

Contents

1 TSC (SOC 2) Compliance Handbook	4
2 System Description	5
2.1 1. Purpose	5
2.2 2. Organization Information	6
2.3 3. System Boundaries	6
2.4 4. Infrastructure	7
2.5 5. Software	8
2.6 6. People	8
2.7 7. Processes	9
2.8 8. Data	10
2.9 9. Service Commitments and System Requirements	10
2.10 10. Subservice Organizations	11
2.11 11. Changes to the System	12
3 System Boundaries and Interfaces	13
3.1 1. Purpose	13
3.2 2. System Boundaries	13
3.3 3. External Interfaces	14
3.4 4. Data Flows Across Boundaries	14
3.5 5. Trust Boundaries	15
3.6 6. Complementary User Entity Controls (CUEC)	15
4 System Components	16
4.1 1. Purpose	16
4.2 2. Infrastructure	16
4.3 3. Software	17
4.4 4. People	17
4.5 5. Processes	18
4.6 6. Data	18
5 Roles and Responsibilities	19
5.1 1. Purpose	19
5.2 2. Management Roles	19
5.3 3. Operational Roles	19
5.4 4. Compliance Roles	20
5.5 5. RACI Matrix	20

5.6 6. Training and Qualifications	21
6 Control Environment	22
6.1 1. Purpose	22
6.2 2. Organizational Structure	22
6.3 3. Integrity and Ethical Values	23
6.4 4. Commitment to Competence	23
6.5 5. Management Philosophy	23
6.6 6. Organizational Structure	23
6.7 7. Oversight	24
7 CC1: Control Environment	25
7.1 1. Purpose	25
7.2 2. CC1.1: Organizational Structure	25
7.3 3. CC1.2: Board Independence	25
7.4 4. CC1.3: Management Oversight	25
7.5 5. CC1.4: Competence	26
7.6 6. CC1.5: Accountability	26
8 CC2: Communication and Information	27
8.1 1. CC2.1: Internal Communication	27
8.2 2. CC2.2: External Communication	27
8.3 3. CC2.3: Information Quality	27
9 CC3: Risk Assessment	29
9.1 1. CC3.1: Risk Identification	29
9.2 2. CC3.2: Risk Analysis	29
9.3 3. CC3.3: Risk Response	29
10 CC4: Monitoring Activities	31
10.1 1. CC4.1: Ongoing Monitoring	31
10.2 2. CC4.2: Separate Evaluations	31
10.3 3. CC4.3: Evaluation and Communication	31
11 CC5: Control Activities	33
11.1 1. CC5.1: Selection and Development of Control Activities	33
11.2 2. CC5.2: Technology Controls	33
11.3 3. CC5.3: Policies and Procedures	33
12 CC6-CC9: Security Controls	35
12.1 1. CC6: Logical and Physical Access Controls	35
12.2 2. CC7: System Operations	35
12.3 3. CC8: Change Management	36
12.4 4. CC9: Risk Mitigation	36
13 A1: Availability	37
13.1 1. A1.1: Availability Commitments	37
13.2 2. A1.2: System Monitoring	37
13.3 3. A1.3: Incident Management	37

13.4 4. A1.4: Recovery Procedures	37
14 PI1: Processing Integrity	39
14.1 1. PI1.1: Processing Commitments	39
14.2 2. PI1.2: Input Validation	39
14.3 3. PI1.3: Processing Controls	39
14.4 4. PI1.4: Output Controls	39
15 C1: Confidentiality	41
15.1 1. C1.1: Confidentiality Commitments	41
15.2 2. C1.2: Access Controls	41
15.3 3. C1.3: Encryption	41
15.4 4. C1.4: Data Disposal	41
16 P1-P8: Privacy	43
16.1 1. P1: Notice and Communication	43
16.2 2. P2-P3: Choice and Consent	43
16.3 3. P4-P5: Collection and Use	43
16.4 4. P6: Access	43
16.5 5. P7: Disclosure to Third Parties	44
16.6 6. P8: Quality	44
17 Appendix: Control Matrix	45
17.1 1. Purpose	45
17.2 2. Common Criteria (Security) - Required	45
17.3 3. Availability (Optional)	45
17.4 4. Processing Integrity (Optional)	46
17.5 5. Confidentiality (Optional)	46
17.6 6. Privacy (Optional)	46
18 Appendix: Glossary	47
18.1 TSC-Specific Terms	47

Chapter 1

TSC (SOC 2) Compliance Handbook

Document Metadata

- **Created on:** 2026-02-10
 - **Author:** Andreas Huemmer [andreas.huemmer@adminsend.de]
 - **Version:** 0.0.5
 - **Type:** TSC Handbook (SOC 2)
-

ewpage

Chapter 2

System Description

Document ID: TSC-0010

Organization: AdminSend GmbH

Owner: IT Operations Manager

Approved by: CIO

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

2.1 1. Purpose

This document describes the service system of AdminSend GmbH that is subject to the SOC 2 audit.

