Contents

Chapter 1

Business Continuity Management Handbuch

Dokument-Metadaten

- **Erstellt am:** 2026-02-05
- **Autor:** Andreas Huemmer [andreas.huemmer@adminsend.de]
- **Version:** 0.0.2
- **Typ:** BCM-Handbuch

---

ewpage

Chapter 2

Zweck und Geltungsbereich

Dokument-ID: BCM-0010
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

2.1 1. Zweck

Das Business Continuity Management System (BCMS) der AdminSend GmbH dient folgenden Zwecken:

- **Schutz kritischer Geschäftsprozesse:** Sicherstellung der Fortführung geschäftskritischer Aktivitäten auch bei schwerwiegenden Störungen
- **Reduktion von Ausfallzeiten:** Minimierung der Auswirkungen von Unterbrechungen auf Geschäftsbetrieb, Kunden und Stakeholder
- **Erfüllung regulatorischer Anforderungen:** Nachweis der Compliance mit gesetzlichen und vertraglichen Verpflichtungen
- **Krisenreaktionsfähigkeit:** Etablierung strukturierter Prozesse zur Bewältigung von Notfällen und Krisen
- **Kontinuierliche Verbesserung:** Systematische Weiterentwicklung der Business Continuity-Fähigkeiten

2.1.1 1.1 Strategische Ziele

Das BCMS verfolgt folgende strategische Ziele:

- Definierte **Recovery Time Objectives (RTO)** und **Recovery Point Objectives (RPO)** für alle kritischen Prozesse
- Aufbau und Aufrechterhaltung der **Krisenreaktionsfähigkeit** auf allen Organisationsebenen

- **Nachweisbarkeit** der Business Continuity-Maßnahmen gegenüber Aufsichtsbehörden, Kunden und Partnern
- **Schutz der Reputation** und des Vertrauens der Stakeholder
- **Minimierung finanzieller Verluste** durch Geschäftsunterbrechungen

2.1.2 1.2 Referenzen zu Standards

Dieses BCMS orientiert sich an folgenden Standards und Best Practices:

- **ISO 22301:2019** - Security and resilience — Business continuity management systems — Requirements
- **ISO 22313:2020** - Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
- **BSI-Standard 100-4** - Notfallmanagement
- **BSI-Standard 200-4** - Business Continuity Management

2.2 2. Geltungsbereich

2.2.1 2.1 Organisationseinheiten

Das BCMS gilt für folgende Organisationseinheiten der AdminSend GmbH:

[TODO: Definieren Sie die eingeschlossenen Organisationseinheiten]

Beispiel: - Geschäftsführung - IT-Abteilung - Produktion - Vertrieb und Marketing - Finanzen und Controlling - Personalwesen

2.2.2 2.2 Standorte

Das BCMS umfasst folgende Standorte:

[TODO: Listen Sie alle Standorte auf, die im Geltungsbereich liegen]

Beispiel: - Hauptsitz: Musterstraße 123, 80331 München - Produktionsstandort: [Adresse] - Rechenzentrum: [Adresse] - Ausweichstandort: [Adresse]

2.2.3 2.3 Services und Prozesse

Das BCMS deckt folgende kritischen Services und Geschäftsprozesse ab:

[TODO: Definieren Sie die kritischen Services und Prozesse]

Beispiel: - Kundenservice und Support - Produktionssteuerung - Auftragsabwicklung - Finanzprozesse (Zahlungsverkehr, Buchhaltung) - IT-Services (E-Mail, ERP-System, Produktionssysteme)

2.2.4 2.4 IT- und OT-Systeme

Das BCMS umfasst folgende IT- und OT-Systeme:

[TODO: Listen Sie kritische IT- und OT-Systeme auf]

Beispiel: - ERP-System - CRM-System - E-Mail und Collaboration-Plattform - Produktionssteuerungssysteme (SCADA, MES) - Netzwerkinfrastruktur - Backup- und Recovery-Systeme

2.2.5 2.5 Ausnahmen und Ausschlüsse

Folgende Bereiche sind explizit vom Geltungsbereich ausgeschlossen:

[TODO: Dokumentieren Sie Ausnahmen mit Begründung und genehmigender Instanz]

Beispiel: - **Tochtergesellschaft XY:** Betreibt eigenes BCMS (Genehmigt durch: {{ meta.roles.ceo.name }}) - **Entwicklungsumgebungen:** Nicht geschäftskritisch (Genehmigt durch: {{ meta.roles.cio.name }})

2.3 3. Annahmen und Einschränkungen

2.3.1 3.1 Grundannahmen

Das BCMS basiert auf folgenden Annahmen:

[TODO: Definieren Sie die Grundannahmen für Ihr BCMS]

Beispiel: - Maximaler Personalausfall: Bis zu 30% der Belegschaft gleichzeitig nicht verfügbar - Wiederherstellung kritischer IT-Systeme: Innerhalb von 24 Stunden möglich - Verfügbarkeit von Ausweichstandorten: Innerhalb von 4 Stunden erreichbar - Lieferketten: Kritische Lieferanten haben eigene BCM-Maßnahmen implementiert - Externe Unterstützung: Notfalldienste (Feuerwehr, Polizei) sind verfügbar

2.3.2 3.2 Abhängigkeiten außerhalb der Kontrolle

Folgende Abhängigkeiten liegen außerhalb der direkten Kontrolle der Organisation:

[TODO: Identifizieren Sie externe Abhängigkeiten]

Beispiel: - Verfügbarkeit öffentlicher Infrastruktur (Strom, Wasser, Telekommunikation) - Verfügbarkeit von Cloud-Service-Providern - Lieferfähigkeit kritischer Zulieferer - Verfügbarkeit von Notfalldiensten - Politische und regulatorische Rahmenbedingungen

2.4 4. Schnittstellen zu anderen Managementsystemen

2.4.1 4.1 Informationssicherheits-Managementsystem (ISMS)

Verantwortlich: {{ meta.roles.ciso.name }} ({{ meta.roles.ciso.email }})

Schnittstellen: - Incident Management und Security Incident Response - IT-Notfallpläne und Disaster Recovery - Risikomanagement und Risikoanalyse - Zugriffskontrolle und Notfallzugänge (Break-Glass)

[TODO: Beschreiben Sie die konkreten Schnittstellen zu Ihrem ISMS]

2.4.2 4.2 IT-Service-Management (ITSM)

Verantwortlich: {{ meta.roles.it_operations_manager.name }} ({{ meta.roles.it_operations_manager.email }})

Schnittstellen: - Incident Management (Major Incidents → BCM-Aktivierung) - Change Management (Emergency Changes) - Problem Management (Post-Incident-Reviews) - Service Level Management (SLA-Definitionen)

[TODO: Beschreiben Sie die konkreten Schnittstellen zu Ihrem ITSM]

2.4.3 4.3 Datenschutz und Compliance

Verantwortlich: [TODO: Datenschutzbeauftragter]

Schnittstellen: - Datenschutz-Folgenabschätzungen (DPIA) für BCM-Maßnahmen - Meldepflichten bei Datenschutzvorfällen - Aufbewahrungsfristen für BCM-Dokumentation - Compliance-Nachweise für Aufsichtsbehörden

[TODO: Beschreiben Sie die konkreten Schnittstellen zum Datenschutz]

2.4.4 4.4 Risikomanagement

Verantwortlich: [TODO: Risikomanager]

Schnittstellen: - Unternehmensweites Risikomanagement - Business Impact Analysis (BIA) - Risikoanalyse und Risikobewertung - Risikominderungsmaßnahmen

[TODO: Beschreiben Sie die konkreten Schnittstellen zum Risikomanagement]

2.4.5 4.5 Krisenkommunikation und Public Relations

Verantwortlich: [TODO: Kommunikationsverantwortlicher]

Schnittstellen: - Interne Krisenkommunikation - Externe Krisenkommunikation (Medien, Kunden, Partner) - Stakeholder-Management - Reputationsschutz

[TODO: Beschreiben Sie die konkreten Schnittstellen zur Krisenkommunikation]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 3

BCM-Leitlinie / BCM-Policy

Dokument-ID: BCM-0020
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

3.1 1. Leitlinie (Policy Statement)

Die Geschäftsführung der AdminSend GmbH verpflichtet sich zur Implementierung und kontinuierlichen Verbesserung eines Business Continuity Management Systems (BCMS) gemäß **ISO 22301:2019**.

3.1.1 1.1 Management-Commitment

Die Geschäftsführung, vertreten durch **{{ meta.roles.ceo.name }}** (CEO), erklärt hiermit:

- **Höchste Priorität:** Business Continuity hat strategische Bedeutung für den Schutz unserer Organisation, unserer Mitarbeiter, Kunden und Stakeholder
- **Ressourcenbereitstellung:** Angemessene finanzielle, personelle und technische Ressourcen werden für das BCMS bereitgestellt
- **Führungsverantwortung:** Die Geschäftsführung übernimmt die Gesamtverantwortung für das BCMS und dessen Wirksamkeit
- **Kontinuierliche Verbesserung:** Das BCMS wird regelmäßig überprüft und kontinuierlich verbessert

3.1.2 1.2 Grundsätze des BCMS

Das BCMS der AdminSend GmbH basiert auf folgenden Grundsätzen:

1. **Risikobasierter Ansatz:** Identifikation, Bewertung und Behandlung von Risiken für die Geschäftskontinuität
2. **Kontinuierliche Verbesserung:** Systematische Weiterentwicklung der BCM-Fähigkeiten durch Übungen, Tests und Lessons Learned
3. **Verantwortlichkeit:** Klare Zuweisung von Rollen und Verantwortlichkeiten auf allen Organisationsebenen
4. **Übung und Test:** Regelmäßige Übungen und Tests zur Validierung der BCM-Maßnahmen
5. **Dokumentation und Nachweisbarkeit:** Vollständige Dokumentation aller BCM-Aktivitäten und -Entscheidungen
6. **Compliance:** Einhaltung aller relevanten gesetzlichen, regulatorischen und vertraglichen Anforderungen

3.1.3 1.3 Verpflichtungen

Die AdminSend GmbH verpflichtet sich zu:

- **Schutz von Menschenleben:** Sicherheit und Wohlergehen von Mitarbeitern, Kunden und Besuchern haben oberste Priorität
- **Geschäftskontinuität:** Aufrechterhaltung kritischer Geschäftsprozesse auch bei schwerwiegenden Störungen
- **Stakeholder-Kommunikation:** Transparente und zeitnahe Kommunikation mit allen betroffenen Stakeholdern
- **Lieferantenmanagement:** Sicherstellung der Business Continuity-Fähigkeiten kritischer Lieferanten
- **Compliance und Nachweisführung:** Erfüllung aller relevanten Anforderungen und Bereitstellung von Nachweisen

3.2 2. Ziele und Grundprinzipien

3.2.1 2.1 Strategische BCM-Ziele

Die AdminSend GmbH verfolgt folgende strategische BCM-Ziele:

Ziel 1: Minimierung von Ausfallzeiten - Wiederherstellung kritischer Geschäftsprozesse innerhalb definierter Recovery Time Objectives (RTO) - Begrenzung von Datenverlusten innerhalb definierter Recovery Point Objectives (RPO) - Messbare Reduktion der durchschnittlichen Wiederherstellungszeit um [TODO: X%] pro Jahr

Ziel 2: Krisenreaktionsfähigkeit - Etablierung einer 24/7-Krisenorganisation mit klaren Eskalationswegen - Schulung aller Mitarbeiter in BCM-Grundlagen und Notfallverhalten - Durchführung von mindestens [TODO: X] BCM-Übungen pro Jahr

Ziel 3: Compliance und Nachweisbarkeit - Erfüllung aller regulatorischen Anforderungen an Business Continuity - Bereitstellung vollständiger Nachweise für Audits und Zertifizierungen - Aufrechterhaltung der ISO 22301-Zertifizierung (falls angestrebt)

Ziel 4: Stakeholder-Vertrauen - Transparente Kommunikation der BCM-Fähigkeiten gegenüber Kunden und Partnern - Nachweis der Business Continuity-Fähigkeiten in Ausschreibungen und Verträgen - Schutz der Reputation und des Markenwertes

Ziel 5: Kontinuierliche Verbesserung - Systematische Auswertung von Übungen, Tests und

realen Vorfällen - Implementierung von Lessons Learned und Best Practices - Regelmäßige Aktualisierung der BCM-Dokumentation und -Pläne

3.2.2 2.2 Operative Grundprinzipien

Prinzip 1: Safety First - Menschenleben und Gesundheit haben immer Vorrang vor materiellen Werten - Im Notfall gilt: Erst Personen in Sicherheit bringen, dann Sachschäden minimieren

Prinzip 2: Kommunikation vor Aktion - Strukturierte Kommunikation und Koordination vor unabgestimmten Einzelaktionen - Klare Befehlsketten und Eskalationswege in der Krise

Prinzip 3: Dokumentation und Nachvollziehbarkeit - Alle Entscheidungen und Maßnahmen werden dokumentiert - Nachvollziehbarkeit für Post-Incident-Reviews und Audits

Prinzip 4: Flexibilität und Anpassungsfähigkeit - BCM-Pläne sind Leitlinien, keine starren Vorgaben - Situationsgerechte Anpassung der Maßnahmen ist erlaubt und erwünscht

3.3 3. Geltungsbereich

Der Geltungsbereich des BCMS ist definiert in:

→ **Siehe Dokument:** `0010_Zweck_und_Geltungsbereich.md`

Das BCMS umfasst alle kritischen Geschäftsprozesse, IT-Systeme und Standorte der AdminSend GmbH gemäß der im Scope-Dokument definierten Abgrenzung.

