Contents

Chapter 1

IT Operations Handbook

Document Metadata

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

---

ewpage

Chapter 2

1. Introduction

This handbook describes the IT operational processes and standards of the organization.

2.1 1.1 Purpose

The IT Operations Handbook defines processes and responsibilities for stable IT operations.

2.2 1.2 Scope

This handbook applies to all IT systems and services of the organization.

ewpage

Chapter 3

2. Operational Processes

3.1 2.1 Monitoring

- 24/7 monitoring of all critical systems
- Automatic alerting when thresholds are exceeded
- Weekly evaluation of monitoring data

3.2 2.2 Maintenance Windows

- Scheduled maintenance: Sundays 02:00-06:00 AM
- Emergency maintenance: After approval by IT management
- Announcement at least 48 hours in advance

3.3 2.3 Change Management

- All changes must be documented
- Critical changes require Change Advisory Board approval
- Rollback plan is mandatory for all changes

ewpage

Chapter 4

Document Control and Versioning

4.1 Document Metadata

Field	Value
Document Title	IT Operations Handbook – AdminSend GmbH
Document ID	[TODO: Unique Document ID]
System/Service	[TODO: System/Service Name]
Owner	IT Operations Manager
Responsible Editor	Andreas Huemmer [andreas.huemmer@adminsend.de]
Approval Authority	CIO
Classification	internal
Storage Location	[TODO: Central Repository/Storage Location]
Organization	AdminSend GmbH
Location	München, Deutschland

4.2 Version History

Version	Date	Author	Changes	Approval
1.0.0	[TODO: Date]	Andreas Huemmer [andreas.huemmer@adminsend.de]	Initial Version	CIO

Note: Use Semantic Versioning (SemVer) for versioning: - **Major.Minor.Patch** (e.g., 1.0.0) - **Major:** Fundamental changes, breaking changes - **Minor:** New features, backward compatible - **Patch:** Bugfixes, minor corrections

4.3 Versioning Guidelines

4.3.1 Semantic Versioning (SemVer)

Format: MAJOR.MINOR.PATCH

- **MAJOR:** Incompatible changes, fundamental revisions
  - Example: Change of system architecture, new operating models
- **MINOR:** New functionality, backward compatible
  - Example: New processes, additional sections
- **PATCH:** Bugfixes, corrections, clarifications
  - Example: Typos, formatting, minor additions

4.3.2 Versioning Rules

1. **Initial Version:** 1.0.0 after initial release
2. **Drafts:** 0.x.x before initial release
3. **Document Changes:** Record every change in version history
4. **Date:** ISO 8601 format (YYYY-MM-DD)
5. **Author:** Full name and email

4.4 Review and Approval Process

4.4.1 1. Change Request

Responsible: Document Owner or Department

Content: - Description of change - Justification and business value - Impact analysis - Affected sections

Approval: IT Operations Manager

4.4.2 2. Technical Review

Reviewers: - **Operations:** Andreas Huemmer (andreas.huemmer@adminsend.de) - **Architecture:** [TODO: Architecture Lead] - **Security:** Thomas Weber (thomas.weber@adminsend.de) - **Compliance:** [TODO: Compliance Lead]

Review Criteria: - Technical correctness - Completeness - Consistency with other documents - Compliance with standards and best practices

4.4.3 3. Approval

Approval Authority: CIO

Approval Criteria: - All reviews completed - No open comments - Quality criteria met - Documentation standards adhered to

Approval Process: 1. Incorporate review comments 2. Create final version 3. Approval by CIO 4. Increment version 5. Publication in repository

4.4.4 4. Publication

Responsible: IT Operations Manager

Steps: 1. Store document in central repository 2. Inform stakeholders 3. Archive old version 4. Publish change notice

4.5 Approval Processes

4.5.1 Standard Changes (Patch)

- **Approval:** Document Owner
- **Review:** Optional
- **Examples:** Typos, formatting, minor additions

4.5.2 Normal Changes (Minor)

- **Approval:** CIO
- **Review:** Department (Operations/Security)
- **Examples:** New sections, process changes

4.5.3 Major Changes (Major)

- **Approval:** Anna Schmidt (anna.schmidt@adminsend.de)
- **Review:** All departments + management
- **CAB Meeting:** Required
- **Examples:** Fundamental revisions, architecture changes

4.6 Documentation Standards

4.6.1 Language and Format

- **Language:** de
- **Format:** Markdown (.md)
- **Character Set:** UTF-8
- **Line Breaks:** Unix (LF)

4.6.2 Required Fields

Every document MUST contain the following information:

- **Title:** Unique document title
- **Version:** According to SemVer
- **Date:** Last change (ISO 8601)
- **Author:** Responsible editor
- **Owner:** Document owner
- **Approval:** Approval authority
- **Classification:** Confidentiality level

4.6.3 Structure Requirements

1. **Headings:** Hierarchical (# H1, ## H2, ### H3)
2. **Tables:** Markdown syntax with alignment
3. **Lists:** Numbered or bullet points
4. **Code:** Fenced code blocks with syntax highlighting
5. **Links:** Relative links preferred

4.6.4 Linking

- **Internal Links:** Relative paths within repository
- **External Links:** Absolute URLs with description
- **References:** Unique identifiers for cross-references

4.6.5 Metadata Placeholders

Use the following placeholders for organization-wide information:

- **Organization:** `AdminSend GmbH`
- **Roles:** `Max Mustermann`, `Anna Schmidt`, `Thomas Weber`
- **Document:** `IT Operations Manager`, `CIO`
- **Author:** `Andreas Huemmer [andreas.huemmer@adminsend.de]`

4.7 Document Classification

Classification	Description	Access	Examples
Public	No restrictions	All	General information
Internal	Employees only	Employees	Operations handbooks, processes
Confidential	Restricted access	Authorized persons	Security concepts, passwords
Strictly Confidential	Highest confidentiality	Management + Authorized	Trade secrets, compliance

Current Classification: internal

4.8 Archiving and Retention

4.8.1 Retention Periods

- **Current Version:** Unlimited in repository
- **Previous Versions:** Minimum 3 years
- **Drafts:** 1 year after release
- **Archived Documents:** According to retention policy

4.8.2 Archiving Process

1. **Version Change:** Move old version to archive

2. **Metadata:** Document archiving date and reason
3. **Access:** Read access for authorized persons
4. **Deletion:** After retention period expires

4.9 Responsibilities

Role	Responsibility	Person
Document Owner	Overall responsibility, currency	IT Operations Manager
Editor	Content maintenance, changes	Andreas Huemmer [andreas.huemmer@adminsend.de]
Approval Authority	Approval of changes	CIO
CIO	Strategic alignment	Anna Schmidt
CISO	Security review	Thomas Weber

4.10 Contacts

For questions about document control: - **Document Owner:** IT Operations Manager - **IT Operations Manager:** Andreas Huemmer (andreas.huemmer@adminsend.de) - **CIO:** Anna Schmidt (anna.schmidt@adminsend.de)

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

ewpage

Chapter 5

Service Description and Criticality

5.1 Service Description

5.1.1 Basic Information

- **Service Name:** [TODO: Unique Service Name]
- **Service ID:** [TODO: Unique Service Identification]
- **Service Owner:** IT Operations Manager
- **Technical Contact:** [TODO: Name and Contact]
- **Organization:** AdminSend GmbH

5.1.2 Brief Description

[TODO: Describe the service in 2-3 sentences. What does the service do? What main functions does it provide?]

5.1.3 Business Purpose

Business Value: [TODO: What business value does this service deliver? Which business processes does it support?]

Strategic Importance: [TODO: How important is this service for the company strategy?]

5.1.4 Customers and User Groups

User Group	Number of Users	Usage Type	Criticality
[TODO: Group 1]	[TODO]	[TODO: Primary/Secondary]	[TODO: High/Medium/Low]
[TODO: Group 2]	[TODO]	[TODO: Primary/Secondary]	[TODO: High/Medium/Low]
[TODO: Group 3]	[TODO]	[TODO: Primary/Secondary]	[TODO: High/Medium/Low]

Primary User Groups: - [TODO: Description of main users]

Secondary User Groups: - [TODO: Description of secondary users]

5.1.5 Dependencies on Other Services

5.1.5.1 Upstream Dependencies (Services this service depends on)

Service	Dependency Type	Criticality	Impact on Failure
[TODO: Service 1]	[TODO: Hard/Soft]	[TODO: High/Medium/Low]	[TODO: Description]
[TODO: Service 2]	[TODO: Hard/Soft]	[TODO: High/Medium/Low]	[TODO: Description]

5.1.5.2 Downstream Dependencies (Services that depend on this service)

Service	Dependency Type	Criticality	Impact on Failure
[TODO: Service 1]	[TODO: Hard/Soft]	[TODO: High/Medium/Low]	[TODO: Description]
[TODO: Service 2]	[TODO: Hard/Soft]	[TODO: High/Medium/Low]	[TODO: Description]

> **Note:** - **Hard Dependency:** Service does not function without dependency - **Soft Dependency:** Service functions with limitations without dependency

5.2 Criticality and Protection Requirements

5.2.1 Criticality Assessment

Criticality is assessed according to the dimensions of availability, integrity, confidentiality, and traceability.

Dimension	Classification			Justification	Measures
Availability	low	medium	high	[TODO: Justification]	[TODO: Protection measures]
Integrity	low	medium	high	[TODO: Justification]	[TODO: Protection measures]
Confidentiality	low	medium	high	[TODO: Justification]	[TODO: Protection measures]
Traceability	low	medium	high	[TODO: Justification]	[TODO: Protection measures]

5.2.2 Criticality Levels

5.2.2.1 Low

- **Availability:** Outage tolerable for several days
- **Integrity:** Data loss acceptable, simple recovery

- **Confidentiality:** Public or non-critical information
- **Traceability:** No audit requirements

5.2.2.2 Medium

- **Availability:** Outage tolerable for hours to 1 day
- **Integrity:** Data loss problematic, recovery required
- **Confidentiality:** Internal information, restricted access
- **Traceability:** Basic logging required

5.2.2.3 High

- **Availability:** Outage only tolerable for minutes
- **Integrity:** Data loss unacceptable, immediate recovery
- **Confidentiality:** Confidential data, strict access control
- **Traceability:** Complete audit trail required

5.2.3 Overall Criticality

Criticality Classification: [TODO: Low/Medium/High/Critical]

Justification: [TODO: Summary justification of overall criticality based on individual dimensions]

5.3 Service Hours and Operating Windows

5.3.1 Service Hours

- **Availability:** [TODO: e.g., 24/7, Mon-Fri 08:00-18:00 CET, Business Hours]
- **Support Hours:** [TODO: When is support available?]
- **Time Zone:** [TODO: e.g., CET/CEST, UTC]

5.3.2 Operating Model

- **Operating Model:** [TODO: 24/7, Business Hours, Follow-the-Sun]
- **On-Call Availability:** [TODO: Yes/No, Times]
- **Escalation Levels:** [TODO: Level 1/2/3 Support]

5.3.3 Maintenance Windows

Maintenance Type	Time Window	Frequency	Duration	Announcement
Planned Maintenance	[TODO: e.g., Sun 02:00-06:00]	[TODO: Weekly/Monthly]	[TODO: Hours]	[TODO: Days in advance]
Emergency Maintenance	[TODO: As needed]	[TODO: Ad-hoc]	[TODO: Variable]	[TODO: Immediate]
Patch Window	[TODO: e.g., 2nd Tuesday/month]	[TODO: Monthly]	[TODO: Hours]	[TODO: Days in advance]

5.3.4 Planned Downtimes

Communication Process: 1. **Announcement:** At least [TODO: X days] in advance 2. **Channel:** [TODO: Email, Portal, Ticket System] 3. **Recipients:** [TODO: All users, Key stakeholders] 4. **Content:** Time window, reason, impacts, contact person

Responsible: Andreas Huemmer (andreas.huemmer@adminsend.de)

5.4 Service Level Agreements (SLA)

5.4.1 SLA Overview

Metric	Target Value	Measurement Method	Measurement Source	Reporting
Availability	[TODO: e.g., 99.9%]	[TODO: Uptime monitoring]	[TODO: Monitoring tool]	[TODO: Monthly]
MTTR	[TODO: e.g., 4h]	[TODO: Ticket analysis]	[TODO: ITSM tool]	[TODO: Monthly]
MTBF	[TODO: e.g., 720h]	[TODO: Incident analysis]	[TODO: ITSM tool]	[TODO: Quarterly]
Response Time	[TODO: e.g., < 200ms]	[TODO: APM]	[TODO: APM tool]	[TODO: Daily]
Throughput	[TODO: e.g., 1000 TPS]	[TODO: Performance monitoring]	[TODO: Monitoring tool]	[TODO: Daily]

5.4.2 Service Level Objectives (SLO)

5.4.2.1 Availability

- **Target:** [TODO: e.g., 99.9% uptime per month]
- **Calculation:** (Total time - Downtime) / Total time × 100%
- **Exceptions:** Planned maintenance windows
- **Measurement:** Continuous uptime monitoring

5.4.2.2 Performance

- **Response Time (P95):** [TODO: e.g., < 200ms]
- **Response Time (P99):** [TODO: e.g., < 500ms]
- **Throughput:** [TODO: e.g., min. 1000 requests/second]
- **Error Rate:** [TODO: e.g., < 0.1%]

5.4.2.3 Recovery

- **RTO (Recovery Time Objective):** [TODO: e.g., 4 hours]
- **RPO (Recovery Point Objective):** [TODO: e.g., 1 hour]
- **MTTR (Mean Time To Repair):** [TODO: e.g., 4 hours]
- **MTBF (Mean Time Between Failures):** [TODO: e.g., 720 hours]

5.4.3 SLA Reporting

Reporting Frequency: [TODO: Monthly/Quarterly]

Recipients: - Service Owner: IT Operations Manager - IT Operations Manager: Andreas Huemmer - CIO: Anna Schmidt - [TODO: Additional stakeholders]

Content: - Availability statistics - Performance metrics - Incident overview - SLA compliance - Improvement measures

5.4.4 SLA Violations

Escalation Process for SLA Violation:

1. **Automatic Notification:** Monitoring system
2. **Analysis:** IT Operations team
3. **Escalation Level 1:** IT Operations Manager
4. **Escalation Level 2:** CIO
5. **Root Cause Analysis:** Within [TODO: X days]
6. **Action Plan:** Within [TODO: X days]

5.5 Capacity Planning

5.5.1 Current Capacity

Resource	Current	Maximum	Utilization	Threshold
[TODO: CPU]	[TODO]	[TODO]	[TODO]%	[TODO]%
[TODO: RAM]	[TODO]	[TODO]	[TODO]%	[TODO]%
[TODO: Storage]	[TODO]	[TODO]	[TODO]%	[TODO]%
[TODO: Network]	[TODO]	[TODO]	[TODO]%	[TODO]%

5.5.2 Growth Forecast

- **User Growth:** [TODO: e.g., +10% per year]
- **Data Growth:** [TODO: e.g., +20% per year]
- **Transaction Growth:** [TODO: e.g., +15% per year]

5.5.3 Scaling Strategies

- **Vertical Scaling:** [TODO: Description]
- **Horizontal Scaling:** [TODO: Description]
- **Auto-Scaling:** [TODO: Yes/No, Configuration]

5.6 Responsibilities

Role	Responsibility	Person	Contact
Service Owner	Overall responsibility	IT Operations Manager	[TODO: Email]
Technical Lead	Technical implementation	[TODO: Name]	[TODO: Email]
Operations Manager	Daily operations	Andreas Huemmer	andreas.huemmer@adminsend.de
Service Desk Lead	First-level support	Julia Becker	julia.becker@adminsend.de

5.7 Contacts and Escalation

For questions about the service: - **Service Owner:** IT Operations Manager - **IT Operations Manager:** Andreas Huemmer (andreas.huemmer@adminsend.de) - **Service Desk:** Julia Becker (julia.becker@adminsend.de)

Escalation Path: 1. **Level 1:** Service Desk - julia.becker@adminsend.de 2. **Level 2:** IT Operations - andreas.huemmer@adminsend.de 3. **Level 3:** CIO - anna.schmidt@adminsend.de

---

Service Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

ewpage

Chapter 6

System Overview and Architecture

6.1 Overview

6.1.1 System Landscape

This chapter describes the system landscape and architecture at a high level.

System/Service: [TODO: System/Service Name]

Brief Description: [TODO: Describe the system landscape in 2-3 sentences. What is the purpose of the system? What are the main functions it provides?]

6.1.2 Main Components

Component	Type	Purpose	Technology	Status
[TODO: Component 1]	[TODO: App/DB/Queue]	[TODO: Description]	[TODO: Tech Stack]	[TODO: Active/Planned]
[TODO: Component 2]	[TODO: App/DB/Queue]	[TODO: Description]	[TODO: Tech Stack]	[TODO: Active/Planned]
[TODO: Component 3]	[TODO: App/DB/Queue]	[TODO: Description]	[TODO: Tech Stack]	[TODO: Active/Planned]

6.1.3 Data Flows

Main Data Flows: 1. [TODO: Data Flow 1 - Source → Target] 2. [TODO: Data Flow 2 - Source → Target] 3. [TODO: Data Flow 3 - Source → Target]

Data Volume: - [TODO: e.g., 10,000 Transactions/Day] - [TODO: e.g., 100 GB Data/Month]

6.1.4 User Access

Access Methods: - **Web Interface:** [TODO: URL] - **API:** [TODO: API Endpoint] - **Mobile App:** [TODO: App Name] - **Desktop Client:** [TODO: Client Name]

Authentication: - [TODO: e.g., SSO, LDAP, OAuth2]

Architecture Diagram

Figure 6.1: Architecture Diagram

Network Diagram

Figure 6.2: Network Diagram

6.2 Architecture Diagram

6.2.1 High-Level Architecture

Note: Insert an architecture diagram here or link to it. Recommended Tools: draw.io, PlantUML, Mermaid, Visio

Diagram Description: [TODO: Describe the main elements of the architecture diagram]

6.2.2 Network Architecture

Note: Insert a network diagram here.

Network Segments: - [TODO: e.g., DMZ, Internal, Management]

Firewall Rules: - [TODO: Description of main firewall rules]

6.2.3 Deployment Architecture

Note: Insert a deployment diagram here.

Deployment Model: - [TODO: e.g., On-Premise, Cloud, Hybrid]

6.3 Component List

6.3.1 Application Components

Component	Type	Purpose	Technology	Responsible	Criticality
[TODO: Frontend]	Web App	[TODO: Description]	[TODO: React/Angular/Vue]	[TODO: Team]	L M H
[TODO: Backend]	API Server	[TODO: Description]	[TODO: Node.js/Java/Python]	[TODO: Team]	L M H
[TODO: Worker]	Background Job	[TODO: Description]	[TODO: Technology]	[TODO: Team]	L M H

6.3.2 Data Components

Deployment Diagram

Figure 6.3: Deployment Diagram

Component	Type	Purpose	Technology	Size	Criticality
[TODO: Database]	RDBMS	[TODO: Description]	[TODO: PostgreSQL/MySQL]	[TODO: GB]	L M H
[TODO: Cache]	In-Memory	[TODO: Description]	[TODO: Redis/Memcached]	[TODO: GB]	L M H
[TODO: Queue]	Message Queue	[TODO: Description]	[TODO: RabbitMQ/Kafka]	[TODO: Messages/s]	L M H

6.3.3 Infrastructure Components

Component	Type	Purpose	Technology	Location	Criticality
[TODO: Load Balancer]	LB	[TODO: Description]	[TODO: HAProxy/Nginx]	[TODO: Location]	L M H
[TODO: Firewall]	Security	[TODO: Description]	[TODO: Vendor]	[TODO: Location]	L M H
[TODO: Monitoring]	Observability	[TODO: Description]	[TODO: Prometheus/Grafana]	[TODO: Location]	L M H

Legend: - **L:** Low - **M:** Medium - **H:** High

6.4 Environments

6.4.1 Environment Overview

Environment	Purpose	URL/Endpoint	Characteristics	Access
DEV	Development	[TODO: dev.example.com]	[TODO: Test Data, Debug Mode]	[TODO: Developers]
TEST	Testing/QA	[TODO: test.example.com]	[TODO: Staging Data]	[TODO: QA Team]
STAGE	Pre-Production	[TODO: stage.example.com]	[TODO: Production-like]	[TODO: Ops Team]
PROD	Production	[TODO: www.example.com]	[TODO: Live System]	[TODO: Authorized]

6.4.2 Environment Configuration

6.4.2.1 Development (DEV)

- **Purpose:** Development and initial testing
- **Data:** Synthetic test data
- **Monitoring:** Basic monitoring
- **Backup:** Not required
- **Availability:** Business Hours

6.4.2.2 Test (TEST)

- **Purpose:** Functional and integration testing
- **Data:** Anonymized production data
- **Monitoring:** Full monitoring
- **Backup:** Weekly
- **Availability:** Business Hours

6.4.2.3 Staging (STAGE)

- **Purpose:** Pre-production testing, release validation
- **Data:** Anonymized production data (current)
- **Monitoring:** Identical to production
- **Backup:** Daily
- **Availability:** 24/7

6.4.2.4 Production (PROD)

- **Purpose:** Live operation
- **Data:** Production data
- **Monitoring:** 24/7 monitoring with alerting
- **Backup:** Multiple times daily
- **Availability:** 24/7 (according to SLA)

6.4.3 Promotion Process

Deployment Pipeline: 1. **DEV:** Automatic deployment on code commit 2. **TEST:** Automatic deployment after successful unit tests 3. **STAGE:** Manual deployment after QA approval 4. **PROD:** Manual deployment after change approval

Approvals: - **DEV → TEST:** Automatic - **TEST → STAGE:** QA Team - **STAGE → PROD:** CIO + Change Advisory Board

6.5 Interfaces

6.5.1 Inbound Interfaces

Partner/System	Protocol	Authentication	Data Format	Purpose	SLA
[TODO: System 1]	[TODO: HTTPS/REST]	[TODO: OAuth2/API Key]	[TODO: JSON/XML]	[TODO: Description]	[TODO: 99.9%]
[TODO: System 2]	[TODO: MQ/AMQP]	[TODO: Certificate]	[TODO: JSON]	[TODO: Description]	[TODO: 99.5%]
[TODO: System 3]	[TODO: SOAP]	[TODO: WS-Security]	[TODO: XML]	[TODO: Description]	[TODO: 99.0%]

6.5.2 Outbound Interfaces

Partner/System	Protocol	Authentication	Data Format	Purpose	SLA
[TODO: System 1]	[TODO: HTTPS/REST]	[TODO: OAuth2]	[TODO: JSON]	[TODO: Description]	[TODO: 99.9%]
[TODO: System 2]	[TODO: SMTP]	[TODO: TLS]	[TODO: Email]	[TODO: Description]	[TODO: 99.0%]
[TODO: System 3]	[TODO: FTP/SFTP]	[TODO: SSH Key]	[TODO: CSV]	[TODO: Description]	[TODO: 99.5%]

6.5.3 API Endpoints

Endpoint	Method	Authentication	Rate Limit	Description
[TODO: /api/v1/users]	GET/POST	[TODO: Bearer Token]	[TODO: 1000/h]	[TODO: User Management]
[TODO: /api/v1/data]	GET/PUT	[TODO: API Key]	[TODO: 5000/h]	[TODO: Data Access]
[TODO: /api/v1/status]	GET	[TODO: None]	[TODO: Unlimited]	[TODO: Health Check]

6.5.4 Interface Documentation

API Documentation: [TODO: Link to API documentation (e.g., Swagger/OpenAPI)]

Integration Guide: [TODO: Link to integration guide]

6.6 Dependencies on Other Systems

6.6.1 Upstream Systems (Dependencies)

System	Type	Criticality	Impact on Failure	Fallback
[TODO: System 1]	[TODO: Data Source]	L M H	[TODO: Description]	[TODO: Fallback Strategy]
[TODO: System 2]	[TODO: Auth Provider]	L M H	[TODO: Description]	[TODO: Fallback Strategy]
[TODO: System 3]	[TODO: Payment Gateway]	L M H	[TODO: Description]	[TODO: Fallback Strategy]

6.6.2 Downstream Systems (Dependent Systems)

System	Type	Criticality	Impact on Failure	Notification
[TODO: System 1]	[TODO: Reporting]	L M H	[TODO: Description]	[TODO: Yes/No]
[TODO: System 2]	[TODO: Analytics]	L M H	[TODO: Description]	[TODO: Yes/No]

System	Type	Criticality	Impact on Failure	Notification
[TODO: System 3]	[TODO: Archiving]	L M H	[TODO: Description]	[TODO: Yes/No]

6.7 Technology Stack

6.7.1 Frontend

- **Framework:** [TODO: e.g., React 18.x]
- **UI Library:** [TODO: e.g., Material-UI]
- **State Management:** [TODO: e.g., Redux]
- **Build Tool:** [TODO: e.g., Webpack/Vite]

6.7.2 Backend

- **Runtime:** [TODO: e.g., Node.js 20.x]
- **Framework:** [TODO: e.g., Express.js]
- **ORM:** [TODO: e.g., Sequelize/TypeORM]
- **API Style:** [TODO: REST/GraphQL/gRPC]

6.7.3 Database

- **RDBMS:** [TODO: e.g., PostgreSQL 15.x]
- **NoSQL:** [TODO: e.g., MongoDB 6.x]
- **Cache:** [TODO: e.g., Redis 7.x]
- **Search:** [TODO: e.g., Elasticsearch 8.x]

6.7.4 Infrastructure

- **Container:** [TODO: e.g., Docker]
- **Orchestration:** [TODO: e.g., Kubernetes]
- **Cloud Provider:** [TODO: e.g., AWS/Azure/GCP]
- **IaC:** [TODO: e.g., Terraform/Ansible]

6.7.5 Monitoring and Observability

- **Metrics:** [TODO: e.g., Prometheus]
- **Logging:** [TODO: e.g., ELK Stack]
- **Tracing:** [TODO: e.g., Jaeger]
- **Dashboards:** [TODO: e.g., Grafana]

6.8 Security Architecture

6.8.1 Network Segmentation

- **DMZ:** [TODO: Description]
- **Application Tier:** [TODO: Description]
- **Data Tier:** [TODO: Description]

- **Management Tier:** [TODO: Description]

6.8.2 Access Control

- **Authentication:** [TODO: e.g., SSO, MFA]
- **Authorization:** [TODO: e.g., RBAC, ABAC]
- **Encryption:** [TODO: e.g., TLS 1.3, AES-256]

6.8.3 Security Components

- **WAF:** [TODO: Web Application Firewall]
- **IDS/IPS:** [TODO: Intrusion Detection/Prevention]
- **SIEM:** [TODO: Security Information and Event Management]

6.9 Responsibilities

Role	Responsibility	Person	Contact
System Architect	Architecture Design	[TODO: Name]	[TODO: Email]
Technical Lead	Technical Implementation	[TODO: Name]	[TODO: Email]
Operations Manager	Operation and Maintenance	Andreas Huemmer	andreas.huemmer@adminsend.de
Security Officer	Security Architecture	Thomas Weber	thomas.weber@adminsend.de

6.10 Contacts

For System Architecture Questions: - **System Architect:** [TODO: Name and Contact] - **IT Operations Manager:** Andreas Huemmer (andreas.huemmer@adminsend.de) - **CISO:** Thomas Weber (thomas.weber@adminsend.de)

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

ewpage

Chapter 7

Infrastructure and Platform

7.1 Overview

7.1.1 Infrastructure Landscape

This chapter describes the physical and virtual infrastructure on which IT services are operated.

Organization: AdminSend GmbH
Location: München, Deutschland

Brief Description: [TODO: Describe the infrastructure landscape in 2-3 sentences. What are the main components? Where is the infrastructure operated?]

7.1.2 Infrastructure Overview

Category	Count	Type	Location	Criticality
Physical Servers	[TODO]	[TODO: Rack/Blade]	[TODO]	L M H
Virtual Machines	[TODO]	[TODO: VMware/Hyper-V]	[TODO]	L M H
Containers	[TODO]	[TODO: Docker/K8s]	[TODO]	L M H
Cloud Instances	[TODO]	[TODO: AWS/Azure/GCP]	[TODO]	L M H
Network Devices	[TODO]	[TODO: Switch/Router]	[TODO]	L M H
Storage Systems	[TODO]	[TODO: SAN/NAS]	[TODO]	L M H

Legend: - **L:** Low - **M:** Medium - **H:** High

7.2 Physical Infrastructure

7.2.1 Data Centers and Sites

7.2.1.1 Primary Site

- **Site Name:** {{ netbox.site.name }}
- **Address:** {{ netbox.site.physical_address }}
- **Data Center:** {{ netbox.site.facility }}
- **Operator:** [TODO: DC Operator]
- **Certifications:** [TODO: e.g., ISO 27001, Tier III]

Site Details: - **Availability:** [TODO: e.g., 99.99%] - **Power Supply:** [TODO: e.g., Redundant UPS, Emergency Power] - **Cooling:** [TODO: e.g., Redundant Air Conditioning] - **Fire Protection:** [TODO: e.g., Gas Suppression System] - **Access Control:** [TODO: e.g., Biometric, 24/7 Surveillance]

7.2.1.2 Secondary Site (DR)

- **Site Name:** [TODO: DR Site]
- **Address:** [TODO: Address]
- **Data Center:** [TODO: DC Name]
- **Operator:** [TODO: DC Operator]
- **Distance to Primary Site:** [TODO: km]

DR Configuration: - **DR Strategy:** [TODO: Hot/Warm/Cold Standby] - **Replication:** [TODO: Synchronous/Asynchronous] - **RTO:** [TODO: Hours] - **RPO:** [TODO: Hours]

7.2.2 Rack Overview

Rack ID	Location	Height (U)	Utilization	Power Supply	Network
[TODO: RACK-01]	{{ netbox.site.name }}	[TODO: 42]	[TODO: 80%]	[TODO: 2x 32A]	[TODO: 2x 10G]
[TODO: RACK-02]	{{ netbox.site.name }}	[TODO: 42]	[TODO: 60%]	[TODO: 2x 32A]	[TODO: 2x 10G]
[TODO: RACK-03]	{{ netbox.site.name }}	[TODO: 42]	[TODO: 40%]	[TODO: 2x 16A]	[TODO: 2x 1G]

7.2.3 Server Hardware

Hostname	Type	CPU	RAM	Storage	Location	Rack	Role
{{ netbox.device.serial }}	[TODO: Dell R740]	[TODO: 2x Xeon]	[TODO: 256GB]	[TODO: 2TB SSD]	{{ netbox.site.name }}	[TODO: RACK-01]	[TODO: Hypervisor]

Hostname	Type	CPU	RAM	Storage	Location	Rack	Role
{{ net-box.device.server02.name }}	[TODO: HP DL380]	[TODO: 2x Xeon]	[TODO: 128GB]	[TODO: 1TB SSD]	{{ net-box.site.name }}	[TODO: RACK-01]	[TODO: Hypervisor]
{{ net-box.device.server03.name }}	[TODO: Dell R640]	[TODO: 2x Xeon]	[TODO: 64GB]	[TODO: 500GB SSD]	{{ net-box.site.name }}	[TODO: RACK-02]	[TODO: Application]

Hardware Lifecycle: - **Procurement:** [TODO: Process] - **Warranty:** [TODO: e.g., 5 years NBD] - **Refresh Cycle:** [TODO: e.g., 5 years] - **End-of-Life:** [TODO: Process]

7.3 Network Infrastructure

7.3.1 Network Architecture

Network Topology: [TODO: e.g., Spine-Leaf, Three-Tier]

Redundancy: [TODO: e.g., Fully Redundant, N+1]

7.3.2 Core Network

Device	Type	Model	Location	Role	Uplinks
{{ net-box.device.core_switch01.name }}	Core Switch	[TODO: Cisco Nexus]	{{ net-box.site.name }}	[TODO: Core]	[TODO: 4x 100G]
{{ net-box.device.core_switch02.name }}	Core Switch	[TODO: Cisco Nexus]	{{ net-box.site.name }}	[TODO: Core]	[TODO: 4x 100G]

7.3.3 Distribution Layer

Device	Type	Model	Location	Role	Uplinks
[TODO: DIST-SW-01]	Distribution Switch	[TODO: Model]	{{ net-box.site.name }}	[TODO: Distribution]	[TODO: 2x 40G]
[TODO: DIST-SW-02]	Distribution Switch	[TODO: Model]	{{ net-box.site.name }}	[TODO: Distribution]	[TODO: 2x 40G]

7.3.4 Access Layer

Device	Type	Model	Location	Ports	Uplinks
[TODO: ACC-SW-01]	Access Switch	[TODO: Model]	{{ net-box.site.name }}	[TODO: 48x 1G]	[TODO: 2x 10G]
[TODO: ACC-SW-02]	Access Switch	[TODO: Model]	{{ net-box.site.name }}	[TODO: 48x 1G]	[TODO: 2x 10G]

7.3.5 VLAN Segmentation

VLAN ID	Name	Purpose	Subnet	Gateway
{{ net-box.vlan.management.vid }}	Management	[TODO: Management Network]	{{ net-box.vlan.management.prefix }}	[TODO: Gateway]
{{ net-box.vlan.production.vid }}	Production	[TODO: Production Network]	{{ net-box.vlan.production.prefix }}	[TODO: Gateway]
[TODO: 30]	DMZ	[TODO: DMZ Network]	[TODO: 10.0.30.0/24]	[TODO: 10.0.30.1]
[TODO: 40]	Storage	[TODO: Storage Network]	[TODO: 10.0.40.0/24]	[TODO: 10.0.40.1]
[TODO: 50]	Backup	[TODO: Backup Network]	[TODO: 10.0.50.0/24]	[TODO: 10.0.50.1]

7.3.6 IP Addressing

IP Address Plan:

Network	Usage	CIDR	Available IPs	Utilization
[TODO: 10.0.0.0/16]	Total	[TODO: /16]	[TODO: 65534]	[TODO: 40%]
[TODO: 10.0.10.0/24]	Management	[TODO: /24]	[TODO: 254]	[TODO: 60%]
[TODO: 10.0.20.0/24]	Production	[TODO: /24]	[TODO: 254]	[TODO: 80%]
[TODO: 10.0.30.0/24]	DMZ	[TODO: /24]	[TODO: 254]	[TODO: 30%]

IPAM (IP Address Management): - **Tool:** [TODO: e.g., NetBox, phpIPAM] - **Responsible:** Andreas Huemmer

7.3.7 Firewall and Security

Device	Type	Model	Location	Role	Throughput
[TODO: FW-01]	Firewall	[TODO: Palo Alto]	{{ net-box.site.name }}	[TODO: Perimeter]	[TODO: 10 Gbps]
[TODO: FW-02]	Firewall	[TODO: Palo Alto]	{{ net-box.site.name }}	[TODO: Perimeter]	[TODO: 10 Gbps]

Firewall Rules: - **Number of Rules:** [TODO: e.g., 500] - **Review Cycle:** [TODO: e.g., Quarterly] - **Responsible:** Thomas Weber

7.3.8 Load Balancer

Device	Type	Model	Location	Algorithm	Capacity
[TODO: LB-01]	Load Balancer	[TODO: F5/HAProxy]	{{ net-box.site.name }}	[TODO: Round-Robin]	[TODO: 10k RPS]
[TODO: LB-02]	Load Balancer	[TODO: F5/HAProxy]	{{ net-box.site.name }}	[TODO: Round-Robin]	[TODO: 10k RPS]

7.3.9 WAN Connections

Provider	Type	Bandwidth	Location	SLA	Cost/Month
[TODO: Provider 1]	[TODO: MPLS]	[TODO: 1 Gbps]	{{ net-box.site.name }}	[TODO: 99.9%]	[TODO: EUR]
[TODO: Provider 2]	[TODO: Internet]	[TODO: 500 Mbps]	{{ net-box.site.name }}	[TODO: 99.5%]	[TODO: EUR]

7.4 Virtualization

7.4.1 Virtualization Platform

Hypervisor: [TODO: e.g., VMware vSphere 8.0, Microsoft Hyper-V, KVM]

Management: [TODO: e.g., vCenter Server, SCVMM]

7.4.2 Cluster Configuration

Cluster Name	Hypervisor	Hosts	vCPUs	RAM (GB)	Storage (TB)	VMs
{{ net-box.cluster.prod.name }}	[TODO: VMware]	[TODO: 4]	[TODO: 128]	[TODO: 1024]	[TODO: 50]	[TODO: 80]
{{ net-box.cluster.test.name }}	[TODO: VMware]	[TODO: 2]	[TODO: 64]	[TODO: 512]	[TODO: 20]	[TODO: 40]

Cluster Features: - **HA (High Availability):** [TODO: Yes/No, Configuration] - **DRS (Distributed Resource Scheduler):** [TODO: Yes/No, Mode] - **vMotion/Live Migration:** [TODO: Yes/No] - **Fault Tolerance:** [TODO: Yes/No]

7.4.3 Virtual Machines

VM Name	Cluster	vCPU	RAM (GB)	Storage (GB)	OS	Role	Status
{{ net-box.vm.app01.name }}	{{ net-box.cluster.prod.name }}	[TODO: 4]	[TODO: 16]	[TODO: 200]	[TODO: Ubuntu 22.04]	[TODO: App Server]	[TODO: Running]
{{ net-box.vm.db01.name }}	{{ net-box.cluster.prod.name }}	[TODO: 8]	[TODO: 32]	[TODO: 500]	[TODO: RHEL 9]	[TODO: DB Server]	[TODO: Running]
{{ net-box.vm.web01.name }}	{{ net-box.cluster.prod.name }}	[TODO: 2]	[TODO: 8]	[TODO: 100]	[TODO: Ubuntu 22.04]	[TODO: Web Server]	[TODO: Running]

VM Lifecycle: - **Provisioning:** [TODO: Automated/Manual, Tool] - **Template Management:** [TODO: Process] - **Snapshot Policy:** [TODO: Policy] - **Decommissioning:** [TODO: Process]

7.4.4 Resource Pools

Pool Name	Cluster	CPU Shares	RAM Reservation	Purpose
[TODO: Production]	{{ net-box.cluster.prod.name }}	[TODO: High]	[TODO: 50%]	[TODO: Production VMs]
[TODO: Development]	{{ net-box.cluster.test.name }}	[TODO: Normal]	[TODO: 25%]	[TODO: Development VMs]
[TODO: Test]	{{ net-box.cluster.test.name }}	[TODO: Low]	[TODO: 10%]	[TODO: Test VMs]

7.5 Container Orchestration

7.5.1 Kubernetes Clusters

Kubernetes Version: [TODO: e.g., 1.28.x]

Distribution: [TODO: e.g., Vanilla K8s, OpenShift, Rancher, EKS, AKS, GKE]

Cluster Name	Environment	Nodes	Pods	Namespaces	Ingress
[TODO: k8s-prod]	Production	[TODO: 6]	[TODO: 200]	[TODO: 20]	[TODO: Nginx]
[TODO: k8s-test]	Test	[TODO: 3]	[TODO: 50]	[TODO: 10]	[TODO: Nginx]

7.5.2 Node Configuration

Node Name	Role	CPU	RAM (GB)	Storage (GB)	Status
[TODO: k8s-master-01]	Control Plane	[TODO: 4]	[TODO: 16]	[TODO: 100]	[TODO: Ready]
[TODO: k8s-worker-01]	Worker	[TODO: 8]	[TODO: 32]	[TODO: 200]	[TODO: Ready]
[TODO: k8s-worker-02]	Worker	[TODO: 8]	[TODO: 32]	[TODO: 200]	[TODO: Ready]

7.5.3 Container Registry

- **Registry:** [TODO: e.g., Harbor, Docker Hub, ECR, ACR, GCR]
- **URL:** [TODO: registry.example.com]
- **Authentication:** [TODO: e.g., LDAP, OAuth2]
- **Scanning:** [TODO: e.g., Trivy, Clair]

7.5.4 Helm Charts

- **Chart Repository:** [TODO: URL]
- **Number of Charts:** [TODO: e.g., 50]
- **Versioning:** [TODO: Process]

7.6 Cloud Infrastructure

7.6.1 Cloud Providers

Primary Cloud Provider: [TODO: e.g., AWS, Azure, Google Cloud]

Cloud Strategy: [TODO: e.g., Cloud-First, Hybrid, Multi-Cloud]