2.1.1 1.1 Objectives

- **System Description:** Complete description of the service system
- **Boundary Definition:** Clear delineation of system boundaries
- **Component Identification:** Identification of all system components
- **Service Commitments:** Documentation of service commitments

2.1.2 1.2 References

- **AICPA TSC:** Trust Services Criteria
- **SOC 2 Reporting:** Description Criteria for a Description of a Service Organization's System
- **Service Level Agreements:** [TODO: Reference to SLAs]

2.2 2. Organization Information

2.2.1 2.1 Service Organization

Organization: AdminSend GmbH

Address: Musterstraße 123, 80331 München

Country: Deutschland

Website: <https://www.adminsend.de>

Business Area: [TODO: e.g., Cloud Hosting, SaaS, Managed Services]

Founded: [TODO: Year]

Employees: [TODO: Number]

2.2.2 2.2 Service Description

Service Name: {{ meta.tsc.system_name }}

Service Type: [TODO: e.g., Cloud-based Application, Hosting Service]

Service Purpose: [TODO: Purpose of service]

Main Functions: - [TODO: Function 1] - [TODO: Function 2] - [TODO: Function 3]

2.2.3 2.3 Report Period

Report Type: [TODO: Type I / Type II]

Report Period: {{ meta.tsc.report_period }}

Report Date: [TODO: Date for Type I or End Date for Type II]

2.3 3. System Boundaries

2.3.1 3.1 In-Scope Systems

Systems within scope:

System ID	System Name	Type	Function	Location
[TODO: SYS-001]	[TODO: Web Application]	Application	Main application	[TODO: Cloud/On-Prem]
[TODO: SYS-002]	[TODO: Database Server]	Database	Data storage	[TODO: Cloud/On-Prem]
[TODO: SYS-003]	[TODO: API Gateway]	Infrastructure	API management	[TODO: Cloud/On-Prem]
[TODO: SYS-004]	[TODO: Load Balancer]	Infrastructure	Traffic distribution	[TODO: Cloud/On-Prem]

2.3.2 3.2 Out-of-Scope Systems

Systems outside scope:

System	Justification
[TODO: Internal HR System]	Not part of customer service
[TODO: Development Environment]	No production data
[TODO: Marketing Website]	No customer data

2.3.3 3.3 System Interfaces

External Interfaces:

Interface	Type	Purpose	Security
[TODO: Payment Gateway]	API	Payment processing	TLS 1.2+
[TODO: Email Service]	SMTP	Notifications	TLS
[TODO: Identity Provider]	SAML/OAuth	Authentication	HTTPS

2.4 4. Infrastructure

2.4.1 4.1 Physical Infrastructure

Hosting Model: [TODO: Cloud / On-Premises / Hybrid]

Cloud Provider (if applicable): - **Provider:** [TODO: AWS / Azure / GCP / Other] - **Regions:** [TODO: eu-central-1, us-east-1] - **Availability Zones:** [TODO: Number]

Data Centers (if On-Premises): - **Primary Data Center:** [TODO: Location] - **Secondary Data Center:** [TODO: Location] - **Certifications:** [TODO: ISO 27001, SOC 2]

2.4.2 4.2 Network Architecture

Network Segmentation: - **Production Network:** [TODO: VLAN/Subnet] - **Management Network:** [TODO: VLAN/Subnet] - **DMZ:** [TODO: VLAN/Subnet]

Network Security: - **Firewalls:** [TODO: Type and quantity] - **IDS/IPS:** [TODO: Yes/No, Type] - **DDoS Protection:** [TODO: Yes/No, Provider]

2.4.3 4.3 Compute Resources

Resource Type	Specification	Quantity	Purpose
[TODO: Web Servers]	[TODO: 4 vCPU, 16GB RAM]	[TODO: 3]	Application hosting
[TODO: Database Servers]	[TODO: 8 vCPU, 32GB RAM]	[TODO: 2]	Data storage
[TODO: Cache Servers]	[TODO: 2 vCPU, 8GB RAM]	[TODO: 2]	Performance

2.5 5. Software

2.5.1 5.1 Application Software

Application	Version	Vendor	Purpose
[TODO: Main Application]	[TODO: v2.5]	[TODO: Internal/Vendor]	Core service
[TODO: API Service]	[TODO: v1.3]	[TODO: Internal/Vendor]	API endpoints
[TODO: Admin Portal]	[TODO: v1.1]	[TODO: Internal/Vendor]	Administration

2.5.2 5.2 System Software

Software	Version	Purpose
[TODO: Operating System]	[TODO: Ubuntu 22.04]	Server OS
[TODO: Database]	[TODO: PostgreSQL 15]	Data storage
[TODO: Web Server]	[TODO: Nginx 1.24]	HTTP server
[TODO: Application Server]	[TODO: Node.js 18]	Runtime

2.5.3 5.3 Security Software

Software	Version	Purpose
[TODO: Antivirus]	[TODO: Latest]	Malware protection
[TODO: SIEM]	[TODO: Version]	Security monitoring
[TODO: Vulnerability Scanner]	[TODO: Version]	Vulnerability management
[TODO: Backup Software]	[TODO: Version]	Data backup

2.6 6. People

2.6.1 6.1 Organizational Structure

Management: - **CEO:** [TODO: Name] - **CTO:** [TODO: Name] - **CISO:** {{ meta.roles.ciso.name }} - **COO:** [TODO: Name]

Teams: - **Engineering:** [TODO: Number of employees] - **Operations:** [TODO: Number of employees] - **Security:** [TODO: Number of employees] - **Support:** [TODO: Number of employees]

2.6.2 6.2 Roles and Responsibilities

Role	Responsibilities	Count
[TODO: System Administrator]	System management, patching	[TODO: 3]

Role	Responsibilities	Count
[TODO: Security Engineer]	Security monitoring, incident response	[TODO: 2]
[TODO: Developer]	Application development	[TODO: 10]
[TODO: Support Engineer]	Customer support	[TODO: 5]

2.6.3 6.3 Training and Qualifications

Mandatory Training: - Security Awareness Training (annual) - Role-specific Technical Training
- Compliance Training

Certifications: - [TODO: CISSP, CISM, AWS Certified, etc.]

