standard 100-3 berücksichtigt die Eintrittswahrscheinlichkeiten hingegen gar nicht, vielmehr wird mittels Expertenwissen (Best Practices)festgestellt, inwiefern die Maßnahmen aus den GS-Katalogen den Gefährdungen vollständig entgegenwirken (Checklisten-Methode).

Ist das Risikoniveau, wenn auch mit gewissen Unsicherheiten bestimmt, erfolgt die Bewertung. Die Bewertung erfolgt durch den Abgleich der Risiken mit den Basiskriterien, welche im Kapitel 3.1.3.1 festgelegt wurden. Das Ergebnis ist eine Liste der Risiken, die priorisiert reduziert werden sollten.

3.1.3.3 Planen

Risiken, die eine Reaktion erforderlich machen, bedürfen einer geeigneten Behandlung und führen i. d. R. zu Maßnahmen, die das Risikoniveau auf ein akzeptables Maß reduzieren. Diese erfordert eine sorgfältige Planung und Priorisierung der Maßnahmenimplementierung.

Im Rahmen von M_o_R bedeutet dies die Vorbereitung einer Management-Reaktion, durch die die Bedrohung reduziert und die Chancen maximiert werden.

Die Standards stellen mehrere Alternativen zur Risikobehandlung bereit:

- Risikoreduzierung mittels Maßnahmenumsetzung
- Vermeidung von Risiken mittels Umstrukturierung
- Risikotransfer
- Risikoakzeptanz

Die Entscheidung für eine oder eine Kombination der vier Alternativen sollte auf der Risikobewertung (vgl. Kap 3.1.3.2) basieren und das Kosten-Nutzen-Verhältnis berücksichtigen.

Im HV-Umfeld sollte das Risiko mittels Maßnahmenumsetzung sowie durch Umstrukturierung reduziert werden.

3.1.3.4 Implementierung und Überwachung

Dieser Abschnitt betrachtet die Risikoreduzierung mittels Umsetzung von Maßnahmen. Die Implementierung von Maßnahmen hat von allen Alternativen die meisten Auswirkungen auf die Beteiligten und unterliegt deshalb einer Reihe von Einschränkungen. Die Einschränkungen resultieren häufig aus Zeitmangel, Geldmangel, Technikinkompatibilität, Einflüsse auf die Ge-

schäftsprozesse, Personalveränderungen und Wechselwirkungen der Maßnahmen untereinander. Im Rahmen der Implementierung sollten diese Einschränkungen umfassend berücksichtigt werden.

Insbesondere im HV-Umfeld kommt neben der Implementierung der risikoreduzierenden Maßnahmen der Überwachung eine besondere Bedeutung zu. Die implementierten Maßnahmen müssen in ihrer Effektivität überwacht werden und weitere korrigierende Maßnahmen werden ergriffen, wenn die Reaktion nicht den Erwartungen entspricht. Darüber hinaus sind im HV-Umfeld eine ständige Überwachung der Bedrohungen und eine Reduzierung der Restrisiken erforderlich. Die Restrisiken, die auch nach der Implementierung von Maßnahmen verbleiben, sowie die Risiken, die im Rahmen der Priorisierung in der ersten Iteration nicht behandelt werden, sollten durch weitere Iterationen minimiert werden.

3.1.3.5 Modell zur Bewertung der Prozesspotentiale im Risikomanagement

Entsprechend der Zielsetzung dieses HV-Kompendiums, zentrale Services zu identifizieren und zu bewerten, wurde für die Bewertung der Prozesspotentiale des Risikomanagements das nachstehende Bewertungsmodell entwickelt:

Gegenstand	*Risikomanagement (RM)*			*Verweise*	
	Berücksichtigung der BSI-Standards 100-1, 100-2, 100-3, 100-4			Standards der IT-Governance	
Potentialstufe	1	2	3	4	5
Sicherheits-Konzeption		100-1/100-2	Risikoanalyse nach 100-3 durch Vorgehen nach HV-Kompendium	Notfallmanagement nach 100-4	IT-Governance nach etablierten Standards umgesetzt
Entspricht in Tabelle RM	Stufe 1	Stufe 2	Stufe 3	Stufe 4	Stufe 5

Tabelle RM

Stufe	*Beschreibung*
1	IT-Risiken werden von den Verantwortlichen situationsbedingt in Projekten berücksichtigt. Der Risikokontext richtet sich nach Projektspezifika und punktuell betrachteten Systemeigenschaften. Einzelne Aktivitäten werden unabgestimmt von unterschiedlichen Rollen ausgeführt. Informelle Risikoeinschätzungen werden nicht durchgängig kommuniziert. Bei den Verantwortlichen besteht ein wachsendes Bewusstsein dafür, dass IT-Risiken wichtig sind und berücksichtigt werden müssen.
2	Die Risiko-Betrachtung geschieht immer noch anlassbezogen, aber durch die Vorgehensweise nach IT-Grundschutz sind Standardrisiken abgedeckt, kritische Geschäftsprozesse sind nicht identifiziert. Die Aktivitäten zur Risikoeinschätzung erfolgen nach einem grob spezifizierten Ablaufplan. Einzelne IT-Ereignisse werden einer Risikobeurteilung zugeführt. Bei wesentlichen Projekten werden Risiken vom Projektmanager betrachtet.

