Contents

1 Business Continuity Management Handbook **6**

2 Purpose and Scope **7**
2.1 1. Purpose . . . 7
2.2 2. Scope . . . 8
2.3 3. Assumptions and Constraints . . . 9
2.4 4. Interfaces to Other Management Systems . . . 9

3 BCM Policy **11**
3.1 1. Policy Statement . . . 11
3.2 2. Objectives and Principles . . . 12
3.3 3. Scope . . . 13
3.4 4. Governance and Responsibilities . . . 13
3.5 5. Approvals and Authorizations . . . 14
3.6 6. Review and Update . . . 14

4 Document Control and Versioning **16**
4.1 1. Document Landscape . . . 16
4.2 2. Versioning . . . 17
4.3 3. Approval and Review Process . . . 18
4.4 4. Distribution and Access Rights . . . 19
4.5 5. Change Log (Changelog) . . . 19

5 Emergency Organization: Roles and Bodies **21**
5.1 1. Organizational Model . . . 21
5.2 2. Role Descriptions . . . 22
5.3 3. RACI Matrix Crisis Management . . . 24
5.4 4. Availability and On-Call . . . 24
5.5 5. Substitution Rules . . . 25

6 Contacts and Escalation **27**
6.1 1. Contact List (Internal) . . . 27
6.2 2. External Contacts . . . 28
6.3 3. Escalation Matrix . . . 30
6.4 4. Alerting Process . . . 31
6.5 5. On-Call and On-Call Duty . . . 32
6.6 6. Contact List Maintenance . . . 33

7 Service and Process Catalog with Criticality **34**
7.1 1. Objective . . . 34
7.2 2. Service and Process Catalog . . . 34
7.3 3. Criticality Assessment Criteria . . . 35
7.4 4. IT Services and Systems . . . 36
7.5 5. Dependency Analysis . . . 37
7.6 6. Stakeholder Overview . . . 38
7.7 7. Maintenance and Updates . . . 38

8 Business Impact Analysis (BIA) – Methodology **40**
8.1 1. Purpose and Output . . . 40
8.2 2. Approach and Methodology . . . 41
8.3 3. Assessment Dimensions . . . 42
8.4 4. Time Dependency of Impacts . . . 44
8.5 5. RTO/RPO Definition . . . 44
8.6 6. Results Approval . . . 45

9 BIA – Results and Target Values (RTO/RPO) **46**
9.1 1. Summary . . . 46
9.2 2. BIA Results Table . . . 47
9.3 3. Dependencies per Critical Process . . . 47
9.4 4. Manual Workarounds and Emergency Operations . . . 48
9.5 5. Open Items and Measures . . . 49
9.6 6. Recovery Prioritization . . . 49
9.7 7. Approval and Authorization . . . 50

10 Risk Analysis and Scenarios **52**
10.1 1. Objective . . . 52
10.2 2. Scenario Catalog . . . 52
10.3 3. Assessment Methodology . . . 54
10.4 4. Risk Register . . . 55
10.5 5. Risk Treatment . . . 56
10.6 6. Monitoring and Review . . . 56

11 Strategy and Continuity Options **58**
11.1 1. Purpose and Overview . . . 58
11.2 2. Scope . . . 58
11.3 3. Responsibilities . . . 58
11.4 4. Main Content . . . 58
11.5 5. References . . . 59
11.6 6. Appendices . . . 59

12 Activation Criteria and Decision Tree **60**
12.1 1. Purpose and Overview . . . 60
12.2 2. Scope . . . 60
12.3 3. Responsibilities . . . 60
12.4 4. Main Content . . . 60
12.5 5. References . . . 61
12.6 6. Appendices . . . 61

13 Crisis Management Plan **62**
13.1 1. Purpose and Overview . . . 62
13.2 2. Scope . . . 62
13.3 3. Responsibilities . . . 62
13.4 4. Main Content . . . 62
13.5 5. References . . . 63
13.6 6. Appendices . . . 63

14 Communication Plan Internal External **64**
14.1 1. Purpose and Overview . . . 64
14.2 2. Scope . . . 64
14.3 3. Responsibilities . . . 64
14.4 4. Main Content . . . 65
14.5 5. References . . . 65
14.6 6. Appendices . . . 65

15 BCP Business Continuity Plan Template **66**
15.1 1. Purpose and Overview . . . 66
15.2 2. Scope . . . 66
15.3 3. Responsibilities . . . 66
15.4 4. Main Content . . . 67
15.5 5. References . . . 67
15.6 6. Appendices . . . 67

16 DRP IT Recovery Plan Template **68**
16.1 1. Purpose and Overview . . . 68
16.2 2. Scope . . . 68
16.3 3. Responsibilities . . . 68
16.4 4. Main Content . . . 68
16.5 5. References . . . 69
16.6 6. Appendices . . . 69

17 Backup and Restore Plan **70**
17.1 1. Purpose and Overview . . . 70
17.2 2. Scope . . . 70
17.3 3. Responsibilities . . . 70
17.4 4. Main Content . . . 70
17.5 5. References . . . 71
17.6 6. Appendices . . . 71

18 Alternative Site and Emergency Workplaces **72**
18.1 1. Purpose and Overview . . . 72
18.2 2. Scope . . . 72
18.3 3. Responsibilities . . . 72
18.4 4. Main Content . . . 73
18.5 5. References . . . 73
18.6 6. Appendices . . . 73

19 Suppliers and Third Parties Continuity **74**

19.1 1. Purpose and Overview . . . 74
19.2 2. Scope . . . 74
19.3 3. Responsibilities . . . 74
19.4 4. Main Content . . . 75
19.5 5. References . . . 75
19.6 6. Appendices . . . 75

20 Resource Planning and Minimum Staffing **76**
20.1 1. Purpose and Overview . . . 76
20.2 2. Scope . . . 76
20.3 3. Responsibilities . . . 76
20.4 4. Main Content . . . 77
20.5 5. References . . . 77
20.6 6. Appendices . . . 77

21 Emergency Access BreakGlass **78**
21.1 1. Purpose and Overview . . . 78
21.2 2. Scope . . . 78
21.3 3. Responsibilities . . . 78
21.4 4. Main Content . . . 78
21.5 5. References . . . 79
21.6 6. Appendices . . . 79

22 Cyber Incident and Ransomware Playbook **80**
22.1 1. Purpose and Overview . . . 80
22.2 2. Scope . . . 80
22.3 3. Responsibilities . . . 80
22.4 4. Main Content . . . 81
22.5 5. References . . . 81
22.6 6. Appendices . . . 81

23 Exercise and Test Program **82**
23.1 1. Purpose and Overview . . . 82
23.2 2. Scope . . . 82
23.3 3. Responsibilities . . . 82
23.4 4. Main Content . . . 82
23.5 5. References . . . 83
23.6 6. Appendices . . . 83

24 Test Protocol and Success Criteria **84**
24.1 1. Purpose and Overview . . . 84
24.2 2. Scope . . . 84
24.3 3. Responsibilities . . . 84
24.4 4. Main Content . . . 84
24.5 5. References . . . 85
24.6 6. Appendices . . . 85

25 Post Incident Review Postmortem **86**
25.1 1. Purpose and Overview . . . 86

25.2 2. Scope . . . 86
25.3 3. Responsibilities . . . 86
25.4 4. Main Content . . . 86
25.5 5. References . . . 87
25.6 6. Appendices . . . 87

26 Maintenance Review and KPIs **88**
26.1 1. Purpose and Overview . . . 88
26.2 2. Scope . . . 88
26.3 3. Responsibilities . . . 88
26.4 4. Main Content . . . 88
26.5 5. References . . . 89
26.6 6. Appendices . . . 89

27 Training and Awareness **90**
27.1 1. Purpose and Overview . . . 90
27.2 2. Scope . . . 90
27.3 3. Responsibilities . . . 90
27.4 4. Main Content . . . 90
27.5 5. References . . . 91
27.6 6. Appendices . . . 91

28 Compliance Audit and Evidence **92**
28.1 1. Purpose and Overview . . . 92
28.2 2. Scope . . . 92
28.3 3. Responsibilities . . . 92
28.4 4. Main Content . . . 92
28.5 5. References . . . 93
28.6 6. Appendices . . . 93

29 Appendix Templates and Checklists **94**
29.1 1. Purpose and Overview . . . 94
29.2 2. Scope . . . 94
29.3 3. Responsibilities . . . 94
29.4 4. Main Content . . . 94
29.5 5. References . . . 95
29.6 6. Appendices . . . 95

30 Glossary and Abbreviations **96**
30.1 1. Purpose and Overview . . . 96
30.2 2. Scope . . . 96
30.3 3. Responsibilities . . . 96
30.4 4. Main Content . . . 96
30.5 5. References . . . 97
30.6 6. Appendices . . . 97

Chapter 1

Business Continuity Management Handbook

Document Metadata

- **Created on:** 2026-02-05
- **Author:** Andreas Huemmer [andreas.huemmer@adminsend.de]
- **Version:** 0.0.2
- **Type:** BCM Handbook

---

ewpage

Chapter 2

Purpose and Scope

Document ID: BCM-0010
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

2.1 1. Purpose

The Business Continuity Management System (BCMS) of AdminSend GmbH serves the following purposes:

- **Protection of critical business processes:** Ensuring the continuation of business-critical activities even during severe disruptions
- **Reduction of downtime:** Minimizing the impact of interruptions on business operations, customers, and stakeholders
- **Fulfillment of regulatory requirements:** Demonstrating compliance with legal and contractual obligations
- **Crisis response capability:** Establishing structured processes for managing emergencies and crises
- **Continuous improvement:** Systematic development of business continuity capabilities

2.1.1 1.1 Strategic Objectives

The BCMS pursues the following strategic objectives:

- Defined **Recovery Time Objectives (RTO)** and **Recovery Point Objectives (RPO)** for all critical processes
- Building and maintaining **crisis response capability** at all organizational levels
- **Demonstrability** of business continuity measures to regulatory authorities, customers, and partners

- **Protection of reputation** and stakeholder trust
- **Minimization of financial losses** due to business interruptions

2.1.2 1.2 Standards References

This BCMS is based on the following standards and 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** - Emergency Management
- **BSI Standard 200-4** - Business Continuity Management

2.2 2. Scope

2.2.1 2.1 Organizational Units

The BCMS applies to the following organizational units of AdminSend GmbH:

[TODO: Define the included organizational units]

Example: - Executive Management - IT Department - Production - Sales and Marketing - Finance and Controlling - Human Resources

2.2.2 2.2 Locations

The BCMS covers the following locations:

[TODO: List all locations within scope]

