(IT) Notfallmanagement

im Unternehmen und in der Behörde

Planung, Umsetzung und Dokumentation gemäß BSI-Standard 100-4, ISO 22301 und BCI-GPG 2013

Praxisleitfaden für eine softwaregestützte Implementierung

eines unternehmensweiten Notfallmanagementsystems

mit DocSetMinder®

Krzysztof M. Paschke

Weitere Informationen zum Thema Prozesse, Governance Risk und Compliance, Compliance Management Software DocSetMinder® finden Sie auf folgenden Internetseiten:
www.docsetminder.de
www.grc-partner.de

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

ISBN 978-3-7322-7418-5

Herstellung und Verlag: Books on Demand GmbH, Norderstedt

Lektorat: Wirtschaftsinformatikerin (BA) Sigrid Paschke

Vorwort

Grundvoraussetzung für die Konzeption und Umsetzung einer unternehmensweiten Notfallvorsorge und -bewältigung ist die genaue Kenntnis der involvierten Mitarbeiter und Führungskräfte über die Unternehmensorganisation und Ressourcen. Ein bestimmter Teil der Prozesse und Ressourcen, die in organisatorischen Einheiten zusammen gefasst sind, sind von existenzieller Bedeutung für das Unternehmen und die Behörde. Im Rahmen deren kritischer Betrachtung, auch als Business Impact Analyse (BIA) bezeichnet, werden die wertschöpfenden Prozesse und beteiligten Ressourcen ermittelt und in der Notfallvorsorge besonders behandelt. Bei der Betrachtung der Ressourcen steht die IT-Infrastruktur im Vordergrund. Generell kann behauptet werden, dass heutzutage nahezu alle Geschäftsprozesse eines Unternehmens oder einer Behörde durch die IT-Infrastruktur (Hardware, Software) abgebildet und gesteuert werden. Von ihrer Verfügbarkeit und Zuverlässigkeit hängt die Leistungserstellung des Unternehmens und der Behörde ab. Ein weiterer Aspekt des betrieblichen Kontinuitätsmanagements ist die Identifizierung von Risiken, die zur Beeinträchtigung oder zum Ausfall der wertschöpfenden Prozesse und Ressourcen führen können. Im Rahmen der Risikoanalyse werden mögliche Ursachen, Auswirkungen, Eintrittswahrscheinlichkeiten und Folgen bestimmt. Die Ergebnisse der Business Impact- und Risikoanalyse sind ausschlaggebend für den Umfang und Inhalt des Notfallvorsorgekonzeptes. Ergebnisse der Notfallvorsorge sind die umgesetzten Notfallvorsorgemaßnahmen und eine strukturierte Notfallbewältigung. Klar definierte Alarmierung, Sofortmaßnahmen und Eskalationsschritte für unterschiedliche Notfallszenarien werden im Notfallhandbuch dokumentiert und den Notfallteams und Mitarbeitern zur Verfügung gestellt. Der vorliegende Praxisleitfaden beschreibt eine systematische Vorgehensweise für die Umsetzung und Etablierung einer effektiven und effizienten Notfallorganisation im Rahmen eines Projektes. Die beschriebene Methodik eignet sich sowohl für produzierende Unternehmen, für Behörden als auch für Non-Profit Organisationen. Sie berücksichtigt die Aufbau- und Ablauforganisation, die vorhandene IT-Infrastruktur und die Ressourcen des Unternehmens

und der Behörde. Die Dokumentation spielt im Verlauf des Projektes eine besondere Rolle. Die Bedeutung ihrer Vollständigkeit und Aktualität wird häufig unterschätzt. Sie dient dem Nachweis sowie als Kommunikationsmedium der getroffenen organisatorischen und technischen Maßnahmen. Durch den Einsatz der Compliance Management Software DocSetMinder® kann die Umsetzung und Etablierung, Verbesserung, Dokumentation und Prüfung des unternehmensweiten Notfallmanagements sehr effizient und effektiv realisiert werden.