7.6.2 Cloud Accounts

Account Name	Provider	Account ID	Environment	Purpose	Cost/Month
[TODO: prod-account]	[TODO: AWS]	[TODO: 123456789012]	Production	[TODO: Production Workloads]	[TODO: EUR]
[TODO: dev-account]	[TODO: AWS]	[TODO: 987654321098]	Development	[TODO: Development/Test]	[TODO: EUR]

7.6.3 Cloud Regions

Region	Provider	Location	Purpose	Services
[TODO: eu-central-1]	[TODO: AWS]	Frankfurt	[TODO: Primary]	[TODO: EC2, RDS, S3]
[TODO: eu-west-1]	[TODO: AWS]	Ireland	[TODO: DR]	[TODO: EC2, RDS, S3]

7.6.4 Cloud Resources

7.6.4.1 Compute (IaaS)

Resource	Type	Size	Count	Region	Purpose	Cost/Month
[TODO: EC2 Instances]	[TODO: t3.large]	[TODO: 2vCPU/8GB]	[TODO: 10]	[TODO: eu-central-1]	[TODO: App Servers]	[TODO: EUR]
[TODO: Lambda Functions]	[TODO: Serverless]	[TODO: -]	[TODO: 50]	[TODO: eu-central-1]	[TODO: Microservices]	[TODO: EUR]

7.6.4.2 Storage

Resource	Type	Size (TB)	Region	Purpose	Cost/Month
[TODO: S3 Buckets]	[TODO: Object Storage]	[TODO: 10]	[TODO: eu-central-1]	[TODO: Backups]	[TODO: EUR]
[TODO: EBS Volumes]	[TODO: Block Storage]	[TODO: 5]	[TODO: eu-central-1]	[TODO: VM Storage]	[TODO: EUR]

7.6.4.3 Database (PaaS)

Resource	Type	Size	Region	Purpose	Cost/Month
[TODO: RDS PostgreSQL]	[TODO: db.r5.large]	[TODO: 500GB]	[TODO: eu-central-1]	[TODO: Production DB]	[TODO: EUR]
[TODO: DynamoDB]	[TODO: NoSQL]	[TODO: On-Demand]	[TODO: eu-central-1]	[TODO: Session Store]	[TODO: EUR]

7.6.4.4 Networking

Resource	Type	Configuration	Region	Purpose
[TODO: VPC]	[TODO: Virtual Network]	[TODO: 10.0.0.0/16]	[TODO: eu-central-1]	[TODO: Network Isolation]
[TODO: VPN Gateway]	[TODO: Site-to-Site VPN]	[TODO: 1 Gbps]	[TODO: eu-central-1]	[TODO: Hybrid Connectivity]
[TODO: Direct Connect]	[TODO: Dedicated Line]	[TODO: 10 Gbps]	[TODO: eu-central-1]	[TODO: Low Latency]

7.6.5 Cloud Costs

Total Cost/Month: [TODO: EUR]

Cost Optimization: - **Reserved Instances:** [TODO: Percentage] - **Spot Instances:** [TODO: Percentage] - **Auto-Scaling:** [TODO: Yes/No] - **Cost Monitoring:** [TODO: Tool]

7.7 Storage Infrastructure

7.7.1 Storage Systems

System	Type	Capacity (TB)	Usage (%)	Protocol	Location	Purpose
[TODO: SAN-01]	SAN	[TODO: 100]	[TODO: 70%]	[TODO: FC/iSCSI]	{{ net-box.site.name }}	[TODO: VM Storage]
[TODO: NAS-01]	NAS	[TODO: 50]	[TODO: 60%]	[TODO: NFS/CIFS]	{{ net-box.site.name }}	[TODO: File Shares]
[TODO: OBJ-01]	Object Storage	[TODO: 200]	[TODO: 40%]	[TODO: S3]	[TODO: Cloud]	[TODO: Backups]

7.7.2 Storage Tiers

Tier	Type	Performance	Capacity (TB)	Cost/TB	Usage
Tier 0	[TODO: NVMe SSD]	[TODO: >100k IOPS]	[TODO: 10]	[TODO: High]	[TODO: Databases]

Tier	Type	Performance	Capacity (TB)	Cost/TB	Usage
Tier 1	[TODO: SAS SSD]	[TODO: 50k IOPS]	[TODO: 50]	[TODO: Medium]	[TODO: VMs]
Tier 2	[TODO: SAS HDD]	[TODO: 5k IOPS]	[TODO: 100]	[TODO: Low]	[TODO: Archive]

7.7.3 Storage Network

SAN Fabric: - **Protocol:** [TODO: e.g., Fibre Channel 32G, iSCSI 10G] - **Switches:** [TODO: e.g., Brocade, Cisco MDS] - **Redundancy:** [TODO: e.g., Dual-Fabric]

NAS Network: - **Protocol:** [TODO: e.g., NFS v4, SMB 3.0] - **Network:** [TODO: e.g., Dedicated 10G Network]

7.7.4 Backup Storage

System	Type	Capacity (TB)	Retention	Location	Purpose
[TODO: BACKUP-01]	[TODO: Disk]	[TODO: 100]	[TODO: 30 Days]	{{ netbox.site.name }}	[TODO: Disk Backup]
[TODO: TAPE-01]	[TODO: Tape Library]	[TODO: 500]	[TODO: 7 Years]	{{ netbox.site.name }}	[TODO: Long-term Archive]
[TODO: CLOUD-BACKUP]	[TODO: Cloud]	[TODO: Unlimited]	[TODO: 90 Days]	[TODO: Cloud]	[TODO: Off-Site Backup]

7.8 Power Supply

7.8.1 Primary Power Supply

- **Connection Capacity:** [TODO: e.g., 200 kW]
- **Redundancy:** [TODO: e.g., N+1, 2N]
- **Provider:** [TODO: Energy Provider]

7.8.2 UPS (Uninterruptible Power Supply)

UPS System	Capacity (kVA)	Runtime (min)	Location	Status
[TODO: UPS-01]	[TODO: 100]	[TODO: 15]	{{ netbox.site.name }}	[TODO: Online]
[TODO: UPS-02]	[TODO: 100]	[TODO: 15]	{{ netbox.site.name }}	[TODO: Online]

UPS Maintenance: - **Maintenance Interval:** [TODO: e.g., Quarterly] - **Battery Test:** [TODO: e.g., Monthly] - **Responsible:** [TODO: Facility Management]

7.8.3 Emergency Power Supply

- **Emergency Generator:** [TODO: e.g., 250 kVA Diesel]
- **Fuel Reserve:** [TODO: e.g., 1000 Liters]
- **Runtime:** [TODO: e.g., 48 Hours]
- **Switchover Time:** [TODO: e.g., $<$ 10 Seconds]

7.9 Cooling and Air Conditioning

7.9.1 Air Conditioning

- **Cooling Capacity:** [TODO: e.g., 150 kW]
- **Redundancy:** [TODO: e.g., N+1]
- **Target Temperature:** [TODO: e.g., 22°C ±2°C]
- **Humidity:** [TODO: e.g., 45% ±5%]

7.9.2 Monitoring

- **Temperature Sensors:** [TODO: Number and Positions]
- **Humidity Sensors:** [TODO: Number and Positions]
- **Alarms:** [TODO: Thresholds and Escalation]

7.10 Physical Security

7.10.1 Access Control

- **System:** [TODO: e.g., Biometric, Card Access]
- **Authorized Personnel:** [TODO: Number of People]
- **Logging:** [TODO: Retention Period]
- **Four-Eyes Principle:** [TODO: Yes/No, for which Areas]

7.10.2 Video Surveillance

- **Cameras:** [TODO: Number and Positions]
- **Recording:** [TODO: Retention Period]
- **Monitoring:** [TODO: 24/7 or Time-controlled]

7.10.3 Fire Protection

- **Fire Alarm System:** [TODO: Type]
- **Suppression System:** [TODO: e.g., Gas Suppression, Sprinkler]
- **Fire Compartments:** [TODO: Number]
- **Escape Routes:** [TODO: Number and Marking]

7.11 Capacity Planning

7.11.1 Current Utilization

Resource	Capacity	Used	Available	Utilization (%)	Threshold (%)
CPU (Cores)	[TODO: 500]	[TODO: 300]	[TODO: 200]	[TODO: 60%]	[TODO: 80%]
RAM (GB)	[TODO: 4000]	[TODO: 2800]	[TODO: 1200]	[TODO: 70%]	[TODO: 85%]
Storage (TB)	[TODO: 200]	[TODO: 140]	[TODO: 60]	[TODO: 70%]	[TODO: 80%]
Network (Gbps)	[TODO: 100]	[TODO: 40]	[TODO: 60]	[TODO: 40%]	[TODO: 70%]

7.11.2 Growth Forecast

Forecast Period: [TODO: e.g., 12 Months]

Resource	Current	Forecast (+12M)	Growth (%)	Actions
CPU	[TODO: 300 Cores]	[TODO: 360 Cores]	[TODO: +20%]	[TODO: Description]
RAM	[TODO: 2800 GB]	[TODO: 3360 GB]	[TODO: +20%]	[TODO: Description]
Storage	[TODO: 140 TB]	[TODO: 182 TB]	[TODO: +30%]	[TODO: Description]

7.11.3 Scaling Strategies

Vertical Scaling: - [TODO: Strategy Description] - [TODO: Maximum Limits]

Horizontal Scaling: - [TODO: Strategy Description] - [TODO: Auto-Scaling Configuration]

Cloud Bursting: - [TODO: Yes/No, Description]

7.12 Lifecycle Management

7.12.1 Hardware Lifecycle

Phase	Duration	Activities	Responsible
Procurement	[TODO: 4-8 Weeks]	[TODO: Requirements, Ordering, Delivery]	Andreas Huemmer
Commissioning	[TODO: 1-2 Weeks]	[TODO: Installation, Configuration, Testing]	[TODO: Team]

Phase	Duration	Activities	Responsible
Operation	[TODO: 5 Years]	[TODO: Monitoring, Maintenance, Support]	[TODO: Team]
Refresh	[TODO: 1-2 Weeks]	[TODO: Migration, Replacement]	[TODO: Team]
Disposal	[TODO: 1 Week]	[TODO: Data Erasure, Recycling]	[TODO: Team]

7.12.2 Software Lifecycle

Phase	Duration	Activities	Responsible
Evaluation	[TODO: 2-4 Weeks]	[TODO: Requirements Analysis, PoC]	[TODO: Team]
Procurement	[TODO: 2-4 Weeks]	[TODO: Licensing, Contracts]	[TODO: Team]
Implementation	[TODO: 4-8 Weeks]	[TODO: Installation, Configuration]	[TODO: Team]
Operation	[TODO: 3-5 Years]	[TODO: Support, Updates]	[TODO: Team]
Retirement	[TODO: 8-12 Weeks]	[TODO: Migration, Decommissioning]	[TODO: Team]

7.12.3 End-of-Life Management

Hardware: - **Data Erasure:** [TODO: Process, e.g., DoD 5220.22-M] - **Certificate:** [TODO: Yes/No] - **Recycling:** [TODO: Certified Partner]

Software: - **License Return:** [TODO: Process] - **Data Export:** [TODO: Process] - **Documentation:** [TODO: Archiving]

7.13 Compliance and Certifications

7.13.1 Data Center Certifications

- **ISO 27001:** [TODO: Yes/No, Valid Until]
- **ISO 9001:** [TODO: Yes/No, Valid Until]
- **Tier Certification:** [TODO: Tier I/II/III/IV]
- **PCI-DSS:** [TODO: Yes/No, Level]

7.13.2 Compliance Requirements

- **GDPR:** [TODO: Measures]
- **BSI Grundschutz:** [TODO: Yes/No, Module]
- **KRITIS:** [TODO: Yes/No, Sector]

7.14 Responsibilities

Role	Responsibility	Person	Contact
Infrastructure Manager	Overall Infrastructure Responsibility	Andreas Huemmer	andreas.huemmer@adminsend.de
Network Administrator	Network Infrastructure	[TODO: Name]	[TODO: Email]
Storage Administrator	Storage Systems	[TODO: Name]	[TODO: Email]
Virtualization Admin	Virtualization	[TODO: Name]	[TODO: Email]
Cloud Architect	Cloud Infrastructure	[TODO: Name]	[TODO: Email]
Facility Manager	Physical Infrastructure	[TODO: Name]	[TODO: Email]

7.15 Contacts

For Infrastructure Questions: - **IT Operations Manager:** Andreas Huemmer (andreas.huemmer@adminsend.de) - **CIO:** Anna Schmidt (anna.schmidt@adminsend.de)

Emergency Contacts: - **Data Center:** [TODO: Phone 24/7] - **Power Provider:** [TODO: Phone] - **Facility Management:** [TODO: Phone]

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

ewpage

Chapter 8

Roles and Responsibilities

8.1 Organizational Structure

8.1.1 Company Information

- **Organization:** AdminSend GmbH
- **Address:** Musterstraße 123, 80331 München
- **Country:** Deutschland
- **Website:** https://www.adminsend.de
- **Phone:** +49 89 12345678
- **Email:** info@adminsend.de

8.1.2 Organizational Overview

[TODO: Insert organizational chart or description of organizational structure here]

8.2 Executive Level

8.2.1 Chief Executive Officer (CEO)

- **Name:** Max Mustermann
- **Title:** Chief Executive Officer
- **Email:** max.mustermann@adminsend.de
- **Phone:** +49 89 12345678-100
- **Department:** Management

Responsibilities: - Overall responsibility for the company - Strategic direction and corporate objectives - Approval of critical IT investments - Escalation point for business-critical IT incidents

8.2.2 Chief Information Officer (CIO)

- **Name:** Anna Schmidt
- **Title:** Chief Information Officer
- **Email:** anna.schmidt@adminsend.de
- **Phone:** +49 89 12345678-200
- **Department:** IT

Responsibilities: - Overall responsibility for IT strategy and operations - IT budget and resource planning - IT governance and compliance - Approval of major changes - Responsibility for IT service quality and SLA compliance

8.2.3 Chief Information Security Officer (CISO)

- **Name:** Thomas Weber
- **Title:** Chief Information Security Officer
- **Email:** thomas.weber@adminsend.de
- **Phone:** +49 89 12345678-300
- **Department:** IT Security

Responsibilities: - IT security strategy and policies - Information Security Management System (ISMS) - Security incident response - Compliance with security standards (ISO 27001, BSI Grundschutz) - Risk management and vulnerability management - Security awareness and training

8.2.4 Chief Financial Officer (CFO)

- **Name:** Maria Müller
- **Title:** Chief Financial Officer
- **Email:** maria.mueller@adminsend.de
- **Phone:** +49 89 12345678-400
- **Department:** Finance

Responsibilities: - Financial approval of IT projects - IT budget monitoring - Cost-benefit analysis for IT investments - Financial compliance and audits

8.2.5 Chief Operating Officer (COO)

- **Name:** Peter Fischer
- **Title:** Chief Operating Officer
- **Email:** peter.fischer@adminsend.de
- **Phone:** +49 89 12345678-500
- **Department:** Operations

Responsibilities: - Operational business processes - Business continuity management - Coordination between IT and business units - Service level requirements from business perspective

8.3 IT Operations Level

8.3.1 IT Operations Manager

- **Name:** Andreas Huemmer
- **Title:** IT Operations Manager
- **Email:** andreas.huemmer@adminsend.de
- **Phone:** +49 89 12345678-250
- **Department:** IT Operations

Responsibilities: - Daily IT operations and service delivery - Monitoring and incident management - Change management coordination - Capacity and performance management - IT operations team leadership - Escalation management for operational incidents - Ensuring SLA compliance

Deputy: [TODO: Name and contact of deputy]

8.3.2 Service Desk Lead

- **Name:** Julia Becker
- **Title:** Service Desk Lead
- **Email:** julia.becker@adminsend.de
- **Phone:** +49 89 12345678-111
- **Department:** Service Desk

Responsibilities: - First-level support and incident management - Ticket management and prioritization - User communication - Service catalog maintenance - Service desk team leadership - Service desk metrics and reporting

Deputy: [TODO: Name and contact of deputy]

8.4 Additional IT Roles

8.4.1 System Administrator

- **Name:** [TODO: Name]
- **Email:** [TODO: Email]
- **Phone:** [TODO: Phone]

Responsibilities: - Server and system administration - Patch and update management - Backup and restore - System monitoring - System configuration documentation

8.4.2 Network Administrator

- **Name:** [TODO: Name]
- **Email:** [TODO: Email]
- **Phone:** [TODO: Phone]

Responsibilities: - Network infrastructure management - Firewall and security configuration - Network monitoring - VPN and remote access management - Network documentation

8.4.3 Database Administrator (DBA)

- **Name:** [TODO: Name]
- **Email:** [TODO: Email]
- **Phone:** [TODO: Phone]

Responsibilities: - Database administration and optimization - Database backup and recovery - Performance tuning - Database security - Database monitoring

8.4.4 Application Manager

- **Name:** [TODO: Name]
- **Email:** [TODO: Email]
- **Phone:** [TODO: Phone]

Responsibilities: - Application support and maintenance - Release management for applications - Application monitoring - Coordination with development teams - Application documentation

8.4.5 Security Administrator

- **Name:** [TODO: Name]
- **Email:** [TODO: Email]
- **Phone:** [TODO: Phone]

Responsibilities: - Security monitoring and incident response - Vulnerability scanning and management - Security patch management - Access management and permissions - Security audits and compliance checks

8.5 RACI Matrix for IT Operations Activities

The RACI matrix defines responsibilities for IT operations activities: - **R** = Responsible (execution responsibility) - **A** = Accountable (overall responsibility, decision authority) - **C** = Consulted (must be consulted) - **I** = Informed (must be informed)

8.5.1 Service Management

Activity	CEO	CIO	CISO	CFO	COO	Ops Manager	Service Desk	Sys Admin	Net Admin	DBA	App Manager	Sec Admin
Service Strategy	A	R	C	C	C	C	I	I	I	I	I	I
Service Design	I	A	C	I	C	R	C	C	C	C	C	C
Service Transition	I	A	C	I	C	R	C	R	R	R	R	C
Service Operation	I	A	C	I	I	R	R	R	R	R	R	R
Continual Improvement	I	A	C	I	C	R	C	C	C	C	C	C

8.5.2 Incident Management

Activity	CEO	CIO	CISO	CFO	COO	Ops Manager	Service Desk	Sys Admin	Net Admin	DBA	App Manager	Sec Admin
Incident Recording	I	I	I	I	C	R	C	C	C	C	C
Incident Classification	I	C	I	I	C	R	C	C	C	C	C
Incident Diagnosis	I	C	I	I	C	R	R	R	R	R	R
Incident Resolution	I	C	I	I	A	C	R	R	R	R	R
Incident Closure	I	I	I	I	A	R	C	C	C	C	C
Major Incident	I	A	C	I	C	R	R	R	R	R	R	R

8.5.3 Problem Management

Activity	CEO	CIO	CISO	CFO	COO	Ops Manager	Service Desk	Sys Admin	Net Admin	DBA	App Manager	Sec Admin
Problem Identification	I	C	I	I	A	R	R	R	R	R	R
Problem Analysis	I	C	I	I	A	C	R	R	R	R	R

Activity	CEO	CIO	CISO	CFO	COO	Ops Manager	Service Desk	Sys Admin	Net Admin	DBA	App Manager	Sec Admin
Root Cause Analysis	I	I	C	I	I	A	C	R	R	R	R	R
Workaround Development	I	C	I	I	A	C	R	R	R	R	R	R
Known Error Documentation	I	I	I	I	I	A	R	C	C	C	C	C
Problem Resolution	In	A	C	I	I	R	C	R	R	R	R	R

8.5.4 Change Management

Activity	CEO	CIO	CISO	CFO	COO	Ops Manager	Service Desk	Sys Admin	Net Admin	DBA	App Manager	Sec Admin
Change Request	I	C	I	I	C	C	R	R	R	R	R	R
Change Assessment	I	C	C	I	C	A	I	R	R	R	R	R
Change Approval (Standard)	I	I	I	I	I	A	I	I	I	I	I	I

Activity	CEO	CIO	CISO	CFO	COO	Ops Manager	Service Desk	Sys Admin	Net Admin	DBA	App Manager	Sec Admin
Change Approval (Normal)	A	C	I	C	R	I	I	I	I	I	I	
Change Approval (Emergency)	A	C	I	C	R	I	I	I	I	I	I	
Change Implementation	I	C	I	I	A	I	R	R	R	R	R	
Change Review	A	C	I	I	R	C	C	C	C	C	C	

8.5.5 Security Management

Activity	CEO	CIO	CISO	CFO	COO	Ops Manager	Service Desk	Sys Admin	Net Admin	DBA	App Manager	Sec Admin
Security Strategy	A	C	R	C	C	C	I	I	I	I	I	I
Security Policies	A	C	R	I	C	C	I	C	C	C	C	C
Security Monitoring	I	I	A	I	I	C	I	C	C	C	C	R
Security Incident	I	A	R	I	C	C	C	C	C	C	C	R

Activity	CEO	CIO	CISO	CFO	COO	Ops Manager	Service Desk	Sys Admin	Net Admin	DBA	App Manager	Sec Admin
Vulnerability Management	I	A	I	I	C	I	C	C	C	C	R
Access Management	I	I	A	I	I	C	C	R	R	R	R	R
Security Audits	I	A	R	C	C	C	I	C	C	C	C	R

8.5.6 Backup and Recovery

Activity	CEO	CIO	CISO	CFO	COO	Ops Manager	Service Desk	Sys Admin	Net Admin	DBA	App Manager	Sec Admin
Backup Strategy	I	A	C	I	C	R	I	C	C	C	C	C
Backup Execution	I	I	I	I	I	A	I	R	C	R	C	I
Backup Monitoring	I	I	I	I	I	A	I	R	C	R	C	I
Backup Testing	I	I	C	I	I	A	I	R	C	R	C	C
Restore Execution	I	I	C	I	I	A	C	R	C	R	C	C
Disaster Recovery	I	A	C	I	C	R	C	R	R	R	R	C

8.5.7 Monitoring and Performance

Activity	CEO	CIO	CISO	CFO	COO	Ops Manager	Service Desk	Sys Admin	Net Admin	DBA	App Manager	Sec Admin
Monitoring Strategy	I	A	C	I	C	R	I	C	C	C	C	C
Monitoring Configuration	I	I	C	I	I	A	I	R	R	R	R	R
24/7 Monitoring	I	I	C	I	I	A	R	R	R	R	R	R
Alert Management	I	I	C	I	I	A	R	R	R	R	R	R
Performance Tuning	I	I	I	I	I	A	I	R	R	R	R	I
Capacity Planning	I	A	I	C	C	R	I	C	C	C	C	I

8.5.8 Compliance and Audits

Activity	CEO	CIO	CISO	CFO	COO	Ops Manager	Service Desk	Sys Admin	Net Admin	DBA	App Manager	Sec Admin
Compliance Strategy	A	R	C	C	C	C	I	I	I	I	I	I
Compliance Controls	I	A	R	C	C	C	I	C	C	C	C	C
Audit Preparation	I	A	R	C	C	R	C	C	C	C	C	C

Activity	CEO	CIO	CISO	CFO	COO	Ops Manager	Service Desk	Sys Admin	Net Admin	DBA	App Manager	Sec Admin
Audit Execution	C	A	R	C	C	R	C	C	C	C	C	C
Audit Follow-up	I	A	R	I	C	R	I	C	C	C	C	C

8.6 Contact Lists and Availability

8.6.1 Executive Level - Contacts

Role	Name	Email	Phone	Mobile	Availability
CEO	Max Mustermann	max.mustermann@adminsend.de	+49 89 12345678-100	[TODO]	Mon-Fri 09:00-17:00
CIO	Anna Schmidt	anna.schmidt@adminsend.de	+49 89 12345678-200	[TODO]	Mon-Fri 08:00-18:00
CISO	Thomas Weber	thomas.weber@adminsend.de	+49 89 12345678-300	[TODO]	Mon-Fri 08:00-18:00
CFO	Maria Müller	maria.mueller@adminsend.de	+49 89 12345678-400	[TODO]	Mon-Fri 09:00-17:00
COO	Peter Fischer	peter.fischer@adminsend.de	+49 89 12345678-500	[TODO]	Mon-Fri 08:00-18:00

8.6.2 IT Operations - Contacts

Role	Name	Email	Phone	Mobile	Availability
IT Ops Manager	Andreas Huemmer	andreas.huemmer@adminsend.de	+49 89 12345678-250	[TODO]	Mon-Fri 07:00-19:00
Service Desk Lead	Julia Becker	julia.becker@adminsend.de	+49 89 12345678-111	[TODO]	Mon-Fri 08:00-17:00
System Admin	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
Network Admin	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
DBA	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
App Manager	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
Security Admin	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

8.6.3 Service Desk - Contacts

Central Service Desk Number: [TODO: Phone number]
Service Desk Email: [TODO: Email address]
Service Portal: [TODO: URL]

Service Hours: - **Regular:** Mon-Fri 08:00-17:00 - **Extended:** [TODO: If applicable] - **24/7:** [TODO: If applicable]

8.7 On-Call and Standby Duty

8.7.1 On-Call Model

Operating Model: [TODO: 24/7, Business Hours, Follow-the-Sun]

On-Call Hours: - **Weekdays:** [TODO: e.g., 17:00-08:00] - **Weekend:** [TODO: e.g., Fri 17:00 - Mon 08:00] - **Holidays:** [TODO: 24 hours]

8.7.2 On-Call Rotation

Week	Primary	Secondary	Escalation
Week [TODO]	[TODO: Name]	[TODO: Name]	Andreas Huemmer
Week [TODO]	[TODO: Name]	[TODO: Name]	Andreas Huemmer
Week [TODO]	[TODO: Name]	[TODO: Name]	Andreas Huemmer
Week [TODO]	[TODO: Name]	[TODO: Name]	Andreas Huemmer

Rotation Schedule: [TODO: Link to current on-call schedule]

8.7.3 On-Call Contacts

Primary On-Call: - **Phone:** [TODO: On-call number] - **Email:** [TODO: On-call email] - **Availability:** [TODO: Response time]

Secondary On-Call: - **Phone:** [TODO: Backup number] - **Email:** [TODO: Backup email] - **Availability:** [TODO: Response time]

Escalation: - **IT Operations Manager:** Andreas Huemmer (+49 89 12345678-250) - **CIO:** Anna Schmidt (+49 89 12345678-200)

8.7.4 On-Call Process

1. Alerting: - Monitoring system sends alert - Automatic notification to on-call person - Channels: SMS, phone, email, push notification

2. Response: - **Response Time:** [TODO: e.g., 15 minutes] - **Acknowledgment:** On-call person confirms receipt - **Initial Analysis:** Within [TODO: e.g., 30 minutes]

3. Escalation: - **Level 1:** Primary on-call (0-15 min) - **Level 2:** Secondary on-call (15-30 min) - **Level 3:** IT Operations Manager (30-60 min) - **Level 4:** CIO ($>$ 60 min or critical incident)

4. Documentation: - Document all activities in ticket system - Timestamps for all actions - Post-incident review for major incidents

8.7.5 On-Call Guidelines

Availability: - On-call person must be reachable - Response time: [TODO: e.g., 15 minutes] - Access to laptop and VPN required - Sobriety during on-call duty

Compensation: - On-call allowance: [TODO: Amount] - Call-out fee: [TODO: Hourly rate] - Time off in lieu: [TODO: Policy]

Handover: - Handover call at end of on-call duty - Documentation of open incidents - Briefing of next on-call person

8.8 Escalation Paths

8.8.1 Standard Escalation

```
Level 1: Service Desk
    ↓ (15 min)
Level 2: Specialist (Sys/Net/DB/App Admin)
    ↓ (30 min)
Level 3: IT Operations Manager
    ↓ (60 min)
Level 4: CIO
    ↓ (critical)
Level 5: CEO
```

8.8.2 Security Incident Escalation

```
Security Alert
    ↓ (immediate)
Security Administrator
    ↓ (15 min)
CISO
    ↓ (30 min for major incident)
CIO + CEO
    ↓ (for data breach)
Data Protection Officer + Authorities
```

8.8.3 Business-Critical Incident Escalation

```
Major Incident
    ↓ (immediate)
IT Operations Manager + On-Call
    ↓ (15 min)
CIO + CISO
    ↓ (30 min)
COO + CEO
    ↓ (if needed)
External Service Providers + Vendors
```

8.8.4 Escalation Criteria

Automatic Escalation When: - No response within defined time - Incident cannot be resolved - Multiple critical systems affected - Data protection or security incident - Business-critical services down

Escalation Times: - **P1 (Critical):** 15 min → 30 min → 60 min - **P2 (High):** 30 min → 60 min → 2 hrs - **P3 (Medium):** 2 hrs → 4 hrs → 8 hrs - **P4 (Low):** 8 hrs → 1 day → 2 days

8.9 Deputy Arrangements

8.9.1 Executive Level - Deputies

Role	Primary	Deputy 1	Deputy 2
CEO	Max Mustermann	[TODO: Name]	[TODO: Name]
CIO	Anna Schmidt	Andreas Huemmer	[TODO: Name]
CISO	Thomas Weber	[TODO: Name]	Anna Schmidt
CFO	Maria Müller	[TODO: Name]	[TODO: Name]
COO	Peter Fischer	[TODO: Name]	[TODO: Name]

8.9.2 IT Operations - Deputies

Role	Primary	Deputy 1	Deputy 2
IT Ops Manager	Andreas Huemmer	[TODO: Name]	Anna Schmidt
Service Desk Lead	Julia Becker	[TODO: Name]	Andreas Huemmer
System Admin	[TODO: Name]	[TODO: Name]	[TODO: Name]
Network Admin	[TODO: Name]	[TODO: Name]	[TODO: Name]
DBA	[TODO: Name]	[TODO: Name]	[TODO: Name]

8.9.3 Deputy Process

For Planned Absence: 1. Inform deputy at least [TODO: e.g., 1 week] in advance 2. Create handover documentation 3. Hand over open issues and incidents 4. Update contact information 5. Set out-of-office message with deputy contact

For Unplanned Absence: 1. Inform supervisor 2. Automatic deputy arrangement takes effect 3. Deputy assumes all ongoing tasks 4. Subsequent handover upon return

8.10 Training and Qualifications

8.10.1 Required Qualifications

Role	Required Certifications	Recommended Training
IT Ops Manager	ITIL Foundation, ITIL Managing Professional	COBIT, ISO 20000

Role	Required Certifications	Recommended Training
Service Desk Lead	ITIL Foundation	ITIL Specialist, HDI Support Center Manager
System Admin	[TODO: e.g., MCSA, RHCSA]	[TODO: Vendor certifications]
Network Admin	[TODO: e.g., CCNA, CCNP]	[TODO: Network security]
DBA	[TODO: e.g., Oracle DBA, MCDBA]	[TODO: Performance tuning]
Security Admin	[TODO: e.g., CISSP, CEH]	[TODO: Security frameworks]

8.10.2 Training Plan

Annual Mandatory Training: - IT security and data protection (all staff) - ITIL refresher (IT operations team) - Incident management processes (service desk) - Change management processes (all IT staff)

Individual Development: - Budget: [TODO: Amount per employee/year] - Approval: IT Operations Manager / CIO - Documentation: Training certificates in personnel file

8.11 Change History

Version	Date	Author	Changes	Approved by
1.0.0	[TODO]	IT Operations Manager	Initial version	CIO

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Classification: internal
Organization: AdminSend GmbH

ewpage

Chapter 9

Operating Concept and Processes

9.1 Overview

This document describes the operating concept and operational processes for the IT service. It defines operating models, process flows according to ITIL standards, interfaces to other processes, and escalation paths.

Service: {{ meta.service_name }}
Responsible: Andreas Huemmer
Version: 1.0.0

9.2 Operating Model

9.2.1 Service Hours

Operating Model	Description	Service Hours
24/7 Operation	Continuous operation without interruption	Mon-Sun, 00:00-24:00
Business Hours	Operation during business hours	Mon-Fri, 08:00-18:00
Extended Hours	Extended business hours	Mon-Fri, 06:00-22:00
Follow-the-Sun	Global operation across time zones	24/7 with regional staffing

Current Operating Model: [TODO: Select operating model]

9.2.2 Maintenance Windows

Type	Time Window	Frequency	Duration
Regular Maintenance	[TODO: e.g., Sunday 02:00-06:00]	[TODO: e.g., Monthly]	[TODO: e.g., 4 hours]

Type	Time Window	Frequency	Duration
Emergency Maintenance	As needed	Ad-hoc	Variable
Patch Window	[TODO: e.g., Tuesday 22:00-24:00]	[TODO: e.g., Weekly]	[TODO: e.g., 2 hours]

9.2.3 Support Model

Support Tiers: - **Level 1 (Service Desk):** Julia Becker - julia.becker@adminsend.de - **Level 2 (IT Operations):** Andreas Huemmer - andreas.huemmer@adminsend.de - **Level 3 (Specialist/Vendor):** [TODO: Specialist contact]

On-Call: - **On-Call Rotation:** [TODO: Describe rotation schedule] - **Availability:** [TODO: Phone/Pager number] - **Response Time:** [TODO: e.g., 15 minutes]

9.3 ITIL Processes

9.3.1 Service Strategy

Objective: Strategic alignment of IT services with business requirements

Activities: - Service Portfolio Management - Financial Management - Demand Management - Business Relationship Management

Responsible: Anna Schmidt

9.3.2 Service Design

Objective: Design of new or changed services for production operation

Activities: - Service Catalogue Management - Service Level Management - Capacity Management - Availability Management - IT Service Continuity Management - Information Security Management - Supplier Management

Responsible: Andreas Huemmer

9.3.3 Service Transition

Objective: Transition of new or changed services into production

Activities: - Change Management (see Chapter 0140) - Release and Deployment Management - Service Validation and Testing - Knowledge Management - Configuration Management (see Chapter 0090)

Responsible: Andreas Huemmer

9.3.4 Service Operation

Objective: Ensure effective and efficient operation

Activities: - Incident Management (see Chapter 0120) - Problem Management (see Chapter 0130) - Event Management - Request Fulfillment - Access Management (see Chapter 0100)

Responsible: Julia Becker (Level 1), Andreas Huemmer (Level 2)

9.3.5 Continual Service Improvement (CSI)

Objective: Continuous improvement of service quality

Activities: - Service Measurement and Reporting - Service Review - Process Improvement - Root Cause Analysis

Responsible: Anna Schmidt

9.4 Process Interfaces

9.4.1 Interfaces to Other IT Processes

Process	Interface	Information Flow	Responsible
Incident Management	Incident reports → Operations	Incidents, Workarounds	Service Desk
Change Management	Change Requests → Operations	Changes, RFCs	CAB
Problem Management	Known Errors → Operations	Problem Records, Solutions	Problem Manager
Configuration Management	CI Updates → CMDB	Configuration Items	CMDB Manager
Capacity Management	Capacity data → Planning	Performance Metrics	Capacity Manager
Availability Management	Availability data → Reporting	Availability Reports	Availability Manager
Security Management	Security Events → Operations	Security Incidents, Patches	Thomas Weber
Backup Management	Backup Status → Operations	Backup Reports, Restore Requests	Backup Administrator

9.4.2 Interfaces to Business Processes

Business Process	Interface	Information Flow	Contact Person
Procurement	Hardware/Software Requirements	Orders, Deliveries	Procurement
Finance	Budget and Costs	Cost Reports, Budget Requests	Maria Müller
Compliance	Audit Requirements	Audit Reports, Evidence	Compliance Officer

Business Process	Interface	Information Flow	Contact Person
HR	Employee Onboarding/Offboarding	Access Management	HR Department

---

9.5 Escalation Paths

9.5.1 Technical Escalation

```
Level 1: Service Desk
Contact: Julia Becker
Email: julia.becker@adminsend.de
Phone: +49 89 12345678-111
Escalate after: 30 minutes (P1), 2 hours (P2)
```

```
Level 2: IT Operations
Contact: Andreas Huemmer
Email: andreas.huemmer@adminsend.de
Phone: +49 89 12345678-250
Escalate after: 1 hour (P1), 4 hours (P2)
```

```
Level 3: Specialist/Vendor
Contact: [TODO: Specialist name]
Email: [TODO: Specialist email]
Phone: [TODO: Specialist phone]
Escalate after: 2 hours (P1), 8 hours (P2)
```

9.5.2 Management Escalation

```
Level 1: IT Operations Manager
Contact: Andreas Huemmer
Email: andreas.huemmer@adminsend.de
Escalate for: Critical Incidents (P1), SLA Violation
```

```
Level 2: Chief Information Officer (CIO)
Contact: Anna Schmidt
Email: anna.schmidt@adminsend.de
Escalate for: Major Incidents, Business Impact
```

```
Level 3: Chief Executive Officer (CEO)
Contact: Max Mustermann
Email: max.mustermann@adminsend.de
Escalate for: Business-critical outages
```

9.5.3 Escalation Criteria

Priority	Technical Escalation	Management Escalation	Timeframe
P1 (Critical)	After 30 min (L1→L2), 1h (L2→L3)	Immediately to IT Ops Manager	Immediate
P2 (High)	After 2h (L1→L2), 4h (L2→L3)	After 4 hours to IT Ops Manager	4 hours
P3 (Medium)	After 8h (L1→L2), 1 day (L2→L3)	After 1 day to IT Ops Manager	1 day
P4 (Low)	After 2 days (L1→L2)	No automatic escalation	2 days

9.6 Operational Process Overview

9.6.1 Daily Operating Routines

Morning Check (08:00): - [ ] Check monitoring dashboards - [ ] Verify backup status - [ ] Review open incidents - [ ] Perform system health check - [ ] Check log files for anomalies

Daily Operations: - [ ] Process incidents by priority - [ ] Implement changes - [ ] Monitor and alerting oversight - [ ] Update documentation - [ ] Communicate with stakeholders

Evening Check (18:00): - [ ] Close or hand over daily incidents - [ ] Initiate backup runs - [ ] Prepare maintenance work - [ ] Handover to night shift (if 24/7) - [ ] Create daily report

9.6.2 Weekly Activities

- ☐ Service review meeting (Monday)
- ☐ Patch management (Tuesday evening)
- ☐ Capacity review (Wednesday)
- ☐ Problem management meeting (Thursday)
- ☐ Week closing and reporting (Friday)

9.6.3 Monthly Activities

- ☐ Service level reporting
- ☐ Capacity planning
- ☐ Security patch review
- ☐ Disaster recovery test
- ☐ Compliance check
- ☐ Vendor review

9.7 Process Metrics and KPIs

9.7.1 Operating Metrics

Metric	Target Value	Measurement Frequency	Responsible
Service Availability	99.5%	Daily	IT Operations
Mean Time To Repair (MTTR)	4 hours	Per Incident	Service Desk
Mean Time Between Failures (MTBF)	720 hours	Monthly	IT Operations
First Call Resolution Rate	70%	Weekly	Service Desk
Change Success Rate	95%	Monthly	Change Manager
Backup Success Rate	100%	Daily	Backup Admin

9.7.2 Process KPIs

KPI	Target Value	Measurement Frequency	Responsible
Incident Resolution Time (P1)	4 hours	Per Incident	Service Desk
Incident Resolution Time (P2)	8 hours	Per Incident	Service Desk
Change Lead Time	5 days	Per Change	Change Manager
Problem Resolution Time	30 days	Per Problem	Problem Manager
SLA Compliance	98%	Monthly	Service Manager

9.8 Continuous Improvement

9.8.1 CSI Process

1. **Identification:** Identify improvement opportunities
2. **Analysis:** Conduct root cause analysis
3. **Planning:** Plan improvement measures
4. **Implementation:** Implement measures
5. **Measurement:** Measure and validate success
6. **Review:** Review and document results

9.8.2 Improvement Sources

- Incident analyses and trends
- Problem management insights
- Service review meetings
- Customer feedback
- Audit results
- Benchmark comparisons

9.8.3 Improvement Register

ID	Improvement	Priority	Status	Responsible	Target Date
CSI-001	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
CSI-002	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

9.9 Documentation and Knowledge Management

9.9.1 Documentation Repository

- **Operations Manuals:** Central repository for all operational documents
- **Runbooks:** Standardized procedure descriptions
- **Known Error Database:** Known errors and solutions
- **Configuration Management Database (CMDB):** CI documentation
- **Change History:** Documentation of all changes

9.9.2 Knowledge Transfer

- **Onboarding:** Training of new employees
- **Training:** Regular training sessions
- **Documentation:** Continuous documentation
- **Knowledge Sharing:** Team meetings and workshops
- **Lessons Learned:** Post-incident reviews

9.10 Compliance and Governance

9.10.1 Relevant Standards

- **ITIL v4:** IT Service Management Framework
- **ISO 20000:** IT Service Management Standard
- **ISO 27001:** Information Security Management
- **COBIT 2019:** IT Governance Framework

9.10.2 Audit Requirements

- Documentation of all operational processes
- Demonstrable compliance with SLAs
- Change management protocols
- Incident management reports
- Compliance evidence

9.11 Contacts

Operations Responsible: - **IT Operations Manager:** Andreas Huemmer - andreas.huemmer@adminsend.de - **Service Desk Lead:** Julia Becker - julia.becker@adminsend.de - **CIO:** Anna Schmidt - anna.schmidt@adminsend.de

Additional Contacts: See Chapter 0270 (Contacts, Escalation and Vendors)

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

ewpage

Chapter 10

Operations Handover and Go-Live Checklist

10.1 Overview

This document describes the operations handover process and contains a comprehensive go-live checklist for transitioning new or changed IT services into production.