Example: - Headquarters: Musterstraße 123, 80331 München - Production site: [Address] - Data center: [Address] - Alternate site: [Address]

2.2.3 2.3 Services and Processes

The BCMS covers the following critical services and business processes:

[TODO: Define critical services and processes]

Example: - Customer service and support - Production control - Order processing - Financial processes (payment transactions, accounting) - IT services (email, ERP system, production systems)

2.2.4 2.4 IT and OT Systems

The BCMS includes the following IT and OT systems:

[TODO: List critical IT and OT systems]

Example: - ERP system - CRM system - Email and collaboration platform - Production control systems (SCADA, MES) - Network infrastructure - Backup and recovery systems

2.2.5 2.5 Exceptions and Exclusions

The following areas are explicitly excluded from scope:

[TODO: Document exceptions with justification and approving authority]

Example: - **Subsidiary XY:** Operates its own BCMS (Approved by: {{ meta.roles.ceo.name }}) - **Development environments:** Not business-critical (Approved by: {{ meta.roles.cio.name }})

2.3 3. Assumptions and Constraints

2.3.1 3.1 Basic Assumptions

The BCMS is based on the following assumptions:

[TODO: Define the basic assumptions for your BCMS]

Example: - Maximum personnel loss: Up to 30% of workforce simultaneously unavailable - Recovery of critical IT systems: Possible within 24 hours - Availability of alternate sites: Accessible within 4 hours - Supply chains: Critical suppliers have implemented their own BCM measures - External support: Emergency services (fire department, police) are available

2.3.2 3.2 Dependencies Outside Control

The following dependencies are outside the organization's direct control:

[TODO: Identify external dependencies]

Example: - Availability of public infrastructure (electricity, water, telecommunications) - Availability of cloud service providers - Delivery capability of critical suppliers - Availability of emergency services - Political and regulatory framework conditions

2.4 4. Interfaces to Other Management Systems

2.4.1 4.1 Information Security Management System (ISMS)

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

Interfaces: - Incident management and security incident response - IT emergency plans and disaster recovery - Risk management and risk analysis - Access control and emergency access (break-glass)

[TODO: Describe the specific interfaces to your ISMS]

2.4.2 4.2 IT Service Management (ITSM)

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

Interfaces: - Incident management (major incidents → BCM activation) - Change management (emergency changes) - Problem management (post-incident reviews) - Service level management (SLA definitions)

[TODO: Describe the specific interfaces to your ITSM]

2.4.3 4.3 Data Protection and Compliance

Responsible: [TODO: Data Protection Officer]

Interfaces: - Data protection impact assessments (DPIA) for BCM measures - Reporting obligations for data protection incidents - Retention periods for BCM documentation - Compliance evidence for regulatory authorities

[TODO: Describe the specific interfaces to data protection]

2.4.4 4.4 Risk Management

Responsible: [TODO: Risk Manager]

Interfaces: - Enterprise-wide risk management - Business impact analysis (BIA) - Risk analysis and risk assessment - Risk mitigation measures

[TODO: Describe the specific interfaces to risk management]

2.4.5 4.5 Crisis Communication and Public Relations

Responsible: [TODO: Communications Manager]

Interfaces: - Internal crisis communication - External crisis communication (media, customers, partners) - Stakeholder management - Reputation protection

[TODO: Describe the specific interfaces to crisis communication]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 3

BCM Policy

Document ID: BCM-0020
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

3.1 1. Policy Statement

The management of AdminSend GmbH commits to the implementation and continuous improvement of a Business Continuity Management System (BCMS) in accordance with **ISO 22301:2019**.

3.1.1 1.1 Management Commitment

The management, represented by **{{ meta.roles.ceo.name }}** (CEO), hereby declares:

- **Highest priority:** Business continuity has strategic importance for protecting our organization, employees, customers, and stakeholders
- **Resource provision:** Adequate financial, personnel, and technical resources are provided for the BCMS
- **Leadership responsibility:** Management assumes overall responsibility for the BCMS and its effectiveness
- **Continuous improvement:** The BCMS is regularly reviewed and continuously improved

3.1.2 1.2 BCMS Principles

The BCMS of AdminSend GmbH is based on the following principles:

1. **Risk-based approach:** Identification, assessment, and treatment of risks to business continuity

2. **Continuous improvement:** Systematic development of BCM capabilities through exercises, tests, and lessons learned
3. **Accountability:** Clear assignment of roles and responsibilities at all organizational levels
4. **Exercise and testing:** Regular exercises and tests to validate BCM measures
5. **Documentation and traceability:** Complete documentation of all BCM activities and decisions
6. **Compliance:** Adherence to all relevant legal, regulatory, and contractual requirements

3.1.3 1.3 Commitments

AdminSend GmbH commits to:

- **Protection of human life:** Safety and well-being of employees, customers, and visitors have top priority
- **Business continuity:** Maintaining critical business processes even during severe disruptions
- **Stakeholder communication:** Transparent and timely communication with all affected stakeholders
- **Supplier management:** Ensuring business continuity capabilities of critical suppliers
- **Compliance and evidence:** Fulfilling all relevant requirements and providing evidence

3.2 2. Objectives and Principles

3.2.1 2.1 Strategic BCM Objectives

AdminSend GmbH pursues the following strategic BCM objectives:

Objective 1: Minimization of Downtime - Recovery of critical business processes within defined Recovery Time Objectives (RTO) - Limitation of data loss within defined Recovery Point Objectives (RPO) - Measurable reduction of average recovery time by [TODO: X%] per year

Objective 2: Crisis Response Capability - Establishment of 24/7 crisis organization with clear escalation paths - Training of all employees in BCM basics and emergency behavior - Conducting at least [TODO: X] BCM exercises per year

Objective 3: Compliance and Demonstrability - Fulfillment of all regulatory requirements for business continuity - Provision of complete evidence for audits and certifications - Maintenance of ISO 22301 certification (if pursued)

Objective 4: Stakeholder Trust - Transparent communication of BCM capabilities to customers and partners - Demonstration of business continuity capabilities in tenders and contracts - Protection of reputation and brand value

Objective 5: Continuous Improvement - Systematic evaluation of exercises, tests, and real incidents - Implementation of lessons learned and best practices - Regular updates of BCM documentation and plans

3.2.2 2.2 Operational Principles

Principle 1: Safety First - Human life and health always take precedence over material values - In emergencies: First bring people to safety, then minimize property damage

Principle 2: Communication Before Action - Structured communication and coordination before uncoordinated individual actions - Clear chains of command and escalation paths in crises

Principle 3: Documentation and Traceability - All decisions and measures are documented - Traceability for post-incident reviews and audits

Principle 4: Flexibility and Adaptability - BCM plans are guidelines, not rigid requirements - Situation-appropriate adaptation of measures is allowed and desired

3.3 3. Scope

The scope of the BCMS is defined in:

→ **See document:** `0010_Purpose_and_Scope.md`

The BCMS covers all critical business processes, IT systems, and locations of AdminSend GmbH according to the scope defined in the scope document.

3.4 4. Governance and Responsibilities

3.4.1 4.1 RACI Matrix BCM Governance

Activity	CEO	CIO	CISO	BCM Manager	Department	IT Ops
Approve BCM policy	**A**	C	C	R	I	I
Define BCM strategy	**A**	R	C	R	C	I
Approve BCM budget	**A**	C	I	R	I	I
Conduct BIA	I	C	I	**A**	R	C
Create BCM plans	I	C	C	**A**	R	R
Conduct BCM exercises	I	C	C	**A**	R	R
Activate crisis	**A**	R	R	R	I	I
Management review	**A**	R	C	R	I	I

Legend: - **R** = Responsible (execution responsibility) - **A** = Accountable (overall responsibility, decision authority) - **C** = Consulted (consulted, subject matter expertise) - **I** = Informed (informed)

3.4.2 4.2 Roles and Responsibilities

Executive Management (CEO) - **Responsible:** {{ meta.roles.ceo.name }} ({{ meta.roles.ceo.email }}) - **Tasks:** Overall responsibility for BCMS, approval of BCM policy, release of resources, crisis activation

Chief Information Officer (CIO) - **Responsible:** {{ meta.roles.cio.name }} ({{ meta.roles.cio.email }}) - **Tasks:** Responsibility for IT continuity, IT disaster recovery, technical BCM measures

Chief Information Security Officer (CISO) - **Responsible:** {{ meta.roles.ciso.name }} ({{ meta.roles.ciso.email }}) - **Tasks:** ISMS-BCMS interface, security incident response, cyber resilience

BCM Manager - **Responsible:** [TODO: BCM Manager name and contact] - **Tasks:** Operational management of BCMS, coordination of BIA and risk analysis, BCM exercises, maintenance of BCM documentation

Departments - **Responsible:** Respective department heads - **Tasks:** Identification of critical processes, participation in BIA, creation of functional BCM plans, participation in exercises

IT Operations - **Responsible:** {{ meta.roles.it_operations_manager.name }} ({{ meta.roles.it_operations_mar }}) - **Tasks:** Implementation of technical BCM measures, IT disaster recovery, backup and restore

3.5 5. Approvals and Authorizations

This BCM policy has been reviewed and approved by:

Role	Name	Function	Date	Signature/Approval
Executive Management	{{ meta.roles.ceo.name }}	CEO	[TODO: Date]	[TODO: Signature]
BCM Owner	[TODO: BCM Manager]	BCM Manager	[TODO: Date]	[TODO: Signature]
IT Management	{{ meta.roles.cio.name }}	CIO	[TODO: Date]	[TODO: Signature]
Information Security	{{ meta.roles.ciso.name }}	CISO	[TODO: Date]	[TODO: Signature]
Compliance	[TODO: Compliance Officer]	Compliance Officer	[TODO: Date]	[TODO: Signature]

3.6 6. Review and Update

This BCM policy is:

- **Annually** reviewed by management as part of the management review
- Updated when **significant changes** occur in the organization, business processes, or regulatory requirements
- Reviewed for adaptation needs after **severe incidents** or exercises

Next planned review: [TODO: Date]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initial creation

ewpage

Chapter 4

Document Control and Versioning

Document ID: BCM-0030
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

4.1 1. Document Landscape

4.1.1 1.1 BCM Document Structure

The BCM documentation of AdminSend GmbH includes the following document types:

Strategic Documents: - BCM policy and guidelines - BCM strategy and objectives - Scope and boundaries

Operational Documents: - Business Impact Analysis (BIA) - Risk analysis and scenarios - Business Continuity Plans (BCP) - IT Disaster Recovery Plans (DRP) - Crisis management plans

