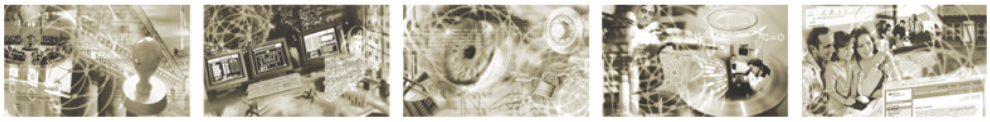
Bundesamt
für Sicherheit in der
Informationstechnik



Band M, Kapitel 1: Meta Ebene

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

Inhaltsverzeichnis

Tabellenverzeichnis

1 Meta Ebene

Die Meta-Ebene ist der Marktplatz der Anforderungskonformität, auf dem die Anforderungen aus Sicht der Geschäftsprozesse auf die Potentiale treffen, welche die IT-Services zur Verfügung stellen. Die Meta-Ebene wurde als sichtbares methodisches Element für das Design von Services geschaffen, damit für kritische Geschäftsprozesse anforderungskonforme IT-Dienstleistungen entwickelt werden und ein angemessenen Service Level erreicht werden kann. Das Design von Services basiert auf dem Service-Modell des BSI, welches unter Band G, Kapitel 8 „Service-Modell“ beschrieben ist. Dort werden Services als Komposition von Prozess- und Kompenenten-Modellen dargestellt, die einen Ausgleich zwischen der Qualität der Anforderungen und der Qualität der Services anstreben und auf höheren Stufen der Anforderungsqualität einen kontinuierlichen Verbesserungsprozess für IT-Dienstleistungen vorsehen. Die Qualität einer IT-Dienstleistung wird von dem gelieferten Service Level der darunterliegenden Assistent Services bestimmt. Der nachstehende Maßnahmenkatalog beschreibt Infrastruktur-Services und Services der Organisationsarchitektur, die nur gemeinsam ein anforderungskonformes Service Level erreichen können. Für die Abbildung funktionaler Anforderungen in adaequaten Services wird auf Band AH, Kapitel 1 „Architektur-Modelle“ verwiesen.

Die nachstehenden Maßnahmenbeschreibungen stellen in ausgewählten Service-Bereichen beispielhafte Potentialstufenmodelle für Services wie sie in einen Service Level Agreement angeboten werden können. Die Beispiele sind so gehalten, dass mit einer beliebig angenommenen Anforderungs-Qualität die jeweils notwendige Service Qualität abgeleitet werden kann. Der Einfachheit halber wird von den funktionalen Anforderungen eines konkreten Geschäftsprozesse abstrahiert und unterstellt, dass die anwendungsnahen Services mit einer anforderungskonformen Architektur entsprechend der Architektur-Modelle abgedeckt sind. Damit bleiben Basis-Services, die von einem IT-Dienstleister über eine verlässliche Basisarchitektur anforderungskonform anzubieten sind. Die Basis-Architektur ist die Grundlage für den Betrieb der IT-Services und IT-Anwendungen. Erklärtes Design-Ziel in der Metatebene ist das Erreichen anforderungskonformer Potentiale für die IT-Leistungen. Die erste MAßnahmenbeschreibung in den nachfolgenden Maßnahmeempfehlungen(VM 1.1) beschreibt das zu erreichende Soll.

2 Anwendung des Reifegradmodells (Potenzialstufen)

2.1 Zentrale Prozesse, ihre Potentiale & Indikatoren für die IT-Prozess-Steuerung

Nr	*Maßnahme*						
VM 1.1	**IT-Prozesse** Nachstehend werden notwendige Prozesse unter der Zielstellung Verlässlichkeit und die gelieferte Servie-Qualität in Potentialstufen beschrieben und der Stufe der Anforderungsqualität gegenübergestellt. Die Gesamtschau liefert die Anforderungen für die Geschäftsprozesse undbeschreibt, auf welcher Potentialstufe eine Prozess-Steuerung erforderlich ist.						
	Potential -Stufe	**0**	**1**	**2**	**3**	**4**	**5**
	Non-existend		Initial	Repeatable	defined	Managed & measurable	optimized

Die nachstehende Tabelle ordnet Kriterien zur Bestimmung der Potentialstufe des Business-Conitunity Management zu und liefert die zu prüfenden prägenden Merkmale für eine konkrete Organisationsarchitektur.

