

Institut für Business
Continuity & Resilience
Management
IBCRM e.V.



BIA-Anwenderleitfaden

Dokumentenhistorie

Version	Datum	Autor(en)	Bemerkung
V1.0	08. April 2019	IBCRM e.V.¹: Thorsten Scheibel, Claudia Krüger, Stefanie Fekonja, Patrick Mümken, Max Kaiser, David Schlenz, Matthias Hämmerle	Erstellung

¹ Inhalte und Meinungen in diesem Dokument geben ausschließlich die Ansichten des IBCRM e.V. bzw. dessen Autoren wieder.

Inhaltsverzeichnis

Dokumentenhistorie	1
Inhaltsverzeichnis	2
1. Resilience und Business Continuity Management	4
2. Business Impact Analyse (BIA) Anwenderleitfaden	5
2.1 Was verbirgt sich hinter dem BIA-Anwenderleitfaden	5
2.2 Was ist Ihr Nutzen?	5
2.3 Wie kann ich mich einbringen?	5
2.4 Was passiert mit meinem Feedback?	5
3. Hintergrundinformationen	6
3.1 Was ist eine BIA, wozu wird diese durchgeführt und in welchem Kontext steht diese zum BCM-Lifecycle?	6
3.2 Erfordernisse/Voraussetzungen	6
3.3 Kritische Erfolgsfaktoren für eine BIA	7
3.4 Wie wird der BIA-Anwenderleitfaden angewendet?	7
3.5 Unterschiede der BIA nach Branchen	8
3.6 Rahmenbedingungen (Recht, Normen, Standards, Kunden) Industrie, Banken, Versicherungen, gängige Normen	10
4. BIA-Anwenderleitfaden	11
4.1 Prozessschritte BIA	11
4.1.1 Visualisierung eines BIA-Durchführungszyklus	11
4.1.2 Rollen und Verantwortlichkeiten	12
4.2 BIA Konzeption	12
4.2.1 Prozessgegenstand	12
4.2.2 Festlegung der Schadensszenarien	12
4.2.3 Auswirkungsklassen	13
4.2.4 Zeithorizonte	15
4.2.5 Risikoappetit	15
4.2.6 Ressourcen	15
4.3 Ablauf der Business Impact Analyse	17
4.3.1 Vorbereitung und Erhebung der BIA	18
4.3.1.1 Vorbereitung und Initiierung	18
4.3.1.2 Bewertung der Geschäftsprozesse	18
4.3.1.3 Bestimmung der Maximum Tolerable Period of Disruption (MTPD)	18
4.3.1.4 Single Points of Failure	19
4.3.1.5 Erhebung der benötigten Ressourcen	19
4.3.1.6 Erhebung Schnittstellen zu anderen Prozessen	19
4.3.1.7 Erfassung kritischer Termine und Ereignisse	19

4.3.2	Nachbereitung BIA	20
4.3.2.1	Zentrale Qualitätsprüfung	20
4.3.2.2	Ableitung der Verfügbarkeitsanforderungen an die Ressourcen	20
4.3.2.3	Abstimmung mit den unterstützenden Einheiten / GAP Analyse	20
4.3.2.4	Erstellung und Freigabe der Ergebnisdokumente	21
4.4	Schnittstellen zu anderen Themenfeldern	21
4.5	Kontinuierliche Verbesserung	21
4.6	Abkürzungen, Begriffe und Definitionen	22
4.6.1	Abkürzungen	22
4.6.2	Begriffe und Definitionen	22
5.	Anhang Hilfsmittel Business Impact Analyse (BIA)	24
5.1	Projektplan zur Einführung und Umsetzung BIA	24
5.2	Template zur Durchführung der BIA	24

1. Resilience und Business Continuity Management

Resilience umfasst die Bestandteile Strategieentwicklung, Prozess- & Organisationsentwicklung, Risk Governance, Risikomanagement sowie Business Continuity Management (BCM).

Das BCM stellt somit einen Teil zur Unternehmensresilience dar (siehe Bild 1). Die Durchführung der Business Impact Analyse (BIA) (gelbe Markierung in Bild 1) wiederum stellt die Basis des BCM dar. Genau auf diesen wesentlichen Baustein der BIA wird in den folgenden Kapiteln eingegangen.

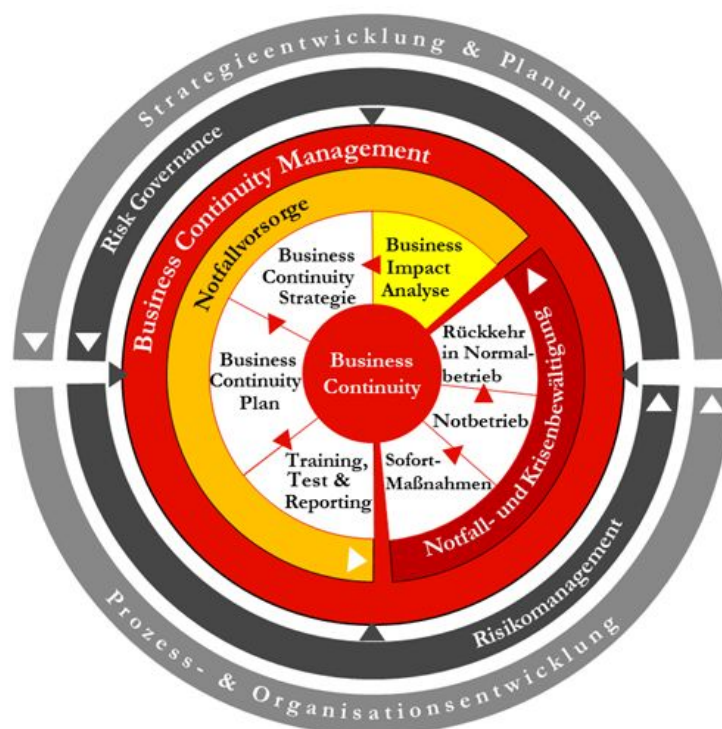


Bild 1: Einordnung der BIA in den Kontext Unternehmensresilience

2. Business Impact Analyse (BIA) Anwenderleitfaden

2.1 Was verbirgt sich hinter dem BIA-Anwenderleitfaden

Der BIA-Anwenderleitfaden hat zum Ziel eine praxisnahe Unterstützung bei der Durchführung einer Business Impact Analyse (BIA) zu liefern. Die BIA stellt dabei die Basis für ein funktionsfähiges Business Continuity Management dar (siehe Kap 3.1). Der Anwenderleitfaden hilft bei der Durchführung indem er einen schnellen Überblick ermöglicht durch eine einfache Darstellung der Inhalte, Abläufe und Anforderungen an eine BIA. Zudem werden Hilfsmittel für eine pragmatische Umsetzung zur Verfügung gestellt.

2.2 Was ist Ihr Nutzen?

Sie stehen vor der Herausforderung erstmalig eine BIA durchführen zu müssen oder wollen ihre bestehende BIA weiterentwickeln?