Gegenstand	*Risikomanagement (RM)*	*Verweise*
3	Kritische Geschäftsprozesse sind identifiziert die für den Schutzbedarf hoch erforderlichen technischen und organisatorischen Maßnahmen nach IT-Grundschutz sind umgesetzt. Alle Aktivitäten, wie Einschätzung und Verwaltung von Risiken, erfolgen nach etablierten Standardverfahren. Der Risikomanagement-Prozess wird von der oberen Management-Ebene gesteuert, die auch die Verantwortung für das IT-Risikomanagement hat. Das Risiko wird in IT-Projekte und auch im Hinblick auf den IT-Gesamtbetrieb eingeschätzt und reduziert. Identifizierte Risiken werden mittels standardisierter Werkzeuge kommuniziert und den Verantwortlichen zugängig gemacht. Das Management ist daher jederzeit in der Lage, die Risikoposition zu überwachen und auf aktueller Datenbasis (HV-Assessment) Entscheidungen zu treffen. Die identifizierten Risiken haben einen zugewiesenen Eigentümer (Service-Verantwortlicher), der aufgrund der eigenen Kenntnisse und durch Unterstützung interner Experten angemessen reagieren kann. Es liegen standardisierte Metriken zur Risikoeinschätzung und Definition vor.	
4	Der 100-4 des BSI ist umgesetzt. Alle Aktivitäten, wie Einschätzung und Verwaltung von Risiken, erfolgen nach etablierten Standardverfahren. Der Risikomanagement-Prozess wird von der oberen Management-Ebene gesteuert, die auch die Verantwortung für das IT-Risikomanagement hat. Das Risiko wird in IT-Projekte und auch im Hinblick auf den IT-Gesamtbetrieb eingeschätzt und reduziert. Identifizierte Risiken werden mittels standardisierter Werkzeuge kommuniziert und den Verantwortlichen zugängig gemacht. Das Management ist daher jederzeit in der Lage, die Risikoposition zu überwachen und auf aktueller Datenbasis (HV-Assessment) Entscheidungen zu treffen. Die identifizierten Risiken haben einen zugewiesenen Eigentümer (Service-Verantwortlicher), der aufgrund der eigenen Kenntnisse und durch Unterstützung interner Experten angemessen reagieren kann. Es liegen standardisierte Metriken zur Risikoeinschätzung und Definition vor.	
5	Umsetzung von Standards der IT-Governance auf der Basis von CobiT oder ITIL Dies bedeutet: Der gesamte Prozess des Risiko-Managements wird kontinuierlich optimiert und somit die Qualität der Services verbessert. Best Practices werden in der gesamten Organisation angewendet. Das Aufzeichnen, Analysieren und Berichten von relevanten Kennwerten wird mit Prozess-übergreifenden Werkzeugen realisiert und überwiegend automatisiert. Erfahrungen im Bereich des Risiko-Managements werden regelmäßig ausgetauscht. Das Risikomanagement ist in allen Ebenen der Organisation integriert und akzeptiert. Das Management bewertet kontinuierlich Strategien zur Risikoreduktion. Die Ergebnisse aus dem HV-Assessment werden mit denen anderer Organisationen verglichen (HV-Benchmarking). Externe und Branchenexperten werden konsultiert.	

Tabelle 4: (RM) Bewertung des Potentials des Risikomanagements

3.2 Service Desk und Incident Management

Das Incident Management weist als Schnittstelle zwischen Kunden und Service Management eine hohe Wirkung auf Verfügbarkeit aus. Professionalität und Geschwindigkeit der Reaktion im Falle von Service-Beeinträchtigungen oder Ausfällen sind prägende Merkmale für ein leistungsfähiges und effizientes Incident-Management (ITIL unter Service Operations 4.2, CobiT DSS02[4]). Neben der betriebswirtschaftlichen Bedeutung, Verletzungen der SLAs zu vermeiden und damit die Vereinbarungen zu erfüllen, wird durch diese Prozesse besonders die Verlässlichkeit von Services gefördert. Dabei steht die Minimierung des MTTR-Wertes im Vordergrund.

Eine wichtige Rolle bei der Reduzierung der Ausfallzeiten spielt der Service Desk (vgl. ITIL Organizing for Service Operation 6.2) als einzige Anlaufstelle, die professionelle Erfassung der Incidents sowie deren geeignete Klassifizierung und Priorisierung. In der Regel wird hierfür ein Ticketing-System oder ein ITSM-Tool eingesetzt. Nach der Registrierung werden die Tickets einer Produktkategorie (Kategorisierung) zugeordnet. Eine CMDB erleichtert die Zuordnung der Störung zu einem IT-Service bzw. einem CI. Die Analyse der gespeicherten Daten eine schnelle Abhilfe im First Level Support oder die Zuweisung von Incidents zu Eskalationsstufen bzw. deren Zuführung zu Lösungen. Hier zeigt sich die Qualität der Vorsorge. Auch das Triggern abhängiger Prozesse und das Erfassen von Bearbeitungszeiten liefern weiteren Prozessen (z. B das Service-Design) wertvolle, aussagekräftige Verfügbarkeitswerte und somit Planungsinformationen und zeigen Optimierungspotenzial auf.

3.2.1 Aktivitäten

Sämtliche HV-relevanten Aktivitäten des Incident Management Prozesses werden durch den Service Desk initiiert und gesteuert. Der Service Desk stellt eine funktionale Einheit dar und sollte innerhalb einer Organisation die einzige und zentrale Anlaufstelle (Single Point of Contact, SPoC) für IT-Anwender und IT-Administratoren sein.

Die wichtigsten Aktivitäten des Service Desk stellen sich wie folgt dar:

3.2.1.1 Identifizierung

Der Incident Management Prozess startet i. d. R. erst nach dem Auftreten eines Incidents. Im HV-Umfeld ist es nicht akzeptabel, mit dem Start des Prozesses solange abzuwarten, bis die Anwender die Auswirkungen eines Incidents spüren und diese Auswirkungen beim Service Desk melden. Die Incident-Identifizierung sollte bereits im Rahmen des Event Managements Prozesses erfolgen und Events so frühzeitig erkennen, dass der Incident Management Prozess schnell gestartet werden kann, bevor diese Auswirkungen für die Anwender haben.

3.2.1.2 Erfassung

Ganz gleich, ob ein Incident durch einen Anruf eines Anwenders, per E-Mail, per Web-Oberfläche eines Ticket-Systems oder durch eine automatisch generierte Alarmmeldung durch das Event Management beim Service Desk gemeldet wird, müssen alle Incidents erfasst werden. Alle den Incident betreffenden relevanten Informationen werden in einem sogenannten Incident Record dokumentiert. Der Incident Record beinhaltet darüber hinaus die gesamte Historie, vom Eingang der Meldung bis hin zum Abschluss des Incidents.

4 Abscnittbezeichnung in der CobiT Version 5.0

3.2.1.3 Kategorisierung

Im Rahmen der Erfassung eines Incidents wird dieser kategorisiert. Kategorisierung bedeutet in diesem Zusammenhang eine Beurteilung der Art des Incidents. Ist z. B. die Hardware betroffen oder handelt es sich um ein Softwareproblem. Diese Kategorisierung ist insbesondere im HV-Umfeld wichtig, um zeitnah entsprechende Support-Gruppen zu involvieren.

3.2.1.4 Priorisierung

In Abhängigkeit der Auswirkungen oder der potentiell möglichen Auswirkungen eines Incidents muss die Dringlichkeit der Behandlung festgelegt werden. Im HV-Umfeld ist davon auszugehen, dass alle Incidents, die zu einer Unterbrechung des Services führen, einer sofortigen Behandlung bedürfen. Bei einer Häufung von Incidents müssen i d. R. aufgrund von Ressourcenengpässen auch innerhalb der dringlich zu behandelnden Incidents Priorisierungen durchgeführt werden. Dabei sind nicht nur die geschäftlichen Auswirkungen zu betrachten, sondern häufig im HV-Umfeld auch Auswirkungen für Leib und Leben.

