



WHITEPAPER

BCM als strategischer Eckpfeiler der Cyber-Resilienz 2026

Strategische Priorisierung des Business Continuity Management
(BCMS) zur Bewältigung komplexer IKT-Bedrohungslagen

AKARION

Inhaltsverzeichnis

1. Business Continuity Management	3
Definition und strategische Bedeutung	3
Eine kurze Historie	3
Nationale Standards in Deutschland	4
1.1. Die Kernkomponenten eines BCMS	4
1.2. Der PDCA-Zyklus: Kontinuierliche Verbesserung der Resilienz	5
2. Die Cyberbedrohungslage 2026: Paradigmenwechsel in der Resilienz	6
2.1. Management-Fokus: Warum BCM heute priorisiert werden muss	7
2.2. ISMS und BCM - Parallel statt seriell	8
Vorteile der parallelen Implementierung	8
2.3. Schnell zu Ergebnissen	10
Phase I - Strategische Ausrichtung und Governance	10
Phase II - Analysephase	10
Phase III - Strategie und Notfallplanung	11
Phase IV - Implementierung und Betrieb	12
Phase V - Evaluierung und Optimierung	12
Komplexität meistern	13
Effizienzsteigerung durch Automatisierung und Zentralisierung	13
Synergien zwischen BCM und ISMS	13
Transparenz und Revisionssicherheit	14
3. Fazit	14

01 Business Continuity Management

Eine Lebensversicherung mit historischen Wurzeln

Das Business Continuity Management (BCM) ist mittlerweile deutlich mehr als eine rein operative Vorsorgemaßnahme auf dem Papier. Was früher oftmals ein Hygienefaktor im Zuge des Aufbaus eines ISMS betrachtet wurde, hat sich heute nicht zuletzt aufgrund einer ständig steigenden Abhängigkeit von IKT Dienstleistungen und -Dienstleistern sowie der stetig steigenden Bedrohungslage zu einer Lebensversicherung für Unternehmen entwickelt. Es ist ein strategisches Führungsinstrument zur Sicherstellung der organisationalen Resilienz geworden und stellt im Idealfall die Handlungsfähigkeit eines Unternehmens in Notfall- und Krisensituationen sicher¹

Definition und strategische Bedeutung

Ein BCMS ist ein systematischer Rahmen, der Organisationen befähigt, sich auf schwerwiegende Störungen oder Notfälle vorzubereiten, mit einem angemessenen Notbetrieb darauf zu reagieren und den Normalbetrieb effizient wiederherzustellen.² Während präventive Informationssicherheitsmanagementsysteme (ISMS) wie die ISO 27001 darauf abzielen, Vorfälle zu verhindern, fokussiert sich das BCM auf die Bewältigung von Vorfällen, wenn alle präventiven Maßnahmen versagen.³ Ziel ist es, die Auswirkungen von Betriebsunterbrechungen auf ein Minimum zu reduzieren und dabei vor allem existenzbedrohende Schäden abzuwenden.

Eine kurze Historie

Heraklit prägte 500 v. Chr. das Zitat "Der Krieg ist der Vater aller Dinge".⁴ Das gilt auch für das Business Continuity Management, denn dieses hat seinen Ursprung im militärischen Umfeld. Historisch nachgewiesen wird die fortdauernde Planung, Umsetzung und Zielerreichung trotz Störung und Feindeinwirkung im Buch "Die

Kunst des Krieges" des altchinesischen Militärstrategen **Sun Tzu**, welches aus der gleichen zeitlichen Epoche wie das Zitat Heraklits stammt.⁵ Die Grundzüge dieser Resilienz gegen Störfaktoren finden sich später in den Werken des deutschsprachigen Militärtheoretikers von Clausewitz⁶ und fanden mit dem Einzug der Industriel-
len Revolution ihren Weg in das betriebliche Geschehen. In den 1950er Jahren wurde die Entwicklung vor allem in den Vereinigten Staaten durch das Department for Homeland Security und dem Department for Civil Defence und in Deutschland durch den Katastrophenschutz und die Zivilverteidigung in der zivilen Nutzung vorangetrieben.

Ab den frühen Achtziger Jahren rückte die Informationstechnologie stärker in den Fokus, da sie mit zunehmender Bedeutung in Geschäftsprozessen zu einem höheren Risikofaktor wurde.

Zuletzt hat sich das Verständnis des BCM zunehmend gewandelt und umfasst nun wieder die gesamte Organisation. Diese Entwicklung wurde maßgeblich durch internationale Gesetze vorangetrieben, wie etwa den

¹ Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 200-4: Notfallmanagement, Bonn 2021, S. 10.

² Vgl. International Organization for Standardization (ISO): ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements, Genf 2019.

³ Vgl. International Organization for Standardization (ISO): ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, Genf 2022.

⁴ Heraklit von Ephesos: Fragmente, zitiert nach Diels-Kranz (DK) 22 B 53.

⁵ Sunzi: Die Kunst des Krieges, ca. 5. Jh. v. Chr.

⁶ Clausewitz, Carl von: Vom Kriege, Berlin 1832.

US-amerikanischen **Sarbanes-Oxley Act (2002)** oder den britischen **Civil Contingencies Act (2004)**.⁷ Auch im deutschsprachigen Raum ist BCM indirekt festgeschrieben, beispielsweise durch das deutsche **KonTraG (1998)** sowie die verschiedenen **Corporate-Governance-Kodizes** in Deutschland und Österreich.⁸

Darüber hinaus wird das BCM durch eine Vielzahl weltweiter Normen und Industriestandards konkretisiert. Zu den wichtigsten zählen:

- **International:** **ISO 22301:2012** und **ISO 17799**.⁹
- **National:** **NFPA 1600** (USA), **BS 7799:2002** (Großbritannien) sowie die **ÖNORM A 7799** (Österreich).¹⁰
- **Regionalspezifisch:** Die BCM Better Practice Guidelines für Australien und Neuseeland.