3.4 4. Governance und Verantwortlichkeiten

3.4.1 4.1 RACI-Matrix BCM-Governance

Aktivität	CEO	CIO	CISO	BCM-Manager	Fachbereich	IT-Ops
BCM-Policy genehmigen	**A**	C	C	R	I	I
BCM-Strategie festlegen	**A**	R	C	R	C	I
BCM-Budget freigeben	**A**	C	I	R	I	I
BIA durchführen	I	C	I	**A**	R	C
BCM-Pläne erstellen	I	C	C	**A**	R	R
BCM-Übungen durchführen	I	C	C	**A**	R	R
Krise aktivieren	**A**	R	R	R	I	I
Management Review	**A**	R	C	R	I	I

Legende: - **R** = Responsible (Durchführungsverantwortung) - **A** = Accountable (Gesamtverantwortung, Entscheidungsbefugnis) - **C** = Consulted (Konsultiert, Fachexpertise) - **I** = Informed (Informiert)

3.4.2 4.2 Rollen und Verantwortlichkeiten

Geschäftsführung (CEO) - **Verantwortlich:** {{ meta.roles.ceo.name }} ({{ meta.roles.ceo.email }}) - **Aufgaben:** Gesamtverantwortung für BCMS, Genehmigung der BCM-Policy, Freigabe von Ressourcen, Krisenaktivierung

Chief Information Officer (CIO) - **Verantwortlich:** {{ meta.roles.cio.name }} ({{ meta.roles.cio.email }}) - **Aufgaben:** Verantwortung für IT-Continuity, IT-Disaster-Recovery, technische BCM-Maßnahmen

Chief Information Security Officer (CISO) - **Verantwortlich:** {{ meta.roles.ciso.name }} ({{ meta.roles.ciso.email }}) - **Aufgaben:** Schnittstelle ISMS-BCMS, Security-Incident-Response, Cyber-Resilience

BCM-Manager - **Verantwortlich:** [TODO: BCM-Manager Name und Kontakt] - **Aufgaben:** Operative Leitung des BCMS, Koordination von BIA und Risikoanalyse, BCM-Übungen, Pflege der BCM-Dokumentation

Fachbereiche - **Verantwortlich:** Jeweilige Bereichsleiter - **Aufgaben:** Identifikation kritischer Prozesse, Mitwirkung bei BIA, Erstellung fachlicher BCM-Pläne, Teilnahme an Übungen

IT-Operations - **Verantwortlich:** {{ meta.roles.it_operations_manager.name }} ({{ meta.roles.it_operations_manager.email }}) - **Aufgaben:** Implementierung technischer BCM-Maßnahmen, IT-Disaster-Recovery, Backup und Restore

3.5 5. Freigaben und Genehmigungen

Diese BCM-Policy wurde geprüft und genehmigt durch:

Rolle	Name	Funktion	Datum	Unterschrift/Approval
Geschäftsführung	{{ meta.roles.ceo.name }}	CEO	[TODO: Datum]	[TODO: Unterschrift]
BCM-Owner	[TODO: BCM-Manager]	BCM-Manager	[TODO: Datum]	[TODO: Unterschrift]
IT-Leitung	{{ meta.roles.cio.name }}	CIO	[TODO: Datum]	[TODO: Unterschrift]
Informationssicherheit	{{ meta.roles.ciso.name }}	CISO	[TODO: Datum]	[TODO: Unterschrift]
Compliance	[TODO: Compliance-Verantwortlicher]	Compliance Officer	[TODO: Datum]	[TODO: Unterschrift]

3.6 6. Überprüfung und Aktualisierung

Diese BCM-Policy wird:

- **Jährlich** durch die Geschäftsführung im Rahmen des Management Reviews überprüft
- Bei **wesentlichen Änderungen** der Organisation, Geschäftsprozesse oder regulatorischen Anforderungen aktualisiert
- Nach **schwerwiegenden Vorfällen** oder Übungen auf Anpassungsbedarf geprüft

Nächste geplante Überprüfung: [TODO: Datum]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 4

Dokumentenlenkung und Versionierung

Dokument-ID: BCM-0030
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

4.1 1. Dokumentenlandkarte

4.1.1 1.1 BCM-Dokumentenstruktur

Die BCM-Dokumentation der AdminSend GmbH umfasst folgende Dokumententypen:

Strategische Dokumente: - BCM-Policy und Leitlinie - BCM-Strategie und Ziele - Geltungsbereich und Scope

Operative Dokumente: - Business Impact Analysis (BIA) - Risikoanalyse und Szenarien - Business Continuity Pläne (BCP) - IT Disaster Recovery Pläne (DRP) - Krisenmanagementpläne

Unterstützende Dokumente: - Kontaktlisten und Eskalationsmatrizen - Runbooks und Checklisten - Testprotokolle und Übungsberichte - Schulungsunterlagen

4.1.2 1.2 Dokumentenablage

Primäre Ablage: [TODO: Definieren Sie das primäre Dokumentenmanagementsystem]

Beispiel: - **System:** SharePoint / Confluence / Dokumentenmanagementsystem - **Pfad:** `BCM/Dokumentation/` - **Zugriff:** Rollenbasiert (RBAC) gemäß Berechtigungskonzept - **Backup:** Tägliche Sicherung, 30 Tage Aufbewahrung

Offline-Verfügbarkeit / Notfallzugriff:

Kritische BCM-Dokumente müssen auch bei Ausfall der IT-Systeme verfügbar sein:

[TODO: Definieren Sie Offline-Zugriffsmöglichkeiten]

Beispiel: - **Notfall-USB-Sticks:** Verschlüsselte USB-Sticks mit aktuellen BCM-Plänen bei Krisenstabsmitgliedern - **Papierausdrucke:** Versiegelte Notfallordner an definierten Standorten (Tresor, Ausweichstandort) - **Cloud-Backup:** Zugriff über mobile Geräte auch bei Ausfall des Hauptstandorts - **Aktualisierung:** Quartalsweise oder bei wesentlichen Änderungen

4.1.3 1.3 Dokumentenregister

Dokument-ID	Dokumentname	Version	Owner	Klassifizierung	Ablageort
BCM-0010	Zweck und Geltungsbereich	1.0.0	IT Operations Manager	internal	[TODO: Pfad]
BCM-0020	BCM-Leitlinie / Policy	1.0.0	IT Operations Manager	internal	[TODO: Pfad]
BCM-0030	Dokumentenlenkung	1.0.0	IT Operations Manager	internal	[TODO: Pfad]
…	…	…	…	…	…

[TODO: Vervollständigen Sie das Dokumentenregister]

4.2 2. Versionierung

4.2.1 2.1 Versionierungsschema

Die AdminSend GmbH verwendet folgendes Versionierungsschema für BCM-Dokumente:

Format: `MAJOR.MINOR.PATCH`

Beispiel: Version 2.3.1

- **MAJOR (2):** Wesentliche inhaltliche Änderungen, neue Struktur, neue Anforderungen
- **MINOR (3):** Ergänzungen, Aktualisierungen ohne grundlegende Änderungen
- **PATCH (1):** Korrekturen, Formatierungen, redaktionelle Änderungen

4.2.2 2.2 Versionserhöhung

MAJOR-Version erhöhen bei: - Grundlegender Neustrukturierung des Dokuments - Wesentlichen Änderungen der BCM-Strategie oder -Prozesse - Neuen regulatorischen Anforderungen - Änderungen des Geltungsbereichs

MINOR-Version erhöhen bei: - Ergänzung neuer Abschnitte oder Prozesse - Aktualisierung von Kontaktdaten oder Rollen - Anpassung an organisatorische Änderungen - Ergebnissen aus Übungen oder Tests

PATCH-Version erhöhen bei: - Rechtschreibkorrekturen - Formatierungsänderungen - Aktualisierung von Verweisen - Redaktionellen Anpassungen

4.2.3 2.3 Versionsstatus

Status	Beschreibung	Verwendung
Entwurf	Dokument in Erstellung	Nur für Autoren sichtbar
In Review	Dokument in Prüfung	Für Reviewer sichtbar
Freigegeben	Dokument genehmigt und aktiv	Für alle Berechtigten sichtbar
Archiviert	Dokument veraltet, historisch	Nur für Archivzwecke

4.3 3. Freigabe- und Review-Prozess

4.3.1 3.1 Rollen im Dokumentenprozess

Ersteller (Author): - **Verantwortlich:** Fachverantwortlicher oder BCM-Manager - **Aufgaben:** Erstellung und Pflege des Dokumenteninhalts

Reviewer (Prüfer): - **Verantwortlich:** Fachexperten, betroffene Stakeholder - **Aufgaben:** Inhaltliche Prüfung, Feedback, Freigabeempfehlung

Approver (Genehmiger): - **Verantwortlich:** CIO oder delegierte Führungskraft - **Aufgaben:** Formale Freigabe, Verantwortungsübernahme

4.3.2 3.2 Freigabeprozess

1. **Erstellung:** Autor erstellt Dokument im Status “Entwurf”
2. **Review:** Dokument wird an Reviewer zur Prüfung übergeben (Status: “In Review”)
3. **Überarbeitung:** Autor arbeitet Feedback ein
4. **Genehmigung:** Approver gibt Dokument frei (Status: “Freigegeben”)
5. **Veröffentlichung:** Dokument wird für Zielgruppe bereitgestellt
6. **Archivierung:** Alte Version wird archiviert

4.3.3 3.3 Review-Intervalle

Dokumenttyp	Review-Intervall	Verantwortlich
BCM-Policy	Jährlich	{{ meta.roles.ceo.name }}
BIA-Ergebnisse	Jährlich	BCM-Manager
BCM-Pläne (BCP/DRP)	Halbjährlich	Fachverantwortliche
Kontaktlisten	Quartalsweise	BCM-Manager
Runbooks	Nach jeder Übung	IT-Operations

Anlassbezogene Reviews: - Nach schwerwiegenden Vorfällen - Bei organisatorischen Änderungen - Bei Änderungen regulatorischer Anforderungen - Nach Audits oder Zertifizierungen

4.4 4. Verteiler und Zugriffsrechte

4.4.1 4.1 Zielgruppen

Krisenstab: - Zugriff auf alle BCM-Dokumente - Offline-Kopien der kritischen Pläne - Benachrichtigung bei Änderungen

IT-Operations: - Zugriff auf IT-DR-Pläne und Runbooks - Technische Dokumentation - Kontaktlisten

Fachbereiche: - Zugriff auf relevante BCP-Pläne - Prozessspezifische Runbooks - Schulungsunterlagen

Externe Dienstleister: - Zugriff auf relevante Auszüge (NDA erforderlich) - Keine Zugriff auf vertrauliche Kontaktdaten - Nur freigegebene Versionen

4.4.2 4.2 Zugriffskontrolle (RBAC)

[TODO: Definieren Sie rollenbasierte Zugriffsrechte]

Beispiel:

Rolle	Lesen	Schreiben	Genehmigen	Löschen
BCM-Manager				
Krisenstab		-	-	-
Fachbereich	(eigene Pläne)	(eigene Pläne)	-	-
IT-Operations	(IT-Pläne)	(IT-Pläne)	-	-
Externe	(freigegebene)	-	-	-

4.4.3 4.3 Schutzbedarf und Klassifizierung

Klassifizierung	Beschreibung	Beispieldokumente
Öffentlich	Keine Schutzbedürftigkeit	BCM-Policy (extern)
Intern	Nur für Mitarbeiter	BCM-Handbuch, Schulungsunterlagen
Vertraulich	Eingeschränkter Personenkreis	BIA-Ergebnisse, Kontaktlisten
Streng vertraulich	Nur für Krisenstab	Notfallzugänge, Passwörter

4.5 5. Änderungsprotokoll (Changelog)

4.5.1 5.1 Dokumenthistorie

Version	Datum	Änderung	Autor	Reviewer	Genehmigt durch
0.1	{{ meta.document.last_updated }}	Initiale Erstellung	{{ meta.defaults.author }}	[TODO]	[TODO]

[TODO: Aktualisieren Sie das Änderungsprotokoll bei jeder Dokumentenänderung]

4.5.2 5.2 Änderungsanforderungen

Änderungsanforderungen an BCM-Dokumente können eingereicht werden durch:

- **E-Mail an:** [TODO: BCM-Manager E-Mail]
- **Ticketsystem:** [TODO: System und Kategorie]
- **Formular:** [TODO: Link zu Änderungsanforderungsformular]

Jede Änderungsanforderung wird geprüft und priorisiert. Die Bearbeitung erfolgt gemäß definierter SLAs.