Inhaltsverzeichnis

1 Ziel und Aufbau des Buches

Die Konzeption, Umsetzung und langfristige Etablierung eines unternehmensweiten Notfallmanagements wird im Rahmen eines Projektes realisiert. Die vorliegende Publikation beschreibt detailliert die strukturierte Vorgehensweise eines Notfallmanagementprojektes und kann als Praxisleitfaden genutzt werden. Sie wendet sich an alle involvierten Mitarbeiter des Projektes: An die Geschäftsführung und Projektleitung sowie an die Mitarbeiter aus den Notfallteams und Fachabteilungen bis hin zu externen Beratern, die mit der genannten Aufgabe beauftragt worden sind. Die Verwendung anerkannter Normen und Standards mit ihren Anforderungen an ein Notfallmanagementsystem setzen die genaue Kenntnis und Dokumentation der Unternehmensorganisation (Aufbau- und Ablauforganisation) und des IT-Verbundes (IT-Organisation, -Infrastruktur und Ressourcen) voraus. Die betriebliche Praxis stellt sich oft anders dar. Eine Dokumentation der genannten Organisations- und IT-Sachverhalte ist häufig nicht vorhanden, nicht vollständig oder nicht mehr aktuell. Bei der hier beschriebenen Methodik geht der Autor von der Annahme aus, dass eine solche Dokumentation nicht vorhanden ist. Eine weitere Annahme ist, dass der Kenntnisstand der Projektmitarbeiter über die Unternehmens- und IT-Organisation unterschiedlich ist.

Wesentliche Abschnitte (Meilensteine) des Projektes beschreiben die IST-Aufnahme, Bewertung und Dokumentation der Unternehmensorganisation und des IT-Verbundes. Die auf diese Art und Weise gewonnenen Informationen werden für die Planung und Umsetzung des Notfallmanagements verwendet und gleichen Informationsdefizite der in dem Projekt involvierten Mitarbeiter aus. Durch die Bereitstellung einer Notfallmanagement-Dokumentation mit den beschriebenen Prozessen, Handlungsanweisungen, Richtlinien und weiteren Unterlagen soll ein gleiches Verständnis der Führungskräfte und der in die Notfallvorsorge und -bewältigung involvierten Mitarbeiter bei der Erfüllung ihrer Tätigkeit für die festgelegten unternehmensweiten Anforderungen an das

Notfallmanagement sichergestellt werden. Die Dokumentation stellt die Basis für eine permanente Verbesserung der bereits etablierten Notfallmanagement-Strukturen und Abläufe im Unternehmen dar. Schwerpunkt der Publikation ist die Darstellung einer strukturierten Vorgehensweise bei der Planung und Umsetzung der Notfallorganisation gemäß BSI-Standard 100-4[1]. Weitere Standards wie ISO 22301:2012[2] und BCI-GPG 2013[3] werden zitiert ohne sie direkt miteinander zu vergleichen.

Abbildung 1: Inhaltsstruktur des Leitfadens.

Durch die große Übereinstimmung der Inhalte der genannten Standards kann der Praxisleitfaden auch bei ihrer Umsetzung verwendet werden. Die im Folgenden beschriebene zentrale, datenbankbasierte Softwarelösung DocSetMinder® bietet viele technische und organisatorische Vorteile, nicht nur bei der Erstellung und Aktualisierung der Dokumentation, sondern insbesondere auch

[1] Bundesamt für Sicherheit in der Informationstechnik – Standard 100-4 Notfallmanagement.
[2] ISO 22301:2012 Business continuity management system.
[3] Business Continuity Institute - Good Practice Guidelines 2013, Global Edition.

bei der systematischen Verbesserung der Notfallorganisation im Laufe der Zeit. Der noch immer weit verbreitete Einsatz von Textverarbeitungsprogrammen und Tabellenkalkulationen bei derartigen Projekten stellt für diese Aufgaben keine echte Alternative dar. Die in dieser Publikation verwendete Projekt-Methodik ist unabhängig von der geplanten oder bereits eingesetzten Softwarelösung. **Abbildung 1** visualisiert die Struktur des Leitfadens.

In **Kapitel 2** wird die Motivation für die Etablierung eines unternehmensweiten Notfallmanagements skizziert. Darüber hinaus wird die Rolle der Unternehmensorganisation (Aufbau- und Ablauforganisation) und des IT-Verbundes (IT-Organisation, -Infrastruktur und Ressourcen) im Notfallmanagement erläutert.

Die Compliance Management Software **DocSetMinder®** unterstützt das Projektteam bei der Durchführung und Dokumentation des Notfallmanagementprojektes in allen Phasen. Der Nutzen und die für das Projekt notwendigen Module „Unternehmensorganisation“, „IT-Dokumentation“ und „Notfallmanagement“ werden in **Kapitel 3** kurz beschrieben.

In **Kapitel 4** werden die gesetzlichen Grundlagen exemplarisch kurz aufgezählt, ohne Anspruch auf Vollständigkeit. Die Einhaltung von Gesetzen und Vorschriften[4] durch die Gestaltung und Umsetzung einer effektiven Corporate Governance[5] stellt eine wesentliche Herausforderung für die Führungskräfte und Aufsichtsgremien in Unternehmen dar. Das betriebliche Kontinuitätsmanagement ist ein fester Bestandteil der Corporate Governance. Die Basis für ihre Umsetzung schaffen geltende Gesetze, Standards, Richtlinien und nicht zuletzt Verträge und Vereinbarungen mit Geschäftspartnern, die von Unternehmen und Behörden einzuhalten sind.