Auch der Finanzsektor spielt eine zentrale Rolle bei der Standardisierung, insbesondere durch die Publikationen des **Basler Ausschusses** zu **Basel II** sowie die deutschen **MaRisk** (Mindestanforderungen an das Risikomanagement), welche spezifische Vorgaben für Kreditinstitute enthalten.¹¹ Die methodischen Grundlagen und der strukturelle Rahmen für das Business Continui-

ty Management (BCM) werden maßgeblich durch den „**Good Practice Guide**“ definiert.¹² Herausgeber dieses Leitfadens ist das britische **Business Continuity Institute (BCI)**. Um eine einheitliche Qualifikation der Fachkräfte sicherzustellen, existieren zudem die sogenannten „**Joint Standards**“.¹³ Diese legen die Kernkompetenzen für Praktiker fest und werden gemeinschaftlich vom BCI sowie dem US-amerikanischen **Disaster Recovery Institute International (DRII)** publiziert.

Nationale Standards in Deutschland

Auf nationaler Ebene hat das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** spezifische Richtlinien für das Notfallmanagement im Kontext des IT-Grundschutzes etabliert:

- **BSI-Standard 100-4:** Ursprüngliche Fassung zum Aufbau eines Notfallmanagements.¹⁴
- **BSI-Standard 200-4:** Der aktuelle Nachfolger, der im Zuge der Modernisierung des IT-Grundschutzes veröffentlicht wurde und den Prozess zeitgemäß abbildet.¹⁵

1.1 Die Kernkomponenten eines BCMS

Ein wirksames BCM-System nach ISO 22301 basiert auf mehreren Säulen:¹⁶

- **Business Impact Analyse (BIA):** Sie ist das analytische Herzstück und dient der Identifikation zeitkritischer Geschäftsprozesse sowie der Bestimmung notwendiger Wiederanlaufparameter wie Wiederherstellungszeiten (RTO) und maximal tolerierbarer Ausfallzeiten (MTPD).¹⁷
- **Risikobeurteilung:** Hierbei werden spezifische Szenarien (z. B. Cyberangriffe, Infrastruktur Ausfälle) bewertet und priorisiert, um gezielte Strategien zu entwickeln.

⁷ Vgl. Sarbanes-Oxley Act of 2002, Pub. L. 107-204, 116 Stat. 745; sowie UK Parliament: Civil Contingencies Act 2004, c. 36.

⁸ Vgl. Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), BGBl. I 1998 S. 786.

⁹ Vgl. Vorläufer-Normen der ISO/IEC 27000-Reihe, ehemals BS 7799 bzw. ISO/IEC 17799.

¹⁰ Vgl. National Fire Protection Association: NFPA 1600: Standard on Continuity, Emergency, and Crisis Management.

¹¹ Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): Rundschreiben 05/2023 (BA) - Mindestanforderungen an das Risikomanagement (MaRisk), Bonn/Frankfurt am Main 2023.

¹² Vgl. Business Continuity Institute (BCI): Good Practice Guidelines (GPG), London (aktuelle Fassung).

¹³ Vgl. The BCI & DRII: Professional Practices for Business Continuity Management.

¹⁴ Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 100-4: Notfallmanagement, Bonn 2008.

¹⁵ Vgl. BSI: BSI-Standard 200-4, a.a.O.

¹⁶ Vgl. ISO 22301:2019, Kapitel 8.

¹⁷ Vgl. International Organization for Standardization (ISO): ISO/TS 22317:2021 Security and resilience — Business continuity management systems — Guidelines for business impact analysis (BIA), Genf 2021.

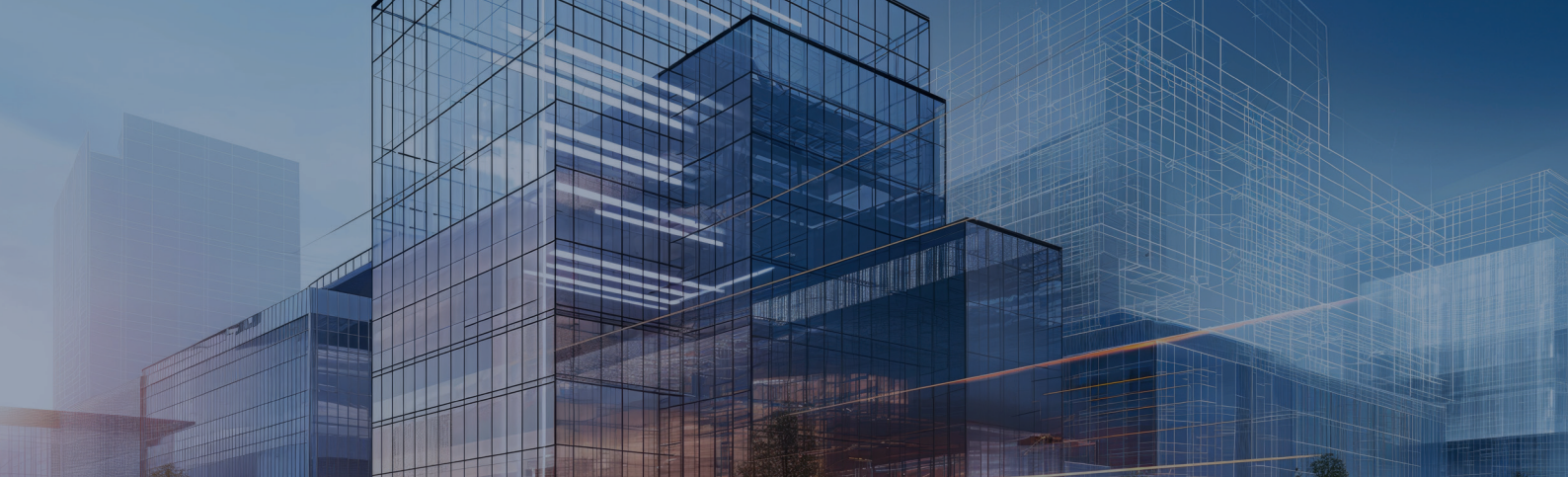
- **Notfallstrategien und -lösungen:** Die Organisation legt fest, welche Ressourcen – wie Personal, IT-Systeme, alternative Standorte oder Partner – zur Aufrechterhaltung der Betriebsfähigkeit zwingend erforderlich sind.
- **Notfallhandbücher und Pläne:** Diese Dokumente dienen der operativen Umsetzung und enthalten konkrete Handlungsanweisungen, Kommunikationswege und Eskalationsprozeduren für den Krisenstab und die Fachbereiche.