2.7 7. Processes

2.7.1 7.1 Operational Processes

Key Processes:

1. **Change Management**
 - Change request and approval
 - Testing and validation
 - Deployment and rollback
2. **Incident Management**
 - Incident detection and logging
 - Incident response and resolution
 - Post-incident review
3. **Monitoring and Alerting**
 - System health monitoring
 - Security event monitoring
 - Performance monitoring
4. **Backup and Recovery**
 - Regular backups
 - Backup testing
 - Disaster recovery procedures

2.7.2 7.2 Security Processes

Security Operations:

1. **Access Management**
 - User provisioning and deprovisioning
 - Access reviews
 - Privileged access management
2. **Vulnerability Management**
 - Regular vulnerability scans
 - Patch management

- Penetration testing

3. Security Monitoring

- Log collection and analysis
- Security event correlation
- Threat intelligence

2.8 8. Data

2.8.1 8.1 Data Types

Customer Data: - **Personal Information:** [TODO: Name, Email, etc.] - **Account Information:** [TODO: Credentials, Preferences] - **Transaction Data:** [TODO: Usage, Billing] - **Content Data:** [TODO: User-generated content]

System Data: - **Configuration Data:** System settings - **Log Data:** Audit logs, system logs - **Monitoring Data:** Metrics, alerts

2.8.2 8.2 Data Classification

Classification	Description	Examples
Public	Publicly available	Marketing materials
Internal	Internal use only	Policies, procedures
Confidential	Sensitive business data	Customer data, financial data
Restricted	Highly sensitive	Encryption keys, credentials

2.8.3 8.3 Data Flow

[TODO: Insert data flow diagram]

Main Data Flows:

1. User Registration:

- User → Web Application → Database
- Encryption: TLS 1.2+ in transit, AES-256 at rest

2. Data Processing:

- Application → Processing Service → Database
- Validation and integrity checks

3. Data Backup:

- Database → Backup Service → Offsite Storage
- Encrypted backups

2.9 9. Service Commitments and System Requirements

2.9.1 9.1 Service Level Agreements (SLAs)

Availability: - **Target:** [TODO: 99.9% uptime] - **Measurement:** Monthly uptime percentage - **Exclusions:** Planned maintenance windows

Performance: - **Response Time:** [TODO: < 200ms for 95% of requests] - **Throughput:** [TODO: 1000 requests/second]

Support: - **Response Time:** [TODO: < 1 hour for critical issues] - **Resolution Time:** [TODO: < 4 hours for critical issues]

2.9.2 9.2 Security Commitments

Data Protection: - Encryption of data in transit and at rest - Access control based on least privilege - Regular security assessments

Availability: - Redundant infrastructure - Disaster recovery capabilities - Regular backup testing

Confidentiality: - Confidentiality agreements with employees - Secure data disposal procedures - Access logging and monitoring

2.9.3 9.3 Compliance Requirements

Regulatory Compliance: - [TODO: GDPR, HIPAA, PCI-DSS, etc.]

Industry Standards: - [TODO: ISO 27001, NIST, CIS Controls]

2.10 10. Subservice Organizations

2.10.1 10.1 Subservice Providers

Provider	Service	SOC 2 Status	Carve-Out/Inclusive
[TODO: Cloud Provider]	Infrastructure	Type II available	Inclusive
[TODO: Email Service]	Email delivery	Type II available	Carve-Out
[TODO: Payment Processor]	Payment processing	Type II available	Carve-Out

2.10.2 10.2 Complementary User Entity Controls (CUEC)

Controls that require customer implementation:

1. **User Access Management**
 - Customers must implement strong password policies
 - Customers must enable multi-factor authentication
2. **Data Backup**
 - Customers must regularly export their data
 - Customers must test data restoration procedures
3. **Security Configuration**
 - Customers must configure security settings appropriately
 - Customers must review access logs regularly

2.11 11. Changes to the System

2.11.1 11.1 Significant Changes During Report Period

Date	Change Description	Impact	Approval
[TODO: 2026-01-15]	[TODO: New feature deployment]	[TODO: Low]	[TODO: CTO]
[TODO: 2026-02-01]	[TODO: Infrastructure upgrade]	[TODO: Medium]	[TODO: CTO]

2.11.2 11.2 Planned Changes

Upcoming Changes: - [TODO: Description of planned changes]

Document History:

Version	Date	Author	Changes
0.1	<pre>{{ meta.document.last_updated_by}} }}</pre>	<pre>{{ meta.document.last_updated_by}} }}</pre>	Initial creation

ewpage

Chapter 3

System Boundaries and Interfaces

Document ID: TSC-0020

Organization: AdminSend GmbH

Owner: IT Operations Manager

Approved by: CIO

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

3.1 1. Purpose

This document defines the boundaries of the service system and documents all interfaces to external systems and organizations.