Folgende Vorteile bietet Ihnen dafür der Anwenderleitfaden:

- Profitieren von jahrelanger Praxiserfahrung von Business Continuity Managern unterschiedlicher Branchen.
- Angegebene Tipps helfen Ihnen mögliche "Anfangsfehler" zu vermeiden.
- Keine Fokussierung auf eine spezielle Norm, sondern der pragmatische Querschnitt aus der Praxis für die Praxis. Dennoch steht der Anwenderleitfaden im Einklang mit gängigen Normen wie der ISO 22301.
- Fokussierung auf das Wesentliche mit dem Motto "weniger ist mehr".
- Bereitstellen von direkt anwendbaren Hilfsmitteln.
- Ein Leitfaden immer auf dem aktuellen Stand, dadurch, dass Sie Ihre Erfahrungen direkt einbringen können und diese regelmäßig eingearbeitet werden (siehe Kap. 2.3).

2.3 Wie kann ich mich einbringen?

Im Sinne der kontinuierlichen Verbesserung setzen wir auf Ihren Beitrag zu Erfahrungen mit den vorgeschlagenen Beschreibungen und Hilfsmitteln. Nach der ersten Veröffentlichung sowie nach Anpassungen bitten wir um Ihre Kommentare bis zu einem definierten Zieldatum. Geplant ist, dass zweimal im Jahr Kommentare abgegeben werden können. Alle Vereinsmitglieder sowie interessierte Kreise werden aktiv informiert, wenn Kommentare wieder möglich sind. Unabhängig davon können Sie uns jederzeit über folgende Adresse kontaktieren: Feedback_Leitfaden@ibcrm.de

2.4 Was passiert mit meinem Feedback?

Wir freuen uns über jeden Kommentar, denn unser Ziel ist ein lebendiges Hilfsmittel zu ermöglichen. Wenn Sie uns direkt kontaktieren, werden Sie von uns eine Antwort erhalten.

Wenn Sie zu Textabschnitten oder Hilfsmitteln während der Kommentierungszeit Anmerkungen abgeben, werden diese nach Sichtung und Bewertung alle veröffentlicht. Der Kommentator erhält eine Rückmeldung wie mit seinem Verbesserungs- oder Weiterentwicklungsvorschlag umgegangen wird.

3. Hintergrundinformationen

3.1 Was ist eine BIA, wozu wird diese durchgeführt und in welchem Kontext steht diese zum BCM-Lifecycle?

Die BIA ist das Werkzeug für die strukturierte und einheitliche Erfassung sowie Bewertung "kritischer" Geschäftsaktivitäten. Die Kriterien zur Bestimmung der Kritikalität sind dabei individuell durch das jeweils durchführende Unternehmen im Vorhinein festzulegen. Mittels der BIA wird auf diese Weise unter Berücksichtigung des individuellen Risikoappetits der Anteil der Geschäftsaktivitäten ermittelt, welche durch Wiederanlauf- und Geschäftsfortführungspläne abgesichert werden sollten. Die BIA ermöglicht somit eine wirtschaftliche Grundlage zur Sicherung des Kernbetriebs. Im BCM-Lifecycle legt die BIA den Grundstein für alle nachfolgenden Aktivitäten.

3.2 Erfordernisse/Voraussetzungen

Für die Durchführung einer BIA sind zahlreiche Detailinformationen über die jeweiligen Unternehmensaktivitäten erforderlich. Neben der Bereitstellung umfangreicher schriftlicher Informationen sind insbesondere auch die Informationen von involvierten Experten aus dem Unternehmen von entscheidender Rolle.

Obwohl mit dem Betreiben eines Business Continuity Managements bereits das grundlegende Management Commitment vorliegt (bzw. vorliegen sollte), ist der besondere Zeit- und Ressourcenaufwand für die Durchführung einer BIA gesondert hervorzuheben und mit allen Beteiligten im Vorfeld näher abzustimmen.

Damit die wesentlichen Informationen bei der Durchführung vorliegen, ist frühzeitig Transparenz herzustellen, welche Informationen vorliegen müssen. Gleichzeitig ist dafür Sorge zu tragen, dass die Voraussetzungen über die verantwortlichen Personen geschaffen werden. Die zwingende Grundlage in der klassischen BIA stellen die Prozesse eines Unternehmens dar, welche idealerweise in einer unternehmensweiten und einheitlichen Prozesslandkarte dokumentiert sind. Darüber hinaus sind folgende Angaben wichtig jedoch nicht alle zwingend Voraussetzung:

- Einordnung der Prozesse (Geschäfts-, Support-, Managementprozesse)
- Rollen und Verantwortlichkeiten, insbesondere Prozessverantwortlichkeit
- Kurzbeschreibung der Prozesse (Input, Aktivität, Output)
- Prozesshäufigkeit (Anzahl der Durchläufe)
- Automatisierungsgrad der Prozesse (vollständig automatisiert z.B. ohne manuellen Eingriff)

- Leistungsniveaus der Prozesse (was liefern die Prozesse im Zeitintervall x? Gibt es interne oder externe Leistungsvereinbarungen wie Service Level oder Operational Level Agreements (SLA, OLA)?)
- Transparenz über die Auswirkungen für das Unternehmen, sofern die Prozesse Ihre regulären Tätigkeiten nicht vollbringen
- Besondere Zeiten/Fristen, welche innerhalb eines Jahres innerhalb des Prozesses auftreten
- Prozessabhängigkeiten zur Darstellung von Prozessketten (welche Prozesse liefern In- bzw. Output)
- Art und Anzahl der Ressourcen (Personal, IT-Applikationen und -ausstattung, Daten und Informationen, Sonderausstattung, Infrastruktur und Räumlichkeiten)
- Interne und externe Dienstleister sowie die Abhängigkeit der Prozesse zu diesen Dienstleistern

3.3 Kritische Erfolgsfaktoren für eine BIA

Damit Geschäftsprozesse im Rahmen einer BIA einheitlich und damit vergleichbar sowie nachvollziehbar und wiederholbar bewertet werden, sind folgende kritische Erfolgsfaktoren zu berücksichtigen:

- Identische Bewertungsgrundlagen für alle betrachteten Prozesse, damit eine Vergleichbarkeit gewährleistet ist (Bspw. Berücksichtigung von Opportunitätskosten wie Personalausfallkosten, Zeitdauer der Kosten- und Verlustbetrachtung, Berücksichtigung von Sekundäreffekten, Prämissen für Zinsen, Zins- und Marktentwicklung, Kundenverhalten etc.)
- Dokumentation und Erläuterung der gewählten Prämissen (Bspw. für finanzielle Schäden. Von welcher Kundenreaktion wird ausgegangen, welche Schäden werden in welcher Höhe berücksichtigt, welche nicht?)
- Nachvollziehbarkeit der Schadenseinschätzungen z.B. durch Werte aus dem Controlling und der Bilanz sowie GuV.
- Inhaltliche Verantwortung für die Angaben in der BIA durch die Prozessverantwortlichen. Abstimmung der Vorgehensweise (Bsp. Skalierungen, finanzielle Schwellenwerte etc.) mit Risikomanagement.

3.4 Wie wird der BIA-Anwenderleitfaden angewendet?

Der BIA-Anwenderleitfaden bietet vor allem eine **praxisnahe** Unterstützung bei der Konzeptionierung und Durchführung von BIAs im Unternehmen. Daher legt das IBCRM e.V. großen Wert auf die direkte Anwendbarkeit der beschriebenen Schritte und Templates, ohne viel zusätzlichen Aufwand z.B. in Form von externer Beratung erforderlich zu machen. Damit unterscheidet sich dieser BIA-Anwenderleitfaden von bestehenden Leitfäden welche zumeist einen größeren Detailgrad aufweisen.

