



Umsetzungsrahmenwerk Notfallmanagement

Rahmenwerk zur Etablierung eines Notfallmanagements auf Basis des
BSI-Standards 100-4

Version 1.0

Inhaltsverzeichnis

1	Einleitung.....	3
1.1	Motivation.....	3
1.2	Zielsetzung des Umsetzungsrahmenwerks.....	4
1.3	Adressatenkreis	5
2	Kurzeinführung zum Notfallmanagement	5
2.1	Grundlagen und Begriffe.....	5
2.1.1	Notfallmanagement	5
2.1.2	Abgrenzung Störung, Notfall und Krise	6
2.2	Notfallmanagement-Prozess	7
3	Darstellung der Phasen und Module des Notfallmanagement-Prozesses.....	9
4	Stufenmodell des Notfallmanagementsystems nach diesem Umsetzungsrahmenwerk	11
4.1	Darstellung des Stufenmodells.....	11
4.2	Stufen des Umsetzungsrahmenwerks.....	13
4.2.1	Stufe 1 – Basis des Notfallmanagements: Notfallreaktion	13
4.2.2	Stufe 2 – Etablierung eines Notfallmanagements: Notfallvorsorge und Notfallreaktion	14
4.2.3	Stufe 3 – BSI Standard 100-4: Etablierung und kontinuierliche Verbesserung eines Notfallmanagementprozesses.....	14
4.3	Auswahl der geeigneten Leitfaden-Variante.....	14
5	Fazit	17
6	Anhang Hilfsmittel der Phasen und Module	18

1 Einleitung

Unternehmen, aber auch Ministerien, Bundesbehörden und sonstige Einrichtungen der öffentlichen Verwaltung müssen sowohl bei internen Notfällen als auch in Krisen und außergewöhnlichen Lagen, wie z. B. großflächigen Unwetterschäden, lang anhaltenden Stromausfällen, massivem Personalausfall oder schwerwiegenden Sicherheitsvorfälle, weiter ihre Kernaufgaben erfüllen.

Institutionen können schneller und effektiver auf Notfälle und Krisen reagieren, wenn sie sich hinreichend auf Ausnahmesituationen vorbereitet haben. Hierbei helfen beispielsweise folgende Fragen:

- Was kann präventiv getan werden, damit Institutionen Notfälle und Krisen möglichst unbeschadet überstehen?
- Was ist zu tun, um bei der Unterbrechung wichtiger Prozesse deren raschen Wiederanlauf zu bewerkstelligen?
- Was sind überhaupt die kritischen Ressourcen und Prozesse einer Institution?

Zu Beantwortung derartiger Fragen trägt der BSI-Standard 100-4 Notfallmanagement bei. Er beschreibt eine Vorgehensweise für die Einführung, den Betrieb und die kontinuierliche Verbesserung eines Notfallmanagements in einer Institution. Für die in den jeweiligen Phasen anstehenden Aufgaben wird eine Fülle an Empfehlungen gegeben.

1.1 Motivation

Viele Unglücke hätte es nicht gegeben, wenn die Ursachen rechtzeitig vorher erkannt und eingedämmt worden wären. Prävention, also der vorbeugende Schutz gegen mögliche Gefährdungen, ist folglich eine wichtige Aufgabe im gesamten Sicherheitsprozess. Die Erfahrung zeigt aber, dass auch noch so gute Vorbereitung gravierende Störungen und Unglücke nicht vollständig verhindern kann. Und oftmals sind es unverhoffte Ereignisse, die die größten Risiken mit sich bringen.

Einige Beispiele verdeutlichen dies:

- Im Januar 2009 verursachten fehlerhaft durchgeführte Wartungsarbeiten in einem Rechenzentrum der Deutschen Bahn AG gravierende Störungen und Ausfälle der IT-Infrastruktur. Dies führte dazu, dass bundesweit über Stunden hinweg keine Bahnfahrkarten mehr verkauft werden konnten, die Züge erhebliche Verspätungen aufwiesen oder teilweise sogar ganz ausfielen. Darüber hinaus beklagten sich vielerorts die Kunden über aus ihrer Sicht unzureichende Informationen durch das betroffene Verkehrsunternehmen.
- Ein Ausbruch des Gletschervulkans Eyjafjalla im April 2010 in Island brachte den Flugverkehr in Europa tagelang nahezu vollständig zum Erliegen. Bei nicht wenigen Unternehmen kam es dadurch zu Produktionsunterbrechungen aufgrund von verzögerten Zulieferungen.

- Im März 2011 legte ein Stromausfall den Bundestag und seine Nebengebäude im Berliner Regierungsviertel lahm. Aufzüge, elektrische Türen und die Computer in den Abgeordnetenbüros konnten nicht benutzt werden, sodass die Bundestagsabgeordneten und weitere Mitarbeiter weitestgehend arbeitsunfähig waren. Erschwerend kam hinzu, dass die Benutzung der Toiletten verboten wurde, da das Spülsystem an elektrisch betriebene Pumpen angeschlossen war. Auslöser des Vorfalls waren Tiefbauarbeiten, die am Morgen drei Stromkabel im Bezirk Mitte beschädigt hatten.

Den Beispielen ist gemeinsam, dass scheinbar kleine oder lokal begrenzte Ereignisse unerwartete Breitenwirkungen und erhebliche Schäden nach sich gezogen haben. Außerdem wird ersichtlich, wie vernetzt, damit aber gleichzeitig auch verletzbar moderne Industrieländer und deren Institutionen sind.

Bei näherer Betrachtung dieser und vergleichbarer Vorfälle zeigen sich aber auch immer wieder Mängel in den Vorbereitungen der betroffenen Institutionen auf solche Ereignisse: Zuständigkeiten sind nicht geregelt, Ausweichkapazitäten fehlen, die Krisenkommunikation ist unzureichend, Notfallpläne sind veraltet oder fehlen vollkommen – die Liste möglicher Mängel ließe sich beliebig verlängern. Ein Notfallmanagement behebt diesen Mangel an Vorbereitung durch ein umfassendes Managementsystem und hilft so die Auswirkungen von Schadensereignissen zu begrenzen.