3.2 2. System Boundaries

3.2.1 2.1 In-Scope Components

Infrastructure: - [TODO: Production servers] - [TODO: Database servers] - [TODO: Network components] - [TODO: Security appliances]

Applications: - [TODO: Main application] - [TODO: API services] - [TODO: Admin portal]

Processes: - [TODO: Change management] - [TODO: Incident management] - [TODO: Access management]

Personnel: - [TODO: Operations team] - [TODO: Security team] - [TODO: Development team]

3.2.2 2.2 Out-of-Scope Components

Component	Justification	Alternative Control
[TODO: HR System]	No customer data	Separate security controls

Component	Justification	Alternative Control
[TODO: Dev Environment]	No production data	Isolated environment
[TODO: Marketing Tools]	No direct service relation	Standard IT controls

3.3 3. External Interfaces

3.3.1 3.1 Customer Interfaces

User Interfaces:

Interface	Type	Access Method	Security
[TODO: Web Portal]	HTTPS	Browser	TLS 1.2+, MFA
[TODO: Mobile App]	HTTPS	Native App	TLS 1.2+, Certificate Pinning
[TODO: API]	REST API	HTTP Client	OAuth 2.0, API Keys

3.3.2 3.2 Subservice Organization Interfaces

Subservice Org	Interface Type	Purpose	Security Controls
[TODO: Cloud Provider]	API	Infrastructure	IAM, Encryption
[TODO: Email Service]	SMTP/API	Notifications	TLS, API Keys
[TODO: Payment Gateway]	REST API	Payments	TLS, Tokenization

3.4 4. Data Flows Across Boundaries

3.4.1 4.1 Inbound Data Flows

Data Flow	Source	Destination	Data Type	Security
[TODO: User Input]	Customer Browser	Web Application	Form Data	TLS 1.2+, Input Validation
[TODO: API Requests]	Customer System	API Gateway	JSON	OAuth 2.0, Rate Limiting

3.4.2 4.2 Outbound Data Flows

Data Flow	Source	Destination	Data Type	Security
[TODO: API Response]	Application	Customer System	JSON	TLS 1.2+, Data Filtering
[TODO: Email Notifications]	Application	Customer Email	Email	TLS, SPF/DKIM

3.5 5. Trust Boundaries

3.5.1 5.1 External Trust Boundary

Internet-facing Components: - Web Application (DMZ) - API Gateway (DMZ) - Load Balancer (DMZ)

Security Controls: - Web Application Firewall (WAF) - DDoS Protection - Rate Limiting - Input Validation

3.5.2 5.2 Internal Trust Boundaries

Production vs. Non-Production: - Separate networks - No direct connectivity - Controlled data migration

3.6 6. Complementary User Entity Controls (CUEC)

3.6.1 6.1 Customer Responsibilities

Access Management: - Customers must implement strong authentication - Customers must regularly review user access - Customers must promptly remove access for terminated users

Data Protection: - Customers must classify their data appropriately - Customers must configure access controls - Customers must encrypt sensitive data before upload (if applicable)

Document History:

Version	Date	Author	Changes
0.1	<pre> {{ meta.document.lastupdate.defaults.author }} {{ meta.document.lastupdate.defaults.author }}</pre>		Initial creation

ewpage

Chapter 4

System Components

Document ID: TSC-0030

Organization: AdminSend GmbH

Owner: IT Operations Manager

Approved by: CIO

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

4.1 1. Purpose

This document describes the five main components of the service system: Infrastructure, Software, People, Processes, and Data.

4.2 2. Infrastructure

4.2.1 2.1 Physical Infrastructure

Hosting: [TODO: Cloud/On-Premises/Hybrid]

Provider: [TODO: AWS/Azure/GCP]

Regions: [TODO: Regions]

Data Centers: [TODO: Locations]

4.2.2 2.2 Compute Resources

Resource	Specification	Quantity	Purpose
[TODO: Web Servers]	[TODO: Spec]	[TODO: #]	Application
[TODO: DB Servers]	[TODO: Spec]	[TODO: #]	Data Storage

4.2.3 2.3 Network Infrastructure

- **Firewalls:** [TODO: Details]
- **Load Balancers:** [TODO: Details]
- **VPN:** [TODO: Details]

4.3 3. Software

4.3.1 3.1 Application Software

Application	Version	Purpose
[TODO: Main App]	[TODO: v1.0]	Core Service
[TODO: API]	[TODO: v1.0]	Integration

4.3.2 3.2 System Software

Software	Version	Purpose
[TODO: OS]	[TODO: Version]	Operating System
[TODO: Database]	[TODO: Version]	Data Storage

4.3.3 3.3 Security Software

Software	Version	Purpose
[TODO: AV]	[TODO: Latest]	Malware Protection
[TODO: SIEM]	[TODO: Version]	Security Monitoring

4.4 4. People

4.4.1 4.1 Organization

Management: - CEO: [TODO: Name] - CTO: [TODO: Name] - CISO: {{ meta.roles.ciso.name }}

Teams: - Engineering: [TODO: #] employees - Operations: [TODO: #] employees - Security: [TODO: #] employees

4.4.2 4.2 Roles

Role	Responsibilities	Count
[TODO: Admin]	System Management	[TODO: #]
[TODO: Engineer]	Development	[TODO: #]