1.2. Der PDCA-Zyklus: Kontinuierliche Verbesserung der Resilienz

Wie alle Managementsysteme im Bereich der Informationssicherheit ist auch ein BCMS kein statisches Projekt, sondern ein lebender Prozess, der dem PDCA-Modell (Plan-Do-Check-Act) folgt:¹⁸



¹⁸ Vgl. Deming, W. Edwards: Out of the Crisis, MIT Press, Cambridge 1986 (Grundlage des PDCA-Modells).



02 Die Cyberbedrohungslage 2026: Paradigmenwechsel in der Resilienz

In den letzten Jahren hat sich die Bedrohungslage dramatisch verändert. Die Angriffe in den späten 1990er und frühen 2000er Jahren waren geprägt von einem anarchistischen „Jugend forscht“ Charakter und länger gediente Informationssicherheits-Experten erinnern sich sicherlich noch an die Wurm-Ära geprägt von Malware-Würmern wie Onel de Guzmans ILOVEYOU oder dem MyDOOM-Wurm. Die explosionsartige Entwicklung des Internets in der Mitte der 2000er Jahre ging Hand in Hand mit der Kommerzialisierung des Hackings einher. Aus den Script Kiddies wurden professionelle Hacker und Datendiebstahl und Phishing wurden zu lukrativen Geschäftsmodellen. Mit dem Einzug von Bitcoin erhielten Cyberkriminelle das perfekte Werkzeug, eine anonyme und nicht verfolgbare Zahlungsmethode. Diese Technologie wirkte wie ein Katalysator für die rasante Entwicklung neuer Ransomware-Angriffe und Ransomware wurde zu einem Milliardenbusiness.

Ein zweiter Faktor ist die immer stärkere Digitalisierung der Wirtschaft. Ein starker Indikator für diese Entwicklung findet sich in der EU-Strategie „Digitale Dekade 2023“¹⁹ mit dem Ziel, Europas digitale Transformation in

den Bereichen Kompetenzen, Infrastruktur, Wirtschaft und öffentliche Dienste voranzutreiben. Darin fordert die EU unter anderem, dass bis 2030 mindestens 75 % der EU-Unternehmen Cloud-Computing, Big Data oder Künstliche Intelligenz nutzen sollen. Zudem sollen mindestens 90 % der kleinen und mittleren Unternehmen eine grundlegende digitale Intensität erreichen.

Heute ist die Bedrohung durch Cyberangriffe – insbesondere Ransomware und Supply-Chain-Attacken – oder weitläufige Systemausfälle keine theoretische Gefahr mehr, sondern eine statistische Gewissheit. Die hohe Abhängigkeit moderner Geschäftsprozesse von IKT-Systemen und Informationswerten führt dazu, dass nahezu jede digitale Störung unmittelbar die Lieferfähigkeit oder Dienstleistungserbringung beeinträchtigt. Hier setzt das BCM an und versucht, den Betrieb der Geschäftsprozesse auch in Notfall- und Krisenzeiten so weit aufrechtzuerhalten, dass das Unternehmen überlebensfähig bleibt. Dies erfordert jedoch die Zeit für eine intensive Vorbereitung und Erprobung. Zeit, die man zum Beginn eines Resilienz- oder Zertifizierungsprojekts oft nicht hat

¹⁹ Vgl. Europäische Kommission: Beschluss (EU) 2022/2481 des Europäischen Parlaments und des Rates über das Politikprogramm 2030 für die digitale Dekade, Brüssel 2022.

2.1. Management-Fokus: Warum BCM heute priorisiert werden muss

Die klassische “Top-Down” Implementierung von Informationssicherheits- Managementsystemen (ISMS) zeigt sich in der Praxis oftmals stark von Regulierung und Prävention getrieben. In der Phase I der ISMS-Implementierungsprojekte wird im Aufbau viel Zeit auf Definition von Richtlinien und Handbüchern gelegt. In der zweiten Phase werden erste Gap- und Risikoanalysen gemacht und dabei liegt der Fokus nicht selten nur auf den IKT-Systemen und IT-Prozessen. Erst in der Phase III wird mit BIAs und davon abgeleitet mit dem Aufbau eines BCM gestartet. Das Problem: Je nach vorhandener Reife, Komplexität und bereitgestellten Ressourcen können Phase I und II mehrere Monate bis hin zu Jahre dauern. In dieser Zeit muss sich das Unternehmen bei der Bewältigung eines Cyberangriffs oder eines IKT-Notfalls

mit der bestehenden Dokumentation begnügen. Diese umfasst nicht selten eine Prozesslandkarte aus den späten 1990ern und Geschäftsfortführungspläne, welche die aktuellen Prozesse nicht mehr widerspiegeln.

Zu behaupten, dass ein Unternehmen ohne ein aufrechtes BCM einen Notfall oder eine Krise nicht bewältigen kann, ist jedoch auch nicht korrekt. Allerdings hat das BCM bzw. seine Reife einen wesentlichen Einfluss auf das Ausmaß des Schadens. Die wichtigste Frage ist jedoch, ob das Unternehmen das Delta (Abb. 1) zwischen einer BCM gestützten Wiederherstellung mit parallelem Notbetrieb und einer Wiederherstellung ohne BCM aus Sicht der potenziellen Schäden (finanziell, Image, etc.) stemmen kann und möchte.