Über die in der Praxis festgestellte Notwendigkeit, sich dem Thema Notfallmanagement zu widmen, hat das Bundeskabinett im Sommer 2005 den „Nationalen Plan zum Schutz der Informationsinfrastrukturen in Deutschland“ (NPSI) beschlossen. Mit der Umsetzung wurde das Bundesministerium des Innern beauftragt. Eine wesentliche Vorgabe des NPSI ist die Festlegung genauer Richtlinien für den Schutz der Informationsinfrastrukturen in der Bundesverwaltung durch die Bundesregierung.

Mit dem Umsetzungsplan für die Bundesverwaltung (UP Bund) wird eine Vorgabe des Nationalen Planes zum Schutz der Informationsinfrastrukturen erfüllt.

Einrichtungen der öffentlichen Verwaltung sind steigenden Risiken ausgesetzt, die die kontinuierliche und zeitnahe Erbringung ihrer Geschäftsprozesse gefährden. Aus diesem Grund ist im UP Bund gefordert, dass Bundesbehörden Notfallvorsorgekonzepte als integralen Teil der Sicherheitskonzeption erstellen und regelmäßig Notfallübungen durchführen.

1.2 Zielsetzung des Umsetzungsrahmenwerks

Das vorliegende Umsetzungsrahmenwerk zum Notfallmanagement des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hat das Ziel, den Unternehmen und Behörden (im Folgenden „Institutionen“ genannt) mehrere Umsetzungsleitfäden zur Etablierung eines Notfallmanagementsystems nach dem BSI-Standard 100-4 „Notfallmanagement“ zur Verfügung zu stellen.

In diesen Leitfäden werden die für die Etablierung eines Notfallmanagement-Prozesses erforderlichen Tätigkeiten in Form von praxisnahen Erläuterungen, Hilfsmitteln und

Ausfüllanleitungen konkretisiert. Sie stellen dabei eine Hilfe zur Selbsthilfe dar und sollen Institutionen bei der stufenweisen Einführung eines Notfallmanagements helfen.

1.3 Adressatenkreis

Die Dokumente richten sich an die Personen einer Institution, die mit der Einführung, Umsetzung und Aufrechterhaltung eines Notfallmanagements betraut wurden (z. B. Notfallbeauftragte oder gegebenenfalls IT-Sicherheitsbeauftragte). Das vorliegende Hauptdokument und die Leitfäden sind insbesondere auch für die Leitungsebene gedacht, während die jeweiligen Module für die Personen gedacht sind, welche die einzelnen Tätigkeiten in der Institution (z. B. Business Impact Analyse, Übungsplanung, Audits) jeweils umsetzen.

2 Kurzeinführung zum Notfallmanagement

2.1 Grundlagen und Begriffe

Zum besseren Verständnis wird im Folgenden kurz auf die wichtigsten Begriffe zum Notfallmanagement eingegangen.

2.1.1 Notfallmanagement

Notfallmanagement (englisch: Business Continuity Management) ist ein systematischer, an den **Geschäftsprozessen** einer Institution orientierter Ansatz zur **Vorsorge gegen und Bewältigung von Notfällen und Krisen**. Es zielt darauf ab, solche Ausnahmesituationen, wenn schon nicht zu verhindern, so doch zumindest in ihren Schadenswirkungen zu begrenzen. Dazu gehört es, organisatorische Strukturen aufzubauen sowie Konzepte zu entwickeln und umzusetzen, die eine **rasche Reaktion** auf Notfälle und die **Fortsetzung** zumindest der **wichtigsten Geschäftsprozesse** ermöglichen. Der Begriff "Geschäftsprozess" bezeichnet dabei nicht nur die wirtschaftlichen und produktiven Prozesse von Unternehmen, sondern allgemein alle Prozesse eines Unternehmens oder einer Behörde, die zu für die Erbringung von Dienstleistungen und die Erfüllung der jeweiligen Fachaufgaben nötig sind.

2.1.2 Abgrenzung Störung, Notfall und Krise

In allen Institutionen gibt es immer wieder kleinere **Störungen**: Kurzfristige Stromausfälle, Personalengpässe, Dienstleistungen verzögern sich, Geräte gehen defekt. Für solche Vorfälle gibt es in der Regel einfache Lösungen, die Bestandteil des Alltagsgeschäfts sind: Beispielsweise werden Stromgeneratoren aktiviert, Überstunden geleistet, Produktionszeiten gestreckt oder Ersatzgeräte beschafft. Der mögliche Schaden solcher Ereignisse ist darüber hinaus aus Sicht der betroffenen Institution nur gering.

Erst dann, wenn Störungen oder Ausfälle **größere Schäden** verursachen können und ihre Behebung mit den üblichen Verfahren nicht mehr möglich ist, erfordern sie ein Notfallmanagement.

Beispiele:

- Durch Brände können wichtige Betriebsräume (z. B. das Rechenzentrum) nicht mehr genutzt werden.
- Überschwemmungen führen zur tagelangen Sperrung von Zufahrtswegen.
- Eine Pandemie führt zu erheblichem Personalausfall.
- Das Stromnetz fällt flächendeckend und über einen längeren Zeitraum hinweg aus.
- Wichtige Kommunikationsnetze (Internet, Telefonnetz) fallen tagelang aus.
- Wichtige Dienstleistungen fallen vollständig aus, weil eine externe Institution Konkurs anmelden musste und auch nicht auf Ersatzdienstleister zurückgegriffen werden kann.

Alle diese Ereignisse können auch zu Krisen oder Katastrophen werden. Krisen und Katastrophen werden von Notfällen dadurch abgegrenzt, dass Notfälle bewältigt werden können, wenn vorgesorgt wurde und konkrete Pläne existieren, während Krisen so weitreichend sind, dass die einzelne Institution sie auch Vorkehrungen und Plänen nur eingeschränkt bewältigen kann. Obschon hiermit der deutlichste Unterschied zwischen Krisen- und Notfallmanagement angesprochen ist, hängen beide Managementsysteme eng zusammen: Ein Notfallmanagement ist eine gute Vorstufe für das Krisenmanagement einer Institution und je umfangreicher das Notfallmanagement, desto unwahrscheinlicher ist der Eintritt einer Krise für die Institution.

Die folgende Tabelle erläutert kurz die Unterschiede zwischen Störungen, Notfällen, Krisen und Katastrophen aus Sicht des BSI-Standards 100-4 und fasst zusammen, wann und in welcher Weise das Notfallmanagement für deren Behandlung zuständig ist.