Häufig werden die Incidents mit den schwersten Auswirkungen für die Organisation oder mit Auswirkungen, die Leib und Leben bedrohen, als Major Incidents bezeichnet. Für solche Major Incidents können spezielle Verfahren zur Behandlung definiert werden. Diese Verfahren weichen oft dahingehend von der Standardbehandlung ab, dass in Abhängigkeit des Incidents dynamisch ad hoc Major Incident Teams gebildet werden. Die Major Incident Teams bestehen in der Regel aus IT-Managern und technischen Experten, und stehen normalerweise unter der Führung des Incident Managers. Die Incident Teams werden einberufen, um gemeinsam eine Lösung für einen Major Incident zu erarbeiten. Innerhalb einer IT-Architektur bestehen häufig Abhängigkeiten zwischen den verwendeten Komponenten. Beispielsweise können Anwender Anwendungen in ihrem Netz nicht nutzen, wenn die dafür notwendige Domänenverwaltung nicht zur Verfügung steht. Im Rahmen der Priorisierung müssen Abhängigkeiten dahingehend berücksichtigt werden, dass im Falle eines Wiederanlaufes die Komponenten in der richtigen, geregelten Reihenfolge wieder anlaufen. Im Fall des o. g. Beispiels sollte daher zunächst die Domänenverwaltung wiederhergestellt werden und dann nachfolgend die einzelnen Anwendungen.

3.2.1.5 Lösung

Eine wesentliche Aufgabe des Service Desk ist die „Erste Diagnose“. Der Service Desk soll in erster Linie, sofern die Meldung auf diesem Weg eingeht, während des Anrufs eines Anwenders eine erste Diagnose durchführen und wenn möglich bereits an dieser Stelle schon geeignete Maßnahmen einleiten. Häufig werden vom Service Desk Workarounds als erste Maßnahmen zur Reduzierung der Auswirkungen bereitgestellt.

Werden Incidents via E-Mail oder Web-Oberfläche eines Ticket-Systems gemeldet, können Anwender eine Kategorisierung und Priorisierung selbst durchführen. Aufgrund der Kategorisierung kann eine entsprechende Rückmeldung automatisch erfolgen und ggf. einen entsprechenden Workaround vorschlagen. Werden hingegen durch das Event Management Alarmmeldungen automatisch generiert, bestehen z. B. die Aufgaben des Service Desk im HV-Umfeld darin, Diagnose- und Korrekturskripte auszuführen oder den Neustart eines Systems zu veranlassen (vgl. Kapitel Überwachung [BSI HV-Komp Band B 2013]).

Im HV-Umfeld sollten in der IT-Architektur bereits automatisierte Maßnahmen vorgesehen sein, die Serviceunterbrechungen verhindern. Dazu zählt beispielsweise die automatisierte Aktivierung von Redundanzen im Rahmen von Komponentenausfällen. In diesem Fall werden der Ausfall sowie die Redundanzaktivierung als Event gemeldet. Auch ohne Serviceunterbrechung ist dieses im HV-Umfeld ein Incident, da die Gesamtverfügbarkeit des Systems im Sinne des Verfügbarkeits-

potenzials beeinträchtigt ist. Der Service Desk muss den Wiederanlauf der ausgefallenen Komponente veranlassen.

Kann der Incident im Rahmen der ersten Diagnose oder ohne Unterstützung von Support-Gruppen nicht gelöst werden, muss der Incident sofort für weiteren Support eskaliert werden.

3.2.1.6 Eskalation

ITIL unterscheidet zwei Arten der Eskalation. Zum einen die „Funktionale Eskalation“ zur Einbindung weiterer Support-Gruppen und zum zweiten die „Hierarchische Eskalation“ bei schwerwiegenden Ereignissen, die eine Involvierung des IT-Management erfordern.

Muss im HV-Umfeld funktional eskaliert werden, müssen die weiteren Support-Gruppen zeitnah einsatzbereit sein. Eine Organisation im HV-Umfeld muss aufgrund der zeitlichen Anforderungen über eine eigene „Second-Level“ Support-Gruppe verfügen. Gegebenenfalls sind zur Behandlung von Ereignissen auch die Mitarbeiter des IT-Betriebes, wie z. B. Operator, Schichtleiter oder IT Operations Manager einzubeziehen.

Mittels Second-Level Support wird im HV-Umfeld das manuelle Eingreifen realisiert. Dies ist erforderlich, wenn Ereignisse aufgetreten sind, die sich durch automatische Reaktionen (z. B. vgl. Failover-Verfahren in Clustern [BSI HV-Komp II 2009]), bedingt durch die Fehlerart nicht automatisiert korrigieren lassen. Hierzu zählen u. a. Totalausfälle von Systemen aufgrund von Hardware- oder Software-Problemen.

Die klassischen „Third-Level“ Support-Gruppen sind im HV-Umfeld häufig nur im Bereich der geplanten Wartung oder im Rahmen der Hardware-Wiederbeschaffung zu finden. Eine Eskalation zum Third-Level Support ist im HV-Umfeld mit den vorherrschenden Dringlichkeitsanforderungen nicht vereinbar. Dementsprechend muss der Second-Level Support den Anforderungen genügend fachlich und organisatorisch aufgestellt sein. Die Regeln für die Eskalation und Bearbeitung müssen in Form von OLAs mit der internen Support-Gruppe vereinbart werden.

Können Incidents innerhalb der vorgegeben Zeit nicht gelöst werden, oder sind die Auswirkungen der Incidents so schwerwiegend, dass SLAs nicht eingehalten werden, muss hierarchisch eskaliert werden. Gegebenenfalls muss das Management zur Behandlung des Incidents weitere Ressourcen bereitstellen. Insbesondere ist im HV-Umfeld zu prüfen, inwiefern zur weiteren Behandlung des Incidents Notfallmaßnahmen (vgl. Continuity Management) zu ergreifen sind.

3.2.1.7 Incident-Abschluss

Nach der Behandlung eines Incidents muss der Service Desk überprüfen, ob der „Normalzustand“ wiederhergestellt ist, ob dieses in dem dafür vorgesehenen Zeitraum erfolgt ist, ob die Dokumentation vollständig ist und ob es sich um ein wiederkehrendes Ereignis gehandelt hat. Insbesondere im HV-Umfeld müssen bei wiederkehrenden Ereignissen präventive Maßnahmen ergriffen werden. Ferner sollten mit dem Problem Management Maßnahmen initiiert werden, die zukünftige Auftritte dieser Ereignisse verhindern. Ist keine ursächliche Störungsbeseitigung möglich, wird der Incident zur weiteren Bearbeitung an das Problem Management übergeben.