Supporting Documents: - Contact lists and escalation matrices - Runbooks and checklists - Test protocols and exercise reports - Training materials

4.1.2 1.2 Document Repository

Primary Repository: [TODO: Define the primary document management system]

Example: - **System:** SharePoint / Confluence / Document Management System - **Path:** `BCM/Documentation/` - **Access:** Role-based (RBAC) according to authorization concept - **Backup:** Daily backup, 30-day retention

Offline Availability / Emergency Access:

Critical BCM documents must be available even when IT systems fail:

[TODO: Define offline access options]

Example: - **Emergency USB drives:** Encrypted USB drives with current BCM plans held by crisis team members - **Paper printouts:** Sealed emergency binders at defined locations (safe, alternate site) - **Cloud backup:** Access via mobile devices even when main site fails - **Update:** Quarterly or upon significant changes

4.1.3 1.3 Document Register

Document ID	Document Name	Version	Owner	Classification	Location
BCM-0010	Purpose and Scope	1.0.0	IT Operations Manager	internal	[TODO: Path]
BCM-0020	BCM Policy	1.0.0	IT Operations Manager	internal	[TODO: Path]
BCM-0030	Document Control	1.0.0	IT Operations Manager	internal	[TODO: Path]
…	…	…	…	…	…

[TODO: Complete the document register]

4.2 2. Versioning

4.2.1 2.1 Versioning Scheme

AdminSend GmbH uses the following versioning scheme for BCM documents:

Format: `MAJOR.MINOR.PATCH`

Example: Version 2.3.1

- **MAJOR (2):** Significant content changes, new structure, new requirements
- **MINOR (3):** Additions, updates without fundamental changes
- **PATCH (1):** Corrections, formatting, editorial changes

4.2.2 2.2 Version Increment

Increment MAJOR version for: - Fundamental restructuring of the document - Significant changes to BCM strategy or processes - New regulatory requirements - Changes to scope

Increment MINOR version for: - Addition of new sections or processes - Update of contact data or roles - Adaptation to organizational changes - Results from exercises or tests

Increment PATCH version for: - Spelling corrections - Formatting changes - Update of references - Editorial adjustments

4.2.3 2.3 Version Status

Status	Description	Usage
Draft	Document in creation	Visible only to authors
In Review	Document under review	Visible to reviewers
Approved	Document approved and active	Visible to all authorized users
Archived	Document obsolete, historical	For archival purposes only

4.3 3. Approval and Review Process

4.3.1 3.1 Roles in Document Process

Author (Creator): - **Responsible:** Subject matter expert or BCM manager - **Tasks:** Creation and maintenance of document content

Reviewer: - **Responsible:** Subject matter experts, affected stakeholders - **Tasks:** Content review, feedback, approval recommendation

Approver: - **Responsible:** CIO or delegated manager - **Tasks:** Formal approval, assumption of responsibility

4.3.2 3.2 Approval Process

1. **Creation:** Author creates document in "Draft" status
2. **Review:** Document is submitted to reviewers for review (Status: "In Review")
3. **Revision:** Author incorporates feedback
4. **Approval:** Approver releases document (Status: "Approved")
5. **Publication:** Document is made available to target audience
6. **Archiving:** Old version is archived

4.3.3 3.3 Review Intervals

Document Type	Review Interval	Responsible
BCM Policy	Annually	{{ meta.roles.ceo.name }}
BIA Results	Annually	BCM Manager
BCM Plans (BCP/DRP)	Semi-annually	Subject matter experts
Contact Lists	Quarterly	BCM Manager
Runbooks	After each exercise	IT Operations

Event-driven Reviews: - After severe incidents - Upon organizational changes - Upon changes to regulatory requirements - After audits or certifications

4.4 4. Distribution and Access Rights

4.4.1 4.1 Target Audiences

Crisis Team: - Access to all BCM documents - Offline copies of critical plans - Notification of changes

IT Operations: - Access to IT DR plans and runbooks - Technical documentation - Contact lists

Departments: - Access to relevant BCP plans - Process-specific runbooks - Training materials

External Service Providers: - Access to relevant excerpts (NDA required) - No access to confidential contact data - Only approved versions

4.4.2 4.2 Access Control (RBAC)

[TODO: Define role-based access rights]

Example:

Role	Read	Write	Approve	Delete
BCM Manager				
Crisis Team		-	-	-
Department	(own plans)	(own plans)	-	-
IT Operations	(IT plans)	(IT plans)	-	-
External	(approved)	-	-	-

4.4.3 4.3 Protection Requirements and Classification

Classification	Description	Example Documents
Public	No protection required	BCM Policy (external)
Internal	For employees only	BCM handbook, training materials
Confidential	Restricted group	BIA results, contact lists
Strictly Confidential	Crisis team only	Emergency access, passwords

4.5 5. Change Log (Changelog)

4.5.1 5.1 Document History

Version	Date	Change	Author	Reviewer	Approved by
0.1	{{ meta.document_last_updated }}	Initial creation	{{ meta.defaults.author }}	[TODO]	[TODO]

[TODO: Update the change log with each document change]

4.5.2 5.2 Change Requests

Change requests for BCM documents can be submitted through:

- **Email to:** [TODO: BCM Manager email]
- **Ticketing system:** [TODO: System and category]
- **Form:** [TODO: Link to change request form]

Each change request is reviewed and prioritized. Processing follows defined SLAs.

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.document.author | default }}	Initial creation

ewpage

Chapter 5

Emergency Organization: Roles and Bodies

Document ID: BCM-0040
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

5.1 1. Organizational Model

5.1.1 1.1 Emergency Organization Structure

The emergency organization of AdminSend GmbH consists of the following levels:

```
      Crisis Team (Strategic)
   Lead: {{ meta.roles.ceo.name }}
```

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

Level 1: Crisis Team (Strategic Level) - Strategic decisions and overall coordination - Activation during severe incidents - Communication with external stakeholders

Level 2: BCM Manager / Coordination (Tactical Level) - Operational coordination of BCM measures - Interface between crisis team and operational teams - Documentation and reporting

Level 3: Operational Teams (Operational Level) - IT-DR Team: IT systems recovery - Department BCP Teams: Business process recovery - Support Teams: Logistics, communication, HR

5.1.2 1.2 Organization Chart

[TODO: Insert detailed organization chart]

Reference: See `diagrams/bcm_organization.png`

5.2 2. Role Descriptions

5.2.1 2.1 Crisis Team Lead

Role: Crisis Team Lead / Crisis Management Team Lead

Responsible: {{ meta.roles.ceo.name }}
Deputy: {{ meta.roles.coo.name }}
Contact: {{ meta.roles.ceo.email }} / {{ meta.roles.ceo.phone }}

Tasks: - Overall responsibility for crisis management and BCM activation - Strategic decisions on resource deployment and prioritization - Approval of communication to external stakeholders - Decision on activation of alternate sites - Approval of extraordinary measures and budgets

Decision Authority: - Activation and deactivation of crisis team - Approval of emergency budgets up to [TODO: Amount] - Decision on business continuation or cessation - Approval of emergency access (break-glass)

Reporting Obligations: - To supervisory board / shareholders during severe crises - To regulatory authorities according to regulatory requirements

5.2.2 2.2 BCM Manager / BCM Coordinator

Role: BCM Manager / Business Continuity Coordinator

Responsible: [TODO: BCM Manager Name]
Deputy: [TODO: Deputy]
Contact: [TODO: Email / Phone]

Tasks: - Operational management of BCMS in normal operations - Coordination of BIA, risk analysis, and BCM planning - Organization and execution of BCM exercises and tests - Maintenance of BCM documentation and contact lists - Training and awareness of employees - Reporting to management and crisis team

Reporting: - Quarterly BCM status reports to {{ meta.roles.ceo.name }} - Ad-hoc reporting for critical events - Annual BCM report

Interfaces: - ISMS / CISO: {{ meta.roles.ciso.name }} - IT Operations: {{ meta.roles.it_operations_manager.nam
}} - Departments: Respective department heads

5.2.3 2.3 Incident Commander / Operational Lead

Role: Incident Commander / Operational Lead

Responsible: [TODO: Incident Commander Name]
Deputy: [TODO: Deputy]
Contact: [TODO: Email / Phone]

Tasks: - Operational management of emergency measures on-site - Coordination of operational teams (IT-DR, BCP teams) - Situation assessment and status reporting to crisis team - Implementation of measures decided by crisis team - Documentation of all measures and decisions

Interface to ITSM/Incident: - Takeover of major incidents from ITSM process - Escalation to crisis team when defined thresholds exceeded - Return to ITSM process after stabilization

Decision Authority: - Operational measures without budget overrun - Prioritization of recovery measures - Request for additional resources

5.2.4 2.4 Communication / Spokesperson Role

Role: Crisis Communication / Spokesperson

Responsible: [TODO: Communications Manager]
Deputy: [TODO: Deputy]
Contact: [TODO: Email / Phone]

Tasks: - Internal crisis communication (employees, management) - External crisis communication (media, customers, partners, authorities) - Creation and approval of press releases - Social media monitoring and response - Stakeholder management

Approval Processes: - Internal communication: Approval by crisis team lead - External communication: Approval by {{ meta.roles.ceo.name }} - Press releases: Approval by management and legal department if applicable

Communication Channels: - Internal: Email, intranet, employee app, phone - External: Website, social media, press releases, customer hotline

5.2.5 2.5 IT-DR Lead

Role: IT Disaster Recovery Lead

Responsible: {{ meta.roles.it_operations_manager.name }}
Deputy: [TODO: Deputy]
Contact: {{ meta.roles.it_operations_manager.email }} / {{ meta.roles.it_operations_manager.phone }}

Tasks: - Leadership of IT-DR team - Coordination of IT recovery measures - Implementation of IT disaster recovery plans - Prioritization of system recovery according to BIA - Status reporting to incident commander and crisis team

Runbooks and Recovery Coordination: - Management and maintenance of IT-DR runbooks - Coordination of system recovery in defined sequence - Execution of restore tests - Documentation of recovery measures

Interfaces: - IT operations team - External IT service providers and cloud providers - Departments (for system approvals)

5.3 3. RACI Matrix Crisis Management

Activity	Crisis Team Lead	BCM Manager	Incident Commander	IT-DR Lead	Department	Communication
Activate crisis	**A**	R	C	I	I	I
Situation assessment	C	C	**A/R**	C	C	I
Strategic decisions	**A**	C	C	I	C	C
Operational measures	I	C	**A**	R	R	I
IT recovery	I	C	C	**A/R**	C	I
BCP implementation	I	C	C	C	**A/R**	I
Internal communication	A	C	C	I	I	**R**
External communication	**A**	C	I	I	I	**R**
Documentation	I	**A**	R	R	R	R
End crisis	**A**	R	C	C	C	I