4.5 5. Processes

4.5.1 5.1 Operational Processes

- **Change Management:** [TODO: Description]
- **Incident Management:** [TODO: Description]
- **Monitoring:** [TODO: Description]

4.5.2 5.2 Security Processes

- **Access Management:** [TODO: Description]
- **Vulnerability Management:** [TODO: Description]
- **Security Monitoring:** [TODO: Description]

4.6 6. Data

4.6.1 6.1 Data Types

Customer Data: - Personal Information - Account Information - Transaction Data

System Data: - Configuration Data - Log Data - Monitoring Data

4.6.2 6.2 Data Classification

Classification	Description
Public	Publicly available
Internal	Internal use only
Confidential	Sensitive data
Restricted	Highly sensitive

Document History:

Version	Date	Author	Changes
0.1	<pre> {{\n meta.document.lastupdateofauthors.author\n }}\n}}</pre>	<pre> {{\n meta.document.lastupdateofauthors.author\n }}\n}}</pre>	Initial creation

ewpage

Chapter 5

Roles and Responsibilities

Document ID: TSC-0040

Organization: AdminSend GmbH

Owner: IT Operations Manager

Approved by: CIO

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

5.1 1. Purpose

This document defines the roles and responsibilities for TSC compliance and SOC 2 audits.

5.2 2. Management Roles

5.2.1 2.1 Executive Management

CEO: - **Name:** [TODO: Name] - **Responsibilities:** - Overall responsibility for compliance - Policy approval - Resource allocation

CTO: - **Name:** [TODO: Name] - **Responsibilities:** - Technical strategy - System architecture - Change approval

CISO: - **Name:** {{ meta.roles.ciso.name }} - **Email:** {{ meta.roles.ciso.email }} - **Responsibilities:** - Security strategy - Risk management - Incident response

5.3 3. Operational Roles

5.3.1 3.1 System Administration

System Administrators: - **Count:** [TODO: #] - **Responsibilities:** - System maintenance - Patch management - Backup management

5.3.2 3.2 Security Operations

Security Engineers: - **Count:** [TODO: #] - **Responsibilities:** - Security monitoring - Incident response - Vulnerability management

5.3.3 3.3 Development

Developers: - **Count:** [TODO: #] - **Responsibilities:** - Application development - Code reviews - Security testing

5.4 4. Compliance Roles

5.4.1 4.1 SOC 2 Program Manager

Name: [TODO: Name]

Email: [TODO: Email]

Responsibilities: - SOC 2 program management - Audit coordination - Documentation - Compliance reporting

5.4.2 4.2 Service Auditor

Firm: {{ meta.roles.auditor.name }}

Contact: {{ meta.roles.auditor.email }}

Responsibilities: - Conduct SOC 2 audit - Test control effectiveness - Issue SOC 2 report

5.5 5. RACI Matrix

5.5.1 5.1 Control Environment

Activity	CEO	CTO	CISO	Ops	Audit
Policy Approval	A	C	R	I	I
Risk Assessment	C	C	A/R	C	I
Control Design	I	C	A	R	C
Control Testing	I	I	C	R	A

5.5.2 5.2 Operations

Activity	CTO	CISO	Ops	Dev	Audit
Change Management	A	C	R	R	I
Incident Response	C	A	R	C	I
Monitoring	C	A	R	I	I
Backup/Recovery	A	C	R	I	I

Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed

5.6 6. Training and Qualifications

5.6.1 6.1 Mandatory Training

- Security Awareness (annual)
- Role-specific Training
- Compliance Training

5.6.2 6.2 Certifications

Security Team: - [TODO: CISSP, CISM, CEH]

Operations Team: - [TODO: AWS Certified, Azure Certified]

Document History:

Version	Date	Author	Changes
0.1	<pre>{{meta.document.lastmodified}}}}</pre>	<pre>{{meta.defaults.author}}</pre>	Initial creation

ewpage

Chapter 6

Control Environment

Document ID: TSC-0050

Organization: AdminSend GmbH

Owner: IT Operations Manager

Approved by: CIO

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

6.1 1. Purpose

This document describes the Control Environment according to TSC Common Criteria CC1.

6.2 2. Organizational Structure

6.2.1 2.1 Governance Structure

Board of Directors: - [TODO: Composition] - [TODO: Meetings: Quarterly]

Executive Management: - CEO, CTO, CISO, CFO, COO - [TODO: Meetings: Monthly]

Management Committees: - Security Committee - Change Advisory Board - Incident Response Team

6.2.2 2.2 Reporting Lines

[TODO: Insert organizational chart]

6.3 3. Integrity and Ethical Values

6.3.1 3.1 Code of Conduct

Principles: - Integrity and Honesty - Respect and Fairness - Compliance with Laws - Confidentiality

Enforcement: - Annual acknowledgment required - Violations reported to HR - Disciplinary actions

6.3.2 3.2 Conflict of Interest

Policy: - Annual disclosure required - Review by management - Mitigation measures

6.4 4. Commitment to Competence

6.4.1 4.1 Job Descriptions

Key Roles: - System Administrator - Security Engineer - Developer - Support Engineer

Requirements: - Education - Experience - Certifications - Skills

6.4.2 4.2 Training Program

Onboarding: - Security Awareness - System Training - Policy Review

Ongoing: - Annual Security Training - Role-specific Training - Compliance Updates