[4] Compliance
[5] Grundsätze der Unternehmensführung.

Aufgrund der Bedeutung des Notfallmanagements für ein Unternehmen oder eine Behörde sollte die Umsetzung generell nur nach anerkannten Standards und Normen erfolgen. In **Kapitel 5** werden die wichtigsten Notfallmanagement Normen und Standards dargestellt, vor allem der BSI-Standard 100-4, ISO 22301:2012 und BCI Good Practice Guidelines 2013 Global Edition. Durch ihre Struktur und Methodik liefern die genannten Standards eine Grundvoraussetzung für eine optimale Projektplanung und effektive Umsetzung sowie für die Ermittlung der Projektkosten. Die Folge ist eine hohe Akzeptanz, bei den direkt involvierten Projektmitarbeitern im Unternehmen und einer Behörde, bei externen Organisationen und Auditoren.

Kapitel 6 ist der Bedeutung der Dokumentation gewidmet. Eine vollständige und sachgerechte Dokumentation der wesentlichen Sachverhalte des Notfallmanagement-Projektes stellt die Grundlage einer erfolgreichen Umsetzung der Notfallorganisation dar und dient dem Nachweis der getroffenen organisatorischen und technischen Maßnahmen. Sie ist Grundelement eines Notfallmanagements und unabdingbar bei deren sorgfältigen Umsetzung, Überwachung und Verbesserung. Darüber hinaus dient sie als sehr effektives organisationsweites Kommunikationsmedium bei der Bekanntmachung und Verbreitung der getroffenen Maßnahmen für alle Mitarbeiter. Die Dokumentation ist erforderlich bei jeder Art von Prüfung, die durch interne oder externe Auditoren und Prüfer durchgeführt wird.

In **Kapitel 7** ist das Projekt „Notfallmanagement“ mit allen Facetten der Projektorganisation sehr detailliert beschrieben. Am Beispiel einer fiktiven Firma, der Wind Seeker AG, wird das gesamte Projekt „Notfallmanagement“ in mehreren Meilensteinen und Vorgängen erläutert. Sie bilden die Anforderungen der in **Kapitel 5** dargestellten Standards ab. Im **Meilenstein 1 „Projektorganisation“** werden alle organisatorischen Maßnahmen für eine strukturierte und erfolgreiche Durchführung des Projektes festgelegt und dokumentiert. Im **Meilenstein 2 „Unternehmensorganisation“** wird die Aufbau- und Ablauforganisation

des Unternehmens systematisch aufgenommen, nach bestimmten Kriterien bewertet und dokumentiert. Die somit gewonnenen Informationen werden im **Meilenstein 4 „Notfallmanagement“** verwendet. Im **Meilenstein 3 „IT-Verbund“** wird die IT-Organisation (IT-Infrastruktur, -Organisation und Ressourcen) des Unternehmens systematisch aufgenommen, nach bestimmten Kriterien bewertet und dokumentiert. Die dokumentierten Sachverhalte werden im **Meilenstein 4 „Notfallmanagement“** verwendet.

In **Kapitel 8** werden die Einsatzbereiche und der Funktionsumfang der Compliance Management Software DocSetMinder® beschrieben. DocSetMinder® unterstützt die Unternehmensleitung und das Projektteam bei der Konzeption, Dokumentation, Prüfung und Verbesserung der Notfallorganisation. Durch den modularen Aufbau kann DocSetMinder® bei weiteren Compliance-Themen effektiv und effizient im Unternehmen eingesetzt werden (vgl. ***www.docsetminder.de***).

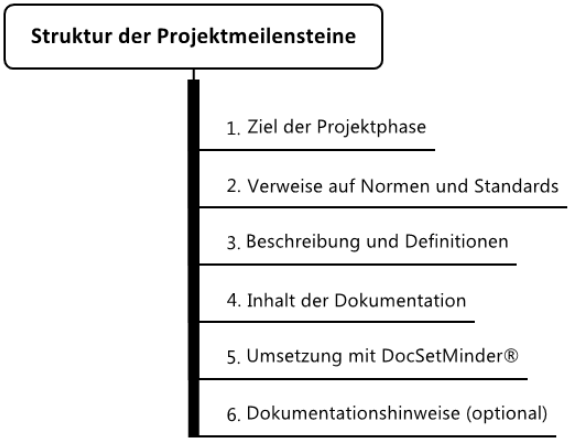

Abbildung 2: Struktur der Projektmeilensteine.