Legend: - **R** = Responsible (execution responsibility) - **A** = Accountable (overall responsibility, decision authority) - **C** = Consulted (consulted, subject matter expertise) - **I** = Informed (informed)

5.4 4. Availability and On-Call

5.4.1 4.1 On-Call Models

[TODO: Define on-call models for critical roles]

Example:

Crisis Team: - **Availability:** 24/7 via mobile phone - **Response time:** Ready within 2 hours - **On-call schedule:** Rotating model, quarterly updates

IT-DR Team: - **Availability:** 24/7 on-call - **Response time:** Ready within 1 hour - **On-call schedule:** Weekly rotation

BCM Manager: - **Availability:** Business days 08:00-18:00, outside via mobile phone - **Response time:** Ready within 4 hours

5.4.2 4.2 Escalation Times

Severity	Response Time	Escalate to	Escalation Time
Low	4 hours	IT Operations	-
Medium	2 hours	Incident Commander	After 4 hours
High	1 hour	Crisis Team	After 2 hours
Critical	Immediate	Crisis Team Lead	Immediate

5.4.3 4.3 Alerting Process

[TODO: Describe the alerting process]

Example: 1. **Initial detection:** Incident detected (monitoring, report, etc.) 2. **Initial assessment:** IT operations assesses severity 3. **Alerting:** For major incident → Alert incident commander 4. **Escalation:** For BCM activation → Alert crisis team 5. **Confirmation:** All alerted persons confirm receipt

Alerting Channels: - Primary: Phone (mobile phone) - Secondary: SMS / Messenger - Tertiary: Email

5.5 5. Substitution Rules

5.5.1 5.1 Deputy Lists

Deputies are defined for all critical roles:

Role	Primary	Deputy 1	Deputy 2
Crisis Team Lead	{{ 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]
Communication	[TODO]	[TODO]	[TODO]

5.5.2 5.2 Handover Process

During substitution or shift change, a structured handover occurs:

Handover Contents: - Current situation status - Ongoing measures and their status - Open decisions and escalations - Critical information and contacts

Handover Documentation: - Handover protocol (Template: [TODO: Link]) - Logbook entry - Briefing of successor

---

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 6

Contacts and Escalation

Document ID: BCM-0050
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: Confidential
Last Updated: {{ meta.document.last_updated }}

6.1 1. Contact List (Internal)

> **Attention:** Contact lists contain personal data and are subject to special data protection requirements (GDPR). Access only for authorized persons. Quarterly updates required.

6.1.1 1.1 Crisis Team

Function	Name	Phone	Mobile	Email	Deputy
Crisis Team Lead	{{ meta.roles.ceo.name }}	{{ meta.roles.ceo.phone }}	[TODO: Mobile]	{{ meta.roles.ceo.email }}	{{ meta.roles.coo.name }}
CIO	{{ meta.roles.cio.name }}	{{ meta.roles.cio.phone }}	[TODO: Mobile]	{{ meta.roles.cio.email }}	[TODO]
CISO	{{ meta.roles.ciso.name }}	{{ meta.roles.ciso.phone }}	[TODO: Mobile]	{{ meta.roles.ciso.email }}	[TODO]
CFO	{{ meta.roles.cfo.name }}	{{ meta.roles.cfo.phone }}	[TODO: Mobile]	{{ meta.roles.cfo.email }}	[TODO]

Function	Name	Phone	Mobile	Email	Deputy
COO	{{ meta.roles.coo.name }}	{{ meta.roles.coo.phone }}	[TODO: Mobile]	{{ meta.roles.coo.email }}	[TODO]

6.1.2 1.2 BCM Organization

Function	Name	Phone	Mobile	Email	Deputy
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]
Communication	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

6.1.3 1.3 IT Operations and Service Desk

Function	Name	Phone	Mobile	Email	Availability
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 on-call
Network Team	[TODO]	[TODO]	[TODO]	[TODO]	24/7 on-call
Server Team	[TODO]	[TODO]	[TODO]	[TODO]	24/7 on-call
Security Team	[TODO]	[TODO]	[TODO]	[TODO]	24/7 on-call

6.1.4 1.4 Departments

Department	Contact Person	Phone	Mobile	Email	Deputy
Production	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
Sales	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
Finance	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
HR	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
Procurement	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

6.2 2. External Contacts

6.2.1 2.1 IT Service Providers and Providers

Organization	Role/Service	Contact	Phone	Email	Contract/Customer No.	Availability
[TODO: Cloud Provider]	Cloud Infrastructure	[TODO]	[TODO]	[TODO]	[TODO]	24/7
[TODO: ISP]	Internet Connection	[TODO]	[TODO]	[TODO]	[TODO]	24/7
[TODO: Telco]	Telephony	[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 Emergency Services and Authorities

Organization	Purpose	Phone	Emergency Number	Address
Fire Department	Fire, hazardous materials	[TODO: Local]	**112**	[TODO]
Police	Security, crimes	[TODO: Local]	**110**	[TODO]
Emergency Medical Services	Medical emergencies	[TODO: Local]	**112**	[TODO]
Poison Control	Hazardous material accidents	[TODO: Regional]	[TODO]	[TODO]
BSI	Cyber incidents	+49 228 99 9582-222	-	Godesberger Allee 185-189, 53175 Bonn

6.2.3 2.3 Critical Suppliers

Supplier	Product/Service	Contact Person	Phone	Email	Criticality
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	High / Medium / Low

6.2.4 2.4 Customers and Partners (if needed)

Organization	Contact Person	Phone	Email	Notify when
[TODO: Major Customer]	[TODO]	[TODO]	[TODO]	Service outage > 4h

6.3 3. Escalation Matrix

6.3.1 3.1 Escalation Levels

Level	Designation	Trigger	Responsible	Response Time	Communication Obligation
1	Disruption	Individual systems affected, no impact on critical services	IT Operations	4 hours	Inform service desk
2	Major Incident	Critical service impaired, RTO at risk	Incident Commander	1 hour	Inform management
3	BCM Activation	Multiple critical services failed, business operations at risk	Crisis Team	30 minutes	Activate crisis team, inform external stakeholders
4	Disaster	Site unavailable, massive impact	Crisis Team Lead	Immediate	All stakeholders, authorities, media

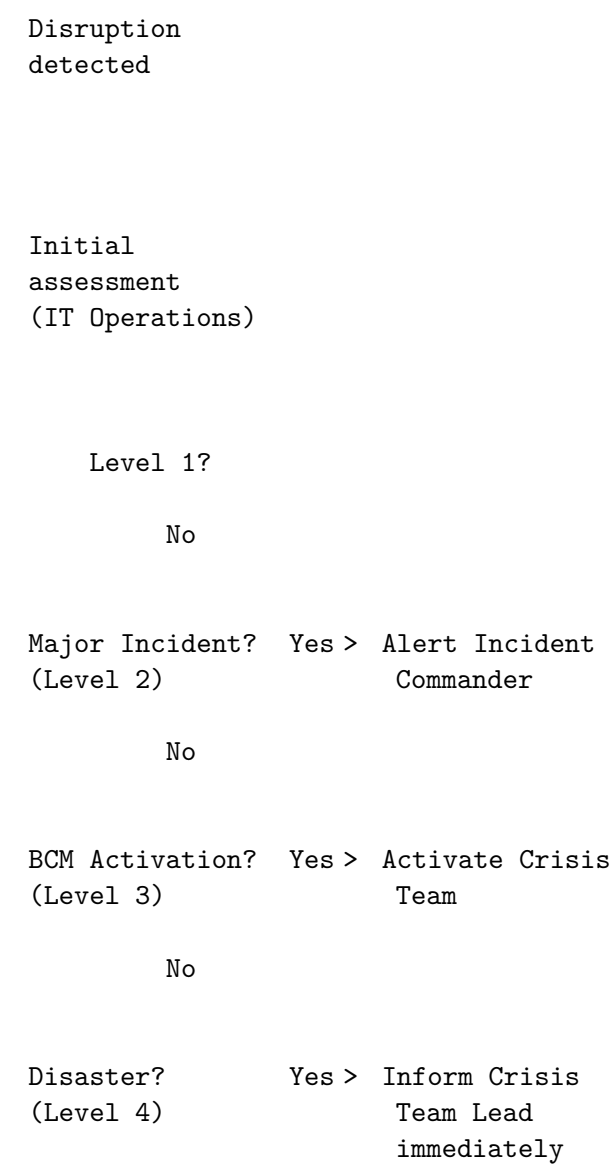
6.3.2 3.2 Escalation Criteria

Escalation to Level 2 (Major Incident): - RTO of a critical service will likely be exceeded - More than [TODO: X] users affected - Financial damage > [TODO: Amount] per hour - Data loss threatens (RPO exceedance) - Security incident with high impact

Escalation to Level 3 (BCM Activation): - Multiple critical services simultaneously failed - Recovery within RTO not possible - Site not accessible - Massive cyber attack (ransomware, DDoS) - Natural disaster or severe accident

Escalation to Level 4 (Disaster): - Main site completely failed - Human lives at risk - Existential threat to the company - Official order (e.g., evacuation)

6.3.3 3.3 Escalation Process



6.4 4. Alerting Process

6.4.1 4.1 Alerting Channels

Primary: Phone (Mobile Phone) - Direct call to defined contact persons - If unreachable: Contact deputy

Secondary: SMS / Messenger - Parallel notification via SMS - Messenger groups for quick coordination

Tertiary: Email - Documentation and traceability - Not suitable for time-critical alerting

6.4.2 4.2 Alerting Procedure

1. **Initial detection:** Disruption detected (monitoring, report, observation)
2. **Initial assessment:** IT operations assesses severity and impact
3. **Alerting:** Contact according to escalation level
4. **Confirmation:** Recipient confirms receipt and availability
5. **Briefing:** Brief situation description and initial measures
6. **Documentation:** Alerting documented in logbook

6.4.3 4.3 Crisis Team Alerting List

For BCM activation (Level 3), the following persons are alerted:

1. {{ meta.roles.ceo.name }} (Crisis Team Lead)
2. {{ meta.roles.cio.name }} (CIO)
3. {{ meta.roles.ciso.name }} (CISO)
4. [TODO: BCM Manager]
5. [TODO: Communications Manager]
6. Additional crisis team members depending on situation

Alerting sequence: Parallel, not sequential

6.5 5. On-Call and On-Call Duty

6.5.1 5.1 On-Call Schedule

[TODO: Define on-call schedules for critical roles]