Service: {{ meta.service_name }}
Responsible: Andreas Huemmer
Version: 1.0.0

10.2 Operations Handover Process

10.2.1 Phases of Operations Handover

1. Preparation

2. Documentation

3. Training

4. Testing

```
5. Go-Live



6. Hypercare
```

10.2.2 Roles and Responsibilities

Role	Responsibility	Contact Person
Service Owner	Overall service responsibility	[TODO: Name]
IT Operations Manager	Coordinate operations takeover	Andreas Huemmer
Technical Lead	Technical implementation	[TODO: Name]
Service Desk Lead	Support readiness	Julia Becker
Change Manager	Change approval	[TODO: Name]
CIO	Final approval	Anna Schmidt

10.3 Go-Live Checklist

10.3.1 Phase 1: Preparation (4-6 Weeks Before Go-Live)

10.3.1.1 Project Planning

- ☐ Go-live date set and communicated
- ☐ Project team assembled
- ☐ Roles and responsibilities defined
- ☐ Communication plan created
- ☐ Risk assessment conducted
- ☐ Rollback plan created

10.3.1.2 Infrastructure

- ☐ Hardware procured and installed
- ☐ Network connectivity configured
- ☐ Virtualization/cloud resources provisioned
- ☐ Storage capacity allocated
- ☐ Backup infrastructure set up
- ☐ Monitoring infrastructure prepared

10.3.1.3 Software and Licenses

- ☐ Software licenses procured

- ☐ Software installed and configured
- ☐ Patches and updates applied
- ☐ License compliance verified
- ☐ Third-party software integrated

10.3.2 Phase 2: Documentation (3-4 Weeks Before Go-Live)

10.3.2.1 Operations Documentation

- ☐ Operations manual created (this document)
- ☐ System architecture documented (Chapter 0040)
- ☐ Infrastructure documented (Chapter 0050)
- ☐ Network diagrams created
- ☐ Configuration documentation complete
- ☐ CMDB entries created (Chapter 0090)

10.3.2.2 Process Documentation

- ☐ Incident management process defined (Chapter 0120)
- ☐ Change management process defined (Chapter 0140)
- ☐ Backup process documented (Chapter 0150)
- ☐ Monitoring process documented (Chapter 0110)
- ☐ Escalation paths defined (Chapter 0070)

10.3.2.3 Runbooks and Guides

- ☐ Standard runbooks created (Chapter 0240)
- ☐ Troubleshooting guides created
- ☐ Emergency runbooks created
- ☐ Maintenance checklists created
- ☐ FAQ document created (Chapter 0260)

10.3.3 Phase 3: Training (2-3 Weeks Before Go-Live)

10.3.3.1 Service Desk Training

- ☐ Service overview presented
- ☐ Incident handling trained
- ☐ Ticketing system trained
- ☐ Escalation processes explained
- ☐ FAQ and known issues reviewed
- ☐ Hands-on training conducted

10.3.3.2 Operations Team Training

- ☐ Technical architecture explained
- ☐ Monitoring tools trained
- ☐ Backup/restore procedures trained
- ☐ Change process reviewed
- ☐ Emergency procedures practiced
- ☐ Runbooks worked through

10.3.3.3 Management Briefing

- ☐ Service overview presented
- ☐ SLAs and KPIs explained
- ☐ Risks and mitigations discussed
- ☐ Escalation processes communicated
- ☐ Reporting mechanisms explained

10.3.4 Phase 4: Testing (1-2 Weeks Before Go-Live)

10.3.4.1 Functional Tests

- ☐ Unit tests conducted
- ☐ Integration tests conducted
- ☐ End-to-end tests conducted
- ☐ User acceptance tests (UAT) conducted
- ☐ Performance tests conducted
- ☐ Security tests conducted

10.3.4.2 Operational Tests

- ☐ Backup test conducted
- ☐ Restore test conducted
- ☐ Failover test conducted
- ☐ Monitoring alerts tested
- ☐ Incident process tested
- ☐ Escalation process tested

10.3.4.3 Disaster Recovery Test

- ☐ DR plan tested
- ☐ Failover to DR site tested
- ☐ Failback to primary site tested
- ☐ RTO/RPO validated
- ☐ DR documentation updated

10.3.5 Phase 5: Go-Live (Go-Live Day)

10.3.5.1 Pre-Go-Live (24 Hours Before)

- ☐ Go/No-Go meeting conducted
- ☐ All stakeholders informed
- ☐ Maintenance window communicated
- ☐ Rollback plan final review
- ☐ Backup before go-live created
- ☐ Change ticket approved

10.3.5.2 Go-Live Activities

- ☐ Maintenance window started
- ☐ Service migration performed

- ☐ Configuration changes applied
- ☐ Smoke tests conducted
- ☐ Monitoring activated
- ☐ Service status communicated

10.3.5.3 Post-Go-Live (Immediately After Go-Live)

- ☐ Service availability confirmed
- ☐ Monitoring dashboards checked
- ☐ First transactions validated
- ☐ Performance metrics checked
- ☐ Stakeholders informed
- ☐ Go-live protocol created

10.3.6 Phase 6: Hypercare (1-4 Weeks After Go-Live)

10.3.6.1 Hypercare Support

- ☐ Extended support hours activated
- ☐ Additional resources provided
- ☐ Daily status meetings conducted
- ☐ Incident tracking intensified
- ☐ Performance monitoring enhanced
- ☐ User feedback collected

10.3.6.2 Stabilization

- ☐ Critical issues resolved
- ☐ Performance optimized
- ☐ Documentation updated
- ☐ Known issues documented
- ☐ Lessons learned documented
- ☐ Post-implementation review conducted

10.4 Handover Documentation

10.4.1 Handover Package

The handover package must contain the following documents:

10.4.1.1 Technical Documentation

1. **System Architecture** (Chapter 0040)
   - Architecture diagrams
   - Component descriptions
   - Data flows
   - Dependencies
2. **Infrastructure** (Chapter 0050)

- Hardware inventory
- Network configuration
- IP addressing
- Virtualization/cloud resources

3. **Configuration** (Chapter 0090)
   - Configuration files
   - CMDB entries
   - Network configuration
   - Security configuration

10.4.1.2 Operations Documentation

4. **Operating Processes** (Chapter 0070)
   - Operating model
   - ITIL processes
   - Escalation paths
   - KPIs and metrics
5. **Monitoring** (Chapter 0110)
   - Monitoring strategy
   - Alert configuration
   - Dashboard overviews
   - Thresholds
6. **Backup and Recovery** (Chapter 0150)
   - Backup strategy
   - Backup schedules
   - Restore procedures
   - RTO/RPO values

10.4.1.3 Support Documentation

7. **Runbooks** (Chapter 0240)
   - Standard operations
   - Troubleshooting guides
   - Emergency procedures
   - Maintenance checklists
8. **Known Issues and FAQ** (Chapter 0260)
   - Known problems
   - Workarounds
   - Frequently asked questions
   - Solutions
9. **Contacts** (Chapter 0270)
   - Contact persons
   - Escalation contacts
   - Vendor contacts
   - On-call information

10.4.2 Handover Meeting

Agenda: 1. Service overview and business purpose 2. Technical architecture and infrastructure 3. Operating processes and responsibilities 4. Monitoring and alerting 5. Incident and problem management 6. Backup and disaster recovery 7. Known issues and risks 8. Questions and answers

Participants: - Service Owner - IT Operations Manager: Andreas Huemmer - Technical Lead - Service Desk Lead: Julia Becker - CIO: Anna Schmidt

---

10.5 Acceptance Criteria

10.5.1 Technical Acceptance Criteria

Criterion	Requirement	Status	Verified By
Functionality	All features work according to specification		[TODO]
Performance	Response times < [TODO] ms		[TODO]
Availability	Service accessible 24/7		[TODO]
Scalability	Supports [TODO] concurrent users		[TODO]
Security	Security tests passed		[TODO]
Backup	Backup tests successful		[TODO]
Monitoring	All metrics captured		[TODO]
Integration	All interfaces functional		[TODO]

10.5.2 Operational Acceptance Criteria

Criterion	Requirement	Status	Verified By
Documentation	Complete operations documentation		IT Ops Manager
Training	Team trained and ready		Service Desk Lead
Runbooks	All runbooks created and tested		IT Ops Manager
CMDB	All CIs documented		CMDB Manager
SLA	SLAs defined and agreed		Service Manager
Support	Support processes established		Service Desk Lead
Monitoring	Monitoring active and functional		Monitoring Team

Criterion	Requirement	Status	Verified By
Backup	Backup process established		Backup Admin

10.5.3 Business Acceptance Criteria

Criterion	Requirement	Status	Verified By
Business Requirements	All business requirements met		Service Owner
User Acceptance	UAT successfully completed		Business Users
Compliance	Compliance requirements met		Compliance Officer
Budget	Within budget		Maria Müller
Timeline	Schedule maintained		Project Manager

10.6 Go/No-Go Decision

10.6.1 Go/No-Go Meeting

Timing: 24 hours before planned go-live
Participants: - Service Owner - IT Operations Manager: Andreas Huemmer - Technical Lead - Change Manager - CIO: Anna Schmidt

10.6.2 Decision Criteria

Criterion	Go	No-Go	Status
All tests passed			
Documentation complete			
Team trained			
No critical issues			
Rollback plan available			
Stakeholders informed			
Change approved			
Backup created			

Decision: GO NO-GO

Justification: [TODO]

Signatures: - Service Owner: _____ Date: _____ - IT Operations Manager: _____ Date: _____ - CIO: _____ Date: _____

10.7 Rollback Plan

10.7.1 Rollback Triggers

Rollback is triggered by: - Critical functional failures - Severe performance problems - Data loss or data corruption - Security incidents - Unmet acceptance criteria

10.7.2 Rollback Procedure

1. **Decision:** IT Operations Manager decides on rollback
2. **Communication:** Inform stakeholders
3. **Maintenance Window:** If required, activate maintenance window
4. **Backup Restore:** Restore last working backup
5. **Configuration:** Restore old configuration
6. **Validation:** Check functionality
7. **Communication:** Communicate rollback completion
8. **Post-Mortem:** Conduct root cause analysis

10.7.3 Rollback Time Window

- **Within 4 hours after go-live:** Quick rollback possible
- **4-24 hours after go-live:** Rollback with increased effort
- **After 24 hours:** Rollback only after careful analysis

10.8 Post-Implementation Review

10.8.1 Review Meeting

Timing: 2-4 weeks after go-live
Participants: All project stakeholders

Agenda: 1. Go-live process review 2. Lessons learned 3. Issues and resolutions 4. Performance analysis 5. User feedback 6. Improvement suggestions 7. Next steps

10.8.2 Lessons Learned

Category	What went well?	What went poorly?	Improvements
Planning	[TODO]	[TODO]	[TODO]
Communication	[TODO]	[TODO]	[TODO]
Testing	[TODO]	[TODO]	[TODO]
Training	[TODO]	[TODO]	[TODO]
Go-Live	[TODO]	[TODO]	[TODO]
Support	[TODO]	[TODO]	[TODO]

10.8.3 Metrics After Go-Live

Metric	Target Value	Actual Value	Status
Availability (first week)	99%	[TODO]%	
Incidents (first week)	10	[TODO]	
MTTR (first week)	4h	[TODO]h	
User Satisfaction	80%	[TODO]%	
Performance	< [TODO] ms	[TODO] ms	

10.9 Contacts

Go-Live Team: - **Service Owner:** [TODO: Name] - [TODO: Email] - **IT Operations Manager:** Andreas Huemmer - andreas.huemmer@adminsend.de - **Technical Lead:** [TODO: Name] - [TODO: Email] - **Service Desk Lead:** Julia Becker - julia.becker@adminsend.de - **Change Manager:** [TODO: Name] - [TODO: Email] - **CIO:** Anna Schmidt - anna.schmidt@adminsend.de

---

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

ewpage

Chapter 11

Configuration Management and CMDB

11.1 Overview

This document describes configuration management and the Configuration Management Database (CMDB) for the IT service. It defines CI categories, attributes, relationships, and change processes for Configuration Items.

Service: {{ meta.service_name }}
Responsible: Andreas Huemmer
CMDB System: NetBox
Version: 1.0.0

11.2 Configuration Management Process

11.2.1 Configuration Management Objectives

- **Transparency:** Complete overview of all IT assets and their relationships
- **Control:** Controlled changes to Configuration Items
- **Compliance:** Adherence to license and compliance requirements
- **Planning:** Solid foundation for capacity and change planning
- **Incident Support:** Faster incident resolution through CI information

11.2.2 ITIL Configuration Management Activities

1. **Management and Planning:** Planning and control of configuration management
2. **Configuration Identification:** Identification and categorization of CIs
3. **Configuration Control:** Control of changes to CIs
4. **Status Accounting:** Recording and reporting of CI status
5. **Verification and Audit:** Verification of CMDB data quality

---

11.3 Configuration Management Database (CMDB)

11.3.1 CMDB System: NetBox

NetBox Instance: - **URL:** {{ netbox.url }} - **Version:** {{ netbox.version }} - **Responsible:** Andreas Huemmer

NetBox Functions: - IP Address Management (IPAM) - Data Center Infrastructure Management (DCIM) - Device Management - Circuit Management - Virtualization Management - Configuration Context

11.3.2 CMDB Structure

```
                    CMDB (NetBox)


     Sites             Racks             Devices


  IP Addresses        VLANs             Circuits


     Clusters      Virtual Machines     Interfaces
```

11.4 CI Categories and Attributes

11.4.1 Hardware CIs

11.4.1.1 Servers

Category: Hardware > Server
Attributes: - **Name:** {{ netbox.device.name }} - **Manufacturer:** {{ netbox.device.manufacturer }} - **Model:** {{ netbox.device.model }} - **Serial Number:** {{ netbox.device.serial }} - **Asset Tag:** {{ netbox.device.asset_tag }} - **Site:** {{ netbox.device.site }} - **Rack:** {{ netbox.device.rack }} - **Rack Position:** {{ netbox.device.position }} - **Status:** Active, Planned, Staged, Failed, Decommissioned - **Role:** {{ netbox.device.role }} - **Primary IP:** {{ netbox.device.primary_ip }}

11.4.1.2 Network Devices

Category: Hardware > Network
Attributes: - **Name:** {{ netbox.device.name }} - **Type:** Switch, Router, Firewall, Load Balancer

- **Manufacturer:** {{ netbox.device.manufacturer }} - **Model:** {{ netbox.device.model }} - **Management IP:** {{ netbox.device.primary_ip }} - **Site:** {{ netbox.device.site }} - **Interfaces:** {{ netbox.device.interfaces }} - **VLANs:** {{ netbox.device.vlans }}

11.4.1.3 Storage

Category: Hardware > Storage
Attributes: - **Name:** {{ netbox.device.name }} - **Type:** SAN, NAS, DAS - **Capacity:** [TODO] TB - **Manufacturer:** {{ netbox.device.manufacturer }} - **Site:** {{ netbox.device.site }}

11.4.2 Software CIs

11.4.2.1 Operating Systems

Category: Software > Operating System
Attributes: - **Name:** [TODO: e.g., Ubuntu Server 22.04] - **Version:** [TODO] - **License:** [TODO] - **Installed on:** {{ netbox.device.name }} - **Patch Level:** [TODO]

11.4.2.2 Applications

Category: Software > Application
Attributes: - **Name:** [TODO: Application name] - **Version:** [TODO] - **Vendor:** [TODO] - **License:** [TODO] - **License Count:** [TODO] - **Installed on:** {{ netbox.device.name }} - **Responsible:** [TODO]

11.4.3 Virtualization CIs

11.4.3.1 Hypervisor Clusters

Category: Virtualization > Cluster
Attributes: - **Name:** {{ netbox.cluster.name }} - **Type:** {{ netbox.cluster.type }} - **Site:** {{ netbox.cluster.site }} - **Host Count:** {{ netbox.cluster.device_count }}

11.4.3.2 Virtual Machines

Category: Virtualization > Virtual Machine
Attributes: - **Name:** {{ netbox.vm.name }} - **Cluster:** {{ netbox.vm.cluster }} - **vCPUs:** {{ netbox.vm.vcpus }} - **Memory:** {{ netbox.vm.memory }} GB - **Disk:** {{ netbox.vm.disk }} GB - **Status:** Active, Offline, Staged - **Primary IP:** {{ netbox.vm.primary_ip }} - **Operating System:** [TODO]

11.4.4 Network CIs

11.4.4.1 IP Addresses

Category: Network > IP Address
Attributes: - **IP Address:** {{ netbox.ip.address }} - **VLAN:** {{ netbox.ip.vlan }} - **Status:** Active, Reserved, Deprecated - **DNS Name:** {{ netbox.ip.dns_name }} - **Assigned to:** {{ netbox.ip.assigned_to }}

11.4.4.2 VLANs

Category: Network > VLAN
Attributes: - **VLAN ID:** {{ netbox.vlan.vid }} - **Name:** {{ netbox.vlan.name }} - **Site:** {{ netbox.vlan.site }} - **Description:** {{ netbox.vlan.description }}

11.4.4.3 Circuits

Category: Network > Circuit
Attributes: - **Circuit ID:** {{ netbox.circuit.cid }} - **Provider:** {{ netbox.circuit.provider }} - **Type:** {{ netbox.circuit.type }} - **Bandwidth:** {{ netbox.circuit.commit_rate }} Mbps - **Status:** Active, Planned, Decommissioned

11.4.5 Location CIs

11.4.5.1 Sites

Category: Location > Site
Attributes: - **Name:** {{ netbox.site.name }} - **Address:** {{ netbox.site.physical_address }} - **Facility:** {{ netbox.site.facility }} - **Status:** Active, Planned, Retired - **Contact:** {{ netbox.site.contact_name }}

11.5 CI Relationships

11.5.1 Relationship Types

Relationship	Description	Example
Hosted on	CI runs on another CI	VM hosted on Hypervisor
Connected to	Physical/logical connection	Server connected to Switch
Depends on	Functional dependency	Application depends on Database
Part of	Component of larger CI	Disk part of Server
Uses	CI uses another CI	Application uses IP Address
Managed by	Management relationship	Device managed by Management System

11.5.2 Relationship Diagram

```
Application

       depends on


Database

       hosted on
```

```
Virtual Machine

        hosted on


 Hypervisor

        installed on


Physical Server

        connected to


   Switch
```

11.5.3 CI Dependencies

Example: Web Application Stack

CI	Depends on	Relationship Type
Web Application	Application Server	depends on
Application Server	Database Server	depends on
Application Server	Load Balancer	connected to
Database Server	Storage Array	uses
Application Server	Virtual Machine	hosted on
Virtual Machine	Hypervisor Cluster	hosted on
Hypervisor Cluster	Physical Servers	consists of
Physical Servers	Network Switch	connected to

11.6 Change Processes for CIs

11.6.1 CI Lifecycle

```
Planned



Staged
```

```
Active
```

```
Deprecated
```

```
Decommissioned
```

11.6.2 CI Change Process

11.6.2.1 1. CI Creation

Trigger: New hardware/software procured
Process: 1. Create CI in CMDB (Status: Planned) 2. Capture attributes 3. Define relationships 4. Approval by IT Operations Manager 5. Set status to “Staged”

11.6.2.2 2. CI Activation

Trigger: CI put into operation
Process: 1. Create change request (see Chapter 0140) 2. Perform CI configuration 3. Conduct tests 4. Set status to “Active” 5. Activate monitoring

11.6.2.3 3. CI Modification

Trigger: Change to existing CI
Process: 1. Create change request 2. Conduct impact analysis 3. Identify dependent CIs 4. Perform change 5. Update CMDB 6. Conduct validation

11.6.2.4 4. CI Deactivation

Trigger: Take CI out of operation
Process: 1. Create change request 2. Check dependencies 3. Create backup 4. Deactivate CI 5. Set status to “Deprecated” 6. Deactivate monitoring

11.6.2.5 5. CI Deletion

Trigger: Permanently remove CI
Process: 1. Ensure no dependencies exist 2. Archive data 3. Return licenses 4. Set status to “Decommissioned” 5. Delete from CMDB after retention period

11.6.3 Change Approval for CIs

CI Category	Approval Required By	Change Type
Critical Servers	IT Operations Manager + CIO	Normal Change
Network Core	IT Operations Manager + CIO	Normal Change
Standard Servers	IT Operations Manager	Standard Change
Workstations	Service Desk Lead	Standard Change
IP Addresses	Network Administrator	Standard Change
Virtual Machines	Virtualization Admin	Standard Change

11.7 CMDB Data Quality

11.7.1 Data Quality Metrics

Metric	Target Value	Measurement Frequency	Responsible
Completeness	95%	Monthly	CMDB Manager
Accuracy	98%	Monthly	CMDB Manager
Timeliness	7 days	Weekly	CMDB Manager
Consistency	95%	Monthly	CMDB Manager
Uniqueness	100%	Continuous	CMDB Manager

11.7.2 Data Quality Process

11.7.2.1 Regular Audits

- **Frequency:** Quarterly
- **Scope:** Sample of 10% of all CIs
- **Method:** Compare CMDB data with actual state
- **Responsible:** Andreas Huemmer

11.7.2.2 Automatic Validation

- **Discovery Tools:** Automatic detection of devices and software
- **Reconciliation:** Comparison between discovery and CMDB
- **Alerts:** Notification of discrepancies
- **Correction:** Automatic or manual correction

11.7.2.3 Manual Verification

- **Trigger:** Before each major change
- **Process:** Manual verification of affected CIs
- **Documentation:** Document changes
- **Approval:** By IT Operations Manager

11.8 CMDB Access and Permissions

11.8.1 Access Roles

Role	Permission	Access to
CMDB Administrator	Full access	All CIs
IT Operations Manager	Read, Write, Delete	All CIs
Network Administrator	Read, Write	Network CIs
Server Administrator	Read, Write	Server CIs
Service Desk	Read	All CIs
Auditor	Read	All CIs (Read-only)

11.8.2 Access Control

CMDB Administrator: Andreas Huemmer
Access via: {{ netbox.url }}
Authentication: SSO/LDAP
Audit Logging: All changes are logged

11.9 CMDB Integration

11.9.1 Integrated Systems

System	Integration	Data Flow	Frequency
Monitoring	API	CMDB → Monitoring	Real-time
Ticketing	API	CMDB Ticketing	Real-time
Asset Management	API	Asset Mgmt → CMDB	Daily
Discovery Tools	API	Discovery → CMDB	Hourly
Backup System	API	CMDB → Backup	Daily
Change Management	API	CMDB Change Mgmt	Real-time

11.9.2 API Access

NetBox API: - **Endpoint:** {{ netbox.url }}/api/ - **Authentication:** API Token - **Documentation:** {{ netbox.url }}/api/docs/ - **Rate Limiting:** [TODO: e.g., 1000 requests/hour]

11.10 CMDB Reporting

11.10.1 Standard Reports

11.10.1.1 CI Inventory Report

Frequency: Monthly
Content: - Number of CIs per category - CI status distribution - New CIs in last month - Deactivated CIs in last month

11.10.1.2 License Compliance Report

Frequency: Quarterly
Content: - Licensed software - Installed instances - License compliance status - Expiring licenses

11.10.1.3 Network Inventory Report

Frequency: Monthly
Content: - IP address usage - VLAN overview - Network device status - Circuit overview

11.10.1.4 Change Impact Report

Frequency: Per change
Content: - Affected CIs - Dependent CIs - Risk assessment - Rollback plan

---

11.11 CMDB Maintenance

11.11.1 Maintenance Activities

11.11.1.1 Daily Activities

- ☐ Review discovery results
- ☐ Validate new CIs
- ☐ Adopt changes from change tickets
- ☐ Check alerts for discrepancies

11.11.1.2 Weekly Activities

- ☐ Check data quality metrics
- ☐ Identify orphaned CIs
- ☐ Validate relationships
- ☐ Perform CMDB backup

11.11.1.3 Monthly Activities

- ☐ Conduct CMDB audit
- ☐ Generate and distribute reports
- ☐ Check license compliance
- ☐ Archive obsolete CIs

11.11.1.4 Quarterly Activities

- ☐ Comprehensive CMDB audit
- ☐ Data quality review
- ☐ Process review
- ☐ Training for CMDB users

11.12 Best Practices

11.12.1 CMDB Best Practices

1. **Unique Identification:** Each CI must be uniquely identifiable
2. **Consistent Naming Convention:** Uniform naming of all CIs
3. **Complete Attributes:** Capture all relevant attributes
4. **Current Relationships:** Maintain relationships between CIs
5. **Regular Audits:** Continuously check data quality
6. **Automation:** Automate discovery and reconciliation
7. **Integration:** Integrate CMDB with other tools
8. **Documentation:** Document changes
9. **Training:** Train users regularly
10. **Governance:** Define clear responsibilities

11.12.2 Naming Conventions

Servers: - Format: `[Site]-[Type]-[Environment]-[Number]` - Example: `MUC-SRV-PROD-001`

Virtual Machines: - Format: `[Site]-[Type]-[Environment]-[Application]-[Number]` - Example: `MUC-VM-PROD-WEB-001`

Network Devices: - Format: `[Site]-[Type]-[Function]-[Number]` - Example: `MUC-SW-CORE-001`

11.13 Contacts

CMDB Responsible: - **CMDB Administrator:** Andreas Huemmer - andreas.huemmer@adminsend.de - **Network Administrator:** [TODO: Name] - [TODO: Email] - **Server Administrator:** [TODO: Name] - [TODO: Email] - **CIO:** Anna Schmidt - anna.schmidt@adminsend.de

NetBox Support: - **URL:** {{ netbox.url }} - **Documentation:** {{ netbox.url }}/docs/ - **Support:** [TODO: Support contact]

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

ewpage

Chapter 12

Access and Permission Management

12.1 Overview

This document describes access and permission management for the IT service. It defines access control models, permission concepts, and role-based access control (RBAC).

Service: {{ meta.service_name }}
Responsible: Andreas Huemmer
Security Officer: Thomas Weber
Version: 1.0.0

12.2 Access Management Strategy

12.2.1 Objectives

- **Least Privilege:** Minimum necessary permissions
- **Separation of Duties:** Task separation for risk minimization
- **Need-to-Know:** Access only to required information
- **Accountability:** Traceability of all access
- **Compliance:** Adherence to regulatory requirements

12.2.2 Core Principles

1. **Default Deny:** No access by default, explicit approval required
2. **Time-Limited Access:** Time-limited permissions where possible
3. **Regular Review:** Regular review of permissions
4. **Audit Trail:** Complete logging of all access
5. **Multi-Factor Authentication:** MFA for privileged access

---

12.3 Access Control Model

12.3.1 Authentication

12.3.1.1 Authentication Methods

Method	Usage	Security Level
Username/Password	Standard access	Basic
Multi-Factor Authentication (MFA)	Privileged access	High
Certificate-Based	System-to-system	Very High
SSO (Single Sign-On)	Enterprise applications	Medium-High
API Keys	Programmatic access	Medium
Biometric	High-security areas	Very High

12.3.1.2 Authentication Infrastructure

Identity Provider: - **System:** [TODO: e.g., Active Directory, Azure AD, Okta] - **URL:** [TODO: SSO URL] - **Responsible:** Andreas Huemmer

MFA System: - **System:** [TODO: e.g., Duo, Microsoft Authenticator] - **Required for:** Administrators, privileged accounts - **Responsible:** Thomas Weber

12.3.2 Authorization

12.3.2.1 Authorization Models

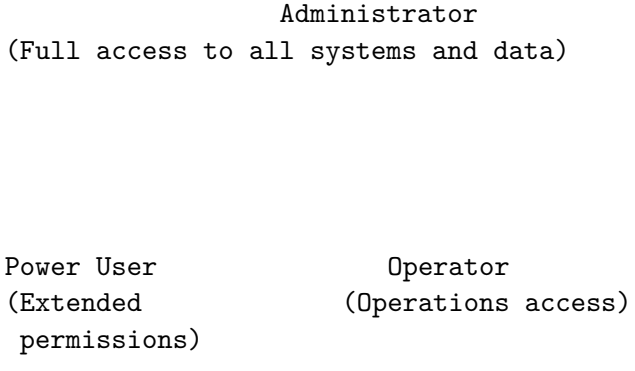
Role-Based Access Control (RBAC): - Permissions assigned to roles - Users receive roles - Simplifies permission management

Attribute-Based Access Control (ABAC): - Permissions based on attributes - More flexible than RBAC - More complex implementation

Current Model: [TODO: Select RBAC/ABAC/Hybrid]

12.4 Role-Based Access Control (RBAC)

12.4.1 Role Hierarchy



```
 Standard User          Read-Only
(Basic access)         (Read only)
```

12.4.2 Role Definitions

12.4.2.1 Administrator

Description: Full access to all systems and functions
Permissions: - Full access to all systems - User management - Configuration changes - System administration - Backup/restore

Assigned to: - Andreas Huemmer - [TODO: Additional administrators]

MFA: Required

12.4.2.2 Power User

Description: Extended permissions for special tasks
Permissions: - Read and write in assigned areas - Use advanced functions - Create reports - Configuration in own area

Assigned to: - [TODO: List power users]

MFA: Recommended

12.4.2.3 Operator

Description: Operations access for daily tasks
Permissions: - Monitoring access - Incident processing - Standard operations - Log access (read-only)

Assigned to: - Julia Becker - [TODO: Additional operators]

MFA: Optional

12.4.2.4 Standard User

Description: Basic access for normal users
Permissions: - Access to own data - Use standard functions - Create tickets - Manage own profile

Assigned to: - All employees

MFA: Optional

12.4.2.5 Read-Only

Description: Read-only access for reporting and auditing
Permissions: - Read access to data - View reports - View dashboards - No changes possible

Assigned to: - Auditors - Management - [TODO: Additional read-only users]

MFA: Optional

12.5 Permission Matrix

12.5.1 System Permissions

System/Resource	Administrator	Power User	Operator	Standard User	Read-Only
Server Administration	Full access	-	-	-	Read
Network Configuration	Full access	-	-	-	Read
Monitoring System	Full access	Read/Write	Read	-	Read
Ticketing System	Full access	Read/Write	Read/Write	Create tickets	Read
CMDB	Full access	Read/Write	Read	-	Read
Backup System	Full access	-	Read	-	Read
Log Management	Full access	Read	Read	-	Read
Documentation	Full access	Read/Write	Read	Read	Read

12.5.2 Data Permissions

Data Classification	Administrator	Power User	Operator	Standard User	Read-Only
Public	Full access	Read/Write	Read	Read	Read
Internal	Full access	Read/Write	Read	Read	Read
Confidential	Full access	As needed	-	-	As needed
Restricted	As needed	-	-	-	-

12.6 Access Request Process

12.6.1 Access Request

```
1. Submit
   Request
```

2. Manager
   Approval

3. Security
   Review

4. Provisioning

5. Confirmation

12.6.2 Request Process

12.6.2.1 1. Submit Request

Who: User or manager
How: Ticket in service desk system
Information: - Username - Requested role/permission - Business justification - Time period (if temporary) - Manager approval

12.6.2.2 2. Manager Approval

Who: Direct supervisor
Review: - Business necessity - Least privilege principle - Separation of duties

Decision: Approve / Reject / Request clarification

12.6.2.3 3. Security Review

Who: Thomas Weber or security team
Review: - Compliance requirements - Risk assessment - Conflict check (separation of duties)

Decision: Approve / Reject / Modify

12.6.2.4 4. Provisioning

Who: Andreas Huemmer or IT operations
Activities: - Create/modify account - Assign permissions - Set up MFA (if required) - Documentation in CMDB

SLA: Within 1 business day

12.6.2.5 5. Confirmation

Who: IT operations
Activities: - Inform user - Provide access credentials - Complete documentation - Close ticket

---

12.7 Privileged Access Management (PAM)

12.7.1 Privileged Accounts

12.7.1.1 Definition

Privileged accounts have extended permissions and access to critical systems.

Examples: - Root/administrator accounts - Service accounts - Database admin accounts - Network admin accounts - Backup admin accounts

12.7.2 PAM Requirements

Requirement	Description	Implementation
Separate Accounts	Privileged accounts separate from standard accounts	[TODO]
MFA	Multi-factor authentication required	[TODO]
Session Recording	Recording of privileged sessions	[TODO]
Just-in-Time Access	Temporary privilege assignment	[TODO]
Password Vault	Centralized password management	[TODO]
Regular Rotation	Regular password rotation	[TODO]
Audit Logging	Complete logging	[TODO]

12.7.3 PAM System

System: [TODO: e.g., CyberArk, BeyondTrust, Thycotic]
Responsible: Thomas Weber
Access: [TODO: PAM system URL]

12.8 Service Accounts

12.8.1 Service Account Management

Definition: Accounts for automated processes and system integrations

Requirements: - Unique naming (e.g., `svc_backup`, `svc_monitoring`) - Documentation in CMDB - Minimal permissions - No interactive logins - Regular password rotation - Usage monitoring

12.8.2 Service Account Inventory

Service Account	Usage	System	Permissions	Owner
`svc_backup`	Backup processes	Backup system	Read, backup	Backup admin
`svc_monitoring`	Monitoring	Monitoring system	Read	Monitoring team
`svc_integration`	System integration	Integration platform	API access	Integration team
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

12.9 Access Review Process

12.9.1 Regular Reviews

12.9.1.1 Quarterly Reviews

Frequency: Every 3 months
Scope: All user permissions
Responsible: Manager + IT operations
Process: 1. Generate review report 2. Managers review their employees' permissions 3. Remove no longer needed permissions 4. Document changes

12.9.1.2 Annual Reviews

Frequency: Annually
Scope: Complete access review
Responsible: Thomas Weber
Process: 1. Comprehensive audit of all accounts 2. Review privileged accounts 3. Validate service accounts 4. Compliance check 5. Create audit report

12.9.2 Automatic Reviews

Triggers: - Employee change (department/role) - Project end - Inactive accounts (> 90 days) - Expiration of temporary permissions

Action: - Automatic notification to manager - Deactivation after deadline - Documentation

---

12.10 Onboarding and Offboarding

12.10.1 Onboarding Process

12.10.1.1 New Employee

Trigger: HR notification
Timeframe: Before first day of work

Activities: 1. [ ] Create account 2. [ ] Assign basic permissions 3. [ ] Set up email account 4. [ ] Provide VPN access 5. [ ] Set up MFA 6. [ ] Provide access credentials 7. [ ] Documentation in CMDB 8. [ ] Send welcome email

Responsible: Julia Becker

12.10.2 Offboarding Process

12.10.2.1 Employee Departure

Trigger: HR notification
Timeframe: On last day of work

Activities: 1. [ ] Deactivate account 2. [ ] Remove all permissions 3. [ ] Set up email forwarding (if required) 4. [ ] Block VPN access 5. [ ] Return hardware 6. [ ] Archive data 7. [ ] Update documentation 8. [ ] Inform manager

Responsible: Julia Becker

12.10.2.2 Role Change

Trigger: HR notification or manager request
Timeframe: On change date

Activities: 1. [ ] Remove old permissions 2. [ ] Assign new permissions 3. [ ] Conduct access review 4. [ ] Update documentation 5. [ ] Inform user

---

12.11 Compliance and Auditing

12.11.1 Compliance Requirements

Standard	Requirement	Implementation
GDPR	Access control for personal data	RBAC, audit logging
ISO 27001	Access control policy	This document
SOX	Separation of duties	Role separation
PCI DSS	Restricted access to cardholder data	Permission matrix

12.11.2 Audit Logging

Logged Events: - Login attempts (successful and failed) - Permission changes - Privileged actions - Access to sensitive data - Account creation/deletion - Password changes

Log Retention: [TODO: e.g., 1 year]
Log System: [TODO: e.g., Splunk, ELK]
Responsible: Thomas Weber

12.11.3 Audit Reports

Monthly Reports: - New accounts - Deleted accounts - Permission changes - Failed login attempts - Privileged access

Quarterly Reports: - Access review results - Compliance status - Risk assessment - Improvement suggestions

---

12.12 Emergency Access

12.12.1 Break-Glass Accounts

Definition: Emergency accounts for critical situations

Usage: - Only for critical outages - When normal access paths unavailable - After approval by Anna Schmidt

Requirements: - Physically secured passwords - Complete logging - Immediate notification to management - Post-incident review

Accounts: - `emergency_admin` - Full access to all systems - `emergency_network` - Network emergency access

Password Management: - Sealed envelopes in safe - Access only by Anna Schmidt or Thomas Weber

---

12.13 Contacts

Access Management Team: - **IT Operations Manager:** Andreas Huemmer - andreas.huemmer@adminsend.de - **CISO:** Thomas Weber - thomas.weber@adminsend.de - **Service Desk Lead:** Julia Becker - julia.becker@adminsend.de - **CIO:** Anna Schmidt - anna.schmidt@adminsend.de

Emergency Contacts: - **Break-Glass Approval:** Anna Schmidt - +49 89 12345678-200 - **Security Incident:** Thomas Weber - +49 89 12345678-300

Document Owner: IT Operations Manager
Approved by: CIO

Version: 1.0.0
Organization: AdminSend GmbH

ewpage

Chapter 13

Monitoring, Alerting and Observability

13.1 Overview

This document describes the monitoring, alerting, and observability strategy for the IT service. It defines monitoring tools, alerting rules, thresholds, and observability concepts.