Vorfallsart	Erläuterung	Behandlung
Störung	Kurzzeitiger Ausfall von Prozessen oder Ressourcen mit nur geringem Schaden	Behandlung ist Teil der üblichen Störungsbehebung.
Notfall	Länger andauernder Ausfall von Prozessen oder Ressourcen mit hohem oder sehr hohem Schaden	Behandlung verlangt besondere Notfallorganisation.
Krise	Im Wesentlichen auf die Institution begrenzter verschärfter Notfall, der die Existenz der Institution bedroht oder die Gesundheit oder das Leben von Personen beeinträchtigt.	Da Krisen nicht großflächig die Umgebung oder das öffentliche Leben beeinträchtigen, können sie, zumindest größtenteils, innerhalb der Institution selbst behoben werden.
Katastrophe	Räumlich und zeitlich nicht begrenztes Großschadensereignis, zum Beispiel als Folge von Überschwemmungen oder Erdbeben	Aus Sicht einer Institution stellt sich eine Katastrophe als Krise dar und wird intern durch deren Notfallorganisation in Zusammenarbeit mit den externen Hilfsorganisationen bewältigt.

Tabelle 1: Störungen, Notfälle, Krisen und Katastrophen im Verständnis des BSI-Standards 100-4

2.2 Notfallmanagement-Prozess

Die präventiven Aufgaben im Notfallmanagement werden anhand eines auf stetige Verbesserung abzielenden Prozessmodells beschrieben.

Im BSI-Standard 100-4 werden dazu die folgenden sechs Phasen unterschieden:

- **Initiierung**
Getragen von der Leitungsebene der Institution werden strategische Zielsetzungen festgelegt und grundlegende organisatorische Voraussetzungen für den Notfallmanagement-Prozess in einer Institution geschaffen.
- **Konzeption**
Die kritischen Geschäftsprozesse und Ressourcen einer Institution werden ermittelt und die Risiken, denen diese ausgesetzt sind, bewertet. Zu diesen Bewertungen und der Notfallstrategie der Institution passende Notfallvorsorgekonzepte werden entwickelt.
- **Umsetzung des Notfallvorsorgekonzepts**
Prioritäten für die Umsetzung der Notfallvorsorgekonzepte werden gesetzt, Ressourcen bereitgestellt, Verantwortlichkeiten festgelegt und gegebenenfalls erforderliche begleitende Maßnahmen identifiziert.

- **Notfallbewältigung**
Verantwortlichkeiten, Pläne und Verhaltensregeln für die Reaktion auf und das Handeln in Notfallsituationen werden in einem Notfallhandbuch geregelt.
- **Tests und Übungen**
Notfallvorsorgekonzepte und Notfallpläne werden getestet und eingeübt, um mögliche Mängel zu identifizieren und das Verhalten im Notfall zu trainieren.
- **Aufrechterhaltung und kontinuierliche Verbesserung**
Angemessenheit und Wirksamkeit der Konzepte und Maßnahmen werden regelmäßig geprüft. Zusammen mit einer Auswertung der Ergebnisse der Tests und Übungen tragen diese Prüfungen zur kontinuierlichen Weiterentwicklung des Notfallmanagement-Prozesses bei.

Der Notfallmanagement-Prozess nach BSI-Standard 100-4 wird im Folgenden noch einmal grafisch dargestellt.