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated | default }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 5

Notfallorganisation: Rollen und Gremien

Dokument-ID: BCM-0040
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

5.1 1. Organisationsmodell

5.1.1 1.1 Notfallorganisationsstruktur

Die Notfallorganisation der AdminSend GmbH besteht aus folgenden Ebenen:

```
      Krisenstab (Strategic)
   Leitung: {{ meta.roles.ceo.name }}
```

```
 BCM-Manager     IT-DR-Team        Fachbereichs
                                   BCP-Teams
```

Ebene 1: Krisenstab (Strategic Level) - Strategische Entscheidungen und Gesamtkoordination - Aktivierung bei schwerwiegenden Vorfällen - Kommunikation mit externen Stakeholdern

Ebene 2: BCM-Manager / Koordination (Tactical Level) - Operative Koordination der

BCM-Maßnahmen - Schnittstelle zwischen Krisenstab und operativen Teams - Dokumentation und Reporting

Ebene 3: Operative Teams (Operational Level) - IT-DR-Team: Wiederherstellung IT-Systeme - Fachbereichs-BCP-Teams: Wiederherstellung Geschäftsprozesse - Support-Teams: Logistik, Kommunikation, HR

5.1.2 1.2 Organigramm

[TODO: Fügen Sie ein detailliertes Organigramm ein]

Verweis: Siehe `diagrams/bcm_organization.png`

5.2 2. Rollenbeschreibungen

5.2.1 2.1 Krisenstabsleitung

Rolle: Krisenstabsleitung / Crisis Management Team Lead

Verantwortlich: {{ meta.roles.ceo.name }}
Stellvertretung: {{ meta.roles.coo.name }}
Kontakt: {{ meta.roles.ceo.email }} / {{ meta.roles.ceo.phone }}

Aufgaben: - Gesamtverantwortung für Krisenmanagement und BCM-Aktivierung - Strategische Entscheidungen über Ressourceneinsatz und Priorisierung - Freigabe von Kommunikation an externe Stakeholder - Entscheidung über Aktivierung von Ausweichstandorten - Genehmigung außerordentlicher Maßnahmen und Budgets

Entscheidungskompetenzen: - Aktivierung und Deaktivierung des Krisenstabs - Freigabe von Notfallbudgets bis [TODO: Betrag] - Entscheidung über Geschäftsfortführung oder -einstellung - Genehmigung von Notfallzugängen (Break-Glass)

Berichtspflichten: - An Aufsichtsrat / Gesellschafter bei schwerwiegenden Krisen - An Aufsichtsbehörden gemäß regulatorischen Anforderungen

5.2.2 2.2 BCM-Manager / BCM-Koordinator

Rolle: BCM-Manager / Business Continuity Coordinator

Verantwortlich: [TODO: BCM-Manager Name]
Stellvertretung: [TODO: Stellvertreter]
Kontakt: [TODO: E-Mail / Telefon]

Aufgaben: - Operative Leitung des BCMS im Normalbetrieb - Koordination von BIA, Risikoanalyse und BCM-Planung - Organisation und Durchführung von BCM-Übungen und Tests - Pflege der BCM-Dokumentation und Kontaktlisten - Schulung und Sensibilisierung der Mitarbeiter - Reporting an Geschäftsführung und Krisenstab

Reporting: - Quartalsweise BCM-Status-Reports an {{ meta.roles.ceo.name }} - Ad-hoc-Reporting bei kritischen Ereignissen - Jährlicher BCM-Jahresbericht

Schnittstellen: - ISMS / CISO: {{ meta.roles.ciso.name }} - IT-Operations: {{ meta.roles.it_operations_manager
}} - Fachbereiche: Jeweilige Bereichsleiter

5.2.3 2.3 Incident Commander / Einsatzleitung (operativ)

Rolle: Incident Commander / Operational Lead

Verantwortlich: [TODO: Incident Commander Name]
Stellvertretung: [TODO: Stellvertreter]
Kontakt: [TODO: E-Mail / Telefon]

Aufgaben: - Operative Leitung der Notfallmaßnahmen vor Ort - Koordination der operativen Teams (IT-DR, BCP-Teams) - Lagebeurteilung und Statusreporting an Krisenstab - Umsetzung der vom Krisenstab beschlossenen Maßnahmen - Dokumentation aller Maßnahmen und Entscheidungen

Schnittstelle zu ITSM/Incident: - Übernahme von Major Incidents aus ITSM-Prozess - Eskalation an Krisenstab bei Überschreitung definierter Schwellwerte - Rückführung in ITSM-Prozess nach Stabilisierung

Entscheidungskompetenzen: - Operative Maßnahmen ohne Budgetüberschreitung - Priorisierung von Wiederherstellungsmaßnahmen - Anforderung zusätzlicher Ressourcen

5.2.4 2.4 Kommunikation / Sprecherrolle

Rolle: Krisenkommunikation / Spokesperson

Verantwortlich: [TODO: Kommunikationsverantwortlicher]
Stellvertretung: [TODO: Stellvertreter]
Kontakt: [TODO: E-Mail / Telefon]

Aufgaben: - Interne Krisenkommunikation (Mitarbeiter, Management) - Externe Krisenkommunikation (Medien, Kunden, Partner, Behörden) - Erstellung und Freigabe von Pressemitteilungen - Social Media Monitoring und Response - Stakeholder-Management

Freigabeprozesse: - Interne Kommunikation: Freigabe durch Krisenstabsleitung - Externe Kommunikation: Freigabe durch {{ meta.roles.ceo.name }} - Pressemitteilungen: Freigabe durch Geschäftsführung und ggf. Rechtsabteilung

Kommunikationskanäle: - Intern: E-Mail, Intranet, Mitarbeiter-App, Telefon - Extern: Website, Social Media, Pressemitteilungen, Kundenhotline

5.2.5 2.5 IT-DR-Lead

Rolle: IT Disaster Recovery Lead

Verantwortlich: {{ meta.roles.it_operations_manager.name }}
Stellvertretung: [TODO: Stellvertreter]
Kontakt: {{ meta.roles.it_operations_manager.email }} / {{ meta.roles.it_operations_manager.phone }}

Aufgaben: - Leitung des IT-DR-Teams - Koordination der IT-Wiederherstellungsmaßnahmen - Umsetzung der IT-Disaster-Recovery-Pläne - Priorisierung der Systemwiederherstellung gemäß BIA - Statusreporting an Incident Commander und Krisenstab

Runbooks und Wiederanlaufkoordination: - Verwaltung und Pflege der IT-DR-Runbooks - Koordination der Systemwiederherstellung in definierter Reihenfolge - Durchführung von Restore-Tests - Dokumentation der Wiederherstellungsmaßnahmen

Schnittstellen: - IT-Operations-Team - Externe IT-Dienstleister und Cloud-Provider - Fachbereiche (für Systemfreigaben)

5.3 3. RACI-Matrix Krisenmanagement

Aktivität	Krisenstabsleitung	BCM-Manager	Incident Commander	IT-DR-Lead	Fachbereich	Kommunikation
Krise aktivieren	**A**	R	C	I	I	I
Lagebeurteilung	I	C	**A/R**	C	C	I
Strategische Entscheidungen	**A**	C	C	I	C	C
Operative Maßnahmen	I	C	**A**	R	R	I
IT-Wiederherstellung	I	C	C	**A/R**	C	I
BCP-Umsetzung	I	C	C	C	**A/R**	I
Interne Kommunikation	A	C	C	I	I	**R**
Externe Kommunikation	**A**	C	I	I	I	**R**
Dokumentation	I	**A**	R	R	R	R
Krise beenden	**A**	R	C	C	C	I

Legende: - **R** = Responsible (Durchführungsverantwortung) - **A** = Accountable (Gesamtverantwortung, Entscheidungsbefugnis) - **C** = Consulted (Konsultiert, Fachexpertise) - **I** = Informed (Informiert)

5.4 4. Erreichbarkeit und Rufbereitschaft

5.4.1 4.1 Bereitschaftsmodelle

[TODO: Definieren Sie Bereitschaftsmodelle für kritische Rollen]

Beispiel:

Krisenstab: - **Erreichbarkeit:** 24/7 über Mobiltelefon - **Reaktionszeit:** Innerhalb von 2 Stunden einsatzbereit - **Bereitschaftsplan:** Rotierendes Modell, quartalsweise Aktualisierung

IT-DR-Team: - **Erreichbarkeit:** 24/7 Rufbereitschaft - **Reaktionszeit:** Innerhalb von 1 Stunde einsatzbereit - **Bereitschaftsplan:** Wöchentliche Rotation

BCM-Manager: - **Erreichbarkeit:** Werktags 08:00-18:00 Uhr, außerhalb über Mobiltelefon - **Reaktionszeit:** Innerhalb von 4 Stunden einsatzbereit

5.4.2 4.2 Eskalationszeiten

Schweregrad	Reaktionszeit	Eskalation an	Eskalationszeit
Niedrig	4 Stunden	IT-Operations	-
Mittel	2 Stunden	Incident Commander	Nach 4 Stunden
Hoch	1 Stunde	Krisenstab	Nach 2 Stunden
Kritisch	Sofort	Krisenstabsleitung	Sofort

5.4.3 4.3 Alarmierungsprozess

[TODO: Beschreiben Sie den Alarmierungsprozess]

Beispiel: 1. **Ersterkennung:** Incident wird erkannt (Monitoring, Meldung, etc.) 2. **Erstbewertung:** IT-Operations bewertet Schweregrad 3. **Alarmierung:** Bei Major Incident → Alarmierung Incident Commander 4. **Eskalation:** Bei BCM-Aktivierung → Alarmierung Krisenstab 5. **Bestätigung:** Alle alarmierten Personen bestätigen Empfang

Alarmierungskanäle: - Primär: Telefon (Mobiltelefon) - Sekundär: SMS / Messenger - Tertiär: E-Mail

5.5 5. Vertretungsregelungen

5.5.1 5.1 Stellvertreterlisten

Für alle kritischen Rollen sind Stellvertreter definiert:

Rolle	Primär	Stellvertreter 1	Stellvertreter 2
Krisenstabsleitung	{{ meta.roles.ceo.name }}	{{ meta.roles.coo.name }}	[TODO]
BCM-Manager	[TODO]	[TODO]	[TODO]
Incident Commander	[TODO]	[TODO]	[TODO]
IT-DR-Lead	{{ meta.roles.it_operations_manager.name }}	[TODO]	[TODO]
Kommunikation	[TODO]	[TODO]	[TODO]

5.5.2 5.2 Übergabeprozess

Bei Vertretung oder Schichtwechsel erfolgt eine strukturierte Übergabe:

Übergabeinhalte: - Aktueller Lagestatus - Laufende Maßnahmen und deren Status - Offene Entscheidungen und Eskalationen - Kritische Informationen und Kontakte

Übergabedokumentation: - Übergabeprotokoll (Template: [TODO: Link]) - Logbuch-Eintrag - Briefing des Nachfolgers

---

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 6

Kontakte und Eskalation

Dokument-ID: BCM-0050
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.document.last_updated }}

6.1 1. Kontaktliste (intern)

> **Achtung:** Kontaktlisten enthalten personenbezogene Daten und unterliegen besonderen Datenschutzanforderungen (DSGVO). Zugriff nur für autorisierte Personen. Quartalsweise Aktualisierung erforderlich.