Example IT Operations:

Week	Primary	Secondary	Tertiary
01	[Name 1]	[Name 2]	[Name 3]
02	[Name 2]	[Name 3]	[Name 1]
03	[Name 3]	[Name 1]	[Name 2]

Update: Weekly, by Friday 12:00 PM latest

6.5.2 5.2 On-Call Obligations

During on-call duty: - Mobile phone switched on and reachable (24/7) - Response time: Within 30 minutes - Sober and ready for duty - Access to laptop and VPN - Knowledge of current runbooks and escalation paths

Compensation: According to company agreement / employment contract

6.6 6. Contact List Maintenance

6.6.1 6.1 Update Process

Responsible: BCM Manager

Update Interval: - Quarterly review of all contact data - Ad-hoc for personnel changes - After each BCM exercise

Process: 1. BCM manager requests update 2. Departments review and report changes 3. BCM manager updates contact lists 4. New version distributed and old version archived

6.6.2 6.2 Data Protection

Contact lists are subject to GDPR: - Access only for authorized persons - Encrypted storage - No disclosure to third parties without consent - Deletion upon employee departure

---

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 7

Service and Process Catalog with Criticality

Document ID: BCM-0060
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

7.1 1. Objective

This document documents all services and business processes of AdminSend GmbH considered in BCM including:

- **Criticality assessment:** Classification by business criticality (High/Medium/Low)
- **Ownership:** Clear assignment of responsibilities
- **Dependencies:** Identification of critical dependencies
- **Stakeholders:** Affected customers and internal/external stakeholders

The service and process catalog forms the basis for: - Business Impact Analysis (BIA) - BCM strategies and continuity options - Business Continuity Plans (BCP) - IT Disaster Recovery Plans (DRP)

7.2 2. Service and Process Catalog

7.2.1 2.1 Business-Critical Services (Criticality: HIGH)

Service/Process	Owner	Description	Top 5 Dependencies	Customers/Stakeholders
[TODO: Service 1]	[TODO: Owner]	[TODO: Description]	[TODO: 1. IT System, 2. Supplier, 3. Personnel, 4. Location, 5. Data]	[TODO: External customers, partners]
[TODO: Service 2]	[TODO: Owner]	[TODO: Description]	[TODO: Dependencies]	[TODO: Stakeholders]

Examples of business-critical services: - Customer service and support (24/7) - Production control and execution - Order processing and logistics - Payment transactions and financial processes - E-commerce platform

7.2.2 2.2 Important Services (Criticality: MEDIUM)

Service/Process	Owner	Description	Top 5 Dependencies	Customers/Stakeholders
[TODO: Service 1]	[TODO: Owner]	[TODO: Description]	[TODO: Dependencies]	[TODO: Stakeholders]

Examples of important services: - Personnel administration and HR processes - Procurement and purchasing - Marketing and sales (not time-critical) - Controlling and reporting - Quality management

7.2.3 2.3 Supporting Services (Criticality: LOW)

Service/Process	Owner	Description	Top 5 Dependencies	Customers/Stakeholders
[TODO: Service 1]	[TODO: Owner]	[TODO: Description]	[TODO: Dependencies]	[TODO: Stakeholders]

Examples of supporting services: - Development environments - Training and learning platforms - Archiving and document management - Internal communication tools (not time-critical)

7.3 3. Criticality Assessment Criteria

7.3.1 3.1 Assessment Dimensions

Criticality is assessed based on the following dimensions:

1. Financial Impact - Direct revenue loss per hour/day - Contractual penalties and damage claims - Additional costs for emergency measures

2. Operational Impact - Impairment of other business processes - Production failure or quality problems - Backlog and rework effort

3. Legal and Regulatory Requirements - Legal obligations and compliance - Contractual obligations (SLAs) - Reporting obligations to authorities

4. Safety - Endangerment of human life - Environmental hazard - Plant safety

5. Reputation and Trust - Customer trust and customer satisfaction - Brand image and public perception - Trust of partners and investors

7.3.2 3.2 Assessment Logic and Scoring

[TODO: Define your assessment logic]

Example Scoring:

Criticality	Financial Impact	Operational Impact	Legal Impact	Safety Impact	Reputation Impact
HIGH	> 50,000 €/day	Multiple processes affected	Legal violation	Personal endangerment	Massive media coverage
MEDIUM	10,000-50,000 €/day	One process affected	Contract violation	Property damage	Customer complaints
LOW	< 10,000 €/day	No impact	No obligation	No damage	No impact

Overall Assessment: - If at least one dimension "HIGH" → Overall criticality: **HIGH** - If at least two dimensions "MEDIUM" → Overall criticality: **MEDIUM** - Otherwise → Overall criticality: **LOW**

7.3.3 3.3 Criticality Matrix

```
Impact

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

M                 [Service D]
     [Service E]

L                 [Service F]  [Service G]


    L           M           H
              Probability
```

[TODO: Place your services in the matrix]

7.4 4. IT Services and Systems

7.4.1 4.1 Critical IT Services

IT Service	Supported Business Processes	Criticality	IT Owner	Technology
[TODO: ERP System]	Order processing, finance, production	HIGH	{{ meta.roles.it_operations_manager.name }}	[TODO: SAP/Oracle/etc.]
[TODO: Email]	All business processes	HIGH	{{ meta.roles.it_operations_manager.name }}	[TODO: Exchange/M365/etc.]
[TODO: CRM]	Sales, customer service	MEDIUM	[TODO]	[TODO: Salesforce/etc.]

7.4.2 4.2 IT Infrastructure

Infrastructure Component	Dependent Services	Criticality	Location	Redundancy
[TODO: Core Switch]	All IT services	HIGH	München	Yes/No
[TODO: Firewall]	Internet access	HIGH	München	Yes/No
[TODO: Storage]	All data	HIGH	München	Yes/No

7.5 5. Dependency Analysis

7.5.1 5.1 Dependency Types

People (Personnel): - Key persons and specialized knowledge - Minimum staffing for operations - External service providers

Facilities (Locations and Premises): - Office buildings and production facilities - Data centers - Warehouses and logistics centers

Technology (IT Systems and Technology): - Business applications (ERP, CRM, etc.) - IT infrastructure (network, servers, storage) - Cloud services

Information (Data and Information): - Business data and customer data - Configuration data - Documentation and knowledge

Suppliers (Suppliers and Partners): - Critical suppliers - IT service providers and cloud providers - Logistics partners

7.5.2 5.2 Dependency Matrix (Example)

[TODO: Create a dependency matrix for your critical services]

Example for service "Order Processing":

Dependency Type	Concrete Dependency	Criticality	Fallback Option
People	Order processors (min. 3)	HIGH	Training of backup personnel
Facilities	Office location headquarters	MEDIUM	Home office possible

Dependency Type	Concrete Dependency	Criticality	Fallback Option
Technology	ERP system	HIGH	None (single point of failure)
Information	Order database	HIGH	Backup available
Suppliers	Logistics service provider	HIGH	Alternative provider available

7.6 6. Stakeholder Overview

7.6.1 6.1 Internal Stakeholders

Stakeholder Group	Affected Services	Communication Need	Contact Person
Executive Management	All critical services	Strategic decisions	{{ meta.roles.ceo.name }}
IT Department	All IT-dependent services	Technical coordination	{{ meta.roles.cio.name }}
Departments	Respective services	Operational implementation	[TODO: Department heads]
Employees	All services	Information and instructions	[TODO: HR/Communication]

7.6.2 6.2 External Stakeholders

Stakeholder Group	Affected Services	Communication Need	Contact Person
Customers	Customer service, production, delivery	Status updates, alternative solutions	[TODO: Customer service]
Suppliers	Procurement, production	Coordination, adjustments	[TODO: Procurement]
Partners	Joint services	Coordination, alignment	[TODO: Partner manager]
Authorities	Regulated services	Reports, evidence	[TODO: Compliance]
Media	All services (in crisis)	Press releases	[TODO: PR/Communication]

7.7 7. Maintenance and Updates

Responsible: BCM Manager

Update Interval: - Annual review of all services and criticality assessments - Ad-hoc for organizational changes (new services, process changes) - After BIA execution

Review Process: 1. BCM manager initiates review 2. Service owners review and update their services 3. Criticality assessment is validated 4. Changes are documented and communicated

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initial creation

ewpage

Chapter 8

Business Impact Analysis (BIA) – Methodology

Document ID: BCM-0070
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

8.1 1. Purpose and Output

8.1.1 1.1 BIA Objectives

The Business Impact Analysis (BIA) of AdminSend GmbH pursues the following objectives:

- **Identification of critical business processes:** Determination of business-critical processes and services
- **Quantification of impacts:** Assessment of financial, operational, and reputational impacts of outages
- **Definition of target values:** Definition of RTO (Recovery Time Objective) and RPO (Recovery Point Objective)
- **Prioritization:** Establishment of recovery prioritization
- **Resource planning:** Determination of resource requirements for business continuity

8.1.2 1.2 Expected Results

The BIA delivers the following results:

RTO (Recovery Time Objective): - Maximum tolerable downtime for each critical process - Point in time by which a process must be restored

RPO (Recovery Point Objective): - Maximum tolerable data loss - Point in time to which data must be restored

MTPD (Maximum Tolerable Period of Disruption): - Maximum time period a process can be down before irreparable damage occurs - Also: MAO (Maximum Acceptable Outage)

Prioritization: - Sequence of recovery of processes and systems - Dependencies between processes

Resource Requirements: - Personnel, premises, IT systems, data, suppliers - Minimum resources for emergency operations

8.2 2. Approach and Methodology

8.2.1 2.1 BIA Process

```
1. Preparation
- Scope
- Stakeholders
```

```
2. Data
   Collection
- Workshops
- Interviews
- Questionnaires
```

```
3. Analysis
- Assessment
- Dependencies
```

```
4. RTO/RPO
- Definition
- Validation
```

```
5. Documentation
- Report
- Presentation
```

```
6. Approval
- Review
- Authorization
```

8.2.2 2.2 Workshops and Interviews

Target Audience: - Department heads and process owners - IT managers - Key persons with specialized knowledge

Format: - **Workshops:** Group format for cross-functional topics (2-4 hours) - **Interviews:** One-on-one conversations for detailed process analysis (1-2 hours) - **Questionnaires:** Standardized collection for less critical processes

Execution: [TODO: Define workshop/interview plan]