Service: {{ meta.service_name }}
Responsible: Andreas Huemmer
Version: 1.0.0

13.2 Monitoring Strategy

13.2.1 Monitoring Objectives

- **Proactive Detection:** Identify problems before they have impact
- **Performance Optimization:** Identify and resolve bottlenecks
- **Availability:** Ensure service availability
- **Capacity Planning:** Identify trends for capacity planning
- **Compliance:** Evidence of service level compliance

13.2.2 Monitoring Layers

```
Layer 7: Business Metrics
(Transactions, User Experience, Business KPIs)



Layer 6: Application Monitoring
(Application Performance, Errors, Response Times)
```

```
Layer 5: Service Monitoring
(Service Health, API Endpoints, Dependencies)


Layer 4: Infrastructure Monitoring
(Servers, Network, Storage, Virtualization)


Layer 3: System Monitoring
(CPU, Memory, Disk, Network Interfaces)


Layer 2: Network Monitoring
(Connectivity, Bandwidth, Latency, Packet Loss)


Layer 1: Physical Monitoring
(Power, Cooling, Environmental)
```

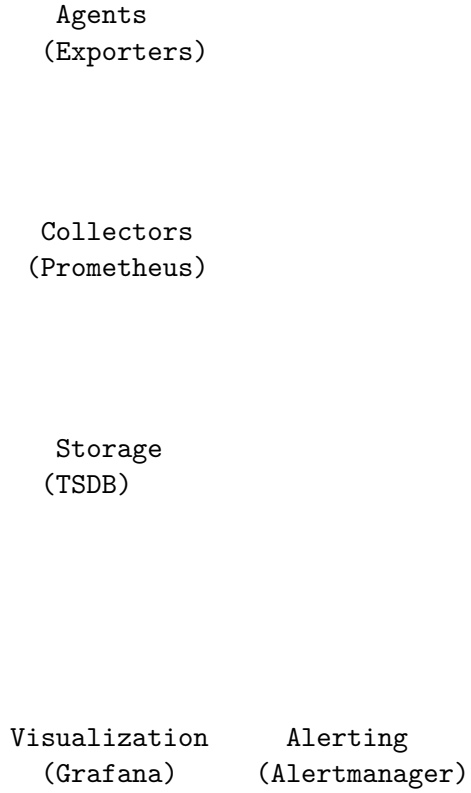
13.3 Monitoring Tools

13.3.1 Tool Stack

Tool	Usage	Responsible	URL
[**TODO: e.g., Prometheus**]	Metrics collection	Monitoring team	[TODO]
[**TODO: e.g., Grafana**]	Visualization	Monitoring team	[TODO]
[**TODO: e.g., Nagios/Zabbix**]	Infrastructure monitoring	IT operations	[TODO]
[**TODO: e.g., ELK Stack**]	Log aggregation	IT operations	[TODO]
[**TODO: e.g., Jaeger**]	Distributed tracing	Development team	[TODO]
[**TODO: e.g., Pingdom**]	Synthetic monitoring	IT operations	[TODO]
[**TODO: e.g., New Relic/Datadog**]	APM	Development team	[TODO]

13.3.2 Tool Integration

Data Flow:



13.4 Infrastructure Monitoring

13.4.1 Server Monitoring

13.4.1.1 Metrics

Metric	Description	Warning Threshold	Critical Threshold	Frequency
CPU Usage	CPU utilization	$> 80\%$	$> 95\%$	1 min
Memory Usage	RAM utilization	$> 85\%$	$> 95\%$	1 min
Disk Usage	Disk utilization	$> 80\%$	$> 90\%$	5 min
Disk I/O	Disk operations	$> 80\%$	$> 95\%$	1 min
Network Traffic	Network throughput	$> 80\%$	$> 95\%$	1 min
Load Average	System load	> 4.0	> 8.0	1 min
Swap Usage	Swap utilization	$> 50\%$	$> 80\%$	5 min

13.4.1.2 Monitored Servers

Server	Location	Role	Monitoring Agent	Status
{{ netbox.device.name }}	{{ netbox.device.site }}	{{ netbox.device.role }}	[TODO: Agent]	Active
[TODO]	[TODO]	[TODO]	[TODO]	Active

13.4.2 Network Monitoring

13.4.2.1 Metrics

Metric	Description	Warning Threshold	Critical Threshold	Frequency
Interface Status	Port up/down	Down	Down > 5 min	30 sec
Bandwidth Usage	Bandwidth utilization	> 80%	> 95%	1 min
Packet Loss	Packet loss	> 1%	> 5%	1 min
Latency	Network latency	> 50ms	> 100ms	1 min
Error Rate	Error rate	> 0.1%	> 1%	1 min
CRC Errors	CRC errors	> 0	> 100	5 min

13.4.2.2 Monitored Network Devices

Device	Type	Location	Management IP	Status
{{ netbox.device.name }}	{{ netbox.device.device_type }}	{{ netbox.device.site }}	{{ netbox.device.primary_ip }}	Active
[TODO]	[TODO]	[TODO]	[TODO]	Active

13.4.3 Storage Monitoring

13.4.3.1 Metrics

Metric	Description	Warning Threshold	Critical Threshold	Frequency
Capacity	Storage capacity	> 80%	> 90%	5 min
IOPS	I/O operations	> 80% max	> 95% max	1 min
Throughput	Throughput	> 80% max	> 95% max	1 min
Latency	Access time	> 20ms	> 50ms	1 min
Disk Health	Disk health	SMART warning	SMART error	1 hour

13.4.4 Virtualization Monitoring

13.4.4.1 Hypervisor Metrics

Metric	Description	Warning Threshold	Critical Threshold	Frequency
Host CPU	Host CPU utilization	> 80%	> 95%	1 min
Host Memory	Host RAM utilization	> 85%	> 95%	1 min
VM Count	Number of VMs	> 80% max	> 95% max	5 min
Datastore Usage	Datastore utilization	> 80%	> 90%	5 min
VM Performance	VM performance	Degraded	Critical	1 min

13.5 Application Monitoring

13.5.1 Application Performance Monitoring (APM)

13.5.1.1 Metrics

Metric	Description	Warning Threshold	Critical Threshold	Frequency
Response Time	Response time	> 500ms	> 2000ms	Real-time
Error Rate	Error rate	> 1%	> 5%	Real-time
Throughput	Requests/second	< 80% normal	< 50% normal	Real-time
Apdex Score	User satisfaction	< 0.85	< 0.70	Real-time
Database Query Time	DB query time	> 100ms	> 500ms	Real-time
External API Latency	API latency	> 200ms	> 1000ms	Real-time

13.5.2 Synthetic Monitoring

Monitored Endpoints:

Endpoint	Type	Frequency	Expected Response	Timeout
[TODO: URL]	HTTP/HTTPS	1 min	200 OK	5 sec
[TODO: URL]	API	1 min	200 OK	3 sec
[TODO: URL]	Health check	30 sec	200 OK	2 sec

Checks: - HTTP status code - Response time - Content validation - SSL certificate validity - DNS resolution

13.6 Observability

13.6.1 The Three Pillars of Observability

13.6.1.1 1. Metrics

Definition: Numerical values over time
Usage: Trends, alerts, dashboards
Tools: Prometheus, Grafana
Examples: - CPU utilization - Request rate - Error rate - Response time

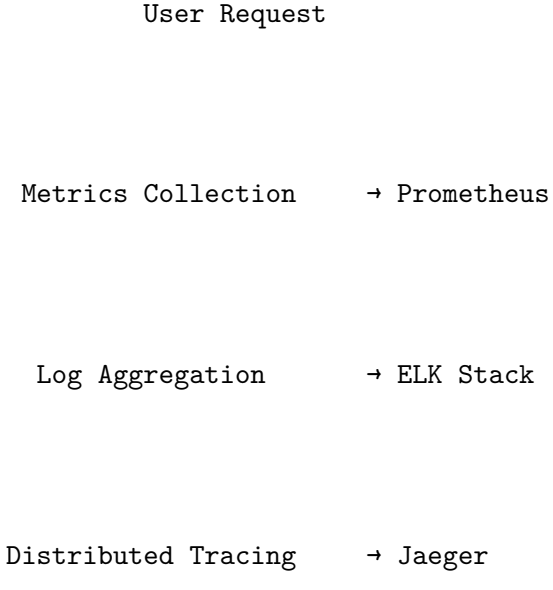
13.6.1.2 2. Logs

Definition: Event-based records
Usage: Debugging, audit, troubleshooting
Tools: ELK Stack, Splunk
Examples: - Application logs - System logs - Access logs - Error logs

13.6.1.3 3. Traces

Definition: Request flow through distributed systems
Usage: Performance analysis, bottleneck identification
Tools: Jaeger, Zipkin
Examples: - Distributed tracing - Service dependencies - Latency breakdown - Error propagation

13.6.2 Observability Strategy



```
Correlation &
Visualization          → Grafana
```

13.7 Alerting

13.7.1 Alerting Strategy

Principles: - **Actionable:** Every alert requires action - **Relevant:** Only alert on critical events - **Timely:** Alerts in real-time - **Clear:** Unambiguous alert descriptions - **Escalation:** Defined escalation paths

13.7.2 Alert Severity Levels

Level	Description	Response Time	Escalation	Example
Critical	Service outage	Immediate	Immediate	Service down
High	Severe problem	15 min	After 30 min	CPU > 95%
Medium	Problem requires attention	1 hour	After 4 hours	Disk > 85%
Low	Informational, no immediate action	1 day	None	Backup warning
Info	Informational	None	None	Backup success

13.7.3 Alerting Rules

13.7.3.1 Infrastructure Alerts

Alert	Condition	Severity	Action	Responsible
Server Down	Ping failed > 5 min	Critical	Check immediately	Julia Becker
High CPU	CPU > 95% for 5 min	High	Check performance	IT operations
High Memory	Memory > 95% for 5 min	High	Check memory leak	IT operations
Disk Full	Disk > 90%	High	Free up space	IT operations
Disk Warning	Disk > 80%	Medium	Plan capacity	IT operations

13.7.3.2 Application Alerts

Alert	Condition	Severity	Action	Responsible
Service Down	Health check failed	Critical	Restart service	Julia Becker

Alert	Condition	Severity	Action	Responsible
High Error Rate	Errors > 5% for 5 min	High	Check logs	Development team
Slow Response	Response time > 2s	High	Check performance	Development team
API Failure	External API down	High	Contact vendor	IT operations

13.7.3.3 Network Alerts

Alert	Condition	Severity	Action	Responsible
Link Down	Interface down > 5 min	Critical	Check connection	Network team
High Bandwidth	Bandwidth > 95%	High	Analyze traffic	Network team
High Latency	Latency > 100ms	Medium	Check routing	Network team
Packet Loss	Loss > 5%	High	Check connection	Network team

13.7.4 Alert Routing

```
  Alert Trigger


Alert Manager


  Email          Slack          SMS          PagerDuty
```

13.7.5 Alert Recipients

Severity	Primary	Secondary	Escalation
Critical	On-call engineer	IT ops manager	CIO
High	IT operations team	IT ops manager	-
Medium	IT operations team	-	-
Low	Email to team	-	-

On-Call Rotation: - **Week 1:** [TODO: Name] - **Week 2:** [TODO: Name] - **Week 3:** [TODO: Name] - **Week 4:** [TODO: Name]

13.8 Dashboards

13.8.1 Dashboard Overview

13.8.1.1 Executive Dashboard

Audience: Management
Content: - Service availability (current and historical) - SLA compliance - Incident overview - Performance trends - Cost overview

URL: [TODO: Dashboard URL]

13.8.1.2 Operations Dashboard

Audience: IT operations
Content: - Current alerts - System health status - Performance metrics - Capacity trends - Incident status

URL: [TODO: Dashboard URL]

13.8.1.3 Application Dashboard

Audience: Development team
Content: - Application performance - Error rates - Response times - Database performance - API latencies

URL: [TODO: Dashboard URL]

13.8.1.4 Infrastructure Dashboard

Audience: Infrastructure team
Content: - Server status - Network status - Storage status - Virtualization status - Environmental status

URL: [TODO: Dashboard URL]

13.8.2 Dashboard Best Practices

1. **Single Pane of Glass:** All important information at a glance
2. **Color Coding:** Red (critical), orange (warning), green (OK)
3. **Drill-Down:** Navigate from overview to details
4. **Real-Time:** Display current data
5. **Historical:** Show trends over time
6. **Annotations:** Mark important events

13.9 Monitoring Processes

13.9.1 Daily Monitoring Routines

Morning Check (08:00): - [ ] Check dashboards - [ ] Review open alerts - [ ] Check overnight incidents - [ ] Validate backup status - [ ] Analyze performance trends

Daily Monitoring: - [ ] Continuous alert monitoring - [ ] Incident response to alerts - [ ] Performance optimization - [ ] Capacity monitoring

Evening Check (18:00): - [ ] Review daily alerts - [ ] Document open issues - [ ] Handover to night shift (if 24/7) - [ ] Plan maintenance work

13.9.2 Weekly Activities

- ☐ Analyze monitoring data
- ☐ Perform alert tuning
- ☐ Reduce false positives
- ☐ Update dashboards
- ☐ Review capacity trends

13.9.3 Monthly Activities

- ☐ Check monitoring coverage
- ☐ Create SLA reports
- ☐ Analyze performance trends
- ☐ Update monitoring tools
- ☐ Optimize alert rules

13.10 Service Level Indicators (SLIs)

13.10.1 Defined SLIs

SLI	Description	Measurement	Target Value
Availability	Service availability	Uptime / total time	99.5%
Latency	Response time	P95 response time	500ms
Error Rate	Error rate	Errors / total requests	0.1%
Throughput	Throughput	Requests / second	[TODO]
Saturation	Resource utilization	CPU/memory/disk usage	80%

13.10.2 SLI Monitoring

Data Sources: - Synthetic monitoring - Real user monitoring (RUM) - Application logs - Infrastructure metrics

Reporting: - Real-time dashboards - Daily reports - Monthly SLA reports

---

13.11 Incident Response

13.11.1 Monitoring-Based Incident Response

```
 Alert Trigger
```

```
Alert Received
```

```
Initial Triage
```

```
Incident Created
```

```
Investigation
```

```
  Resolution
```

```
Post-Mortem
```

Details: See Chapter 0120 (Incident Management)

13.12 Monitoring Documentation

13.12.1 Runbooks

For each critical alert, a runbook exists: - Alert description - Possible causes - Diagnosis steps - Resolution steps - Escalation path

Runbook Directory: See Chapter 0240 (Runbooks)

13.12.2 Known Issues

Known monitoring problems and workarounds: - False-positive alerts - Monitoring gaps - Tool limitations

Known Issues: See Chapter 0260 (Known Problems and FAQ)

13.13 Monitoring Tool Access

13.13.1 Tool Access

Tool	URL	Authentication	Access
[TODO: Monitoring tool]	[TODO: URL]	SSO	IT operations
[TODO: Dashboard tool]	[TODO: URL]	SSO	All
[TODO: Log tool]	[TODO: URL]	SSO	IT operations
[TODO: APM tool]	[TODO: URL]	SSO	Development

13.13.2 Permissions

- **Administrator:** Andreas Huemmer
- **Operator:** IT operations team
- **Read-Only:** Management, auditors

13.14 Contacts

Monitoring Team: - **IT Operations Manager:** Andreas Huemmer - andreas.huemmer@adminsend.de - **Service Desk Lead:** Julia Becker - julia.becker@adminsend.de - **On-Call Engineer:** [TODO: Rotation] - [TODO: On-call number]

Escalation: - **Level 2:** Andreas Huemmer - +49 89 12345678-250 - **Level 3:** Anna Schmidt - +49 89 12345678-200

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

ewpage

Chapter 14

Incident Management Runbook

14.1 Purpose and Scope

This document describes the incident management process for AdminSend GmbH according to ITIL v4 best practices. It defines categories, priorities, escalation processes, and standard runbooks for handling service disruptions.

Scope: All IT services and systems of AdminSend GmbH

Responsible: Andreas Huemmer (andreas.huemmer@adminsend.de)

14.2 Incident Definition

An **incident** is an unplanned interruption or quality reduction of an IT service. The goal of incident management is to restore normal service operation as quickly as possible.

14.2.1 Distinction from Other Processes

Process	Focus	Goal
Incident Management	Symptom treatment	Quick restoration
Problem Management	Root cause analysis	Permanent solution
Change Management	Planned changes	Controlled implementation
Service Request	Standard requests	Fulfillment of requirements

14.3 Incident Categories

14.3.1 Categorization by Area

Category	Description	Examples
Hardware	Physical devices and components	Server failure, disk defect, network hardware
Software	Applications and operating systems	Application crash, license issues, software bugs

Category	Description	Examples
Network	Network connections and services	Connection drops, DNS problems, firewall blocks
Security	Security incidents	Malware, unauthorized access, data breach
Performance	Performance problems	Slow response times, high CPU load, memory leaks
Data	Data loss or corruption	Database corruption, backup errors, data loss
User	Access and permission problems	Login problems, password reset, missing permissions

14.3.2 Categorization by Service

- **Email Service**
- **File Server**
- **Database Service**
- **Web Applications**
- **Network Infrastructure**
- **Backup Systems**
- **Monitoring Systems**
- **[Additional services per service catalog]**

14.4 Incident Priorities

The priority of an incident is determined by **impact** and **urgency**.

14.4.1 Impact Assessment

Impact	Description	Affected Users
High	Critical service completely failed	$>$ 50% of users or business-critical service
Medium	Service limited availability	10-50% of users or important service
Low	Individual users affected	$<$ 10% of users or non-critical service

14.4.2 Urgency Assessment

Urgency	Description	Time Window
High	Immediate processing required	Business process blocked
Medium	Timely processing required	Business process impaired
Low	Can be processed as planned	No immediate impact

14.4.3 Priority Matrix

	Urgency: High	**Urgency: Medium**	**Urgency: Low**
Impact: High	**P1 - Critical**	**P2 - High**	**P3 - Medium**
Impact: Medium	**P2 - High**	**P3 - Medium**	**P4 - Low**
Impact: Low	**P3 - Medium**	**P4 - Low**	**P5 - Planned**

14.4.4 Service Level Targets

Priority	Response Time	Resolution Time	Escalate After
P1 - Critical	15 minutes	4 hours	1 hour
P2 - High	30 minutes	8 hours	2 hours
P3 - Medium	2 hours	24 hours	8 hours
P4 - Low	4 hours	48 hours	24 hours
P5 - Planned	1 business day	5 business days	-

14.5 Incident Management Process

14.5.1 Process Overview (ITIL v4)

```
Incident
Detection



Incident
Logging



Categorization
& Prioritization



Initial
Diagnosis



    Known     Yes
    Error?       Apply
               Workaround
         No
```

```
Investigation
& Diagnosis



Resolution
& Recovery



Incident
Closure
```

14.5.2 1. Incident Detection

Detection Sources: - Monitoring alerts ({{ netbox.monitoring_system }}) - Service desk tickets - User reports - Automatic event correlation

Responsible: Monitoring system, service desk

14.5.3 2. Incident Logging

Required Information: - Incident ID (automatically generated) - Timestamp of report - Affected service/system - Symptom description - Affected users/locations - Reporter (name, contact)

Tool: {{ meta.ticketing_system }}

Responsible: Service desk

14.5.4 3. Categorization & Prioritization

Activities: - Assign category (hardware, software, network, etc.) - Assess impact - Assess urgency - Calculate priority (P1-P5) - Identify affected service

Responsible: Service desk / incident manager

14.5.5 4. Initial Diagnosis

Activities: - Analyze symptoms - Check logs - Evaluate monitoring data - Search known error database - First resolution attempts (level 1)

Responsible: Service desk (level 1)

14.5.6 5. Investigation & Diagnosis

Activities: - Detailed technical analysis - Root cause identification (if possible) - Workaround development - Escalation to specialists (level 2/3)

Responsible: IT operations team (level 2/3)

14.5.7 6. Resolution & Recovery

Activities: - Implement solution - Restore service - Test functionality - Inform users

Responsible: IT operations team

14.5.8 7. Incident Closure

Activities: - Obtain user confirmation - Complete documentation - Close incident - Create problem ticket if needed

Responsible: Service desk

14.6 Escalation Processes

14.6.1 Hierarchical Escalation

Level	Role	Contact	Escalate For
Level 1	Service desk	julia.becker@adminsend.de	Standard incidents
Level 2	IT operations team	andreas.huemmer@adminsend.de	Complex technical problems
Level 3	Specialists / vendor	[Vendor contacts]	Specialist knowledge required
Management	CIO	anna.schmidt@adminsend.de	P1 incidents > 2h

14.6.2 Functional Escalation

Area	Contact Person	Contact	Responsibility
Network	Network team	Email	Network infrastructure
Server	Server team	Email	Servers and virtualization
Database	DBA team	Email	Database systems
Security	Security team	thomas.weber@adminsend.de	Security incidents
Applications	Application team	Email	Business applications

14.6.3 Escalation Triggers

Automatic Escalation For: - P1 incident not resolved after 1 hour - P2 incident not resolved after 2 hours - P3 incident not resolved after 8 hours - Multiple reopenings of same incident - Security incidents (immediately to CISO)

Management Escalation For: - P1 incidents (inform CIO) - Incidents with high media attention - Incidents with legal implications - Multiple simultaneous P1/P2 incidents

14.7 Standard Runbooks

14.7.1 Runbook 1: Server Unreachable

Symptoms: Server not responding to ping, services unavailable

Priority: P1 or P2 (depending on service criticality)

Diagnosis Steps: 1. Perform ping test: `ping {{ netbox.server.ip }}` 2. Check monitoring dashboard 3. Check physical state (if on-site) 4. Check network connectivity 5. Check hypervisor status (for VMs)

Resolution Steps: 1. Restore network connection (if network problem) 2. Perform server restart (if hanging) 3. Perform hypervisor migration (for VM problem) 4. Initiate hardware replacement (for hardware defect) 5. Activate backup system (if primary system defective)

Escalation: After 30 minutes to level 2, after 1 hour to management

14.7.2 Runbook 2: Application Slow / Unreachable

Symptoms: Long response times, timeouts, HTTP 500/503 errors

Priority: P2 or P3

Diagnosis Steps: 1. Check application logs 2. Analyze performance metrics (CPU, RAM, disk I/O) 3. Check database performance 4. Measure network latency 5. Check load balancer status

Resolution Steps: 1. Perform application restart 2. Clear cache 3. Optimize database queries 4. Scale resources (increase CPU/RAM) 5. Redirect traffic to other instances

Escalation: After 2 hours to application team

14.7.3 Runbook 3: Database Connection Error

Symptoms: Connection timeout, "too many connections", application cannot access DB

Priority: P1 or P2

Diagnosis Steps: 1. Check database status: `systemctl status postgresql` 2. Check connection pool 3. Analyze database logs 4. Check disk space 5. Check network connectivity to DB

Resolution Steps: 1. Restart database service 2. Increase connection pool limits 3. Terminate long-running queries 4. Free up disk space 5. Failover to standby database

Escalation: Immediately to DBA team for P1

14.7.4 Runbook 4: Backup Failed

Symptoms: Backup job reports error, backup monitoring alert

Priority: P2 or P3

Diagnosis Steps: 1. Check backup logs 2. Check disk space on backup target 3. Check network connection to backup storage 4. Check backup software status 5. Check source system status

Resolution Steps: 1. Manually restart backup job 2. Free up disk space on backup target 3. Restore network connection 4. Restart backup software 5. Use alternative backup method

Escalation: After 4 hours to backup team

14.7.5 Runbook 5: Security Incident (Malware/Intrusion)

Symptoms: Malware alert, unusual network activity, unauthorized access

Priority: P1 (always)

Diagnosis Steps: 1. Analyze alert details 2. Identify affected systems 3. Assess extent of compromise 4. Secure logs (forensics) 5. Inform CISO

Resolution Steps: 1. Isolate affected systems (network separation) 2. Perform malware scan 3. Block compromised accounts 4. Reset passwords 5. Perform forensic analysis 6. Rebuild systems (if required)

Escalation: Immediately to CISO (thomas.weber@adminsend.de)

14.7.6 Runbook 6: Network Outage

Symptoms: No network connectivity, devices unreachable

Priority: P1 or P2

Diagnosis Steps: 1. Identify affected network segments 2. Check switch/router status 3. Check physical cabling 4. Check VLAN configuration 5. Check routing tables

Resolution Steps: 1. Restart network devices 2. Replace defective cables 3. Correct VLAN configuration 4. Fix routing problems 5. Failover to backup connection

Escalation: After 30 minutes to network team

14.8 Communication Processes

14.8.1 Internal Communication

At Incident Opening: - Service desk informs affected users - IT operations team immediately informed for P1/P2 - Management informed for P1

During Processing: - Regular status updates (P1: every 30 min, P2: every 2h) - Escalation notifications - Team communication via {{ meta.collaboration_tool }}

At Incident Resolution: - User notification of resolution - Management information for P1/P2 - Documentation in ticket system

14.8.2 External Communication

Stakeholder Information: - Executive management for critical incidents - Customers for service outages - External partners for dependencies

Communication Channels: - Email: info@adminsend.de - Status page: {{ meta.status_page_url }} - Phone: +49 89 12345678

Communication Template:

```
Subject: [P1/P2] Service Disruption: [Service Name]

Dear Sir or Madam,
```

```
We inform you about a current service disruption:

Service: [Service Name]
Priority: [P1/P2/P3]
Start: [Timestamp]
Impact: [Description]
Status: [In Progress / Resolved]

We are working intensively on the solution and will keep you informed.

Next update: [Time]

Best regards
AdminSend GmbH
IT Operations Team
```

14.9 Major Incident Management

14.9.1 Major Incident Definition

A **major incident** is an incident with: - Priority P1 - Impact on critical business processes - High number of affected users ($> 50\%$) - Potential financial or legal consequences

14.9.2 Major Incident Team

Role	Person	Responsibility
Incident Manager	Andreas Huemmer	Coordination and communication
Technical Lead	[Name]	Technical solution finding
Communication Lead	[Name]	Stakeholder communication
Management Rep	Anna Schmidt	Decisions and escalation

14.9.3 Major Incident Process

1. **Incident Declaration:** Incident manager declares major incident
2. **Team Assembly:** Major incident team is convened
3. **War Room:** Dedicated communication channel (e.g., conference call)
4. **Status Updates:** Every 30 minutes to stakeholders
5. **Resolution:** Coordinated solution implementation
6. **Post-Incident Review:** Mandatory postmortem within 48h

14.10 Metrics and Reporting

14.10.1 Key Performance Indicators (KPIs)

Metric	Target Value	Measurement
Mean Time to Respond (MTTR)	< 15 min (P1)	Average response time
Mean Time to Resolve (MTTR)	< 4h (P1)	Average resolution time
First Call Resolution Rate	> 70%	Resolution on first contact
Incident Reopen Rate	< 5%	Reopening rate
SLA Compliance	> 95%	Adherence to SLA times

14.10.2 Reporting

Daily Reporting: - Number of open incidents (by priority) - P1/P2 incidents in progress - SLA violations

Weekly Reporting: - Incident trend analysis - Top 5 incident categories - Escalation statistics

Monthly Reporting: - KPI dashboard - Service availability - Improvement measures

14.11 Tools and Systems

14.11.1 Incident Management Tool

- **System:** {{ meta.ticketing_system }}
- **URL:** {{ meta.ticketing_system_url }}
- **Access:** All IT staff

14.11.2 Monitoring System

- **System:** {{ netbox.monitoring_system }}
- **URL:** {{ meta.monitoring_url }}
- **Access:** IT operations team

14.11.3 Communication Tools

- **Chat:** {{ meta.collaboration_tool }}
- **Conference:** {{ meta.conference_system }}
- **Status Page:** {{ meta.status_page_url }}

14.12 Appendix

14.12.1 Incident Categories (Complete)

- Hardware > Server
- Hardware > Storage
- Hardware > Network
- Software > Operating System
- Software > Application
- Software > Database
- Network > Connectivity

- Network > Performance
- Security > Malware
- Security > Unauthorized Access
- Security > Data Breach
- Performance > Slow Response
- Performance > High Load
- Data > Corruption
- Data > Loss
- User > Access
- User > Authentication

14.12.2 Contacts and On-Call

Team	Primary	Secondary	On-Call
Service Desk	julia.becker@adminsend.de	[Backup]	24/7
IT Operations	andreas.huemmer@adminsend.de	[Backup]	24/7
Network Team	Email	[Backup]	On-call
Security Team	thomas.weber@adminsend.de	[Backup]	24/7

14.12.3 References

- ITIL v4 Foundation
- ISO/IEC 20000-1:2018 - Service Management
- Internal Service Level Agreements
- Escalation Matrix

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Classification: internal
Last Update: {{ meta.date }}

ewpage

Chapter 15

Problem Management and Postmortems

15.1 Purpose and Scope

This document describes the problem management process for AdminSend GmbH according to ITIL v4 best practices. It defines the systematic analysis of recurring incidents, root cause analysis methods, postmortem processes, and the management of the Known Error Database.

Scope: All IT services and systems of AdminSend GmbH

Responsible: Andreas Huemmer (andreas.huemmer@adminsend.de)

15.2 Problem Definition

A **problem** is the unknown cause of one or more incidents. The goal of problem management is to identify and eliminate the root cause to prevent future incidents.

15.2.1 Distinction: Incident vs. Problem

Aspect	Incident	Problem
Focus	Symptoms	Causes
Goal	Quick restoration	Permanent solution
Timeframe	Immediate	Planned
Approach	Workaround	Root-Cause-Elimination
Process	Reactive	Proactive

15.3 Problem Management Process

15.3.1 Process Overview (ITIL v4)

```
Problem
Detection
```

```
Problem
Logging


Problem
Categorization


Problem
Prioritization


Investigation
& Diagnosis
(RCA)


Workaround
Identification


Known Error
Recording


Problem
Resolution


Problem
Closure
```

15.3.2 1. Problem Detection

Detection Sources: - Recurring incidents (> 3x in 30 days) - Trend analysis of incident data - Proactive monitoring analyses - Major incident reviews - Vendor bulletins and security advisories

Triggers for Problem Creation: - Multiple similar incidents - Incidents with high business

impact - Incidents without known solution - Structural weaknesses

Responsible: Problem Manager, IT Operations Team

15.3.3 2. Problem Logging

Required Information: - Problem ID (automatically generated) - Linked incident IDs - Symptom description - Affected services/systems - Affected configuration items (CIs) - Initial hypotheses about cause

Tool: {{ meta.ticketing_system }}

Responsible: Problem Manager

15.3.4 3. Problem Categorization

Categories: - Hardware problems - Software problems - Network problems - Process problems - Documentation problems - Capacity problems - Security problems

Responsible: Problem Manager

15.3.5 4. Problem Prioritization

Priority Factors: - Number of affected incidents - Business impact - Frequency of occurrence - Availability of workarounds - Resource availability

Priority Levels:

Priority	Description	Processing Time
P1 - Critical	Frequent P1 incidents, no workaround	Immediate
P2 - High	Frequent P2 incidents, temporary workaround	1 week
P3 - Medium	Moderate frequency, workaround available	1 month
P4 - Low	Rare incidents, low impact	Planned

15.3.6 5. Investigation & Diagnosis (Root Cause Analysis)

RCA Methods: - 5-Why analysis - Fishbone diagram (Ishikawa) - Fault tree analysis - Timeline analysis - Log correlation

Activities: - Collect data (logs, monitoring, configurations) - Develop hypotheses - Conduct tests - Identify root cause - Create documentation

Responsible: Problem Manager, Technical Specialists

15.3.7 6. Workaround Identification

Workaround Criteria: - Reduces impact or frequency - Practical for incident teams - Documented and tested - Temporary solution until permanent fix

Documentation: - Workaround description - Application steps - Limitations - Validity period

15.3.8 7. Known Error Recording

Known Error Database (KEDB): - Problem description - Root cause - Workaround - Permanent solution (if available) - Linked incidents - Linked CIs

Access: All IT staff (Read), Problem Manager (Write)

15.3.9 8. Problem Resolution

Solution Approaches: - Software patch or update - Configuration change - Hardware replacement - Process improvement - Documentation update - Training

Change Management: - Permanent solutions require change request - Change planning and approval - Implementation via change process

15.3.10 9. Problem Closure

Closure Criteria: - Root cause identified and documented - Permanent solution implemented - No new incidents occurred (monitoring period) - Documentation complete - Lessons learned documented

Responsible: Problem Manager

15.4 Root Cause Analysis (RCA) Methods

15.4.1 5-Why Analysis

Method: Ask "Why?" five times to get to the root cause

Example: 1. **Why** did the database fail? → Disk full 2. **Why** was the disk full? → Log files not rotated 3. **Why** were logs not rotated? → Logrotate job failed 4. **Why** did the job fail? → Incorrect cron configuration 5. **Why** was the configuration incorrect? → No validation after change

Root Cause: Missing change validation

15.4.2 Fishbone Diagram (Ishikawa)

Categories: - **People:** Errors, knowledge, training - **Methods:** Processes, procedures, standards - **Machines:** Hardware, software, tools - **Materials:** Data, configurations, documentation - **Environment:** Infrastructure, network, location - **Management:** Decisions, resources, priorities

Application: 1. Define problem as "fish head" 2. Draw main categories as "bones" 3. Identify causes per category 4. Add deeper causes as sub-bones 5. Identify root cause

15.4.3 Timeline Analysis

Method: Chronological reconstruction of events

Steps: 1. Create timeline 2. Enter all relevant events 3. Identify causalities 4. Work out critical path 5. Find root cause at beginning of causal chain

Data Sources: - Incident tickets - Change records - Monitoring logs - System logs - Deployment history

15.5 Postmortem Process

15.5.1 Postmortem Definition

A **postmortem** is a structured analysis of a major incident or critical problem with the goal of identifying lessons learned and implementing improvements.

15.5.2 Postmortem Triggers

Mandatory Postmortems for: - Major incidents (P1) - Service outages > 4 hours - Data loss or security breach - Incidents with media attention - Repeated incidents despite previous solution

Optional Postmortems for: - P2 incidents with interesting lessons learned - Successful incident management (best practices) - Near-miss situations

15.5.3 Postmortem Timeline

Phase	Timing	Activity
Initiation	Within 24h	Announce postmortem, invite participants
Data Collection	24-48h	Collect logs, timelines, facts
Meeting	Within 1 week	Conduct postmortem meeting
Documentation	Within 2 weeks	Finalize postmortem report
Follow-up	Ongoing	Implement and track action items

15.5.4 Postmortem Meeting

Participants: - Incident Manager - Affected teams - Service Owner - Management (for major incidents) - Optional: External stakeholders

Agenda: 1. **Incident Overview** (5 min) - What happened? - When did it happen? - Who was affected?

2. **Timeline Review** (15 min)
   - Chronological events
   - Decision points
   - Communication
3. **Root Cause Analysis** (20 min)
   - 5-Why or Fishbone
   - Contributing factors
   - Root cause
4. **What Went Well** (10 min)
   - Successful measures
   - Good collaboration
   - Effective tools
5. **What Went Wrong** (10 min)
   - Problems and delays
   - Communication issues
   - Tool or process deficiencies

6. **Action Items** (15 min)
    - Improvement measures
    - Responsible parties
    - Deadlines

Duration: 60-90 minutes

Moderator: Problem Manager or neutral facilitator

15.5.5 Postmortem Principles

Blameless Culture: - Focus on systems and processes, not people - No blame assignment - Psychological safety - Learning from mistakes

Fact-Based: - Objective data (logs, metrics) - No speculation - Verifiable statements

Constructive: - Solution-oriented - Concrete action items - Actionable improvements

15.6 Postmortem Template

15.6.1 1. Executive Summary

Incident Overview: - **Incident ID:** [ID] - **Date/Time:** [Start] - [End] - **Duration:** [Hours] - **Priority:** P1 / P2 - **Affected Service:** [Service Name] - **Impact:** [Number of users, business impact]

Summary: [2-3 sentences: What happened and what was the cause?]

15.6.2 2. Timeline

Time	Event	Action	Responsible
10:00	Alert: Database CPU 100%	Monitoring alert triggered	Monitoring System
10:05	Service Desk receives calls	Incident ticket created	Service Desk
10:15	Escalation to DBA team	Database analysis started	IT Operations
10:30	Root cause identified	Slow query found	DBA Team
10:45	Query optimized	Deployment performed	DBA Team
11:00	Service restored	Monitoring confirmed	IT Operations

15.6.3 3. Root Cause Analysis

5-Why Analysis: 1. Why was the database overloaded? → Slow query 2. Why was there a slow query? → Missing index 3. Why was the index missing? → Not included in deployment 4. Why wasn't it in the deployment? → Not caught in code review 5. Why wasn't it caught? → No performance tests

Root Cause: Missing performance tests in CI/CD pipeline

Contributing Factors: - Insufficient code review checklist - No automated query analysis - Missing staging environment with production data volume

15.6.4 4. Impact Assessment

Technical Impact: - Database CPU: 100% for 60 minutes - Response times: $>$ 30 seconds (normal: $<$ 1s) - Service availability: 0% for 60 minutes

Business Impact: - Affected users: 500 (100%) - Blocked business processes: Order Processing - Estimated revenue loss: [Amount] - Reputation damage: Medium

SLA Impact: - SLA target: 99.9% availability - Actual availability: 99.86% - SLA breach: Yes

15.6.5 5. What Went Well

- Quick escalation to DBA team (10 minutes)
- Effective communication between teams
- Root cause quickly identified (25 minutes)
- Solution successfully implemented
- No data loss

15.6.6 6. What Went Wrong

- Slow query not detected before deployment
- No automatic performance tests
- Staging environment not representative
- Monitoring alert too late (CPU threshold too high)
- Rollback procedure not documented

15.6.7 7. Action Items

ID	Measure	Responsible	Deadline	Status
AI-001	Integrate performance tests in CI/CD	DevOps Team	2 weeks	Open
AI-002	Extend code review checklist	Dev Team	1 week	Open
AI-003	Staging database with prod volume	DBA Team	1 month	Open
AI-004	Adjust monitoring thresholds	Ops Team	1 week	Open
AI-005	Create rollback runbook	DBA Team	2 weeks	Open

15.6.8 8. Lessons Learned

Technical: - Performance tests are essential before deployments - Staging environment must simulate production data volume - Automated query analysis can detect problems early

Process: - Code review checklists must cover performance aspects - Rollback procedures must be documented and tested - Monitoring thresholds must be reviewed regularly

Organizational: - Team communication worked well - Escalation processes were effective - Documentation needs improvement

15.6.9 9. Follow-up

Review Date: [Date, 4 weeks after incident]

Review Agenda: - Status of all action items - Effectiveness of measures - Further improvements

Responsible: Problem Manager

15.7 Known Error Database (KEDB)

15.7.1 KEDB Structure

Required Fields: - **Known Error ID:** Unique identifier - **Title:** Brief description - **Symptoms:** How does the problem manifest? - **Root Cause:** Identified root cause - **Workaround:** Temporary solution - **Permanent Solution:** Permanent fix (if available) - **Affected CIs:** Configuration items - **Linked Incidents:** Incident IDs - **Linked Problems:** Problem IDs - **Status:** Open, Workaround Available, Resolved, Closed - **Priority:** P1-P4 - **Created:** Date, author - **Updated:** Date, author

15.7.2 KEDB Example

Known Error ID: KE-2024-001

Title: PostgreSQL Connection Pool Exhaustion

Symptoms: - Application reports "Connection timeout" - Database logs show "too many connections" - Monitoring shows 100% connection pool utilization

Root Cause: - Connection pool limit configured too low (max_connections=100) - Application not releasing connections correctly (connection leak) - Missing connection timeout configuration

Workaround: 1. Restart PostgreSQL service: `systemctl restart postgresql` 2. Restart application: `systemctl restart app-service` 3. Monitoring: Observe connection pool utilization

Permanent Solution: 1. Increase max_connections in postgresql.conf: `max_connections = 200` 2. Fix connection leak in application (code fix) 3. Configure connection timeout: `idle_in_transaction_session_timeout = 60000` 4. Improve connection pool monitoring

Affected CIs: - {{ netbox.database.server }} - {{ netbox.application.server }}

Linked Incidents: INC-2024-123, INC-2024-145, INC-2024-167

Status: Resolved

Priority: P2

15.7.3 KEDB Usage

Incident Handling: 1. Match incident symptoms with KEDB 2. If match: Apply workaround 3. Link incident with known error 4. Reference problem ticket

Problem Analysis: 1. Enter new known errors in KEDB 2. Document workarounds 3. Track permanent solutions 4. Update status

Knowledge Management: - Use KEDB as knowledge base - Regular reviews (monthly) - Archive outdated entries - Document best practices

15.8 Proactive Problem Management

15.8.1 Trend Analysis

Data Sources: - Incident statistics - Monitoring metrics - Performance data - Capacity utilization

Analysis Methods: - Time series analysis - Correlation analysis - Anomaly detection - Predictive analytics

Goal: Identify problems before they become incidents

15.8.2 Proactive Measures

Regular Reviews: - Weekly incident trend reviews - Monthly problem reviews - Quarterly service reviews

Preventive Measures: - Capacity upgrades - Software updates and patches - Configuration optimizations - Process improvements - Training and documentation

15.8.3 Continuous Improvement

Improvement Cycle: 1. **Measure:** Capture metrics 2. **Analyze:** Identify trends 3. **Improve:** Implement measures 4. **Control:** Check effectiveness

Improvement Areas: - Processes - Tools - Documentation - Skills and training - Infrastructure

15.9 Metrics and Reporting

15.9.1 Key Performance Indicators (KPIs)

Metric	Target Value	Measurement
Problem Resolution Rate	$> 80\%$	Resolved problems / Total problems
Mean Time to Resolve Problem	< 30 days	Average resolution time
Known Error Utilization	$> 60\%$	Incidents with KEDB workaround
Recurring Incident Rate	$< 10\%$	Incidents with known cause
Postmortem Completion Rate	100%	Postmortems for major incidents

15.9.2 Reporting

Monthly Problem Report: - Number of open problems (by priority) - Newly created problems - Resolved problems - Top 5 problem categories - KEDB statistics - Action items status

Quarterly Trend Analysis: - Problem trends over time - Recurring problem patterns - Effectiveness of improvement measures - ROI of problem management

15.10 Roles and Responsibilities

15.10.1 Problem Manager

Responsibilities: - Problem process ownership - Problem prioritization - RCA coordination - KEDB management - Postmortem moderation - Reporting

Person: Andreas Huemmer

15.10.2 Technical Specialists

Responsibilities: - Technical analysis - RCA execution - Solution development - Workaround identification

Teams: Server Team, Network Team, DBA Team, Application Team

15.10.3 Service Owner

Responsibilities: - Business impact assessment - Prioritization decisions - Resource provisioning - Stakeholder communication

15.11 Tools and Systems

15.11.1 Problem Management Tool

- **System:** {{ meta.ticketing_system }}
- **URL:** {{ meta.ticketing_system_url }}
- **Access:** IT Operations Team

15.11.2 Known Error Database

- **System:** {{ meta.ticketing_system }} (KEDB module)
- **URL:** {{ meta.kedb_url }}
- **Access:** All IT staff (Read)

15.11.3 RCA Tools

- **Collaboration:** {{ meta.collaboration_tool }}
- **Diagramming:** {{ meta.diagramming_tool }}
- **Log Analysis:** {{ meta.log_analysis_tool }}

15.12 References

- ITIL v4 Foundation - Problem Management
- ISO/IEC 20000-1:2018 - Problem Management
- Site Reliability Engineering (SRE) - Postmortem Culture
- Internal Incident Management Processes
- Change Management Processes

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Classification: internal
Last Updated: {{ meta.date }}

ewpage

Chapter 16

Change and Release Management

16.1 Purpose and Scope

This document describes the change and release management processes for AdminSend GmbH according to ITIL v4 best practices. It defines change categories, approval processes, release strategies, and rollback procedures for controlled implementation of changes to IT services and systems.