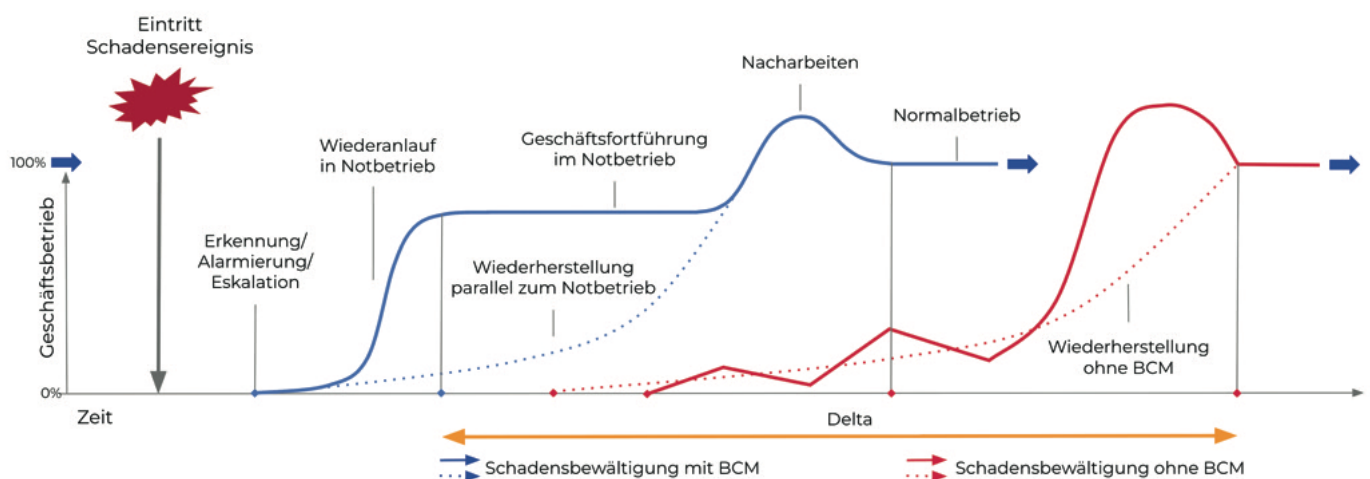


Abb. 1 - Unterschiede in der Bewältigung mit und ohne BCM

Im Jahr 2026 hat sich das Paradigma daher verschoben. Aufgrund der rasanten Entwicklung der Cyberbedrohungslage, der immer höheren Digitalisierung und der strengen regulatorischen Anforderungen (z. B. in **NIS2** oder **DORA**) sollte die Entwicklung des BCM nicht mehr erst am Ende der Sicherheits-Roadmap stehen. Die Geschäftsführung trägt vor allem im Umfeld von NIS2 die Verantwortung für die Aufrechterhaltung der Lieferfähigkeit und haftet zunehmend persönlich für Versäumnisse in der Notfall- und Krisenvorsorge.²⁰

²⁰ Vgl. Artikel 20 der Richtlinie (EU) 2022/2555 (NIS-2), welcher die Verantwortlichkeit der Leitungsorgane explizit vorschreibt.

2.2. ISMS und BCM - Parallel statt seriell

Unbestritten ist, dass die Integration von Informationssicherheitsmanagementsystem (**ISMS** nach **ISO/IEC 27001**) und Business Continuity Managementsystemen (**BCMS** nach **ISO 22301**) essentiell ist. Während eine serielle Implementierung (zuerst ISMS, dann BCMS) oft als übersichtlicher gilt, weil das BCMS auf Erkenntnisse aus dem ISMS aufbauen kann, bietet die parallele Implementierung signifikante strategische und operative Vorteile, ist jedoch mit spezifischen Herausforderungen verbunden.

Vorteile der parallelen Implementierung

1

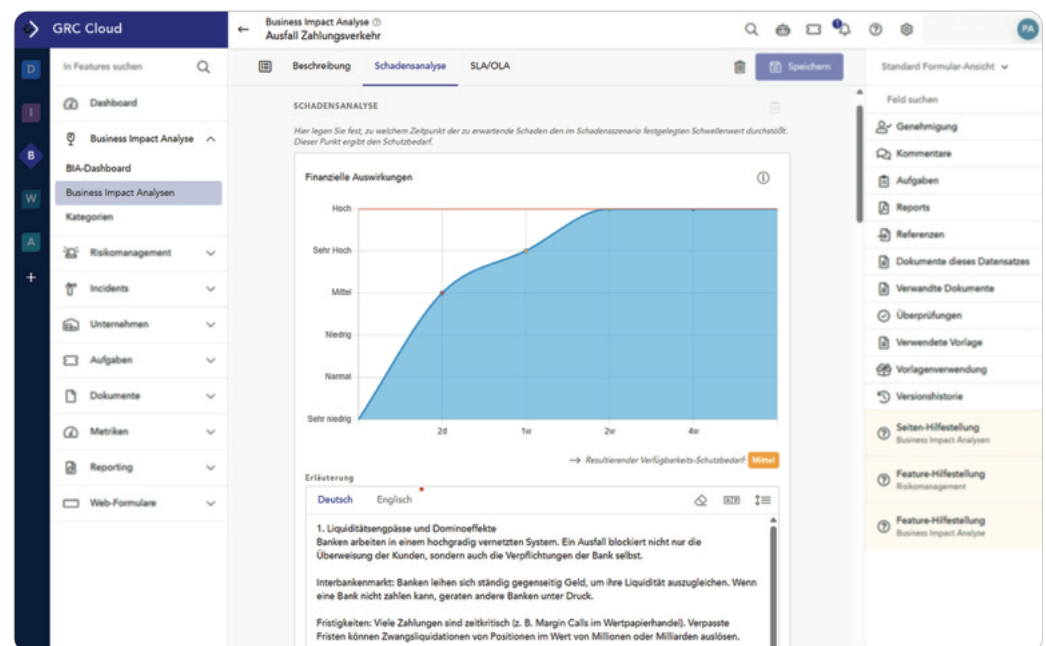
Nutzung von Synergien durch den Annex SL