6.1.1 1.1 Krisenstab

Funktion	Name	Telefon	Mobil	E-Mail	Stellvertretung
Krisenstabsleitung	{{ meta.roles.ceo.name }}	{{ meta.roles.ceo.phone }}	[TODO: Mobil]	{{ meta.roles.ceo.email }}	{{ meta.roles.coo.name }}
CIO	{{ meta.roles.cio.name }}	{{ meta.roles.cio.phone }}	[TODO: Mobil]	{{ meta.roles.cio.email }}	[TODO]
CISO	{{ meta.roles.ciso.name }}	{{ meta.roles.ciso.phone }}	[TODO: Mobil]	{{ meta.roles.ciso.email }}	[TODO]
CFO	{{ meta.roles.cfo.name }}	{{ meta.roles.cfo.phone }}	[TODO: Mobil]	{{ meta.roles.cfo.email }}	[TODO]

Funktion	Name	Telefon	Mobil	E-Mail	Stellvertretung
COO	{{ meta.roles.coo.name }}	{{ meta.roles.coo.phone }}	[TODO: Mobil]	{{ meta.roles.coo.email }}	[TODO]

6.1.2 1.2 BCM-Organisation

Funktion	Name	Telefon	Mobil	E-Mail	Stellvertretung
BCM-Manager	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
Incident Commander	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
IT-DR-Lead	{{ meta.roles.it_operations_manager.name }}	{{ meta.roles.it_operations_manager.phone }}	[TODO]	{{ meta.roles.it_operations_manager.email }}	[TODO]
Kommunikation	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

6.1.3 1.3 IT-Operations und Service Desk

Funktion	Name	Telefon	Mobil	E-Mail	Verfügbarkeit
Service Desk	{{ meta.roles.service_desk_lead.name }}	[TODO]	[TODO]	{{ meta.roles.service_desk_lead.email }}	24/7
IT-Operations Manager	{{ meta.roles.it_operations_manager.name }}	{{ meta.roles.it_operations_manager.phone }}	[TODO]	{{ meta.roles.it_operations_manager.email }}	24/7 Rufbereitschaft
Netzwerk-Team	[TODO]	[TODO]	[TODO]	[TODO]	24/7 Rufbereitschaft
Server-Team	[TODO]	[TODO]	[TODO]	[TODO]	24/7 Rufbereitschaft
Security-Team	[TODO]	[TODO]	[TODO]	[TODO]	24/7 Rufbereitschaft

6.1.4 1.4 Fachbereiche

Fachbereich	Ansprechpartner	Telefon	Mobil	E-Mail	Stellvertretung
Produktion	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
Vertrieb	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
Finanzen	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
HR	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
Einkauf	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

6.2 2. Externe Kontakte

6.2.1 2.1 IT-Dienstleister und Provider

Organisation	Rolle/Service	Kontakt	Telefon	E-Mail	Vertrags-/Kundennr.	Verfügbarkeit
[TODO: Cloud-Provider]	Cloud-Infrastruktur	[TODO]	[TODO]	[TODO]	[TODO]	24/7
[TODO: ISP]	Internet-Anbindung	[TODO]	[TODO]	[TODO]	[TODO]	24/7
[TODO: Telco]	Telefonie	[TODO]	[TODO]	[TODO]	[TODO]	24/7
[TODO: Backup-Provider]	Backup-Services	[TODO]	[TODO]	[TODO]	[TODO]	24/7
[TODO: Security-Provider]	Security-Services	[TODO]	[TODO]	[TODO]	[TODO]	24/7

6.2.2 2.2 Notfalldienste und Behörden

Organisation	Zweck	Telefon	Notrufnummer	Adresse
Feuerwehr	Brand, Gefahrstoffe	[TODO: Lokal]	**112**	[TODO]
Polizei	Sicherheit, Straftaten	[TODO: Lokal]	**110**	[TODO]
Rettungsdienst	Medizinische Notfälle	[TODO: Lokal]	**112**	[TODO]
Giftnotruf	Gefahrstoffunfälle	[TODO: Regional]	[TODO]	[TODO]
BSI	Cyber-Vorfälle	+49 228 99 9582-222	-	Godesberger Allee 185-189, 53175 Bonn

6.2.3 2.3 Kritische Lieferanten

Lieferant	Produkt/Service	Ansprechpartner	Telefon	E-Mail	Kritikalität
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	Hoch / Mittel / Niedrig

6.2.4 2.4 Kunden und Partner (bei Bedarf)

Organisation	Ansprechpartner	Telefon	E-Mail	Benachrichtigung bei
[TODO: Großkunde]	[TODO]	[TODO]	[TODO]	Serviceausfall > 4h

6.3 3. Eskalationsmatrix

6.3.1 3.1 Eskalationsstufen

Stufe	Bezeichnung	Auslöser	Verantwortlich	Reaktionszeit	Kommunikationspflicht
1	Störung	Einzelne Systeme betroffen, keine Auswirkung auf kritische Services	IT-Operations	4 Stunden	Service Desk informieren
2	Major Incident	Kritischer Service beeinträchtigt, RTO gefährdet	Incident Commander	1 Stunde	Management informieren
3	BCM-Aktivierung	Mehrere kritische Services ausgefallen, Geschäftsbetrieb gefährdet	Krisenstab	30 Minuten	Krisenstab aktivieren, externe Stakeholder informieren
4	Katastrophe	Standort nicht verfügbar, massive Auswirkungen	Krisenstabsleitung	Sofort	Alle Stakeholder, Behörden, Medien

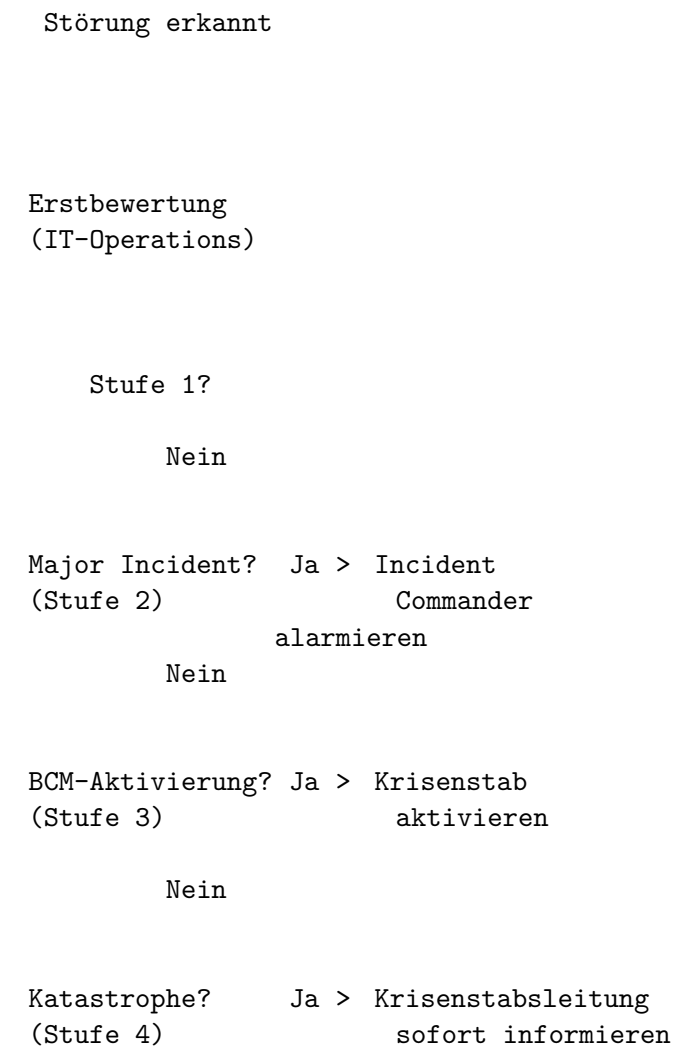
6.3.2 3.2 Eskalationskriterien

Eskalation auf Stufe 2 (Major Incident): - RTO eines kritischen Services wird voraussichtlich überschritten - Mehr als [TODO: X] Benutzer betroffen - Finanzieller Schaden > [TODO: Betrag] pro Stunde - Datenverlust droht (RPO-Überschreitung) - Sicherheitsvorfall mit hohem Impact

Eskalation auf Stufe 3 (BCM-Aktivierung): - Mehrere kritische Services gleichzeitig ausgefallen - Wiederherstellung innerhalb RTO nicht möglich - Standort nicht zugänglich - Massive Cyber-Attacke (Ransomware, DDoS) - Naturkatastrophe oder schwerer Unfall

Eskalation auf Stufe 4 (Katastrophe): - Hauptstandort komplett ausgefallen - Menschenleben in Gefahr - Existenzbedrohende Situation für das Unternehmen - Behördliche Anordnung (z.B. Evakuierung)

6.3.3 3.3 Eskalationsprozess



6.4 4. Alarmierungsprozess

6.4.1 4.1 Alarmierungskanäle

Primär: Telefon (Mobiltelefon) - Direktanruf an definierte Kontaktpersonen - Bei Nichterreichbarkeit: Stellvertreter kontaktieren

Sekundär: SMS / Messenger - Parallele Benachrichtigung via SMS - Messenger-Gruppen für schnelle Koordination

Tertiär: E-Mail - Dokumentation und Nachvollziehbarkeit - Nicht für zeitkritische Alarmierung geeignet

6.4.2 4.2 Alarmierungsablauf

1. **Ersterkennung:** Störung wird erkannt (Monitoring, Meldung, Beobachtung)

2. **Erstbewertung:** IT-Operations bewertet Schweregrad und Auswirkungen
3. **Alarmierung:** Kontaktaufnahme gemäß Eskalationsstufe
4. **Bestätigung:** Empfänger bestätigt Empfang und Verfügbarkeit
5. **Briefing:** Kurze Lagebeschreibung und erste Maßnahmen
6. **Dokumentation:** Alarmierung wird im Logbuch dokumentiert

6.4.3 4.3 Alarmierungsliste Krisenstab

Bei BCM-Aktivierung (Stufe 3) werden folgende Personen alarmiert:

1. {{ meta.roles.ceo.name }} (Krisenstabsleitung)
2. {{ meta.roles.cio.name }} (CIO)
3. {{ meta.roles.ciso.name }} (CISO)
4. [TODO: BCM-Manager]
5. [TODO: Kommunikationsverantwortlicher]
6. Weitere Krisenstabsmitglieder je nach Situation

Alarmierungsreihenfolge: Parallel, nicht sequenziell

6.5 5. Rufbereitschaft und On-Call

6.5.1 5.1 Rufbereitschaftsplan

[TODO: Definieren Sie Rufbereitschaftspläne für kritische Rollen]

Beispiel IT-Operations:

KW	Primär	Sekundär	Tertiär
01	[Name 1]	[Name 2]	[Name 3]
02	[Name 2]	[Name 3]	[Name 1]
03	[Name 3]	[Name 1]	[Name 2]

Aktualisierung: Wöchentlich, spätestens Freitag 12:00 Uhr

6.5.2 5.2 On-Call-Verpflichtungen

Während der Rufbereitschaft: - Mobiltelefon eingeschaltet und erreichbar (24/7) - Reaktionszeit: Innerhalb von 30 Minuten - Nüchtern und einsatzfähig - Zugriff auf Laptop und VPN - Kenntnis der aktuellen Runbooks und Eskalationswege

Vergütung: Gemäß Betriebsvereinbarung / Arbeitsvertrag

6.6 6. Kontaktlistenpflege

6.6.1 6.1 Aktualisierungsprozess

Verantwortlich: BCM-Manager

Aktualisierungsintervall: - Quartalsweise Überprüfung aller Kontaktdaten - Ad-hoc bei personellen Änderungen - Nach jeder BCM-Übung

Prozess: 1. BCM-Manager fordert Aktualisierung an 2. Fachbereiche prüfen und melden Änderungen 3. BCM-Manager aktualisiert Kontaktlisten 4. Neue Version wird verteilt und alte Version archiviert

6.6.2 6.2 Datenschutz

Kontaktlisten unterliegen der DSGVO: - Zugriff nur für autorisierte Personen - Verschlüsselte Speicherung - Keine Weitergabe an Dritte ohne Einwilligung - Löschung bei Ausscheiden von Mitarbeitern

---

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 7

Service- und Prozesskatalog mit Kritikalität

Dokument-ID: BCM-0060
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

7.1 1. Ziel

Dieses Dokument dokumentiert alle im BCM betrachteten Services und Geschäftsprozesse der AdminSend GmbH inklusive:

- **Kritikalitätsbewertung:** Einstufung nach Geschäftskritikalität (Hoch/Mittel/Niedrig)
- **Ownership:** Klare Zuordnung von Verantwortlichkeiten
- **Abhängigkeiten:** Identifikation kritischer Abhängigkeiten
- **Stakeholder:** Betroffene Kunden und interne/externe Stakeholder

Der Service- und Prozesskatalog bildet die Grundlage für: - Business Impact Analysis (BIA) - BCM-Strategien und Kontinuitätsoptionen - Business Continuity Pläne (BCP) - IT Disaster Recovery Pläne (DRP)

7.2 2. Service- und Prozesskatalog

7.2.1 2.1 Geschäftskritische Services (Kritikalität: HOCH)

Service/Prozess	Owner	Beschreibung	Top 5 Abhängigkeiten	Kunden/Stakeholder
[TODO: Service 1]	[TODO: Owner]	[TODO: Beschreibung]	[TODO: 1. IT-System, 2. Lieferant, 3. Personal, 4. Standort, 5. Daten]	[TODO: Externe Kunden, Partner]
[TODO: Service 2]	[TODO: Owner]	[TODO: Beschreibung]	[TODO: Abhängigkeiten]	[TODO: Stakeholder]

Beispiele für geschäftskritische Services: - Kundenservice und Support (24/7) - Produktionssteuerung und -durchführung - Auftragsabwicklung und Logistik - Zahlungsverkehr und Finanzprozesse - E-Commerce-Plattform

7.2.2 2.2 Wichtige Services (Kritikalität: MITTEL)

Service/Prozess	Owner	Beschreibung	Top 5 Abhängigkeiten	Kunden/Stakeholder
[TODO: Service 1]	[TODO: Owner]	[TODO: Beschreibung]	[TODO: Abhängigkeiten]	[TODO: Stakeholder]

Beispiele für wichtige Services: - Personalverwaltung und HR-Prozesse - Einkauf und Beschaffung - Marketing und Vertrieb (nicht zeitkritisch) - Controlling und Reporting - Qualitätsmanagement

7.2.3 2.3 Unterstützende Services (Kritikalität: NIEDRIG)

Service/Prozess	Owner	Beschreibung	Top 5 Abhängigkeiten	Kunden/Stakeholder
[TODO: Service 1]	[TODO: Owner]	[TODO: Beschreibung]	[TODO: Abhängigkeiten]	[TODO: Stakeholder]

Beispiele für unterstützende Services: - Entwicklungsumgebungen - Schulungs- und Trainingsplattformen - Archivierung und Dokumentenmanagement - Interne Kommunikationstools (nicht zeitkritisch)

7.3 3. Kriterien zur Kritikalitätsbewertung

7.3.1 3.1 Bewertungsdimensionen

Die Kritikalität wird anhand folgender Dimensionen bewertet:

1. Finanzieller Impact - Direkter Umsatzverlust pro Stunde/Tag - Vertragsstrafen und Schadensersatzforderungen - Zusätzliche Kosten für Notfallmaßnahmen

2. Operativer Impact - Beeinträchtigung anderer Geschäftsprozesse - Produktionsausfall oder Qualitätsprobleme - Rückstau und Nacharbeitsaufwand

3. Rechtliche und regulatorische Anforderungen - Gesetzliche Verpflichtungen und Compliance - Vertragliche Verpflichtungen (SLAs) - Meldepflichten gegenüber Behörden

4. Sicherheit - Gefährdung von Menschenleben - Umweltgefährdung - Anlagensicherheit

5. Reputation und Vertrauen - Kundenvertrauen und Kundenzufriedenheit - Markenimage und öffentliche Wahrnehmung - Vertrauen von Partnern und Investoren

7.3.2 3.2 Bewertungslogik und Scoring

[TODO: Definieren Sie Ihre Bewertungslogik]

Beispiel-Scoring:

Kritikalität	Finanzieller Impact	Operativer Impact	Rechtlicher Impact	Sicherheits-Impact	Reputations-Impact
HOCH	> 50.000 €/Tag	Mehrere Prozesse betroffen	Gesetzesverstoß	Personengefährdung	Massive Medienberichterstattung
MITTEL	10.000-50.000 €/Tag	Ein Prozess betroffen	Vertragsverletzung	Sachschaden	Kundenbeschwerden
NIEDRIG	< 10.000 €/Tag	Keine Auswirkung	Keine Verpflichtung	Kein Schaden	Keine Auswirkung

Gesamtbewertung: - Wenn mindestens eine Dimension "HOCH" → Gesamtkritikalität: **HOCH** - Wenn mindestens zwei Dimensionen "MITTEL" → Gesamtkritikalität: **MITTEL** - Sonst → Gesamtkritikalität: **NIEDRIG**

7.3.3 3.3 Kritikalitätsmatrix

```
Impact

H    [Service A]  [Service B]
     [Service C]

M                 [Service D]
     [Service E]

L                 [Service F]  [Service G]


    L           M           H
              Wahrscheinlichkeit
```

[TODO: Ordnen Sie Ihre Services in die Matrix ein]

7.4 4. IT-Services und Systeme

7.4.1 4.1 Kritische IT-Services

IT-Service	Unterstützte Geschäftsprozesse	Kritikalität	IT-Owner	Technologie
[TODO: ERP-System]	Auftragsabwicklung, Finanzen, Produktion	HOCH	{{ meta.roles.it_operations_manager.name }}	[TODO: SAP/Oracle/etc.]
[TODO: E-Mail]	Alle Geschäftsprozesse	HOCH	{{ meta.roles.it_operations_manager.name }}	[TODO: Exchange/M365/etc.]
[TODO: CRM]	Vertrieb, Kundenservice	MITTEL	[TODO]	[TODO: Salesforce/etc.]

7.4.2 4.2 IT-Infrastruktur

Infrastruktur-Komponente	Abhängige Services	Kritikalität	Standort	Redundanz
[TODO: Core Switch]	Alle IT-Services	HOCH	München	Ja/Nein
[TODO: Firewall]	Internet-Zugang	HOCH	München	Ja/Nein
[TODO: Storage]	Alle Daten	HOCH	München	Ja/Nein

7.5 5. Abhängigkeitsanalyse

7.5.1 5.1 Abhängigkeitstypen

People (Personal): - Schlüsselpersonen und Spezialwissen - Mindestbesetzung für Betrieb - Externe Dienstleister

Facilities (Standorte und Räumlichkeiten): - Bürogebäude und Produktionsstätten - Rechenzentren - Lager und Logistikzentren

Technology (IT-Systeme und Technologie): - Geschäftsanwendungen (ERP, CRM, etc.) - IT-Infrastruktur (Netzwerk, Server, Storage) - Cloud-Services

Information (Daten und Informationen): - Geschäftsdaten und Kundendaten - Konfigurationsdaten - Dokumentation und Wissen

Suppliers (Lieferanten und Partner): - Kritische Zulieferer - IT-Dienstleister und Cloud-Provider - Logistikpartner

7.5.2 5.2 Abhängigkeitsmatrix (Beispiel)

[TODO: Erstellen Sie eine Abhängigkeitsmatrix für Ihre kritischen Services]

Beispiel für Service "Auftragsabwicklung":

Abhängigkeitstyp	Konkrete Abhängigkeit	Kritikalität	Ausweichmöglichkeit
People	Auftragsbearbeiter (mind. 3)	HOCH	Schulung von Backup-Personal
Facilities	Bürostandort Hauptsitz	MITTEL	Home-Office möglich
Technology	ERP-System	HOCH	Keine (Single Point of Failure)

Abhängigkeitstyp	Konkrete Abhängigkeit	Kritikalität	Ausweichmöglichkeit
Information	Auftragsdatenbank	HOCH	Backup vorhanden
Suppliers	Logistikdienstleister	HOCH	Alternativdienstleister verfügbar

7.6 6. Stakeholder-Übersicht

7.6.1 6.1 Interne Stakeholder

Stakeholder-Gruppe	Betroffene Services	Kommunikationsbedarf	Ansprechpartner
Geschäftsführung	Alle kritischen Services	Strategische Entscheidungen	{{ meta.roles.ceo.name }}
IT-Abteilung	Alle IT-abhängigen Services	Technische Koordination	{{ meta.roles.cio.name }}
Fachbereiche	Jeweilige Services	Operative Umsetzung	[TODO: Bereichsleiter]
Mitarbeiter	Alle Services	Information und Anweisungen	[TODO: HR/Kommunikation]

7.6.2 6.2 Externe Stakeholder

Stakeholder-Gruppe	Betroffene Services	Kommunikationsbedarf	Ansprechpartner
Kunden	Kundenservice, Produktion, Lieferung	Statusupdates, Alternativlösungen	[TODO: Kundenservice]
Lieferanten	Beschaffung, Produktion	Koordination, Anpassungen	[TODO: Einkauf]
Partner	Gemeinsame Services	Abstimmung, Koordination	[TODO: Partnerverantwortlicher]
Behörden	Regulierte Services	Meldungen, Nachweise	[TODO: Compliance]
Medien	Alle Services (bei Krise)	Pressemitteilungen	[TODO: PR/Kommunikation]

7.7 7. Pflege und Aktualisierung

Verantwortlich: BCM-Manager

Aktualisierungsintervall: - Jährliche Überprüfung aller Services und Kritikalitätsbewertungen - Ad-hoc bei organisatorischen Änderungen (neue Services, Prozessänderungen) - Nach BIA-Durchführung

Review-Prozess: 1. BCM-Manager initiiert Review 2. Service-Owner prüfen und aktualisieren ihre Services 3. Kritikalitätsbewertung wird validiert 4. Änderungen werden dokumentiert und kommuniziert

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 8

Business Impact Analysis (BIA) – Methodik

Dokument-ID: BCM-0070
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

8.1 1. Zweck und Output

8.1.1 1.1 Ziele der BIA

Die Business Impact Analysis (BIA) der AdminSend GmbH verfolgt folgende Ziele:

- **Identifikation kritischer Geschäftsprozesse:** Ermittlung der geschäftskritischen Prozesse und Services
- **Quantifizierung von Auswirkungen:** Bewertung der finanziellen, operativen und reputationsbezogenen Auswirkungen von Ausfällen
- **Festlegung von Zielwerten:** Definition von RTO (Recovery Time Objective) und RPO (Recovery Point Objective)
- **Priorisierung:** Festlegung der Wiederherstellungspriorisierung
- **Ressourcenplanung:** Ermittlung des Ressourcenbedarfs für Business Continuity

8.1.2 1.2 Erwartete Ergebnisse

Die BIA liefert folgende Ergebnisse:

RTO (Recovery Time Objective): - Maximale tolerierbare Ausfallzeit für jeden kritischen Prozess - Zeitpunkt, bis zu dem ein Prozess wiederhergestellt sein muss

RPO (Recovery Point Objective): - Maximaler tolerierbarer Datenverlust - Zeitpunkt, bis zu dem Daten wiederhergestellt werden müssen

MTPD (Maximum Tolerable Period of Disruption): - Maximale Zeitspanne, die ein Prozess ausfallen kann, bevor irreparable Schäden entstehen - Auch: MAO (Maximum Acceptable Outage)

Priorisierung: - Reihenfolge der Wiederherstellung von Prozessen und Systemen - Abhängigkeiten zwischen Prozessen

Ressourcenbedarf: - Personal, Räumlichkeiten, IT-Systeme, Daten, Lieferanten - Mindestressourcen für Notbetrieb

8.2 2. Vorgehen und Methodik

8.2.1 2.1 BIA-Prozess

```
1. Vorbereitung
- Scope
- Stakeholder
```

```
2. Datenerhebung
- Workshops
- Interviews
- Fragebögen
```

```
3. Analyse
- Bewertung
- Abhängigkeiten
```

```
4. RTO/RPO
- Festlegung
- Validierung
```

```
5. Dokumentation
- Bericht
- Präsentation
```

```
6. Freigabe
- Review
- Genehmigung
```

8.2.2 2.2 Workshops und Interviews

Zielgruppe: - Fachbereichsleiter und Prozessverantwortliche - IT-Verantwortliche - Schlüsselpersonen mit Spezialwissen

Format: - **Workshops:** Gruppenformat für übergreifende Themen (2-4 Stunden) - **Interviews:** Einzelgespräche für detaillierte Prozessanalyse (1-2 Stunden) - **Fragebögen:** Standardisierte Erhebung für weniger kritische Prozesse

Durchführung: [TODO: Definieren Sie Workshop-/Interview-Plan]