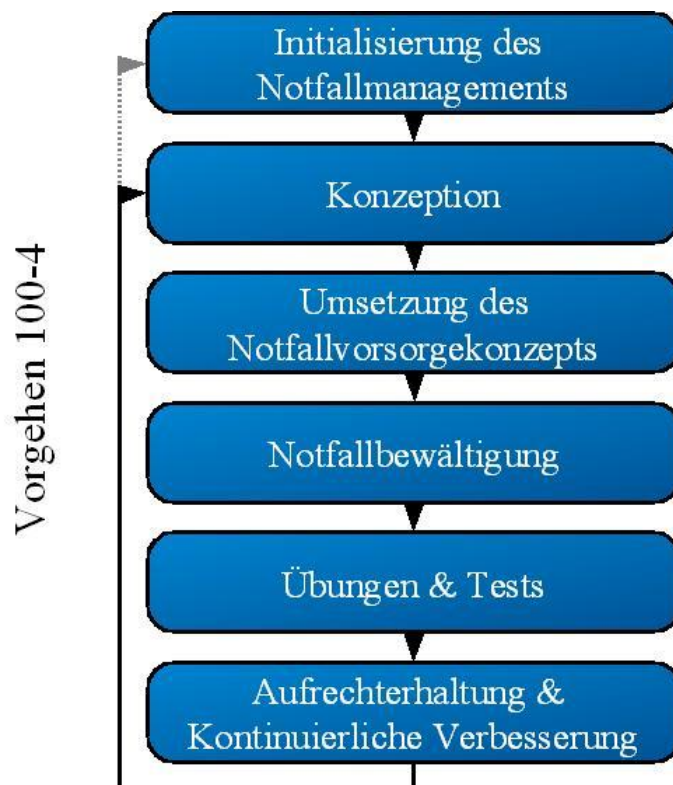


Abbildung 1: Ablauf des Notfallmanagement-Prozesses

3 Darstellung der Phasen und Module des Notfallmanagement-Prozesses

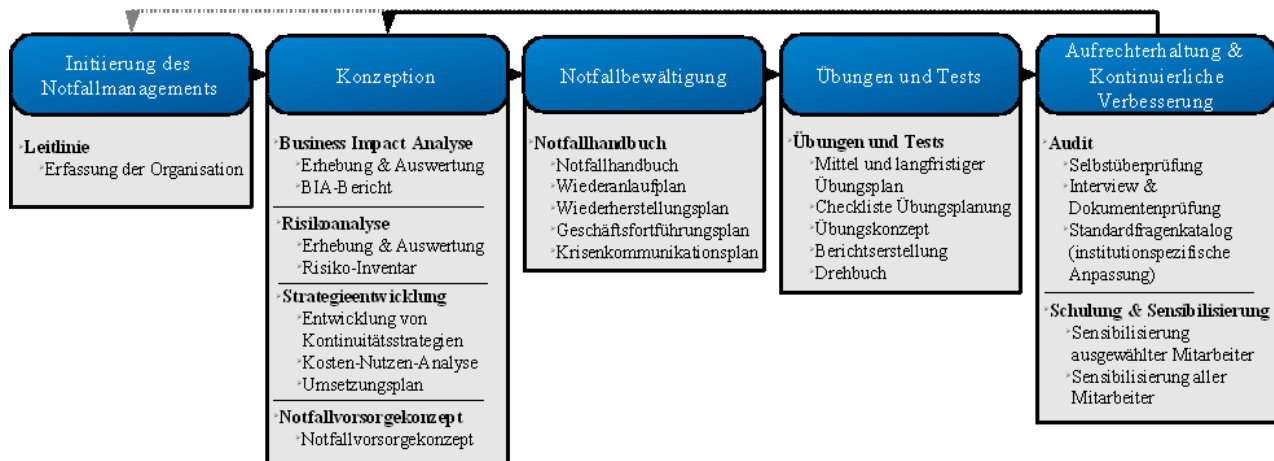


Abbildung 2: Darstellung der Phasen und Module des Umsetzungsrahmenwerks

Das Umsetzungsrahmenwerk (kurz UMRA) beinhaltet Module für die im Folgenden dargestellten Phasen des Notfallmanagement-Prozesses des BSI-Standards 100-4. Eine detaillierte Übersicht der enthaltenen Hilfsmittel der jeweiligen Module kann dem Kapitel 6 „Anhang: Hilfsmittel der Phasen und Module“ entnommen werden.

Im Folgenden werden die Inhalte der einzelnen Module näher dargestellt und kurz erklärt. Im Vergleich mit Abbildung 1 scheint bei Abbildung 2 ein Modul "Umsetzung des Notfallvorsorgekonzepts" zu fehlen. Die Module selbst enthalten allerdings bereits Hilfsmittel (Beschreibungen, Ausfüllanleitungen, Vorlagen, Foliensätze usw.), um die jeweiligen konkreten Aufgaben zu erledigen. Jedes Modul enthält daher schon den Teil "Umsetzung", sodass ein einzelnes Modul für die Umsetzung unnötig ist.

Modul Leitlinie

Bevor ein Notfallmanagement institutionsweit etabliert werden kann, sind zunächst die Rahmenbedingungen zur Umsetzung des Notfallmanagements festzulegen. Diese Rahmenbedingungen und Ziele des Notfallmanagements werden in einer sogenannten Leitlinie dokumentiert. Zentrale Inhalte sind der Geltungsbereich des Notfallmanagements, Kernaussagen zur Notfallstrategie und die Übernahme der Verantwortung durch die Leitung der Institution. Die Leitlinie zum Notfallmanagement ist das zentrale Strategiedokument im Notfallmanagement.

Modul Business Impact Analyse

Die Business Impact Analyse ist das wesentliche Instrument, um kritische Geschäftsprozesse und deren Abhängigkeiten zu den prozessunterstützenden Ressourcen zu erkennen. Sie hat zum Ziel, zu verstehen, welche Geschäftsprozesse wichtig für die Aufrechterhaltung des Geschäftsbetriebs und damit für die Institution sind und welche Folgen ein Ausfall haben kann.

Modul Risikoanalyse

Die Risikoanalyse dient dazu, Gefährdungen zu identifizieren, die auf eine Institution wirken und einen Ausfall der kritischen Ressourcen unter Berücksichtigung der „maximalen tolerierbaren Ausfallzeit“ (MTA) verursachen können. Zusammen mit einer Business Impact Analyse bildet die Risikoanalyse die Grundlage für die Kontinuitätsstrategien und daraus abgeleiteter, präventiver und reaktiver Notfallmaßnahmen.

Modul Strategieentwicklung

Als abschließender Teil der Konzeptionsphase geht die Strategieentwicklung auf die gewonnenen Erkenntnisse der Business Impact Analyse und Risikoanalyse ein. Ziel der Strategieentwicklung ist es, Gegenmaßnahmen in Form von Kontinuitätsstrategien zu definieren, um Risiken und Schwachstellen sowie Restrisiken durch eine funktionierende Notfallvorsorge und -bewältigung zu minimieren. Um dies zu erreichen, sind die wesentlichen Alternativen zu identifizieren und anschließend die für die Institution beste Vorgehensweise auszuwählen.

Modul Notfallvorsorgekonzept

Das Notfallvorsorgekonzept bildet die Grundlage zur Umsetzung der Notfallvorsorge- und Kontinuitätsstrategien. Im Notfallvorsorgekonzept sind alle organisatorischen und konzeptionellen Aspekte sowie alle Maßnahmen und Tätigkeiten des Notfallmanagements, die nicht zur direkten Bewältigung eines Notfalls beitragen, zu beschreiben.

Modul Notfallhandbuch

Das Notfallhandbuch bildet die Gesamtheit aller für die Notfallbewältigung benötigten Dokumente. Es beinhaltet die benötigten Prozeduren, Informationen sowie die erforderlichen Reaktionsmaßnahmen, die nach Eintritt eines Notfalls bis zur Wiederaufnahme des Geschäftsbetriebs erforderlich sind.

Ziel des Notfallhandbuches ist es, eine dokumentierte Vorgehensweise beziehungsweise Hilfestellung für alle Phasen der Notfallbewältigung bereitzustellen, mit deren Unterstützung eine Institution einen Notfall bewältigen und ihre kritischen Geschäftsprozesse fortführen kann.

Modul Übungen und Tests

In Übungen und Tests werden Pläne oder Abläufe der Notfallplanung mit praktischer Beteiligung der Mitarbeiter überprüft. Die in Übungen und Tests festgestellten Ergebnisse liefern wertvolle Erkenntnisse, um die Notfallplanung ständig zu verbessern und weiter auf die speziellen Begebenheiten der Institution anzupassen.

Modul Audit

Um sicherstellen zu können, dass die Anforderungen an die Umsetzung des Notfallmanagements in der Institution erfüllt werden, ist eine regelmäßige Überprüfung in Form von Audits und Selbstüberprüfungen (Self-Assessments) des Notfallmanagementsystems durchzuführen. Hierbei ist neben der Funktions- und Leistungsfähigkeit auch die Angemessenheit des Notfallmanagements zu berücksichtigen.