3.2.1.8 Modell zur Bewertung der Prozesspotentiale im Service Desk und Incident Management

Mit den Abläufen im Service Desk und Incident Management sind weitere Prozesse identifiziert, die einen zentralen Beitrag zur Förderung der Verfügbarkeit und der Verlässlichkeit liefern. Die vorliegenden Prozesspotentiale werden in diesem Kompendium über das nachstehende Bewertungsmodell bewertbar gemacht:

– Service Desk & Incident Management (SDIM) –					Verweise
Umsetzung der Prozesse im Service Desk und Incident Management;			CobiT DS8 (V5 DSS02) ITIL Band4		
0 Non-existend	1 Initial	2 Repeatable	3 defined	4 Managed & measurable	5 Optimized
Entspricht in Tabelle SDIM	Stufe 1	Stufe 2	Stufe 3	Stufe 4	Stufe 5

Tabelle SDIM	
Stufe	***Beschreibung***
1	Die Ansprechstelle für Kunden/Nutzer in der Organisation liegt in der Verantwortung der IT-Administration und es wird davon ausgegangen, dass der Support von den Administratoren geleistet wird. Eine Überwachung der Anfragen findet nicht statt. Bei auftretenden Incidents an den Systemen wird aus der Situation heraus reagiert.
2	Die Notwendigkeit der Benutzerunterstützung ist erkannt und Verantwortlichkeiten zur Unterstützung und zum Incident-Handling sind geregelt. Wie die Mitarbeiter des SD mit Anfragen und Ereignissen umgehen, bleibt weitgehend deren Qualifikation Initiative überlassen.
3	Eine Anlaufstelle für Nutzeranfragen ist ausgewiesen und Verfahren zur Benutzerunterstützung und zum Incident-Handling sind mit Eskalationswegen definiert. Die Verantwortlichkeiten SD, 2nd Level und 3rd Level Support sind eindeutig zugewiesen. Eine Anfrage- & Ereignisdokumentation ist eingerichtet und kann nachverfolgt werden. Die Mitarbeiter sind eingewiesen und entsprechend geschult. Der Baustein B 1.8 Behandlung von Sicherheitsvorfällen ist umgesetzt.
4	Für die Benutzerunterstützung wurde eine eigene Funktions-/Organisationseinheit eingerichtet. Für die Bearbeitung von Anfragen und Ereignissen steht eine Tool-Unterstützung zur Verfügung und die Bearbeitung und Lösung wird regelmäßig bewertet und überwacht. Verfahren für die Kommunikation, Eskalation und Lösung von Ereignissen in Zusammenwirken mit anderen Prozessgebieten sind definiert. Das Personal wird nach den Zielvorgaben regelmäßig geschult.
5	Bearbeitungsstände werden ständig kontrolliert und festgestellte Ereignisse den Prozessen Event & Incident Management zugeführt. Abhängige Prozesse werden rechtzeitig getriggert (z.B. Problem/Change Management). Die Prozesse werden über Indikatoren gesteuert und an einer Zielstellung (Benchmark) überwacht. Abweichungen werden in einem ständigen KVP korrigiert.

Tabelle 5: (SDIM) Bewertung des Potentials für Service Desk und Incident Management

3.3 IT-Service Continuity Management

Mit dem Prozess **IT-Service Continuity Management** wird ein weiterer bedeutender IT-Service zur Förderung der Verfügbarkeit zur Verfügung gestellt. Es ist definiertes Ziel, im Falle eines Schadenseintritts den schnellstmöglichen Wiederanlauf der Prozesse und Services zu ermöglichen und Auswirkungen von Katastrophen proaktiv vorzubeugen. Betrachtet werden schwerwiegende Katastrophenszenarien z.B. den Ausbruch eines Feuers im Rechenzentrum und es sind angemessene Maßnahmen zu treffen, die genau in einer solchen Situation greifen, um die Verfügbarkeit sicherzustellen. Der zentralen Bedeutung von IT-Service Continuity Management wird durch Anwendung des BSI-Standards 100-4 „Notfallmanagement“ Rechnung getragen. Die nachstehenden Ausführungen fassen die Darstellungen aus diesem Standard aus den Kapiteln 4 bis 9 zusammen. Diese sollten für die Ausgestaltung der Prozesse des IT-Service Continuity Management bereits ab dem Verfügbarkeitsbedarf „hoch“ herangezogen werden.

3.3.1 Erstellen einer ITSCM-Richtlinie

In der Initiierungsphase des ITSCM-Prozesses müssen in Form einer Richtlinie die Intention, die Ziele und die Verantwortlichkeiten festgelegt werden. Die Richtlinie muss mindestens allen Mitgliedern der Organisation, die sich mit Business Continuity befassen, bekannt gegeben werden.

3.3.2 Business Impact Analyse (BIA)

Im Rahmen der Business-Auswirkungsanalyse (Business Impact Analysis, BIA) werden die Auswirkungen eines Ausfalls eines IT-Service auf das Business quantifiziert. Neben den direkten finanziellen Schäden müssen darüber hinaus Schäden wie Image-Schäden, Moral-beeinträchtigungen, Auswirkungen auf Leib und Leben, Verlust der Handlungsfähigkeit oder Verlust von Wettbewerbsvorteilen in der BIA Berücksichtigung finden.

Die BIA ist im HV-Umfeld das geeignete und wichtigste Instrument, die Auswirkungen von Ausfällen von IT-Services auf das Business zu ermitteln. Die BIA ermöglicht, Prozesse oder Services mit frühen und erheblichen Auswirkungen zu identifizieren, für die vorrangig präventive Maßnahmen ergriffen werden sollten. Für Prozesse oder Services mit geringfügigen oder zeitlich verzögerten Auswirkungen sollte hingegen der Schwerpunkt auf Wiederherstellungsmaßnahmen gelegt werden.

3.3.3 Risikoanalyse (RA)

Die Risikoanalyse befasst sich mit der Bewertung von Risiken, die zu Serviceunterbrechungen oder Sicherheitsverletzungen führen können. Aufgabe der Risikoanalyse ist die Risikoidentifizierung und Risikobewertung. Dabei werden potentielle Bedrohungen für die Kontinuität ermittelt und es wird festgestellt, wie hoch die Eintrittswahrscheinlichkeit der realen Bedrohung ist.

Die Risikoanalyse entwickelt darüber hinaus Maßnahmen zum Umgang mit den identifizierten Bedrohungen unter Berücksichtigung des Kosten-Schaden-Verhältnisses.

Für die Risikoanalyse und das Risikomanagement stehen eine Reihe von Methoden zur Verfügung. Zur Bewertung und zum Management der Risiken sollte eine Standardmethodik angewendet werden.

3.3.4 ITSCM-Strategie entwickeln

Das IT-Service Continuity Management (ITSCM) erstellt eine ITSCM-Strategie, die in die allgemeine Business Continuity Management (BCM)-Strategie integriert werden muss. Durch die

ITSCM-Strategie wird abgeleitet aus der BIA und der RA ein optimales Gleichgewicht zwischen der Risikoreduzierung und der Wiederherstellung hergestellt.

Bei Services, bei denen laut BIA Ausfälle kurzfristig größere Auswirkungen nach sich ziehen, konzentrieren sich die Maßnahmen auf Methoden der präventiven Risikoreduzierung z. B. durch Fehlertoleranz, Redundanz oder Maßnahmen zum Schutz der Infrastruktur. Die Kapitel 1 bis 11 des HV-Kompendiums [BSI HV-Komp Band B 2013] beinhalten Prinzipien und Techniken, die zur Risikoreduzierung geeignet sind.