Beispiel-Zeitplan: | Woche | Aktivität | Teilnehmer | Verantwortlich | |——-|————|————|————-| | 1 | Kick-off Workshop | Alle Bereichsleiter | BCM-Manager | | 2-3 | Einzelinterviews Fachbereiche | Prozessverantwortliche | BCM-Manager | | 4 | IT-Workshop | IT-Team | BCM-Manager + {{ meta.roles.cio.name }} | | 5 | Konsolidierung und Analyse | BCM-Team | BCM-Manager | | 6 | Ergebnispräsentation | Management | BCM-Manager |

8.2.3 2.3 Datenquellen

Primäre Datenquellen: - Workshops und Interviews mit Fachbereichen - Bestehende Prozessdokumentation - IT-Service-Katalog und CMDB - Finanzberichte und Umsatzdaten

Sekundäre Datenquellen: - Vertragsdokumente und SLAs - Compliance-Anforderungen - Historische Vorfallsdaten - Benchmarks und Best Practices

8.2.4 2.4 Review- und Validierungsschritte

Validierung durch Fachbereiche: 1. Entwurf der BIA-Ergebnisse wird an Prozessverantwortliche gesendet 2. Fachbereiche prüfen und kommentieren innerhalb von [TODO: X] Tagen 3. Feedback wird eingearbeitet

Management-Review: 1. Konsolidierte BIA-Ergebnisse werden dem Management präsentiert 2. RTO/RPO-Werte werden diskutiert und validiert 3. Priorisierung wird festgelegt

Formale Freigabe: - Genehmigung durch {{ meta.roles.ceo.name }} (CEO) - Bestätigung durch Fachbereichsleiter - Dokumentation der Freigabe

8.3 3. Bewertungsdimensionen

8.3.1 3.1 Finanzielle Auswirkungen

Direkte finanzielle Verluste: - Umsatzverlust pro Stunde/Tag - Vertragsstrafen und Schadensersatzforderungen - Zusätzliche Kosten für Notfallmaßnahmen

Bewertungsskala: [TODO: Definieren Sie Ihre Bewertungsskala]

Beispiel: | Stufe | Beschreibung | Umsatzverlust pro Tag | |——-|————|————————-| | 5 - Kritisch | Existenzbedrohend | > 500.000 € | | 4 - Sehr hoch | Massive Auswirkungen | 100.000 - 500.000 € | | 3 - Hoch | Erhebliche Auswirkungen | 50.000 - 100.000 € | | 2 - Mittel | Spürbare Auswirkungen | 10.000 - 50.000 € | | 1 - Niedrig | Geringe Auswirkungen | < 10.000 € |

8.3.2 3.2 Operative Auswirkungen

Beeinträchtigung des Geschäftsbetriebs: - Durchsatz und Produktionskapazität - Rückstau und Nacharbeitsaufwand - Qualitätsprobleme - Beeinträchtigung anderer Prozesse

Bewertungsskala: | Stufe | Beschreibung | Operative Auswirkung | |——-|————|———————————| | 5 - Kritisch | Kompletter Stillstand | Alle Prozesse betroffen | | 4 - Sehr hoch | Massive Beeinträchtigung | Mehrere kritische Prozesse betroffen | | 3 - Hoch | Erhebliche Beeinträchtigung | Ein kritischer Prozess betroffen | | 2 - Mittel | Spürbare Beeinträchtigung | Verzögerungen, aber Betrieb möglich | | 1 - Niedrig | Geringe Beeinträchtigung | Keine wesentliche Auswirkung |

8.3.3 3.3 Rechtliche und regulatorische Auswirkungen

Compliance-Risiken: - Gesetzliche Verpflichtungen (z.B. DSGVO, Arbeitsschutz) - Vertragliche Verpflichtungen (SLAs, Lieferverträge) - Meldepflichten gegenüber Behörden - Haftungsrisiken

Bewertungsskala: | Stufe | Beschreibung | Rechtliche Auswirkung | |——-|————|———————————-| | 5 - Kritisch | Schwerer Gesetzesverstoß | Strafverfahren, Lizenzverlust | | 4 - Sehr hoch | Erheblicher Verstoß | Bußgelder > 100.000 € | | 3 - Hoch | Verstoß | Bußgelder 10.000 - 100.000 € | | 2 - Mittel | Vertragsverletzung | Vertragsstrafen | | 1 - Niedrig | Keine Verpflichtung | Keine rechtlichen Folgen |

8.3.4 3.4 Sicherheitsauswirkungen

Gefährdung von Personen und Anlagen: - Personensicherheit (Mitarbeiter, Kunden, Besucher) - Umweltgefährdung - Anlagensicherheit - Datensicherheit

Bewertungsskala: | Stufe | Beschreibung | Sicherheitsauswirkung | |——-|————|———————————-| | 5 - Kritisch | Lebensgefahr | Todesfälle oder schwere Verletzungen | | 4 - Sehr hoch | Erhebliche Gefährdung | Verletzungen, Umweltschäden | | 3 - Hoch | Gefährdung | Gesundheitsrisiken | | 2 - Mittel | Geringe Gefährdung | Sachschäden | | 1 - Niedrig | Keine Gefährdung | Keine Sicherheitsrisiken |

8.3.5 3.5 Reputationsauswirkungen

Image und Vertrauen: - Kundenvertrauen und Kundenzufriedenheit - Markenimage und öffentliche Wahrnehmung - Vertrauen von Partnern und Investoren - Medienberichterstattung

Bewertungsskala: | Stufe | Beschreibung | Reputationsauswirkung | |——-|————|———————————-| | 5 - Kritisch | Irreparabler Schaden | Massive negative Medienberichterstattung, Kundenabwanderung | | 4 - Sehr hoch | Schwerer Schaden | Nationale Medienberichterstattung, erheblicher Vertrauensverlust | | 3 - Hoch | Erheblicher Schaden | Regionale Medienberichterstattung, Kundenbeschwerden | | 2 - Mittel | Spürbarer Schaden | Social Media Kritik, einzelne Beschwerden | | 1 - Niedrig | Geringer Schaden | Keine öffentliche Wahrnehmung |

8.4 4. Zeitabhängigkeit der Auswirkungen

8.4.1 4.1 Zeitfenster-Analyse

Die Auswirkungen von Prozessausfällen werden für verschiedene Zeitfenster bewertet:

Zeitfenster: - **0-4 Stunden:** Sofortige Auswirkungen - **4-24 Stunden:** Kurzfristige Auswirkungen - **1-3 Tage:** Mittelfristige Auswirkungen - **> 3 Tage:** Langfristige Auswirkungen

8.4.2 4.2 Impact-Progression

[TODO: Dokumentieren Sie die zeitabhängige Entwicklung der Auswirkungen]

Beispiel für Prozess "Auftragsabwicklung":

Zeitfenster	Finanzielle Auswirkung	Operative Auswirkung	Reputationsauswirkung
0-4h	Gering (Stufe 1)	Mittel (Stufe 2)	Niedrig (Stufe 1)
4-24h	Mittel (Stufe 2)	Hoch (Stufe 3)	Mittel (Stufe 2)
1-3d	Hoch (Stufe 3)	Sehr hoch (Stufe 4)	Hoch (Stufe 3)
> 3d	Kritisch (Stufe 5)	Kritisch (Stufe 5)	Sehr hoch (Stufe 4)

8.4.3 4.3 MTPD-Bestimmung

Maximum Tolerable Period of Disruption (MTPD):

Der MTPD ist der Zeitpunkt, ab dem die Auswirkungen eines Ausfalls inakzeptabel werden.

Bestimmung: - MTPD = Zeitpunkt, ab dem Auswirkungen Stufe 4 oder 5 erreichen - Oder: Zeitpunkt, ab dem mehrere Dimensionen Stufe 3 erreichen

Beispiel: - Prozess "Auftragsabwicklung": MTPD = 24 Stunden (ab dann Stufe 4/5) - Prozess "E-Mail": MTPD = 4 Stunden (ab dann Stufe 3 in mehreren Dimensionen)

8.5 5. RTO/RPO-Festlegung

8.5.1 5.1 RTO-Bestimmung

Recovery Time Objective (RTO): - RTO muss deutlich unter MTPD liegen (Sicherheitspuffer) - Empfehlung: RTO = 50-70% des MTPD

Beispiel: - MTPD = 24 Stunden → RTO = 12-16 Stunden - MTPD = 4 Stunden → RTO = 2-3 Stunden

8.5.2 5.2 RPO-Bestimmung

Recovery Point Objective (RPO): - Maximaler tolerierbarer Datenverlust - Abhängig von Datenänderungsrate und Geschäftskritikalität

Beispiel: - Transaktionsdaten: RPO = 15 Minuten (kontinuierliche Replikation) - Konfigurationsdaten: RPO = 24 Stunden (tägliches Backup) - Archivdaten: RPO = 7 Tage (wöchentliches Backup)

8.6 6. Ergebnisfreigabe

8.6.1 6.1 Verantwortliche für Abnahme

Fachbereichsebene: - Prozessverantwortliche bestätigen BIA-Ergebnisse für ihre Prozesse - Validierung der RTO/RPO-Werte

Management-Ebene: - {{ meta.roles.ceo.name }} (CEO) genehmigt Gesamt-BIA - {{ meta.roles.cio.name }} (CIO) genehmigt IT-bezogene RTO/RPO - Fachbereichsleiter genehmigen ihre Bereiche

8.6.2 6.2 Freigabeprozess

1. **Entwurf:** BCM-Manager erstellt BIA-Bericht
2. **Fachbereichs-Review:** Prozessverantwortliche prüfen (2 Wochen)
3. **Überarbeitung:** Feedback wird eingearbeitet
4. **Management-Präsentation:** Vorstellung der Ergebnisse
5. **Formale Freigabe:** Unterschriften der Verantwortlichen
6. **Veröffentlichung:** BIA-Ergebnisse werden kommuniziert

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 9

BIA – Ergebnisse und Zielwerte (RTO/RPO)

Dokument-ID: BCM-0080
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.document.last_updated }}

9.1 1. Zusammenfassung

9.1.1 1.1 Top-kritische Prozesse und Services

Die folgenden Prozesse wurden als geschäftskritisch identifiziert (RTO < 24 Stunden):

[TODO: Listen Sie die top-kritischen Prozesse auf]

Beispiele: 1. **Auftragsabwicklung** - RTO: 4 Stunden, RPO: 15 Minuten 2. **Kundenservice (24/7)** - RTO: 2 Stunden, RPO: 1 Stunde 3. **Produktionssteuerung** - RTO: 8 Stunden, RPO: 30 Minuten 4. **Zahlungsverkehr** - RTO: 4 Stunden, RPO: 15 Minuten 5. **E-Mail und Kommunikation** - RTO: 4 Stunden, RPO: 1 Stunde

9.1.2 1.2 Wesentliche Erkenntnisse

[TODO: Dokumentieren Sie die wichtigsten Erkenntnisse aus der BIA]

Beispiel-Erkenntnisse: - **Single Points of Failure:** ERP-System hat keine Redundanz, kritische Abhängigkeit - **Personalabhängigkeiten:** Schlüsselpersonen in Produktion ohne ausreichende Vertretung - **Lieferantenrisiken:** Kritischer Lieferant hat kein eigenes BCM - **IT-Infrastruktur:** Netzwerkinfrastruktur teilweise nicht redundant ausgelegt

9.2 2. BIA-Ergebnis-Tabelle

9.2.1 2.1 Geschäftskritische Prozesse (Kritikalität: HOCH)

Service/Prozess	MTPD/MAO	RTO	RPO	Manuelle Workarounds möglich?	Bemerkungen
[TODO: Prozess 1]	[TODO: 24h]	[TODO: 4h]	[TODO: 15min]	Ja/Nein/Teilweise	[TODO: Bemerkungen]
[TODO: Prozess 2]	[TODO]	[TODO]	[TODO]	Ja/Nein/Teilweise	[TODO]

Beispiel: | Service/Prozess | MTPD/MAO | RTO | RPO | Manuelle Workarounds möglich? | Bemerkungen | |—————|———-|—-|—-|———————————-|————-| | Auftragsabwicklung | 24h | 4h | 15min | Teilweise (Excel-Listen) | ERP-System kritisch | | Kundenservice | 8h | 2h | 1h | Ja (Telefon, E-Mail) | CRM-System hilfreich, aber nicht zwingend | | Produktionssteuerung | 48h | 8h | 30min | Nein | Vollautomatisiert, keine manuelle Alternative |

9.2.2 2.2 Wichtige Prozesse (Kritikalität: MITTEL)