6.5 5. Management Philosophy

6.5.1 5.1 Risk Management

Approach: - Risk-based decision making - Regular risk assessments - Risk treatment plans

6.5.2 5.2 Performance Management

Metrics: - System availability - Security incidents - Compliance status

Reviews: - Monthly operational reviews - Quarterly management reviews - Annual strategic reviews

6.6 6. Organizational Structure

6.6.1 6.1 Authority and Responsibility

Delegation: - Clear authority levels - Documented responsibilities - Approval matrices

6.6.2 6.2 Human Resources

Policies: - Background checks - Confidentiality agreements - Termination procedures

6.7 7. Oversight

6.7.1 7.1 Internal Audit

Program: - Annual audit plan - Risk-based approach - Follow-up on findings

6.7.2 7.2 External Audit

SOC 2 Audit: - Annual Type II audit - Service auditor: {{ meta.roles.auditor.name }} - Report distribution

Document History:

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

ewpage

Chapter 7

CC1: Control Environment

Document ID: TSC-0100

Organization: AdminSend GmbH

Owner: IT Operations Manager

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

7.1 1. Purpose

This document describes the controls for TSC Common Criteria CC1: Control Environment.

7.2 2. CC1.1: Organizational Structure

Control Objective: The entity demonstrates a commitment to integrity and ethical values.

Control Activities: - Code of Conduct established and communicated - Annual acknowledgment by all employees - Ethics hotline available - Disciplinary actions for violations

Evidence: - [TODO: Code of Conduct document] - [TODO: Employee acknowledgments] - [TODO: Ethics training records]

7.3 3. CC1.2: Board Independence

Control Objective: The board of directors demonstrates independence from management.

Control Activities: - [TODO: Board composition] - [TODO: Independent directors] - [TODO: Oversight responsibilities]

7.4 4. CC1.3: Management Oversight

Control Objective: Management establishes oversight responsibilities.

Control Activities: - Organizational structure defined - Reporting lines established - Authority and responsibility assigned - Performance evaluations conducted

7.5 5. CC1.4: Competence

Control Objective: The entity demonstrates a commitment to attract, develop, and retain competent individuals.

Control Activities: - Job descriptions defined - Hiring process includes background checks - Training programs established - Performance reviews conducted

7.6 6. CC1.5: Accountability

Control Objective: The entity holds individuals accountable for their responsibilities.

Control Activities: - Performance metrics defined - Regular performance reviews - Consequences for non-performance - Rewards for good performance

Document History:

Version	Date	Author	Changes
0.1	<pre> {{ meta.document.lastupdate.defaults.author }}}</pre>	<pre> {{ meta.document.lastupdate.defaults.author }}}</pre>	Initial creation

ewpage

Chapter 8

CC2: Communication and Information

Document ID: TSC-0110

Organization: AdminSend GmbH

Owner: IT Operations Manager

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

8.1 1. CC2.1: Internal Communication

Control Activities: - Policies and procedures documented - Regular team meetings - Internal communication channels - Policy updates communicated

8.2 2. CC2.2: External Communication

Control Activities: - Service commitments documented - Customer communication procedures - Incident notification process - Regulatory reporting procedures

8.3 3. CC2.3: Information Quality

Control Activities: - Information accuracy verified - Timely information delivery - Information accessibility - Information retention policies

Document History:

Version	Date	Author	Changes
0.1	<pre> {{ meta.document.lastmap[defaults.author }}}</pre>	<pre> {{ meta[}}}</pre>	Initial creation

ewpage

Chapter 9

CC3: Risk Assessment

Document ID: TSC-0120

Organization: AdminSend GmbH

Owner: IT Operations Manager

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

9.1 1. CC3.1: Risk Identification

Control Activities: - Annual risk assessment conducted - Risk identification process - Threat and vulnerability analysis - Risk register maintained

9.2 2. CC3.2: Risk Analysis

Control Activities: - Risk likelihood and impact assessed - Risk prioritization - Risk treatment options evaluated - Risk acceptance criteria defined

9.3 3. CC3.3: Risk Response

Control Activities: - Risk treatment plans developed - Controls implemented - Residual risk monitored - Risk reporting to management

Document History:

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

ewpage

Chapter 10

CC4: Monitoring Activities

Document ID: TSC-0130

Organization: AdminSend GmbH

Owner: IT Operations Manager

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

10.1 1. CC4.1: Ongoing Monitoring

Control Activities: - Continuous monitoring of controls - Performance metrics tracked - Automated monitoring tools - Regular control testing

10.2 2. CC4.2: Separate Evaluations

Control Activities: - Internal audits conducted - External audits (SOC 2) - Penetration testing - Vulnerability assessments

10.3 3. CC4.3: Evaluation and Communication

Control Activities: - Findings documented - Remediation plans developed - Management reporting - Follow-up on corrective actions

Document History:

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

ewpage

Chapter 11

CC5: Control Activities

Document ID: TSC-0140

Organization: AdminSend GmbH

Owner: IT Operations Manager

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

11.1 1. CC5.1: Selection and Development of Control Activities

Control Activities: - Controls designed to mitigate risks - Preventive and detective controls - Manual and automated controls - Control documentation