Die BIA im HV-Umfeld wird sicherlich die Mehrzahl der IT-Services als kritisch einstufen und zwangsläufig wird das Hauptaugenmerk auf der präventiven Risikoreduzierung liegen. Doch trotz noch so guter Planung können letztlich nicht alle Risiken (Restrisiken) beseitigt werden. Dieser Fall wird auch als (IT-)Notfall bezeichnet. Im HV-Umfeld gilt allgemein, dass Wiederherstellungsmaßnahmen nur als letztes Mittel eingesetzt werden sollten. Beispielsweise wird im Rahmen hoher Verfügbarkeitsklassen auch die Desastertoleranz gefordert. Dies hat zur Folge, dass auch katastrophale Ereignisse in die präventive Risikoreduzierung (z. B. Ausweichrechenzentrum) einbezogen werden müssen.

Bei Ausfällen, die nur geringe Auswirkungen haben, sind umfassende Wiederherstellungsoptionen geeigneter. Beispiele für klassische Wiederherstellungsmaßnahmen sind die s. g. Standby-Varianten „Cold“, „Warm“ und „Hot“. Letztlich stellen aber auch diese Varianten Maßnahmen präventiver Risikoreduzierung dar, da die Standy-Komponenten präventiv bevorratet werden müssen, deren Aktivierung (bei Cold- und Warm-Standby) jedoch einen längeren Zeitraum in Anspruch nimmt.

Darüber hinaus existieren Mischformen der o. g. Strategien. Beispielsweise können bei Ausfällen, die kurzfristig nur geringe Auswirkungen haben, Komponenten die eine große Wiederherstellungszeit haben, im Cold- oder Warm-Standby betriebsbereit bevorratet werden. Die Komponenten, die in kurzer Zeit wiederhergestellt werden können, werden kurzfristig wiederbeschafft. Klassisches Beispiel ist die Bereitstellung einer Ausweichfläche mit entsprechender Infrastruktur, die IT-Komponenten werden jedoch bei Bedarf kurzfristig beschafft.

3.3.5 ITSCM-Pläne erstellen

Ist die ITSCM-Strategie durch das Management der Organisation genehmigt und verabschiedet, müssen ITSCM-Pläne in Abstimmung mit den Business Continuity Plänen (BCP) entwickelt werden. Die ITSCM-Pläne enthalten alle notwendigen Informationen, damit die in der RA ermittelten kritischen Komponenten für das Business aufrechterhalten bleiben oder im Rahmen eines IT-Notfalls innerhalb der maximal tolerierbaren Ausfallzeit wieder hergestellt werden können.

Der wichtigste ITSCM-Plan ist der Wiederherstellungsplan. In diesem Plan müssen alle Details zur Wiederherstellung der IT-Services nach einem IT-Notfall vollständig dokumentiert werden. Die Details sollten so dokumentiert sein, dass eine Person mit entsprechender Fachkunde in der Lage ist, den Anweisungen zu folgen, auch dann, wenn die Person mit der entsprechenden Komponente nicht vertraut ist.

Darüber hinaus existieren häufig weitere Pläne, die den Wiederherstellungsplan ergänzen und in die BCP integriert werden müssen:

- Notfallreaktionsplan
- Schadensfeststellungsplan
- Rettungsplan

- Aufzeichnungsplan
- Krisenmanagement- und Public Relation-Plan
- Unterbringungs- und Serviceplan
- Sicherheitsplan
- Personalplan
- Kommunikationsplan
- Finanz- und Verwaltungsplan

Zur Erhaltung der Aktualität der ITSCM-Pläne müssen diese gepflegt werden. Ändern sich bspw. die Anforderungen aus dem Business (BIA) oder sind neue Risiken (RA) aufgetreten, müssen die Pläne entsprechend aktualisiert werden. Ferner können aufgrund von Tests (vgl. Kapitel 3.3.6) Erkenntnisse gewonnen werden, die eine Anpassung der ITSCM-Pläne notwendig werden lassen.

Die erstellten ITSCM-Pläne müssen an die zuständigen Mitarbeiter verteilt werden. Um sicherzustellen, dass diesen immer die aktuellen Versionen zur Verfügung stehen, sollten die Pläne durch das Change Management kontrolliert und durch das Configuration Management verwaltet werden.

3.3.6 Testen

Wiederherstellungspläne müssen getestet werden. Der Test ist die einzige Möglichkeit, sicherzustellen, dass die Strategie, Standby-Szenarien und die damit verbundene Logistik in der Praxis funktionieren. Die Tests sollten so realistisch wie möglich und in definierten Testszenarien beschrieben sein. In der Regel können im HV-Umfeld Tests nicht vollumfänglich durchgeführt werden. Gründe dafür sind beispielsweise, dass der reguläre Betrieb durch den Test zu stark beeinträchtigt wird oder durch den Test herbeigeführte Serviceunterbrechungen zu Gefahren für Leib und Leben führen.

Um im HV-Umfeld die o. g. Problematik zu umgehen, sollten Tests in einer Simulationsumgebung durchgeführt werden. Dabei ist es möglich, im Rahmen von Teil-, Vollumfassenden- oder Szenariotests die Wiederherstellung von IT-Services zu testen, ohne in den laufenden Betrieb einzugreifen.

3.3.7 Weiterbildung, Bewusstsein und Schulung

Mittels Weiterbildungen und Schulungen muss sichergestellt werden, dass sich alle Mitarbeiter der Bedeutung der Business- und IT-Service-Continuity bewusst sind. Die betroffenen Mitarbeiter müssen durch regelmäßige Schulungen in die Lage versetzt werden, im Ereignis- oder Katastrophenfall alle erforderlichen Maßnahmen zu ergreifen. Ferner müssen alle betroffenen Mitarbeiter über ihre Rollen und Verantwortlichkeiten informiert sein.

3.3.8 Auslösen

Die Entscheidung, einen Plan auszulösen, muss schnell aber mit Sorgfalt geschehen. Zum einen darf keine wertvolle Zeit verloren gehen, die aufgrund von verzögerter Auslösung dem Wiederherstellungsteam zur Wiederherstellung fehlt. Zum anderen darf nicht leichtfertig ein Plan ausgelöst werden, der den laufenden Betrieb stört oder ggf. zu erheblichen Kosten führt.

Bereits im Vorfeld sollte ein Auslöseprozess definiert werden, der die folgenden Aspekte zur Entscheidungsfindung betrachtet:

- Ausmaß des Schadens

– voraussichtliche Dauer der Unterbrechung
– Nichtverfügbarkeit von Gebäuden und Räumen
– Auslösezeitpunkte mit den zugehörigen Business-Auswirkungen

Im HV-Umfeld muss der Auslöseprozess Handlungsanweisungen beinhalten, wie die o. g. Aspekte zu bewerten sind, um eine Entscheidung, den Plan auszulösen, herbeizuführen.