Example Schedule: | Week | Activity | Participants | Responsible | |——|———-|————-|———-| | 1 | Kick-off workshop | All department heads | BCM Manager | | 2-3 | Individual department interviews | Process owners | BCM Manager | | 4 | IT workshop | IT team | BCM Manager + {{ meta.roles.cio.name }} | | 5 | Consolidation and analysis | BCM team | BCM Manager | | 6 | Results presentation | Management | BCM Manager |

8.2.3 2.3 Data Sources

Primary Data Sources: - Workshops and interviews with departments - Existing process documentation - IT service catalog and CMDB - Financial reports and revenue data

Secondary Data Sources: - Contract documents and SLAs - Compliance requirements - Historical incident data - Benchmarks and best practices

8.2.4 2.4 Review and Validation Steps

Validation by Departments: 1. Draft BIA results sent to process owners 2. Departments review and comment within [TODO: X] days 3. Feedback is incorporated

Management Review: 1. Consolidated BIA results presented to management 2. RTO/RPO values discussed and validated 3. Prioritization established

Formal Approval: - Approval by {{ meta.roles.ceo.name }} (CEO) - Confirmation by department heads - Documentation of approval

8.3 3. Assessment Dimensions

8.3.1 3.1 Financial Impact

Direct Financial Losses: - Revenue loss per hour/day - Contractual penalties and damage claims - Additional costs for emergency measures

Assessment Scale: [TODO: Define your assessment scale]

Example: | Level | Description | Revenue Loss per Day | |——-|————-|————————| | 5 - Critical | Existential threat | > 500,000 € | | 4 - Very High | Massive impact | 100,000 - 500,000 € | | 3 - High | Significant impact | 50,000 - 100,000 € | | 2 - Medium | Noticeable impact | 10,000 - 50,000 € | | 1 - Low | Minor impact | < 10,000 € |

8.3.2 3.2 Operational Impact

Impairment of Business Operations: - Throughput and production capacity - Backlog and rework effort - Quality problems - Impairment of other processes

Assessment Scale: | Level | Description | Operational Impact | |——-|————-|————————-| | 5 - Critical | Complete standstill | All processes affected | | 4 - Very High | Massive impairment | Multiple critical processes affected | | 3 - High | Significant impairment | One critical process affected | | 2 - Medium | Noticeable impairment | Delays, but operation possible | | 1 - Low | Minor impairment | No significant impact |

8.3.3 3.3 Legal and Regulatory Impact

Compliance Risks: - Legal obligations (e.g., GDPR, occupational safety) - Contractual obligations (SLAs, supply contracts) - Reporting obligations to authorities - Liability risks

Assessment Scale: | Level | Description | Legal Impact | |——-|————-|————————| | 5 - Critical | Severe legal violation | Criminal proceedings, license loss | | 4 - Very High | Significant violation | Fines > 100,000 € | | 3 - High | Violation | Fines 10,000 - 100,000 € | | 2 - Medium | Contract violation | Contractual penalties | | 1 - Low | No obligation | No legal consequences |

8.3.4 3.4 Safety Impact

Endangerment of Persons and Facilities: - Personal safety (employees, customers, visitors) - Environmental hazard - Plant safety - Data security

Assessment Scale: | Level | Description | Safety Impact | |——-|————-|————————| | 5 - Critical | Life-threatening | Deaths or serious injuries | | 4 - Very High | Significant hazard | Injuries, environmental damage | | 3 - High | Hazard | Health risks | | 2 - Medium | Minor hazard | Property damage | | 1 - Low | No hazard | No safety risks |

8.3.5 3.5 Reputation Impact

Image and Trust: - Customer trust and customer satisfaction - Brand image and public perception - Trust of partners and investors - Media coverage

Assessment Scale: | Level | Description | Reputation Impact | |——-|————-|————————-| | 5 - Critical | Irreparable damage | Massive negative media coverage, customer exodus | | 4 - Very High | Severe damage | National media coverage, significant loss of trust | | 3 - High | Significant damage | Regional media coverage, customer complaints | | 2 - Medium | Noticeable damage | Social media criticism, individual complaints | | 1 - Low | Minor damage | No public perception |

8.4 4. Time Dependency of Impacts

8.4.1 4.1 Time Window Analysis

The impacts of process outages are assessed for different time windows:

Time Windows: - **0-4 hours:** Immediate impacts - **4-24 hours:** Short-term impacts - **1-3 days:** Medium-term impacts - **> 3 days:** Long-term impacts

8.4.2 4.2 Impact Progression

[TODO: Document the time-dependent development of impacts]

Example for process "Order Processing":

Time Window	Financial Impact	Operational Impact	Reputation Impact
0-4h	Low (Level 1)	Medium (Level 2)	Low (Level 1)
4-24h	Medium (Level 2)	High (Level 3)	Medium (Level 2)
1-3d	High (Level 3)	Very High (Level 4)	High (Level 3)
> 3d	Critical (Level 5)	Critical (Level 5)	Very High (Level 4)

8.4.3 4.3 MTPD Determination

Maximum Tolerable Period of Disruption (MTPD):

The MTPD is the point at which the impacts of an outage become unacceptable.

Determination: - MTPD = Point at which impacts reach Level 4 or 5 - Or: Point at which multiple dimensions reach Level 3

Example: - Process "Order Processing": MTPD = 24 hours (from then Level 4/5) - Process "Email": MTPD = 4 hours (from then Level 3 in multiple dimensions)

8.5 5. RTO/RPO Definition

8.5.1 5.1 RTO Determination

Recovery Time Objective (RTO): - RTO must be significantly below MTPD (safety buffer) - Recommendation: RTO = 50-70% of MTPD

Example: - MTPD = 24 hours → RTO = 12-16 hours - MTPD = 4 hours → RTO = 2-3 hours

8.5.2 5.2 RPO Determination

Recovery Point Objective (RPO): - Maximum tolerable data loss - Dependent on data change rate and business criticality

Example: - Transaction data: RPO = 15 minutes (continuous replication) - Configuration data: RPO = 24 hours (daily backup) - Archive data: RPO = 7 days (weekly backup)

8.6 6. Results Approval

8.6.1 6.1 Responsible for Acceptance

Department Level: - Process owners confirm BIA results for their processes - Validation of RTO/RPO values

Management Level: - {{ meta.roles.ceo.name }} (CEO) approves overall BIA - {{ meta.roles.cio.name }} (CIO) approves IT-related RTO/RPO - Department heads approve their areas

8.6.2 6.2 Approval Process

1. **Draft:** BCM manager creates BIA report
2. **Department Review:** Process owners review (2 weeks)
3. **Revision:** Feedback is incorporated
4. **Management Presentation:** Presentation of results
5. **Formal Approval:** Signatures of responsible parties
6. **Publication:** BIA results are communicated

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 9

BIA – Results and Target Values (RTO/RPO)

Document ID: BCM-0080
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: Confidential
Last Updated: {{ meta.document.last_updated }}

9.1 1. Summary

9.1.1 1.1 Top-Critical Processes and Services

The following processes have been identified as business-critical (RTO < 24 hours):

[TODO: List the top-critical processes]

Examples: 1. **Order Processing** - RTO: 4 hours, RPO: 15 minutes 2. **Customer Service (24/7)** - RTO: 2 hours, RPO: 1 hour 3. **Production Control** - RTO: 8 hours, RPO: 30 minutes 4. **Payment Transactions** - RTO: 4 hours, RPO: 15 minutes 5. **Email and Communication** - RTO: 4 hours, RPO: 1 hour

9.1.2 1.2 Key Findings

[TODO: Document the most important findings from the BIA]

Example Findings: - **Single Points of Failure:** ERP system has no redundancy, critical dependency - **Personnel Dependencies:** Key persons in production without adequate backup - **Supplier Risks:** Critical supplier has no own BCM - **IT Infrastructure:** Network infrastructure partially not redundantly designed

9.2 2. BIA Results Table

9.2.1 2.1 Business-Critical Processes (Criticality: HIGH)

Service/Process	MTPD/MAO	RTO	RPO	Manual Workarounds Possible?	Remarks
[TODO: Process 1]	[TODO: 24h]	[TODO: 4h]	[TODO: 15min]	Yes/No/Partially	[TODO: Remarks]
[TODO: Process 2]	[TODO]	[TODO]	[TODO]	Yes/No/Partially	[TODO]

Example: | Service/Process | MTPD/MAO | RTO | RPO | Manual Workarounds Possible? | Remarks | |—————|———-|—-|—-|————————–|———| | Order Processing | 24h | 4h | 15min | Partially (Excel lists) | ERP system critical | | Customer Service | 8h | 2h | 1h | Yes (phone, email) | CRM system helpful but not mandatory | | Production Control | 48h | 8h | 30min | No | Fully automated, no manual alternative |

9.2.2 2.2 Important Processes (Criticality: MEDIUM)

Service/Process	MTPD/MAO	RTO	RPO	Manual Workarounds Possible?	Remarks
[TODO: Process 1]	[TODO]	[TODO]	[TODO]	Yes/No/Partially	[TODO]

9.2.3 2.3 Supporting Processes (Criticality: LOW)

Service/Process	MTPD/MAO	RTO	RPO	Manual Workarounds Possible?	Remarks
[TODO: Process 1]	[TODO]	[TODO]	[TODO]	Yes/No/Partially	[TODO]

9.3 3. Dependencies per Critical Process

9.3.1 3.1 Process: [TODO: Process Name]

People (Personnel): - [TODO: Minimum staffing, key persons, specialized knowledge] - Example: At least 3 order processors, backup arrangement required

Facilities (Locations and Premises): - [TODO: Required locations, rooms, infrastructure] - Example: Office workstations, home office as alternative possible

Technology (IT Systems): - [TODO: Critical IT systems and applications] - Example: ERP system (SAP), email, network access

Information (Data): - [TODO: Critical data and information] - Example: Order database, customer master data, product configurations

Suppliers (Suppliers and Partners): - [TODO: Critical suppliers and service providers] - Example: Logistics service provider, cloud provider, payment service provider

9.3.2 3.2 Dependency Matrix

[TODO: Create a dependency matrix for all critical processes]

Process	People	Facilities	Technology	Information	Suppliers
Order Processing	3 employees	Office/Home-Office	ERP, Email	Order data	Logistics
Customer Service	5 employees	Call center	CRM, Phone	Customer data	Telco
Production	10 employees	Production hall	MES, SCADA	Production data	Suppliers

9.4 4. Manual Workarounds and Emergency Operations

9.4.1 4.1 Workaround Strategies

[TODO: Document manual workarounds for critical processes]

Example for process "Order Processing":