Scope: All IT services, systems, and infrastructure components of AdminSend GmbH

Responsible: Andreas Huemmer (andreas.huemmer@adminsend.de)

16.2 Change Management

16.2.1 Change Definition

A **change** is the addition, modification, or removal of anything that could have a direct or indirect effect on services. The goal of change management is to minimize risks while maximizing business value.

16.2.2 Change Principles

Core Principles: - **Controlled:** All changes go through defined processes - **Documented:** Complete documentation of all changes - **Approved:** Authorization before implementation - **Tested:** Validation before production deployment - **Reversible:** Rollback plan for every change

16.2.3 Change Categories

16.2.3.1 Standard Change

Definition: Pre-approved, low-risk, frequently performed changes with documented procedure.

Characteristics: - Low risk - Known procedure - Pre-approval by CAB - No individual approval required - Documented runbooks

Examples: - Password reset - User creation/deletion - Standard software installation - Backup restore (non-critical) - Certificate renewal - Routine patches (tested)

Approval: Automatic (pre-approved)

Processing Time: Immediate to 24 hours

16.2.3.2 Normal Change

Definition: Changes that require individual assessment, approval, and planning.

Characteristics: - Medium to high risk - Individual assessment required - CAB approval required - Detailed planning - Test phase required

Examples: - New software deployments - Infrastructure changes - Network reconfigurations - Database schema changes - Major version upgrades - New service introductions

Approval: Change Advisory Board (CAB)

Processing Time: 1-4 weeks (depending on complexity)

16.2.3.3 Emergency Change

Definition: Urgent changes to resolve critical incidents or security issues.

Characteristics: - High urgency - Shortened approval processes - Minimal documentation before implementation - Retrospective complete documentation - Emergency CAB (ECAB) approval

Examples: - Security patches (zero-day) - Critical bugfixes - Disaster recovery measures - Service restoration - Security incidents

Approval: Emergency CAB (ECAB) or CIO

Processing Time: Immediate to 4 hours

16.2.4 Change Process

16.2.4.1 Process Overview

```
Change Request
Creation



Change
Assessment



Change
Authorization
(CAB)



Change
Planning
```

```
Change
Implementation


Change
Review


Change
Closure
```

16.2.4.2 1. Change Request Creation

Required Information: - **Change ID:** Automatically generated - **Title:** Brief description - **Description:** Detailed description of change - **Justification:** Business reason, problem reference - **Category:** Standard / Normal / Emergency - **Affected Services:** Service list - **Affected CIs:** Configuration items - **Risk Assessment:** Low / Medium / High - **Implementation Plan:** Step-by-step instructions - **Rollback Plan:** Reversal procedure - **Test Plan:** Validation steps - **Time Window:** Planned maintenance window - **Requester:** Requestor - **Implementer:** Executor

Tool: {{ meta.ticketing_system }}

Responsible: Change Requester

16.2.4.3 2. Change Assessment

Assessment Criteria: - **Impact:** Effect on services and users - **Risk:** Probability and severity of problems - **Complexity:** Technical complexity - **Dependencies:** Affected systems and services - **Resources:** Required skills and time

Risk Matrix:

	Impact: Low	**Impact: Medium**	**Impact: High**
Probability: Low	Low Risk	Medium Risk	Medium Risk
Probability: Medium	Medium Risk	Medium Risk	High Risk
Probability: High	Medium Risk	High Risk	Very High Risk

Responsible: Change Manager

16.2.4.4 3. Change Authorization (CAB)

Change Advisory Board (CAB):

Members: - **Chair:** Andreas Huemmer (Change Manager) - **CIO:** Anna Schmidt - **CISO:** Thomas Weber - **Service Owner:** [Service-dependent] - **Technical Leads:** [Change-dependent] - **Business Representatives:** [For business impact]

CAB Meeting: - **Frequency:** Weekly (Tuesday 10:00) - **Duration:** 60 minutes - **Agenda:** Review all normal changes - **Decision:** Approve / Reject / Defer

Emergency CAB (ECAB): - **Members:** CIO, Change Manager, Technical Lead - **Convening:** Ad-hoc for emergency changes - **Decision:** Within 1 hour

Approval Criteria: - Complete documentation - Acceptable risk - Resources available - Test plan present - Rollback plan present - Maintenance window available

16.2.4.5 4. Change Planning

Planning Activities: - Detailed implementation steps - Resource allocation - Create schedule - Communication plan - Define test scenarios - Define rollback triggers

Change Calendar: - Visualize all planned changes - Identify conflicts - Coordinate maintenance windows - Inform stakeholders

Responsible: Change Implementer, Change Manager

16.2.4.6 5. Change Implementation

Pre-Implementation: - Create backup - Provide rollback procedure - Conduct team briefing - Inform stakeholders

Implementation: - Execute implementation plan step-by-step - Document progress - If problems: Check rollback triggers

Post-Implementation: - Test functionality - Check monitoring - Inform stakeholders - Update documentation

Responsible: Change Implementer

16.2.4.7 6. Change Review

Review Activities: - Assess implementation success - Document deviations from plan - Identify lessons learned - Capture metrics (duration, downtime, etc.)

Review Criteria: - Change successfully implemented? - Rollback required? - Unexpected problems occurred? - Schedule maintained? - Documentation complete?

Responsible: Change Manager

16.2.4.8 7. Change Closure

Closure Activities: - Finalize documentation - Update CMDB - Close change ticket - Include metrics in reporting

Responsible: Change Manager

16.2.5 Maintenance Windows

Standard Maintenance Windows:

Type	Time Window	Frequency	Approval
Routine	Tuesday 22:00-02:00	Weekly	Standard Changes
Planned	Saturday 20:00-06:00	Monthly	Normal Changes
Emergency	Anytime	Ad-hoc	Emergency Changes

Maintenance Window Rules: - Minimal service interruption - User notification 48h in advance - Plan rollback time (50% of implementation time) - No changes during business-critical times

16.2.6 Rollback Procedures

Rollback Triggers: - Critical errors during implementation - Service availability < SLA - Unexpected impact on other services - Test validation failed - Change manager decision

Rollback Plan Requirements: - Step-by-step instructions - Estimated rollback duration - Required resources - Data recovery (if required) - Validation steps

Rollback Process: 1. Make rollback decision 2. Inform stakeholders 3. Execute rollback plan 4. Validate system status 5. Create incident ticket (if required) 6. Conduct post-rollback review

16.3 Release Management

16.3.1 Release Definition

A **release** is a collection of hardware, software, documentation, processes, or other components required to implement one or more approved changes.

16.3.2 Release Types

16.3.2.1 Major Release

Definition: Significant new functionality or architecture changes

Characteristics: - Large changes - Extensive testing required - Long planning phase - High risk - Extensive documentation

Examples: - New software version (e.g., v2.0.0) - Platform migration - Architecture redesign

Frequency: Quarterly or semi-annually

Approval: CAB + Management

16.3.2.2 Minor Release

Definition: New features or improvements without architecture changes

Characteristics: - Moderate changes - Standard testing - Medium risk - Backward compatible

Examples: - Feature releases (e.g., v1.1.0) - Performance improvements - New integrations

Frequency: Monthly

Approval: CAB

16.3.2.3 Patch Release

Definition: Bugfixes and security patches

Characteristics: - Small changes - Focus on stability - Low risk - Quick implementation

Examples: - Bugfix releases (e.g., v1.0.1) - Security patches - Hotfixes

Frequency: As needed (weekly)

Approval: Change Manager

16.3.3 Release Process

16.3.3.1 Process Overview

```
Release
Planning



Release
Build



Release
Testing



Release
Deployment



Release
Review
```

16.3.3.2 1. Release Planning

Planning Activities: - Define release scope - Select changes for release - Create release schedule - Plan resources - Conduct risk assessment - Create communication plan

Release Scope: - Included changes - New features - Bugfixes - Dependencies - Exclusions

Responsible: Release Manager

16.3.3.3 2. Release Build

Build Activities: - Code integration - Automated builds (CI/CD) - Artifact creation - Versioning - Build documentation

Build Pipeline: 1. Code commit 2. Automated tests (unit, integration) 3. Code quality checks (linting, security scan) 4. Create build artifact 5. Store artifact in repository

Responsible: DevOps Team

16.3.3.4 3. Release Testing

Test Phases:

Phase	Environment	Focus	Duration
Unit Tests	Dev	Code functionality	Automatic
Integration Tests	Dev	Component integration	Automatic
System Tests	Test	Overall system	1-2 days
UAT	Staging	Business requirements	3-5 days
Performance Tests	Staging	Load and performance	1-2 days
Security Tests	Staging	Security	1-2 days

Test Criteria: - All tests passed - No critical bugs - Performance goals achieved - Security scan without high findings - UAT acceptance by business

Responsible: QA Team, Business Users

16.3.3.5 4. Release Deployment

Deployment Strategies:

16.3.3.5.1 Blue-Green Deployment

Description: Two identical production environments (Blue and Green). New version is deployed to inactive environment, then traffic is switched.

Advantages: - Zero downtime - Quick rollback - Complete testing in prod environment

Disadvantages: - Double infrastructure costs - Database migrations complex

Application: Critical services with high availability requirements

16.3.3.5.2 Canary Deployment

Description: New version is gradually rolled out to a small percentage of users, then gradually increased.

Advantages: - Risk minimization - Early error detection - Gradual rollout

Disadvantages: - Complex traffic control - Longer deployment duration

Application: Services with large user base

16.3.3.5.3 Rolling Deployment Description: New version is gradually deployed to server instances while old version continues running.

Advantages: - No additional infrastructure - Gradual rollout - Automatable

Disadvantages: - Temporary version inconsistency - Complex rollbacks

Application: Standard deployments with load balancing

16.3.3.5.4 Big Bang Deployment Description: All components are updated simultaneously.

Advantages: - Simple - Fast - No version inconsistency

Disadvantages: - Downtime required - High risk - Complex rollbacks

Application: Only for non-critical services or with maintenance window

Deployment Checklist: - [ ] Backup created - [ ] Rollback plan ready - [ ] Monitoring activated - [ ] Stakeholders informed - [ ] Team available - [ ] Deployment runbook reviewed - [ ] Change ticket approved

Responsible: DevOps Team, Release Manager

16.3.3.6 5. Release Review

Review Activities: - Assess deployment success - Analyze metrics - Document lessons learned - Identify improvements

Review Metrics: - Deployment duration - Downtime (if any) - Number of rollbacks - Post-deployment incidents - User feedback

Responsible: Release Manager

16.3.4 CI/CD Pipeline

Continuous Integration (CI): - Automatic builds on code commit - Automated tests (unit, integration) - Code quality checks - Security scans - Artifact creation

Continuous Deployment (CD): - Automatic deployment to dev/test - Manual deployment to staging/prod - Automatic rollbacks on errors - Deployment monitoring

Pipeline Tools: - **CI/CD System:** {{ meta.cicd_system }} - **Version Control:** {{ meta.version_control }} - **Artifact Repository:** {{ meta.artifact_repository }} - **Container Registry:** {{ meta.container_registry }}

16.4 Metrics and Reporting

16.4.1 Change Management Metrics

Metric	Target Value	Measurement
Change Success Rate	$> 95\%$	Successful changes / Total changes

Metric	Target Value	Measurement
Emergency Change Rate	< 5%	Emergency changes / Total changes
Change-Related Incidents	< 10%	Incidents from changes / Total incidents
CAB Approval Rate	> 90%	Approved changes / Submitted changes
Rollback Rate	< 5%	Rollbacks / Implemented changes

16.4.2 Release Management Metrics

Metric	Target Value	Measurement
Release Frequency	Monthly	Number of releases per month
Lead Time	< 2 weeks	Time from commit to production
Deployment Frequency	Weekly	Number of deployments per week
Mean Time to Recovery	< 1 hour	Average recovery time
Change Failure Rate	< 15%	Failed deployments / Total

16.4.3 Reporting

Weekly Change Report: - Number of changes (by category) - Planned changes (next week) - Change calendar - Open change requests

Monthly Release Report: - Release overview - Deployment statistics - Metrics dashboard - Improvement measures

16.5 Roles and Responsibilities

16.5.1 Change Manager

Responsibilities: - Change process ownership - CAB moderation - Change assessment - Change calendar management - Reporting

Person: Andreas Huemmer

16.5.2 Release Manager

Responsibilities: - Release planning - Release coordination - Deployment oversight - Release documentation

Person: [Name]

16.5.3 Change Advisory Board (CAB)

Responsibilities: - Change assessment - Change approval - Risk assessment - Prioritization

Members: See section “Change Authorization”

16.6 Tools and Systems

16.6.1 Change Management Tool

- **System:** {{ meta.ticketing_system }}
- **URL:** {{ meta.ticketing_system_url }}
- **Access:** All IT staff

16.6.2 CI/CD Pipeline

- **System:** {{ meta.cicd_system }}
- **URL:** {{ meta.cicd_url }}
- **Access:** DevOps Team

16.6.3 Version Control

- **System:** {{ meta.version_control }}
- **URL:** {{ meta.version_control_url }}
- **Access:** Development Team

16.7 References

- ITIL v4 Foundation - Change Enablement
- ITIL v4 Foundation - Release Management
- ISO/IEC 20000-1:2018 - Change Management
- DevOps Handbook - Deployment Strategies
- Site Reliability Engineering (SRE) - Release Engineering

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Classification: internal
Last Updated: {{ meta.date }}

ewpage

Chapter 17

Backup and Restore

17.1 Purpose and Scope

This document describes the backup and restore strategies for AdminSend GmbH. It defines backup methods, schedules, retention periods, RPO/RTO objectives, and restore procedures to ensure data integrity and availability.

Scope: All IT systems, databases, applications, and data of AdminSend GmbH

Responsible: Andreas Huemmer (andreas.huemmer@adminsend.de)

17.2 Backup Fundamentals

17.2.1 Backup Objectives

Primary Objectives: - **Data Protection:** Protection against data loss - **Disaster Recovery:** Recovery after disasters - **Compliance:** Meeting regulatory requirements - **Business Continuity:** Minimizing downtime - **Ransomware Protection:** Recovery after cyber attacks

17.2.2 Recovery Objectives

17.2.2.1 Recovery Point Objective (RPO)

Definition: Maximum tolerable data loss (time period between last backup and failure)

RPO Categories:

Category	RPO	Backup Frequency	Application
Critical	< 1 hour	Continuous / Hourly	Transaction systems, databases
Important	< 4 hours	4x daily	Business applications
Standard	< 24 hours	Daily	File servers, email
Non-Critical	< 7 days	Weekly	Archive data, test systems

17.2.2.2 Recovery Time Objective (RTO)

Definition: Maximum tolerable downtime (time until restoration)

RTO Categories:

Category	RTO	Restore Method	Application
Critical	< 1 hour	Hot standby, snapshots	Production databases
Important	< 4 hours	Fast restore systems	Business applications
Standard	< 24 hours	Standard restore	File servers
Non-Critical	< 7 days	Archive restore	Test systems

17.2.3 Backup Strategies

17.2.3.1 Full Backup

Description: Complete backup of all data

Advantages: - Simple restoration - Only one backup set required - Fast restore time

Disadvantages: - Long backup duration - High storage requirements - High network load

Application: Weekly base backups

17.2.3.2 Incremental Backup

Description: Backup only of data changed since last backup (full or incremental)

Advantages: - Fast backup duration - Low storage requirements - Low network load

Disadvantages: - Complex restoration - All incremental backups required - Longer restore time

Application: Daily backups between full backups

17.2.3.3 Differential Backup

Description: Backup of all data changed since last full backup

Advantages: - Faster restoration than incremental - Only full + last differential required - Moderate backup duration

Disadvantages: - Growing backup size - Higher storage requirements than incremental

Application: Alternative to incremental for critical systems

17.2.3.4 Continuous Data Protection (CDP)

Description: Continuous backup of all changes in real-time

Advantages: - Minimal data loss (RPO < 1 min) - Point-in-time recovery - No backup windows required

Disadvantages: - High costs - Complex infrastructure - High performance requirements

Application: Critical databases and transaction systems

17.2.4 Backup Architecture

17.2.4.1 3-2-1 Backup Rule

Rule: 3 copies, 2 different media, 1 offsite copy

Implementation: - **3 Copies:** Production data + 2 backups - **2 Media:** Disk + tape or cloud - **1 Offsite:** Geographically separated copy

Example: 1. Production data on {{ netbox.storage.primary }} 2. Backup on {{ netbox.storage.backup_disk }} 3. Offsite backup in {{ meta.backup_cloud_provider }}

17.2.4.2 Backup Tiers

Tier	Storage Type	Restore Time	Cost	Application
Tier 1	SSD / NVMe	Minutes	High	Snapshots, CDP
Tier 2	HDD / NAS	Hours	Medium	Daily backups
Tier 3	Tape / Object Storage	Days	Low	Long-term archiving
Tier 4	Cloud Cold Storage	Weeks	Very low	Compliance archive

17.3 Backup Schedules

17.3.1 Production Systems

17.3.1.1 Databases (Critical)

System: {{ netbox.database.server }}

Backup Strategy: - **Full Backup:** Sunday 02:00 - **Differential Backup:** Daily 02:00 (Mon-Sat) - **Transaction Log Backup:** Hourly - **Snapshots:** Every 4 hours

RPO: < 1 hour
RTO: < 1 hour

Retention: - Daily backups: 30 days - Weekly backups: 12 weeks - Monthly backups: 12 months - Yearly backups: 7 years

17.3.1.2 Application Servers (Important)

System: {{ netbox.application.server }}

Backup Strategy: - **Full Backup:** Sunday 03:00 - **Incremental Backup:** Daily 03:00 (Mon-Sat) - **Snapshots:** Daily before deployments

RPO: < 24 hours
RTO: < 4 hours

Retention: - Daily backups: 14 days - Weekly backups: 8 weeks - Monthly backups: 6 months

17.3.1.3 File Servers (Standard)

System: {{ netbox.fileserver.server }}

Backup Strategy: - **Full Backup:** Sunday 01:00 - **Incremental Backup:** Daily 01:00 (Mon-Sat)

RPO: < 24 hours
RTO: < 24 hours

Retention: - Daily backups: 7 days - Weekly backups: 4 weeks - Monthly backups: 3 months

17.3.2 Backup Calendar

Day	01:00	02:00	03:00	Hourly
Sunday	File Server (Full)	Database (Full)	App Server (Full)	DB Logs
Monday	File Server (Inc)	Database (Diff)	App Server (Inc)	DB Logs
Tuesday	File Server (Inc)	Database (Diff)	App Server (Inc)	DB Logs
Wednesday	File Server (Inc)	Database (Diff)	App Server (Inc)	DB Logs
Thursday	File Server (Inc)	Database (Diff)	App Server (Inc)	DB Logs
Friday	File Server (Inc)	Database (Diff)	App Server (Inc)	DB Logs
Saturday	File Server (Inc)	Database (Diff)	App Server (Inc)	DB Logs

17.4 Backup Processes

17.4.1 Backup Process Overview

```
Backup
Scheduling



Pre-Backup
Checks



Backup
Execution



Backup
Verification



Backup
Reporting
```

```
Offsite
Replication
```

17.4.2 1. Backup Scheduling

Automation: - Backup jobs configured in {{ meta.backup_system }} - Time-controlled execution - Dependencies between jobs - Retry mechanisms on errors

Responsible: Backup Administrator

17.4.3 2. Pre-Backup Checks

Checks: - Sufficient storage space available - Backup target reachable - Source system available - No ongoing maintenance - Previous backup successful

On Errors: Alert to operations team

17.4.4 3. Backup Execution

Activities: - Create application-consistent snapshots - Compress data - Encrypt data (AES-256) - Transfer data to backup target - Store metadata

Monitoring: Real-time monitoring in {{ meta.monitoring_system }}

17.4.5 4. Backup Verification

Verification Methods: - **Checksum Validation:** MD5/SHA-256 checksums - **Catalog Check:** Backup catalog consistency - **Restore Test:** Sample restores (monthly) - **Integrity Scan:** Backup data integrity

On Errors: Repeat backup, escalate alert

17.4.6 5. Backup Reporting

Reports: - Backup status (success/failure) - Backup size and duration - Storage space utilization - Failed backups - Trend analyses

Recipients: andreas.huemmer@adminsend.de

17.4.7 6. Offsite Replication

Replication Methods: - **Cloud Sync:** Automatic replication to {{ meta.backup_cloud_provider }} - **Tape Rotation:** Weekly tape offsite storage - **Remote Site:** Replication to {{ netbox.site.dr_location }}

Encryption: TLS in transit, AES-256 at rest

17.5 Restore Processes

17.5.1 Restore Process Overview

```
Restore
Request



Restore
Planning



Restore
Preparation



Restore
Execution



Restore
Verification



Restore
Documentation
```

17.5.2 1. Restore Request

Restore Reasons: - Data loss (accidental deletion) - Data corruption - Ransomware attack - Hardware failure - Disaster recovery - Test/development

Required Information: - What should be restored? - Which point in time? (Point-in-time) - Where should it be restored? - Urgency (RTO) - Approval

Tool: {{ meta.ticketing_system }}

17.5.3 2. Restore Planning

Planning Activities: - Identify backup set - Select restore method - Prepare restore target - Plan downtime (if required) - Inform stakeholders

Restore Methods: - **File-Level Restore:** Individual files/folders - **Volume-Level Restore:** Complete volumes - **System-Level Restore:** Bare-metal recovery - **Database Restore:** Database

restoration - **VM Restore:** Virtual machines

17.5.4 3. Restore Preparation

Preparations: - Check backup integrity - Provide restore target - Ensure sufficient storage space - Check network connectivity - Mount backup media (if tape)

17.5.5 4. Restore Execution

Restore Steps:

17.5.5.1 File-Level Restore

1. Browse backup catalog
2. Select files/folders
3. Specify restore target
4. Start restore
5. Monitor progress

Estimated Duration: 10 GB/hour (from disk)

17.5.5.2 Database Restore

1. Stop database service
2. Restore full backup
3. Apply differential backup (if available)
4. Apply transaction logs (point-in-time)
5. Check database consistency
6. Start database service

Estimated Duration: 100 GB/hour

17.5.5.3 VM Restore

1. Power off VM (if running)
2. Select VM backup
3. Select restore target (datastore)
4. Restore VM
5. Check VM configuration
6. Start VM

Estimated Duration: 50 GB/hour

17.5.5.4 Bare-Metal Restore

1. Create boot media
2. Boot system from boot media
3. Connect backup source
4. Select system backup
5. Perform restore to hardware
6. Restart system

Estimated Duration: 20 GB/hour

17.5.6 5. Restore Verification

Verification Steps: - Check data completeness - Validate data integrity - Test application functionality - Perform performance check - Obtain user acceptance

Verification Checklist: - [ ] All requested data restored - [ ] Data integrity confirmed - [ ] Application functional - [ ] Performance acceptable - [ ] Users informed

17.5.7 6. Restore Documentation

Documentation: - Update restore ticket - Document restore duration - Record problems and solutions - Identify lessons learned - Capture metrics

17.6 Backup Technologies

17.6.1 Backup Software

Primary Backup System: - **System:** {{ meta.backup_system }} - **Version:** {{ meta.backup_system_version }} - **License:** {{ meta.backup_system_license }}

Features: - Application-consistent backups - Deduplication - Compression - Encryption - Cloud integration - Automatic verification

17.6.2 Snapshot Technology

Storage Snapshots: - **System:** {{ netbox.storage.system }} - **Snapshot Frequency:** Every 4 hours - **Retention:** 48 hours - **Usage:** Quick rollbacks, pre-change snapshots

VM Snapshots: - **System:** {{ netbox.hypervisor.system }} - **Snapshot Type:** Crash-consistent - **Usage:** Pre-deployment snapshots - **Warning:** Not a long-term backup solution

17.6.3 Cloud Backup

Cloud Provider: - **Provider:** {{ meta.backup_cloud_provider }} - **Region:** {{ meta.backup_cloud_region }} - **Storage Tier:** Standard / Glacier

Advantages: - Offsite backup automatic - Scalable - Geo-redundancy - Pay-per-use

Disadvantages: - Dependency on internet connection - Restore duration for large data volumes - Ongoing costs

17.7 Backup Security

17.7.1 Encryption

In Transit: - TLS 1.3 for network transmission - VPN for remote backups

At Rest: - AES-256 encryption - Separate key management - Key rotation every 90 days

Key Management: - Keys in {{ meta.key_management_system }} - Access only for authorized administrators - Backup of keys (escrow)

17.7.2 Immutable Backups

Concept: Backups cannot be modified or deleted (protection against ransomware)

Implementation: - Object lock in cloud storage - WORM tapes (Write Once Read Many) - Air-gapped backups

Retention: At least 30 days immutable

17.7.3 Access Control

Permissions: - Backup administrators: Full access - System administrators: Restore permission - Service desk: No backup permission

Audit Logging: - All backup/restore activities logged - Logs in SIEM system {{ meta.siem_system }} - Monthly audit reviews

17.8 Backup Testing

17.8.1 Test Strategy

Test Types: - **Verification Tests:** Automatic after each backup - **Restore Tests:** Monthly samples - **DR Tests:** Quarterly full restore tests - **Compliance Tests:** Annual audits

17.8.2 Restore Test Process

Monthly Restore Test: 1. Select random system 2. Restore to isolated test environment 3. Validate functionality 4. Measure restore duration 5. Document results

Test Criteria: - Restore successful - RTO maintained - Data complete - Application functional

On Errors: - Create incident ticket - Review backup strategy - Implement corrective measures - Perform re-test

17.8.3 DR Test

Quarterly DR Test: 1. Simulate disaster scenario 2. Restore complete system to DR site 3. Perform failover 4. Test business processes 5. Perform failback

Documentation: - Test plan - Test results - Identified problems - Improvement measures

17.9 Metrics and Reporting

17.9.1 Backup Metrics

Metric	Target Value	Measurement
Backup Success Rate	$> 98\%$	Successful backups / Total backups
Backup Window Compliance	$> 95\%$	Backups in time window / Total backups
Restore Success Rate	$> 99\%$	Successful restores / Total restores

Metric	Target Value	Measurement
RTO Compliance	> 95%	Restores within RTO / Total restores
RPO Compliance	> 99%	Data loss < RPO / Total incidents

17.9.2 Reporting

Daily Backup Report: - Backup status (success/failure) - Failed backups - Storage space utilization - Alerts and warnings

Monthly Backup Report: - Backup statistics - Restore activities - Metrics dashboard - Trend analyses - Capacity planning

Quarterly Management Report: - Backup strategy review - DR test results - Compliance status - Improvement measures - Budget planning

17.10 Roles and Responsibilities

17.10.1 Backup Administrator

Responsibilities: - Backup system management - Backup job configuration - Monitoring and alerting - Restore execution - Reporting

Person: [Name]

17.10.2 Storage Administrator

Responsibilities: - Backup storage management - Capacity planning - Performance optimization - Snapshot management

Person: [Name]

17.10.3 IT Operations Manager

Responsibilities: - Backup strategy ownership - Budget responsibility - Compliance assurance - Escalation management

Person: Andreas Huemmer

17.11 Compliance and Regulation

17.11.1 Regulatory Requirements

GDPR: - Data encryption - Access control - Audit logging - Data deletion after retention period

ISO 27001: - Backup policy documented - Regular backup tests - Incident response plan - Continuous improvement

Industry-Specific: - [Additional regulatory requirements]

17.11.2 Retention Periods

Data Type	Retention Period	Justification
Financial Data	10 years	Tax law
Personnel Data	7 years	Labor law
Contract Data	6 years	Contract law
Emails	6 years	Compliance
System Logs	1 year	Security
Backup Logs	3 years	Audit

17.12 References

- ITIL v4 - Service Continuity Management
- ISO/IEC 27001:2013 - Backup Controls
- GDPR - Article 32 (Data Security)
- 3-2-1 Backup Rule
- Backup System Documentation: {{ meta.backup_system_docs }}

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Classification: internal
Last Updated: {{ meta.date }}

ewpage

Chapter 18

Disaster Recovery and Business Continuity

18.1 Purpose and Scope

This document describes the disaster recovery and business continuity strategies for AdminSend GmbH. It defines disaster scenarios, impact analyses, DR strategies, failover/failback procedures, and business continuity plans to ensure business continuity during disasters.

Scope: All critical IT services and business processes of AdminSend GmbH

Responsible: Anna Schmidt (anna.schmidt@adminsend.de)

18.2 Fundamentals

18.2.1 Definitions

Disaster: An event that leads to a significant failure of IT services or business processes and exceeds normal recovery measures.

Disaster Recovery (DR): Processes and technologies for restoring IT systems and services after a disaster.

Business Continuity (BC): An organization's ability to maintain critical business processes during and after a disruption.

18.2.2 Distinction: DR vs. BC

Aspect	Disaster Recovery	Business Continuity
Focus	IT systems and infrastructure	Business processes
Scope	Technical recovery	Entire organization
Goal	System availability	Business continuity
Responsibility	IT department	Management + all departments
Timeframe	Hours to days	Immediate to weeks

18.2.3 Recovery Objectives

18.2.3.1 Recovery Time Objective (RTO)

Definition: Maximum tolerable downtime of a service

RTO Categories for DR:

Service Tier	RTO	DR Strategy	Examples
Tier 0 - Critical	< 1 hour	Hot standby	Transaction systems, e-commerce
Tier 1 - Important	< 4 hours	Warm standby	ERP, CRM, email
Tier 2 - Standard	< 24 hours	Cold standby	File servers, intranet
Tier 3 - Non-Critical	< 7 days	Backup restore	Test systems, archives

18.2.3.2 Recovery Point Objective (RPO)

Definition: Maximum tolerable data loss

RPO Categories for DR:

Service Tier	RPO	Replication Method
Tier 0 - Critical	< 15 minutes	Synchronous replication
Tier 1 - Important	< 1 hour	Asynchronous replication
Tier 2 - Standard	< 24 hours	Daily backups
Tier 3 - Non-Critical	< 7 days	Weekly backups

18.3 Disaster Scenarios

18.3.1 Scenario Categories

18.3.1.1 Natural Disasters

Scenarios: - Fire in data center - Flooding - Earthquake - Storm/severe weather - Power outage (regional)

Probability: Low
Impact: Very high
Affected Sites: {{ netbox.site.primary }}, {{ netbox.site.secondary }}

Mitigations: - Geographically separated DR site - Redundant power supply (UPS, generator) - Building security measures - Insurance

18.3.1.2 Technical Failures

Scenarios: - Complete data center failure - Network failure (WAN) - Storage system failure - Hypervisor cluster failure - Cloud provider failure

Probability: Medium
Impact: High

Mitigations: - Redundant systems - Multi-cloud strategy - Automatic failover mechanisms - Regular maintenance

18.3.1.3 Cyber Attacks

Scenarios: - Ransomware attack - DDoS attack - Data breach - Insider threat - Supply chain attack

Probability: High
Impact: Very high

Mitigations: - Security monitoring (SIEM) - Immutable backups - Network segmentation - Incident response plan - Security awareness training

18.3.1.4 Human Errors

Scenarios: - Accidental deletion of critical data - Misconfiguration with service outage - Untested changes in production - Faulty deployment

Probability: Medium
Impact: Medium to high

Mitigations: - Change management processes - Four-eyes principle - Automated deployments - Rollback mechanisms - Regular backups

18.3.2 Business Impact Analysis (BIA)

18.3.2.1 Critical Business Processes

Business Process	Dependent IT Services	RTO	RPO	Financial Impact/Hour
Order Processing	ERP, database, e-commerce	1h	15 min	€50,000
Customer Support	CRM, ticketing, telephony	2h	1h	€10,000
Email Communication	Email server, Exchange	4h	1h	€5,000
Financial Accounting	ERP, database	8h	4h	€2,000
HR Management	HR system	24h	24h	€500

18.3.2.2 Impact Assessment

Financial Impact: - Direct costs (revenue loss) - Indirect costs (productivity loss) - Recovery costs - Penalties (SLA violations)

Non-Financial Impact: - Reputation damage - Customer loss - Legal consequences - Employee morale

Impact Matrix:

	< 1h	1-4h	4-24h	> 24h
Critical	Catastrophic	Very high	High	Medium
Important	Very high	High	Medium	Low
Standard	High	Medium	Low	Minimal
Non-Critical	Medium	Low	Minimal	Minimal

18.4 DR Strategies

18.4.1 Hot Standby (Active-Active)

Description: - Parallel production environments at two sites - Synchronous data replication - Load balancing between sites - Automatic failover

Advantages: - RTO: < 1 hour (often minutes) - RPO: < 15 minutes - No downtime during failover - Continuous availability

Disadvantages: - Very high costs (double infrastructure) - Complex configuration - High network requirements

Application: Tier 0 services ({{ netbox.service.critical }})

Cost: ~200% of production infrastructure

18.4.2 Warm Standby (Active-Passive)

Description: - DR site with reduced resources - Asynchronous data replication - Systems running but not productive - Manual or automatic failover

Advantages: - RTO: < 4 hours - RPO: < 1 hour - Moderate costs - Quick activation

Disadvantages: - Brief downtime during failover - Reduced initial performance - Regular testing required

Application: Tier 1 services ({{ netbox.service.important }})

Cost: ~50-70% of production infrastructure

18.4.3 Cold Standby (Backup-based)

Description: - DR site with minimal infrastructure - Backup-based recovery - Systems built on demand - Manual activation

Advantages: - RTO: < 24 hours - RPO: < 24 hours - Low costs - Simple management

Disadvantages: - Longer downtime - Manual processes - Higher risk

Application: Tier 2 services ({{ netbox.service.standard }})

Cost: ~20-30% of production infrastructure

18.4.4 Backup & Restore

Description: - No dedicated DR site - Recovery from backups - Procure new hardware as needed - Completely manual process

Advantages: - Minimal costs - Simple management

Disadvantages: - RTO: > 7 days - RPO: > 7 days - Very high risk - Long recovery time

Application: Tier 3 services (non-critical)

Cost: Backup costs only

18.5 DR Infrastructure

18.5.1 Primary Site

Site: {{ netbox.site.primary }}
Address: {{ netbox.site.primary_address }}
Data Center: {{ netbox.site.primary_datacenter }}

Infrastructure: - Production servers: {{ netbox.device.count_primary }} - Storage capacity: {{ netbox.storage.capacity_primary }} - Network bandwidth: {{ netbox.network.bandwidth_primary }} - Power supply: Redundant (N+1)

18.5.2 DR Site

Site: {{ netbox.site.dr }}
Address: {{ netbox.site.dr_address }}
Data Center: {{ netbox.site.dr_datacenter }}
Distance: {{ netbox.site.distance }} km

Infrastructure: - DR servers: {{ netbox.device.count_dr }} - Storage capacity: {{ netbox.storage.capacity_dr }} - Network bandwidth: {{ netbox.network.bandwidth_dr }} - Power supply: Redundant (N+1)

18.5.3 Replication Connection

Connection Type: {{ netbox.network.replication_type }}
Bandwidth: {{ netbox.network.replication_bandwidth }}
Latency: {{ netbox.network.replication_latency }} ms
Redundancy: Dual-path

Replication Technologies: - Storage replication: {{ meta.storage_replication_tech }} - Database replication: {{ meta.database_replication_tech }} - VM replication: {{ meta.vm_replication_tech }}

18.6 Failover Procedures

18.6.1 Failover Triggers

Automatic Failover Triggers: - Primary site unreachable (> 5 min) - Critical system failures (> 3 systems) - Storage system failure - Network failure (WAN)

Manual Failover Triggers: - Natural disaster at primary site - Planned maintenance (site switch) - DR test - Management decision

18.6.2 Failover Process

18.6.2.1 Process Overview

```
Disaster
Declaration



DR Team
Activation



Impact
Assessment



Failover
Execution



Service
Validation



Communication
& Monitoring
```

18.6.2.2 1. Disaster Declaration

Responsible: CIO or IT Operations Manager

Criteria: - Primary site unavailable - RTO at risk for critical services - No quick recovery possible

Activities: - Officially declare disaster - Activate DR team - Inform management - Activate communication plan

18.6.2.3 2. DR Team Activation

DR Team Members: - **DR Coordinator:** Anna Schmidt - **Technical Lead:** Andreas Huemmer - **Network Lead:** [Name] - **Storage Lead:** [Name] - **Application Lead:** [Name] - **Communication Lead:** [Name]

Activities: - Contact team members - Establish war room (physical or virtual) - Activate communication channels - Provide checklists

18.6.2.4 3. Impact Assessment

Assessment Activities: - Assess extent of disaster - Identify affected systems - Check DR site availability - Check replication status - Determine estimated RTO/RPO

Decision: - Complete failover to DR site - Partial failover (critical services only) - Alternative measures

18.6.2.5 4. Failover Execution

Failover Steps (Hot Standby):

1. **Prepare DNS switchover**
   - Reduce DNS TTL to 60 seconds (if not already)
   - Prepare DNS entries for DR site
2. **Reconfigure load balancer**
   - Redirect traffic from primary to DR
   - Switch health checks to DR systems
3. **Database failover**
   - Stop replication
   - Promote DR database to primary
   - Switch application connections
4. **Application activation**
   - Start application services on DR site
   - Validate configurations
   - Check database connections
5. **Perform DNS switchover**
   - Switch DNS entries to DR site
   - Monitor DNS propagation
6. **Adjust network routing**
   - Redirect VPN connections to DR site
   - Adjust firewall rules
   - Switch monitoring to DR site

Estimated Duration: 30-60 minutes (hot standby)

Failover Steps (Warm Standby):

1. **Boot DR systems**
   - Start servers
   - Activate storage systems
   - Check network components
2. **Finalize data synchronization**
   - Perform final replication
   - Check data consistency
   - Restore backups (if required)
3. **Database recovery**
   - Start database services
   - Perform consistency checks
   - Performance tuning
4. **Application deployment**

- Deploy applications
- Adjust configurations
- Test integrations

5. **Network and DNS**
   - See hot standby steps 5-6

Estimated Duration: 2-4 hours (warm standby)

18.6.2.6 5. Service Validation

Validation Steps: - [ ] All critical services reachable - [ ] Database connections working - [ ] Application functionality tested - [ ] Performance acceptable - [ ] Monitoring active - [ ] Backup jobs running

Test Scenarios: - Login test - Transaction test - Integration test - Performance test

18.6.2.7 6. Communication & Monitoring

Communication: - Inform stakeholders about failover - Status updates (every 30 min) - User communication - Management briefing

Monitoring: - Continuous monitoring of DR site - Performance metrics - Error logs - User feedback

18.7 Failback Procedures

18.7.1 Failback Planning

Failback Triggers: - Primary site restored - All systems tested and validated - Planned maintenance window available - Management approval

Failback Strategy: - **Planned failback:** During maintenance window - **Gradual failback:** Service by service - **Complete failback:** All services simultaneously

18.7.2 Failback Process

18.7.2.1 1. Prepare Primary Site

Activities: - Repair infrastructure damage - Rebuild systems (if required) - Restore network connectivity - Set up replication from DR to primary

Validation: - All systems functional - Replication running - Performance acceptable

18.7.2.2 2. Data Synchronization

Activities: - Reverse replication (DR → Primary) - Ensure data consistency - Perform delta synchronization

Duration: Depends on data volume (hours to days)

18.7.2.3 3. Failback Execution

Steps: 1. Announce maintenance window 2. Finalize replication 3. Start applications on primary 4. Switch DNS and load balancer 5. Put DR site in standby mode

Estimated Duration: 2-4 hours

18.7.2.4 4. Post-Failback Validation

Validation: - All services running on primary - Replication primary → DR restored - Monitoring active - Backup jobs running

18.8 Business Continuity Management

18.8.1 BC Strategy

Objectives: - Maintain critical business processes - Ensure employee safety - Ensure communication - Protect reputation

18.8.2 BC Plans

18.8.2.1 Emergency Communication

Communication Channels: - **Primary:** Email (info@adminsend.de) - **Secondary:** Phone (+49 89 12345678) - **Emergency:** Mobile apps, SMS

Contact Lists: - Management team - All employees - Customers - Partners and suppliers - Authorities

18.8.2.2 Alternative Workplaces

Home Office: - VPN access for all employees - Laptops and mobile devices - Cloud-based collaboration tools

Backup Office: - Location: [Address] - Capacity: [Number of workstations] - Equipment: IT, telephony, internet

18.8.2.3 Critical Suppliers

Supplier	Service	Contact	Backup Supplier
{{ meta.isp_provider }}	Internet	{{ meta.isp_contact }}	{{ meta.isp_backup }}
{{ meta.cloud_provider }}	Cloud services	{{ meta.cloud_contact }}	{{ meta.cloud_backup }}
{{ meta.hardware_vendor }}	Hardware	{{ meta.hardware_contact }}	-

18.9 DR Testing

18.9.1 Test Strategy

Test Types: - **Tabletop Exercise:** Theoretical walkthrough (quarterly) - **Partial Failover Test:** Individual services (semi-annually) - **Full Failover Test:** Complete failover (annually)

18.9.2 Test Process

18.9.2.1 Tabletop Exercise

Duration: 2-3 hours

Participants: - DR team - Management - Service owners

Procedure: 1. Present disaster scenario 2. Review roles and responsibilities 3. Walk through process steps 4. Identify problems 5. Document improvements

18.9.2.2 Full Failover Test

Duration: 1 day

Preparation: - Create test plan - Inform stakeholders - Plan maintenance window - Provide rollback plan

Execution: 1. Failover to DR site 2. Validate services 3. Test business processes 4. Measure performance 5. Failback to primary

Follow-up: - Create test report - Document lessons learned - Implement improvements - Plan next test

18.10 Metrics and Reporting

18.10.1 DR Metrics

Metric	Target Value	Measurement
RTO Achievement	> 95%	Actual RTO / Target RTO
RPO Achievement	> 99%	Actual RPO / Target RPO
DR Test Success Rate	100%	Successful tests / Total tests
Failover Time	< Target RTO	Average failover duration
Data Loss	< Target RPO	Average data loss

18.10.2 Reporting

Quarterly DR Report: - DR test results - RTO/RPO compliance - Infrastructure status - Improvement measures

Annual BC Report: - BC strategy review - BIA update - DR cost analysis - Management presentation

18.11 Roles and Responsibilities

18.11.1 DR Coordinator

Responsibilities: - DR strategy ownership - DR plan management - Coordinate DR tests - Disaster declaration

Person: Anna Schmidt

18.11.2 BC Manager

Responsibilities: - BC strategy development - Conduct BIA - Create BC plans - BC training

Person: Peter Fischer

18.11.3 DR Team

Members: See section “DR Team Activation”

18.12 References

- ITIL v4 - Service Continuity Management
- ISO 22301:2019 - Business Continuity Management
- ISO/IEC 27031:2011 - ICT Readiness for Business Continuity
- NIST SP 800-34 - Contingency Planning Guide
- Business Impact Analysis (BIA) Document

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Classification: internal
Last Updated: {{ meta.date }}

ewpage

Chapter 19

Security Operations and Hardening

19.1 Purpose and Scope

This document describes the security operations processes and hardening guidelines for AdminSend GmbH. It defines security monitoring, incident response processes, vulnerability management, and compliance requirements to ensure information security.