Stufe der Anforderungsqualität nach Phase S	*Anforderungs-Kriterien*	*Realisierung*
1	Keine kritischen Geschäftsprozesse, geringe Anforderungen an Vertraulichkeit und Integrität.	Hausstandards sind in Teilbereichen eingeführt, Rudimentäre IT-Prozesse sind eingeführt, IT-Sicherheit ist partiell realisiert.
2	Einzelne kritische Geschäftsprozesse, Auswirkungen sind beschränkt bzw. korrigierbar.	Hausstandards sind weitgehend eingeführt, zentrale IT-Prozesse sind eingeführt, IT-Sicherheit ist auf der Basis von IT-Grundschutz (BSI 100-1 u. BSI 100-2) umgesetzt.
3	Kritische Geschäftsprozesse in operativen Geschäftsfeldern mit hohen Schdensfolgen.	Hausstandards, IT-Planung und Umsetzung orientieren sich an gesetzten IT-Zielen und etablierten Standards. Services sind auf Anforderungskonformität ausgerichtet. Technische und organisatorische Maßnahmen nach IT-Grundschutz sind umgesetzt eine ergänzende Risikoanalyse nach BSI 100-3 ist erfolgt.
4	Kritische Geschäftsprozesse in strategischen und operativen Geschäftsfeldern. Beeiträchtigungen führen zu deutlichen Auswirkungen nach Außen.	Umsetzung IT-Governance: IT-Ziele und Anforderungen sind bewertet. IT-Prozesse sind mit den Anforderungen der Gechäftsprozesse abgestimmt, Service Potentiale sind analysiert. Umsetzung des BSI-Standards 100-4: Die Notfallvorsorge funktioniert, es erfolgt eine automatisierte Wiederherstellung von Services. Übungen bestätigen die Wiederherstellung in der vorgegebenen Zeit.
5	Extrem kritische Geschäftsprozesse in strategischen und operativen Geschäftsfeldern. Beeiträchtigungen haben katastrophale Auswirkungen.	Prozess Potentiale sind bewertet, Systemzustände werden ständig kontrolliert und festgestellte Ereignisse dem Prozess Incident Management zugeführt. Änderungen werden dem Change Management Prozess zugeführt. Zielstellungen und Zielereichung werden in einem transparenten Prozess zwischen Auftragnehmer und Auftraggeber abgestimmt und Feststellungen einem KVP zugeführt. Umsetzung von

Stufe der Anforderungsqualität nach Phase S	*Anforderungs-Kriterien*	*Realisierung*
		ITIL/CobiT.

Tabelle 1-1: Maßnahmenkatalog Meta Ebene:Anforderungsqualität und notwendige Prozess-Potentiale

2.2 Reifegrade & Indikatoren Monitoring Prozess

Nr.	*Maßnahme*						
VM 1.2	**Reifegrade&Indikatoren für den Monitoring Prozeß** Die Potentialstufen für den Monitoring Prozess orientieren sich an nachstehendem Reifegradmodell. Für die Bewertung ist die Gesamtschau der Aktivitäten für das Prozessgebiet Monitoring erforderlich, um die Professionalität der unterstützenden IT-Prozesse in diesem Bereich bewerten zu können.						
	Potential -Stufe	**0**	**1**	**2**	**3**	**4**	**5**
	Non-existend		Initial	Repeatable	defined	Managed & measurable	optimized

Die nachstehende Zuordnung von Kriterien zur Bestimmung der Potentialstufe der Monitoring-Prozesse liefert die zu prüfenden prägenden Merkmale für eine konkrete Organisationsarchitektur.