Die Bestandteile des BIA-Anwenderleitfadens sind modular und je nach Reifegrad flexibel im Unternehmen einzusetzen, anzupassen und zu erweitern. Bei der Konzeption und Durchführung der BIA sind individuelle Unternehmensanforderungen sowie rechtliche und regulatorische Erfordernisse zu berücksichtigen.

Der BIA-Anwenderleitfaden ist ein lebendes Hilfsmittel des IBCRM e.V. Das bedeutet die Inhalte werden sich im Laufe der Zeit durch Vereinsmitglieder oder andere interessierte Kreise weiterentwickeln. Konzeptionelle Änderungen, die sich daraus ergeben, können damit auch zu einer kontinuierlichen Verbesserungen in Ihrer BIA beitragen.

3.5 Unterschiede der BIA nach Branchen

Die grundlegende Logik - die Ermittlung der kritischen Unternehmensaktivitäten - ist branchenübergreifend das zentrale Element der BIA. Dennoch haben insbesondere die nachfolgenden Faktoren Einfluss auf die Art und Weise der BIA-Durchführung:

Merkmal	Differentiator
Branche	<ul style="list-style-type: none"> • Rechtliche und regulatorische Anforderungen (z.B. MaRisk) • Kundenanforderungen (z.B. Supply-Chain-Continuity) • Berücksichtigung technischer Ausstattungen (Maschinen, Anlagen, Produktionsmittel, Rohstoffe) und Versorgung (Bspw. Druckluft)
Unternehmensgröße	<ul style="list-style-type: none"> • Umfang der BIA • Detailgrad der BIA

Die Merkmale in der o.g. Tabelle wirken sich konkret in folgender Hinsicht auf die BIA aus:

BIA Bestandteil	Beschreibung
Untersuchungsgegenstand	Klassisch bilden Prozesse den Untersuchungsgegenstand der BIA. Daneben können aber auch Produkte, Aktivitäten, "Ergebnisse", Services oder der organisatorische Aufbau als Basis für die Durchführung einer BIA herangezogen werden. ² Entscheidend ist, dass eine möglichst einheitliche Grundlage verwendet wird, um eine Vergleichbarkeit herzustellen.
Kritikalitätsmerkmale	Je nach Branche ist es sinnvoll, unterschiedliche Faktoren für die Ermittlung der Kritikalitäten von Geschäftsaktivitäten heranzuziehen. Während Faktoren wie finanzielle, reputative oder rechtliche & regulatorische Auswirkungen recht universell einsetzbar sind, können und sollten diese bei Bedarf um andere Faktoren erweitert oder gar ersetzt werden. So können beispielsweise auch Faktoren wie Safety (Bsp. Arbeitsschutz) und Security (IT, phys. Sicherheit), Unternehmensstrategie, Umweltschäden oder auch die Dringlichkeit kombiniert mit der Fallzahl von Patientenbehandlungen im Gesundheitswesen zum Einsatz kommen.

² Die ISO/TS 22317 beschreibt verschiedene Untersuchungsgegenstände für die BIA.

Schadensperioden	In Abhängigkeit der Branche sind auch die betrachteten zeitlichen Ausfallspannen unterschiedlich. Während einige Branchen eine minuten- oder stundengenaue Differenzierung erfordern (bspw. Krankenhäuser oder Finanzdienstleister), sind in anderen Branchen Tages- oder Wochenhorizonte der Planungszeitraum der Wahl (z.B. verarbeitende Industrie).
Kritikalitätsbestimmung	Auch die Branche kann einen Einfluss auf den Risikoappetit eines Unternehmens haben, welcher sich wiederum auf die Art und Weise der Ermittlung von kritischen Geschäftsaktivitäten auswirkt. Dies liegt insbesondere an den Schwellenwerten sowie den einzubeziehenden Faktoren für die Kritikalität. Dabei stellt sich auch die Frage, ob bei mehreren verwendeten Kritikalitätsmerkmalen eine Kombination, also Zusammenführung, oder separate Betrachtung genutzt wird.
Detailgrad der Unternehmensaktivitäten	Das Granularitätslevel bei der Analyse von Unternehmensaktivitäten zeigt auf, wie sehr aggregiert bzw. detailliert die Betrachtungsweise in der BIA ist. Während einige Branchen eine sehr kleinteilige Betrachtung erfordern, sind in anderen Branchen deutlich gröbere Abläufe Untersuchungsgegenstand. Entscheidend ist, dass die gleiche "Flughöhe" in der BIA für das gesamte Unternehmen verwendet wird, um eine Vergleichbarkeit herzustellen.
Ressourcen	Je nach Branche werden andere Arten und Stückzahlen von Ressourcen verwendet. Diese können kleinteilig von einzelnen Teilkomponenten bis hin zu Großgeräten wie Maschinen und Fahrzeugen reichen. Auch eine Kombination ist möglich.
Umfang	Insbesondere durch rechtliche und regulatorische Anforderungen wird der Umfang der zu untersuchenden Aktivitäten beeinflusst. Vor allem in der Banken- und Versicherungsbranche legen die Aufsichtsinstanzen auf eine lückenlose Gesamtbetrachtung des Unternehmens wert, wohingegen in anderen Branchen auch die Fokussierung oder strikte Unterscheidung von Geschäfts-, Support- und Managementprozessen zulässig ist.
Häufigkeit der Durchführung	Ebenfalls wie beim Umfang, beeinflussen eigene Anforderungen des Unternehmens sowie rechtliche und regulatorische Anforderungen die Häufigkeit der BIA-Durchführung. Auch hier gelten besonders für Banken und Versicherungen verschärfte Auflagen, sodass beispielsweise eine jährliche Aktualisierung der BIA erforderlich ist. In anderen Branchen kann ein Zwei- oder

	gar Dreijahresrhythmus ausreichend sein. Wichtig ist zu beachten, dass es vom Durchführungszyklus unabhängige Trigger geben kann, welche eine anlassbezogene Aktualisierung der BIA-Ergebnisse erforderlich machen. Dies ist vor allem bei Umstrukturierungen im Unternehmen der Fall, in deren Folge sich die Geschäftsaktivitäten verändern.
--	--

3.6 Rahmenbedingungen (Recht, Normen, Standards, Kunden) Industrie, Banken, Versicherungen, gängige Normen

Bei der Konzeptionierung und Implementierung der BIA gibt es Rahmenbedingungen zu beachten, welche sich durch Recht & Regulatorik, Normen und Standards sowie industrie- und unternehmensspezifische Anforderungen ergeben. Das jeweilige Unternehmen sollte sich daher im Voraus der BIA-Einführung bewusst machen, ob und welche

- verbindlichen Auflagen (rechtlich & regulatorisch) bestehen
- weiteren Ausarbeitungen für die BIA in Betracht gezogen werden sollten (z.B. Normen und Standards, Good/Best Practices)

Bei diesen Überlegungen der Rahmenbedingungen ist zwischen zwingend verpflichtenden und freiwilligen Auflagen bzw. Anforderungen zu unterscheiden. Denn rechtliche und regulatorische Anforderungen sind zwar unumgänglich, jedoch bleibt auch hier ein gewisser Gestaltungsspielraum.

Folgend finden Sie beispielhaft eine Liste von Anforderungen, die Sie zur Bewertung benötigen werden.

Rahmen- bedingung	Branche	Normen, Standards, Rechtsanforderungen	National	Inter- national
Normen		<ul style="list-style-type: none"> • ISO 22301 und • ISO 22317 • alle BCM Standards aus ISO/TC 292 "Security & Resilience" Catalogue 		x
Rechtlich und regulatorisch	Allgemein	<ul style="list-style-type: none"> • BGB • IT-SiG • KritisV 	x x x	
	Banken	<ul style="list-style-type: none"> • CRR • BCBS 239 • EBA Leitlinie zur internen Governance • KWG • MaRisk • BAIT 	x x x	x x x

	Versicherungen	<ul style="list-style-type: none"> • Solvency II • VAG • MaGo • VAIT 	<p>x</p> <p>x</p> <p>x</p>	<p>x</p>
Good/Best Practices	Allgemein	BSI 100-4	x	
		BCI Good Practice Guidelines		x

Good oder Best Practices dienen als Hilfestellung bei der Umsetzung von Anforderungen und sind oftmals für deren Erfüllung ausreichend.

Sofern eine Zertifizierung angestrebt wird, sind Anforderungen aus der jeweils zu zertifizierenden Norm besonders hervorzuheben, da diese erfüllt und die Nachweis gegenüber dem Auditor erbracht werden müssen.

4. BIA-Anwenderleitfaden

4.1 Prozessschritte BIA

4.1.1 Visualisierung eines BIA-Durchführungszyklus

Folgende Grafik stellt einen BIA Durchführungszyklus dar.

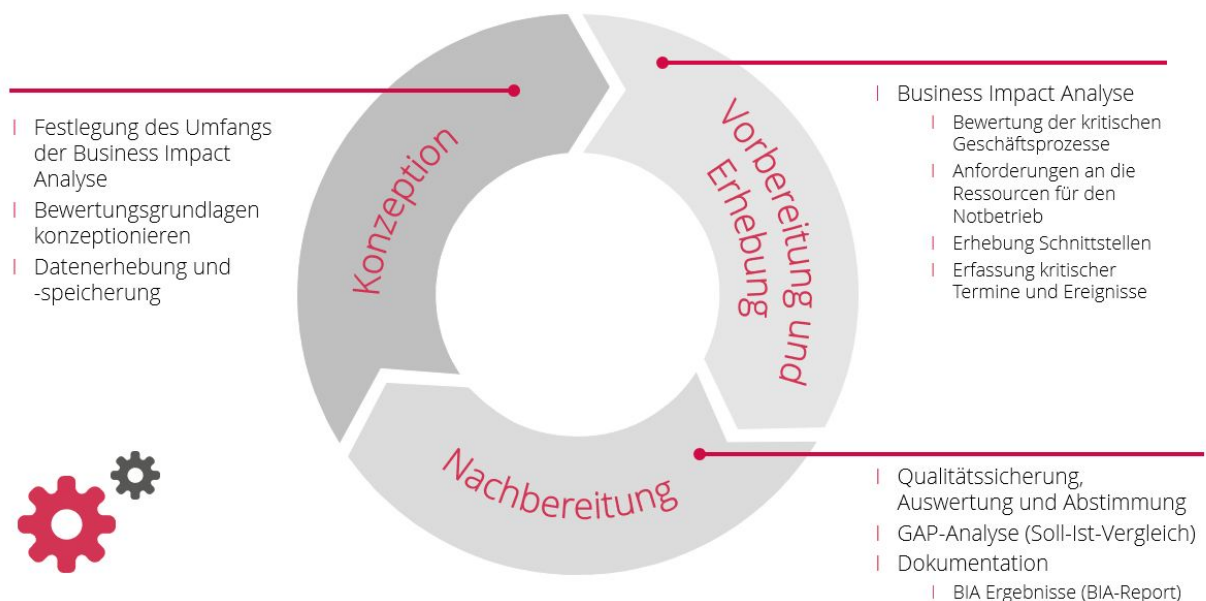


Bild 2: BIA Durchführungszyklus

In der Konzeptionsphase wird der Umfang der Business Impact Analyse festgelegt. Dazu gehört auch die Wahl der Geschäftsprozesse. Ebenfalls werden in dieser Phase die Bewertungsgrundlagen konzipiert und die Datenerhebung und -Speicherung abgestimmt. Diese Phase ist ausführlich in der initialen BIA erforderlich. In den Folgejahren werden üblicherweise lediglich Anpassungen durchgeführt, falls dies erforderlich sein sollte. In der Erhebungsphase werden die kritischen Geschäftsprozesse identifiziert und die Anforderungen an die Ressourcen im Notbetrieb erhoben. In der Nachbereitungsphase findet eine GAP-Analyse (Soll-Ist-Vergleich) der RTO Werte der Ressourcen statt. Zudem erfolgt die Qualitätssicherung, Auswertung und Erstellung eines Ergebnisberichts.

4.1.2 Rollen und Verantwortlichkeiten

Nachstehende Rollen und Verantwortlichkeiten gibt es während des BIA Zyklus.

Prozessverantwortlicher

Wird von der verantwortlichen Leitung bestimmt. Ist für die Führung der im Prozess tätigen Mitarbeiter³ verantwortlich. Außerdem auch für die Planung und Einführung des Prozesses sowie für die Schulung und das Training der Prozessteilnehmer verantwortlich.

Notfallmanager / BC-Manager

Definiert den Rahmen der BIA und macht die Vorgaben für den Notfallkoordinator. Er steht beratend bei der Durchführung der BIA zu Verfügung. Alle BIA Ergebnisse werden vom Notfallmanager/BC-Manager geprüft und freigegeben.

Notfallkoordinator

Ist verantwortlich für die Durchführung der BIA und Erstellung des BCP in seinem Geschäftsbereich.

Fachbereiche

Sind Wissensträger, da sie die Abläufe in ihren Prozessen kennen. Sie verfügen über die Informationen zu den Ressourcen, welche für die Abläufe im Prozess notwendig sind.

Bereichsleiter

Stellt sicher, dass die vorgegebenen Ziele erreicht werden. Koordiniert und verantwortet die Vorgaben.

4.2 BIA Konzeption

4.2.1 Prozessgegenstand

In der BIA werden die Hauptprozesse betrachtet. Ein Hauptprozess ist eine Zusammenfassung aller darunterliegenden Teilprozesse mit gleicher Zielsetzung und gleichem Ressourcenbedarf.

³ Aus Gründen der besseren Lesbarkeit wird in diesem Dokument die Sprachform des generischen Maskulinums angewendet. Diese Formulierung ist ausdrücklich geschlechtsunabhängig zu verstehen.

4.2.2 Festlegung der Schadensszenarien

Der Ausfall eines Geschäftsprozesses kann unterschiedliche Auswirkungen nach sich ziehen. Aus diesem Grund erfolgt die Bewertung einer ungeplanten Unterbrechung von Prozessen anhand von drei verschiedenen Schadensszenarien:

1. Wirtschaftlicher Schaden
2. Verstöße gegen Gesetze, Vorschriften und Verträge
3. Negative Innen- und Außenwirkungen (Reputationsverlust)

Der Ausfall eines Prozesses kann z.B. keine oder geringe wirtschaftliche Schäden verursachen, jedoch erhebliche Reputationsverluste - beispielsweise auf die Kunden - mit sich bringen. Für bestimmte Prozesse z.B. in der IT kann es hilfreich sein, noch eine vierte Kategorie zur Bewertung hinzuzunehmen: Auswirkungen auf abhängige Prozesse.

4.2.3 Auswirkungsklassen

Die Bewertung der Auswirkungen eines Prozessausfalls erfolgt anhand der drei Schadensszenarien. Folgende Beispiele können hierbei als Orientierung herangezogen werden:

Wirtschaftlicher Schaden	
Auswirkungsklasse	Beschreibung
1 - keine oder sehr gering	<ul style="list-style-type: none"> • Der mögliche finanzielle Schaden ist sehr gering (z.B. unter XXX Euro). • Die Abläufe im Unternehmen werden nicht nennenswert beeinträchtigt.
2 - gering	<ul style="list-style-type: none"> • Der finanzielle Schaden bleibt gering (z.B. zwischen XXX und XXX Euro). • Bereiche, Kunden oder Geschäftspartner werden nur unwesentlich beeinträchtigt, die Beeinträchtigung wird von den Betroffenen toleriert.
3 - erheblich	<ul style="list-style-type: none"> • Der Vorfall verursacht erheblich finanzielle Schäden (z.B. zwischen XXX und XXX Euro). • Der Vorfall hat erhebliche Auswirkungen auf den Arbeitsablauf von Bereichen, Kunden oder Geschäftspartnern und wird als nicht tolerabel eingeschätzt.
4 - hoch	<ul style="list-style-type: none"> • Der Vorfall verursacht hohe finanzielle Schäden (z.B. über XXX Euro). • Der Vorfall hat gravierende Auswirkungen auf den Arbeitsablauf von Bereichen, Kunden oder Geschäftspartnern und wird auch von den nicht betroffenen Bereichen, Kunden und

	Geschäftspartnern als nicht tolerabel eingeschätzt.
Verstöße gegen Gesetze, Vorschriften und Verträge	
Auswirkungsklasse	Beschreibung
1 - keine oder sehr gering	<ul style="list-style-type: none"> • Es drohen nur sehr geringe Konsequenzen oder Konventionalstrafen (z.B. Buß- oder Zwangsgeldzahlungen bis maximal XXX Euro).
2 - gering	<ul style="list-style-type: none"> • Verstöße mit geringfügigen Konsequenzen oder Konventionalstrafen (z.B. Buß- oder Zwangsgeldzahlungen zwischen XXX und XXX Euro). • Verstöße werden außerhalb des Unternehmens nicht bemerkt und müssen nicht nach außen gemeldet werden.
3 - erheblich	<ul style="list-style-type: none"> • Verstöße mit erheblichen Konsequenzen, diese werden auch außerhalb des Unternehmens bemerkt. • Konventionalstrafen sind abzusehen oder bereits fällig (z.B. Buß- oder Zwangsgeldzahlungen zwischen XXX und XXX Euro).
4 - hoch	<ul style="list-style-type: none"> • Verstöße mit gravierenden Konsequenzen oder Haftungsansprüchen (z.B. Buß- oder Zwangsgeldzahlungen über XXX Euro). • Verstöße müssen an externe Stellen gemeldet werden.
Negative Innen- und Außenwirkungen (Reputationsverlust)	
Auswirkungsklasse	Beschreibung
1 - keine oder sehr gering	<ul style="list-style-type: none"> • Verwunderung: Keine oder nur sehr geringe Änderung der Wahrnehmung der Stakeholder • Vertrauen ist maximal kurzfristig in Frage gestellt • Ursprüngliches Vertrauensniveau lässt sich leicht wieder herstellen
2 - gering	<ul style="list-style-type: none"> • Enttäuschung/Besorgnis: Vertrauens-/Reputationsniveau ist reduziert • Ursprüngliches Vertrauen lässt sich jedoch mit Aufwänden/Kosten und Zeit wiederherstellen
3 - erheblich	<ul style="list-style-type: none"> • Verärgerung: Vertrauens-/Reputationsniveau ist sehr stark reduziert • Ursprüngliches Vertrauen ist sehr schwer bis gar nicht wieder herstellbar
4 - hoch	<ul style="list-style-type: none"> • Entrüstung/Empörung: Reputationsschaden ist

	<p>eingetreten</p> <ul style="list-style-type: none"> • Maximale Konsequenzen werden gezogen • Interaktion mit dem Unternehmen wird beendet • Langfristig keine Erwartungen mehr an das Unternehmen
--	--

4.2.4 Zeithorizonte

Die aus einem Prozessausfall resultierenden Schäden können im Zeitverlauf linear oder sogar exponentiell ansteigen. Folgende Zeithorizonte werden z.B. bei einem Prozessausfall im Rahmen der BIA einzeln betrachtet:

- < 4h A (kleiner 4 Stunden / bezogen auf die Betriebszeit, +1 Stunde WRT)
- < 1d B (kleiner 1 Kalendertag inkl. 1 Stunde WRT)
- < 2d C (kleiner 2 Kalendertage inkl. 1 Stunde WRT)
- < 5d D (kleiner 5 Kalendertage inkl. 1 Stunde WRT)
- < 10d E (kleiner 10 Kalendertage inkl. 1 Stunde WRT)
- < 30d F (kleiner 30 Kalendertage inkl. 1 Stunde WRT)

Die unterschiedlichen Zeithorizonte beschreiben Zeiten, in denen ein Prozess oder eine Ressource wieder zu Verfügung stehen muss. Zur Unterscheidung der Zeithorizonte als Verfügbarkeitsangabe können Abkürzungen verwendet werden. In diesem Fall stellt der Buchstabe A die kürzeste Zeitspanne zur Anforderung an die Wiederverfügbarkeit dar und der Buchstabe F die längste Zeitspanne. Die angegebenen Zeithorizonte stellen Best Practices dar, können jedoch beliebig weiter unterteilt oder zusammengefasst werden.

4.2.5 Risikoappetit

Der Risikoappetit eines Unternehmens wird über das individuelle Festlegen der Schwellenwerte für die Auswirkungsklassen berücksichtigt, bezogen auf die Kategorien wirtschaftlicher Schaden, Verstöße gegen Gesetze, Vorschriften und Verträge sowie Reputationsverlust (siehe auch Kap. 3.1 und Kap. 4.2.3). Auswirkungen die das Unternehmen in besonderer Weise nicht tolerieren möchte, können durch eine Gewichtung in den Auswirkungsklassen berücksichtigt werden.

4.2.6 Ressourcen

Für die Durchführung eines Notbetriebs ist die Verfügbarkeit von Ressourcen – wenn auch reduziert in Umfang und Kapazität – unabdingbar. Die Informationen über benötigte Ressourcen werden zum einen zur Erstellung von Anforderungskatalogen an die unterstützenden Einheiten genutzt, die für die Absicherung der Verfügbarkeit bzw. für die Bereitstellung dieser Ressourcen im Notfall verantwortlich sind.

