IDR Prüfungsleitlinie IDR-L 113-2 „Notfallmanagement“

Stand: 09.2023

Autoren:

Alexander Ehrbar; Gemeindeprüfungsanstalt Nordrhein-Westfalen

Ralf Klomfaß; Revisionsamt Landeshauptstadt Mainz

Matthias Warnecke, LWL-Rechnungsprüfungsamt

Inhalt

I. Abbildungsverzeichnis

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

II. Dokumentenhistorie

Version	Datum	Verfasser	Änderung / Grund	Status
01.0	2022	Alexander Ehrbar Ralf Klomfaß	Erstellung des Dokuments	In Arbeit
01.0	12.2022	AK DITS	Vorstellung / Sichtung im AK	ENTWURF
01.0	09.2023	AK DITS	Einarbeitung redaktioneller Änderungen	FINAL

2. Anforderungen an das Notfallmanagement

2.1. Zielsetzung

Ziel des Notfallmanagements ist es sicherzustellen, dass wichtige Geschäftsprozesse selbst in kritischen Situationen nicht oder nur temporär unterbrochen werden und die wirtschaftliche Existenz der Institution sowie die Handlungsfähigkeit auch bei einem größeren Schadensereignis gesichert bleiben. Das Notfallmanagement umfasst das geplante und organisierte Vorgehen, um die Widerstandsfähigkeit der (zeit-)kritischen Geschäftsprozesse einer Institution nachhaltig zu steigern, auf Schadensereignisse angemessen reagieren und die Geschäftstätigkeiten so schnell wie möglich wieder aufnehmen zu können.

2.2. Rechtsgrundlagen

- BSI-Standard 100-4 „Notfallmanagement“

3. Erläuterung/Grundinformation

Nach der Definition des Bundesamtes für Informationssicherheit (BSI) wird unter Notfallmanagement (englisch: Business Continuity Management) ein systematischer, an den Geschäftsprozessen einer Institution orientierter Ansatz zur Vorsorge gegen und Bewältigung von Notfällen und Krisen verstanden. 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, sondern allgemein alle Prozesse einer Behörde, die für die Erbringung von Dienstleistungen und die Erfüllung der jeweiligen Fachaufgaben nötig sind.

Das Notfallmanagement soll die Kontinuität des Geschäftsbetriebs bei Notfällen sicherstellen. Es ermöglicht Organisationen, bei Störungen von kritischen Geschäftsprozessen angemessen zu reagieren.

3.1. Was ist ein Notfall?

Ein Notfall ist ein Schadensereignis, bei dem Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren. Die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen kann innerhalb einer geforderten Zeit nicht wiederhergestellt werden. Der Geschäftsbetrieb ist stark beeinträchtigt. Eventuell vorhandene SLAs (Service Level Agreements) können nicht eingehalten werden. Es entstehen hohe bis sehr hohe Schäden, die sich signifikant und in nicht akzeptablem Rahmen auf das Gesamtjahresergebnis eines Unternehmens oder die Aufgabenerfüllung einer Behörde auswirken. Notfälle können nicht mehr im allgemeinen Tagesgeschäft abgewickelt werden, sondern erfordern eine gesonderte Notfallbewältigungsorganisation.

Daraus folgt, dass kleinere Störungen wie kurzfristige Stromausfälle, Personalengpässe, sich verzögernde Dienstleistungen, kleinere Gerätedefekte in der Regel keine Notfälle darstellen. Für solche Vorfälle gibt es normalerweise einfache Lösungen, die Bestandteil des Alltagsgeschäfts sind. 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.

Zur Abgrenzung der Begriffe und Darstellung der erforderlichen Behandlung von Vorfällen hat das BSI nachfolgende Matrix veröffentlicht:

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	Aus Sicht einer Institution stellt sich eine Katastrophe als Krise dar und wird intern durch deren Notfallorganisation in

	Überschwemmungen oder Erdbeben	Zusammenarbeit mit den externen Hilfsorganisationen bewältigt.

Daraus folgt:

Erst dann, wenn Störungen oder Ausfälle größere Schäden verursachen können und ihre Behebung mit den üblichen Verfahren nicht mehr möglich ist, sollte ein Notfallmanagement etabliert und formal verabschiedet werden.

Beispiele aus der Praxis:

- Durch Brände können Serverräume nicht mehr genutzt werden
- Überschwemmungen oder Wassereinbruch in Technikräumen
- 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 Insolvenz anmelden musste und auch nicht auf Ersatzdienstleister zurückgegriffen werden kann
- Beschädigung zentraler Strukturen durch Vandalismus
- Beschädigung der Infrastrukturen durch Virenbefall / Verschlüsselung

Ein vollständiges Notfallmanagementsystem erfordert eine detaillierte Konzeption von Rollen, Verantwortlichkeiten, Prozessen, Dokumenten und Plänen. Um einen Mindeststandard für ein Notfallmanagement für die öffentliche Verwaltung zu etablieren, sollten zumindest die nachfolgenden Aspekte konzeptionell betrachtet und Festlegungen getroffen werden.