Potential-Stufe	*Beschreibung*
1	IT-Komponenten bzw. einzelne Objekte werden nur sporadisch nach Bedarf überwacht. Der Prozess dafür ist nicht definiert und findet deshalb unstrukturiert statt. Überwachungstools, wie z. B. Nagios, HP OpenView, Tivoli, werden gar nicht oder nur teilweise eingesetzt. Überwiegend erfolgt eine manuelle bzw. halbautomatische Überwachung.
2	IT-Komponenten bzw. Objekte werden regelmäßig überwacht. Abläufe sind dokumentiert und die Verantwortlichen sind festgelegt. Monitoring-Tools, wie z. B. Nagios, HP OpenView, Tivoli, werden teilweise eingesetzt, überwiegend erfolgt eine halbautomatische Überwachung, die Auswertung erfolgt manuell.
3	Der Monitoring-Prozess ist definiert, als Standard freigegeben und wurde kommuniziert. Die Verantwortlichen sind klar definiert. Das Monitoring erfolgt überwiegend Tool-unterstützt (Echtzeitdatenüberwachung). Auswertungen werden durch die Tools erzeugt.
4	Der Monitoring-Prozess wird geplant und entsprechend der Definition durch-geführt. Erfahrungswerte fließen in die Prozessdefinition mit ein. Das eingesetzte Monitoring-Tool ist entsprechend "best practice"-Ansätzen konfiguriert. Überwachung und Auswertung geschieht zur Steuerung der IT-Komponenten.
5	Der Monitoring-Prozess wird regelmäßig überprüft, es finden Prozess-Reviews statt und der Prozess wird regelmäßig optimiert. Überwachung und Auswertung erfolgt nicht nur zur Steuerung der Objekte, sondern bei Abweichungen von Soll-Werten werden entsprechende korrigierende Prozesse eingeleitet.

Tabelle 1-2: Maßnahmenkatalog Meta-Ebene: Anwendung des Reifegradmodells auf den Monitoring Prozeß

2.3 Reifegrade & Indikatoren Zutrittskontrolle

<table>
<tr><th>Nr.</th><th colspan="7">Maßnahme</th></tr>
<tr><td>VM 1.3</td><td colspan="7">Reifegrade&Indikatoren für die Zutrittskontrolle
Die Potentialstufen für die Zutrittskontrolle orientieren sich an nachstehendem Reifegradmodell. Für die Bewertung ist die Gesamtschau der Aktivitäten für das Prozessgebiet „Zutrittskontrolle“ erforderlich, um die Professionalität der unterstützenden IT-Prozesse in diesem Bereich bewerten zu können.</td></tr>
<tr><td></td><td>Potential -Stufe</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td></td><td colspan="2">Non-existend</td><td>Initial</td><td>Repeatable</td><td>defined</td><td>Managed & measurable</td><td>optimized</td></tr>
</table>

Die nachstehende Zuordnung von Kriterien zur Bestimmung der Potentialstufe der Prozesse Zutrittskontrolle liefert die zu prüfenden prägenden Merkmale für eine konkrete Organisationsarchitektur.

Potential -Stufe	*Beschreibung*
1	Für die Zutrittskontrolle existiert ein mechanisches Schließsystem, das auf Schlüsseln basiert. Auf eine Verletzung der Zutrittsberechtigung wird nach Feststellen des Ereignisses spontan reagiert.
2	Es wurde eine Zutrittsregelung festgelegt. Die technischen Komponenten der Zutrittskontrollanlage (ÜZKZ, BAE, ZKZ, Chipkartenleser etc.) sind vorhanden. Auf eine Verletzung der Zutrittsberechtigung wird entsprechend der Zutrittsregelung reagiert.
3	Es wurde ein Zutrittskontrollsystems (ZKS) mit allen erforderlichen baulichen, apparativen und organisatorischen Details nach DIN V VDE 0830-8-1 eingerichtet. Die Zutrittskontrollzentralen (ZKZ) sind redundant vorhanden. Als Ergänzung für die Schutzfunktionen der Zutrittskontrolle wurde eine Videokontrollanlagen eingerichtet. In der ÜZKZ erfolgen weitere Funktionen und die Umsetzung der Zutrittsorganisation, wie beispielsweise Zutrittswiederholkontrolle (Anti-Pass-Back) oder eine Zwei-Personen-Zutrittskontrolle (Vier-Augen-Prinzip). Auf eine Verletzung der Zutrittsberechtigung wird entsprechend der Soll-Vorgaben in den Zutrittsregelung reagiert.
4	Das Zutrittskontrollsystems und die Zutrittskontrollregelung sind eingebettet in ein übergeordnetes IT-Security-Management-System. Lokale Zutrittskontrollen erfolgen automatisiert und werden an eine übergeordnete Instanz (ÜZKZ) weitergeleitet. Zutrittsberechtigungsdaten werden in einer zentralen Datenbank vorgehalten und ausgewertet. Die Zutrittskontrolle ist als kontinuierlicher IT-Prozess etabliert und wird von speziell geschultem Personal gelebt.
5	Der Zutrittskontroll-Prozess wird im Rahmen eines zentralen IT-Management-Systems überwacht und optimiert. Das Personal wird nach klar definierten Zielen entsprechend der Best Practices für die Zutrittskontrolle geschult. Unberechtigtem Zutritt wird durch automatisierte Prozesse, die den Zutrittsschutz gewährleisten, präventiv begegnet. Die in Prozessen koordinierten Maßnahmen sind zeitlich so ausgelegt, dass zusätzlich ein manuelles Eingreifen (z. B. Wachdienst) rechtzeitig erfolgen kann.