Zum anderen werden die Informationen zur Entwicklung von Geschäftsfortführungsplänen (Business Continuity Plans - BCP) verwendet. Im Folgenden werden die in der BIA zu berücksichtigenden Ressourcen festgelegt und anhand von Beispielangaben näher erläutert.

Ressourcenkategorie	Beschreibung und Beispielangaben
Personal / Notfallbelegschaft	Zur Durchführung von Geschäftsprozessen werden Mitarbeiter benötigt, die Entscheidungen treffen, Aufgaben ausführen und eventuell über spezielle Qualifikationen verfügen. Diese Mitarbeiter werden qualifikationsbasiert angegeben (z.B. Sachbearbeiter, Bereichsleiter, SAP-Administrator). Bei der Bewertung des Personalbedarfs ist zwischen der Anzahl im Normalbetrieb und dem Mindestbedarf für den Notbetrieb (eingeschränkte Aufgabenerfüllung) zu unterscheiden. Da der Personalbedarf abhängig von der Dauer eines Notfalls variieren kann, ist dieser über die Zeithorizonte hinweg einzuschätzen. Es müssen Workarounds für den Notbetrieb (z.B. kann auf Mitarbeiter aus anderen Bereichen oder auf externe Mitarbeiter zugegriffen werden) angegeben werden.
Gebäude	Es wird das Gebäude abgefragt, in dem der Geschäftsprozess im Normalbetrieb abläuft. Somit kann bei einem Gebäudeausfall sofort benannt werden, welche Prozesse von dem Ausfall betroffen sind. Es ist anzugeben, wann in einem Notfall das Gebäude für die Fortsetzung des Prozesses benötigt wird (RTO des Gebäudes). Zudem sind Workarounds für den Notbetrieb (z.B. Notfallarbeitsplätze) anzugeben.
IT-Assets	Es sind die zur Aufrechterhaltung des Geschäftsprozesses benötigten IT-Assets dem Prozess zuzuordnen. Es ist anzugeben, wann in einem Notfall das jeweilige IT-Asset für die Fortsetzung des Prozesses zwingend benötigt wird (RTO des IT-Assets). Zudem ist der maximal tolerierbare Datenverlust für das IT-Asset anzugeben (RPO). Es sind mögliche Workarounds (z.B. alternative IT-Assets oder manuelle Prozesse) anzugeben.
Information Assets / Dokumente	Hier sind für den Prozess benötigte physische Dokumente (z.B. Verträge, Akten, Dokumente, Belege) anzugeben. Zudem wird abgefragt, wann in einem Notfall das jeweilige Dokument für die Fortsetzung des Prozesses zwingend benötigt wird (RTO des Dokuments) und ob es einen Workaround (z.B. eine Wiederbeschaffung) gibt. Zusätzlich sind der Lagerort sowie die Beurteilung der Wiederherstellbarkeit der Dokumente zu erfassen.
Vertragsbeziehungen / Dienstleistungen	Vertragsbeziehungen / Dienstleistungen, die zur Aufrechterhaltung eines Prozesses benötigt werden, sind pro Geschäftsprozess zu erfassen. Es ist anzugeben, wann in einem Notfall die Dienstleistung zwingend wieder benötigt wird (RTO der Dienstleistung) und welche alternativen Workarounds es gibt. Zudem kann der Grad der Abhängigkeit aufgenommen werden (unbedingt benötigter Dienstleister oder

	ist die Leistung ersetzbar durch andere Dienstleister oder den Prozess selbst).
Nachgelagerte Prozesse (Schnittstellen)	Wenn eine für den Notbetrieb relevante Schnittstelle zu einem anderen Hauptprozess besteht, ist diese zu dokumentieren. Die Schnittstelle ist entsprechend zu beschreiben und mit dem Folgeprozess abzustimmen. Die Abstimmung erfolgt zwischen den Koordinatoren der betroffenen Bereiche. Die Notfallplanung des vor- bzw. nachgelagerten Bereiches ist entsprechend auf die Schnittstellen anzupassen. Es sind mögliche Workarounds für einen Ausfall der Schnittstelle zu benennen. Es ist anzugeben, wann in einem Notfall die Schnittstelle zur Verfügung stehen muss (RTO der Schnittstelle). Die RTO der Schnittstelle sollte mit der MTPD des Prozesses übereinstimmen. Begründete Ausnahmen sind zu dokumentieren.
Zusätzliche Informationen	Wird Arbeitsplatzausstattung benötigt, die über den Standard hinausgeht, sind diese Komponenten mit anzugeben. Zudem sind alle eventuell benötigten weiteren Ressourcen, wie spezielle Schlüssel oder Freigabestempel, anzugeben.

Für die Erfassung der benötigten Mitarbeiter je Geschäftsprozess werden zwei Varianten vorgestellt:

Variante 1

Die Anzahl der Mitarbeiter im Normalbetrieb und im Notbetrieb werden während des BIA Gesprächs erhoben.

Rollen	Anzahl im Normalbetrieb	Anzahl im Notbetrieb					
		<4h	<1d	<2d	<5d	<10d	<30d
Gruppenleiter	1	0	0	0	1	1	1
Datenerfasser	3	0	0	1	2	3	3
Datenfreigabe	5	0	0	1	3	3	5

Variante 2

Die benötigte Anzahl der Mitarbeiter im Notbetrieb kann auch im Rahmen der Notfallkonzeption erhoben werden.

4.3 Ablauf der Business Impact Analyse

Für die Konzeption, zentrale Vorbereitung und Initiierung sowie für die Nachbereitung und Koordination ist der zentrale BC-Manager verantwortlich. Für die Durchführung der BIA sind die jeweiligen Organisationseinheiten (Bereichsleiter und dezentrale BC-Koordinatoren) verantwortlich. In den folgenden Kapiteln werden die Schritte zur Erhebung und Nachbereitung beschrieben.

4.3.1 Vorbereitung und Erhebung der BIA

4.3.1.1 Vorbereitung und Initiierung

Der Prozess zur Durchführung einer BIA kann durch verschiedene Ereignisse ausgelöst werden. Diese Ereignisse sind:

- Jährliche Aktualisierung: Die BIA ist zur kontinuierlichen Weiterentwicklung und Anpassung der Maßnahmen und Pläne jährlich durchzuführen.
- Anlassbezogene Aktualisierung: Bei signifikanten Veränderungen des Geschäftsbetriebs ist die BIA partiell oder ganzheitlich zu aktualisieren.

Im Rahmen der Initiierung sind Termine mit den beteiligten Personen abzustimmen, Schulungsbedarfe der durchführenden Personen zu ermitteln und ggf. Hilfsmittel zur Durchführung vorzubereiten.

4.3.1.2 Bewertung der Geschäftsprozesse

Zur Ermittlung der zeitkritischen Geschäftsprozesse sind im Rahmen der BIA ausnahmslos alle Hauptprozesse zu analysieren und zu bewerten. Pro Schadensszenario wird die erwartete Auswirkung für jeden Zeithorizont bewertet. Der Ausfallzeitpunkt ist als Worst-Case-Szenario innerhalb des Geschäftsbetriebs bzw. der Kernarbeitszeit anzunehmen. Für die Bewertung ist der Ausfall des Geschäftsprozesses anzunehmen und die erwartete Auswirkung je Zeithorizont einzuschätzen. Auf mögliche Ausfallgründe wird innerhalb einer Risikoanalyse separat eingegangen, eine Analyse der Eintrittswahrscheinlichkeiten eines Prozessausfalls ist somit nicht Bestandteil der BIA.