3.3.9 Reifegradmodell

Ergänzend zu den Ausführungen aus dem BSI-Standard 100-4 wird nachstehend aus der Gesamtschau der Aktivitäten für das Prozessgebiet Service Continuity Management das nachstehende Modell für die Potentialbewertung geliefert, um die Professionalität der unterstützenden IT-Prozesse in diesem Bereich bewertbar zu machen:

Service-Continuity Management (SCM)				*Verweise*	
Prozesse des Business- und Service-Continuity Management Reifegrade				CobiT DS4 (V5 DSS04) ITIL Band 2	
0 Non-existend	1 Initial	2 Repeatable	3 defined	4 Managed & measurable	5 Optimized
Tabelle SCM	Stufe 1	Stufe 2	Stufe 3	Stufe 4	Stufe 5

Tabelle SCM

Stufe	*Beschreibung*
1	Bei unvorhergesehenen Unterbrechungen wird aus der Situation heraus reagiert. Die einzige Vorbereitung besteht in einer Datensicherung.
2	Der Baustein B 1.4 Datensicherungskonzept ist umgesetzt. Es bestehen in den Abteilungen Verantwortlichkeiten und Verfahrensweisen zur Prävention von Ausfällen. Die Datensicherung umfasst die wesentlichen Datenbestände, das Wiedereinspielen der Daten nach Ausfällen hat bislang funktioniert.
3	Der Baustein B 1.3 Notfallmanagement ist umgesetzt und es wurde ein Notfallvorsorgekonzept entwickelt. Danach sind Verantwortlichkeiten aktuell und eindeutig zugewiesen, die erforderlichen technischen und organisatorischen Maßnahmen sind umgesetzt. Datensicherung und das Wiederanlaufen erfolgen nach festgelegten Regeln und Prioritäten. Die Mitarbeiter sind eingewiesen und entsprechen geschult. Übungen zur Feststellung der Erfüllung der Anforderungen finden regelmäßig statt.
4	Es wurde ein Service Continuity Plan auf der Basis des BSI 100-4 entwickelt. Der Service Continuity Plan(SCP) wird regelmäßig gepflegt, Es findet eineÜberwachung aller existentiellen Systemkomponenten statt, die erhobenen Ist-Daten werden mit den Soll-Vorgaben abgeglichen. Die Überwachung der Anforderungen, die Feststellung des Service-Delivery sowie die Datensicherung sind eingebettet in einen übergeordneten IT-Sicherheitsmanagementprozess. Es erfolgt eine automatisierte

Service-Continuity Management (SCM)	*Verweise*
	Wiederherstellung von Services. Übungen bestätigen die Wiederherstellung in der vorgegebenen Zeit. Für das SCM steht eine TOOL-Unterstützung zur Verfügung. Das Personal wir regelmäßig nach den Zielvorgaben geschult.
5	Systemzustände werden ständig kontrolliert und festgestellte Ereignisse den Prozessen Event & Incident Management zugeführt. Abhängige Prozesse werden rechtzeitig getriggert (z.B. Problem oder Change Management). Die Prozesse werden über KPIs gesteuert und an einer Zielstellung (Benchmark) überwacht. Abweichungen werden in einem ständigen Kontinuierlichen Verbesserungsprozess (KVP) korrigiert.

Tabelle 6: (SCM) Bewertung des Potentials der Notfallvorsorge

3.4 Manage Operations & Facility Management

Professioneller Betrieb der IT-Komponenten, die Unterhaltung der IT-Infrastruktur sowie die Bereitstellung einer geeigneten Betriebsumgebung sind unabdingbare Voraussetzung für hochverfügbare IT-Services. Zur Professionalität gehören standardisierte Verfahren fixiert in transparenten Anweisungen und Aufgabenbeschreibungen, welche Ziele, Verantwortlichkeiten und Abläufe für einen verlässlichen, geordneten und nachhaltigen Verfahrensbetrieb dokumentieren. Dazu fordert CobiT im Prozessgebiet „Manage Operations“ (DS 13 (DSS01[5])) die nachstehenden Aktivitäten:

- standardisierte Verfahrensanweisungen und Aufgabenbeschreibungen,
- Job-Planung,
- Überwachung der IT-Infrastruktur
- physische Absicherung und deren Überwachung,
- Zugangskontrolle für sensitive Dokumente & Anlagen und Inventarisierung,
- präventive Hardwarewartung.

Neben dem täglichen Betrieb, der Steuerung und Wartung der Infrastruktur ist ein proaktives **Event Management** aufzusetzen, mit dem geeignet auf Ereignisse reagiert werden kann. IT-Operation kann daher ohne eine adäquate Überwachung und ohne die verlässliche Auswertung der Überwachungsdaten keine hinreichende Professionalität entwickeln. Die Potentialstufe der Überwachung ist daher ein weiterer Indikator für die Professionalität des IT-Service Betriebes. Alle Ereignisse, die von den beteiligten Ressourcen bzw. Überwachungssystemen als Meldungen abgesetzt werden, sind grundsätzlich zu dokumentierende Events. Dabei sind regelkonforme Ereignisse (z.B. Login eines berechtigten Nutzers) auszufiltern, da sie keiner Reaktion bedürfen. Sobald ein Event von der definierten Regel abweicht, wird der Event Management Prozess angestoßen. Die Überwachung der eingesetzten Ressourcen zum frühzeitigen Erkennen von Abweichungen ist Voraussetzung für das frühestmögliche Gegensteuern und wird im Band B Kapitel 10 „Überwachung“ dieses Kompendiums beschrieben.

Für die Potenzialbewertung werden auch hier qualitative Indikatoren zur Steuerung der IT-Leistung „Service-Operation“ genutzt:

5 In der CobiT Version 5.0

Service-Operation (SO)				*Verweise*	
Prozesse des Service Operation				CobiT DS 13 (V5 DSS01) ITIL BAND 4	
0 Non-existend	1 Initial	2 Repeatable	3 defined	4 Managed & measurable	5 Optimized
Tabelle SO	Stufe 1	Stufe 2	Stufe 3	Stufe 4	Stufe 5