Tabelle 1-3: Maßnahmenkatalog Meta-Ebene: Anwendung des Reifegradmodells auf die Zutrittskontrolle

2.4 Reifegrade & Indikatoren Energieversorgung

In der nachstehenden Tabelle wurde exemplarisch das Reifegradmodell in dem Maßnahmen-Cluster „Energieversorgung“ angewendet.

<table>
<tr><th>Nr.</th><th colspan="7">Maßnahme</th></tr>
<tr><td>VM 1.4</td><td colspan="7">Reifegrade&Indikatoren für die Energieversorgung
Die Potentialstufen für die Energieversorgung orientieren sich an nachstehendem Reifegradmodell. Für die Bewertung ist die Gesamtschau der Aktivitäten für das Prozessgebiet „Energieversorgung“ erforderlich, um die Professionalität der unterstützenden IT-Prozesse in diesem Bereich bewerten zu können.</td></tr>
<tr><td rowspan="2"></td><td colspan="2">Potential -Stufe</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td colspan="2">Non-existend</td><td>Initial</td><td>Repeatable</td><td>defined</td><td>Managed & measurable</td><td>optimized</td></tr>
</table>

Potential -Stufe	*Beschreibung*
1	Über den Bedarf einer sicheren elektrischen Energieversorgung besteht Konsens. Die elektrische Energie wird vom Energieversorgungsunternehmen (EVU) bereitgestellt.
2	Die Notwendigkeit von erhöhten Schutzmaßnahmen hinsichtlich des Ausfalls der elektrischen Energieversorgung sind erkannt und werden kommuniziert. Zur Prävention von Ausfällen der elektrischen Energieversorgung wird die durch das EVU bereitgestellte Stromversorgung durch eine USV ergänzt, die sicherstellt dass bei einem Stromausfall die angeschlossenen Geräte ordnungsgemäß heruntergefahren werden können.
3	Es wurde ein Konzept zur Erhöhung der Verfügbarkeit hinsichtlich der elektrischen Energieversorgung auf der Basis eines etablierten Standards entwickelt, die erforderlichen technischen und organisatorischen Maßnahmen sind umgesetzt. Das Konzept umfasst mindestens eine USV-Anlage und wird durch eine Netzersatzanlage ergänzt.
4	Es findet ein Monitoring aller relevanten Systemkomponenten und Größen statt. Die Überwachung der Anforderungen sind auf eine Gebäudeleittechnik aufgeschaltet und eingebettet in einen übergeordneten Sicherheitsmanagementprozess. Es erfolgt eine automatisierte Wiederherstellung der Versorgung mit elektrischer Energie. Übungen bestätigen die maximal zu bewältigende tolerierbare Ausfallzeit.
5	Die aus dem Monitoring erkenntlichen Werte werden optimiert. Diese Optimierung kann beispielsweise durch eine redundante USV und eine redundante NEA erfolgen.

Tabelle 1-4: Maßnahmenkatalog Meta-Ebene: Anwendung des Reifegradmodells auf die Energieversorgung

2.5 Reifegrade & Indikatoren Klimatisierung

Nr.	*Maßnahme*
VM 1.5	**Reifegrade&Indikatoren für die Klimatisierung** Die Potentialstufen für die Klimatisierung orientieren sich an nachstehendem Reifegradmodell. Für die Bewertung ist die Gesamtschau der Aktivitäten für das Prozessgebiet „Klimatisierung“ erforderlich, um die Professionalität der unterstützenden IT-Prozesse in diesem Bereich bewerten zu können.