Die Beschreibung der einzelnen Projektmeilensteine (vgl. **Abbildung 2**) im Wind Seeker AG-Notfallmanagementprojekt ist jeweils gleich strukturiert und besteht aus folgenden Abschnitten:

- **Ziel der Projektphase** - Beschreibung der Ziele, die am Ende der Projektphase erreicht werden sollen.
- **Verweise auf Standards** - Jede Phase des Notfallmanagementprojektes ist durch Normen und Standards begründet. Die Standards BSI-Standard 100-4, ISO 22301 und BCI-GPG 2013 werden an dieser Stelle auszugsweise zitiert.
- **Beschreibung** und **Definitionen** - Sachverhalte und Definitionen werden im jeweiligen Meilenstein detailliert beschrieben und erläutert.
- **Inhalt der Dokumentation** - Das Ergebnis des Projektmeilensteines ist in Form einer Dokumentation zusammengefasst. Sie ist ein Bestandteil der Notfallmanagementdokumentation. Für die Erfassung der Sachverhalte werden zahlreiche Checklisten vorgeschlagen.
- **Umsetzung** mit DocSetMinder® - Beispiele der Dokumentation werden mit Hilfe der DocSetMinder® Software mit einigen Screenshots präsentiert. Es handelt sich dabei um Auszüge aus der Notfallmanagement-Dokumentation der Wind Seeker AG (vgl. **Kapitel 7.3**)
- **Dokumentationshinweise** (optional) - Hinweise zur Methodik für die Erstellung und Pflege der Dokumentation. Dazu gehören u.a. Imports von Informationen aus anderen Systemen, wie z.B. ERP, Active Directory, Inventory-Systeme etc.

2 Notfallmanagement – Motivation

Hauptaufgabe der Unternehmensleitung ist die Umsetzung der geplanten Unternehmensziele und eine langfristige Marktbehauptung. Grundvoraussetzung hierfür ist ein kontinuierlicher und störungsfreier Geschäftsbetrieb des Unternehmens oder der Behörde, insbesondere in den globalisierten und sich schnell veränderten Märkten. Eine vorübergehende Unterbrechung der Produktion oder Dienstleistung kann zum Verlust von Kunden führen. Durch die Verkettung der Geschäftsprozesse von Lieferanten und Auftraggebern ist ein hoher Grad an wirtschaftlicher Abhängigkeit erreicht. Sehr deutlich ist dies bei der Betrachtung der „just-in-time“ Lieferketten zu erkennen. Eine Unterbrechung der Lieferung kann nicht nur einen wirtschaftlichen sondern auch einen Imageschaden bedeuten. Das Image eines langjährigen zuverlässigen Geschäftspartners wird über Jahre durch die sorgfältige Erfüllung der vereinbarten Leistungen aufgebaut. Bereits geringe Zweifel des Auftraggebers an der genannten Zuverlässigkeit können zum Verlust der Marktposition führen, u.U. mit gravierenden wirtschaftlichen und sozialen Folgen. Die gezielte Vorbeugung einer Geschäftsunterbrechung gehört aufgrund ihrer Bedeutung zu den Aufgaben der Unternehmensleitung. Bei branchenübergreifenden Abhängigkeiten (Interdependenzen) können bereits verhältnismäßig kleine Störungen weitgehende Folgen nach sich ziehen.

2.1 Betriebliches Kontinuitätsmanagement

Eine Geschäftsunterbrechung kann durch unterschiedliche interne und externe Schadensereignisse verursacht werden. Im Rahmen des betrieblichen Kontinuitätsmanagements werden mögliche Risiken, die eine Geschäftsunterbrechung verursachen und zur existenziellen Bedrohung für ein Unternehmen werden können, identifiziert. Zur ihrer Vorbeugung und ggf. Bewältigung werden ge-

zielte Maßnahmen geplant und umgesetzt[6]. Aufgrund der Bedeutung des betrieblichen Kontinuitätsmanagements handelt es sich hierbei um einen sogenannten Managementprozess. Die Umsetzung und Etablierung des Prozesses unterliegt der direkten Verantwortung der Geschäftsleitung. Die genaue Definition und der Ablauf des Notfallmanagement-Prozesses sind im Projektmeilenstein 4 (vgl. **Kapitel 7.12**) ausführlich beschrieben. Allgemein betrachtet teilt sich der Prozess in zwei Abschnitte: Notfallvorsorge und -bewältigung. In der Notfallvorsorge werden technische und organisatorische Maßnahmen geplant und umgesetzt, die eine Geschäftsunterbrechung verhindern (vorbeugen) sollen. Trotz aller Maßnahmen kann es zu einem Schadensereignis kommen. Die Aufgabe der Notfallbewältigung wiederum ist eine zeitnahe und koordinierte Wiederherstellung des Normalbetriebes. Eine Reihe von technischen und organisatorischen Maßnahmen erlauben eine effektive Alarmierung, die Umsetzung von Sofortmaßnahmen bis hin zur Wiederherstellung der Ressourcen bzw. Prozesse.