11.2 2. CC5.2: Technology Controls

Control Activities: - Access controls implemented - Encryption for data protection - Network security controls - Endpoint protection

11.3 3. CC5.3: Policies and Procedures

Control Activities: - Policies established and documented - Procedures defined - Regular policy reviews - Policy compliance monitoring

Document History:

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

ewpage

Chapter 12

CC6-CC9: Security Controls

Document ID: TSC-0150

Organization: AdminSend GmbH

Owner: IT Operations Manager

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

12.1 1. CC6: Logical and Physical Access Controls

12.1.1 1.1 CC6.1: Logical Access

Control Activities: - User authentication required - Multi-factor authentication for privileged access - Access based on least privilege - Regular access reviews

12.1.2 1.2 CC6.2: Physical Access

Control Activities: - Badge access to data centers - Visitor logs maintained - Security cameras - Physical security reviews

12.2 2. CC7: System Operations

12.2.1 2.1 CC7.1: Detection and Monitoring

Control Activities: - Security monitoring tools deployed - Log collection and analysis - Alerting for security events - Incident detection procedures

12.2.2 2.2 CC7.2: System Capacity

Control Activities: - Capacity monitoring - Performance metrics tracked - Capacity planning process - Scalability testing

12.3 3. CC8: Change Management

12.3.1 3.1 CC8.1: Change Authorization

Control Activities: - Change request process - Change approval required - Testing before deployment - Rollback procedures

12.4 4. CC9: Risk Mitigation

12.4.1 4.1 CC9.1: Risk Assessment

Control Activities: - Annual risk assessment - Risk treatment plans - Risk monitoring - Risk reporting to management

12.4.2 4.2 CC9.2: Vendor Management

Control Activities: - Vendor risk assessment - Vendor contracts include security requirements - Vendor performance monitoring - Annual vendor reviews

Document History:

Version	Date	Author	Changes
0.1	<pre> {{ meta.document.lastmodified.defaults.author }}}</pre>	<pre> {{ meta.modifiedBy }}}</pre>	Initial creation

ewpage

Chapter 13

A1: Availability

Document ID: TSC-0200

Organization: AdminSend GmbH

Owner: IT Operations Manager

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

13.1 1. A1.1: Availability Commitments

Service Level Agreement: - **Target Uptime:** [TODO: 99.9%] - **Measurement Period:** Monthly - **Exclusions:** Planned maintenance

Control Activities: - SLA documented and communicated - Availability monitoring - SLA reporting to customers - SLA breach procedures

13.2 2. A1.2: System Monitoring

Control Activities: - 24/7 system monitoring - Automated alerting - Performance metrics tracked - Capacity planning

13.3 3. A1.3: Incident Management

Control Activities: - Incident detection and logging - Incident response procedures - Escalation procedures - Post-incident reviews

13.4 4. A1.4: Recovery Procedures

Control Activities: - Backup procedures defined - Regular backup testing - Disaster recovery plan - Recovery time objectives (RTO) defined

Document History:

Version	Date	Author	Changes
0.1	<pre>{{meta.document.lastupdate}}</pre>	<pre>{{adults.author}}</pre>	Initial creation

ewpage

Chapter 14

PI1: Processing Integrity

Document ID: TSC-0240

Organization: AdminSend GmbH

Owner: IT Operations Manager

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

14.1 1. PI1.1: Processing Commitments

Processing Integrity Commitments: - Complete processing - Valid processing - Accurate processing - Timely processing - Authorized processing

14.2 2. PI1.2: Input Validation

Control Activities: - Input validation rules defined - Data type and format checks - Range and boundary checks - Rejection of invalid inputs

14.3 3. PI1.3: Processing Controls

Control Activities: - Processing logic documented - Error handling procedures - Transaction logging - Processing reconciliation

14.4 4. PI1.4: Output Controls

Control Activities: - Output validation - Output completeness checks - Output distribution controls - Output retention policies

Document History:

Version	Date	Author	Changes
0.1	<pre> {{ meta.document.lastmap[defaults.author }}}</pre>	<pre> {{ meta[defaults] }}}</pre>	Initial creation

ewpage

Chapter 15

C1: Confidentiality

Document ID: TSC-0280

Organization: AdminSend GmbH

Owner: IT Operations Manager

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

15.1 1. C1.1: Confidentiality Commitments

Confidentiality Commitments: - Confidential data identified - Confidentiality agreements in place - Access restrictions enforced - Secure disposal procedures

15.2 2. C1.2: Access Controls

Control Activities: - Access based on need-to-know - Role-based access control - Regular access reviews - Privileged access management

15.3 3. C1.3: Encryption

Control Activities: - Data encrypted in transit (TLS 1.2+) - Data encrypted at rest (AES-256) - Key management procedures - Encryption key rotation

15.4 4. C1.4: Data Disposal

Control Activities: - Secure deletion procedures - Media sanitization - Certificate of destruction - Disposal verification

Document History:

Version	Date	Author	Changes
0.1	<pre> {{ meta.document.lastmap[defaults.author }}}</pre>	<pre> {{ meta[defaults] }}}</pre>	Initial creation

ewpage

Chapter 16

P1-P8: Privacy

Document ID: TSC-0320

Organization: AdminSend GmbH

Owner: IT Operations Manager

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

16.1 1. P1: Notice and Communication

Control Activities: - Privacy notice published - Privacy policy communicated - Changes to privacy policy notified - Privacy contact information provided