Anmerkung: Die BIA zielt darauf ab, die zeitkritischen Geschäftsprozesse zu erheben. Diese Bewertung ist nicht mit der Bedeutung bzw. Wichtigkeit eines Geschäftsprozesses zu verwechseln bzw. gleichzusetzen. Ein Geschäftsprozess kann sehr wohl eine hohe Bedeutung für das Unternehmen haben, aber für das Notfallmanagement eine geringe Priorität im Notfall besitzen.

4.3.1.3 Bestimmung der Maximum Tolerable Period of Disruption (MTPD)

Zur Klassifizierung und Priorisierung der Geschäftsprozesse wird die Maximum Tolerable Period of Disruption (MTPD) ermittelt. Die MTPD ergibt sich aus den Bewertungen des erwarteten Schadens bei einem Prozessausfall und stellt den Zeitrahmen dar, in der der

Wiederanlauf erfolgen muss, um schwerwiegende Schäden zu vermeiden. Die MTPD zeigt auf, ab welchem Zeitpunkt die Auswirkungen eines Prozessausfalls nicht mehr toleriert werden können und entsprechende Ausweichprozeduren zu definieren sind. Die MTPD bezieht sich auf die Betriebszeit des Prozesses.

Die MTPD wird erreicht, wenn Auswirkungen in einem Zeitfenster als "erheblich" (3) eingestuft werden.

Anmerkung: Für eine initiale BIA bei einem nicht regulierten Unternehmen reicht es auch, die MTPD zu ermitteln. Bei regulierten Unternehmen müssen zudem die WAZ erhoben werden.

4.3.1.4 Single Points of Failure

Es wird abgefragt, ob für den Geschäftsprozess Single-Points-of-Failure bekannt sind, d.h. einzelne Fehlerquellen, die einen sofortigen Ausfall des Geschäftsprozesses verursachen können.

4.3.1.5 Erhebung der benötigten Ressourcen

Für jeden Geschäftsprozess sind das zur Aufrechterhaltung des Geschäftsbetriebs benötigte Personal sowie die benötigten Ressourcen (z.B. Infrastruktur, IT, Dienstleister) aufzunehmen.

Anforderungen an den Notbetrieb

Für die erhobenen Ressourcen werden Workarounds für den Notbetrieb definiert und festgelegt:

- Beim Personalausfall: Wie hoch muss der Personalausfall sein, so dass der Normalbetrieb nicht weiter aufrechterhalten werden kann und ein Notbetrieb aktiviert werden muss? Welche Workarounds können hier genutzt werden?
- Beim Ausfall einer Ressource: Welche Ideen bzw. bereichsspezifischen Strategien zur Arbeit im Notbetrieb sind möglich?

Rückführung in den Normalbetrieb

Um von einem Notbetrieb geordnet zurück in den Normalbetrieb zu kommen, sind Rückführprozeduren für die jeweiligen Ressourcen zu definieren. Hierbei ist zu berücksichtigen, dass im Notbetrieb nicht alle Tätigkeiten vollumfänglich durchgeführt wurden und somit ein möglicher Arbeitsrückstand abzuarbeiten ist.

4.3.1.6 Erhebung Schnittstellen zu anderen Prozessen

Liegen notfallrelevante Zulieferungen für nachgelagerte Prozesse vor, sind diese im Prozess zu hinterlegen. Hiermit wird sichergestellt, dass im Folgeschritt die Schnittstellen aufeinander abgestimmt werden können und auch im Notfall die benötigten Zulieferungen geleistet werden.

Es ist anzugeben, wann in einem Notfall die Schnittstelle zur Verfügung stehen muss (RTO der Schnittstelle).

4.3.1.7 Erfassung kritischer Termine und Ereignisse

Die Bewertung des erwarteten Schadens infolge eines Prozessausfalls kann zu bestimmten Terminen oder Ereignissen abweichen. Dies ist z.B. während des Jahresabschlusses, Quartalsendes, Monatsultimos oder zum Fälligkeitszeitpunkt zeitkritischer Bearbeitungen möglich.

Um eine zielgerichtete Notfallplanung durchzuführen, sind die Termine und Ereignisse zu erfassen, an denen ein Prozessausfall höhere Auswirkungen zur Folge hat.

Es ist eine MTPD zu den verschiedenen kritischen Terminen und Ereignissen anzugeben.

4.3.2 Nachbereitung BIA

4.3.2.1 Zentrale Qualitätsprüfung

Die im Rahmen der BIA erhobenen Informationen werden durch den zentralen Notfallmanager hinsichtlich der folgenden Punkte geprüft:

- **Vollständigkeit:** Sind alle Pflichtfelder vollständig ausgefüllt worden? Wurden bspw. die Auswirkungen des Prozessausfalls in allen Schadensszenarien und Zeithorizonten bewertet? Gibt es eine Übereinstimmung der dokumentierten Schnittstellen von vorgelagerten und nachgelagerten Prozessen?
- **Plausibilität:** Inwieweit sind die Bewertungen nachvollziehbar? Auch sind die Schadensverläufe auf eventuelle Fehlangaben hin zu überprüfen (z.B. absteigende Schadensverläufe, da der Schaden über den Zeitverlauf meist gleichbleibend oder zunehmen ist).
- **Konsistenz:** Sind Widersprüche in den angegebenen Informationen erkennbar und die Angaben im Vergleich zur Gesamtsicht konsistent?

Werden Unregelmäßigkeiten festgestellt, sind diese möglichst in Form von Einzelgesprächen mit den jeweiligen BC-Koordinatoren zu klären.

4.3.2.2 Ableitung der Verfügbarkeitsanforderungen an die Ressourcen

Um die benötigten Ressourcen im Notbetrieb in der benötigten Zeit (RTO) zur Verfügung stellen zu können, sind die aus der MTPD resultierenden Verfügbarkeitsanforderungen der Prozesse auf die benötigten Ressourcen zu übertragen. Bei den jeweiligen Ressourcen wird abgefragt, wann im Notbetrieb die Ressource wieder benötigt wird.

Die RTO kann ggfs. auch größer als die MTPD sein, wenn die Ressource innerhalb des Notbetriebs erst zu einem späteren Zeitpunkt benötigt wird. Beim Wiederanlauf eines IT-Assets sind Abhängigkeiten und die Wiederanlaufreihenfolge zu berücksichtigen.

4.3.2.3 Abstimmung mit den unterstützenden Einheiten / GAP Analyse

Quartalsweise wird eine Gap-Analyse bezogen auf die Anforderungen des BCM durchgeführt.

Die Gap-Analyse umfasst im Wesentlichen den Abgleich benötigter und verfügbarer Ressourcen und Notfallarbeitsplätze sowie – sofern zutreffend – die Abstimmung der zugesicherten vertraglichen Konditionen für zeitkritische externe Dienstleistungen.