Nr.	*Maßnahme*						
	Potential-Stufe	**0**	**1**	**2**	**3**	**4**	**5**
	Non-existend		Initial	Repeatable	defined	Managed & measurable	optimized

In der nachstehenden Tabelle wurde exemplarisch das Reifegradmodell in dem Maßnahmen-Cluster „Klimatisierung“ angewendet.

Potential-Stufe	*Beschreibung*
1	Durch Be- und Entlüftung ist eine ausreichende Klimatisierung gegeben
2	Über den Einsatz von Technik zur Kälteerzeugung besteht konsens.
3	Es werden Werte hinsichtlich Umgebungstemperatur und Luftfeuchte festgelegt. Auf eine Über- und Unterschreitung der Werte wird reagiert.
4	Es findet ein Monitoring der Werte statt. Im Luftsrom der durch die Klimaanlage abgesogen wird werden Lufttemperatur und Luftfeuchte ständig gemessen.
5	Die Werte die sich aus dem Monitoring ergeben werden verbessert und optimiert, ggf. durch redundante Klimaanlagen.

Tabelle 1-5: Maßnahmenkatalog Meta-Ebene: Anwendung des Reifegradmodells auf die Klimatisierung

2.6 Reifegrade & Indikatoren Brandschutz

Nr.	*Maßnahme*
VM 1.6	**Reifegrade&Indikatoren für den Brandschutz** Die Potentialstufen für den Monitoring Prozess orientieren sich an nachstehendem Reifegradmodell. Für die Bewertung ist die Gesamtschau der Aktivitäten für das Prozessgebiet „Brandschutz“ erforderlich, um die Professionalität der unterstützenden IT-Prozesse in diesem Bereich bewerten zu können.

Nr.	*Maßnahme*						
	Potential-Stufe	**0**	**1**	**2**	**3**	**4**	**5**
	Non-existend		Initial	Repeatable	defined	Managed & measurable	optimized

In der nachstehenden Tabelle wurde exemplarisch das Reifegradmodell in dem Maßnahmen-Cluster „Brandschutz“ angewendet.

Potential-Stufe	*Beschreibung*
1	Es existieren im wesentlichen Maßnahmen zum baulichen Brandschutz. Baulicherseits sind Maßnahmen wie verminderte Brennbarkeit der Baustoffe, die Feuerwiderstandsklasse, die Dichtheit von Verschlüssen und Öffnungen sowie die Anordnungen von Flucht und Rettungswegen realisiert. Eine Löschung ist mittels Handfeuerlöschern vorgesehen.
2	Decken und Wände erfüllen die Brandschutzklasse F30 nach DIN 4102, Türen und Fenster sind in T30 rauch und gasdicht ausgeführt. Brandschottungen sind in S30 K30 und R30 ausgeführt. Brandschottungen sind in S 90 K 90 und R 90 ausgeführt. Als technischer Brandschutz ist eine Brandmeldeanlage / Überwachungseinheit mit Brandfrüherkennung vorhanden.
3	Die Wände und Decken erfüllen die Brandschutzklasse F90 oder höher nach DIN 4102.Türen und Fenster sind in T 90 rauch und gasdicht ausgeführt. Brandschottungen sind in S 90 K 90 und R 90 ausgeführt. Es sind zusätzlich Werte für die maximale Temperaturerhöhung im Serverraum definiert. Es existiert eine Überwachungseinheit mit Brandfrühesterkennung und Löschtechnik. Diese werden in regelmäßigen zeitlichen Intervallen gewartet.
4	Die Wände und Decken erfüllen die Brandschutzklasse F90 oder höher nach DIN 4102.Türen und Fenster sind in T 90 rauch und gasdicht ausgeführt. Brandschottungen sind in S 90 K 90 und R 90 ausgeführt. Der Serverraum hat eine zusätzliche Isolierung zur Begrenzung der Temperaturerhöhung. Es existiert eine Überwachungseinheit mit Brandfrühesterkennung und Löschtechnik. Die Anlagen werden regelmäßig gewartet und getestet.
5	Es ist eine systemgeprüfte Sicherheitszelle vorhanden deren Einbaumodule erfüllen die Brandschutzklasse F 120 nach DIN 4102