Tabelle SO	
Stufe	***Beschreibung***
1	Prozesse des IT-Betriebs laufen undifferenziert nach technischen Anforderungen oder Kundenanfragen auf Mitarbeiter zu, welche mit der System-Administration beauftragt sind. Da eine systematische Ausbildung und die standardisierte Festlegung von Abläufen fehlt, sind diese oft von den Ereignissen überfordert. Die Notwendigkeit der Systemaktualisierung (Rechteentzug bei Umsetzung von Mitarbeitern, Umsetzung von Patches) erfolgt ungeregelt, z.B. im Zuge der Bearbeitung aufkommender Störungen.
2	Prozesse des IT-Betriebs einer Organisationseinheit IT-Betrieb zugeordnet oder an einen IT-Dienstleister übertragen. Die Verantwortlichkeiten für IT-Betrieb und IT-Sicherheit sind geregelt. Die notwendigen Abläufe sind dokumentiert und vereinbart. Es besteht eine hohe Abhängigkeit von den Fähigkeiten einzelner Mitarbeiter. Die Maßnahmen des IT-Grundschutzes für den normalen Schutzbedarf sind umgesetzt.
3	Verfahren und Abläufe zum IT-Betrieb sind beschrieben, definiert und als Standard festgelegt bzw. vereinbart (Service-Vereinbarungen liegen vor). Die Professionalität des internen oder externen IT-Dienstleisters ist durch Qualität und Stand der Aus-und Fortbildung der Mitarbeiter nachweisbar (z.B. Zertifikate des Trainings an den eingesetzten Systemen). Die Verantwortlichkeiten für IT, Infrastruktur und Sicherheit sind eindeutig zugewiesen. Die für hohen Schutzbedarf bei Verfügbarkeit erforderlichen technischen und organisatorischen Maßnahmen nach IT-Grundschutz sind umgesetzt. Die Ablaufsteuerung ist weitgehend automatisiert.
4	Der IT-Betrieb wird über Service Level mit festgelegten Zielwerten gesteuert, die sich an den Anforderungen (z.B. kritische Geschäftsprozesse) orientieren. Für die Steuerung und Überwachung der eingesetzten Ressourcen steht eine Tool-Unterstützung zur Verfügung, welche die Zielwerte überwacht. Verfahren für die Kommunikation und Beteiligung an Lösungen in Zusammenwirken mit anderen Prozessgebieten (Problem Management, Capacity Management, Availability Management, Service Level Management) sind definiert.
5	Der IT-Betrieb arbeitet auf der Basis der festgelegten Ziele mit effizienten Abläufen, um die vereinbarten Service Level angemessen zu erfüllen. Effizienz und Effektivität werden anhand eines Benchmarks im Zeitvergleich optimiert. Abweichungen oder Produktivitäts-Einschränkungen werden ständig überwacht und minimalisiert.

Tabelle 7: (SO) Bewertung des Potentials des Service Operation

3.5 Define & Manage Service-Level

Das **Service-Level-Management** (SLM) ist ein zentraler Prozess für die Verfügbarkeitsbetrachtung. Vor dem Design der IT-Services sind zunächst die Service- und auch Verfügbarkeitsanforderungen der Geschäftsprozesse zu konkretisieren. Diese sind durch das SLM sowie die weiteren beteiligten ITIL-Prozesse z. B. das Capacity Management oder das Availability Management auf Realisierbarkeit zu prüfen. Das SLM umfasst auch die kontinuierliche und zweckgemäße Überwachung der Service-Level angebotener IT-Services. Dazu werden Delivery-Werte zur Bewertung der gelieferten Service-Qualität erhoben und bei Abweichungen von den Zielwerten Optimierungsmaßnahmen für IT-Services und IT-Prozesse abgeleitet.

Das SLM stellt für die STIL-Design-Prozesse „Availability Management“, „Capacity Management“ und „Service Continuity Management“ die Requirements für die Ausgestaltung der Prozesse und IT-Services zur Verfügung. Die Ausgestaltung hochverfügbarer IT-Services erfolgt nach der Phase M dieses HV-Kompendiums über fünf Schichten, wobei die in diesem Kapitel angestellten Betrachtungen zu IT-Prozessen sich auf die Schicht Organisation und Personal beziehen. ITIL schafft dazu Subprozesse, die ein Aufgliedern der Business-Services in Infrastruktur-Services und organisatorisches und technisches Service-Design ermöglichen, ohne jedoch die Seiten von Technik und Infrastruktur weiter zu beschreiben. Die Ergänzung zwischen ITIL und diesem HV-Kompendium wird damit evident.

Nachstehend werden die Aktivitäten des Service Level Managements beschrieben.

3.5.1 SLAs vereinbaren und dokumentieren

Das Service Level Management definiert zusammen mit dem operationalen Betrieb (Service Operation) die IT-Services und die zugehörigen Service Levels. Die Gesamtheit aller IT-Services des Service Providers bildet ein Service Portfolio, das in Form eines Kataloges die IT-Services sowie die dazugehörigen Parameter, also die Größen, die üblicherweise in SLAs vereinbart werden, beinhaltet.

Mit dem Kunden (Service Requester) zusammen ermittelt das Service-Level-Management dessen IT-Bedarfe und Anforderungen und dokumentiert diese in Service-Level-Requirements (SLR).

Nach einem Abgleich der Requirements mit dem Portfolio vereinbart das Service-Level- Management diese schließlich in einem Service Level Agreement (SLA), welches die wichtigsten Serviceziele, Überwachungsgrößen und Zuständigkeiten definiert. Dabei ist besonders darauf zu achten, dass die IT-Organisation des Service Providers tatsächlich in der Lage ist, die zu vereinbarenden Serviceziele zu erreichen.

3.5.2 Überwachen und Messen

Eine weitere Aktivität des Service Level Management ist das Überwachen und Messen der erreichten Service-Performance aller operativen Services im Hinblick auf die Ziele in den SLAs.

Es ist wichtig, dass die Überwachung die tatsächliche Wahrnehmung des Service durch den Service Requester widerspiegelt. Die Überwachung einzelner Komponenten wie Server oder Netze garantiert beispielsweise nicht, dass der Service insgesamt für den Service Requester verfügbar ist.

Eine bevorzugte Methode ist die Überwachung der IT-Dienstleistung am Endanwender-Arbeitsplatz (vgl. Band B Kapitel 10 „Überwachung“). Bei dieser Methode wird die Performance des IT-Services aus der Sicht des Endanwenders gemessen. Dies geschieht häufig durch den Einsatz von

„Roboter“-Tools, die kontinuierlich oder stichprobenhaft Client/Server-Antwortzeiten überwachen, indem sie typische Client-Anfragen stellen und die Dauer bis zum Eintreffen der Antwort messen. Hierbei ist zu beachten, dass im Rahmen des Endanwender-Monitorings häufig mehrere Service Provider involviert sind. Nicht nur der Service Provider, der den IT-Dienst der Anwendung zur Verfügung stellt, ist beteiligt, vielmehr ist auch der Service Provider, der den Netz-Dienst bereitstellt in diesem Fall einbezogen. Eine Differenzierung, wer z. B. für eine Servicebeeinträchtigung verantwortlich ist, ist in diesem Fall durch reines Endanwender-Monitoring nicht möglich. Hier muss auf die Überwachung der Service Provider zurückgegriffen werden (vgl. Kapitel 3.5.3).