Dabei wird unterschieden zwischen der

- Betrachtung von präventiven Maßnahmen zur Vermeidung von Notfällen, zumindest aber mit dem Ziel der Risikominimierung und
- der Behandlung von eingetretenen Notfallsituationen (Notfallbehandlung) durch über ein Notfallhandbuch festgelegte Maßnahmen im Akutfall, die zielgerichtet auf den aufgetretenen Schaden gerichtet werden (Incident Response = Vorfallreaktion).

Die Tabelle beinhaltet Kernaspekte des Notfallmanagements, die im Rahmen der Prüfung durch die Rechnungsprüfungsämter zumindest abgefragt werden sollten, stellt

aber keine vollständige Prüfliste aller Aspekte dar, die im Rahmen des Notfallmanagements geprüft werden könnten. Die im Leitfaden dargestellten Aspekte stellen vielmehr auf eine systemische Prüfung ab, die auch ohne tieferes Expertenwissen vorhalten zu müssen, wichtige Schwachstellen ermitteln und damit Handlungsbedarfe aufzeigen kann.

4. Checkliste:

Lfd. Nr.	Soll-Vorgabe / Best-Practice-Empfehlung	Prüffrage	Zusatzinformationen
1	Durchführung einer Gefährdungsanalyse (Business Impact Analyse)	• Wie abhängig sind die Fachbereiche bzw. Abteilungen von IT-Systemen? • Welche Art von Risiken bringen identifizierte Schwachstellen mit sich? • Wer ist für die Festlegung von Service Level Agreements zuständig? • Welche und wie viele Mitarbeitende sind von evtl. Ausfällen betroffen? • Welche Art von Ressourcen/Ausrüstung wird bei einem Ausfall benötigt?	Die Business Impact Analyse (BIA) 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. Eine BIA ist also ein systematischer Prozess, der aus einer untersuchenden Komponente und einer Planungskomponente besteht. Die untersuchende Komponente umfasst die Ermittlung von potenziellen Risiken, denen eine Behörde bei Störungen des Geschäftsbetriebs gegenübersteht. Die Planungskomponente besteht aus der Entwicklung von Strategien, die die Risiken minimieren sollen. Grundsätzlich sollten folgende Informationen abgefragt werden:

			• Liste der Fachverfahren mit Zuordnung zu den Fachbereichen; Priorisierung der Verfahren nach Wichtigkeit. • genaue Beschreibung, verantwortliche Fachstelle Anzahl der Anwender des Fachverfahrens und Auswirkungen auf interne Leistungen / externe Leistungen beschreiben • Liste aller Abteilungen, die von Fachanwendungen abhängig sind • Maximale Ausfallzeit ohne merkbare Auswirkungen • Betriebliche und finanzielle Auswirkungen bei einem Ausfall • Externe/rechtliche Auswirkungen bei einem Ausfall (z. B. Bürger, Behörden, Vertragspartner, usw.) • Beschreibung früherer Ausfälle und die damit verbundenen Folgen
2	Durchführung einer Risikoanalyse	• Was sind die Bedrohungen? Hauptbedrohungen für die IT sind: Naturkatastrophen, Menschliches Versagen, böswillige Absicht und Systemausfall. • Was sind die Schwachstellen? • Wie hoch ist die Wahrscheinlichkeit von	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. Bei der Beschreibung der Gefährdungspotentiale sind die jeweiligen örtlichen Gegebenheiten in den Blick zu nehmen. Wichtige Faktoren sind hierbei: • direkte Lage an einem fließenden Gewässer • Starkwindzone • benachbarte Industrieanlagen / AKW´s

		Zwischenfällen, die Bewertung der Verwundbarkeit einzuschätzen? • Was sind die möglichen Auswirkungen?	• Bergbauschäden • Einflugschneise Flughafen • Hanglagen • Anschlaggefahr bei Betrieb kritischer Infrastrukturen Jede Behörde sollte die Bedrohungen und Schwachstellen kennen, die ihre Informationssicherheit mit einem Mindestmaß an Wahrscheinlichkeit bedrohen könnte. Bei der Risikoanalyse werden verschiedene Phasen nacheinander durchlaufen: 1. Identifikation der IT Risiken 2. Beurteilung der Eintrittswahrscheinlichkeiten Nachdem ein IT Risiko identifiziert ist, wird die Eintrittswahrscheinlichkeit näher bestimmt. Was sind eventuelle Auswirkungen und Folgen? 3. Abschätzung der Folgen und eventuellen Schäden Das tatsächliche IT Risiko ergibt sich aus dem Ergebnis der Eintrittswahrscheinlichkeit und Höhe des Schadens. 4. Bestimmung des Gesamtumfangs der Schäden Bei der Risikoanalyse für IT-Sicherheit kann man zwischen qualitativer und quantitativer Bewertung unterscheiden. Die qualitative IT Risikoanalyse versucht, einen Gesamteindruck von einem bestimmten Risiko zu bekommen.
3	Erstellen eines Notfallvorsorgekonzeptes	• Gibt es ein formelles Notfallvorsorgekonzept?	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.