Beide Normen, sowohl die ISO 27001 wie auch die ISO 22301, basieren auf der „High Level Structure“ (Annex SL), was eine identische Kapitelstruktur (z. B. Kontext der Organisation, Führung, Planung, Unterstützung, Bewertung der Leistung) bedeutet.²¹ Eine parallele Einführung ermöglicht es, frühzeitig im Zuge der Scope Definition bereits die relevanten wichtigen oder kritischen Prozesse, welche das BCM berücksichtigen muss, zu identifizieren. Ebenfalls lassen sich übergreifende Prozesse wie das Dokumentenmanagement, interne Audits und die Managementbewertung nur einmal für beide Systeme aufsetzen. Dies reduziert den administrativen Aufwand erheblich.

2

Ganzheitliche Risikobewertung und Business-Impact-Analyse (BIA)

In einem parallelen Ansatz können die Risikoanalyse nach ISO 27001 (Fokus auf CIA-Schutzziele: Vertraulichkeit, Integrität, Verfügbarkeit) und die BIA nach ISO 22301 (Fokus auf Zeitkritikalität und Wiederherstellung) verzahnt werden. Da IKT-Systeme oft die kritischsten Ressourcen für Geschäftsprozesse darstellen, liefert die BIA dem ISMS präzise Anforderungen für die Verfügbarkeit (RTO, RPO), während das ISMS die notwendigen Sicherheitskontrollen liefert, um Vorfälle bereits im Vorfeld zu verhindern.



²¹ Vgl. International Organization for Standardization (ISO): ISO/IEC Directives, Part 1 — Consolidated ISO Supplement, Annex SL (Harmonized structure for MSS).

3

Konsistente Ressourcenplanung

Ein paralleles Vorgehen verhindert Redundanzen bei der Ressourcenallokation. Anstatt separate Teams für Notfall- und Krisenmanagement und Informationssicherheit mit ähnlichen Aufgaben zu betrauen, können Verantwortlichkeiten (z. B. Rollendefinitionen nach Kapitel 5.3 beider Normen) klar abgegrenzt und personelle Ressourcen effizienter genutzt werden. Vor allem wird das Zusammenspiel dieser Akteure deutlich gestärkt, denn nicht selten sind gerade das Notfall- und Krisenmanagement fachlich sehr weit von der Informationssicherheit.

4

Frühere Implementierung

Der vermutlich wichtigste Vorteil dieser Herangehensweise ist die deutlich frühere Implementierung. Wird sofort nach der Identifikation der kritischen/wesentlichen Geschäftsprozessen mit der BIA begonnen, kann umgehend mit der Erstellung wichtiger Dokumente wie der Notfallstrategien, Notfallpläne, Wiederherstellung- und Wiederanlaufpläne sowie definierter Sofortmaßnahmen begonnen werden. Schafft man es dann noch, zeitnah die Pläne und Sofortmaßnahmen im Zuge eines Schreibtischtests, oder besser noch eines Echttests, zu validieren, dann kann das Unternehmen frühzeitig auf eine zuverlässige und effiziente Notfallorganisation zurückgreifen.

Herausforderungen und Stolpersteine

1

Unterschiede zwischen Prävention und Bewältigung

Obwohl die Struktur ähnlich ist, unterscheiden sich die Kernelemente zwischen ISMS und BCM methodisch. Während das ISMS stark präventiv und kontrollorientiert arbeitet, ist das BCMS reaktiv und auf die Aufrechterhaltung der Betriebsfähigkeit in Ausnahmesituationen ausgerichtet. Diese unterschiedlichen Denkweisen (Schutz vs. Fortführung) müssen harmonisiert werden, um Zielkonflikte in der Erarbeitung und Priorisierung von Maßnahmen zu vermeiden.

2

Koordinationsaufwand zwischen Fachabteilungen

Der Aufbau und Betrieb eines ISMS wird oft in der IT-Governance oder im Bereich des CISO verortet, während BCM als ganzheitlicher Business-Ansatz die Fachbereiche (Business Units) stärker einbindet. Eine parallele Implementierung erfordert eine straffe Governance, um sicherzustellen, dass die IT-Notfallplanung (Teil des ISMS) sich möglichst nahtlos mit den Geschäftsfortführungsplänen der Fachbereiche verbindet.

3

Hohe Komplexität und Projektbelastung

Die gleichzeitige Einführung zweier komplexer Managementsysteme erfordert eine hohe Kapazität an Fachpersonal und Zeit. Die Organisation muss sicherstellen, dass Schlüsselpersonen nicht durch zwei Mammutprojekte gleichzeitig gesperrt und überlastet werden, was die Qualität der Umsetzung gefährden könnte.

2.3. Schnell zu Ergebnissen

Wie lässt sich der Drahtseilakt zwischen ISMS und BCM Implementierung in der Praxis umsetzen? Beide Systeme bauen auf dem PDCA Zyklus auf und so macht es Sinn, vorhandene Synergien zu identifizieren und zu nutzen.

Phase I Strategische Ausrichtung und Governance

Festlegung der Leitlinien:

Erstellung und Verabschiedung einer gemeinsamen Grundsatzerklärung der obersten Leitung, welche die Ziele für Informationssicherheit und Business Continuity definiert. Darin sollte sich der besondere Stellenwert und die damit verbundene Priorisierung des BCM aufgrund der Cyberbedrohungslage und der hohen IKT Abhängigkeit des Unternehmens wiederfinden.

Strukturierung der Verantwortlichkeiten:

Im Zuge der Festlegung der ISMS Organisation erfolgt die Ernennung der Verantwortlichen. Es sollte darauf geachtet werden, dass es dabei Brückenfunktionen zwischen ISMS- und BCM-Team geben sollte, um Informationsverluste zu vermeiden. Ein Krisenstab sowie BCM-Verantwortliche werden benannt und mit den notwendigen Befugnissen ausgestattet (Anforderung aus ISO 22301, Kap. 5.3).²²

Definition des Anwendungsbereichs (Scope):

Der Anwendungsbereich des ISMS und BCM werden definiert. Dabei sollten vor allem bei der Festlegung des BCM Scopes die Fachbereiche mit eingebunden werden. Ebenso sind die Schnittstellen zwischen ISMS und BCM für die 2. Phase zu definieren.

Phase II Analysephase

Business Impact Analyse (BIA)

Es werden BIAs über die Kernprozesse des Unternehmens durchgeführt, um die kritischen Geschäftsprozesse zu identifizieren. Dabei werden mögliche Schäden in Abhängigkeit der Zeit und daraus abgeleitete Ausfallzeiten (MTPD – Maximum Tolerable Period of Disruption) und Wiederherstellungsziele (RTO – Recovery Time Objective) festgelegt.

Informationsfluss zum ISMS

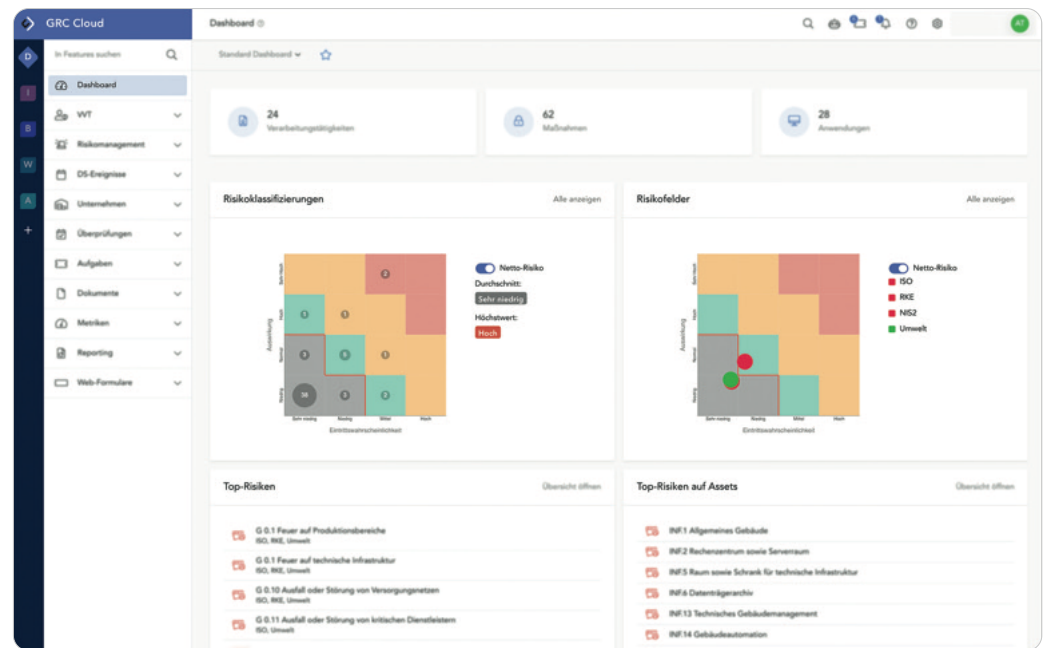
Die Ergebnisse der BIA werden dem ISMS-Projekt zur Verfügung gestellt, damit dort die Schutzbedarfsfeststellung der zugrundeliegenden IKT-Assets synchronisiert werden kann.

Risikobewertung

Identifikation und Bewertung der größten Bedrohungen für die Kontinuität (z.B. Ransomware, Infrastrukturausfall). Dabei sollte sichergestellt werden, dass die Methodik mit dem Risikomanagement des ISMS (z.B. nach ISO 27005)²³ kompatibel ist. Diese Bedrohungen zusammen mit den identifizierten kritischen Geschäftsprozessen sind der Ausgangspunkt für die Phase III, Strategie und Notfallplanung.

²² Vgl. ISO 22301:2019, Kap. 5.3 (Organizational roles, responsibilities and authorities).

²³ Vgl. International Organization for Standardization (ISO): ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks, Genf 2022.



Phase III Strategie und Notfallplanung

Kontinuitätsstrategien:

Auf Basis der BIA werden Strategien zur Fortführung des Betriebs festgelegt (z.B. alternative Standorte, manuelle Notbetriebe, Cloud-Redundanz).

Erstellung der GFPs (Geschäftsfortführungspläne):

Detaillierte Pläne zur Wiederherstellung der kritischen Prozesse werden dokumentiert (vgl. Kap. 8.4 ISO 22301:2019). Diese Pläne sollten derart ausgestaltet sein, dass sie ein fachkundiger Mitarbeiter im Notfall findet (elektronisch oder auf Papier) und derart umsetzen kann, dass der Notbetrieb erreicht wird. Diese Pläne werden eng mit den IT-Service-Continuity-Plänen des ISMS abgestimmt, damit die für den Notbetrieb erforderlichen Ressourcen im Notfall zur Verfügung stehen.

Notfall- und Krisenmanagementstruktur:

In dieser Phase macht es Sinn, das Notfall- und Krisenmanagement im Unternehmen einzubinden bzw., falls nicht vorhanden, aufzubauen. Diese besondere Aufbauorganisation sollte als hierarchisches System die zentrale Drehscheibe für Alarmierung, Eskalation, Kommunikation und Bewältigung darstellen. (vgl. dazu ISO 22320 Notfallmanagement und 22361:2023 Krisenmanagement).²⁴

²⁴ Vgl. International Organization for Standardization (ISO): ISO 22320:2018 Security and resilience — Emergency management und ISO 22361:2022 Security and resilience — Crisis management.