Im HV-Umfeld dient das Überwachen und Messen nicht nur zur „Beweisführung“ dem Kunden gegenüber, dass SLAs eingehalten wurden – oder auch nicht. Es ermöglicht auch ohne Auftreten von Incidents (die der Kunde in der Regel als Serviceunterbrechung erfährt) Aussagen zur Service-Performance aus der Sicht des Kunden zu treffen und entsprechend im Rahmen des Incident Managements basierend auf Events zu reagieren. Als Event ist in diesem Fall die Abweichung von dem SLA-Ziel zu bezeichnen, die allerdings noch nicht zu einer Serviceunterbrechung führte.

3.5.3 Berichten

Sobald SLAs vereinbart sind, müssen Überwachungs-Aktivitäten initiiert werden und Berichte zur erreichten Servicequalität in regelmäßigen Abständen erstellt werden. Wurden SLAs nicht eingehalten, muss ggf. unmittelbar ein Bericht erstellt werden. In vielen Fällen wird bereits im SLA festgelegt, wann und wie Servicequalitätsberichte zu erstellen sind.

Die Berichte sollten neben den Details der Service Performance ggf. auch beobachtete Trends oder zur Verbesserung der Servicequalität durchgeführte Aktionen beinhalten. Im HV-Umfeld ist es besonders wichtig, dass der Bericht nicht nur die aktuelle Performance enthält, sondern auch historische Performances und Trends, so dass die Auswirkungen auf die zukünftige Servicequalität prognostiziert, aber auch Verbesserungen gemessen werden können.

Insbesondere im HV-Umfeld empfiehlt sich der Einsatz integrierter Support-Tools zur automatischen Erstellung von Berichten. Mit dem Einsatz integrierter Support-Tools können der Umfang, die Aktualität und die Präzession der Berichterstattung deutlich angehoben werden. Nicht zu unterschätzen ist die deutliche Reduzierung des enormen Aufwands zur Berichtserstellung.

3.5.4 Service-Reviews

In regelmäßigen Abständen sollten Reviews zur Beurteilung der im letzten Zeitraum erreichten Servicequalität durchgeführt werden. In den Bereichen, in denen die Ziele nicht erreicht wurden, besteht Handlungsbedarf. Im HV-Umfeld sollte ein besonderes Augenmerk auf die Verletzung einzelner Service Levels gelegt werden. Hier muss geklärt werden, was die Zielverfehlung verursacht hat und wie verhindert werden kann, dass dieses zukünftig erneut geschieht.

3.5.5 Überprüfen und Überarbeiten von SLAs und OLAS

Alle Vereinbarungen, die im Rahmen des Service Level Managements abgeschlossen wurden, müssen regelmäßig überprüft und ggf. überarbeitet werden. Wenn man zu dem Schluss kommt, dass ein Service Level nicht erreichbar war oder ist, ist es notwendig, neue Serviceziele zu verhandeln und zu vereinbaren.

Insbesondere bei kritischen Geschäftsprozessen im HV-Umfeld ist es aus der Sicht des Service Requesters aufgrund der hohen Anforderungen (vgl. SLR) i. d. R. nicht möglich, die Serviceziele hinsichtlich einer Reduzierung der Verfügbarkeit zu verändern. In diesem Fall muss mit dem Service Provider eine Lösung entwickelt werden, wie die Serviceziele erreicht werden können, oder ggf. muss auf einen alternativen Service Provider zurückgegriffen werden.

3.5.6 Modell zur Bewertung der Prozesspotentiale im Service-Level Management

Das **Service-Level Management** (SLM) ist ein zentraler Prozess für die Verfügbarkeitsbetrachtung. Der Beitrag der IT für Geschäftsprozesse wird mit dem Vergleich zwischen nachgefragtem Service Level und gelieferten Service Level offenkundig. Die Erhebung der Anforderungen ist notwendige Voraussetzung für das SLM und das Design der IT-Services. Das SLM umfasst die kontinuierliche und zweckgemäße Überwachung der Service-Level angebotener IT-Services. Dazu werden Delivery-Werte zur Bewertung der gelieferten Service-Qualität erhoben und bei Abweichungen von den Zielwerten Optimierungsmaßnahmen für IT-Services und IT-Prozesse abgeleitet. Eine analytische Betrachtung Service Delivery ist erst ex Ante möglich und lässt nur eine beschränkte Prognose für die Verlässlichkeit der IT-Dienstleistung zu. Eine valide Aussage zur Verlässlichkeit kann über die qualitative Betrachtung der eingesetzten Komponenten und der Professionalität der Prozesse erfolgen, die eine hinreichende Widerstandskraft (z.B. Robustheit) gegen schädigende Einflüsse aufbringen. Dazu dient das nachstehende Potential-Profil:

Service-Level Management (SLM)				*Verweise*	
Umsetzung der Prozesse im Service-Level Management; Reifegrade				CobiT DS1 (V5 AP009)	
0 Non-existend	1 Initial	2 Repeatable	3 defined	4 Managed & measurable bewertet	5 Optimiert
	Für einen angenommenen Bedarf wird ein scheinbar angemessenes Service-Niveau angeboten, Ausfälle treten sporadisch auf.	Der Schutzbedarf hinsichtlich Verfügbarkeit ist mit normal bewertet. Die Notwendigkeit von festgeschrieben en SLAs wird nicht gesehen.	Verfügbarkeit sbedarf hoch, SLAs sind festgelegt.	Aus dem Verfügbarkeit sbedarf kritischer Geschäftsproz esse sind Servicelevel abgeleitet, deren Einhaltung bewertet, überwacht und berichtet wird.	Die vereinbarten Servicelevel werden mit den Service-Potentialen ständig abgeglichen, und die Potentiale optimiert.

Tabelle 8: (SLM) Potentiale des Service-Level-Management

Das SLM steht in enger Verzahnung mit den Aktivitäten im Bereich Identifikation kritischer Geschäftsprozesse und Potentialabgleich (siehe Tabelle 4). Je nach Gestaltung in der Organisation liefert die obige Tabelle „Service-Level-Management“ bzw. die Tabelle 4 „Erforderliche

Identifikation kritischer Geschäftsprozesse“ die Requirements für die Ausgestaltung der Prozesse und IT-Services.

Die Phase S des HV-Kompendiums beschreibt dazu ein geeignetes Vorgehen. Das Zusammenwirken dieser Prozessgebiete wird in den Fragenkatalogen abgebildet. z.B. in Fragen wie: „Ist die „Dauer der Verzichtbarkeit“ für kritische Geschäftsprozesse erhoben, analysiert, bewertet hinterlegt, erfüllt & optimiert“. Die Nennung in der beschreibenden Aufzählung gibt die Stellung im Reifegradmodell wieder.

Anhang: Verzeichnisse

Abkürzungsverzeichnis

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