Modul Schulung und Sensibilisierung

Alle Mitarbeiter einer Institution müssen über den Sinn und Zweck des Notfallmanagements Bescheid wissen und dessen Mehrwert erkennen. Vor allem müssen sie alle Aktivitäten des Notfallmanagements rund um ihren Arbeitsplatz kennen, sowohl diejenigen, die sie selbst ausführen müssen, als auch diejenigen, von denen sie indirekt betroffen sein können. Die einzelnen Mitarbeitergruppen (Leitungsebene, Referatsleiter, Techniker, Sachbearbeiter, etc.) müssen für ihre jeweiligen Aufgaben geschult und für die Gefahren eines Notfalls sensibilisiert werden. Dieses Modul unterstützt den Notfallbeauftragten dabei, entsprechende Schulungs- und Sensibilisierungspläne zu erstellen und die Wirkung dieser Schulungs- und Sensibilisierungsmaßnahmen zu erheben, auszuwerten und zu verbessern.

4 Stufenmodell des Notfallmanagementsystems nach diesem Umsetzungsrahmenwerk

4.1 Darstellung des Stufenmodells

Ein vollständiges Notfallmanagementsystem erfordert eine detaillierte Konzeption von Rollen, Verantwortlichkeiten, Prozessen, Dokumenten und Plänen. Die vollständige Entwicklung und institutionsspezifische Anpassung ist schrittweise einzuführen und kontinuierlich anzupassen.

Die Einführung eines Notfallmanagements umfasst eine Anzahl von Arbeitsschritten und Dokumentationen und ist somit – je nach Größe einer Institution – mit einem nicht zu vernachlässigenden Aufwand bei der erstmaligen Etablierung verbunden.

Das Stufenmodell zum Umsetzungsrahmenwerk (kurz UMRA) dient dem Zweck, es Institutionen jeder Größe und Art zu ermöglichen, bereits frühzeitig ein Notfallmanagement konform zum BSI-

Standard 100-4 aufzubauen, beziehungsweise erste zielgerichtete Aktivitäten durchführen zu können, ohne schon im ersten Schritt den gesamten Umfang aller Module des Umsetzungsrahmenwerks umzusetzen. Die Module sind so ausgestaltet, dass eine Erweiterung zu höheren Stufen jederzeit teilweise oder vollständig erfolgen kann.

Damit jede Institution ein angemessenes Notfallmanagement etablieren kann, werden in diesem Stufenmodell drei aufeinander aufbauende Stufen beschrieben. Diese Stufen erlauben es, unter Berücksichtigung der verfügbaren Ressourcen (personeller und finanzieller Art) sowie den institutionsspezifischen Anforderungen, ein geeignetes Notfallmanagement einzuführen.

Aus diesem Grund werden im Folgenden drei unterschiedliche Stufen betrachtet, die aufeinander aufbauen und zur kontinuierlichen Verbesserung des Notfallmanagements beitragen:

- Stufe 1: Die Institution wird dazu befähigt, in Notfall- und Krisensituationen grundsätzlich handlungsfähig zu bleiben. Dazu werden rein reaktive Maßnahmen zum Notfallmanagement etabliert.
- Stufe 2: Es erfolgt eine zum BSI-Standard 100-4 kompatible, jedoch noch auf das Notwendigste reduzierte Umsetzung eines Notfallmanagements. Dazu werden grundlegende präventive und reaktive Maßnahmen zum Notfallmanagement etabliert.
- Stufe 3: Das im BSI-Standard 100-4 beschriebene Notfallmanagementsystem ist vollständig umgesetzt. Auf Basis eines kontinuierlichen Verbesserungsprozesses wird sichergestellt, dass sich die Umsetzung auf einem angemessenen, wirtschaftlichen Niveau befindet und bedarfsgerechte Korrektur- und Optimierungsmaßnahmen durchgeführt werden.

Je höher die angestrebte Stufe ist, desto mehr Ressourcen müssen eingesetzt werden, um diese zu erreichen, und desto länger dauert auch die Umsetzung. Die folgende Abbildung stellt die Wirkungsbeziehung zwischen dem Entwicklungszeitraum und dem benötigten Ressourceneinsatz über die einzelnen Stufen hinweg dar.