Scope: All IT systems, networks, applications, and data of AdminSend GmbH

Responsible: Thomas Weber (thomas.weber@adminsend.de)

19.2 Security Fundamentals

19.2.1 Security Objectives (CIA Triad)

Confidentiality: - Protection against unauthorized access - Encryption of sensitive data - Access control and authentication - Data Loss Prevention (DLP)

Integrity: - Protection against unauthorized modification - Digital signatures - Checksums and hashing - Change management processes

Availability: - Protection against denial of service - Redundancy and high availability - Backup and disaster recovery - Capacity management

19.2.2 Defense-in-Depth Strategy

Security Layers:

Perimeter Security	Firewall, IDS/IPS, DDoS protection
Network Security	Segmentation, VLANs, NAC
Host Security	Hardening, antivirus, EDR
Application Security	WAF, input validation, SAST/DAST

Data Security	Encryption, DLP, backup
Identity & Access Management	MFA, RBAC, PAM

19.2.3 Security Frameworks

ISO 27001:2013: - Information Security Management System (ISMS) - 114 controls in 14 categories - Risk-based approach - Continuous improvement

BSI Grundschutz: - IT-Grundschutz Compendium - Building blocks for IT systems - Standard security measures - Basic and core protection

NIST Cybersecurity Framework: - Identify, Protect, Detect, Respond, Recover - Risk management approach - Cross-industry applicable

CIS Controls: - 18 critical security controls - Prioritized implementation - Measurable implementation

19.3 Hardening Guidelines

19.3.1 Operating System Hardening

19.3.1.1 Linux Server Hardening

Basic Hardening: - Minimal installation (only required packages) - Regular updates and patches - Disable unused services - Firewall configuration (iptables/nftables) - Enable SELinux or AppArmor

Users and Authentication: - Disable root login via SSH - SSH key-based authentication - Sudo instead of direct root access - Password policies (complexity, expiration) - Account lockout after failed attempts

Network Hardening: - Disable unnecessary network services - Configure TCP wrappers - Restrictive iptables rules - Disable IPv6 (if not required)

Logging and Monitoring: - Syslog server configuration - Enable audit daemon (auditd) - Configure log rotation - Central log collection

Reference: CIS Benchmark for Linux

19.3.1.2 Windows Server Hardening

Basic Hardening: - Automatic Windows updates - Disable unnecessary features - Enable Windows Firewall - Enable Windows Defender - BitLocker for disk encryption

Users and Authentication: - Rename local administrator accounts - Password policies via GPO - Account lockout policies - Privileged Access Management (PAM) - LAPS for local admin passwords

Network Hardening: - Disable SMBv1 - Disable LLMNR and NetBIOS - Restrictive Windows Firewall rules - IPSec for server communication

Logging and Monitoring: - Configure Advanced Audit Policy - Enable PowerShell logging - Event log forwarding - Install Sysmon

Reference: CIS Benchmark for Windows Server, Microsoft Security Baseline

19.3.2 Network Hardening

19.3.2.1 Firewall Configuration

Principles: - Default deny (deny all, allow only required) - Least privilege (minimal permissions) - Segmentation (network zones)

Firewall Rules:

Source	Destination	Port	Protocol	Action	Justification
Internet	DMZ	443	TCP	Allow	HTTPS traffic
DMZ	Internal	3306	TCP	Allow	Database access
Internal	Internet	80,443	TCP	Allow	Web access
Any	Any	Any	Any	Deny	Default rule

Firewall System: {{ netbox.firewall.system }}
Management: {{ netbox.firewall.management_url }}

19.3.2.2 Network Segmentation

Network Zones:

Zone	VLAN	Subnet	Purpose	Security Level
DMZ	{{ netbox.vlan.dmz }}	{{ netbox.subnet.dmz }}	Public services	High
Production	{{ netbox.vlan.production }}	{{ netbox.subnet.production }}	Production systems	Very high
Management	{{ netbox.vlan.management }}	{{ netbox.subnet.management }}	Admin access	Critical
User	{{ netbox.vlan.user }}	{{ netbox.subnet.user }}	User network	Medium
Guest	{{ netbox.vlan.guest }}	{{ netbox.subnet.guest }}	Guest WLAN	Low

Segmentation Rules: - No direct communication between zones - Traffic via firewall/router - Micro-segmentation for critical systems - Zero-trust principle

19.3.2.3 VPN Hardening

VPN Type: {{ meta.vpn_type }}
Encryption: AES-256
Authentication: Certificate-based + MFA

Hardening Measures: - Strong encryption algorithms - Perfect Forward Secrecy (PFS) - Certificate-based authentication - Multi-Factor Authentication (MFA) - Disable split tunneling - Inactivity timeout (15 min)

19.3.3 Application Hardening

19.3.3.1 Web Applications

OWASP Top 10 Mitigations:

Risk	Mitigation
Injection	Prepared statements, input validation
Broken Authentication	MFA, session management, password policies
Sensitive Data Exposure	Encryption at rest/transit, HTTPS
XML External Entities	Disable XML external entity processing
Broken Access Control	RBAC, least privilege
Security Misconfiguration	Hardening, security headers
XSS	Input validation, output encoding, CSP
Insecure Deserialization	Input validation, integrity checks
Using Components with Known Vulnerabilities	Dependency scanning, updates
Insufficient Logging	Security logging, monitoring

Security Headers:

```
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer
```

19.3.3.2 Database Hardening

MySQL/MariaDB: - Change root password - Remove anonymous users - Delete test database - Disable remote root login - Least privilege for application users - SSL/TLS for connections - Enable audit plugin

PostgreSQL: - Configure pg_hba.conf restrictively - Enforce SSL connections - Password encryption (SCRAM-SHA-256) - Enable audit logging - Least privilege permissions

Reference: CIS Benchmark for databases

19.3.4 Cloud Hardening

19.3.4.1 AWS Hardening

IAM Best Practices: - Don't use root account - MFA for all users - Least privilege policies - Roles instead of users for services - Rotate access keys

Network Security: - Restrictive security groups - NACLs for additional control - Enable VPC Flow Logs - Private subnets for backend - VPN/Direct Connect for hybrid

Monitoring: - Enable CloudTrail - Enable GuardDuty - Config rules for compliance - CloudWatch alarms

Reference: CIS AWS Foundations Benchmark

19.3.4.2 Azure Hardening

Identity Management: - Azure AD with MFA - Conditional Access Policies - Privileged Identity Management (PIM) - Identity Protection

Network Security: - Network Security Groups (NSG) - Azure Firewall - DDoS Protection Standard - Private Endpoints

Monitoring: - Azure Security Center - Azure Sentinel - Activity Logs - Diagnostic Settings

Reference: CIS Microsoft Azure Foundations Benchmark

19.4 Security Monitoring

19.4.1 Security Information and Event Management (SIEM)

SIEM System: {{ meta.siem_system }}
Version: {{ meta.siem_version }}
Management: {{ meta.siem_url }}

Log Sources: - Firewalls and IDS/IPS - Servers (Windows, Linux) - Network devices (switches, routers) - Applications - Cloud services (AWS, Azure) - Endpoint security (EDR) - Identity management (AD, Azure AD)

Use Cases:

Use Case	Description	Priority
Failed Login Attempts	Multiple failed logins	High
Privilege Escalation	Unexpected admin rights	Critical
Malware Detection	Antivirus/EDR alerts	Critical
Data Exfiltration	Unusual data transfers	High
Lateral Movement	Unusual network connections	High
Account Anomalies	Unusual account activities	Medium
Configuration Changes	Changes to critical systems	Medium

19.4.2 Intrusion Detection/Prevention (IDS/IPS)

IDS/IPS System: {{ netbox.ids.system }}
Deployment: Inline (IPS mode)
Location: {{ netbox.ids.location }}

Detection Methods: - **Signature-based:** Known attack patterns - **Anomaly-based:** Deviations from normal behavior - **Heuristic-based:** Suspicious behavior

Rule Sets: - Emerging Threats - Snort Community Rules - Custom rules for specific environment

Tuning: - False positive reduction - Rule prioritization - Whitelist for legitimate traffic

19.4.3 Endpoint Detection and Response (EDR)

EDR System: {{ meta.edr_system }}
Coverage: All workstations and servers

Features: - Real-time threat detection - Behavioral analysis - Automated response - Forensic capabilities - Threat hunting

Response Actions: - Generate alert - Terminate process - Block network connection - Isolate host - Collect forensic data

19.4.4 Security Metrics

Metric	Target Value	Measurement
Mean Time to Detect (MTTD)	$<$ 1 hour	Average detection time
Mean Time to Respond (MTTR)	$<$ 4 hours	Average response time
False Positive Rate	$<$ 5%	False positives / Total alerts
Security Incidents	Decreasing trend	Number of incidents per month
Patch Compliance	$>$ 95%	Patched systems / Total systems

19.5 Vulnerability Management

19.5.1 Vulnerability Scanning

Scanning Tools: - **Network Scanner:** {{ meta.vulnerability_scanner }} - **Web App Scanner:** {{ meta.web_scanner }} - **Container Scanner:** {{ meta.container_scanner }}

Scan Frequency: - **Critical Systems:** Weekly - **Production Systems:** Monthly - **Development Systems:** Quarterly - **Ad-hoc:** After new vulnerabilities (zero-days)

Scan Types: - **Authenticated Scans:** With credentials (more detailed) - **Unauthenticated Scans:** Without credentials (attacker perspective) - **Internal Scans:** From internal network - **External Scans:** From internet

19.5.2 Vulnerability Assessment

CVSS Score (Common Vulnerability Scoring System):

CVSS Score	Severity	SLA for Remediation
9.0 - 10.0	Critical	7 days
7.0 - 8.9	High	30 days
4.0 - 6.9	Medium	90 days

CVSS Score	Severity	SLA for Remediation
0.1 - 3.9	Low	180 days

Prioritization Factors: - CVSS score - Exploit availability - Asset criticality - Exposure (internet-facing) - Data sensitivity

19.5.3 Remediation Process

```
Vulnerability
Identified



Risk
Assessment



Remediation
Planning



Patch/Fix
Implementation



Verification
& Closure
```

Remediation Options: - **Patching:** Install software updates - **Configuration Change:** Secure configuration - **Workaround:** Temporary mitigation - **Compensating Control:** Alternative security measure - **Accept Risk:** Accept risk (with management approval)

19.5.4 Penetration Testing

Test Frequency: Annually + after major changes

Test Types: - **Black-Box:** No prior knowledge - **Gray-Box:** Partial information - **White-Box:** Complete information

Test Scope: - External infrastructure (internet-facing) - Internal network segments - Web applications - Mobile apps - Social engineering

Penetration Test Provider: {{ meta.pentest_provider }}

19.6 Security Incident Response

19.6.1 Incident Categories

Category	Examples	Severity
Malware	Virus, ransomware, trojan	High - Critical
Unauthorized Access	Compromised accounts, brute force	High
Data Breach	Data exfiltration, data leak	Critical
DDoS	Denial-of-service attacks	High
Phishing	Phishing emails, social engineering	Medium - High
Insider Threat	Malicious insider activities	High - Critical
Policy Violation	Security policy violations	Low - Medium

19.6.2 Incident Response Process

19.6.2.1 1. Preparation

Preparation Activities: - Define incident response team - Create incident response plan - Provide tools and resources - Conduct training and exercises - Maintain contact lists

IR Team: - **IR Manager:** Thomas Weber - **Technical Lead:** Andreas Huemmer - **Forensic Analyst:** [Name] - **Communication Lead:** [Name] - **Legal Counsel:** [Name]

19.6.2.2 2. Detection & Analysis

Detection Sources: - SIEM alerts - IDS/IPS alerts - EDR alerts - User reports - Threat intelligence

Analysis Activities: - Alert validation (true/false positive) - Scope determination (affected systems) - Impact assessment - Incident classification - Incident prioritization

Incident Ticket: {{ meta.ticketing_system }}

19.6.2.3 3. Containment

Short-term Containment: - Isolate affected systems - Block network connections - Disable compromised accounts - Stop malware spread

Long-term Containment: - Implement temporary fixes - Move systems to isolated environment - Increase monitoring

19.6.2.4 4. Eradication

Eradication Activities: - Remove malware - Close backdoors - Delete compromised accounts - Patch vulnerabilities - Rebuild systems (if required)

19.6.2.5 5. Recovery

Recovery Activities: - Restore systems from clean backups - Reset passwords - Harden systems - Enable monitoring - Gradually return to production

Validation: - No malware traces - No backdoors - Normal functionality - Acceptable performance

19.6.2.6 6. Post-Incident Activity

Lessons Learned Meeting: - What happened? - How was it detected? - What went well? - What went wrong? - Improvement measures

Documentation: - Create incident report - Document timeline - Collect IOCs (Indicators of Compromise) - Record costs

Follow-up: - Implement improvement measures - Update policies - Conduct training - Share threat intelligence

19.6.3 Incident Response Playbooks

Ransomware Playbook: 1. Immediately isolate affected systems 2. No ransom payment (policy) 3. Conduct forensic analysis 4. Inform law enforcement 5. Restore from backups 6. Patch vulnerabilities

Data Breach Playbook: 1. Determine scope (which data, how many affected) 2. Stop exfiltration 3. Forensic analysis 4. Involve legal team 5. Check reporting obligations (GDPR: 72h) 6. Inform affected parties 7. Report to supervisory authority

Phishing Playbook: 1. Identify phishing email 2. Update email filter 3. Identify affected users 4. Reset passwords (if credentials entered) 5. Conduct awareness training

19.7 Compliance and Regulation

19.7.1 ISO 27001:2013

Implementation Status:

Annex A Control	Title	Status	Responsible
A.9	Access Control	Implemented	Thomas Weber
A.10	Cryptography	Implemented	IT Security
A.12	Operations Security	Implemented	IT Operations
A.13	Communications Security	Implemented	Network Team
A.14	System Acquisition	Partial	IT Management
A.16	Incident Management	Implemented	IR Team
A.17	Business Continuity	Implemented	BC Manager
A.18	Compliance	Implemented	Compliance Officer

Audit Frequency: Annually (external), Quarterly (internal)

Next Audit: {{ meta.next_iso_audit }}

19.7.2 BSI Grundschutz

Basic Protection: - All basic protection building blocks implemented - Standard security measures implemented - Documentation complete

Core Protection: - Critical building blocks identified - Enhanced security measures implemented - Regular reviews

Certification: [Planned/In Progress/Certified]

19.7.3 GDPR

Technical and Organizational Measures (TOMs):

Measure	Implementation
Encryption	AES-256 at rest, TLS 1.3 in transit
Pseudonymization	Implemented where possible
Access Control	RBAC, MFA, PAM
Logging	Central log collection, SIEM
Backup	3-2-1 rule, encrypted
Incident Response	IR plan, 72h reporting obligation

Data Protection Impact Assessment (DPIA): - Conducted for high-risk processing - Documented and approved

Data Protection Officer: {{ meta.data_protection_officer }}

19.7.4 Other Standards

PCI-DSS: [If applicable]
HIPAA: [If applicable]
SOX: [If applicable]

19.8 Security Awareness and Training

19.8.1 Awareness Program

Target Audience: All employees

Training Topics: - Password security - Phishing recognition - Social engineering - Secure use of IT systems - Data classification - Incident reporting - GDPR basics

Training Frequency: - Onboarding: Immediate - Refresher: Annually - Phishing simulations: Quarterly

Phishing Simulations: - Quarterly campaigns - Various phishing types - Immediate feedback - Additional training on click

19.8.2 Security Champions

Concept: Security contact persons in each department

Tasks: - Promote security awareness - Answer security questions - Report security incidents - Spread best practices

Training: Extended security training

19.9 Roles and Responsibilities

19.9.1 Chief Information Security Officer (CISO)

Responsibilities: - Security strategy ownership - Risk management - Compliance assurance - Incident response coordination - Security budget

Person: Thomas Weber

19.9.2 Security Operations Team

Responsibilities: - SIEM monitoring - Incident response - Vulnerability management - Security tool management

Team Size: [Number]

19.9.3 IT Operations Team

Responsibilities: - System hardening - Patch management - Security configuration - Backup security

Lead: Andreas Huemmer

19.10 Metrics and Reporting

19.10.1 Security Metrics

Metric	Target Value	Frequency
Security Incidents	Decreasing trend	Monthly
MTTD	$<$ 1 hour	Monthly
MTTR	$<$ 4 hours	Monthly
Patch Compliance	$>$ 95%	Weekly
Vulnerability Remediation	$>$ 90% in SLA	Monthly
Phishing Click Rate	$<$ 5%	Quarterly
Security Training Completion	100%	Annually

19.10.2 Reporting

Weekly Security Dashboard: - New security incidents - Open vulnerabilities - Patch status - SIEM alert statistics

Monthly Security Report: - Security metrics - Incident summary - Vulnerability trends - Compliance status

Quarterly Management Report: - Security posture assessment - Risk assessment - Compliance status - Budget and resources - Strategic recommendations

19.11 References

- ISO/IEC 27001:2013 - Information Security Management

- BSI IT-Grundschutz Compendium
- NIST Cybersecurity Framework
- CIS Controls v8
- OWASP Top 10
- SANS Top 25 Software Errors
- MITRE ATT&CK Framework
- GDPR

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Classification: internal
Last Updated: {{ meta.date }}

ewpage

Chapter 20

Patch and Update Management

20.1 Purpose and Scope

This document describes the patch and update management processes for AdminSend GmbH. It defines patch categories, schedules, test and rollout processes, as well as vulnerability scanning and prioritization to ensure system security and stability.

Scope: All IT systems, operating systems, applications, and firmware of AdminSend GmbH

Responsible: Andreas Huemmer (andreas.huemmer@adminsend.de)

20.2 Patch Management Fundamentals

20.2.1 Objectives

Primary Objectives: - **Security:** Closing security vulnerabilities - **Stability:** Fixing bugs and errors - **Compliance:** Meeting regulatory requirements - **Performance:** Optimization and new features - **Compatibility:** Supporting new technologies

20.2.2 Patch Categories

20.2.2.1 Security Patches

Description: Patches that close security vulnerabilities

Priority: Critical to High

Examples: - CVE-affected vulnerabilities - Zero-day exploits - Critical security vulnerabilities

SLA: - **Critical (CVSS 9.0-10.0):** 7 days - **High (CVSS 7.0-8.9):** 30 days - **Medium (CVSS 4.0-6.9):** 90 days - **Low (CVSS 0.1-3.9):** 180 days

20.2.2.2 Feature Updates

Description: Updates with new features and improvements

Priority: Medium

Examples: - New features - Performance improvements - UI/UX enhancements

SLA: As needed, scheduled in maintenance windows

20.2.2.3 Bugfix Patches

Description: Patches to fix bugs without security relevance

Priority: Low to Medium

Examples: - Functional errors - Performance issues - Compatibility problems

SLA: 90 days or as needed

20.2.2.4 Firmware Updates

Description: Updates for hardware firmware

Priority: Medium to High

Examples: - BIOS/UEFI updates - Storage controller firmware - Network equipment firmware

SLA: According to vendor recommendation, scheduled

20.2.3 Patch Sources

System Type	Patch Source	Update Mechanism
Windows	Windows Update, WSUS	Automatic/Manual
Linux (RHEL/CentOS)	Red Hat Network, YUM	yum update
Linux (Ubuntu/Debian)	Ubuntu Repositories, APT	apt update && apt upgrade
VMware	VMware Update Manager	VUM
Applications	Vendor websites, Package Manager	Manual/Automatic
Firmware	Vendor support sites	Manual
Cloud Services	Provider-managed	Automatic

20.3 Patch Management Process

20.3.1 Process Overview

```
Vulnerability
Identification



Patch
Assessment



Patch
Acquisition
```

```
Patch
Testing


Patch
Deployment


Verification
& Reporting
```

20.3.2 1. Vulnerability Identification

Identification Sources: - **Vulnerability Scanner:** {{ meta.vulnerability_scanner }} - **Vendor Advisories:** Microsoft, Red Hat, VMware, etc. - **Security Mailing Lists:** CERT, US-CERT, vendor-specific - **Threat Intelligence:** {{ meta.threat_intelligence_source }} - **SIEM Alerts:** {{ meta.siem_system }}

Activities: - Conduct vulnerability scans (weekly) - Monitor vendor advisories (daily) - Check CVE database - Identify affected systems - Check patch availability

Responsible: Security Operations Team

20.3.3 2. Patch Assessment

Assessment Criteria:

Criterion	Assessment
CVSS Score	0.0 - 10.0
Exploit Availability	Yes/No
Asset Criticality	Critical/Important/Standard
Exposure	Internet-facing/Internal
Vendor Recommendation	Immediate/Planned/Optional

Risk Matrix:

	Internet-facing	**Internal**
Critical (CVSS 9-10)	Immediate (7 days)	High (14 days)
High (CVSS 7-8.9)	High (14 days)	Medium (30 days)
Medium (CVSS 4-6.9)	Medium (30 days)	Low (90 days)
Low (CVSS 0-3.9)	Low (90 days)	Very low (180 days)

Impact Assessment: - Which systems are affected? - Which business processes are dependent? - Is a reboot required? - Are there known compatibility issues? - Which maintenance window is available?

Decision: - **Patch:** Install patch - **Defer:** Postpone patch (with justification) - **Reject:** Do not install patch (with justification) - **Workaround:** Alternative mitigation

Responsible: Patch Management Team

20.3.4 3. Patch Acquisition

Acquisition Activities: - Download patch from vendor source - Verify patch integrity (checksums, signatures) - Store patch in patch repository - Document patch metadata

Patch Repository: {{ meta.patch_repository }}

Documentation: - Patch ID - Vendor - Release date - CVE IDs - Affected systems - Installation instructions

Responsible: Patch Management Team

20.3.5 4. Patch Testing

Test Environments:

Environment	Purpose	Systems
Dev	Developer tests	{{ netbox.environment.dev }}
Test	Functional tests	{{ netbox.environment.test }}
Staging	Pre-production tests	{{ netbox.environment.staging }}
Production	Production systems	{{ netbox.environment.production }}

Test Process:

20.3.5.1 Phase 1: Dev Testing (Optional)

Duration: 1-2 days

Activities: - Install patch in dev environment - Test basic functionality - Identify obvious problems

20.3.5.2 Phase 2: Test Testing

Duration: 3-5 days

Activities: - Install patch in test environment - Conduct functional tests - Conduct performance tests - Conduct compatibility tests - Test rollback procedure

Test Checklist: - [ ] Patch successfully installed - [ ] System boots after reboot - [ ] Applications start - [ ] Basic functionality works - [ ] Performance acceptable - [ ] No error logs - [ ] Rollback successfully tested

20.3.5.3 Phase 3: Staging Testing

Duration: 2-3 days

Activities: - Install patch in staging environment - Conduct business process tests - User acceptance tests (UAT) - Load tests (if critical)

Go/No-Go Decision: - All tests passed → Go - Critical problems → No-Go, defer patch - Non-critical problems → Go with workaround

Responsible: QA Team, Application Owners

Exceptions (Emergency Patches): - Critical security patches can shorten test phase - Minimum basic tests in test environment - Increased risk accepted and documented

20.3.6 5. Patch Deployment

Deployment Strategies:

20.3.6.1 Phased Rollout (Standard)

Description: Gradual rollout in phases

Phases: 1. **Pilot Group:** 5-10% of systems (1-2 days) 2. **Phase 1:** 25% of systems (2-3 days) 3. **Phase 2:** 50% of systems (2-3 days) 4. **Phase 3:** All remaining systems

Advantages: - Risk minimization - Early problem detection - Controlled rollout

Application: Standard patches, feature updates

20.3.6.2 Big Bang (All at once)

Description: Patch all systems simultaneously

Advantages: - Fast rollout - Simple coordination

Disadvantages: - High risk - Large impact if problems occur

Application: Only for non-critical systems or emergencies

20.3.6.3 Rolling Update

Description: Patch systems one after another (e.g., in clusters)

Advantages: - No downtime - Continuous availability

Application: High-availability systems, load-balanced clusters

Deployment Methods:

Method	Tool	Application
Automatic	WSUS, SCCM, Ansible	Standard patches
Semi-Automatic	Patch management tool	Scheduled patches
Manual	Remote session	Critical systems, firmware

Deployment Time Windows:

System Tier	Maintenance Window	Frequency
Tier 0 (Critical)	Sunday 02:00-06:00	Monthly
Tier 1 (Important)	Saturday 22:00-02:00	Monthly
Tier 2 (Standard)	Wednesday 20:00-22:00	Monthly
Tier 3 (Non-critical)	Anytime	As needed

Deployment Checklist: - [ ] Change ticket created and approved - [ ] Stakeholders informed - [ ] Backup created - [ ] Rollback plan ready - [ ] Monitoring activated - [ ] On-call team available

Responsible: IT Operations Team

20.3.7 6. Verification & Reporting

Verification Activities: - Confirm patch installation - Check system functionality - Monitor performance metrics - Check error logs - Repeat vulnerability scan

Verification Checklist: - [ ] Patch installed on all target systems - [ ] Systems running stable - [ ] No critical errors - [ ] Performance normal - [ ] Vulnerability closed (scan)

Reporting: - Patch status report - Success/failure rate - Open patches - Compliance status

Responsible: Patch Management Team

20.4 Patch Schedules

20.4.1 Monthly Patch Cycle

Microsoft Patch Tuesday: - **Patch Release:** 2nd Tuesday of month - **Assessment:** Tuesday-Wednesday - **Testing:** Wednesday-Friday (Week 1) - **Staging:** Monday-Wednesday (Week 2) - **Production Deployment:** Saturday/Sunday (Week 2-3)

Linux Patches: - **Assessment:** Weekly (Monday) - **Testing:** Tuesday-Thursday - **Deployment:** Saturday (monthly)

Application Patches: - **Assessment:** Upon vendor release - **Testing:** 1 week - **Deployment:** Next maintenance window

20.4.2 Emergency Patches

Trigger: - Critical vulnerability (CVSS $>$ 9.0) - Active exploits in the wild - Zero-day vulnerabilities - Vendor recommendation "Immediate"

Process: - **Assessment:** Immediate ($<$ 4 hours) - **Testing:** Minimal ($<$ 8 hours) - **Deployment:** Immediate ($<$ 24 hours)

Approval: CIO or CISO

Communication: Inform all stakeholders immediately

20.4.3 Patch Calendar

Week	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Week 1	Assessment	Testing	Testing	Testing	Testing	-	-
Week 2	Staging	Staging	Staging	Go/No-Go	-	Tier 1 Deploy	Tier 0 Deploy
Week 3	Verification	Reporting	Tier 2 Deploy	-	-	-	-
Week 4	-	-	-	-	-	-	-

20.5 Patch Management Tools

20.5.1 Windows Patch Management

Tool: Windows Server Update Services (WSUS)
Server: {{ netbox.wsus.server }}
Management: {{ netbox.wsus.management_url }}

Configuration: - Automatic synchronization with Microsoft Update - Patch approval workflow - Computer groups by tier - Reporting and compliance dashboard

Patch Groups: - **Pilot:** Test systems - **Tier-0:** Critical production systems - **Tier-1:** Important production systems - **Tier-2:** Standard systems - **Tier-3:** Non-critical systems

20.5.2 Linux Patch Management

Tool: Ansible / Satellite
Server: {{ netbox.ansible.server }}

Playbooks: - `patch-assessment.yml` - Check available updates - `patch-security.yml` - Security updates only - `patch-all.yml` - All updates - `patch-rollback.yml` - Rollback

Example Playbook:

```yaml
---
- name: Patch Linux Servers
  hosts: linux_servers
  become: yes
  tasks:
    - name: Update package cache
      apt:
        update_cache: yes
      when: ansible_os_family == "Debian"

    - name: Install security updates
      apt:
        upgrade: safe
        autoremove: yes
      when: ansible_os_family == "Debian"
```

```yaml
- name: Check if reboot required
  stat:
    path: /var/run/reboot-required
  register: reboot_required

- name: Reboot if required
  reboot:
    msg: "Reboot for security updates"
  when: reboot_required.stat.exists
```

20.5.3 VMware Patch Management

Tool: VMware Update Manager (VUM)
Integration: vCenter {{ netbox.vcenter.server }}

Baseline Groups: - **Critical-Patches:** Critical security patches - **Non-Critical-Patches:** All other patches - **Upgrades:** ESXi upgrades

Remediation Process: - Check baseline compliance - Put hosts in maintenance mode - Install patches - Reboot hosts - Verify compliance

20.5.4 Vulnerability Scanner

Tool: {{ meta.vulnerability_scanner }}
Scan Frequency: Weekly

Scan Profiles: - **Full Scan:** All vulnerabilities - **Patch Scan:** Missing patches only - **Compliance Scan:** Compliance checks

Integration: SIEM, Ticketing System

20.6 Rollback Procedures

20.6.1 Rollback Triggers

Rollback required when: - Critical functionality not available - Performance degradation > 20% - Data corruption - Security issues caused by patch - Business process failure

Rollback Decision: IT Operations Manager or higher

20.6.2 Rollback Methods

20.6.2.1 Windows Rollback

Method 1: Windows Uninstall

```
# Display patch list
Get-HotFix

# Uninstall patch
wusa /uninstall /kb:KBXXXXXX /quiet /norestart
```

Method 2: System Restore - Restore point before patch installation - Perform system recovery

Method 3: Backup Restore - Restore VM snapshot - Bare-metal restore

20.6.2.2 Linux Rollback

Method 1: Package Downgrade

```
# Ubuntu/Debian
apt-cache policy <package>
apt-get install <package>=<old-version>

# RHEL/CentOS
yum downgrade <package>
```

Method 2: Snapshot Rollback - Restore LVM snapshot - Restore VM snapshot

20.6.2.3 VMware Rollback

Method: VUM Rollback - Undo baseline remediation - Install previous patch version

20.6.3 Rollback Process

1. **Make Rollback Decision**
   - Assess impact
   - Inform stakeholders
2. **Perform Rollback**
   - Select rollback method
   - Execute rollback
   - Restart system (if required)
3. **Verification**
   - Check functionality
   - Check performance
   - Check logs
4. **Documentation**
   - Document rollback reason
   - Lessons learned
   - Evaluate alternative solutions

20.7 Compliance and Reporting

20.7.1 Patch Compliance Metrics

Metric	Target Value	Measurement
Patch Compliance Rate	$> 95\%$	Patched systems / Total systems
Critical Patch SLA	$> 95\%$	Patches in SLA / Total patches
Mean Time to Patch (MTTP)	< 30 days	Average patch duration
Patch Success Rate	$> 98\%$	Successful patches / Total patches
Rollback Rate	$< 2\%$	Rollbacks / Total patches

20.7.2 Patch Compliance Dashboard

Metrics: - Patch status by system tier - Open critical patches - SLA compliance - Patch trends (monthly) - Top 10 vulnerabilities

Tool: {{ meta.patch_dashboard }}

Access: IT Management, Security Team

20.7.3 Reporting

Weekly Patch Status Report: - New patches available - Patches in testing - Planned deployments - Open critical patches

Monthly Patch Compliance Report: - Patch compliance rate - SLA compliance - Patch statistics - Trend analysis - Improvement measures

Quarterly Management Report: - Patch management strategy review - Risk assessment - Compliance status - Budget and resources

Recipients: - Weekly: IT Operations Team - Monthly: IT Management, Security Team - Quarterly: CIO, CISO, Management

20.8 Exceptions and Special Cases

20.8.1 Patch Exceptions

Reasons for Exceptions: - Vendor support ends (End-of-Life) - Application incompatibility - Business-critical systems (change freeze) - Special vendor requirements

Exception Process: 1. Submit exception request 2. Conduct risk assessment 3. Define compensating measures 4. Obtain management approval 5. Document exception 6. Review regularly (quarterly)

Exception Register: {{ meta.exception_register }}

20.8.2 End-of-Life Systems

Strategy: - Plan migration - Network segmentation - Additional monitoring - Compensating controls - Document risk acceptance

EOL Register: {{ meta.eol_register }}

20.8.3 Legacy Applications

Challenges: - No patches available - Incompatibility with new OS versions - Vendor support discontinued

Mitigations: - Virtualization/containerization - Network isolation - WAF/IPS in front of application - Regular vulnerability scans - Migration roadmap

20.9 Roles and Responsibilities

20.9.1 Patch Management Team

Responsibilities: - Patch process ownership - Vulnerability assessment - Patch testing coordination - Deployment planning - Reporting

Team Lead: Andreas Huemmer

20.9.2 System Administrators

Responsibilities: - Perform patch deployment - System monitoring - Perform rollback - Documentation

20.9.3 Security Team

Responsibilities: - Vulnerability scanning - Risk assessment - Security patch prioritization - Compliance monitoring

Lead: Thomas Weber

20.9.4 Application Owners

Responsibilities: - Check application compatibility - User acceptance tests - Go/No-Go decision - Business impact assessment

20.9.5 Change Manager

Responsibilities: - Approve change tickets - Manage change calendar - Stakeholder communication - Post-implementation review

20.10 Best Practices

20.10.1 Patch Management Best Practices

1. **Regular Vulnerability Scans**
   - Weekly scans
   - Automated scans
   - Prioritization by risk
2. **Test Before Deployment**
   - Always test in test environment
   - Have rollback plan ready
   - Keep documentation current
3. **Phased Rollout**
   - Pilot group first
   - Gradual rollout
   - Monitoring during rollout
4. **Backup Before Patching**
   - Always create backup
   - Check backup integrity
   - Test restore procedure

5. **Communication**
    - Inform stakeholders early
    - Status updates during deployment
    - Post-deployment communication
6. **Documentation**
    - Document patch process
    - Record lessons learned
    - Maintain knowledge base
7. **Automation**
    - Automate patch deployment
    - Automate reporting
    - Automate compliance checks
8. **Continuous Improvement**
    - Review process regularly
    - Analyze metrics
    - Implement optimizations

20.11 References

- NIST SP 800-40 Rev. 4 - Guide to Enterprise Patch Management Planning
- ISO/IEC 27002:2013 - Control 12.6.1 (Management of Technical Vulnerabilities)
- CIS Controls v8 - Control 7 (Continuous Vulnerability Management)
- ITIL v4 - Change Enablement Practice
- Vendor Patch Documentation (Microsoft, Red Hat, VMware)
- CVE Database: https://cve.mitre.org
- NVD Database: https://nvd.nist.gov

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Classification: internal
Last Update: {{ meta.date }}

ewpage

Chapter 21

Log Management and Audit

21.1 Purpose and Scope

This document describes the log management and audit processes for AdminSend GmbH. It defines log collection, aggregation, retention, audit trail requirements, and SIEM integration to ensure traceability, compliance, and security monitoring.