Phase IV Implementierung und Betrieb

Ressourcenbereitstellung:

Die für den Notbetrieb notwendigen Ressourcen (Personal, Ersatz-IKT, Logistik) werden definiert. Hier ist es wichtig,

- vertragliche Aspekte zu beachten (z.B. bietet der Hersteller einen Cold Stand By in einer definierten Zeit an, stimmen die vereinbarten SLAs grundsätzlich mit den Erfordernissen aus dem BCM überein?)
- personelle Ressourcen sicherzustellen - Gibt es ausreichend geschultes Personal, um einen Notbetrieb über längere Zeit aufrechtzuerhalten?
- sind physische Ressourcen wie Ersatzräume oder Ersatzhardware zugesichert und entsprechen Sie den Sicherheitsvorgaben des Unternehmens?

Awareness-Maßnahmen:

Das Personal wird über die Notfallrollen informiert und für die Bedeutung des Business Continuity Managements sensibilisiert.

Phase V Evaluierung und Optimierung

Notfall und Krisen Übungsprogramm:

Der wichtigste Schritt für die Sicherstellung der Wirksamkeit der Phasen I-IV. Es wird ein Plan erstellt, welcher regelmäßige Notfall- und Krisenstabsübungen auf einen längeren Zeitraum plant. Diese Übungen sollen Schwachstellen in der Planung aufdecken und stellen sicher, dass das Unternehmen bei einem echten Notfall möglichst wenige Überraschungen erleben muss. Als Beispiel seien hier die immer wieder unterschätzten Wiederherstellungszeiten im Bereich von Datenbankservern genannt. Hier wird oftmals mit optimistischen Werten gearbeitet, welche sich in der Praxis als völlig falsch herausstellen und aufgrund von Abhängigkeiten massive Verzögerungen im Wiederanlauf nachfolgender Applikationen niederschlagen. Wenn es die Unternehmensstruktur zulässt, dann sind "Echt-Tests" für solche Szenarien Gold wert, denn jeder noch so gute Schreibtischtest beachtet nie alle Faktoren.

Interne Audits:

Lassen Sie das Gesamtsystem regelmäßig auditieren, um die Erfüllung aller Vorgaben aus der ISO 22301 sicherzustellen.

Management-Bewertung:

Schließlich ist es wichtig, dass die oberste Leitung über die Ergebnisse der Übungen und Audits informiert wird. Dieser Schritt ist unerlässlich, um zum einen das Bewusstsein der Leitung aufrechtzuerhalten, aber auch um sicherzustellen, dass das System von der Leitung getragen wird, Ressourcen weiterhin zur Verfügung stehen und um kontinuierliche Verbesserungsmaßnahmen (KVP) sicherzustellen.

- Integriertes Risikomanagement: Risikoszenarien, Bedrohungen und Schwachstellen werden modulübergreifend verwaltet. Eine im ISMS identifizierte Bedrohung für ein Asset kann direkt in die Business Impact Analyse des BCM einfließen, um die Auswirkungen auf kritische Geschäftsprozesse zu bewerten.
- Zentrale Maßnahmenverfolgung: Kontrollen und Maßnahmen zur Risikoreduktion können zentral gesteuert werden. Der Umsetzungsstatus einer Sicherheitsmaßnahme im ISMS ist für den BCM-Verantwortlichen sofort sichtbar, um die Wiederherstellungsfähigkeit des Unternehmens realistisch einzuschätzen.

03 Fazit

Im Jahr 2026 ist Business Continuity Management (BCM) kein optionaler „Hygienefaktor“ mehr, sondern eine strategische Lebensversicherung für Unternehmen. Die Bedrohungslage hat sich durch hochprofessionelle Ransomware-Angriffe, Supply-Chain-Attacken und eine massive Abhängigkeit von IKT-Systemen verschärft. Gleichzeitig steigen die regulatorischen Anforderungen (z. B. durch NIS2 und DORA), wobei die Geschäftsführung zunehmend persönlich für Versäumnisse in der Krisenvorsorge haftet.

Ein zentraler Punkt des Dokuments ist die Abkehr von der klassischen, nacheinander folgenden Implementierung von ISMS (Informationssicherheit) und BCM. Das Problem dabei ist, dass eine serielle Einführung oft Jahre dauert, in denen das Unternehmen bei einem Notfall nur unzureichend geschützt ist. Daher ist der Ansatz einer parallelen Implementierung unter Nutzung von Synergien zwischen ISMS und BCM sowie einer Verzahnung von Risikoanalyse und Business Impact Analyse eine Chance, deutlich schneller zu einer operativen Handlungsfähigkeit in Krisenzeiten zu kommen.

Nicht zuletzt ist ein möglichst realitätsnahes Notfall- und Krisenübungen Programm ein essentieller Weg, um zu prüfen, ob das, was sich Notfall-, Geschäftsfortführungs- und Wiederherstellungsplänen findet, auch in der Praxis funktioniert.

Transparenz und Revisionssicherheit

Im Gegensatz zu Excel bietet die Akarion GRC Cloud eine lückenlose Historisierung und Revisionssicherheit. Durch integrierte Dashboards und automatisierte Reports lassen sich der Status der BCM-Planung und die aktuelle Risikosituation jederzeit managementtauglich aufbereiten. Die grafische Darstellung in Form einer Prozesslandkarte oder eines Vererbungsbaums macht Abhängigkeiten auf einen Blick sichtbar, die in Tabellen verborgen bleiben.

Ein Schlüssel zum Erfolg ist dabei die möglichst effiziente Nutzung der gewonnenen Daten und damit verbundenen Automatisierungen. Die Komplexität der Datenverknüpfungen (N:N-Beziehungen zwischen Prozessen, Assets und Bedrohungen) ist mit Excel-Lösungen kaum mehr fehlerfrei beherrschbar und der Einsatz spezialisierter GRC-Software wie die Akarion GRC Cloud stellt einen der größten Erfolgsfaktoren dar.