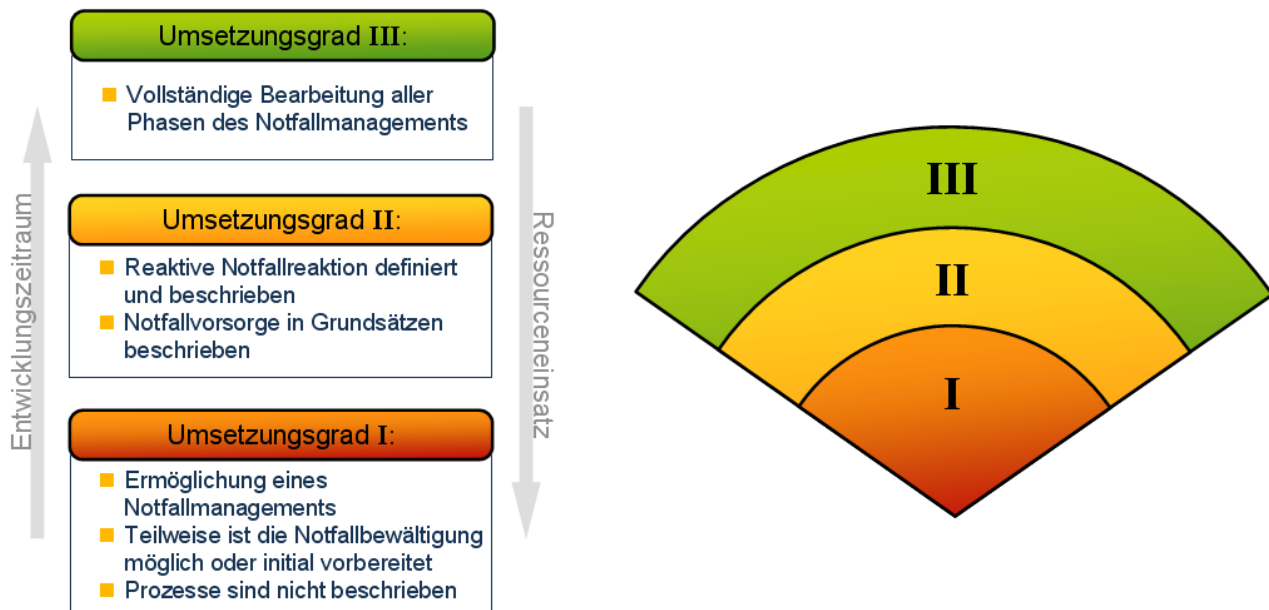


Abbildung 3: Das UMRA-Stufenkonzept

Die einzelnen Stufen werden in separaten Leitfäden beschrieben. In diesen Leitfäden werden zudem die Voraussetzungen der einzelnen Phasen und Module erläutert, Mindestinhalte zur Erreichung der jeweiligen Stufe angegeben und die einzelnen Hilfsmittel detailliert dargestellt. Dadurch wird verdeutlicht, welche Anforderungen zur Erreichung der jeweiligen Stufe erfüllt werden müssen. Die jeweiligen Modulbeschreibungen geben das Vorgehen zur Bearbeitung der Hilfsmittel in der Maximalausprägung an. Es steht selbstverständlich jeder Institution frei, Anforderungen des Leitfadens der gewählten Stufe zu übertreffen und Module in einer höheren Ausprägung zu bearbeiten.

4.2 Stufen des Umsetzungsrahmenwerks

4.2.1 Stufe 1 – Basis des Notfallmanagements: Notfallreaktion

Die Stufe 1 stellt den Einstieg in das Notfallmanagement dar und fokussiert mehr darauf, eine angemessene Notfallreaktion zu ermöglichen als das Managementsystem vollständig aufzubauen. Es werden keine Prozesse entwickelt und umgesetzt, vielmehr werden einzelne Maßnahmen für eine Reaktion auf bestimmte Arten von Notfällen festgelegt. Die Stufe 1 dient somit dazu, zunächst Basismaßnahmen zur Ermöglichung eines (reaktiven) Notfallmanagements zu entwickeln. Der Schwerpunkt liegt dabei darauf, eine geeignete Notfalldokumentation zur Reaktion auf Notfälle zu erstellen und darin Maßnahmen zur Sofortreaktion, zum Wiederanlauf, zur Geschäftsfortführung und der Wiederherstellung zu beschreiben.

4.2.2 Stufe 2 – Etablierung eines Notfallmanagements: Notfallvorsorge und Notfallreaktion

Die Stufe 2 beinhaltet alle Aktivitäten der Stufe 1. In der Stufe 2 werden außerdem die kritischen Ressourcen der Geschäftsprozesse hinsichtlich möglicher Gefährdungen überprüft. Diese werden innerhalb einer Risikoanalyse erhoben und fließen mit den Ergebnissen der Business Impact Analyse in die Strategieentwicklung zum Notfallmanagement ein. Darüber hinaus erfolgt eine strukturierte Konzeption der Notfallvorsorge. Ferner werden Selbstüberprüfungen durchgeführt. Ein umfassender Prozess zur Sicherstellung eines dauerhaften Qualitätsniveaus des Notfallmanagementsystems wird jedoch nicht vollständig sichergestellt.

4.2.3 Stufe 3 – BSI Standard 100-4: Etablierung und kontinuierliche Verbesserung eines Notfallmanagementprozesses

Um Stufe 3 zu erreichen, wird zusätzlich zu den Aktivitäten der Stufen 1 und 2 der ganzheitliche Prozess eines Notfallmanagementsystems etabliert. Mit dieser Stufe wird ein dauerhaftes Qualitätsniveau des Notfallmanagements erreicht. Es werden somit nicht nur initiale Dokumente zur Reaktion auf einzelne Notfallszenarien erstellt. Vielmehr werden Verfahren aufgesetzt, die es einer Institution ermöglichen, sich jederzeit auf neue oder sich verändernden Anforderungen an das Notfallmanagementsystem einzustellen und das Notfallmanagementsystem entsprechend anpassen zu können.

4.3 Auswahl der geeigneten Leitfaden-Variante

Aufbauend auf dem vorliegenden Umsetzungsrahmenwerk, den darauf folgenden Leitfäden und den darin erläuterten Anforderungen zur Umsetzung ergibt sich die im Folgenden dargestellte Struktur. Zusätzlich unterscheiden sich die Stufen in der Menge der zu nutzenden Dokumente und Hilfsmittel sowie dem zur Umsetzung erforderlichen Ressourceneinsatz.