In case of ERP system failure: - **Workaround:** Manual order entry in Excel lists - **Capacity:** Reduced to 30% of normal operations - **Duration:** Maximum 24 hours (then data entry backlog too large) - **Prerequisites:** Excel templates available, employees trained - **Limitations:** No real-time inventory check, no automatic invoicing

In case of site failure: - **Workaround:** Home office for order processing - **Capacity:** 80% of normal operations - **Duration:** Unlimited - **Prerequisites:** VPN access, laptops, telephony via softphone - **Limitations:** No physical document processing

9.4.2 4.2 Emergency Operations Capacities

Process	Normal Operations	Emergency Operations (manual)	Emergency Operations (IT-DR)	Remarks
Order Processing	100%	30%	80%	Manual entry very labor-intensive
Customer Service	100%	70%	90%	Phone as fallback
Production	100%	0%	100%	No manual alternative

9.5 5. Open Items and Measures

9.5.1 5.1 Identified Risks and Measures

Measure	Description	Owner	Priority	Due	Status	Cost (estimated)
[TODO: Measure 1]	[TODO: Description]	[TODO: Owner]	High/Medium/Low	[TODO: Date]	Open/In Progress/Done	[TODO: Amount]

Examples:

Measure	Description	Owner	Priority	Due	Status	Cost (estimated)
ERP Redundancy	Implementation of high-availability cluster	{{ meta.roles.cio.name }}	High	Q2 2026	In Progress	150,000 €
Backup Personnel	Training of backups for key persons	HR	High	Q1 2026	Open	20,000 €
Supplier BCM	Request BCM evidence from critical suppliers	Procurement	Medium	Q2 2026	Open	5,000 €
Network Redundancy	Second internet connection	{{ meta.roles.it_operations_manager.name }}	High	Q1 2026	In Progress	30,000 €

9.5.2 5.2 Prioritization of Measures

Priority HIGH (implement immediately): - Measures to eliminate single points of failure - Measures to meet critical RTO/RPO values - Measures to fulfill regulatory requirements

Priority MEDIUM (within 6-12 months): - Measures to improve resilience - Measures to reduce dependencies - Measures to improve workarounds

Priority LOW (Nice-to-have): - Measures for further optimization - Measures for less critical processes

9.6 6. Recovery Prioritization

9.6.1 6.1 Prioritization Matrix

In case of comprehensive failure, recovery occurs in the following order:

Priority 1 (0-4 hours): 1. Network infrastructure and internet connection 2. Email and communication 3. Authentication and access control

Priority 2 (4-8 hours): 4. ERP system (order processing, finance) 5. CRM system (customer service) 6. Production control systems

Priority 3 (8-24 hours): 7. Other business applications 8. Development and test environments 9. Reporting and analytics

9.6.2 6.2 Dependencies in Recovery

```
Network/Internet




Email       Authenti-    Firewall
            cation




    ERP             CRM
```

9.7 7. Approval and Authorization

9.7.1 7.1 Approval by Departments

Department	Responsible	Date	Signature
[TODO: Department 1]	[TODO: Name]	[TODO: Date]	[TODO]
[TODO: Department 2]	[TODO: Name]	[TODO: Date]	[TODO]

9.7.2 7.2 Management Approval

Role	Name	Date	Signature
CEO	{{ meta.roles.ceo.name }}	[TODO: Date]	[TODO]
CIO	{{ meta.roles.cio.name }}	[TODO: Date]	[TODO]
BCM Manager	[TODO: Name]	[TODO: Date]	[TODO]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 10

Risk Analysis and Scenarios

Document ID: BCM-0090
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: Confidential
Last Updated: {{ meta.document.last_updated }}

10.1 1. Objective

The risk analysis of AdminSend GmbH serves to:

- **Identify** risks that can impair business continuity
- **Assess** probability of occurrence and impacts
- **Treat** through appropriate measures (avoidance, reduction, transfer, acceptance)
- **Monitor** and regularly review risks

The risk analysis complements the Business Impact Analysis (BIA) and forms the basis for the BCM strategy.

10.2 2. Scenario Catalog

10.2.1 2.1 IT and Cyber Risks

2.1.1 Cyber Attack / Ransomware - **Description:** Encryption of data by ransomware, extortion - **Affected Services:** All IT-dependent processes - **Typical Impacts:** Data loss, system failure, extortion payment - **Reference:** BSI Standard 200-4, Cyber Resilience section

2.1.2 Data Center / Cloud Region Failure - **Description:** Complete failure of primary data center or cloud region - **Affected Services:** All IT services - **Typical Impacts:** Total IT system failure, data access not possible

2.1.3 Network Failure / Internet Outage - **Description:** Failure of network infrastructure or internet connection - **Affected Services:** All network-dependent services - **Typical Impacts:** No communication, no data access

2.1.4 Data Loss / Backup Failure - **Description:** Loss of critical data, backup not recoverable - **Affected Services:** Data-dependent processes - **Typical Impacts:** Permanent data loss, RPO exceedance

10.2.2 2.2 Infrastructure Risks

2.2.1 Power Outage - **Description:** Failure of power supply at site - **Affected Services:** All power-dependent systems and processes - **Typical Impacts:** Production failure, IT failure, building technology failure

2.2.2 Fire - **Description:** Fire in building or data center - **Affected Services:** All services at affected site - **Typical Impacts:** Site unusable, property damage, personal endangerment

2.2.3 Water Damage - **Description:** Flooding, pipe burst, extinguishing water - **Affected Services:** Services at affected site - **Typical Impacts:** Building damage, IT hardware damage

2.2.4 Site Not Accessible - **Description:** Evacuation, closure, natural event - **Affected Services:** All site-dependent processes - **Typical Impacts:** Employees cannot work, production stands still

10.2.3 2.3 Personnel Risks

2.3.1 Personnel Loss / Pandemic - **Description:** Wave of illness, pandemic, mass absence - **Affected Services:** Personnel-intensive processes - **Typical Impacts:** Reduced capacity, key persons not available

2.3.2 Loss of Key Persons - **Description:** Long-term loss of persons with specialized knowledge - **Affected Services:** Processes with knowledge dependencies - **Typical Impacts:** Processes cannot be performed

10.2.4 2.4 Supplier Risks

2.4.1 Supplier Failure - **Description:** Critical supplier cannot deliver - **Affected Services:** Production and procurement processes - **Typical Impacts:** Production stop, delivery bottlenecks

2.4.2 IT Service Provider Failure - **Description:** Failure of a critical IT service provider or cloud provider - **Affected Services:** Outsourced IT services - **Typical Impacts:** Service not available, no alternative

10.2.5 2.5 Natural Events and Environment

2.5.1 Severe Weather / Storm - **Description:** Severe weather, storm, hail - **Affected Services:** Site-dependent processes, logistics - **Typical Impacts:** Building damage, traffic routes blocked

2.5.2 Flooding - **Description:** Flooding by river or heavy rain - **Affected Services:** Site-dependent processes - **Typical Impacts:** Site flooded, massive property damage

2.5.3 Earthquake (depending on location) - **Description:** Seismic event - **Affected Services:** All services at site - **Typical Impacts:** Building damage, infrastructure failure

[TODO: Add or remove scenarios according to your sites and risks]

10.3 3. Assessment Methodology

10.3.1 3.1 Assessment Scheme

Probability of Occurrence (1-5): | Level | Designation | Description | Frequency | |——-|———-|————-|————| | 5 | Very High | Occurs regularly | Multiple times per year | | 4 | High | Occurs occasionally | Once per year | | 3 | Medium | Can occur | Once in 1-5 years | | 2 | Low | Unlikely | Once in 5-10 years | | 1 | Very Low | Very unlikely | Less than every 10 years |

Impact (1-5): | Level | Designation | Description | Financial Impact | |——-|————-|————-|——————| | 5 | Catastrophic | Existential threat | > 1 million € | | 4 | Very High | Massive impact | 500,000 - 1 million € | | 3 | High | Significant impact | 100,000 - 500,000 € | | 2 | Medium | Noticeable impact | 10,000 - 100,000 € | | 1 | Low | Minor impact | < 10,000 € |

Risk Score: - Risk Score = Probability of Occurrence × Impact - Value range: 1-25

10.3.2 3.2 Risk Tolerance and Thresholds

[TODO: Define your risk tolerance]

Example:

Risk Score	Risk Level	Treatment	Escalation
15-25	Critical (Red)	Immediate measures required	{{ meta.roles.ceo.name }}
10-14	High (Orange)	Measures within 3 months	BCM Manager
5-9	Medium (Yellow)	Measures within 12 months	Department
1-4	Low (Green)	Monitoring, no measures	Department

10.3.3 3.3 Risk Matrix

```
Impact

  5    10     15     20     25
      [Yellow][Orange][Red][Red]
  4     8     12     16     20
      [Yellow][Orange][Orange][Red]
  3     6      9     12     15
      [Yellow][Yellow][Orange][Orange]
  2     4      6      8     10
      [Green][Yellow][Yellow][Orange]
  1     2      3      4      5
      [Green][Green][Green][Yellow]
```

```
      1     2     3     4     5
           Probability
```

10.4 4. Risk Register

10.4.1 4.1 Assessed Risks

Risk/Scenario	Affected Services	Prob.	Impact	Score	Risk Level	Controls (existing)	Measures (planned)	Owner
[TODO: Risk 1]	[TODO]	3	5	15	Orange	[TODO]	[TODO]	[TODO]

Examples:

Risk/Scenario	Affected Services	Prob.	Impact	Score	Risk Level	Controls (existing)	Measures (planned)	Owner
Ransomware Attack	All IT services	4	5	20	Red	Firewall, AV, Backup	EDR, Segmentation, Offline Backup	{{ meta.roles.ciso.name }}
Power Outage	Production, IT	3	4	12	Orange	UPS (15min)	Emergency generator	Facility Manager
Personnel Loss (Pandemic)	All processes	2	4	8	Yellow	Home office possible	Pandemic plan	HR
Supplier Failure	Production	3	3	9	Yellow	Inventory (2 weeks)	Second supplier	Procurement
Data Center Failure	All IT services	2	5	10	Orange	Backup available	DR site	{{ meta.roles.cio.name }}

10.4.2 4.2 Top Risks (Score 15)

[TODO: List the top risks requiring immediate measures]

1. **Ransomware Attack** (Score: 20)
   - Measures: EDR implementation, network segmentation, offline backups
   - Responsible: {{ meta.roles.ciso.name }}
   - Due: Q1 2026
2. [TODO: Additional top risk]

10.5 5. Risk Treatment

10.5.1 5.1 Treatment Strategies

Risk Avoidance: - Activity is not performed or discontinued - Example: Renounce use of insecure cloud services