Scope: All IT systems, networks, applications, and security components of AdminSend GmbH

Responsible: Thomas Weber (thomas.weber@adminsend.de)

21.2 Log Management Fundamentals

21.2.1 Objectives

Primary Objectives: - **Security Monitoring:** Detection of security incidents - **Compliance:** Meeting regulatory requirements - **Troubleshooting:** Error analysis and problem resolution - **Forensics:** Traceability of events - **Audit:** Evidence of controls and processes - **Performance Analysis:** System and application performance

21.2.2 Log Types

21.2.2.1 System Logs

Description: Operating system events

Examples: - Windows Event Logs (Security, System, Application) - Linux Syslog (/var/log/messages, /var/log/auth.log) - Boot logs, Kernel logs

Important Events: - System start/stop - Service start/stop - Errors and warnings - Hardware events

21.2.2.2 Security Logs

Description: Security-relevant events

Examples: - Authentication events (Login, Logout, Failed Login) - Authorization events (Access denial) - Privilege changes - Security policy changes - Firewall logs - IDS/IPS alerts

Important Events: - Failed login attempts - Privilege escalation - Account changes - Security policy changes

21.2.2.3 Application Logs

Description: Application-specific events

Examples: - Web server logs (Apache, Nginx, IIS) - Database logs (MySQL, PostgreSQL, SQL Server) - Application logs (Custom apps) - Middleware logs (Tomcat, JBoss)

Important Events: - Application errors - Transaction logs - Performance metrics - User activities

21.2.2.4 Network Logs

Description: Network events

Examples: - Firewall logs - Router/Switch logs - VPN logs - DNS logs - DHCP logs - Proxy logs

Important Events: - Connection attempts (allowed/blocked) - Network changes - Bandwidth usage - Anomalies

21.2.2.5 Audit Logs

Description: Compliance and audit-relevant events

Examples: - Data access - Configuration changes - Administrative activities - Privileged access

Important Events: - Who did what when? - Changes to critical systems - Access to sensitive data

21.2.3 Log Levels

Level	Description	Usage	Example
EMERGENCY	System unusable	Critical system errors	Kernel Panic
ALERT	Immediate action required	Critical errors	Database unreachable
CRITICAL	Critical conditions	Severe errors	Disk full
ERROR	Error conditions	Errors	Application error
WARNING	Warning conditions	Warnings	Disk 80% full
NOTICE	Normal but significant condition	Important events	Service started
INFO	Informational messages	Normal events	User login
DEBUG	Debug messages	Development	Function calls

21.3 Log Collection and Aggregation

21.3.1 Log Architecture

```
Log Sources
```

```
  Servers, Network, Applications, Security Devices


                      Syslog, Agents, APIs


              Log Collectors/Forwarders
  Rsyslog, Fluentd, Logstash, Splunk Forwarders


                      Parsing, Filtering, Enrichment


              Log Aggregation Platform
  SIEM, ELK Stack, Splunk, Graylog




 Hot Storage            Cold Storage / Archive
 (Fast Access)          (Long-term Retention)
```

21.3.2 Log Collection Methods

21.3.2.1 Syslog

Protocol: RFC 5424 (Syslog Protocol)
Transport: UDP 514 (Standard), TCP 514 (Reliable), TLS 6514 (Secure)

Advantages: - Standard protocol - Widely adopted - Simple configuration

Disadvantages: - UDP not reliable - Limited structure - No authentication (without TLS)

Usage: Linux/Unix systems, Network devices

21.3.2.2 Agent-based

Agents: - Splunk Universal Forwarder - Elastic Beats (Filebeat, Metricbeat) - Fluentd - NXLog

Advantages: - Reliable transmission - Local buffering - Parsing and filtering - Encrypted transmission

Disadvantages: - Agent installation required - Agent management - Resource consumption

Usage: Servers, Workstations

21.3.2.3 API-based

Methods: - REST APIs - Cloud provider APIs (AWS CloudWatch, Azure Monitor) - Webhook integration

Advantages: - Structured data - Real-time integration - No agent installation

Disadvantages: - API limits - Network dependency - More complex configuration

Usage: Cloud services, SaaS applications

21.3.2.4 Windows Event Forwarding (WEF)

Method: Windows-native event forwarding

Advantages: - No additional agents - Central configuration via GPO - Reliable

Disadvantages: - Windows only - Limited parsing options

Usage: Windows environments

21.3.3 Log Aggregation Platform

SIEM System: {{ meta.siem_system }}
Version: {{ meta.siem_version }}
Management URL: {{ meta.siem_url }}

Components: - **Log Collectors:** {{ meta.log_collectors }} - **Indexers:** {{ meta.log_indexers }} - **Search Heads:** {{ meta.log_search_heads }} - **Storage:** {{ meta.log_storage }}

Capacity: - **Ingestion Rate:** {{ meta.log_ingestion_rate }} GB/day - **Storage Capacity:** {{ meta.log_storage_capacity }} TB - **Retention (Hot):** {{ meta.log_retention_hot }} days - **Retention (Cold):** {{ meta.log_retention_cold }} days

21.4 Log Retention and Archiving

21.4.1 Retention Policies

21.4.1.1 Retention by Log Type

Log Type	Hot Storage	Cold Storage	Total	Rationale
Security Logs	90 days	7 years	7 years	Compliance, Forensics
Audit Logs	90 days	7 years	7 years	Compliance, Regulation
System Logs	30 days	1 year	1 year	Troubleshooting
Application Logs	30 days	1 year	1 year	Troubleshooting
Network Logs	30 days	1 year	1 year	Security, Troubleshooting
Web Access Logs	30 days	6 months	6 months	Analytics, Security
Debug Logs	7 days	-	7 days	Development

21.4.2 Storage Tiers

21.4.2.1 Hot Storage (Fast Access)

Technology: SSD, NVMe
Retention: 30-90 days
Access: Real-time search, Dashboards
Cost: High

Usage: - Active monitoring - Security analysis - Troubleshooting

21.4.2.2 Warm Storage (Medium Access)

Technology: HDD, Object Storage
Retention: 3-12 months
Access: Search (slower)
Cost: Medium

Usage: - Historical analysis - Compliance audits - Forensics

21.4.2.3 Cold Storage (Archive)

Technology: Tape, Cloud Glacier, Object Storage
Retention: 1-7 years
Access: Restore required (hours to days)
Cost: Low

Usage: - Long-term archiving - Compliance requirements - Legal retention

21.5 Log Analysis and Monitoring

21.5.1 SIEM Integration

SIEM System: {{ meta.siem_system }}

Functions: - **Real-time Monitoring:** Real-time monitoring - **Correlation:** Event correlation - **Alerting:** Automatic alerts - **Dashboards:** Visualization - **Reporting:** Compliance reports - **Threat Intelligence:** Integration of threat feeds

21.5.2 Use Cases and Correlation Rules

21.5.2.1 Failed Login Attempts

Use Case: Detection of brute-force attacks

Rule:

```
IF failed_login_count > 5
   AND time_window = 5 minutes
   AND same_source_ip
THEN alert "Possible Brute-Force Attack"
```

Severity: High
Response: Temporarily lock account, block IP

21.5.2.2 Privilege Escalation

Use Case: Detection of unauthorized privilege changes

Rule:

```
IF event_type = "privilege_change"
   AND new_privilege = "admin"
   AND user NOT IN admin_group
THEN alert "Unauthorized Privilege Escalation"
```

Severity: Critical
Response: Immediate investigation, deactivate account

21.6 Compliance and Regulation

21.6.1 GDPR

Requirements: - Logging of access to personal data - Right to information (which data was processed) - Right to deletion (logs with personal data) - Breach notification obligation (72h)

Implementation: - Access logs for all personal data - Pseudonymization where possible - Observe retention policies - Deletion processes implemented

21.6.2 ISO 27001

Requirements: - A.12.4.1: Event Logging - A.12.4.2: Protection of log information - A.12.4.3: Administrator and operator logs - A.12.4.4: Time synchronization

Implementation: - Comprehensive event logging - Log integrity ensured - Privileged access logged - NTP synchronization

21.7 References

- ISO/IEC 27001:2013 - A.12.4 (Logging and Monitoring)
- NIST SP 800-92 - Guide to Computer Security Log Management
- PCI-DSS v4.0 - Requirement 10
- GDPR - Article 30 (Record of processing activities)
- CIS Controls v8 - Control 8 (Audit Log Management)
- ITIL v4 - Monitoring and Event Management

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Classification: internal
Last Update: {{ meta.date }}

ewpage

Chapter 22

Capacity and Performance Management

22.1 Overview

This document describes the processes and methods for capacity and performance management of the IT service. The goal is to ensure that sufficient IT resources are available to meet current and future business requirements.

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

22.2 Capacity Planning

22.2.1 Planning Cycle

Phase	Timeframe	Responsible	Activities
Short-term	1-3 months	Andreas Huemmer	Monitoring, adjustments
Medium-term	3-12 months	Anna Schmidt	Capacity forecasts, budget planning
Long-term	1-3 years	Max Mustermann	Strategic planning, investments

22.2.2 Capacity Dimensions

22.2.2.1 Compute Resources

- **CPU Capacity:** {{ netbox.cluster.total_cpu_cores }} Cores
- **RAM Capacity:** {{ netbox.cluster.total_memory_gb }} GB

- **Utilization Target:** 70% (Average), 85% (Peak)
- **Scaling Threshold:** 80% over 7 days

22.2.2.2 Storage Resources

- **Total Capacity:** {{ netbox.storage.total_capacity_tb }} TB
- **Available Capacity:** {{ netbox.storage.available_capacity_tb }} TB
- **Utilization Target:** 75% (Average), 85% (Maximum)
- **Scaling Threshold:** 80% utilization

22.2.2.3 Network Resources

- **WAN Bandwidth:** {{ netbox.circuit.bandwidth_mbps }} Mbps
- **LAN Bandwidth:** {{ netbox.network.lan_bandwidth_gbps }} Gbps
- **Utilization Target:** 60% (Average), 80% (Peak)
- **Scaling Threshold:** 75% over 5 days

22.3 Performance Monitoring

22.3.1 Performance Metrics

22.3.1.1 System Performance

Metric	Target	Warning Threshold	Critical	Measurement Interval
CPU Utilization	$< 70\%$	$> 80\%$	$> 90\%$	1 Minute
RAM Utilization	$< 75\%$	$> 85\%$	$> 95\%$	1 Minute
Disk I/O Latency	< 10ms	> 20ms	> 50ms	1 Minute
Disk I/O Throughput	> 100 MB/s	< 50 MB/s	< 20 MB/s	1 Minute
Network Latency	< 5ms	> 10ms	> 20ms	30 Seconds
Network Packet Loss	$< 0.1\%$	$> 0.5\%$	$> 1\%$	1 Minute

22.3.1.2 Application Performance

Metric	Target	Warning Threshold	Critical	Measurement Interval
Response Time	< 200ms	> 500ms	> 1000ms	1 Minute
Throughput (TPS)	> 1000	< 500	< 100	1 Minute

Metric	Target	Warning Threshold	Critical	Measurement Interval
Error Rate	$< 0.1\%$	$> 1\%$	$> 5\%$	1 Minute
Concurrent Users	[TODO]	[TODO]	[TODO]	5 Minutes
Queue Length	< 10	> 50	> 100	1 Minute

22.4 Trend Analysis

22.4.1 Analysis Process

22.4.1.1 Weekly Analysis

- **Execution:** Every Monday
- **Responsible:** IT Operations Team
- **Focus:** Short-term trends and anomalies
- **Output:** Weekly report with recommendations

22.4.1.2 Monthly Analysis

- **Execution:** First business day of month
- **Responsible:** Andreas Huemmer
- **Focus:** Medium-term trends and capacity forecasts
- **Output:** Monthly report with capacity recommendations

22.4.1.3 Quarterly Analysis

- **Execution:** End of quarter
- **Responsible:** Anna Schmidt
- **Focus:** Strategic trends and investment planning
- **Output:** Quarterly report with budget recommendations

22.5 Scaling Strategies

22.5.1 Vertical Scaling (Scale-Up)

22.5.1.1 Use Cases

- Database servers with high I/O requirements
- Monolithic applications
- Legacy systems without cluster support

22.5.1.2 Advantages

- Simple implementation
- No application changes required

- Lower complexity

22.5.1.3 Disadvantages

- Hardware limits
- Single point of failure
- Higher cost per unit

22.5.2 Horizontal Scaling (Scale-Out)

22.5.2.1 Use Cases

- Stateless web applications
- Microservices architectures
- Container-based workloads

22.5.2.2 Advantages

- Nearly unlimited scalability
- Higher availability through redundancy
- Cost efficiency through commodity hardware

22.5.2.3 Disadvantages

- Higher complexity
- Application changes required
- Load balancing and state management

22.5.3 Auto-Scaling

22.5.3.1 Trigger Conditions

Metric	Scale-Up	Scale-Down	Cool-Down
CPU Utilization	$> 75\%$ (5 Min)	$< 30\%$ (15 Min)	5 Minutes
RAM Utilization	$> 80\%$ (5 Min)	$< 40\%$ (15 Min)	5 Minutes
Request Queue	> 50 (3 Min)	< 10 (10 Min)	3 Minutes
Response Time	> 500ms (5 Min)	< 200ms (15 Min)	5 Minutes

22.6 Reporting

22.6.1 Performance Reports

22.6.1.1 Weekly Performance Report

- **Recipients:** IT Operations Team
- **Content:**
  - Performance metrics of the week
  - Incidents and outages

  - Trend analysis
  - Recommendations

22.6.1.2 Monthly Capacity Report

- **Recipients:** Anna Schmidt, Andreas Huemmer
- **Content:**
  - Capacity utilization
  - Growth trends
  - Scaling recommendations
  - Budget implications

22.6.1.3 Quarterly Management Report

- **Recipients:** Max Mustermann, Anna Schmidt, Maria Müller
- **Content:**
  - Strategic capacity planning
  - Investment recommendations
  - ROI analysis
  - Risk assessment

22.7 Processes and Responsibilities

22.7.1 RACI Matrix

Activity	CIO	Ops Manager	Ops Team	Finance
Capacity Planning	A	R	C	I
Performance Monitoring	I	A	R	-
Trend Analysis	C	A	R	-
Scaling Decisions	A	R	C	C
Budget Planning	A	C	I	R
Optimization Measures	C	A	R	-
Reporting	I	R	C	I

Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed

---

22.8 Compliance and Standards

22.8.1 Relevant Standards

- **ITIL v4:** Capacity and Performance Management Practice
- **ISO 20000:** Clause 8.7 - Capacity Management
- **COBIT 2019:** APO03 - Managed Architecture, BAI04 - Managed Availability and Capacity

---

Last Update: {{ meta.date }}
Next Review: [TODO: Date]
Contact: andreas.huemmer@adminsend.de

ewpage

Chapter 23

Availability and Service Level

23.1 Overview

This document defines availability requirements, Service Level Agreements (SLAs), and Service Level Objectives (SLOs) for the IT service. It describes measurement methods, reporting processes, and measures for continuous improvement of service availability.

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

23.2 Availability Requirements

23.2.1 Service Classification

Service Class	Availability	Max Downtime/Year	Max Downtime/Month	Business Criticality
Critical	99.95%	4.38 hours	21.6 minutes	High
Important	99.5%	43.8 hours	3.6 hours	Medium
Standard	99.0%	87.6 hours	7.2 hours	Low
Non-critical	95.0%	438 hours	36 hours	Very low

23.2.2 Service Times

23.2.2.1 Production Services

- **Availability:** 24/7/365
- **Support Hours:** 24/7 with on-call availability
- **Maintenance Window:** Sunday 02:00-06:00 (after announcement)
- **Emergency Maintenance:** After approval by Anna Schmidt

23.2.2.2 Business Services

- **Availability:** Mon-Fri 06:00-22:00
- **Support Hours:** Mon-Fri 08:00-18:00
- **Maintenance Window:** Saturday 20:00-24:00
- **Emergency Maintenance:** After approval by Andreas Huemmer

---

23.3 Service Level Agreements (SLA)

23.3.1 SLA Definitions

23.3.1.1 Availability SLA

Service: [TODO: Service Name]
Valid from: [TODO: Date]
Duration: 12 months with automatic renewal

Metric	Target	Measurement Method	Measurement Interval
Availability	99.5%	Uptime Monitoring	Monthly
Planned Downtime	< 4h/month	Change Calendar	Monthly
Unplanned Downtime	< 2h/month	Incident Tracking	Monthly
MTBF (Mean Time Between Failures)	> 720h	Incident Analysis	Quarterly
MTTR (Mean Time To Repair)	< 2h	Incident Tickets	Monthly

23.3.1.2 Performance SLA

Metric	Target	Warning Threshold	Measurement Method	Measurement Interval
Response Time (Avg)	< 200ms	> 300ms	APM Tool	Continuous
Response Time (95th)	< 500ms	> 750ms	APM Tool	Continuous
Response Time (99th)	< 1000ms	> 1500ms	APM Tool	Continuous
Throughput	> 1000 TPS	< 800 TPS	APM Tool	Continuous
Error Rate	< 0.1%	> 0.5%	APM Tool	Continuous

23.3.1.3 Support SLA

Priority	Response Time	Resolution Time	Availability	Escalation
P1 - Critical	15 minutes	4 hours	24/7	Immediately to CIO
P2 - High	1 hour	8 hours	24/7	After 4h to Ops Manager
P3 - Medium	4 hours	24 hours	Mon-Fri 08-18	After 24h to Ops Manager
P4 - Low	8 hours	72 hours	Mon-Fri 08-18	After 72h to Ops Manager

---

23.4 Service Level Objectives (SLO)

23.4.1 Internal SLOs

23.4.1.1 Infrastructure SLOs

Component	SLO	Measurement Method	Responsible
Compute Cluster	99.9%	Hypervisor Monitoring	Andreas Huemmer
Storage System	99.95%	Storage Monitoring	Andreas Huemmer
Network Core	99.99%	Network Monitoring	Andreas Huemmer
Firewall	99.95%	Security Monitoring	Thomas Weber
Load Balancer	99.9%	LB Monitoring	Andreas Huemmer

23.4.2 Error Budget

23.4.2.1 Error Budget Concept

- **Definition:** Tolerable downtime within the SLO period
- **Calculation:** (100% - SLO) × Period
- **Usage:** Balance between innovation and stability

23.4.2.2 Error Budget Example (99.5% SLO)

Period	Availability	Error Budget	Downtime
Month	99.5%	0.5%	3.6 hours
Quarter	99.5%	0.5%	10.8 hours
Year	99.5%	0.5%	43.8 hours

23.5 Availability Measurement

23.5.1 Measurement Methods

23.5.1.1 Synthetic Monitoring

- **Method:** Automated tests of defined endpoints
- **Frequency:** Every 1-5 minutes
- **Locations:** Multiple geographic locations
- **Metrics:** Availability, Response Time, Functionality

23.5.1.2 Real User Monitoring (RUM)

- **Method:** Measurement of actual user interactions
- **Collection:** Client-side metrics
- **Metrics:** Page Load Time, User Experience, Error Rate
- **Privacy:** GDPR compliant, anonymized

23.6 Service Level Reporting

23.6.1 Report Types

23.6.1.1 Daily Availability Report

- **Recipients:** IT Operations Team
- **Content:**
  - Availability of last 24 hours
  - Incidents and outages
  - Performance metrics
  - Current alerts
- **Delivery:** Automatically at 08:00

23.6.1.2 Weekly SLA Report

- **Recipients:** Andreas Huemmer
- **Content:**
  - Weekly availability
  - SLA compliance status
  - Trend analysis
  - Recommendations
- **Delivery:** Every Monday

23.6.1.3 Monthly SLA Report

- **Recipients:** Anna Schmidt, Stakeholders
- **Content:**
  - Monthly availability
  - SLA fulfillment vs. targets
  - Incident summary

  - Error Budget status
  - Improvement measures
- **Delivery:** First business day of following month

23.7 Processes and Responsibilities

23.7.1 RACI Matrix

Activity	CIO	Ops Manager	Ops Team	Stakeholder
SLA Definition	A	R	C	C
Availability Measurement	I	A	R	-
SLA Reporting	C	A	R	I
SLA Review	A	R	C	C
Improvement Measures	A	R	C	I
Incident Response	I	A	R	I
Postmortems	C	A	R	I

Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed

---

23.8 Compliance and Standards

23.8.1 Relevant Standards

- **ITIL v4:** Availability Management Practice
- **ISO 20000:** Clause 8.9 - Availability Management
- **COBIT 2019:** DSS01 - Managed Operations

Last Update: {{ meta.date }}
Next Review: [TODO: Date]
Contact: andreas.huemmer@adminsend.de

ewpage

Chapter 24

Data Management and Privacy

24.1 Overview

This document describes the processes and policies for data management and data protection in the IT service. It defines data classification, data protection requirements according to GDPR, data retention and deletion, as well as data governance structures.

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

24.2 Data Classification

24.2.1 Classification Levels

Level	Description	Examples	Protection Measures
Public	Intended for public	Marketing material, Press releases	No special measures
Internal	For internal use only	Internal policies, Org charts	Access control
Confidential	Sensitive business information	Contracts, Financial reports, Strategies	Encryption, strict access control
Highly Confidential	Highly sensitive data	Personnel data, Health data, Salaries	Encryption, MFA, Audit logging

24.2.2 Classification Criteria

24.2.2.1 Business Value

- **High:** Critical for business operations
- **Medium:** Important for business processes
- **Low:** Supporting information

24.2.2.2 Confidentiality

- **High:** Severe damage if disclosed
- **Medium:** Moderate damage if disclosed
- **Low:** Little or no damage

24.2.2.3 Integrity

- **High:** Critical for decisions
- **Medium:** Important for processes
- **Low:** Informational

24.2.2.4 Availability

- **High:** Immediate availability required
- **Medium:** Availability within hours
- **Low:** Availability within days

24.3 Data Protection Requirements (GDPR)

24.3.1 Legal Basis

24.3.1.1 EU General Data Protection Regulation (GDPR)

- **Effective since:** May 25, 2018
- **Scope:** Processing of personal data in the EU
- **Fines:** Up to 20 million EUR or 4% of worldwide annual revenue

24.3.1.2 Federal Data Protection Act (BDSG)

- **Effective since:** May 25, 2018
- **Supplement:** National regulations to GDPR
- **Application:** Germany-specific requirements

24.3.2 Personal Data

24.3.2.1 Definition

All information relating to an identified or identifiable natural person.

24.3.2.2 Categories

Category	Examples	Special Protection Measures
Basic Data	Name, Address, Email, Phone	Access control, Encryption
Identification Data	ID number, Social security number	Strict access control, Encryption
Special Categories	Health, Religion, Political opinion	Highest protection measures, explicit consent

Category	Examples	Special Protection Measures
Financial Data	Bank details, Credit card number	PCI-DSS compliance, Tokenization
Location Data	GPS coordinates, IP addresses	Anonymization, Pseudonymization

24.3.3 GDPR Principles

24.3.3.1 Lawfulness, Fairness, and Transparency

- Legal basis for each processing
- Transparent information to data subjects
- Documentation of processing purposes

24.3.3.2 Purpose Limitation

- Collect data only for specified purposes
- No further processing for other purposes
- Documentation of processing purposes

24.3.3.3 Data Minimization

- Collect only necessary data
- No excessive data collection
- Regular review of necessity

24.3.3.4 Accuracy

- Ensure data currency
- Correct inaccurate data
- Delete outdated data

24.3.3.5 Storage Limitation

- Store data only as long as necessary
- Defined retention periods
- Automatic deletion after expiry

24.3.3.6 Integrity and Confidentiality

- Protection against unauthorized access
- Encryption of sensitive data
- Access control and audit logging

24.3.3.7 Accountability

- Demonstrate GDPR compliance
- Documentation of all processing activities
- Regular audits

24.3.4 Data Subject Rights

Right	Description	Response Time	Responsible
Right of Access	Information about stored data	1 month	Thomas Weber
Right to Rectification	Correction of inaccurate data	Without delay	Thomas Weber
Right to Erasure	Deletion of personal data	Without delay	Thomas Weber
Right to Restriction	Restriction of processing	Without delay	Thomas Weber
Right to Data Portability	Transfer to another controller	1 month	Thomas Weber
Right to Object	Object to processing	Without delay	Thomas Weber

---

24.4 Data Retention and Deletion

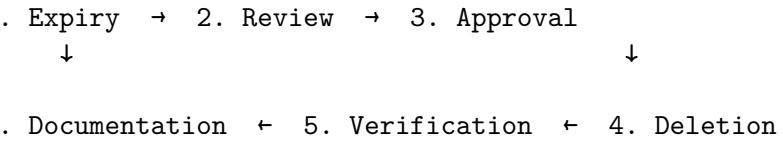
24.4.1 Retention Periods

24.4.1.1 Legal Retention Periods

Data Type	Retention Period	Legal Basis	Responsible
Business Letters	6 years	HGB § 257	Maria Müller
Accounting Documents	10 years	HGB § 257, AO § 147	Maria Müller
Annual Financial Statements	10 years	HGB § 257	Maria Müller
Payroll Documents	6 years	AO § 147	Maria Müller
Tax Documents	10 years	AO § 147	Maria Müller
Personnel Files	3-10 years	Various	Peter Fischer

24.4.2 Deletion Concept

24.4.2.1 Deletion Process



24.4.2.2 Deletion Methods

Media	Method	Standard	Responsible
Hard Drives	Secure Erase / Degaussing	NIST SP 800-88	Andreas Huemmer
SSDs	Crypto Erase / Destruction	NIST SP 800-88	Andreas Huemmer
Backup Media	Overwrite / Destruction	NIST SP 800-88	Andreas Huemmer
Cloud Data	API-based Deletion	Provider Standard	Andreas Huemmer
Databases	SQL DELETE / TRUNCATE	Database Standard	Andreas Huemmer
Paper	Shredding (P-4)	DIN 66399	Peter Fischer

24.5 Data Governance

24.5.1 Governance Structure

24.5.1.1 Data Governance Board

- **Chair:** Anna Schmidt
- **Members:** Thomas Weber, Maria Müller, Department Heads
- **Frequency:** Quarterly
- **Tasks:**
  - Strategic data governance
  - Approval of data policies
  - Compliance monitoring
  - Escalation of data protection incidents

24.5.1.2 Data Stewards

- **Role:** Functional data owners
- **Tasks:**
  - Ensure data quality
  - Perform data classification
  - Grant access permissions
  - Monitor data protection compliance

24.5.1.3 Data Custodians

- **Role:** Technical data owners
- **Tasks:**
  - Technical implementation of data policies
  - Ensure data security
  - Backup and recovery
  - Implement access control

24.6 Data Security

24.6.1 Encryption

24.6.1.1 Encryption at Rest (Data at Rest)

Data Type	Encryption	Algorithm	Key Length	Responsible
Highly Confidential	Mandatory	AES	256 Bit	Thomas Weber
Confidential	Mandatory	AES	256 Bit	Thomas Weber
Internal	Recommended	AES	128/256 Bit	Andreas Huemmer
Public	Not required	-	-	-

24.6.1.2 Encryption in Transit (Data in Transit)

Connection Type	Protocol	Minimum Version	Responsible
Web Traffic	HTTPS/TLS	TLS 1.2	Andreas Huemmer
Email	TLS/S/MIME	TLS 1.2	Andreas Huemmer
File Transfer	SFTP/FTPS	TLS 1.2	Andreas Huemmer
VPN	IPsec/OpenVPN	-	Andreas Huemmer
Database	TLS	TLS 1.2	Andreas Huemmer

24.7 Data Protection Incidents

24.7.1 Notification Obligation

24.7.1.1 GDPR Notification Obligation

- **Deadline:** 72 hours after becoming aware
- **Recipient:** Competent supervisory authority
- **Content:**
  - Nature of the breach
  - Affected data categories and persons
  - Likely consequences
  - Measures taken

24.7.1.2 Notification of Data Subjects

- **Requirement:** High risk to rights and freedoms
- **Deadline:** Without delay
- **Content:**
  - Nature of the breach
  - Contact point
  - Likely consequences
  - Measures taken

24.8 Processes and Responsibilities

24.8.1 RACI Matrix

Activity	CIO	CISO	Ops Manager	DPO	Data Stewards
Data Classification	I	C	I	C	R/A
GDPR Compliance	A	R	C	C	I
Data Protection Impact Assessment	C	R	C	A	C
Data Retention	C	C	R	C	A
Data Deletion	I	C	R	C	A
Data Governance	A	C	C	C	R
Data Security	C	A	R	C	I
Data Protection Incidents	A	R	C	C	I

Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed

---

24.9 Compliance and Standards

24.9.1 Relevant Standards

- **GDPR:** EU General Data Protection Regulation
- **BDSG:** Federal Data Protection Act
- **ISO 27001:** Information Security Management
- **ISO 27701:** Privacy Information Management
- **NIST SP 800-88:** Guidelines for Media Sanitization

Last Update: {{ meta.date }}
Next Review: [TODO: Date]
Contact: thomas.weber@adminsend.de

ewpage

Chapter 25

Maintenance and Operations Routines

25.1 Overview

This document describes regular maintenance tasks, operations checklists, and housekeeping procedures for the IT service. The goal is to ensure system stability, performance, and security through proactive maintenance.

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

25.2 Maintenance Overview

25.2.1 Maintenance Categories

Category	Description	Frequency	Responsible
Preventive	Preventive measures to avoid failures	Regular	Andreas Huemmer
Corrective	Fixing known problems	As needed	Andreas Huemmer
Adaptive	Adaptation to new requirements	As needed	Andreas Huemmer
Perfective	Improvement and optimization	Planned	Andreas Huemmer

25.2.2 Maintenance Windows

25.2.2.1 Regular Maintenance Windows

Type	Time Window	Duration	Announcement	Approval
Weekly	Sunday 02:00-04:00	2 hours	3 days	Ops Manager
Monthly	First Sunday 02:00-06:00	4 hours	7 days	Ops Manager
Quarterly	First Sunday of quarter 00:00-08:00	8 hours	14 days	CIO

25.2.2.2 Emergency Maintenance

- **Time Window:** Anytime after approval
- **Announcement:** Minimum 4 hours (if possible)
- **Approval:** Anna Schmidt
- **Communication:** Inform all stakeholders

25.3 Daily Routines

25.3.1 Morning Checks (08:00)

25.3.1.1 System Health Check

☐ Check monitoring dashboard
☐ Review critical alerts
☐ Validate system availability
☐ Check performance metrics
☐ Verify backup status

25.3.1.2 Incident Review

☐ Check overnight incidents
☐ Review open tickets
☐ Set priorities for the day
☐ Identify escalations

25.3.1.3 Capacity Check

☐ Check CPU utilization
☐ Check RAM utilization
☐ Check storage utilization
☐ Check network utilization

Responsible: Operations Team
Duration: 15-30 minutes
Documentation: Daily Operations Log

25.3.2 Midday Checks (12:00)

25.3.2.1 Performance Monitoring

- ☐ Check response times
- ☐ Review error rates
- ☐ Validate throughput
- ☐ Check queue lengths

25.3.2.2 Security Check

- ☐ Check security alerts
- ☐ Review failed login attempts
- ☐ Check firewall logs
- ☐ Identify anomalies

Responsible: Operations Team
Duration: 10-15 minutes
Documentation: Daily Operations Log

25.3.3 Evening Checks (18:00)

25.3.3.1 End of Day

- ☐ Review all incidents of the day
- ☐ Update open tickets
- ☐ Prepare backup jobs for the night
- ☐ Plan maintenance work for the night

25.3.3.2 Handover to Night Shift/On-Call

- ☐ Communicate critical issues
- ☐ Document ongoing work
- ☐ Update on-call contacts
- ☐ Confirm escalation paths

Responsible: Operations Team
Duration: 15-20 minutes
Documentation: Shift Handover Log

25.4 Weekly Routines

25.4.1 Monday: Week Planning

25.4.1.1 Week Start Meeting (09:00)

- ☐ Review weekend incidents
- ☐ Define week goals
- ☐ Plan maintenance work
- ☐ Assign resources

- ☐ Identify risks

Participants: Andreas Huemmer, Operations Team
Duration: 30 minutes
Documentation: Weekly Planning Notes

25.4.2 Tuesday: Backup Validation

25.4.2.1 Backup Verification

- ☐ Check backup logs of last week
- ☐ Validate backup success rate
- ☐ Review backup sizes
- ☐ Analyze failed backups
- ☐ Perform restore test (sample)

Responsible: Operations Team
Duration: 1-2 hours
Documentation: Backup Verification Report

25.4.3 Wednesday: Performance Analysis

25.4.3.1 Weekly Performance Review

- ☐ Analyze performance trends
- ☐ Identify bottlenecks
- ☐ Update capacity forecasts
- ☐ Identify optimization potentials

Responsible: Operations Team
Duration: 1 hour
Documentation: Weekly Performance Report

25.4.4 Thursday: Security Review

25.4.4.1 Weekly Security Check

- ☐ Analyze security logs
- ☐ Review vulnerability scans
- ☐ Check patch status
- ☐ Review security incidents
- ☐ Check compliance status

Responsible: Operations Team, Thomas Weber
Duration: 1-2 hours
Documentation: Weekly Security Report

25.4.5 Friday: Week Closure

25.4.5.1 Week Closure Meeting (15:00)

- ☐ Review week goals
- ☐ Summarize incidents of the week

- ☐ Discuss lessons learned
- ☐ Prepare next week
- ☐ Brief weekend on-call

Participants: Andreas Huemmer, Operations Team
Duration: 30 minutes
Documentation: Weekly Summary Report

25.4.6 Sunday: Maintenance Window

25.4.6.1 Weekly Maintenance (02:00-04:00)

- ☐ Install system updates
- ☐ Perform database maintenance
- ☐ Log archiving
- ☐ Disk cleanup
- ☐ Performance optimization

Responsible: On-Call Engineer
Duration: 2 hours
Documentation: Maintenance Log

25.5 Monthly Routines

25.5.1 First Week: Month Planning

25.5.1.1 Month Start Meeting

- ☐ Review previous month
- ☐ Define month goals
- ☐ Plan major maintenance work
- ☐ Check budget status
- ☐ Update capacity planning

Participants: Anna Schmidt, Andreas Huemmer, Team Leads
Duration: 1 hour
Documentation: Monthly Planning Document

25.5.2 First Week: Patch Management

25.5.2.1 Monthly Patch Deployment

- ☐ Check patch availability
- ☐ Assess criticality
- ☐ Patch test environment
- ☐ Perform validation
- ☐ Plan production deployment
- ☐ Create rollback plan

Responsible: Operations Team
Duration: 4-8 hours (over several days)
Documentation: Patch Management Report

25.5.3 Second Week: Capacity Review

25.5.3.1 Monthly Capacity Analysis

- ☐ Analyze resource utilization
- ☐ Identify growth trends
- ☐ Create capacity forecasts
- ☐ Assess scaling needs
- ☐ Check budget implications

Responsible: Andreas Huemmer
Duration: 2-3 hours
Documentation: Monthly Capacity Report

25.5.4 Third Week: Security Audit

25.5.4.1 Monthly Security Audit

- ☐ Review access rights
- ☐ Deactivate inactive accounts
- ☐ Check password policies
- ☐ Review firewall rules
- ☐ Perform vulnerability scan
- ☐ Check compliance status

Responsible: Thomas Weber, Operations Team
Duration: 3-4 hours
Documentation: Monthly Security Audit Report

25.5.5 Fourth Week: Disaster Recovery Test

25.5.5.1 Monthly DR Test

- ☐ Select DR scenario
- ☐ Create test plan
- ☐ Execute DR procedures
- ☐ Document results
- ☐ Identify improvements
- ☐ Update DR plan

Responsible: Andreas Huemmer
Duration: 2-4 hours
Documentation: DR Test Report

25.6 Quarterly Routines

25.6.1 First Week: Quarter Planning

25.6.1.1 Quarter Start Meeting

- ☐ Review previous quarter
- ☐ Define quarter goals
- ☐ Plan major projects
- ☐ Conduct budget review
- ☐ Update resource planning

Participants: Max Mustermann, Anna Schmidt, Andreas Huemmer
Duration: 2 hours
Documentation: Quarterly Planning Document

25.6.2 Second Week: Infrastructure Review

25.6.2.1 Quarterly Infrastructure Analysis

- ☐ Check hardware condition
- ☐ Identify end-of-life systems
- ☐ Assess upgrade needs
- ☐ Identify consolidation potentials
- ☐ Conduct investment planning

Responsible: Andreas Huemmer
Duration: 1 day
Documentation: Quarterly Infrastructure Report

25.7 Annual Routines

25.7.1 Q1: Annual Planning

25.7.1.1 Year Start Meeting

- ☐ Review previous year
- ☐ Define year goals
- ☐ Plan strategic initiatives
- ☐ Finalize annual budget
- ☐ Resource planning for the year

Participants: Max Mustermann, Anna Schmidt, Maria Müller, Andreas Huemmer
Duration: 1 day
Documentation: Annual Planning Document

25.7.2 Q2: Infrastructure Audit

25.7.2.1 Annual Infrastructure Audit

- ☐ Complete hardware inventory

- ☐ Software license audit
- ☐ Conduct compliance audit
- ☐ Security assessment
- ☐ Architecture review
- ☐ Identify modernization needs

Responsible: Anna Schmidt, Andreas Huemmer
Duration: 1 week
Documentation: Annual Infrastructure Audit Report

25.8 Housekeeping Procedures

25.8.1 Database Maintenance

25.8.1.1 Weekly Database Maintenance

- ☐ Check index fragmentation
- ☐ Update statistics
- ☐ Clean transaction logs
- ☐ Check database integrity
- ☐ Analyze performance metrics

Responsible: Database Administrator
Frequency: Weekly (Sunday 02:00)
Duration: 1-2 hours

25.8.2 Log Management

25.8.2.1 Daily Log Rotation

- ☐ Rotate application logs
- ☐ Rotate system logs
- ☐ Compress old logs
- ☐ Send logs to central system

Responsible: Automated
Frequency: Daily (00:00)
Duration: Automatic

25.9 Automation

25.9.1 Automated Routines

Routine	Frequency	Tool/Script	Responsible
Backup Jobs	Daily	[TODO: Backup Tool]	Andreas Huemmer
Log Rotation	Daily	logrotate	Automated
Health Checks	Hourly	[TODO: Monitoring Tool]	Automated

Routine	Frequency	Tool/Script	Responsible
Disk Cleanup	Weekly	[TODO: Script]	Automated
Security Scans	Daily	[TODO: Security Tool]	Automated
Performance Reports	Weekly	[TODO: Script]	Automated

25.10 Processes and Responsibilities

25.10.1 RACI Matrix

Activity	CIO	Ops Manager	Ops Team	On-Call
Daily Routines	I	A	R	C
Weekly Routines	I	A	R	C
Monthly Routines	C	A	R	I
Quarterly Routines	A	R	C	I
Annual Routines	A	R	C	I
Automation	C	A	R	I
Housekeeping	I	A	R	C

Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed

---

25.11 Compliance and Standards

25.11.1 Relevant Standards

- **ITIL v4:** Service Operation Practice
- **ISO 20000:** Clause 8.1 - Operational Planning and Control
- **COBIT 2019:** DSS01 - Managed Operations

Last Update: {{ meta.date }}
Next Review: [TODO: Date]
Contact: andreas.huemmer@adminsend.de

ewpage

Chapter 26

Runbooks and Standard Operations

26.1 Overview

This document contains standard runbooks, step-by-step guides, and troubleshooting guides for common operational tasks. The goal is to ensure consistent and efficient execution of standard operations.

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

26.2 Runbook Structure

26.2.1 Runbook Template

Each runbook follows this standardized structure:

```
# [RUNBOOK TITLE]

**Runbook ID:** RB-[NUMBER]
**Version:** [VERSION]
**Last Update:** [DATE]
**Responsible:** [NAME]

## Purpose
[Description of purpose and use case]

## Prerequisites
- [Required permissions]
- [Required tools]
- [Required knowledge]

## Estimated Duration
```

```
[TIME] minutes/hours

## Risk Assessment
- **Risk:** Low / Medium / High
- **Impact:** Low / Medium / High
- **Rollback possible:** Yes / No

## Steps
1. [Step 1]
2. [Step 2]
3. [Step 3]

## Validation
- [Validation step 1]
- [Validation step 2]

## Rollback
[Rollback procedure if required]

## Troubleshooting
[Common problems and solutions]

## References
- [Documentation]
- [Tickets]
```

26.3 System Management Runbooks

26.3.1 RB-001: Server Restart

Runbook ID: RB-001
Version: 1.0
Responsible: Andreas Huemmer

26.3.1.1 Purpose

Controlled restart of a server to fix problems or after updates.

26.3.1.2 Prerequisites

- Root/Administrator access to server
- Approval for restart (for production systems)
- Maintenance window (if required)

26.3.1.3 Estimated Duration

15-30 minutes

26.3.1.4 Risk Assessment

- **Risk:** Medium
- **Impact:** High (for production systems)
- **Rollback possible:** No

26.3.1.5 Steps

1. **Preparation**

```
# Check current system load
uptime
top

# Check running processes
ps aux | grep [critical_processes]

# Inform users (if required)
wall "System will restart in 5 minutes"
```

2. **Stop Services**

```
# Stop application services
systemctl stop [service_name]

# Check status
systemctl status [service_name]
```

3. **Perform Restart**

```
# Initiate restart
shutdown -r now
# or
reboot
```

4. **After Restart: Validation**

```
# Check system uptime
uptime

# Check services
systemctl status [service_name]

# Check logs
journalctl -xe
tail -f /var/log/syslog
```

26.3.1.6 Validation

☐ Server is reachable (ping, SSH)
☐ All critical services running
☐ No errors in system logs

☐ Monitoring shows green status
☐ Application is functional

26.3.2 RB-002: Service Restart

Runbook ID: RB-002
Version: 1.0
Responsible: Andreas Huemmer

26.3.2.1 Purpose

Restart a single service without system restart.