Zudem werden Abweichungen identifiziert, die auf eine unterschiedliche Klassifizierung der Verfügbarkeitsanforderungen im Rahmen der BIA und der Schutzbedarfsfeststellung der IT-Assets zurückzuführen sind. Sofern in der BIA eine höhere Einstufung als in der Schutzbedarfsfeststellung vorgenommen wurde, ist nicht sichergestellt, dass die notwendigen Sicherheitsanforderungen zur Gewährleistung der Verfügbarkeit formuliert und auch im Notfall umgesetzt sind.

4.3.2.4 Erstellung und Freigabe der Ergebnisdokumente

Als abschließendes Ergebnisdokument wird ein BIA Bericht erstellt. Der BIA Bericht enthält mindestens die folgenden Inhalte:

- Management Summary
- Darstellung der Ergebnisse
- Zentrale Bewertung der Ergebnisse durch den BC-Manager und Ableitung von Handlungsempfehlungen

Der Vorstand/die Geschäftsführung sollten den BIA Bericht innerhalb von einem Monat freigeben.

4.4 Schnittstellen zu anderen Themenfeldern

Nachfolgende Schnittstellen sind bei der Konzeptionierung und teils bei der Durchführung der BIA mit einzubeziehen:

Schnittstelle	Beschreibung
ITSCM	Die RTO und RPO Werte der IT-Assets müssen in einer Gap-Analyse abgeglichen werden.
Outsourcing	Die Anforderungen aus der BIA müssen mit den Notfallplänen der Dienstleister übereinstimmen (siehe auch SLA in Kap. 4.7.2).
Risikomanagement	Entwicklung und Abstimmung der Methodik zur Bestimmung der Kritikalität von Prozessen. Informationen aus dem Risikomanagement können helfen, die Ergebnisse aus der BIA zu plausibilisieren. Das Gleiche gilt in die andere Richtung.
Recht	Entwicklung und Abstimmung der Methodik zur Bestimmung der Kritikalität von Prozessen.
Informationssicherheit	Abgleich der Angaben zur Verfügbarkeit aus der Schutzbedarfsanalyse mit den Angaben aus der BIA.

4.5 Kontinuierliche Verbesserung

Die kontinuierliche Verbesserung ist ein integraler Bestandteil eines jeden Managementsystems. Das Ziel ist es, den Reifegrad zu erhöhen, indem die Erkenntnisse aus der Durchführung der BIA sowie den Reviews der BIA-Berichte durch das Management eingearbeitet werden. Aus den identifizierten Verbesserungspotentialen werden konkrete Maßnahmen abgeleitet, welche wiederum mit Zuständigkeiten und Terminen hinterlegt werden. Verbesserungen fließen in die zukünftigen BIA-Durchführungszyklen ein.

4.6 Abkürzungen, Begriffe und Definitionen

4.6.1 Abkürzungen

BCP	Business Continuity Plan
BIA	Business Impact Analyse
DRP	Disaster Recovery Plan
MBCO	Minimum Business Continuity Objective
MTPD/MTD	Maximum Tolerable Period of Disruption
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
SPoF	Single Points of Failure
SPoK	Single Point of Knowledge
WAZ	Wiederanlaufzeit
WRT	Work Recovery Time
ITSCM	Information Technology Service Continuity Management

4.6.2 Begriffe und Definitionen

BIA

Die BIA wird in der Regel einmal im Jahr durchgeführt. Sie identifiziert, quantifiziert und beschreibt die Auswirkung eines Ausfalls von Ressourcen auf die Geschäftsprozesse. Ein wesentliches Ergebnis der BIA ist eine Übersicht über die kritischen Geschäftsprozesse und die benötigten Ressourcen (siehe auch Kap. 3.1)

Aufgaben der Business Impact Analyse:

- Darstellung der Prioritäten der Prozesse im Unternehmen
- Bewertung von Auswirkungen bei einem Ausfall von Ressourcen in der Prozesskette
- Darstellung der Zeit zur Wiederherstellung der Prozesse bei dem Ausfall von Ressourcen

RTO

Ist die Zeitspanne innerhalb welcher die jeweiligen Services, Prozesse, IT-Services und Bereiche zur Durchführung der entsprechenden Geschäftsprozesse in einem Mindestmaß an Funktionalität und Leistungsstärke wieder zur Verfügung stehen müssen.

RPO

Ist der Zeitpunkt, an dem die letzte Datensicherung stattgefunden hat. Dieser stellt somit den maximal tolerierbaren Datenverlust dar.

MTPoD / MTPD

Stellt die maximal tolerierbare Ausfallzeit für die kritischen Geschäftsprozesse in einem Unternehmen dar. Ist der Zeitraum nach einer Störung, indem der Prozess wieder aufgenommen werden muss, um den Fortbestand des Unternehmens sichern zu können. Der RTO plus Puffer ergibt den MTPD.

MBCO

Ist das vorher definierte Minimum, auf dem die Dienstleistungen oder die Produkte im Notfall zur Verfügung gestellt werden.

WRT

Ist der Zeitpuffer, der nach dem Wiederanlauf der Ressourcen für den Prozess-Wiederanlauf benötigt wird. Zum Beispiel für die Abstimmungen mit dem Personal oder zur Überprüfung der Integrität von wiederhergestellten Daten.

WAZ

Gibt den Zeitraum an, innerhalb welchem der Notbetrieb für die Ressourcen nach Auftreten einer Unterbrechung wieder aufgenommen werden sollte.

SPoF

Kann alle Arten von Ressourcen betreffen. Beispiele sind: Spezielle Know-how-Träger, Entscheidungs- und Freigabeverantwortlichkeiten, bestimmte Log-In oder Freigabegeräte (USB-Keys, Schlüssel), Spezielle Druck- und Archivierungskomponenten.

SPoK

Ist eine Person innerhalb eines Unternehmens, welche ein Wissensmonopol besitzt. Wenn diese Person das Unternehmen verlassen würde oder ausfallen würde könnten Prozesse nur noch schwer oder gar nicht mehr laufen.

SLA

Ein SLA ist ein Vertrag zwischen einem Service-Provider und einem Kunden. Das SLA des Service-Providers muss die eigene Verfügbarkeitsanforderung erfüllen können. Die Verfügbarkeitsanforderung ergibt sich aus der BIA.

DRP / BCP

Nach der Prüfung des BIA-Reports, wird ein DRP/BCP aufgesetzt. Dieser Plan beschreibt, wie ein Unternehmen mit einem möglichen Notfall umzugehen hat. Er ermöglicht eine schnelle Fortführung der kritischen Geschäftsprozesse in einem Unternehmen mit dem Ziel, schädliche Auswirkungen zu minimieren.

Worst Case

Der Worst Case beschreibt den schlechtesten bzw. ungünstigsten Fall, der eintreten könnte. Bspw. kann man sich die Frage stellen, zu welchem Zeitpunkt in einem Jahr es die stärksten Auswirkungen hätte, wenn ein Bereich oder eine Tätigkeit ausfallen würde.

Geschäftsprozess

Besteht aus einer Folge von Einzelaktivitäten, mit denen die Geschäftsziele erreicht werden sollen.

Prozesskette/Abhängigkeiten

Eine Reihe von mehreren abhängigen Geschäftsprozessen.

5. Anhang Hilfsmittel Business Impact Analyse (BIA)

5.1 Projektplan zur Einführung und Umsetzung BIA

5.2 Template zur Durchführung der BIA