Risk Reduction: - Measures to reduce probability or impact - Example: Implementation of redundancies, backup strategies

Risk Transfer: - Transfer of risk to third parties (insurance, outsourcing) - Example: Cyber insurance, SLA with service providers

Risk Acceptance: - Conscious acceptance of residual risk - Example: Low risks without measures

10.5.2 5.2 Measures Plan

Measure	Risk	Strategy	Description	Owner	Priority	Cost	Due	Status
[TODO: Measure 1]	[TODO: Risk]	Reduction	[TODO: Description]	[TODO]	High	[TODO]	[TODO]	Open

Examples:

Measure	Risk	Strategy	Description	Owner	Priority	Cost	Due	Status
EDR Implementation	Ransomware	Reduction	Endpoint Detection & Response on all clients	{{ meta.roles.ciso.name }}	High	50,000 €	Q1 2026	In Progress
Emergency Generator	Power Outage	Reduction	Diesel generator for 48h operation	Facility	Medium	80,000 €	Q2 2026	Planned
Cyber Insurance	Ransomware	Transfer	Insurance for cyber incidents	CFO	High	20,000 €/year	Q1 2026	Open

10.6 6. Monitoring and Review

10.6.1 6.1 Risk Monitoring

Responsible: BCM Manager

Monitoring Interval: - Quarterly review of risk register - Ad-hoc for new threats or incidents - Annual complete risk analysis

Indicators: - New threats (e.g., new ransomware variants) - Incidents at comparable organizations - Changes in threat landscape - Technological developments

10.6.2 6.2 Escalation

Escalation Criteria: - New risk with score 15 - Existing risk increases to score 15 - Risk occurs (incident)

Escalation Paths: - Score 15: Immediate report to {{ meta.roles.ceo.name }} - Score 10-14: Report to BCM manager - Score < 10: Documentation in risk register

---

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.document.author | default }}	Initial creation

ewpage

Chapter 11

Strategy and Continuity Options

Document ID: BCM-0100
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

11.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

11.2 2. Scope

This document applies to: - [TODO: Define the scope]

11.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

11.4 4. Main Content

[TODO: Add specific content for this template]

11.4.1 4.1 Section 1

[TODO: Content]

11.4.2 4.2 Section 2

[TODO: Content]

11.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

11.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.document.author | default }}	Initial creation

ewpage

Chapter 12

Activation Criteria and Decision Tree

Document ID: BCM-0110
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

12.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

12.2 2. Scope

This document applies to: - [TODO: Define the scope]

12.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

12.4 4. Main Content

[TODO: Add specific content for this template]

12.4.1 4.1 Section 1

[TODO: Content]

12.4.2 4.2 Section 2

[TODO: Content]

12.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

12.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 13

Crisis Management Plan

Document ID: BCM-0120
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

13.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

13.2 2. Scope

This document applies to: - [TODO: Define the scope]

13.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

13.4 4. Main Content

[TODO: Add specific content for this template]

13.4.1 4.1 Section 1

[TODO: Content]

13.4.2 4.2 Section 2

[TODO: Content]

13.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

13.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.document.author | default }}	Initial creation

ewpage

Chapter 14

Communication Plan Internal External

Document ID: BCM-0130
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

14.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

14.2 2. Scope

This document applies to: - [TODO: Define the scope]

14.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

14.4 4. Main Content

[TODO: Add specific content for this template]

14.4.1 4.1 Section 1

[TODO: Content]

14.4.2 4.2 Section 2

[TODO: Content]

14.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

14.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initial creation

ewpage

Chapter 15

BCP Business Continuity Plan Template

Document ID: BCM-0140
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

15.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

15.2 2. Scope

This document applies to: - [TODO: Define the scope]

15.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

15.4 4. Main Content

[TODO: Add specific content for this template]

15.4.1 4.1 Section 1

[TODO: Content]

15.4.2 4.2 Section 2

[TODO: Content]

15.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

15.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.defaults.author }}	Initial creation

ewpage

Chapter 16

DRP IT Recovery Plan Template

Document ID: BCM-0150
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

16.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

16.2 2. Scope

This document applies to: - [TODO: Define the scope]

16.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

16.4 4. Main Content

[TODO: Add specific content for this template]

16.4.1 4.1 Section 1

[TODO: Content]

16.4.2 4.2 Section 2

[TODO: Content]

16.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

16.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 17

Backup and Restore Plan

Document ID: BCM-0160
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

17.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

17.2 2. Scope

This document applies to: - [TODO: Define the scope]

17.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

17.4 4. Main Content

[TODO: Add specific content for this template]

17.4.1 4.1 Section 1

[TODO: Content]

17.4.2 4.2 Section 2

[TODO: Content]

17.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

17.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.document.author | default }}	Initial creation

ewpage

Chapter 18

Alternative Site and Emergency Workplaces

Document ID: BCM-0170
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

18.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

18.2 2. Scope

This document applies to: - [TODO: Define the scope]

18.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

18.4 4. Main Content

[TODO: Add specific content for this template]

18.4.1 4.1 Section 1

[TODO: Content]

18.4.2 4.2 Section 2

[TODO: Content]

18.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

18.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default('') }}	{{ meta.defaults.author }}	Initial creation

ewpage

Chapter 19

Suppliers and Third Parties Continuity

Document ID: BCM-0180
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

19.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

19.2 2. Scope

This document applies to: - [TODO: Define the scope]

19.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

19.4 4. Main Content

[TODO: Add specific content for this template]

19.4.1 4.1 Section 1

[TODO: Content]

19.4.2 4.2 Section 2

[TODO: Content]

19.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

19.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initial creation

ewpage

Chapter 20

Resource Planning and Minimum Staffing

Document ID: BCM-0190
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

20.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

20.2 2. Scope

This document applies to: - [TODO: Define the scope]

20.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

20.4 4. Main Content

[TODO: Add specific content for this template]

20.4.1 4.1 Section 1

[TODO: Content]

20.4.2 4.2 Section 2

[TODO: Content]

20.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

20.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.defaults.author }}	Initial creation

ewpage

Chapter 21

Emergency Access BreakGlass

Document ID: BCM-0200
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

21.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

21.2 2. Scope

This document applies to: - [TODO: Define the scope]

21.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

21.4 4. Main Content

[TODO: Add specific content for this template]

21.4.1 4.1 Section 1

[TODO: Content]

21.4.2 4.2 Section 2

[TODO: Content]

21.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

21.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.document.author | default }}	Initial creation

ewpage

Chapter 22

Cyber Incident and Ransomware Playbook

Document ID: BCM-0210
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

22.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

22.2 2. Scope

This document applies to: - [TODO: Define the scope]

22.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

22.4 4. Main Content

[TODO: Add specific content for this template]

22.4.1 4.1 Section 1

[TODO: Content]

22.4.2 4.2 Section 2

[TODO: Content]

22.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

22.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initial creation

ewpage

Chapter 23

Exercise and Test Program

Document ID: BCM-0220
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

23.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

23.2 2. Scope

This document applies to: - [TODO: Define the scope]

23.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

23.4 4. Main Content

[TODO: Add specific content for this template]

23.4.1 4.1 Section 1

[TODO: Content]

23.4.2 4.2 Section 2

[TODO: Content]

23.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

23.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.document.author | default }}	Initial creation

ewpage

Chapter 24

Test Protocol and Success Criteria

Document ID: BCM-0230
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

24.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

24.2 2. Scope

This document applies to: - [TODO: Define the scope]

24.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

24.4 4. Main Content

[TODO: Add specific content for this template]

24.4.1 4.1 Section 1

[TODO: Content]

24.4.2 4.2 Section 2

[TODO: Content]

24.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

24.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.document.author | default }}	Initial creation

ewpage

Chapter 25

Post Incident Review Postmortem

Document ID: BCM-0240
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

25.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

25.2 2. Scope

This document applies to: - [TODO: Define the scope]

25.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

25.4 4. Main Content

[TODO: Add specific content for this template]

25.4.1 4.1 Section 1

[TODO: Content]

25.4.2 4.2 Section 2

[TODO: Content]

25.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

25.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.document.author | default }}	Initial creation

ewpage

Chapter 26

Maintenance Review and KPIs

Document ID: BCM-0250
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

26.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

26.2 2. Scope

This document applies to: - [TODO: Define the scope]

26.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

26.4 4. Main Content

[TODO: Add specific content for this template]

26.4.1 4.1 Section 1

[TODO: Content]

26.4.2 4.2 Section 2

[TODO: Content]

26.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

26.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 27

Training and Awareness

Document ID: BCM-0260
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

27.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

27.2 2. Scope

This document applies to: - [TODO: Define the scope]

27.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

27.4 4. Main Content

[TODO: Add specific content for this template]

27.4.1 4.1 Section 1

[TODO: Content]

27.4.2 4.2 Section 2

[TODO: Content]

27.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

27.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.document.author | default }}	Initial creation

ewpage

Chapter 28

Compliance Audit and Evidence

Document ID: BCM-0270
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

28.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

28.2 2. Scope

This document applies to: - [TODO: Define the scope]

28.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

28.4 4. Main Content

[TODO: Add specific content for this template]

28.4.1 4.1 Section 1

[TODO: Content]

28.4.2 4.2 Section 2

[TODO: Content]

28.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

28.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.defaults.author }}	Initial creation

ewpage

Chapter 29

Appendix Templates and Checklists

Document ID: BCM-0280
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

29.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

29.2 2. Scope

This document applies to: - [TODO: Define the scope]

29.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

29.4 4. Main Content

[TODO: Add specific content for this template]

29.4.1 4.1 Section 1

[TODO: Content]

29.4.2 4.2 Section 2

[TODO: Content]

29.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

29.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 30

Glossary and Abbreviations

Document ID: BCM-0290
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

30.1 1. Purpose and Overview

[TODO: Describe the purpose of this document]

This document is part of the Business Continuity Management System (BCMS) of AdminSend GmbH.

30.2 2. Scope

This document applies to: - [TODO: Define the scope]

30.3 3. Responsibilities

Role	Responsible	Tasks
BCM Manager	[TODO]	Maintenance and updates of this document
Department	[TODO]	Implementation of defined measures

30.4 4. Main Content

[TODO: Add specific content for this template]

30.4.1 4.1 Section 1

[TODO: Content]

30.4.2 4.2 Section 2

[TODO: Content]

30.5 5. References

- ISO 22301:2019 - Business Continuity Management Systems
- BSI Standard 100-4 - Emergency Management
- Related BCM documents: [TODO]

30.6 6. Appendices

[TODO: Add relevant appendices]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.author }}	Initial creation

ewpage