		• Was ist vorbeugend zu tun, um Notfälle zu verhindern und Schäden zu begrenzen?	Ein Notfallvorsorgekonzept beschreibt somit detailliert, mit welchen infrastrukturellen, technischen, organisatorischen und personellen Maßnahmen die Kontinuität des behördlichen Betriebs sichergestellt werden soll. Es umfasst damit präventive Maßnahmen, um die Eintrittswahrscheinlichkeit eines Notfalls zu verringern oder dessen Auswirkungen zu begrenzen. Die Erfahrung zeigt aber, dass eine 100-prozentige Sicherheit nicht erreichbar sein wird. Insoweit ist auch die konzeptionelle Planung und Beschreibung reaktiver Maßnahmen erforderlich, um in Notfallsituationen schnell und angemessen handeln zu können (Notfallhandbuch).
4	Erstellen eines Notfall-Handbuchs	• Wurde ein Notfallhandbuch erstellt? • Sind die Verantwortlichkeiten eindeutig geregelt? • Sind die für die Notfallbewältigung erforderlichen Mitarbeitenden auskömmlich geschult? • Gibt es Einsatz- und Bereitschaftspläne? • Gibt es eine Liste der vertraglich gesicherten Supportleistungen?	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. Das eigentliche Notfallhandbuch muss vor allem organisatorische Regelungen enthalten und die folgenden Fragen beantworten: Wer hat welche Verantwortlichkeiten und Aufgaben? Welche Notfallbewältigungsmaßnahmen sind durchzuführen und welche Pläne sind dafür anzuwenden? Diese Punkte sind organisationsweit zu regeln. Abhängig von der Größe und Komplexität der Behörde kann es aber auch sinnvoll bzw. notwendig sein, ein gesondertes Notfallhandbuch für die IT-Organisation zu erstellen. Dabei sollten folgende Einzelaspekte Berücksichtigung finden:

		• Ist eine Liste von Händlern für Ersatzbeschaffungen vorhanden / gibt es vereinbarte Ersatzgestellung durch IT- Dienstleister (z.B. kommunale Rechenzentren)?	• Notfallorganisation Notfallstab, Notfallteams, Alarmierungs- und Eskalationspläne bzw. Verweise auf Kommunikationspläne, alle erforderlichen Kontaktdaten auch von Dienstleistern, Verweise auf zusätzlich erforderliche Informationen (z. B. Netzwerkpläne oder Raumpläne), Vorgaben und Vorlagen für die Dokumentation während des Notfalls • Notfallbewältigung Verweise auf die Geschäftsfortführungspläne beispielsweise für spezifische Szenarien einschließlich Wiederanlaufpläne, Wiederherstellungspläne für kritische Systeme (für den Not- und den Normalbetrieb)
5	Durchführung von Übungen und Tests	• Werden von der IT regelmäßige Tests durchgeführt, im Hinblick auf Systemausfälle, Datenwiederherstellung, Wiederanlauf von Systemen, etc.? • Werden die Übungen und Tests systematisch dokumentiert?	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.
6	Verfügbarkeitsanforderun-gen mit der	• Sind mit der Verwaltungsleitung Vereinbarungen getroffen	Beschreibung und Festlegung von Anforderungen der Leitungsebenen (Behörden – und

	Verwaltungsleitung vereinbaren	worden, welche Ausfallzeiten für die zentralen Systeme und einzelne Fachanwendungen toleriert werden? • Sind die festgelegten tolerierten Ausfallzeiten bei den Maßnahmen zur Notfallbewältigung mit berücksichtigt (z.B. durch Service- Verträge, Ersatzbeschaffungsplanung, Redundanzplanung, etc.)?	Fachbereichsanleitungen) für die Festlegung der maximal tolerablen Ausfallzeiten. Für die Basis-Systemdienste, sowie für die Fachanwendungen selbst sollten die Verfügbarkeitsanforderungen nach Fachanwendungen getrennt festgelegt werden. Ein erprobtes Maß dazu ist die Angabe der maximal tolerierbaren Ausfallzeit. Sie gibt an, über welchen Zeitraum die Fachaufgabe ohne diese Daten weitergeführt werden kann, ohne dass auf Datensicherungsbestände zurückgegriffen werden muss.

5. Weiterführende Literatur

- BSI 200-4 Kompendium Notfallmanagement (Weiterentwicklung des bisherigen 100-4 mit Neuerungen im Bereich Business Continuity, praxisnahe Anleitung, um ein Business Continuity Management System (BCMS) in der eigenen Institution aufzubauen und zu etablieren.)