Service/Prozess	MTPD/MAO	RTO	RPO	Manuelle Workarounds möglich?	Bemerkungen
[TODO: Prozess 1]	[TODO]	[TODO]	[TODO]	Ja/Nein/Teilweise	[TODO]

9.2.3 2.3 Unterstützende Prozesse (Kritikalität: NIEDRIG)

Service/Prozess	MTPD/MAO	RTO	RPO	Manuelle Workarounds möglich?	Bemerkungen
[TODO: Prozess 1]	[TODO]	[TODO]	[TODO]	Ja/Nein/Teilweise	[TODO]

9.3 3. Abhängigkeiten pro kritischem Prozess

9.3.1 3.1 Prozess: [TODO: Prozessname]

People (Personal): - [TODO: Mindestbesetzung, Schlüsselpersonen, Spezialwissen] - Beispiel: Mindestens 3 Auftragsbearbeiter, Vertretungsregelung erforderlich

Facilities (Standorte und Räumlichkeiten): - [TODO: Benötigte Standorte, Räume, Infrastruktur] - Beispiel: Büroarbeitsplätze, Home-Office als Alternative möglich

Technology (IT-Systeme): - [TODO: Kritische IT-Systeme und Anwendungen] - Beispiel: ERP-System (SAP), E-Mail, Netzwerkzugang

Information (Daten): - [TODO: Kritische Daten und Informationen] - Beispiel: Auftragsdatenbank, Kundenstammdaten, Produktkonfigurationen

Suppliers (Lieferanten und Partner): - [TODO: Kritische Lieferanten und Dienstleister] - Beispiel: Logistikdienstleister, Cloud-Provider, Zahlungsdienstleister

9.3.2 3.2 Abhängigkeitsmatrix

[TODO: Erstellen Sie eine Abhängigkeitsmatrix für alle kritischen Prozesse]

Prozess	People	Facilities	Technology	Information	Suppliers
Auftragsabwicklung	3 Mitarbeiter	Büro/Home-Office	ERP, E-Mail	Auftragsdaten	Logistik
Kundenservice	5 Mitarbeiter	Call-Center	CRM, Telefon	Kundendaten	Telco
Produktion	10 Mitarbeiter	Produktionshalle	MES, SCADA	Produktionsdaten	Zulieferer

9.4 4. Manuelle Workarounds und Notbetrieb

9.4.1 4.1 Workaround-Strategien

[TODO: Dokumentieren Sie manuelle Workarounds für kritische Prozesse]

Beispiel für Prozess "Auftragsabwicklung":

Bei Ausfall ERP-System: - **Workaround:** Manuelle Auftragserfassung in Excel-Listen - **Kapazität:** Reduziert auf 30% des Normalbetriebs - **Dauer:** Maximal 24 Stunden (dann Dateneingabe-Rückstau zu groß) - **Voraussetzungen:** Excel-Templates vorhanden, Mitarbeiter geschult - **Einschränkungen:** Keine Echtzeit-Bestandsprüfung, keine automatische Rechnungserstellung

Bei Ausfall Standort: - **Workaround:** Home-Office für Auftragsbearbeitung - **Kapazität:** 80% des Normalbetriebs - **Dauer:** Unbegrenzt - **Voraussetzungen:** VPN-Zugang, Laptops, Telefonie über Softphone - **Einschränkungen:** Keine physische Dokumentenbearbeitung

9.4.2 4.2 Notbetrieb-Kapazitäten

Prozess	Normalbetrieb	Notbetrieb (manuell)	Notbetrieb (IT-DR)	Bemerkungen
Auftragsabwicklung	100%	30%	80%	Manuelle Erfassung sehr aufwändig
Kundenservice	100%	70%	90%	Telefon als Fallback
Produktion	100%	0%	100%	Keine manuelle Alternative

9.5 5. Offene Punkte und Maßnahmen

9.5.1 5.1 Identifizierte Risiken und Maßnahmen

Maßnahme	Beschreibung	Owner	Priorität	Fällig	Status	Kosten (geschätzt)
[TODO: Maßnahme 1]	[TODO: Beschreibung]	[TODO: Owner]	Hoch/Mittel/Niedrig	[TODO: Datum]	Offen/In Arbeit/Erledigt	[TODO: Betrag]

Beispiele:

Maßnahme	Beschreibung	Owner	Priorität	Fällig	Status	Kosten (geschätzt)
ERP-Redundanz	Implementierung Hochverfügbarkeits-Cluster	{{ meta.roles.cio.name }}	Hoch	Q2 2026	In Arbeit	150.000 €
Backup-Personal	Schulung von Vertretungen für Schlüsselpersonen	HR	Hoch	Q1 2026	Offen	20.000 €
Lieferanten-BCM	Anforderung BCM-Nachweise von kritischen Lieferanten	Einkauf	Mittel	Q2 2026	Offen	5.000 €
Netzwerk-Redundanz	Zweite Internet-Anbindung	{{ meta.roles.it_operations_manager.name }}	Hoch	Q1 2026	In Arbeit	30.000 €

9.5.2 5.2 Priorisierung der Maßnahmen

Priorität HOCH (sofort umsetzen): - Maßnahmen zur Beseitigung von Single Points of Failure - Maßnahmen zur Einhaltung kritischer RTO/RPO-Werte - Maßnahmen zur Erfüllung regulatorischer Anforderungen

Priorität MITTEL (innerhalb 6-12 Monate): - Maßnahmen zur Verbesserung der Resilienz - Maßnahmen zur Reduktion von Abhängigkeiten - Maßnahmen zur Verbesserung von Workarounds

Priorität NIEDRIG (Nice-to-have): - Maßnahmen zur weiteren Optimierung - Maßnahmen für weniger kritische Prozesse

9.6 6. Wiederherstellungspriorisierung

9.6.1 6.1 Priorisierungsmatrix

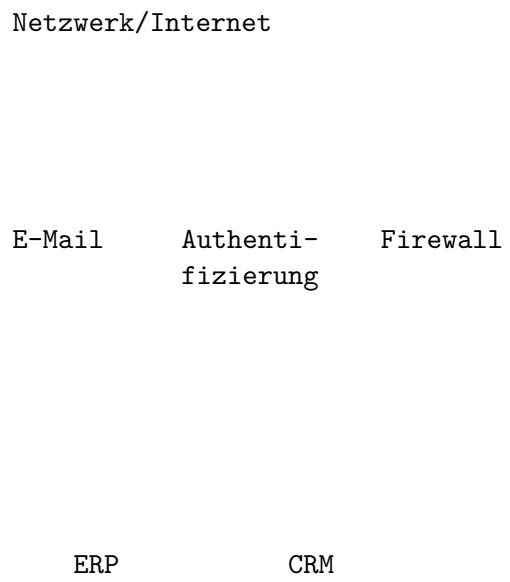
Bei einem umfassenden Ausfall erfolgt die Wiederherstellung in folgender Reihenfolge:

Priorität 1 (0-4 Stunden): 1. Netzwerkinfrastruktur und Internet-Anbindung 2. E-Mail und Kommunikation 3. Authentifizierung und Zugriffskontrolle

Priorität 2 (4-8 Stunden): 4. ERP-System (Auftragsabwicklung, Finanzen) 5. CRM-System (Kundenservice) 6. Produktionssteuerungssysteme

Priorität 3 (8-24 Stunden): 7. Weitere Geschäftsanwendungen 8. Entwicklungs- und Testumgebungen 9. Reporting und Analytics

9.6.2 6.2 Abhängigkeiten bei Wiederherstellung



9.7 7. Genehmigung und Freigabe

9.7.1 7.1 Freigabe durch Fachbereiche

Fachbereich	Verantwortlicher	Datum	Unterschrift
[TODO: Bereich 1]	[TODO: Name]	[TODO: Datum]	[TODO]
[TODO: Bereich 2]	[TODO: Name]	[TODO: Datum]	[TODO]

9.7.2 7.2 Management-Freigabe

Rolle	Name	Datum	Unterschrift
CEO	{{ meta.roles.ceo.name }}	[TODO: Datum]	[TODO]
CIO	{{ meta.roles.cio.name }}	[TODO: Datum]	[TODO]
BCM-Manager	[TODO: Name]	[TODO: Datum]	[TODO]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 10

Risikoanalyse und Szenarien

Dokument-ID: BCM-0090
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.document.last_updated }}

10.1 1. Ziel

Die Risikoanalyse der AdminSend GmbH dient der:

- **Identifikation** von Risiken, die die Geschäftskontinuität beeinträchtigen können
- **Bewertung** der Eintrittswahrscheinlichkeit und Auswirkungen
- **Behandlung** durch geeignete Maßnahmen (Vermeidung, Reduktion, Transfer, Akzeptanz)
- **Überwachung** und regelmäßigen Überprüfung der Risiken

Die Risikoanalyse ergänzt die Business Impact Analysis (BIA) und bildet die Grundlage für die BCM-Strategie.

10.2 2. Szenario-Katalog

10.2.1 2.1 IT- und Cyber-Risiken

2.1.1 Cyberangriff / Ransomware - **Beschreibung:** Verschlüsselung von Daten durch Ransomware, Erpressung - **Betroffene Services:** Alle IT-abhängigen Prozesse - **Typische Auswirkungen:** Datenverlust, Systemausfall, Erpressungszahlung - **Referenz:** BSI-Standard 200-4, Abschnitt Cyber-Resilience

2.1.2 Ausfall Rechenzentrum / Cloud-Region - **Beschreibung:** Komplettausfall des primären Rechenzentrums oder Cloud-Region - **Betroffene Services:** Alle IT-Services - **Typische Auswirkungen:** Totalausfall IT-Systeme, Datenzugriff nicht möglich

2.1.3 Netzwerkausfall / Internet-Ausfall - **Beschreibung:** Ausfall der Netzwerkinfrastruktur oder Internet-Anbindung - **Betroffene Services:** Alle netzwerkabhängigen Services - **Typische Auswirkungen:** Keine Kommunikation, kein Datenzugriff

2.1.4 Datenverlust / Backup-Ausfall - **Beschreibung:** Verlust kritischer Daten, Backup nicht wiederherstellbar - **Betroffene Services:** Datenabhängige Prozesse - **Typische Auswirkungen:** Permanenter Datenverlust, RPO-Überschreitung

10.2.2 2.2 Infrastruktur-Risiken

2.2.1 Stromausfall - **Beschreibung:** Ausfall der Stromversorgung am Standort - **Betroffene Services:** Alle stromabhängigen Systeme und Prozesse - **Typische Auswirkungen:** Produktionsausfall, IT-Ausfall, Gebäudetechnik-Ausfall

2.2.2 Brand - **Beschreibung:** Feuer im Gebäude oder Rechenzentrum - **Betroffene Services:** Alle Services am betroffenen Standort - **Typische Auswirkungen:** Standort nicht nutzbar, Sachschäden, Personengefährdung

2.2.3 Wasserschaden - **Beschreibung:** Überschwemmung, Rohrbruch, Löschwasser - **Betroffene Services:** Services am betroffenen Standort - **Typische Auswirkungen:** Gebäudeschäden, IT-Hardware-Schäden

2.2.4 Standort nicht zugänglich - **Beschreibung:** Evakuierung, Sperrung, Naturereignis - **Betroffene Services:** Alle standortabhängigen Prozesse - **Typische Auswirkungen:** Mitarbeiter können nicht arbeiten, Produktion steht still

10.2.3 2.3 Personal-Risiken

2.3.1 Personalausfall / Pandemie - **Beschreibung:** Krankheitswelle, Pandemie, Massenausfall - **Betroffene Services:** Personalintensive Prozesse - **Typische Auswirkungen:** Reduzierte Kapazität, Schlüsselpersonen nicht verfügbar

2.3.2 Ausfall Schlüsselpersonen - **Beschreibung:** Langfristiger Ausfall von Personen mit Spezialwissen - **Betroffene Services:** Prozesse mit Wissensabhängigkeiten - **Typische Auswirkungen:** Prozesse können nicht durchgeführt werden

10.2.4 2.4 Lieferanten-Risiken

2.4.1 Lieferantenausfall - **Beschreibung:** Kritischer Lieferant kann nicht liefern - **Betroffene Services:** Produktions- und Beschaffungsprozesse - **Typische Auswirkungen:** Produktionsstopp, Lieferengpässe

2.4.2 IT-Dienstleister-Ausfall - **Beschreibung:** Ausfall eines kritischen IT-Dienstleisters oder Cloud-Providers - **Betroffene Services:** Ausgelagerte IT-Services - **Typische Auswirkungen:** Service nicht verfügbar, keine Alternative