26.3.2.2 Prerequisites

- Sudo/Administrator rights
- Service name known

26.3.2.3 Estimated Duration

5-10 minutes

26.3.2.4 Steps

1. **Check Service Status**

   ```
   # Linux
   systemctl status [service_name]

   # Windows
   Get-Service [service_name]
   ```

2. **Stop Service**

   ```
   # Linux
   systemctl stop [service_name]

   # Windows
   Stop-Service [service_name]
   ```

3. **Wait and Validate**

   ```
   # Confirm process end
   ps aux | grep [service_name]

   # Check ports released
   netstat -tulpn | grep [port]
   ```

4. **Start Service**

```
# Linux
systemctl start [service_name]

# Windows
Start-Service [service_name]
```

5. **Validation**

```
# Check status
systemctl status [service_name]

# Check logs
journalctl -u [service_name] -f
```

26.3.2.5 Validation

- ☐ Service running (Status: active/running)
- ☐ No errors in logs
- ☐ Port is bound
- ☐ Application responds

26.4 Database Management Runbooks

26.4.1 RB-010: Database Backup

Runbook ID: RB-010
Version: 1.0
Responsible: Database Administrator

26.4.1.1 Purpose

Manual database backup before critical changes.

26.4.1.2 Prerequisites

- Database admin rights
- Sufficient storage space
- Backup directory exists

26.4.1.3 Estimated Duration

15-60 minutes (depending on DB size)

26.4.1.4 Steps

PostgreSQL:

```
# Full Backup
pg_dump -U postgres -F c -b -v -f /backup/db_$(date +%Y%m%d_%H%M%S).backup [database_name]
```

```
# Schema-only Backup
pg_dump -U postgres -s -f /backup/schema_$(date +%Y%m%d_%H%M%S).sql [database_name]
```

MySQL/MariaDB:

```
# Full Backup
mysqldump -u root -p --single-transaction --routines --triggers [database_name] > /backup/db_$(

# All Databases
mysqldump -u root -p --all-databases > /backup/all_dbs_$(date +%Y%m%d_%H%M%S).sql
```

26.4.1.5 Validation

- ☐ Backup file created
- ☐ Backup size plausible
- ☐ Backup integrity checked
- ☐ Backup location documented

26.5 Network Management Runbooks

26.5.1 RB-020: Add Firewall Rule

Runbook ID: RB-020
Version: 1.0
Responsible: Thomas Weber

26.5.1.1 Purpose

Adding a new firewall rule.

26.5.1.2 Prerequisites

- Firewall admin rights
- Change ticket approved
- Rule details documented

26.5.1.3 Estimated Duration

15-30 minutes

26.5.1.4 Steps

1. **Document Rule Details**
    - Source IP/Network
    - Destination IP/Network
    - Port/Protocol
    - Action (Allow/Deny)
    - Justification

2. **Add Rule**

   iptables (Linux):

   ```
   # Add rule
   iptables -A INPUT -s [source_ip] -p tcp --dport [port] -j ACCEPT

   # Save rule
   iptables-save > /etc/iptables/rules.v4
   ```

   firewalld (Linux):

   ```
   # Open port
   firewall-cmd --permanent --add-port=[port]/tcp

   # Reload
   firewall-cmd --reload
   ```

3. **Validation**

   ```
   # Check rule
   iptables -L -n -v

   # Test connectivity
   telnet [target_ip] [port]
   nc -zv [target_ip] [port]
   ```

26.5.1.5 Validation

- ☐ Rule is active
- ☐ Connectivity works
- ☐ No unwanted side effects
- ☐ Rule documented

26.6 Troubleshooting Guides

26.6.1 General Troubleshooting Methodology

1. **Identify Problem**
   - Collect symptoms
   - Note error messages
   - Time of occurrence
2. **Gather Information**
   - Analyze logs
   - Check monitoring data
   - Identify changes
3. **Form Hypothesis**
   - List possible causes
   - Assess probability
   - Prioritize

4. **Test**
    - Test hypothesis
    - Document results
    - Next hypothesis
5. **Implement Solution**
    - Perform corrective action
    - Validate
    - Document
6. **Prevention**
    - Root cause analysis
    - Identify improvements
    - Implement

26.7 Processes and Responsibilities

26.7.1 RACI Matrix

Activity	CIO	Ops Manager	Ops Team	On-Call
Runbook Creation	C	A	R	C
Runbook Execution	I	C	R	R
Runbook Update	I	A	R	C
Troubleshooting	I	C	R	R

Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed

---

Last Update: {{ meta.date }}
Next Review: [TODO: Date]
Contact: andreas.huemmer@adminsend.de

ewpage

Chapter 27

Tooling and Access Methods

27.1 Overview

This document describes the tools and systems used, access methods and URLs, as well as authentication methods for the IT service. The goal is to provide a central overview of all relevant tools and their access.

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

27.2 Tool Categories

27.2.1 Tool Categories Overview

Category	Number of Tools	Main Responsible	Criticality
Monitoring & Observability	[TODO]	Andreas Huemmer	High
Infrastructure Management	[TODO]	Andreas Huemmer	High
Security & Compliance	[TODO]	Thomas Weber	High
Development & Deployment	[TODO]	Andreas Huemmer	Medium
Collaboration & Communication	[TODO]	Peter Fischer	Medium
Documentation & Knowledge	[TODO]	Andreas Huemmer	Medium
Backup & Recovery	[TODO]	Andreas Huemmer	High

27.3 Monitoring and Observability

27.3.1 System Monitoring

27.3.1.1 [TODO: Monitoring Tool Name]

- **Purpose:** System and infrastructure monitoring
- **URL:** [TODO: https://monitoring.example.com]
- **Access:** VPN + SSO
- **Authentication:** AdminSend GmbH SSO
- **Responsible:** Andreas Huemmer
- **Support:** [TODO: Support Contact]
- **Documentation:** [TODO: Documentation URL]

Main Functions: - Server monitoring (CPU, RAM, Disk, Network) - Service monitoring (Uptime, Response Time) - Alerting and notifications - Dashboards and visualization

---

27.4 Infrastructure Management

27.4.1 Configuration Management Database (CMDB)

27.4.1.1 NetBox

- **Purpose:** CMDB and IPAM
- **URL:** {{ netbox.url }}
- **Access:** VPN + Username/Password
- **Authentication:** Local accounts or LDAP
- **Responsible:** Andreas Huemmer
- **API:** {{ netbox.api_url }}
- **Documentation:** https://docs.netbox.dev/

Main Functions: - Device inventory - IP address management (IPAM) - Rack management - Cable documentation - Virtualization tracking

---

27.5 Security and Compliance

27.5.1 Security Information and Event Management (SIEM)

27.5.1.1 [TODO: SIEM Tool Name]

- **Purpose:** Security event monitoring and analysis
- **URL:** [TODO: https://siem.example.com]
- **Access:** VPN + SSO
- **Authentication:** AdminSend GmbH SSO
- **Responsible:** Thomas Weber
- **Support:** [TODO: Support Contact]

Main Functions: - Security event aggregation - Threat detection - Incident response - Compliance reporting

27.6 Access Methods

27.6.1 VPN Access

27.6.1.1 Corporate VPN

- **Purpose:** Secure remote access
- **URL:** [TODO: https://vpn.example.com]
- **Client:** [TODO: VPN Client Name]
- **Authentication:** AdminSend GmbH AD + MFA
- **Responsible:** Thomas Weber
- **Support:** julia.becker@adminsend.de

Connection Instructions: 1. Install VPN client 2. Import/configure profile 3. Connect with AD credentials + MFA 4. Validate connection

---

27.6.2 SSH Access

27.6.2.1 SSH Bastion Host

- **Purpose:** Secure SSH access to servers
- **Hostname:** [TODO: bastion.example.com]
- **Port:** 22
- **Authentication:** SSH Keys + MFA
- **Responsible:** Andreas Huemmer

Connection Instructions:

```
# Generate SSH key (if not exists)
ssh-keygen -t ed25519 -C "your_email@example.com"

# Add public key to bastion host
# (by admin)

# Connect to bastion host
ssh -i ~/.ssh/id_ed25519 username@bastion.example.com

# From bastion to target server
ssh username@target-server
```

27.7 Authentication Methods

27.7.1 Single Sign-On (SSO)

27.7.1.1 AdminSend GmbH SSO

- **Provider:** [TODO: SSO Provider]
- **Protocol:** SAML 2.0 / OAuth 2.0 / OpenID Connect
- **MFA:** Required for all external access
- **Session Timeout:** 8 hours
- **Responsible:** Thomas Weber

Supported Applications: - [TODO: List of SSO-integrated applications]

27.7.2 API Authentication

27.7.2.1 API Tokens

- **Usage:** Programmatic access to APIs
- **Generation:** Via respective tool interface
- **Rotation:** Every 90 days
- **Storage:** Secrets management system
- **Responsible:** Andreas Huemmer

Best Practices: - Never commit tokens in code - Minimal permissions (Least Privilege) - Regular rotation - Monitor token usage

---

27.8 Emergency Access

27.8.1 Break-Glass Accounts

27.8.1.1 Emergency Admin Account

- **Purpose:** Emergency access in case of SSO failure
- **Storage:** Sealed envelope in safe
- **Access:** Only by Anna Schmidt or Thomas Weber
- **Logging:** Every use is logged and reviewed
- **Password Rotation:** Quarterly

Usage Process: 1. Identify and document emergency 2. Obtain approval from CIO/CISO 3. Open envelope and document 4. Perform access 5. Log all actions 6. Change password and seal new envelope 7. Create incident report

---

27.9 Processes and Responsibilities

27.9.1 RACI Matrix

Activity	CIO	CISO	Ops Manager	Ops Team
Tool Selection	A	C	R	C
Tool Implementation	C	C	A	R
Access Management	C	A	R	I
Tool Maintenance	I	C	A	R
Tool Review	A	C	R	C
Emergency Access	A	A	C	I

Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed

---

Last Update: {{ meta.date }}
Next Review: [TODO: Date]
Contact: andreas.huemmer@adminsend.de

ewpage

Chapter 28

Known Issues and FAQ

28.1 Overview

This document contains known issues and workarounds, frequently asked questions (FAQ), and troubleshooting tips for the IT service. The goal is to provide quick solutions for recurring problems and increase support efficiency.

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

28.2 Known Issues

28.2.1 Issue Tracking

All known issues are captured in the ticketing system with the label “Known Issue” and documented here.

Responsible: Andreas Huemmer
Review Cycle: Monthly

28.2.2 KI-001: [TODO: Issue Title]

Status: Open / In Progress / Resolved
Priority: P1 (Critical) / P2 (High) / P3 (Medium) / P4 (Low)
Created: [TODO: Date]
Last Update: [TODO: Date]
Ticket ID: [TODO: Ticket Number]

28.2.2.1 Description

[TODO: Detailed description of the issue]

28.2.2.2 Affected Systems

- [TODO: System 1]
- [TODO: System 2]

28.2.2.3 Symptoms

- [TODO: Symptom 1]
- [TODO: Symptom 2]

28.2.2.4 Root Cause

[TODO: Cause of the issue, if known]

28.2.2.5 Workaround

```
[TODO: Step-by-step workaround]
1. Step 1
2. Step 2
3. Step 3
```

28.2.2.6 Permanent Solution

- **Status:** Planned / In Development / Tested / Deployed
- **ETA:** [TODO: Expected date]
- **Responsible:** [TODO: Name]

28.3 Frequently Asked Questions (FAQ)

28.3.1 General Questions

28.3.1.1 Q: How do I reach IT support?

A: IT support can be reached through the following channels: - **Email:** julia.becker@adminsend.de - **Phone:** +49 89 12345678-111 - **Ticketing System:** [TODO: URL] - **Chat:** [TODO: Chat Channel]

Support Hours: - Mon-Fri: 08:00-18:00 - 24/7 for critical incidents (P1)

28.3.1.2 Q: How do I create a support ticket?

A: Support tickets can be created through the following methods:

1. **Web Portal:**
   - Go to [TODO: Ticketing URL]
   - Log in with SSO
   - Click “New Ticket”
   - Fill out form and submit
2. **Email:**

- Email to julia.becker@adminsend.de
- Subject: Brief problem description
- Content: Detailed description, screenshots

3. **Phone:**
   - Call +49 89 12345678-111
   - Describe problem
   - Note ticket number

28.3.2 Access and Authentication

28.3.2.1 Q: I forgot my password. What should I do?

A: Password reset via self-service portal:

1. Go to [TODO: Self-Service URL]
2. Click "Forgot Password"
3. Enter username or email
4. Answer security questions or receive code via email/SMS
5. Set new password

Alternative: Contact IT support

28.3.2.2 Q: How do I set up MFA (Multi-Factor Authentication)?

A: MFA setup:

1. Go to [TODO: MFA Portal URL]
2. Log in with current password
3. Choose MFA method:
   - **Authenticator App** (recommended): Scan QR code
   - **SMS:** Verify phone number
   - **Hardware Token:** Register token
4. Generate backup codes and store securely
5. Test MFA

Important: Keep backup codes in a safe place!

28.3.3 Applications

28.3.3.1 Q: The application loads very slowly. What can I do?

A: Performance troubleshooting:

1. **Clear browser cache:**
   - Chrome: Ctrl+Shift+Del
   - Firefox: Ctrl+Shift+Del
   - Edge: Ctrl+Shift+Del
2. **Disable browser extensions:**

- Temporarily disable all extensions
- Test if performance improves

3. **Test another browser:**
   - Try Chrome, Firefox, or Edge
4. **Check network:**
   - Run speed test
   - Check VPN connection
5. **Check system resources:**
   - Open Task Manager
   - Check CPU/RAM usage
   - Close other programs

If problem persists: Create ticket with: - Browser and version - Affected application - Time of problem - Screenshot

---

28.3.4 Email

28.3.4.1 Q: I cannot send emails. What should I do?

A: Email sending troubleshooting:

1. **Check outbox:**
   - Are emails stuck in outbox?
   - Error message present?
2. **Check mailbox size:**
   - Is mailbox full?
   - Archive/delete old emails
3. **Check attachments:**
   - Are attachments too large? (Max: [TODO: Size])
   - Compress attachments or send via file sharing
4. **Check recipient address:**
   - Is email address correct?
   - Typo?
5. **Spam filter:**
   - Was email marked as spam?

If problem persists: Contact IT support

28.3.5 Files and Storage

28.3.5.1 Q: I accidentally deleted a file. Can it be recovered?

A: File recovery:

1. **Check recycle bin:**
   - Windows: Recycle Bin on desktop
   - macOS: Trash in dock
   - Linux: Trash folder

2. **Network drive:**
   - Check previous versions (Right-click → Properties → Previous Versions)
   - Shadow copies available?
3. **Backup recovery:**
   - Create ticket (P3 - Medium)
   - Provide filename, path, and approximate deletion date
   - IT team restores from backup

Important: The sooner reported, the higher the success rate!

Backup Retention: - Daily backups: 30 days - Weekly backups: 90 days - Monthly backups: 1 year

---

28.4 Troubleshooting Tips

28.4.1 General Troubleshooting Steps

1. **Restart:**
   - Often the simplest solution
   - Restart computer, application, or service
2. **Document error:**
   - Create screenshot
   - Note error message
   - Record time
3. **Reproduce:**
   - Trigger problem again
   - Document steps
4. **Isolate:**
   - Different computer?
   - Different browser?
   - Different network?
5. **Research:**
   - Check known issues (this document)
   - Search wiki
   - Ask colleagues
6. **Escalate:**
   - Create ticket
   - Contact IT support

28.5 Self-Service Resources

28.5.1 Documentation

- **Wiki:** [TODO: Wiki URL]
- **Video Tutorials:** [TODO: Video URL]
- **Manuals:** [TODO: Manual URL]

28.5.2 Tools

- **Self-Service Portal:** [TODO: Portal URL]
- **Password Reset:** [TODO: Reset URL]
- **Software Download:** [TODO: Download URL]

28.6 Feedback and Improvements

28.6.1 Give Feedback

Do you have suggestions for improving this document or IT services?

Contact: - **Email:** andreas.huemmer@adminsend.de - **Feedback Form:** [TODO: Form URL]

28.6.2 Document Updates

This document is regularly updated based on: - New known issues - Frequently asked questions - User feedback - Process improvements

Review Cycle: Monthly
Responsible: Andreas Huemmer

Last Update: {{ meta.date }}
Next Review: [TODO: Date]
Contact: andreas.huemmer@adminsend.de

ewpage

Chapter 29

Contacts, Escalation, and Vendors

29.1 Overview

This document contains contact lists, escalation paths, vendors and suppliers, as well as support contacts for the IT service. The goal is to ensure quick access to relevant contact information in all situations.

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

29.2 Internal Contacts

29.2.1 Management

29.2.1.1 Chief Executive Officer (CEO)

- **Name:** Max Mustermann
- **Title:** Chief Executive Officer
- **Email:** max.mustermann@adminsend.de
- **Phone:** +49 89 12345678-100
- **Department:** Management
- **Availability:** Mon-Fri 09:00-18:00
- **Escalation:** Only for critical business impact situations

29.2.1.2 Chief Information Officer (CIO)

- **Name:** Anna Schmidt
- **Title:** Chief Information Officer
- **Email:** anna.schmidt@adminsend.de
- **Phone:** +49 89 12345678-200
- **Department:** IT
- **Availability:** Mon-Fri 08:00-18:00

- **Escalation:** IT strategic decisions, critical incidents

29.2.1.3 Chief Information Security Officer (CISO)

- **Name:** Thomas Weber
- **Title:** Chief Information Security Officer
- **Email:** thomas.weber@adminsend.de
- **Phone:** +49 89 12345678-300
- **Department:** IT Security
- **Availability:** Mon-Fri 08:00-18:00, 24/7 for security incidents
- **Escalation:** Security incidents, compliance questions

29.2.2 IT Operations

29.2.2.1 IT Operations Manager

- **Name:** Andreas Huemmer
- **Title:** IT Operations Manager
- **Email:** andreas.huemmer@adminsend.de
- **Phone:** +49 89 12345678-250
- **Department:** IT Operations
- **Availability:** Mon-Fri 08:00-18:00, On-call for P1 incidents
- **Responsibility:** Overall responsibility for IT operations

29.2.2.2 Service Desk Lead

- **Name:** Julia Becker
- **Title:** Service Desk Lead
- **Email:** julia.becker@adminsend.de
- **Phone:** +49 89 12345678-111
- **Department:** Service Desk
- **Availability:** Mon-Fri 08:00-18:00
- **Responsibility:** First-level support, ticket management

29.3 On-Call and Standby

29.3.1 On-Call Rotation

29.3.1.1 Primary On-Call

- **Current:** [TODO: Name]
- **Email:** [TODO: Email]
- **Phone:** [TODO: Mobile Number]
- **Availability:** 24/7
- **Rotation:** Weekly (Monday 08:00)

29.3.1.2 Secondary On-Call (Backup)

- **Current:** [TODO: Name]
- **Email:** [TODO: Email]
- **Phone:** [TODO: Mobile Number]
- **Availability:** 24/7
- **Rotation:** Weekly (Monday 08:00)

29.3.2 On-Call Calendar

- **URL:** [TODO: Calendar URL]
- **Access:** All IT staff
- **Update:** Automatic through rotation tool

29.4 Escalation Paths

29.4.1 Incident Escalation

29.4.1.1 Level 1: Service Desk

- **Contact:** julia.becker@adminsend.de
- **Phone:** +49 89 12345678-111
- **Availability:** Mon-Fri 08:00-18:00
- **Responsibility:** First-level support, ticket creation

Escalation to Level 2: - P1: Immediately - P2: After 1 hour without solution - P3: After 4 hours without solution - P4: After 8 hours without solution

---

29.4.1.2 Level 2: Operations Team

- **Contact:** [TODO: ops-team@example.com]
- **Phone:** [TODO: Phone Number]
- **Availability:** Mon-Fri 08:00-18:00, On-call 24/7
- **Responsibility:** Second-level support, technical analysis

Escalation to Level 3: - P1: After 2 hours without solution - P2: After 4 hours without solution - P3: After 8 hours without solution

---

29.4.1.3 Level 3: IT Operations Manager

- **Contact:** andreas.huemmer@adminsend.de
- **Phone:** +49 89 12345678-250
- **Availability:** Mon-Fri 08:00-18:00, On-call for P1
- **Responsibility:** Coordination, resource allocation

Escalation to Level 4: - P1: After 4 hours without solution - P2: After 8 hours without solution - When external support required

29.4.1.4 Level 4: CIO

- **Contact:** anna.schmidt@adminsend.de
- **Phone:** +49 89 12345678-200
- **Availability:** Mon-Fri 08:00-18:00, reachable for critical incidents
- **Responsibility:** Strategic decisions, management communication

Escalation to Level 5: - Critical business impact - Media relevance - Regulatory implications

---

29.5 External Vendors and Suppliers

29.5.1 Hardware Vendor

29.5.1.1 [TODO: Hardware Vendor Name]

- **Contact Person:** [TODO: Name]
- **Email:** [TODO: Email]
- **Phone:** [TODO: Phone Number]
- **Support Hotline:** [TODO: Support Number]
- **Contract Number:** [TODO: Contract Number]
- **Contract End:** [TODO: Date]
- **Support Level:** [TODO: 24/7, Business Hours]
- **Response Time:** [TODO: 4h, 8h, Next Business Day]
- **Services:**
  - Hardware delivery
  - Warranty and repair
  - Spare parts service

29.5.2 Software Vendor

29.5.2.1 [TODO: Software Vendor Name]

- **Contact Person:** [TODO: Name]
- **Email:** [TODO: Email]
- **Phone:** [TODO: Phone Number]
- **Support Portal:** [TODO: URL]
- **Contract Number:** [TODO: Contract Number]
- **License Count:** [TODO: Number]
- **Contract End:** [TODO: Date]
- **Support Level:** [TODO: Standard, Premium, Enterprise]
- **Services:**
  - Software updates
  - Bug fixes
  - Technical support
  - Training

29.5.3 Cloud Provider

29.5.3.1 [TODO: Cloud Provider Name]

- **Account Manager:** [TODO: Name]
- **Email:** [TODO: Email]
- **Phone:** [TODO: Phone Number]
- **Support Hotline:** [TODO: Support Number]
- **Account ID:** [TODO: Account ID]
- **Support Plan:** [TODO: Basic, Business, Enterprise]
- **Services:**
  - Cloud infrastructure
  - 24/7 support
  - SLA: [TODO: Availability]
  - Technical support

29.6 Emergency Contacts

29.6.1 Critical Situations

29.6.1.1 Fire / Medical Emergency

- **Emergency:** 112
- **Building Security:** [TODO: Phone Number]
- **First Aid:** [TODO: First Responder Contact]

29.6.1.2 Police

- **Emergency:** 110
- **Local Police:** [TODO: Phone Number]

29.6.1.3 Building Management

- **Facility Management:** [TODO: Phone Number]
- **Availability:** 24/7
- **Responsibility:** Building security, access

29.7 Communication Channels

29.7.1 Internal Communication

29.7.1.1 Email

- **Primary:** Official communication
- **Distribution Lists:**

  - IT Team: [TODO: it-team@example.com]
  - Management: [TODO: management@example.com]
  - All Hands: [TODO: all@example.com]

29.7.1.2 Chat / Collaboration

- **Platform:** [TODO: Chat Platform]
- **Channels:**
  - #it-operations: Daily operations
  - #incidents: Incident communication
  - #changes: Change communication
  - #general: General communication

29.8 Contact Update

29.8.1 Update Process

1. **Report Changes:**
   - Email to andreas.huemmer@adminsend.de
   - Provide new contact details
   - Specify effective date
2. **Validation:**
   - IT Operations Manager reviews change
   - Obtain approval (if required)
3. **Update:**
   - Update document
   - Update CMDB
   - Inform affected teams
4. **Verification:**
   - Test new contact details
   - Obtain confirmation

29.8.2 Review Cycle

- **Frequency:** Quarterly
- **Responsible:** Andreas Huemmer

29.9 Quick Reference

29.9.1 Most Important Contacts

Situation	Contact	Phone
IT Support	Julia Becker	+49 89 12345678-111
Critical Incident	IT Operations Manager	+49 89 12345678-250
Security Incident	Thomas Weber	+49 89 12345678-300

Situation	Contact	Phone
Management Escalation	Anna Schmidt	+49 89 12345678-200
Emergency (Fire/Medical)	Emergency	112
Police	Emergency	110

Last Update: {{ meta.date }}
Next Review: [TODO: Date]
Contact: andreas.huemmer@adminsend.de

ewpage

Chapter 30

Compliance and Audits

30.1 Purpose and Scope

This document describes the compliance and audit processes for AdminSend GmbH. It defines relevant standards, audit processes, compliance controls, evidence, and non-compliance risks to ensure adherence to regulatory and contractual requirements.

Scope: All IT systems, processes, and activities of AdminSend GmbH

Responsible: {{ meta.compliance_officer }} ({{ meta.compliance_officer_email }})

30.2 Compliance Fundamentals

30.2.1 Compliance Definition

Compliance: Adherence to laws, regulations, standards, policies, and contractual obligations

Objectives: - **Legal Certainty:** Avoidance of legal consequences - **Risk Minimization:** Reduction of compliance risks - **Reputation:** Protection of company reputation - **Trust:** Trust of customers and partners - **Competitive Advantage:** Certifications as differentiator

30.2.2 Compliance Areas

Regulatory Compliance: - Legal requirements (GDPR, IT Security Act) - Industry-specific regulations - Data protection requirements

Standard Compliance: - ISO standards (ISO 27001, ISO 20000) - Industry standards (PCI-DSS, HIPAA) - Best practice frameworks (ITIL, COBIT)

Contractual Compliance: - Service Level Agreements (SLAs) - Customer contracts - Supplier contracts

Internal Compliance: - Company policies - IT guidelines - Security standards

30.3 Relevant Standards and Regulations

30.3.1 ISO/IEC 27001:2013 - Information Security Management

Description: International standard for Information Security Management Systems (ISMS)

Scope: All IT systems and information processing

Status: {{ meta.iso27001_status }}
Certification: {{ meta.iso27001_certification }}
Certification Body: {{ meta.iso27001_certifier }}
Valid Until: {{ meta.iso27001_valid_until }}

Core Requirements: - Establish, implement, operate, monitor, review, maintain, and improve ISMS - Risk assessment and treatment - 114 controls in 14 categories (Annex A) - Management review and continuous improvement

Audit Frequency: - **Certification Audit:** Every 3 years - **Surveillance Audit:** Annually - **Internal Audit:** Quarterly

Responsible: Thomas Weber

30.3.2 ISO/IEC 20000-1:2018 - IT Service Management

Description: International standard for IT Service Management Systems (SMS)

Scope: IT service management processes

Status: {{ meta.iso20000_status }}

Core Requirements: - Service Management System (SMS) - Service planning and delivery - Relationship processes - Resolution processes - Control processes

Alignment: ITIL v4 Framework

Responsible: Andreas Huemmer

30.3.3 GDPR - General Data Protection Regulation

Description: EU regulation for the protection of personal data

Scope: All processing of personal data

Effective: May 25, 2018

Core Requirements: - Lawfulness of processing (Art. 6) - Information obligations (Art. 13, 14) - Data subject rights (Art. 15-22) - Technical and organizational measures (Art. 32) - Breach notification obligation (Art. 33, 34) - Data protection impact assessment (Art. 35)

Fines: Up to 20 million EUR or 4% of worldwide annual revenue

Data Protection Officer: {{ meta.data_protection_officer }}

Record of Processing Activities: {{ meta.processing_activities_register }}

30.4 Compliance Management Process

30.4.1 Process Overview

```
Compliance
Identification



Gap
Analysis



Remediation
Planning



Implementation
& Monitoring



Audit &
Assessment



Continuous
Improvement
```

30.5 Audit Processes

30.5.1 Audit Types

30.5.1.1 Internal Audits

Purpose: Self-assessment of compliance

Frequency: - **ISO 27001:** Quarterly - **ISO 20000:** Quarterly - **GDPR:** Semi-annually - **Internal Policies:** Annually

Execution: - Internal Audit Team - Independent from audited area - Risk-based approach

Process: 1. Audit planning 2. Audit preparation 3. Audit execution (Interviews, document review, tests) 4. Document findings 5. Create audit report 6. Plan corrective actions 7. Follow-up

Responsible: Internal Audit Team

30.5.1.2 External Audits (Certification)

Purpose: Certification according to standards

Frequency: - **Certification Audit:** Every 3 years - **Surveillance Audit:** Annually - **Re-certification:** Every 3 years

Execution: - Accredited certification body - Independent auditors - Document review and on-site audit

Audit Phases: - **Stage 1:** Document review - **Stage 2:** On-site audit - **Surveillance:** Annual monitoring

Certification Bodies: - ISO 27001: {{ meta.iso27001_certifier }} - ISO 20000: {{ meta.iso20000_certifier }}

30.6 Compliance Controls and Evidence

30.6.1 Technical Controls

30.6.1.1 Access Control

Controls: - Multi-Factor Authentication (MFA) - Role-Based Access Control (RBAC) - Least Privilege Principle - Privileged Access Management (PAM) - Access Reviews (quarterly)

Evidence: - Access Control Matrix - User Access Reports - Access Review Protocols - MFA Activation Rate

30.6.1.2 Encryption

Controls: - Encryption at Rest (AES-256) - Encryption in Transit (TLS 1.3) - Key Management - Certificate Management

Evidence: - Encryption Inventory - Key Management Procedures - Certificate Inventory - Encryption Scan Reports

---

30.7 Non-Compliance Risks and Measures

30.7.1 Risk Categories

30.7.1.1 Legal Risks

Risks: - Fines and penalties - Legal proceedings - Liability claims - Executive liability

Examples: - GDPR violation: Up to 20 million EUR or 4% annual revenue - PCI-DSS violation: Up to $500,000 per month - SOX violation: Criminal consequences

Mitigations: - Establish compliance program - Regular audits - Involve legal counsel - Insurance (Cyber insurance)

30.8 Compliance Metrics and Reporting

30.8.1 Key Performance Indicators (KPIs)

KPI	Target	Measurement	Frequency
Audit Findings Rate	< 5 Major Findings	Findings per audit	After audit
Corrective Action Closure Rate	> 95% on time	Closed CAs / Total CAs	Monthly
Training Completion Rate	100%	Completed trainings / Required trainings	Quarterly
Policy Review Compliance	100%	Reviewed policies / Total policies	Annually
Incident Reporting Time	< 24h	Time from incident to report	Per incident
Vulnerability Remediation SLA	> 95%	Remediated in SLA / Total	Monthly

30.9 References

- ISO/IEC 27001:2013 - Information Security Management
- ISO/IEC 20000-1:2018 - IT Service Management
- GDPR (EU 2016/679) - General Data Protection Regulation
- BSI IT-Grundschutz Compendium
- PCI-DSS v4.0 - Payment Card Industry Data Security Standard
- SOX (Sarbanes-Oxley Act)
- COBIT 2019 - Control Objectives for Information and Related Technologies

---

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Classification: internal
Last Update: {{ meta.date }}

ewpage

Chapter 31

Appendix: Checklists and Templates

31.1 Overview

This document contains a collection of checklists, templates for standard documents, and forms for IT operations. The goal is to ensure consistent and efficient execution of standard processes.

Document Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Organization: AdminSend GmbH

31.2 Checklists

31.2.1 Incident Management Checklists

31.2.1.1 Incident Response Checklist

```
# Incident Response Checklist

**Incident ID:** [INC-XXXXX]
**Date/Time:** [YYYY-MM-DD HH:MM]
**Reporter:** [Name]
**Priority:** P1 / P2 / P3 / P4

## Phase 1: Detection and Recording
- [ ] Incident detected and documented
- [ ] Priority assessed (P1-P4)
- [ ] Ticket created
- [ ] Affected systems identified
- [ ] Affected users identified
- [ ] Initial symptoms documented

## Phase 2: Classification and Prioritization
- [ ] Incident category assigned
```

```
- [ ] Business impact assessed
- [ ] Urgency assessed
- [ ] Priority confirmed
- [ ] Assigned to responsible person

## Phase 3: Diagnosis and Investigation
- [ ] Logs analyzed
- [ ] Monitoring data checked
- [ ] Similar incidents searched
- [ ] Known issues checked
- [ ] Root cause identified (if possible)

## Phase 4: Resolution and Recovery
- [ ] Solution approach defined
- [ ] Approval obtained (if required)
- [ ] Solution implemented
- [ ] Functionality validated
- [ ] Users informed

## Phase 5: Closure
- [ ] Incident resolved
- [ ] Documentation completed
- [ ] User confirmation obtained
- [ ] Ticket closed
- [ ] Lessons learned documented (for P1/P2)

## Communication
- [ ] Stakeholders informed
- [ ] Status updates communicated
- [ ] Solution communicated

**Processed by:** [Name]
**Completed on:** [YYYY-MM-DD HH:MM]
**Duration:** [HH:MM]
```

31.2.2 Change Management Checklists

31.2.2.1 Standard Change Checklist

```
# Standard Change Checklist

**Change ID:** [CHG-XXXXX]
**Date:** [YYYY-MM-DD]
**Change Manager:** [Name]

## Planning
- [ ] Change request created
```

```
- [ ] Description complete
- [ ] Justification documented
- [ ] Risk assessment performed
- [ ] Affected systems identified
- [ ] Dependencies identified
- [ ] Time window defined
- [ ] Resources allocated

## Approval
- [ ] Change category determined (Standard/Normal/Emergency)
- [ ] Approver identified
- [ ] Approval obtained
- [ ] CAB review (if required)

## Preparation
- [ ] Implementation plan created
- [ ] Rollback plan created
- [ ] Test plan created
- [ ] Communication plan created
- [ ] Backup performed
- [ ] Test environment validated

## Implementation
- [ ] Maintenance window started
- [ ] Users informed
- [ ] Change implemented
- [ ] Step-by-step documented
- [ ] Problems documented

## Validation
- [ ] Functionality tested
- [ ] Performance validated
- [ ] Monitoring checked
- [ ] No errors in logs
- [ ] User acceptance test (if required)

## Closure
- [ ] Change successful
- [ ] Documentation updated
- [ ] CMDB updated
- [ ] Users informed
- [ ] Change closed
- [ ] Lessons learned (if problems)

## Rollback (if required)
- [ ] Rollback decision made
- [ ] Rollback plan executed
- [ ] System restored
```

```
- [ ] Validation performed
- [ ] Incident created for analysis

**Change Manager:** [Name]
**Implemented by:** [Name]
**Status:** Successful / Rollback / Cancelled
```

31.2.3 Backup and Recovery Checklists

31.2.3.1 Backup Verification Checklist

```
# Backup Verification Checklist

**Date:** [YYYY-MM-DD]
**Performed by:** [Name]

## Backup Status
- [ ] All scheduled backups performed
- [ ] Backup logs checked
- [ ] No errors in logs
- [ ] Backup sizes plausible
- [ ] Backup times acceptable

## Backup Integrity
- [ ] Checksums validated
- [ ] Backup files readable
- [ ] No corruption detected
- [ ] Encryption working

## Restore Test
- [ ] Random backup selected
- [ ] Test environment prepared
- [ ] Restore performed
- [ ] Data validated
- [ ] Functionality tested
- [ ] Restore time measured

## Documentation
- [ ] Test result documented
- [ ] Problems documented
- [ ] Improvements identified
- [ ] Report created

## Systems Checked
- [ ] Databases
- [ ] File servers
- [ ] Application servers
```

```
- [ ] Configurations
- [ ] Virtualization hosts

**Result:** Successful / With Problems / Failed
**Next Test:** [YYYY-MM-DD]
```

31.3 Templates

31.3.1 Incident Report Template

```
# Incident Report

**Incident ID:** [INC-XXXXX]
**Date:** [YYYY-MM-DD]
**Created by:** [Name]

## Executive Summary
[Brief summary of the incident for management]

## Incident Details
- **Priority:** P1 / P2 / P3 / P4
- **Category:** [Category]
- **Affected Systems:** [List]
- **Affected Users:** [Number/Description]
- **Start:** [YYYY-MM-DD HH:MM]
- **End:** [YYYY-MM-DD HH:MM]
- **Duration:** [HH:MM]

## Timeline
| Time | Event | Action |
|---|---|---|
| HH:MM | [Event] | [Action] |
| HH:MM | [Event] | [Action] |

## Root Cause
[Detailed description of the cause]

## Impact
- **Business Impact:** [Description]
- **Financial Impact:** [Estimate]
- **Reputation Damage:** [Assessment]
- **Affected Services:** [List]

## Solution
[Description of implemented solution]
```

```
## Improvement Measures
1. [Measure 1] - Responsible: [Name] - Deadline: [Date]
2. [Measure 2] - Responsible: [Name] - Deadline: [Date]
3. [Measure 3] - Responsible: [Name] - Deadline: [Date]

## Lessons Learned
- [Lesson 1]
- [Lesson 2]
- [Lesson 3]

## Attachments
- [Logs]
- [Screenshots]
- [Monitoring Data]

**Created by:** [Name]
**Approved by:** Andreas Huemmer
**Date:** [YYYY-MM-DD]
```

31.3.2 Change Request Template

```
# Change Request

**Change ID:** [CHG-XXXXX]
**Date:** [YYYY-MM-DD]
**Requester:** [Name]

## Change Details
- **Title:** [Short title]
- **Category:** Standard / Normal / Emergency
- **Priority:** Low / Medium / High / Critical
- **Planned Date:** [YYYY-MM-DD]
- **Planned Time:** [HH:MM - HH:MM]
- **Duration:** [Estimated duration]

## Description
[Detailed description of the change]

## Justification
[Why is this change necessary?]

## Affected Systems
- [System 1]
- [System 2]
- [System 3]

## Affected Users
```

```
[Number and description of affected users]

## Risk Assessment
- **Risk:** Low / Medium / High
- **Impact:** Low / Medium / High
- **Probability:** Low / Medium / High

## Risks and Mitigations
| Risk | Probability | Impact | Mitigation |
|---|---|---|---|
| [Risk 1] | [L/M/H] | [L/M/H] | [Measure] |
| [Risk 2] | [L/M/H] | [L/M/H] | [Measure] |

## Implementation Plan
1. [Step 1]
2. [Step 2]
3. [Step 3]

## Rollback Plan
1. [Step 1]
2. [Step 2]
3. [Step 3]

## Test Plan
1. [Test 1]
2. [Test 2]
3. [Test 3]

## Communication Plan
- **Before Change:** [Who, When, How]
- **During Change:** [Who, When, How]
- **After Change:** [Who, When, How]

## Approvals
- [ ] Technical Approval: [Name] - [Date]
- [ ] Business Approval: [Name] - [Date]
- [ ] CAB Approval: [Name] - [Date]

**Requester:** [Name]
**Change Manager:** Andreas Huemmer
**Status:** Requested / Approved / Rejected / Implemented
```

31.4 Forms

31.4.1 Access Request Form

```
# Access Request

**Requester:** [Name]
**Date:** [YYYY-MM-DD]
**Department:** [Department]

## User Information
- **Name:** [Full Name]
- **Email:** [Email Address]
- **Phone:** [Phone Number]
- **Department:** [Department]
- **Position:** [Position]
- **Manager:** [Manager Name]

## Access Details
- **System/Application:** [Name]
- **Access Level:** Read / Write / Admin
- **Justification:** [Business justification]
- **Duration:** Permanent / Temporary until [Date]

## Required Permissions
- [ ] [Permission 1]
- [ ] [Permission 2]
- [ ] [Permission 3]

## Approvals
- [ ] Manager Approval: [Name] - [Date]
- [ ] Data Owner Approval: [Name] - [Date]
- [ ] Security Approval: [Name] - [Date]

## IT Processing
- **Processed by:** [Name]
- **Date:** [YYYY-MM-DD]
- **Access Granted:** Yes / No
- **Comments:** [Comments]

**Status:** Requested / Approved / Rejected / Implemented
```

31.5 Processes and Responsibilities

31.5.1 RACI Matrix

Activity	Ops Manager	Ops Team	Service Desk	User
Checklist Creation	A	R	C	-
Template Creation	A	R	C	-
Checklist Usage	C	R	R	-
Template Usage	C	R	R	R
Update	A	R	C	-

Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed

---

Last Update: {{ meta.date }}
Next Review: [TODO: Date]
Contact: andreas.huemmer@adminsend.de

ewpage