Potential-Stufe	*Beschreibung*
	und der Prüfung nach ECB-S (Begrenzung der maximalen Temperaturerhöhung im Raum). Weiterhin ist hinsichtlich des technischen Brandschutzes eine Löschtechnik in redundanter Ausführung vorhanden oder ein Sauerstoffreduzierungssystem. Eine regelmäßige Wartung sowie ein Test hinsichtlich des Optimierungspotentials werden durchgeführt.

Tabelle 1-6: Maßnahmenkatalog Meta Ebene: Anwendung des Reifegradmodells auf den Brandschutz

2.7 Reifegrade & Indikatoren Perimeter Schutz

Nr.	*Maßnahme*						
VM 1.7	**Reifegrade&Indikatoren für den Perimeter Schutz** Die Potentialstufen für den Perimeter Schutz orientieren sich an nachstehendem Reifegradmodell. Für die Bewertung ist die Gesamtschau der Aktivitäten für das Prozessgebiet „Perimeter Schutz“ erforderlich, um die Professionalität der unterstützenden IT-Prozesse in diesem Bereich bewerten zu können.						
	Potential -Stufe	**0**	**1**	**2**	**3**	**4**	**5**
	Non-existend		Initial	Repeatable	defined	Managed & measurable	optimized

Stufe	*Beschreibung*
1	Über den Bedarf eines geschützten Umfeldes besteht konsens. Es existieren grundlegende Maßnahmen zum Schutz des Umfeldes eines Gebäudes oder einer Anlage. Die erste Stufe einer Zutritts- und Zufahrtskontrolle ist gegeben.

Stufe	*Beschreibung*
2	Die Notwendigkeit von erhöhten Schutzmaßnahmen hinsichtlich des Umfeldes oder einer Anlage sind erkannt und werden kommuniziert. Es existieren Maßnahmen, die einem erhöhten Anspruch an den Perimeter-Schutz gerecht werden. Diese Maßnahmen umfassen beispielsweise die äußere Umfriedung, Geländegestaltung, Zufahrtssperren, die Beleuchtung des Geländes und des Gebäudes, Bewachungsunternehmen und die Video- überwachung des Geländes.
3	Es wurde ein Perimeterschutzkonzept entwickelt. Das Perimeterschutzkonzept besteht in der Regel aus drei Bestandteilen: – aus mechanisch, baulichen Maßnahmen – elektronische Detektionsmaßnahmen – organisatorisch, personelle Maßnahmen
4	Das Perimeterschutzkonzept ist in ein übergeordnetes Gesamtschutzkonzept eingebettet. Die Auswerteeinheiten von Perimeterschutzsystemen verfügen über Schnittstellen, die mit dem Gebäudemanagementsystem verbunden sind. Über das GMS sind folgende Einstellungen und Funktionalitäten möglich: – Kalibrierung von Meldelinien (zur Einstellung von Ansprechempfindlichkeiten) – Statusinformationen zu einzelnen Sensoren (Kabelbruc oder Störung) – Scharf und Unscharfschalten von Anlagenteilen – Testmodi für Kabel, Sensoren etc.
5	Gemeinsam mit der Gefahrenmeldeanlage des Objektes und den anderen Komponenten des GMS bietet der Anschluss des Perimeterschutzsystems und die sinnvolle Verknüpfung mit den anderen Subsystemen die Möglichkeit, frühzeitig vor dem Eindringversuch auf das eigentliche Objekt die Gefahr zu erkennen und die Interventionszeit erheblich zu verkürzen.

Tabelle 1- 7: Maßnahmenkatalog Meta-Ebene: Anwendung des Reifegradmodells auf den Perimeter-Schutz

3 Bausteine zum Design von hochverfügbaren Organisations-Architekturen

3.1 Service Level Management

Nr.	*Maßnahme*						
VM 1.8	**Service Level Management** Umsetzung der Prozesse im Service-Level Management						
	Potential -Stufe	**0**	**1**	**2**	**3**	**4**	**5**
	Non-existend		Initial	Repeatable	defined	Managed & measurable	Optimiert

Stufe	*Beschreibung*
1	Für einen angenommenen Bedarf wird ein scheinbar angemessenes Service-Niveau angeboten, Ausfälle treten sporadisch auf.
2	Der Schutzbedarf hinsichtlich Verfügbarkeit ist mit normal bewertet. Die Notwendigkeit von festgeschriebenen SLAs wird nicht gesehen.
3	Verfügbarkeitsbedarf hoch, SLAs sind festgelegt.
4	Aus dem Verfügbarkeitsbedarf kritischer Geschäftsprozesse sind Servicelevel abgeleitet, deren Einhaltung bewertet, überwacht und berichtet wird.
5	Die vereinbarten Servicelevel werden mit den Service-Potentialen ständig abgeglichen, und die Potentiale optimiert.

Tabelle 1-8: Maßnahmenkatalog Meta Ebene: Anwendung des Reifegradmodells auf das Service Level Management

3.2 Service Desk und Incident Management

Nr.	*Maßnahme*						
VM 1.9	**Service Desk und Incident Management** Umsetzung der Prozesse im Service Desk und Incident Management						
	Potential -Stufe	**0**	**1**	**2**	**3**	**4**	**5**
	Non-existend		Initial	Repeatable	defined	Managed & measurable	Optimiert

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.

Stufe	*Beschreibung*
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 Porzessgebieten 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 1-9: Maßnahmenkatalog Meta Ebene: Anwendung des Reifegradmodells auf das Service Desk und Incident Management

3.3 Service Continuity Management

Nr.	*Maßnahme*						
VM 1.10	**Service Continuity Management** Reifegrad der Prozesse des Business- und Service-Continuity Management						
	Potential-Stufe	**0**	**1**	**2**	**3**	**4**	**5**
	Non-existend		Initial	Repeatable	defined	Managed & measurable	Optimiert

Stufe	*Beschreibung*
1	Bei unvorhergesehenen Unterbrechungen wird aus der Situation heraus reagiert. Die einzige Vorbereitung besteht in einer Datensicherung.
2	Der Baustein 1.4 Datensicherung 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 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 Wiederanlauf 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 ein Monitoring 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 Wiederherstellung von Services. Übungen bestätigen die Wiederherstellung in der vorgegebenen Zeit. Für das SCM steht eine TOOLunterstützung 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 KVP korrigiert.

Tabelle 1-10: Maßnahmenkatalog Meta Ebene: Anwendung des Reifegradmodells auf das Service Continuity Management

3.4 Service Operation

Nr.	*Maßnahme*						
VM 1.11	**Service Operation** Reifegrad der Prozesse des Service Operation						
	Potential -Stufe	**0**	**1**	**2**	**3**	**4**	**5**
	Non-existend		Initial	Repeatable	defined	Managed & measurable	Optimiert

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 Organsiationseinheit 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-Grunschutzes 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 Training 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

Stufe	*Beschreibung*
	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 Ablaufen um die vereinbarten Service Level angemessen zu erfüllen. Effizienz uns Effktivität werden an einer Benchmark im Zeitvergleich optimiert. Abweichungen oder Produktivitäts-Einschränkungen werden ständig überwacht und minimalisiert.

Tabelle 1-11: Maßnahmenkatalog Meta Ebene: Anwendung des Reifegradmodells auf Service Operation

3.5 Risiko Management

<table>
<tr><th>Nr.</th><th colspan="7">Maßnahme</th></tr>
<tr><td rowspan="3">VM 1.12</td><td colspan="7">Risiko Management
Reifegrad der Prozesse des Risk Management</td></tr>
<tr><td>Potential-Stufe</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>Non-existend</td><td>Initial</td><td>Repeatable</td><td>defined</td><td>Managed & measurable</td><td>Optimiert</td></tr>
</table>