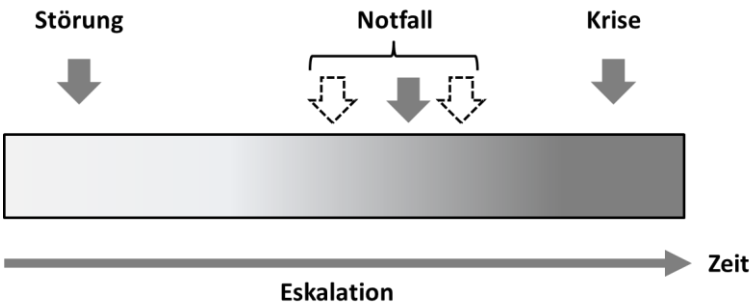

Abbildung 3: Eskalation eines Schadensereignisses.

Abbildung 3 skizziert die Eskalation eines Schadensereignisses. Ein Ausfall oder eine unkorrekte Funktionsweise einer Ressource oder eines Prozesses ist eine Störung. Wird die ursprüngliche Funktion nicht innerhalb einer angemessenen

[6] Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), Standard 100-4, Einleitung S. 1.

Zeit wiederhergestellt, kann sie zu ihrer Notfall eskalieren. Wenn alle geplanten Maßnahmen zu seiner Bewältigung fehlgeschlagen sind, kann aus einem Notfall eine Krise hervorgehen. Die referenzierten Standards definieren das betriebliche Kontinuitätsmanagement wie folgt:

- **BSI 100-4:** Kapitel 1, Einleitung. S. 1. *Das Notfallmanagement ist ein Managementprozess mit dem Ziel, gravierende Risiken für eine Institution, die das Überleben gefährden, frühzeitig zu erkennen und Maßnahmen dagegen zu etablieren. Um die Funktionsfähigkeit und damit das Überleben eines Unternehmens oder einer Behörde zu sichern, sind geeignete Präventivmaßnahmen zu treffen, die zum einen die Robustheit und Ausfallsicherheit der Geschäftsprozesse erhöhen und zum anderen ein schnelles und zielgerichtetes Reagieren in einem Notfall oder einer Krise ermöglichen.*[7]
- **ISO 22301:** Kapitel 3, Terms and Definitions. S. 1. Business continuity management - *holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.*[8]
- **BCI-GPG 2013:** Introduction. S. 5. *holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capa-*

[7] Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI) , BSI-Standard 100-4. Sämtliche Zitate aus dem BSI-Standard 100-4 sind schriftlich vom Bundesamt für Sicherheit in der Informationstechnik (BSI) genehmigt.

[8] Quelle: International Organization for Standardization (ISO), ISO 22301. Sämtliche Zitate aus der ISO 22301 Norm sind schriftlich genehmigt - „Reproduced by permission of ISO International Organization for Standardization, Genf".

bility of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.[9],[10]

2.2 Grundprinzip

Eine Reihe von Normen und Standards (vgl. **Kapitel 5**) definieren die Anforderungen an ein wirksames, effizientes und nachvollziehbares Notfallmanagement. Ein vollständig umgesetztes betriebliches Kontinuitätsmanagement[11] gemäß der genannten Standards kann in drei wesentliche Bereiche strukturiert werden:

- Unternehmensorganisation (Aufbau- und Ablauforganisation)
- IT-Verbund (IT-Infrastruktur, -Organisation und Mitarbeiter)
- Notfallmanagementprozess

Kenntnisse über die Aufbau- und Ablauforganisation gehören zu den Grundinformationen, die u.a. in der Definition der Notfallorganisation (vgl. **Kapitel 7.12.2**) und in der Business Impact Analyse (BIA) (vgl. **Kapital 7.12.3**) verwendet werden. Ein Teil der Führungskräfte und Mitarbeiter eines Unternehmens übernehmen die Verantwortung und bestimmte Funktionen bzw. Rollen in der Notfallorganisation. Die BIA ist ein wesentlicher Teil des Notfallmanagements. Im Rahmen des BIA-Prozesses werden Unternehmensprozesse ermittelt, die von besonderer Bedeutung für die Existenz des Unternehmens bzw. der Behörde sind. Im Umkehrschluss, ohne Betrachtung oder genaue Kenntnis der Unternehmensorganisation ist eine sorgfältige, detaillierte und zuverlässige Notfallvorsorge nicht möglich. Heutzutage ist ein effektiver, kostenoptimierter,

---

[9] Quelle: Business Continuity Institutes (BCI), Good Practice Guidelines 2013. Sämtliche Zitate aus der Good Practice Guidelines 2013 sind schriftlich mit dem Business Continuity Institutes abgestimmt.