10.2.5 2.5 Naturereignisse und Umwelt

2.5.1 Unwetter / Sturm - **Beschreibung:** Schwere Unwetter, Sturm, Hagel - **Betroffene Services:** Standortabhängige Prozesse, Logistik - **Typische Auswirkungen:** Gebäudeschäden, Verkehrswege blockiert

2.5.2 Hochwasser - **Beschreibung:** Überschwemmung durch Fluss oder Starkregen - **Betroffene Services:** Standortabhängige Prozesse - **Typische Auswirkungen:** Standort überflutet, massive Sachschäden

2.5.3 Erdbeben (je nach Standort) - **Beschreibung:** Seismisches Ereignis - **Betroffene Services:** Alle Services am Standort - **Typische Auswirkungen:** Gebäudeschäden, Infrastrukturausfall

[TODO: Ergänzen oder streichen Sie Szenarien entsprechend Ihrer Standorte und Risiken]

10.3 3. Bewertungsmethodik

10.3.1 3.1 Bewertungsschema

Eintrittswahrscheinlichkeit (1-5): | Stufe | Bezeichnung | Beschreibung | Häufigkeit | |——-|———-|————-|————| | 5 | Sehr hoch | Tritt regelmäßig ein | Mehrmals pro Jahr | | 4 | Hoch | Tritt gelegentlich ein | Einmal pro Jahr | | 3 | Mittel | Kann eintreten | Einmal in 1-5 Jahren | | 2 | Niedrig | Unwahrscheinlich | Einmal in 5-10 Jahren | | 1 | Sehr niedrig | Sehr unwahrscheinlich | Seltener als alle 10 Jahre |

Auswirkung (1-5): | Stufe | Bezeichnung | Beschreibung | Finanzielle Auswirkung | |——-|———-|————-|———————-| | 5 | Katastrophal | Existenzbedrohend | > 1 Mio. € | | 4 | Sehr hoch | Massive Auswirkungen | 500.000 - 1 Mio. € | | 3 | Hoch | Erhebliche Auswirkungen | 100.000 - 500.000 € | | 2 | Mittel | Spürbare Auswirkungen | 10.000 - 100.000 € | | 1 | Niedrig | Geringe Auswirkungen | < 10.000 € |

Risiko-Score: - Risiko-Score = Eintrittswahrscheinlichkeit × Auswirkung - Wertebereich: 1-25

10.3.2 3.2 Risikotoleranz und Schwellwerte

[TODO: Definieren Sie Ihre Risikotoleranz]

Beispiel:

Risiko-Score	Risikostufe	Behandlung	Eskalation
15-25	Kritisch (Rot)	Sofortige Maßnahmen erforderlich	{{ meta.roles.ceo.name }}
10-14	Hoch (Orange)	Maßnahmen innerhalb 3 Monate	BCM-Manager
5-9	Mittel (Gelb)	Maßnahmen innerhalb 12 Monate	Fachbereich
1-4	Niedrig (Grün)	Überwachung, keine Maßnahmen	Fachbereich

10.3.3 3.3 Risikomatrix

```
Auswirkung

  5    10    15    20    25
```

```
    [Gelb] [Orange] [Rot]  [Rot]
4     8      12      16      20
    [Gelb] [Orange] [Orange] [Rot]
3     6      9       12      15
    [Gelb] [Gelb]  [Orange] [Orange]
2     4      6       8       10
    [Grün] [Gelb]  [Gelb]   [Orange]
1     2      3       4       5
    [Grün] [Grün]  [Grün]   [Gelb]

      1      2       3       4       5
             Wahrscheinlichkeit
```

10.4 4. Risikoregister

10.4.1 4.1 Bewertete Risiken

Risiko/Szenario	Betroffene Services	Wahrsch.	Auswirkung	Score	Risikostufe	Kontrollen (bestehend)	Maßnahmen (geplant)	Owner
[TODO: Risiko 1]	[TODO]	3	5	15	Orange	[TODO]	[TODO]	[TODO]

Beispiele:

Risiko/Szenario	Betroffene Services	Wahrsch.	Auswirkung	Score	Risikostufe	Kontrollen (bestehend)	Maßnahmen (geplant)	Owner
Ransomware-Angriff	Alle IT-Services	4	5	20	Rot	Firewall, AV, Backup	EDR, Segmentierung, Offline-Backup	{{ meta.roles.ciso.nam }}
Stromausfall	Produktion, IT	3	4	12	Orange	USV (15min)	Notstromgenerator	Facility-Manager
Personalausfall (Pandemie)	Alle Prozesse	2	4	8	Gelb	Home-Office möglich	Pandemieplan	HR
Lieferantenausfall	Produktion	3	3	9	Gelb	Lagerbestand (2 Wochen)	Zweitlieferant	Einkauf
Rechenzentrumsausfall	Alle IT-Services	2	5	10	Orange	Backup vorhanden	DR-Standort	{{ meta.roles.cio.name }}

10.4.2 4.2 Top-Risiken (Score 15)

[TODO: Listen Sie die Top-Risiken auf, die sofortige Maßnahmen erfordern]

1. **Ransomware-Angriff** (Score: 20)

- Maßnahmen: EDR-Implementierung, Netzwerksegmentierung, Offline-Backups
- Verantwortlich: {{ meta.roles.ciso.name }}
- Fällig: Q1 2026

2. [TODO: Weiteres Top-Risiko]

10.5 5. Risikobehandlung

10.5.1 5.1 Behandlungsstrategien

Risikovermeidung: - Aktivität wird nicht durchgeführt oder eingestellt - Beispiel: Verzicht auf Nutzung unsicherer Cloud-Services

Risikoreduktion: - Maßnahmen zur Reduktion von Wahrscheinlichkeit oder Auswirkung - Beispiel: Implementierung von Redundanzen, Backup-Strategien

Risikotransfer: - Übertragung des Risikos auf Dritte (Versicherung, Outsourcing) - Beispiel: Cyber-Versicherung, SLA mit Dienstleistern

Risikoakzeptanz: - Bewusste Akzeptanz des Restrisikos - Beispiel: Niedrige Risiken ohne Maßnahmen

10.5.2 5.2 Maßnahmenplan

Maßnahme	Risiko	Strategie	Beschreibung	Owner	Priorität	Kosten	Fällig	Status
[TODO: Maßnahme 1]	[TODO: Risiko]	Reduktion	[TODO: Beschreibung]	[TODO]	Hoch	[TODO]	[TODO]	Offen

Beispiele:

Maßnahme	Risiko	Strategie	Beschreibung	Owner	Priorität	Kosten	Fällig	Status
EDR-Implementierung	Ransomware	Reduktion	Endpoint Detection & Response auf allen Clients	{{ meta.roles.ciso.name }}	Hoch	50.000 €	Q1 2026	In Arbeit
Notstromgenerator	Stromausfall	Reduktion	Diesel-Generator für 48h Betrieb	Facility	Mittel	80.000 €	Q2 2026	Geplant
Cyber-Versicherung	Ransomware	Transfer	Versicherung für Cyber-Vorfälle	CFO	Hoch	20.000 €/Jahr	Q1 2026	Offen

10.6 6. Überwachung und Review

10.6.1 6.1 Risiko-Monitoring

Verantwortlich: BCM-Manager

Überwachungsintervall: - Quartalsweise Überprüfung des Risikoregisters - Ad-hoc bei neuen Bedrohungen oder Vorfällen - Jährliche vollständige Risikoanalyse

Indikatoren: - Neue Bedrohungen (z.B. neue Ransomware-Varianten) - Vorfälle bei vergleichbaren Organisationen - Änderungen in der Bedrohungslandschaft - Technologische Entwicklungen

10.6.2 6.2 Eskalation

Eskalationskriterien: - Neues Risiko mit Score 15 - Bestehend Risiko erhöht sich auf Score 15 - Risiko tritt ein (Incident)

Eskalationswege: - Score 15: Sofortige Meldung an {{ meta.roles.ceo.name }} - Score 10-14: Meldung an BCM-Manager - Score < 10: Dokumentation im Risikoregister

---

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 11

Strategie und Kontinuitaetsoptionen

Dokument-ID: BCM-0100
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

11.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

11.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

11.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

11.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

11.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

11.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

11.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

11.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 12

Aktivierungskriterien und Entscheidungsbaum

Dokument-ID: BCM-0110
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

12.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

12.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

12.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

12.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

12.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

12.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

12.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

12.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 13

Krisenmanagementplan

Dokument-ID: BCM-0120
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

13.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

13.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

13.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

13.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

13.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

13.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

13.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

13.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 14

Kommunikationsplan Intern Extern

Dokument-ID: BCM-0130
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

14.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

14.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

14.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

14.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

14.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

14.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

14.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

14.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 15

BCP Geschaeftsfortfuehrungsplan Template

Dokument-ID: BCM-0140
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

15.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

15.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

15.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

15.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

15.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

15.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

15.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

15.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 16

DRP IT Wiederanlaufplan Template

Dokument-ID: BCM-0150
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

16.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

16.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

16.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

16.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

16.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

16.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

16.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

16.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 17

Backup und Restore Plan

Dokument-ID: BCM-0160
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

17.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

17.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

17.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

17.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

17.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

17.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

17.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

17.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 18

Alternativstandort und Notfallarbeitsplaetze

Dokument-ID: BCM-0170
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

18.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

18.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

18.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

18.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

18.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

18.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

18.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

18.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 19

Lieferanten und Drittparteien Kontinuitaet

Dokument-ID: BCM-0180
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

19.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

19.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

19.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

19.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

19.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

19.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

19.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

19.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 20

Ressourcenplanung und Mindestbesetzung

Dokument-ID: BCM-0190
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

20.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

20.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

20.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

20.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

20.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

20.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

20.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

20.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 21

Notfallzugang BreakGlass

Dokument-ID: BCM-0200
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

21.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

21.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

21.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

21.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

21.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

21.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

21.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

21.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 22

Cyber Incident und Ransomware Playbook

Dokument-ID: BCM-0210
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

22.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

22.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

22.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

22.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

22.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

22.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

22.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

22.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 23

Uebungs und Testprogramm

Dokument-ID: BCM-0220
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

23.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

23.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

23.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

23.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

23.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

23.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

23.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

23.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 24

Testprotokoll und Erfolgskriterien

Dokument-ID: BCM-0230
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

24.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

24.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

24.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

24.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

24.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

24.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

24.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

24.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 25

Nachbereitung Postmortem

Dokument-ID: BCM-0240
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

25.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

25.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

25.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

25.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

25.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

25.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

25.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

25.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 26

Pflege Review und KPIs

Dokument-ID: BCM-0250
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

26.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

26.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

26.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

26.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

26.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

26.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

26.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

26.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 27

Schulungen und Sensibilisierung

Dokument-ID: BCM-0260
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

27.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

27.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

27.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

27.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

27.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

27.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

27.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

27.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 28

Compliance Audit und Nachweise

Dokument-ID: BCM-0270
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

28.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

28.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

28.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

28.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

28.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

28.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

28.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

28.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 29

Anhang Vorlagen und Checklisten

Dokument-ID: BCM-0280
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

29.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

29.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

29.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

29.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

29.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

29.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

29.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

29.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 30

Glossar und Abkuerzungen

Dokument-ID: BCM-0290
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

30.1 1. Zweck und Übersicht

[TODO: Beschreiben Sie den Zweck dieses Dokuments]

Dieses Dokument ist Teil des Business Continuity Management Systems (BCMS) der AdminSend GmbH.

30.2 2. Geltungsbereich

Dieses Dokument gilt für: - [TODO: Definieren Sie den Geltungsbereich]

30.3 3. Verantwortlichkeiten

Rolle	Verantwortlich	Aufgaben
BCM-Manager	[TODO]	Pflege und Aktualisierung dieses Dokuments
Fachbereich	[TODO]	Umsetzung der definierten Maßnahmen

30.4 4. Hauptinhalt

[TODO: Fügen Sie den spezifischen Inhalt für dieses Template ein]

30.4.1 4.1 Abschnitt 1

[TODO: Inhalt]

30.4.2 4.2 Abschnitt 2

[TODO: Inhalt]

30.5 5. Referenzen

- ISO 22301:2019 - Business Continuity Management Systems
- BSI-Standard 100-4 - Notfallmanagement
- Verwandte BCM-Dokumente: [TODO]

30.6 6. Anhänge

[TODO: Fügen Sie relevante Anhänge hinzu]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage