
2.1 Einleitung

Die Norm ISO 22301 steht für die neueste internationale Richtlinie zum IT-Notfallmanagement (englisch: Business Continuity Management) und wurde im Mai 2012 freigegeben. Ihre Zielsetzung besteht darin, Hilfestellung bei der Reduzierung von Betriebsunterbrechungen durch unvorhergesehene Notfälle zu gewährleisten. Im Prinzip ist die Norm eine Fortschreibung der Standards ISO 31000 und ISO 27001. Sie gilt als universell im dem Sinne, dass sie auf Unternehmen jeglicher Größe anwendbar und unabhängig von den eingesetzten Technologien ist.

In diesem Kapitel wird ein erster Überblick über die wichtigsten Komponenten des Notfallmanagements, die in den Folgekapiteln dann ausführlicher behandelt werden, gegeben.

2.2 Notfallmanagementsysteme

Notfallmanagementsysteme kommen nicht nur zum Einsatz, wenn der Ernstfall eingetreten ist, sondern dienen ebenso der Prävention zur Vorbereitung auf Krisen- und Notfallszenarien. Dabei werden im Vorfeld Maßnahmen festgelegt, die Auswirkungen durch plötzlich eintretende Notfälle auf Kernprozesse einer Organisation (Behörde, Unternehmen) minimieren sollen und ein zeitnahes Wiederaufnehmen normaler Aktivitäten voranbringen. Um diese planerischen Vorbereitungen für alle Eventualitäten sinnvoll gestalten zu können, muss man diese Prozesse und die betroffenen Mitarbeiter und System zuerst einmal identifizieren.

2.2.1 Warum Notfallmanagement?

Neben dem reinen Interesse an der Fortführung des Tagesgeschäfts und damit der existenziellen Erhaltung z. B. eines Unternehmens gibt es andere handfeste Gründe für die Konzeptionierung eines Notfallmanagements. Obwohl grundsätzlich gesetzlich nicht explizit vorgeschrieben, gibt es dennoch gesetzliche und vertragliche Verpflichtungen, die sich aus dem Geschäftsgegenstand ergeben können.

Dazu gehören z. B. alle vertraglichen Verpflichtungen zur Erfüllung von Lieferungen und Dienstleistungen, die ein Unternehmen mit Kunden eingegangen ist. In ganz bestimmten Branchen wird die Notwendigkeit für solche Maßnahmen aus anderen gesetzlichen Vorgaben abgeleitet. Das ist z. B. bei den Banken der Fall, aber auch bei börsennotierten Kapitalgesellschaften, die dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich unterliegen. Für letztere ist ein Risikomanagement vorgeschrieben. Daneben gibt es eine Reihe anderer gesetzlicher Vorschriften im Geschäftsbereich, die ein Notfallmanagement erforderlich machen (Kreditwesen, Arbeitsschutz etc.).

Im Falle von Kommunikationsunternehmen bestehen die vertraglichen Verpflichtungen

- in der Bereitstellung ausreichender Netzkapazitäten, um Kommunikation der Kunden zu ermöglichen,
- in der Bereitstellung von anderen Diensten, für die Kunden Gebühren zahlen, und
- in der Zuschaltung von Kunden, die erst kürzlich einen Vertrag eingegangen sind.

2.2.2 Was ist Notfallmanagement?

Auf den Punkt gebracht, kann man Notfallmanagement folgendermaßen definieren:

Notfallmanagement ist

- ein systematischer, an den Geschäftsprozessen orientierter Ansatz
 - zur Begrenzung von Ausnahmesituationen,
 - zur Begrenzung von Schadensauswirkungen,die durch unvorhergesehene Einwirkungen von außen oder innen entstehen können.
- der Aufbau organisatorischer Voraussetzungen; dazu gehören
 - eine Strukturorganisation, die teilweise im Vorfeld schon aktiv ist bei der Definition von Präventivmaßnahmen, aber teilweise erst im Ernstfall zum Leben erweckt wird,
 - eine Prozessorganisation, welche beim Eintreten eines Notfalls aktiviert wird.
- die Entwicklung von entsprechenden Konzepten in Anlehnung an die strategischen Ziele einer Organisation und deren Kernprozesse,
- eine rasche Reaktion auf Notfälle unter Zuhilfenahme der vordefinierten Maßnahmen und

- die Ermöglichung der Fortsetzung der wichtigsten Geschäftsprozesse im Rahmen der durch den Notfall entstandenen Randbedingungen.

2.3 Standards

2.3.1 BSI

Das Bundesamt für Sicherheit in der Informationstechnik veröffentlicht regelmäßig detaillierte Empfehlungen und Erfahrungsberichte zu Fragen der IT-Sicherheit (wie sein Name es besagt), u. a. in seinem Grundschatzkatalog, nach Veröffentlichung der ISO 22301 jetzt auch ein eigenes Regelwerk für das IT-Notfallmanagement: den Standard 100-4.

2.3.1.1 Der Standard 100-4

Hierbei handelt es sich um ein echtes Regelwerk für den Aufbau und die Dokumentation eines Notfallmanagements mit den Zielen

- systematische Wege für adäquate Reaktionen im Vorfeld aufzubauen, um für den Notfall gerüstet zu sein,
- schnelle Wiederaufnahme von Geschäftsprozessen
 - einmal durch die Bereitstellung eines Notbetriebs während der Notfallsituation
 - zum anderen durch eine systematische Vorgehensweise beim Wiederanlauf der Prozesse nach Beendigung der Notsituation,
- Vermeidung von Notfällen durch entsprechende Vorsorgemaßnahmen sowie
- die Minimierung von Schäden, ebenfalls durch entsprechende Vorsorgemaßnahmen.

Historisch gesehen vollzieht sich dabei ein Trendwechsel von der Notfallplanung zum Notfallmanagement, d. h. um die Konzeptionierung eines eigenständigen Managementsystems. Wie bereits erwähnt, fügt sich dieser neue Standard nahtlos in die Grundsatzvorgehensweisen des BSI mit Methoden, die aus unterschiedlichen Standards, unter anderen den BS 25999, gewachsen sind, ein (Abb. 2.1).

Abb. 2.1 BSI-Standards.
(Quelle: BSI)

BSI Standards zur Informationssicherheit

- 100-1: ISMS: Managementsysteme für Informationssicherheit
- 100-2: IT-Grundsatz-Vorgehensweise
- 100-3: Risikoanalyse auf der Basis von IT-Grundsatz
- **100-4: Notfallmanagement**

2.3.1.2 Weitere Standards und Methodologien zur IT-Sicherheit

Da ist zunächst die 2700x-Reihe, die zwar grundsätzliche Richtlinien und Empfehlungen vorgibt, aber hinter den Details zurückbleibt. Durch den ISO 22301 kann man sie als obsolet betrachten.

Im Grunde findet man in jeder Methodologie (ITIL und andere) irgendwelche Hinweise, zum Teil ganze Abschnitte, zu dem Thema Notfallmanagement. Wer solche Methoden nutzt, und wenn diese bereits in einer Organisation eingeführt sind, sollte zunächst dort nachsehen, ob ein Notfallmanagement sinnvoll darauf aufgebaut werden kann. Eventuell sind die dort vorgeschlagenen Maßnahmen durch Elemente aus dem BSI 100-4 zu ergänzen.

2.4 Wichtige Merkmale des ISO 22301

Der Standard stellt Anforderungen an eine Organisation, fordert grundlegende analytische Vorbereitung, eine ausgefeilte Planung und steckt innerhalb bestimmter Geltungsbereiche Verantwortlichkeiten ab.

2.4.1 Anforderungen an Unternehmen

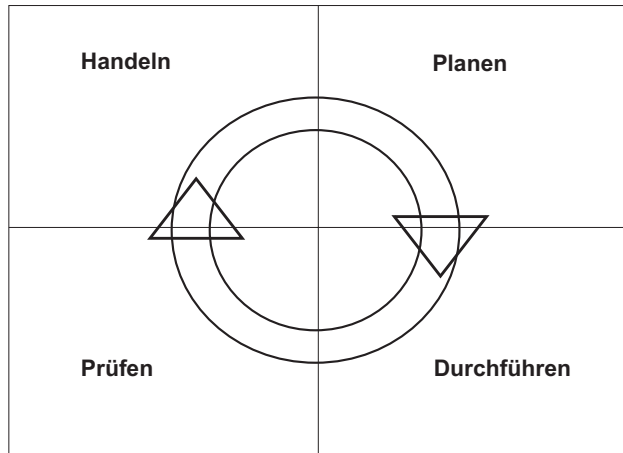
Bei einem IT-Notfallsystem handelt es sich um ein ganzheitliches Managementsystem und weniger um eine Sammlung von Vorschriften. Deshalb ist es unabdingbar, dass die Leitungsebene einer Organisation nicht nur eingebunden wird, sondern das Vorhaben aktiv vorantreibt, wozu auch die Bereitstellung von personellen und materiellen Ressourcen gehört. Zur Überwachung und regelmäßigen Überprüfung werden gesonderte Verantwortlichkeiten benannt (s. u.), die nach oben berichten.

Die oberste Leitungsebene sollte ebenfalls eingebunden werden, wenn es um das Business Continuity Management – also die Weiterführung der wichtigsten Geschäftsprozesse – geht, weil nur sie letztendlich die Prioritäten vorgeben kann. Ein Notfallmanagementsystem ist einerseits wichtig für die Existenz einer Organisation, andererseits aber auch ein Ausweis nach draußen, um das Vertrauen von Geschäftspartnern und Kunden zu erhalten, dass man unter allen Umständen in der Lage sein wird, sein Geschäft weiter zu betreiben. Zu diesem Zweck kann man sich sein Notfallmanagement auch zertifizieren lassen.

Wie andere Managementsysteme auch, unterliegt ein Notfallmanagement einer Art Deming-Zyklus, auch als PDCA-Zyklus bekannt (s. Abb. 2.2). Alles beginnt mit der Planung. Dabei werden festgelegt:

- organisatorische Einbettung
- Management-Verantwortlichkeiten
- Prozessplanung
- Ressourcen.

Abb. 2.2 Kontinuierlicher Verbesserungsprozess



Bei der Durchführung müssen folgende Aspekte erledigt werden:

- Business-Impact-Analyse
- Risikoanalyse
- Geschäftsfortführungsstrategie
- Tests und Übungen.

Das Prüfen dient

- der Bewertung der einzuleitenden Maßnahmen,
- als Basis für interne Audits und
- als Management-Review.

Daraus folgen Konsequenzen für das weitere Handeln als eigentlicher Anstoß zum kontinuierlichen Verbesserungsprozess.

2.4.2 Analyse vor der Planung

Bevor man nun eine (Detail-)Planung für ein Notfallmanagement in Angriff nimmt, muss sorgfältig analysiert werden, wie die strategische Grundausrichtung des Unternehmens ist und wie andere Grundvoraussetzungen der Organisation sich darstellen. Dazu gehört eine Erfassung aller Unternehmensaktivitäten, wie sie beispielsweise in den ERP-Prozessen abgebildet sind, im Falle von Kommunikationsunternehmen die Kernprozesse, wie in Kap. 6 niedergelegt, der wichtigsten Produkte und Verpflichtungen gegenüber Dritten.

Wichtig sind auch die Schnittstellen zu bereits bestehenden anderen organisatorischen Voraussetzungen, wie z. B. ein schon existierendes Risikomanagement, welches Über-

schneldungen mit einem Notfallmanagement haben kann. Zu berücksichtigen sind zudem die Erwartungen aller am Gesamtprozess Beteiligten sowie die Beachtung gesetzlicher Vorschriften.

2.4.3 Verantwortlichkeiten des Managements

Die oberste Leitungsebene muss dafür sorgen, dass das Business Continuity Management (BCM) nicht zu einem Fremdkörper innerhalb einer Organisation wird, sondern in die übergeordnete Strategie passt. Dazu gehört die Einbindung der BCM-Prozesse in die existierende Prozesslandschaft. Am besten geschieht das dadurch, dass eine BC-Strategie formuliert wird, die folgende Gesichtspunkte berücksichtigt:

- Dokumentation von Zielen und Notfallplänen: Unter den strategischen Zielen sind diejenigen geschäftlichen Aktivitäten zusammenzufassen, die auch im Notfall erforderlich sind, um das Geschäft am Laufen zu halten; die Notfallpläne haben das zu berücksichtigen.
- Bereitstellung von erforderlichen Kommunikationsstrukturen: Das Kommunikationsverhalten in Notfällen gestaltet sich anders als im Normalbetrieb. Entsprechende Kanäle sind zu definieren.
- Festlegen von Verantwortlichkeiten: Für eine funktionsfähige Notfallorganisation sind eigene Hierarchien zu schaffen.

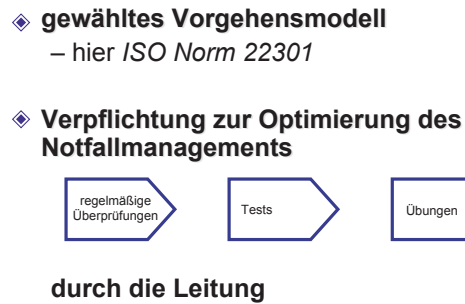
Eine so erstmalig formulierte Strategie mit den zugehörigen Zielen ist nichts Statisches, sondern lebt mit den Veränderungen des Geschäftsbetriebs, ist somit Gegenstand von regelmäßigen Überprüfungen und Überwachungen.

2.5 Leitlinie

Eine Leitlinie gemäß *BSI 100-4* sollte die folgenden Aspekte beschreiben:

- Definition des Notfallmanagements
 - Bedeutung für die eigene Organisation
 - Zuständigkeiten
 - Zusammenwirken mit anderen Unternehmensbereichen
- Geltungsbereich des Notfallmanagements
 - Bereiche
 - Objekte
 - Lokalitäten
 - zeitliche Gültigkeit
- Vereinbarkeit mit den übrigen Unternehmenszielen

Abb. 2.3 Verantwortlichkeiten
der Leitungsebene



- wesentliche Aspekte der Notfallstrategie
 - ausgewählte strategische Ziele
 - Bedrohungsszenarien
 - Risikobereitschaft
 - Schadensszenarien
 - Prioritäten innerhalb des Geschäftsbetriebs
- Vorgehensmodell (hier *ISO Norm 22301*)
- Sicherstellung der Notfallfunktionen (s. Abb. 2.3)
- rechtlicher Rahmen
- formelle Verantwortung durch die Unterschriften der Geschäftsführung.

In Kap. 10 wird die Leitlinie ausführlicher behandelt.

2.6 BCM im Überblick

2.6.1 Phasen und Schritte der BCM-Umsetzung

Die Phasen der BCM-Umsetzung sind in Abb. 2.4 schematisch dargestellt:

Nach einer BIA (Business-Impact-Analyse, s. Abschn. 2.6.2) erfolgt die Risikobeurteilung unter Hinzuziehung der Fachleute und der Unternehmensleitung. Auf dieser Basis werden die BCS (Business Continuity Strategy) entwickelt sowie die Verfahren, die einen Notgeschäftsbetrieb gewährleisten sollen. Nach Vorliegen dieser Konzepte sind daraus Übungshandbücher (s. Kap. 10) zu schreiben. Nach diesen Handlungsanweisungen können dann Notfälle als Gesamtszenarien oder in Teilen geübt und die Verfahren getestet werden.

2.6.2 Business-Impact-Analyse (BIA)

Die Business-Impact-Analyse ist ein aufwändiges Unterfangen, welches als Vorsorgemaßnahme punktuell wichtige Unternehmensressourcen binden wird: Fachspezialisten, Führungskräfte, Unternehmensleitung. Zu einer solchen Analyse gehören:

Abb. 2.4 BCM-Umsetzung

Phasen und Schritte der BCM-Umsetzung



- Die Sammlung und Identifizierung von Prozessen und Funktionen: Dazu gehören sämtliche Abläufe – nicht nur die kritischen oder zu den Kernprozessen gehörende (letztere werden später gesondert herausgehoben, weil auf ihnen das gesamte Geschäft beruht).
- Zugrunde liegende Ressourcen: Dazu gehört das Personal, aber auch Hardware-Ressourcen wie IT-Einrichtungen, Gebäude, Lagerhallen mit ihrer technischen Ausrüstung. Im Falle eines Kommunikationsunternehmens sind natürlich das Netz und seine Funktionsfähigkeit die Grundlage aller weiteren Überlegungen.
- Abhängigkeiten von IT-Prozessen: Die kritische Frage hinter diesem Aspekt ist letztendlich: Welche Prozessanteile lassen sich sinnvoll auch ohne direkte IT-Stützung aufrecht erhalten?
- Priorisierungen: Spätestens hier muss die Entscheidung über die Kernprozesse fallen.
- Auswirkungen und Wiederanlaufzeiten: Auswirkungsszenarien variieren offensichtlich mit dem angenommenen Notfallszenario, ebenso die projizierten Wiederanlaufzeiten; deshalb müssen unterschiedliche Szenarien durchgespielt werden (s. Kap. 7 „Notfallklassen“).

Dies alles sind Voraussetzungen, um eine Risikoanalyse und -beurteilung durchführen zu können.

Die BIA wird in Kap. 8 ausführlicher behandelt.

2.6.3 Strategie und Verfahren

Die Notfallstrategie legt die Minimalziele fest, an denen für einen sinnvollen Geschäftsbetrieb unbedingt festgehalten werden muss. Dazu gehören:

- Festlegung der Wiederherstellungszeiten für kritische Aktivitäten, die sich aus den Kernprozessen ableiten lassen. Bei einem Kommunikationsunternehmen gehört unabdingbar die Funktionsfähigkeit wesentlicher Teile des Netzes dazu.

- Frühzeitige Verfügbarkeiten: werden aus den Wiederherstellungszeiten abgeleitet; ergeben diese inakzeptable Werte, muss über Alternativstrategien nachgedacht werden, bis brauchbare Zielvorgaben erreicht sind.
- Ausrichtung auf die gesamte Geschäftsstrategie und somit integraler Bestandteil der Unternehmensstrategie: Obwohl Notfallstrategie – selbstverständlich muss diese, wenn auch in reduzierter Form, auf die ursprüngliche Unternehmensstrategie abbildbar sein.

All die gerade beschriebenen Überlegungen haben ein übergeordnetes Ziel in sich:

- Die Organisation muss adäquate Verfahren dokumentieren, um die Kontinuität von Aktivitäten und die Bewältigung von Betriebsunterbrechungen sicherzustellen!

2.7 Üben und Testen

Man kann und sollte die entwickelten Verfahren auch ohne akuten Notfall testen – und zwar aus zwei Gründen:

- Sicherstellen der Konsistenz der Business-Continuity-Verfahren mit den Business-Continuity-Zielen
- Gewährleistung, dass die gewählten Strategien in Krisensituationen die richtigen Antworten und Wiederherstellungsergebnisse liefern.

In Kap. 10 wird diese Thematik ausführlich abgehandelt.

2.8 BIA und Risiken

Zusammenfassend lässt sich sagen, dass die Business-Impact-Analyse

- eine Methode zur Identifizierung von kritischen Geschäftsprozessen ist,
- die Auswirkungen von Prozessausfällen ermittelt,
- die Abhängigkeiten von Prozessen untereinander aufzeigt und
- die benötigten Wiederanlaufzeiten generiert.

BIA und Risikoanalyse sind sozusagen das Rückgrat des Notfallmanagements. Sie

- sind Basis für das gesamte Notfallkonzept,
- legen fest, was ein Notfall ist, und
- identifizieren die Zusammenhänge und Bedrohungen.



Abb. 2.5 Schrittfolge bei der BIA

Die Erkenntnis, dass Prozesse eines Unternehmens logisch miteinander verknüpft sind und kaum ein Geschäftsbereich ohne IT-Prozesse auskommt, bedingt die Notwendigkeit, diese Prozesse bei der BIA zu erfassen, um im Nachhinein die kritischen Systeme zu identifizieren (s. Abb. 2.5).

Bei der Bewertung dieser Prozesse sind bestimmte Gesichtspunkte zu beachten. Da geht es um

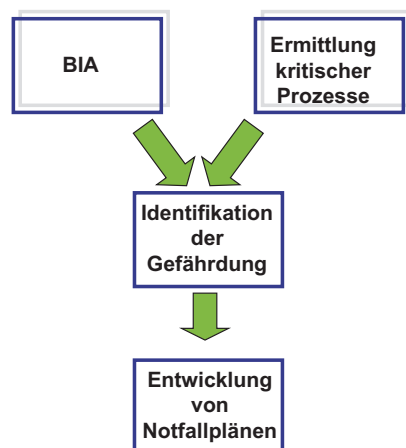
- alle Auswirkungen (deshalb „Impact“) (z. B. logistische, finanzielle, gesetzliche etc.),
- Behinderungen oder die Unmöglichkeit, Aufgaben und Tätigkeiten durchzuführen,
- Imageschäden nach innen und in den Markt hinein und nicht zuletzt
- Leib und Leben der Mitarbeiter.

2.8.1 Risikoanalyse

Das Vorgehen bei der Risikoanalyse ist in Abb. 2.6 schematisch dargestellt. Erst nach BIA und der Ermittlung kritischer Prozesse kann die wirkliche Gefährdung identifiziert werden und – darauf aufbauend – die Entwicklung von Notfallplänen.

Damit ist allerdings noch nichts gesagt über die Akzeptanz bzw. Toleranz gegenüber einem erkannten Risiko. Hier spielen noch einmal andere Gesichtspunkte eine Rolle:

Abb. 2.6 Risiko-Analyse



Notfallmanagement in Kommunikationsnetzen

Osterhage, W.W.

2016, XI, 141 S. 50 Abb. in Farbe., Hardcover

ISBN: 978-3-662-45659-0