[10] Business Continuity Institutes (BCI), Good Practice Guidelines 2013 verwendet weitgehend die ISO 22301:2012 Terminologie. Vgl. Introduction to the Good Practice Guidelines 2013, S.5.

[11] Der Begriff des betrieblichen Kontinuitätsmanagements wird in der Literatur oft neben den Begriffen Notfallmanagement und Business Continuity Management verwendet.

handels- und steuerrechtlich konformer Betrieb eines Unternehmens oder einer Behörde ohne IT bzw. IT-Organisation nicht realisierbar. Das gilt branchenunabhängig für jede Unternehmens- und Behördengröße. Die IT-Organisation, häufig auch IT-Verbund[12] genannt besteht aus der IT-Infrastruktur, IT-Prozessen und Mitarbeitern. Sie bildet unternehmensrelevante Prozesse, wie die Leistungserstellung, die Buchführung und den Geschäftsverkehr mit Kunden und Lieferanten ab. Die Unternehmensorganisation insbesondere die Unternehmensprozesse hängen direkt von der IT-Organisation ab.

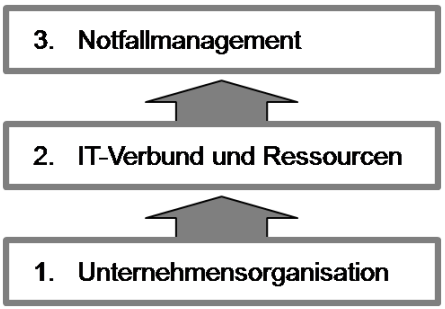

Abbildung 4: Grundprinzip der Informationserhebung

Der Ausfall einer oder mehrerer IT-Komponenten kann zu schwerwiegenden Ausfällen der Unternehmensprozesse führen. Die Unternehmensorganisation und der kontinuierliche, störungsfreie Geschäftsbetrieb hängen direkt von der IT ab. IT-Notfallmanagement ist ein Bestandteil des betrieblichen Kontinuitätsmanagements[13]. **Zusammengefasst:** Die Umsetzung des Notfallmanagement-Prozesses erfordert eine Reihe von Informationen aus den kurz zuvor skizzierten Bereichen (vgl. **Abbildung 4**). Sind die Informationen nicht verfügbar bzw. nicht mehr aktuell, müssen sie erhoben, dokumentiert und bewertet werden.

[12] Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), Standard 100-2, Kapitel 4.1. S.38.
[13] Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), Standard 100-4, Kapitel 1. S.1.

3 DocSetMinder[14] - Software

3.1 Notfallmanagement- und Projektdokumentation

Für die Planung und Umsetzung eines unternehmensweiten Notfallmanagements ist es empfehlenswert, ein zu diesem Zweck konzipiertes Tool einzusetzen. Die Compliance Management Software **DocSetMinder®** der GRC Partner GmbH ist bereits im Jahre 2004 für die Etablierung von IT-Governance-Themen im Unternehmen und in der Behörde entwickelt worden. Die Softwaremodule bilden anerkannte nationale und internationale IT-Governance Standards und Normen ab.

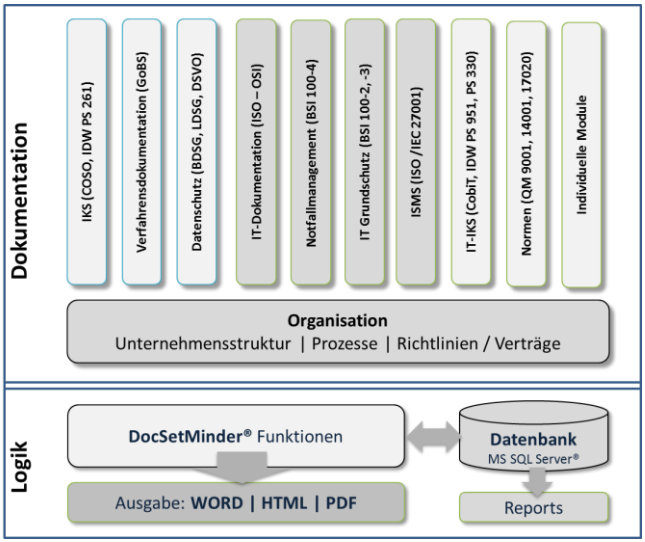

Abbildung 5: DocSetMinder® Aufbau und Module.