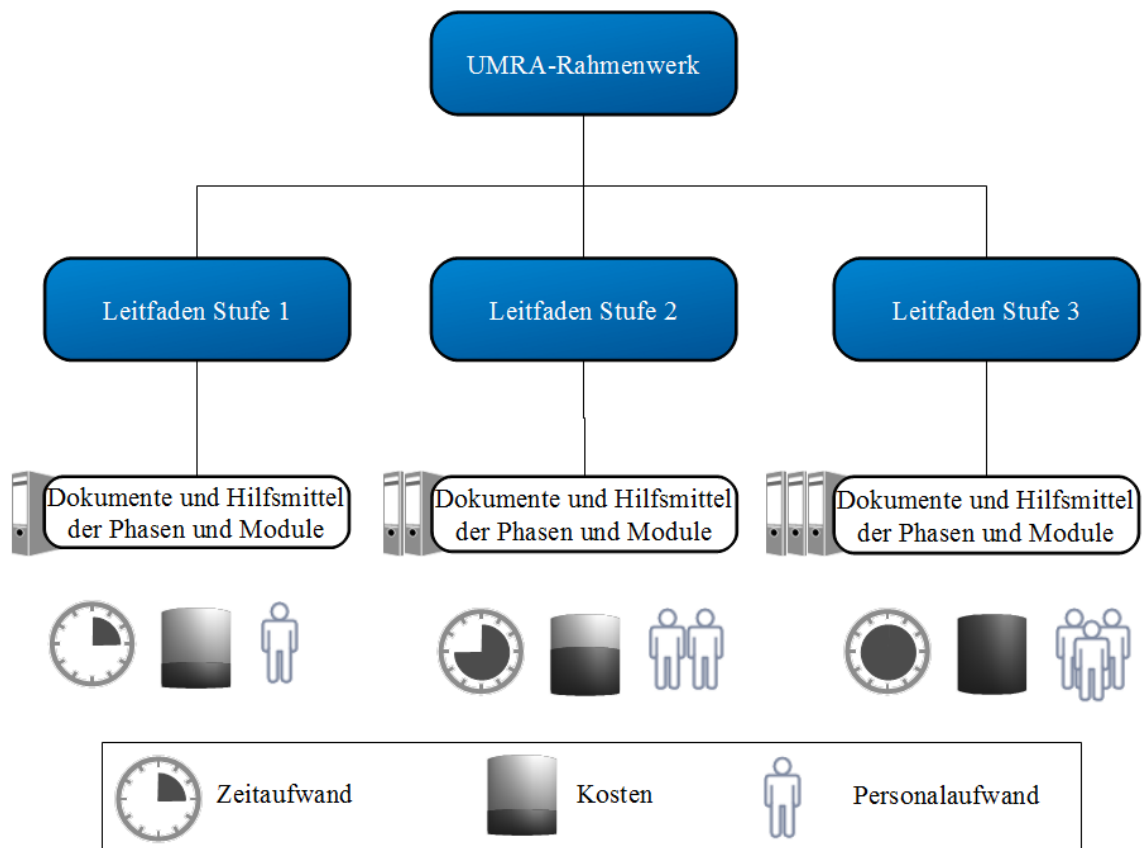


Abbildung 4: Struktur des Umsetzungsrahmenwerks

Der Umfang und die Ausprägung eines für die jeweilige Institution geeigneten Notfallmanagements hängt in der Praxis von zahlreichen Faktoren ab.

Wie viel Ressourcen zum Aufbau und Betrieb eines angemessenen Notfallmanagements benötigt werden, hängt entscheidend von der Größe und der Art der Institution, der Art der Geschäftsprozesse, aber auch der Art und Anzahl der Standorte, der Umgebung der Standorte, dem Geschäftsumfeld, den Kunden, der eingesetzten Technik oder der Bereitschaft der Institution, Risiken einzugehen (Risikoappetit), ab.

Daneben gibt es eine Vielzahl weiterer Einflussfaktoren. Einige davon sind teilweise auch spezifisch für Einrichtungen der öffentlichen Verwaltung geltende Aspekte. Diese sind beispielsweise:

- Aktueller Stand bzw. Umsetzungsgrad des Notfallmanagements: Dieser kann anhand von Auditierungen oder Selbstüberprüfungen festgestellt werden.
- Verfügbare Haushaltsmittel
- Verfügbare personelle Ressourcen
- Art des IT-Betriebs (IT im Eigenbetrieb oder ausgelagerte IT)
- Vorhandener Schutzbedarf

- Parallel zur Umsetzung eines Notfallmanagements geplante oder bereits laufende Vorhaben innerhalb der Institution, wie z. B. größere Umstrukturierungen oder Projekte

Aufgrund der vielfältigen Varianten, die sich aus der Kombination der oben genannten Faktoren ergeben, ist es schwierig, für jede einzelne Möglichkeit separate Beschreibungen für eine geeignete Umsetzung zu erstellen.

Zur Auswahl der geeigneten Stufe kann die Vorbetrachtung der erwarteten Ergebnisse der jeweiligen Stufe beitragen.

Ergebnisse der Stufe 1

Mit der Bearbeitung der Stufe 1 stehen lediglich die reaktiven Hilfsmittel in initialer Ausprägung zur Verfügung. Auf die Erarbeitung präventiver Maßnahmen wird komplett verzichtet. Darüber hinaus wird auf eine Analyse möglicher Gefährdungen und einer Selbstüberprüfung verzichtet.

Ergebnisse der Stufe 2

In Stufe 2 werden Anforderungen zur Erstellung und Umsetzung präventiver und reaktiver Maßnahmen gestellt. Darüber hinaus sind in dieser Stufe Anforderungen zur Identifikation von Gefährdungen und Risiken beschrieben und es wird auf alle Schritte des Notfallmanagement-Prozesses eingegangen. Ein umfassender Prozess zur Sicherstellung eines dauerhaften Qualitätsniveaus wird jedoch nicht vollständig etabliert. Unter anderem sind die Anforderungen an Übungen und Tests sowie Selbstüberprüfungen reduziert.

Ergebnisse der Stufe 3

Mit der Bearbeitung der Stufe 3 wird ein vollständiges Notfallmanagement nach dem BSI-Standard 100-4 umgesetzt. Außerdem werden Maßnahmen eingeführt, die eine kontinuierliche Weiterentwicklung und Verbesserung des Notfallmanagementsystems ermöglichen.

5 Fazit

Das Umsetzungsrahmenwerk unterstützt Behörden und Unternehmen bei der Umsetzung eines Notfallmanagements, indem hier Leitfäden, Modulbeschreibungen und weitere Hilfsmittel zur Verfügung gestellt werden, die als Grundlagen zum Aufbau und Betrieb eines Notfallmanagements genutzt werden können. Alle Module und ihre Hilfsmittel können auf den Webseiten des BSI kostenfrei heruntergeladen werden. Für Behörden steht eine ausführlichere Variante der Hilfsmittel auf den Seiten der Sicherheitsberatung des Bundes zur Verfügung.

Mit Fragen, Anregungen und Kritik können Sie sich gerne jederzeit an den IT-Grundschutz wenden.

Die Kontaktdaten sind wie folgt:

Bundesamt für Sicherheit in der Informationstechnik Referat B 21
Postfach 200363
53133 Bonn
Telefon: 0228 99 9582-5369
+49 228 99 9582-5369
E-Mail: grundschutz@bsi.bund.de

Darüber hinaus unterstützt das Bundesamt für Sicherheit in der Informationstechnik bei folgenden Themen:

- Fragen oder Problemstellungen, die bei der Bearbeitung der Phasen und Module entstehen
- Identifikation möglicher Seiteneffekte bei institutionsspezifischen Anpassungen der Hilfsmittel und Inhalte
- Aufnahme von identifizierten Verbesserungs- und Optimierungsvorschlägen

Ausführliche Informationen sind im BSI-Standard 100-4 und im BSI Webkurs Notfallmanagement zu finden.

Die Dokumente des Umsetzungsrahmenwerks wurden durch die Firma HiSolutions AG im Auftrag des BSI erstellt.