16.2 2. P2-P3: Choice and Consent

Control Activities: - Consent obtained for data collection - Opt-in/opt-out mechanisms - Consent withdrawal procedures - Consent records maintained

16.3 3. P4-P5: Collection and Use

Control Activities: - Data collection limited to stated purposes - Data minimization practiced - Purpose limitation enforced - Secondary use requires consent

16.4 4. P6: Access

Control Activities: - Data subject access requests processed - Data provided in accessible format - Identity verification for access requests - Access request logging

16.5 5. P7: Disclosure to Third Parties

Control Activities: - Third-party disclosures documented - Data processing agreements in place
- Third-party compliance verified - Disclosure notifications

16.6 6. P8: Quality

Control Activities: - Data accuracy procedures - Data correction mechanisms - Data quality monitoring - Data retention policies

Document History:

Version	Date	Author	Changes
0.1	<pre> {{ meta.document.lastmodified }} {{ adults.author }}</pre>		Initial creation

ewpage

Chapter 17

Appendix: Control Matrix

Document ID: TSC-0400

Organization: AdminSend GmbH

Owner: IT Operations Manager

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

17.1 1. Purpose

This document contains the complete TSC Control Matrix with all implemented controls.

17.2 2. Common Criteria (Security) - Required

Control ID	Control Description	Control Owner	Test Frequency
CC1.1	Integrity and ethical values	CISO	Annual
CC1.2	Board independence	CEO	Annual
CC2.1	Internal communication	CISO	Quarterly
CC3.1	Risk identification	CISO	Annual
CC4.1	Ongoing monitoring	Security Team	Continuous
CC5.1	Control activities	Operations	Quarterly
CC6.1	Logical access	Security Team	Quarterly
CC7.1	Detection and monitoring	Security Team	Continuous
CC8.1	Change authorization	Change Manager	Per change
CC9.1	Risk assessment	CISO	Annual

17.3 3. Availability (Optional)

Control ID	Control Description	Control Owner	Test Frequency
A1.1	Availability commitments	Operations	Monthly
A1.2	System monitoring	Operations	Continuous
A1.3	Incident management	Operations	Per incident
A1.4	Recovery procedures	Operations	Quarterly

17.4 4. Processing Integrity (Optional)

Control ID	Control Description	Control Owner	Test Frequency
PI1.1	Processing commitments	Development	Quarterly
PI1.2	Input validation	Development	Per release
PI1.3	Processing controls	Development	Per release
PI1.4	Output controls	Development	Per release

17.5 5. Confidentiality (Optional)

Control ID	Control Description	Control Owner	Test Frequency
C1.1	Confidentiality commitments	CISO	Annual
C1.2	Access controls	Security Team	Quarterly
C1.3	Encryption	Security Team	Quarterly
C1.4	Data disposal	Operations	Per disposal

17.6 6. Privacy (Optional)

Control ID	Control Description	Control Owner	Test Frequency
P1	Notice and communication	Legal/Privacy	Annual
P2-P3	Choice and consent	Legal/Privacy	Per collection
P4-P5	Collection and use	Legal/Privacy	Quarterly
P6	Access	Legal/Privacy	Per request
P7	Disclosure	Legal/Privacy	Per disclosure
P8	Quality	Data Team	Quarterly

Document History:

Version	Date	Author	Changes
0.1	<pre> {{meta.document.last_update}} {{meta.defaults.author}} }}</pre>		Initial creation

Chapter 18

Appendix: Glossary

Document ID: TSC-0440

Organization: AdminSend GmbH

Owner: IT Operations Manager

Version: 1.0.0

Status: Draft / In Review / Approved

Classification: internal

Last Updated: {{ meta.document.last_updated }}

18.1 TSC-Specific Terms

18.1.1 A

AICPA: American Institute of Certified Public Accountants

Availability: The system is available for operation and use as committed or agreed.

18.1.2 C

Carve-Out Method: Subservice organization controls are not included in the service organization's description.

Common Criteria (CC): Security criteria required for all SOC 2 reports.

Complementary User Entity Controls (CUEC): Controls that the service organization assumes will be implemented by user entities.

Confidentiality: Information designated as confidential is protected as committed or agreed.

18.1.3 I

Inclusive Method: Subservice organization controls are included in the service organization's description.

18.1.4 P

Processing Integrity: System processing is complete, valid, accurate, timely, and authorized.

Privacy: Personal information is collected, used, retained, disclosed, and disposed of in conformity with privacy commitments.

18.1.5 S

Service Auditor: Independent CPA firm that performs the SOC 2 audit.

Service Organization: Entity that provides services to user entities.

SOC 2: Service Organization Control 2 report.

Subservice Organization: Service organization used by another service organization.

18.1.6 T

Trust Services Criteria (TSC): Criteria for SOC 2 reports developed by AICPA.

Type I Report: Report on the design of controls at a point in time.

Type II Report: Report on the design and operating effectiveness of controls over a period of time.

18.1.7 U

User Entity: Entity that uses the services of a service organization.

Document History:

Version	Date	Author	Changes
0.1	<pre> {{ meta.document.lastupdate.defaults.author }}</pre>	<pre> {{ meta.document.lastupdate.defaults.author }}</pre>	Initial creation

ewpage