Der Autor

PHILIPP AMANN
Product Manager

Philipp Amann verfügt über mehr als 25 Jahre Erfahrung im Bank- und kommunalen Versorgungswesen als CISO, CISA und DSB. Wenn er dieses Wissen nicht gerade in die Weiterentwicklung der AKARION GRC Cloud einbringt, dann übt er „Hands On Risikomanagement“ als Guide bei Enduro Touren abseits der befestigten Straßen.



Quellen

Internationale Standards und Managementsysteme

- ISO 22301:2019 (Business Continuity Management System, BCMS)
- ISO/IEC 27001 (Informationssicherheits-Managementsysteme, ISMS)
- ISO 17799
- Annex SL (High Level Structure), die identische Grundstruktur beider ISO-Normen.
- ISO 22320 (Notfallmanagement)
- ISO 22361:2023 (Krisenmanagement)
- PDCA-Zyklus (Plan-Do-Check-Act) – Modell zur kontinuierlichen Verbesserung.

Nationale Standards und Gesetze (DACH-Raum und International)

- BSI-Standard 200-4 (Deutschland): Aktueller Nachfolger zum Aufbau eines Notfallmanagements im IT-Grundschutz.
- BSI-Standard 100-4 (Deutschland): Ursprüngliche Fassung zum Notfallmanagement.
- KonTraG (1998) (Deutschland): Gesetz zur Kontrolle und Transparenz im Unternehmensbereich.
- Corporate-Governance-Kodizes (Deutschland und Österreich).
- MaRisk (Mindestanforderungen an das Risikomanagement) (Deutschland): Spezifische Vorgaben für Kreditinstitute.
- NIS2-Richtlinie und DORA (Digital Operational Resilience Act): Aktuelle EU-Regulierungen, die die Priorisierung des BCM fordern.
- Sarbanes-Oxley Act (2002) (USA).
- Civil Contingencies Act (2004) (Großbritannien).
- NFPA 1600 (USA).
- BS 7799:2002 (Großbritannien).
- ÖNORM A 7799 (Österreich).

Fachliche Leitfäden und Organisationen

- Business Continuity Institute (BCI): Herausgeber des „Good Practice Guide“.
- Disaster Recovery Institute International (DRII): Mitherausgeber der „Joint Standards“ zur Qualifikation von Fachkräften.
- Basler Ausschuss: Publikationen zu Basel II (für den Finanzsektor).
- BCM Better Practice Guidelines für Australien und Neuseeland.

Historische und Strategische Referenzen

- Heraklit (Zitat).
- Sun Zu („Die Kunst des Krieges“).
- Von Clausewitz (Militärtheoretiker).
- EU-Strategie „Digitale Dekade 2023“.

Werkzeug-Referenz

- Akarion GRC Cloud: Eine spezialisierte GRC-Software, die im Kontext der Effizienzsteigerung und Datenverwaltung genannt wird.

Die smarte & intuitive SaaS-Lösung für ganzheitliches Management von Informationssicherheit, BCM & Datenschutz

information security

- ✓ ISO 27001
- ✓ ISO 27019
- ✓ BSI IT-Grundschutz (++)
- ✓ BSI 200-1/2/3
- ✓ B3S Gesundheit
- ✓ B3S Energie
- ✓ BSI C5
- ✓ VDA ISA (TISAX®)
- ✓ PCI DSS
- ✓ NIS-2
- ✓ DORA
- ✓ CUSTOM CONTROLS

business continuity

- ✓ NIS-2
- ✓ ISO 22301
- ✓ BSI IT-Grundschutz 200-4

audit

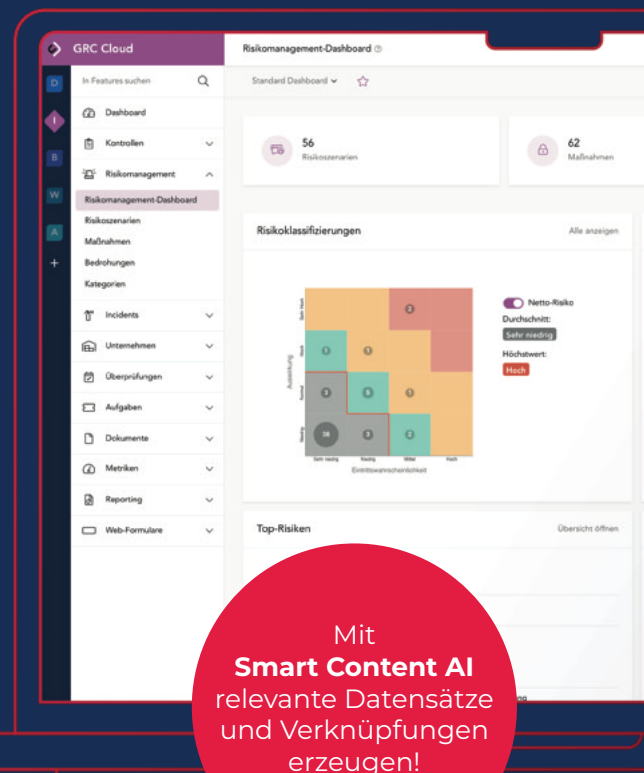
- ✓ ISO 27001
- ✓ ISO 27019
- ✓ NIS-2
- ✓ DORA

data protection

- ✓ ISO 27701
- ✓ SDM (DSGVO)

whistleblowing

- ✓ HinSchG
- ✓ EU-Whistleblower-Richtlinie



Digitale Souveränität durch
Hosting in Deutschland bei



**Kontaktieren Sie uns gerne für Ihre
individuelle Demo oder Ihren 14-tägigen Test!**

✉ sales@akarion.com | ☎ +49 89 628 265 64 | 🌐 www.akarion.com

Akarion AG

c/o ARQIS | Theatinerstr. 8
80333 Munich | Germany
www.akarion.com
munich@akarion.com



bitkom