[14] In der vorliegenden Publikation wird die Unternehmens- und IT-Dokumentation sowie die Umsetzung des Notfallmanagements mit der Compliance Management-Lösung DocSetMinder® beschrieben.

Die strikten Anforderungen der Normen und Standards an die Notfallmanagement- und Projektdokumentation (vgl. **Kapitel 6**) sind durch diverse Softwarefunktionen vollständig abgedeckt.

3.2 DocSetMinder® - Module und Nutzen

Um die Dokumentation effizient und vollständig zu erstellen, zu kommunizieren und aktuell zu halten, stehen den Projektverantwortlichen und Mitarbeitern diverse Standard- und Compliance-Module zur Verfügung. **DocSetMinder®** bietet zum Thema IT-Governance eine komplette Suite von aufeinander abgestimmten Modulen mit Dokumentstrukturen und Vorlagen mit denen die **BSI-Standards 100-1** bis **100-4**, **ISO 22301**, **ISO 27001** und **BCI-GPG 2013** vollständig abgebildet werden können. Sie bilden den Grundstein für diverse ISO-Zertifizierungen. Alle Module bauen aufeinander auf. Im Einzelnen handelt es sich um:

- Modul – **„Unternehmensorganisation“** (Aufbau-, Ablauforganisation, Richtlinien, Verträge und Versicherungen)
- Modul – **„IT-Dokumentation“** (IT-Organisation, -Infrastruktur und Ressourcen)
- Modul – **„Notfallmanagement“** (BSI-Standard 100-4, ISO 22301, BCI-GPG 2013)
- Modul – **„Informationssicherheits-Managementsystems - ISMS“** (DIN ISO /IEC 27001)
- Modul – **„IT-Grundschutz“** (BSI-Standard 100-2, 100-3)
- Modul – **„RESISCAN“** (BSI Technische Richtlinie 03138 - Ersetzendes Scannen)
- Modul – **„IKS“** (IDW PS 261, PS 951)
- Module – **„Datenschutz“** (BDSG, LDSG, DSVO)

3.2.1 DocSetMinder® - Modul „Unternehmensorganisation“

Das Modul „Unternehmensorganisation“ erlaubt den Einsatz des **DocSetMinder®** als Implementierungsplattform für ein unternehmensweites Integriertes

Managementsystem (IMS)[15]. Informationen über die Aufbau- und Ablauforganisation eines Unternehmens oder einer Behörde werden nur einmal erfasst und können in Normen, wie z.B. **ISO 9001**, **ISO 14001**, **ISO 27001**, **ISO 20000** oder **ISO 22301** gemeinsam verwendet werden. Ändern sich z.B. die Prozessabläufe oder die Struktur der Organisation, so muss die Aktualisierung nur an einer Stelle vorgenommen werden. Die genannten Standards setzen in ihrer Umsetzung die Kenntnis der Unternehmensorganisation voraus. Es geht vor allem um die Dokumentation der Aufbau- und Ablauforganisation, Richtlinien, Verträge und Versicherungen. In der Aufbauorganisation werden generell alle organisatorischen Einheiten sowie Verantwortlichkeiten erfasst, in der Ablauforganisation die Prozessstrukturen bzw. der Ablauf der betrieblichen Wertschöpfungskette. Das Modul „Unternehmensorganisation“ stellt die notwendigen Informationen für alle IT-Governance Module zur Verfügung. Durch gezielte Verlinkung wird eine Relation zu den IT-Komponenten gesetzt - übersichtlich, aktuell und vollständig.

3.2.2 DocSetMinder® - Modul „IT-Dokumentation“

Das **DocSetMinder®**-Modul „IT-Dokumentation“ erlaubt eine systematische, strukturierte und lückenlose Dokumentation der IT-Infrastruktur, IT-Prozesse und Mitarbeiter. Die Modulstruktur basiert auf dem ISO - OSI Referenzmodell und erlaubt eine systematische Dokumentation der IT-Infrastruktur von den passiven Netzwerkkomponenten bis hin zu den im Unternehmen eingesetzten Anwendungen und den damit verbundenen Berechtigungen. Die Dokumentation der Gebäude, der IT-Räume und der Gebäudesicherheit kann ebenfalls realisiert werden. Bereits im **DocSetMinder®**-Grundmodul „Unternehmensorganisation“ ist die ITIL-konforme Struktur für die Dokumentation der IT-Prozesse enthalten. Die Dokumentation der IT-Infrastruktur umfasst sowohl technische als auch administrative bzw. organisatorische Aspekte. So beinhal-

[15] Vgl. K. Paschke, „Organisationshandbuch - Umsetzung, Dokumentation und Kommunikation“ 2011.