6 Anhang: Hilfsmittel der Phasen und Module

Zu den Hilfsmitteln des Umsetzungsrahmenwerks gehören Modulbeschreibungen, Dokumentenvorlagen, Ausfüllanleitungen, Frage- und Erhebungsbögen, Auswertungsbögen sowie Berichts- und Präsentationsvorlagen. Alle Hilfsmittel stehen in den Formaten von Microsoft Office und OpenOffice zur Verfügung. In der folgenden Liste sind in der Spalte "Enthaltene Hilfsmittel" die jeweiligen Dateinamen ohne Dateiendung angegeben. Die Phasen und Module sind je nach Stufe unterschiedlich stark zu bearbeiten. Die Hilfsmittel enthalten bis auf die Risikoanalyse immer die maximale Detailtiefe und sind je nach Anforderung des Leitfadens der Stufe anzupassen. Die Risikoanalyse ist aufgrund spezieller Anforderungen in drei Varianten unterteilt.

Behörden finden ergänzende Hilfsmittel zu den Modulen auf den Webseiten der Sicherheitsberatung des Bundes, diese sind in der folgenden Auflistung mit einem „*“ gekennzeichnet. Hilfsmittel, die in einer ausführlicheren Variante auf den Webseiten der Sicherheitsberatung des Bundes zur Verfügung stehen, sind mit folgendem Zeichen „#“ gekennzeichnet. Diese ausführlicheren Hilfsmittel stehen in einer gekürzten Fassung auch auf den Webseiten des BSI für alle offen zur Verfügung.

Phase	Modul	Enthaltene Hilfsmittel
Initiierung des Notfallmanagements	Leitlinie	Leitlinie_Modulbeschreibung
		Leitlinie_Dokumentenvorlage
		Leitlinie_Ausfüllanleitung #
		Leitlinie_Präsentation
Konzeption	Business Impact Analyse (BIA)	BIA_Modulbeschreibung
		BIA_Erhebungsbogen
		BIA_Erhebungsbogen_Ausfüllanleitung
		BIA_Auswertungsbogen *
		BIA_Auswertungsbogen_Ausfüllanleitung *
		BIA_Bericht #
		BIA_Workshop_Präsentation
		BIA_Abschlusspräsentation

Phase	Modul	Enthaltene Hilfsmittel
Konzeption	Risikoanalyse	Risikoanalyse_Modulbeschreibung_Variante_A
		Risikoanalyse_Modulbeschreibung_Variante_B
		Risikoanalyse_Modulbeschreibung_Variante_C
		Risikoanalyse_Erhebungsbogen_Variante_A
		Risikoanalyse_Erhebungsbogen_Variante_B
		Risikoanalyse_Erhebungsbogen_Variante_C
		Risikoanalyse_Erhebungsbogen_Ausfüllanleitung_Variante_A
		Risikoanalyse_Erhebungsbogen_Ausfüllanleitung_Variante_B
		Risikoanalyse_Erhebungsbogen_Ausfüllanleitung_Variante_C
		Risikoanalyse_Workshop_Präsentation_Variante_A
		Risikoanalyse_Workshop_Präsentation_Variante_B
		Risikoanalyse_Workshop_Präsentation_Variante_C
		Risiko-Inventar_Variante_A
		Risiko-Inventar_Variante_B
		Risiko-Inventar_Variante_C
Konzeption	Strategieentwicklung	Strategieentwicklung_Modulbeschreibung
		Strategieentwicklung_Kosten-Nutzen-Analyse
		Strategieentwicklung_Kosten-Nutzen-Analyse_Ausfüllanleitung
		Strategieentwicklung_Umsetzungsplan
		Strategieentwicklung_Umsetzungsplan_Ausfüllanleitung

Phase	Modul	Enthaltene Hilfsmittel
		Strategieentwicklung_Präsentation_zur_Auswahl_von_Kontinuitätsstrategien
		Strategieentwicklung_Workshop_Präsentation
Konzeption	Notfallvorsorgekonzept	Notfallvorsorgekonzept_Modulbeschreibung
		Notfallvorsorgekonzept_Dokumentenvorlage
		Notfallvorsorgekonzept_Dokumentenvorlage_Ausfüllanleitung
		Notfallvorsorgekonzept_Präsentation
Notfallbewältigung	Notfallhandbuch	Notfallhandbuch_Modulbeschreibung
		Notfallhandbuch_Dokumentenvorlage
		Notfallhandbuch_Dokumentenvorlage_Ausfüllanleitung
		Notfallhandbuch_Präsentation
		Notfallhandbuch_Wiederanlauf_Wiederherstellung_Dokumentenvorlage
		Notfallhandbuch_Wiederanlauf_Wiederherstellung_Dokumentenvorlage_Ausfüllanleitung
		Notfallhandbuch_Wiederanlauf_Wiederherstellung_Präsentation
		Notfallhandbuch_Geschäftsfortführungsplan_Dokumentenvorlage
		Notfallhandbuch_Geschäftsfortführungsplan_Dokumentenvorlage_Ausfüllanleitung
		Notfallhandbuch_Notfall_und_Kommunikationsplan_Dokumentenvorlage
		Notfallhandbuch_Notfall_und_Kommunikationsplan_Dokumentenvorlage_Ausfüllanleitung

Phase	Modul	Enthaltene Hilfsmittel
Übungen und Tests	Übungen und Tests	Übungen_und_Tests_Modulbeschreibung
		Übungen_und_Tests_Ausfüllanleitung #
		Übungen_und_Tests_Übungsplan
		Übungen_und_Tests_Übungssteckbrief
		Übungen_und_Tests_Übungskonzept
		Übungen_und_Tests_Übungsdrehbuch
		Übungen_und_Tests_Einladungen
		Übungen_und_Tests_Protokoll_kurz
		Übungen_und_Tests_Protokoll_umfänglich
		Übungen_und_Tests_Fragebogen_Sofortauswertung
		Übungen_und_Tests_Ergebnisbericht
		Übungen_und_Tests_Präsentation
Aufrechterhaltung & kontinuierliche Verbesserung	Audit	Audit_Modulbeschreibung
		Audit_Ausfüllanleitung #
		Audit_Auditplanung
		Audit_Workshop_Selbstüberprüfung *
		Audit_Fragebogen_Selbstüberprüfung *
		Audit_Ergebniszusammenführung_Selbstüberprüfungen *
		Audit_Ergebnisbericht *
	Schulung und Sensibilisierung	Schulung_Sensibilisierung_Modulbeschreibung

Phase	Modul	Enthaltene Hilfsmittel
		Schulung_Sensibilisierung_Schulungsplan
		Schulung_Sensibilisierung_Ausfuellanleitung
		Schulung_Sensibilisierung_Dokumentenvorlage