Stufe	*Beschreibung*
1	Risiken der IT werden Anlassbezogen betrachtet
2	Die Risiko-Betrachtung geschieht immer noch anlassbezogen, aber durch dieVorgehensweise nach IT-Grundschutz sind Standardrisiken abgedeckt, kritische Geschäftsprozesse sind nicht identifiziert .
3	Kritische Geschäftsprozesse sind identifiziert die für den Schutzbedarf hoch erforderlichen technischen und organisatorischen Maßnahmen nach IT-Grundschutz sind umgesetzt. Die Maßnahme-Empfehlungen aus den Archtekturmodellen des HV-Kompendiums für die Potentialstufe 3 sind umgesetzt.
4	Der 100-4 des BSI ist umgesetzt
5	Umsetzung von Standards der IT-Governance auf der Basis von CobiT oder ITIL

Tabelle 1-12: Maßnahmenkatalog Meta Ebene: Anwendung des Reifegradmodells auf das Risiko Management

3.6 Anforderungsmanagement

Nr.	*Maßnahme*						
VM 1.12	**Requirements Management** Reifegrad der Prozesse des Requirements Management						
	Potential -Stufe	**0**	**1**	**2**	**3**	**4**	**5**

Nr.	*Maßnahme*					
	Non-existend	Initial	Repeatable	defined	Managed & measurable	Optimiert

Stufe	*Beschreibung*
1	Bedarf informell bekannt
2	Bedarf z.B. über Schutzbedarfsfeststellung nach IT-Grundschutz systematisch erhoben
3	Anforderungen sind erhoben und abgestimmt mit den Gechäftsprozessverantwortlichen, Services sind auf Anforderungskonformität ausgerichtet.
4	Anforderungen sind bewertet und funktional und qualitativ auf Gechäftsprozesse abgestimmt, Service Potentiale sind analysiert.
5	Service Potentiale sind bewertet und die Nachfrage-& Potential-analyse erfolgt als kontinuierlicher Prozess zur IT-Steuerung und Prozess-Optimierung.

Tabelle 1-13: Maßnahmenkatalog Meta Ebene: Anwendung des Reifegradmodells auf das Requirements Management

4 Service Level-Analyse für kritische Geschäftsprozesse

Die Ermittlung der Anforderungskonformität von IT-Dienstleistungen erfolgt über die Feststellung der Potentiale einzelner Assistent Services. Dazu wurden mit den Maßnahmenbeschreibungen der Meta-Ebene Kriterien festgelegt und bewertbare Indikatoren definiert, die den Merkmalen der Potentialstufe zugeordnet werden können. Prägendes Merkmal für die Potentialstufe 4 ist immer ein Service Management auf der Basis von qualitativen oder quantitativen Kennzahlen. Potentiale sind qualitative Kennzahlen zur Ermittlung der Anforderungskonformität. Sie schließen weitere Kriterien mit quantitaiven oder qualitativen Indikatoren nicht aus, sondern werden durch diese weiter spezifiziert. Bei höchsten Anforderungen an die Verfügbarkeit ist eine hoch professionelle Service-Qualität zu liefern, die über qualitative und quantitative Indikatoren eine Steuerung und Optimierung der IT-Services ermöglicht und erreicht.

Für die Bewertung der Servicepotentiale für eine IT-Dienstleistung bestimmt das schwächste Glied der Kette die Qualität des Service Levels.

Für die Analyse von Service Level, welche die funktionalen Aspekte der Geschäftsprozesse stärker mit einbezieht wird auf das Datenblatt 1 „Service-Level-Analyse“ im Band AH Kapitel 3.4 Datenblätter verwiesen. Die Komplexität der SLA-Analyse kann durch ein Assessment nach diesem HV-Kompendium reduziert werden, da diesem ein standardisiertes Abhängigkeitsmodell zugrunde liegt.

4.1 Service-Potentiale & Gesamt-Potential für IT-Dienstleistung

Service nach M1 Service-Modell	**Service-Potential**				
Potentialstufe des Service	**1**	**2**	**3**	**4**	**5 Minimalprinzip**
VM 1.1					
VM 1.2					
VM 1.3					
...					

Service nach M1 Service-Modell	**Service-Potential**				
VM 1.12					
…	Raum für weitere	Assisstent Services z.B.	Server	Netze	Speicher
Service-Potential	Es gilt das Minimalprinzip, d.h. der niedrigste Wert bestimmt die gelieferte Service-Qualität.				

Tabelle 1-14: Maßnahmenkatalog Meta Ebene: Service Level Analyse