tet die Beschreibung eines beliebigen Servers neben technischen Informationen zu Prozessor, Speicher, Festplatte, Betriebssystem etc. auch administrative Angaben, z.B. zu den zuständigen IT-Mitarbeitern, zu Wartungs- und ggf. Leasingverträgen. Darüber hinaus bildet eine vollständige Dokumentation auch die logischen Zusammenhänge zwischen Geschäftsprozessen, Software, Datenbanken und Servern ab. Die zur Verfügung stehenden Schnittstellen erlauben den Datenimport aus Inventory-Tools, Verzeichnisdiensten (LDAP und Active Directory) und ERP-Systemen. Diese Beschreibung der Abhängigkeiten der Unternehmensorganisation und IT liefert wesentliche Informationen (Strukturanalyse) für die Business Impact Analyse (BIA). Die mit Hilfe des Moduls erstellte Dokumentation liefert notwendige Inhalte für Prüfungen nach IDW PS 330, IDW PS 951, ISAE 3402, PCI DSS sowie für die Umsetzung von Standards, wie z.B. BSI-Standard 100-1 bis -4, ISO 22301 oder BCI GPG 2013. Teile der IT-Dokumentation können auch im Bereich des Datenschutzes (BDSG, LDSG) verwendet werden.

3.2.3 DocSetMinder® - (IT-)Notfallmanagement

Das **DocSetMinder®**-Modul „Notfallmanagement" basiert auf dem BSI-Standard 100-4, ISO 22301 und BCI-GPG 2013 und bildet die Methodik zur Etablierung eines adäquaten Notfallmanagementsystems im Unternehmen oder einer Behörde ab. Das Modul erlaubt eine vollständige Erstellung und Pflege von Dokumentationen des Anwendungsbereichs, der Notfallorganisation, der Business Impact Analyse, der Risikoanalyse sowie der Alarmierung und Eskalation bis hin zu Geschäftsfortführungs- und Wiederanlaufplänen (Notfallhandbücher). Die Planung und Durchführung von Notfallübungen und der Verbesserungsprozess der Notfallorganisation (P-D-C-A) werden ebenfalls strukturiert unterstützt (vgl. **Kapitel 6.8.3**).

3.2.4 DocSetMinder® - Modul „IT-Grundschutz“

Um die komplexen Maßnahmen aus den Grundschutzkatalogen des BSI planen, umsetzen und administrieren zu können, ist eine strukturierte Vorgehensweise und Dokumentation notwendig. Das Modul "IT-Grundschutz" bildet die IT-Grundschutz-Kataloge des BSI ab, erlaubt die Definition des Schutzbedarfes der einzelnen Zielobjekte und die Bestimmung von notwendigen Sicherheitsmaßnahmen durch Modellierung des Informationsverbundes. Die Modulstruktur unterstützt den BSI-Standard 100-2 und 100-3 bei der Planung, Durchführung und Erhaltung einer effektiven Informationssicherheit im Unternehmen oder in der Behörde. Das Modul nutzt die bereits im Grundmodul „Unternehmensorganisation“ bereitgestellten Informationen zur Aufbauorganisation, den Prozessen und zentralen Inhalten wie Richtlinien, Verträge, Anweisungen sowie die im Modul "IT-Dokumentation" erfassten Sachverhalte des IT-Verbunds für die Strukturanalyse der Organisation. Die Inhalte der IT-Grundschutz-Kataloge sind in die Modulstruktur integriert.

3.2.5 DocSetMinder® - Modul „ISMS gemäß ISO/IEC 27001“

Die Norm ISO/IEC 27001 ist für die Planung, Umsetzung, Überwachung und stetige Verbesserung des Informationssicherheits-Managementsystems (ISMS) konzipiert. Das Modul "ISMS – ISO 27001" bildet die Anforderungen der Norm ISO/IEC 27001 vollständig ab. Die Modulstruktur erlaubt die Definition und Dokumentation des Anwendungsbereichs, der Verantwortlichkeiten, der ISMS-Leitlinie, die Analyse und Bewertung der Risiken sowie die Definition der Maßnahmenziele und Maßnahmen zur Behebung der festgestellten Risiken. Dieses Modul nutzt die bereits im Modul "Unternehmensorganisation" erfassten Informationen zur Aufbau- und Ablauforganisation im Unternehmen, die im Modul "IT-Dokumentation" beschriebenen IT-Ressourcen und -organisation sowie das betriebliche Kontinuitätsmanagement im Modul „Notfallmanagement“. Die Dokumentationsanforderungen und der P-D-C-A Zyklus der Norm sind detailliert umsetzbar.