Contents

1 Information Security Policy (Top Management) 14
1.1 1. Purpose and Objectives . . . 14
1.2 2. Scope . . . 15
1.3 3. Principles . . . 15
1.4 4. Responsibilities . . . 16
1.5 5. Communication and Enforcement . . . 16
1.6 6. Review and Update . . . 16
1.7 7. Approval . . . 17

2 ISMS Organization, Roles and Responsibilities 18
2.1 1. ISMS Organization . . . 18
2.2 2. Roles and Responsibilities . . . 20
2.3 3. RACI Matrix for BSI IT-Grundschutz Processes . . . 20
2.4 4. Escalation Paths . . . 21
2.5 5. Communication and Reporting . . . 22
2.6 6. Resources and Budget . . . 22
2.7 7. Review and Update . . . 22

3 Document Control and Document Register 23
3.1 1. Purpose and Scope . . . 23
3.2 2. Storage and Access . . . 23
3.3 3. Document Lifecycle . . . 24
3.4 4. Document Register . . . 26
3.5 5. Change Log . . . 26
3.6 6. Quality Assurance . . . 26
3.7 7. Training and Awareness . . . 27
3.8 8. Monitoring and Improvement . . . 27

4 Scope and Information Domain (Boundaries) 28
4.1 1. Purpose and Objectives . . . 28
4.2 2. Scope Definition . . . 28
4.3 3. Information Domain Boundaries . . . 30
4.4 4. Interfaces and Dependencies . . . 31
4.5 5. Information Domain Diagram . . . 32
4.6 6. Scope Changes . . . 32
4.7 7. Documentation and Evidence . . . 33
4.8 8. Approval . . . 33

5 Structure Analysis (Template) 34
5.1 1. Objective and Purpose . . . 34
5.2 2. Approach and Methodology . . . 34
5.3 3. Structure Register . . . 35
5.4 4. Dependencies and Interfaces . . . 37
5.5 5. Diagrams and Visualizations . . . 38
5.6 6. Validation and Quality Assurance . . . 38
5.7 7. Update and Maintenance . . . 39
5.8 8. Approval . . . 39

6 Protection Needs Assessment (Template) 40
6.1 1. Objective and Purpose . . . 40
6.2 2. Protection Needs Categories and Criteria . . . 40
6.3 3. Protection Needs Assessment . . . 42
6.4 4. Protection Needs Inheritance and Dependencies . . . 45
6.5 5. Validation and Quality Assurance . . . 46
6.6 6. Impact on Security Measures . . . 46
6.7 7. Documentation and Evidence . . . 47
6.8 8. Update and Maintenance . . . 47
6.9 9. Approval . . . 47

7 Modeling: Module Assignment (Template) 48
7.1 1. Objective and Purpose . . . 48
7.2 2. IT-Grundschutz Modules: Overview . . . 48
7.3 3. Module Assignment . . . 49
7.4 4. Summary and Statistics . . . 54
7.5 5. Validation and Quality Assurance . . . 55
7.6 6. Next Steps . . . 55
7.7 7. Update and Maintenance . . . 56
7.8 8. Approval . . . 56

8 Basic Security Check / Gap Analysis (Template) 57
8.1 1. Objective and Purpose . . . 57
8.2 2. Approach and Methodology . . . 57
8.3 3. Basic Security Check: Results . . . 59
8.4 4. Summary and Statistics . . . 63
8.5 5. Management Summary . . . 64
8.6 6. Next Steps . . . 65
8.7 7. Update and Maintenance . . . 65
8.8 8. Approval . . . 65

9 Risk Analysis (BSI Standard 200-3) – Template 66
9.1 1. Objective and Trigger . . . 66
9.2 2. Risk Objects and Scope . . . 66
9.3 3. Threats, Vulnerabilities and Scenarios . . . 67
9.4 4. Risk Assessment . . . 68
9.5 5. Risk Register . . . 69
9.6 6. Risk Assessment: Summary . . . 69

9.7 7. Approval and Risk Acceptance . . . 69
9.8 8. Update and Maintenance . . . 70

10 Security Concept and Action Plan 71
10.1 1. Target Vision and Strategy . . . 71
10.2 2. Measure Catalog . . . 72
10.3 3. Measure Prioritization . . . 73
10.4 4. Roadmap . . . 74
10.5 5. Resource Planning . . . 75
10.6 6. Dependencies and Risks . . . 75
10.7 7. Success Measurement . . . 76
10.8 8. Governance and Control . . . 76
10.9 9. Approval . . . 76

11 Implementation Control, Reporting and KPIs 78
11.1 1. Control Model . . . 78
11.2 2. Key Performance Indicators (KPIs) . . . 79
11.3 3. KPI Dashboard . . . 82
11.4 4. Escalation Rules . . . 83
11.5 5. Reporting Templates . . . 83
11.6 6. Continuous Improvement . . . 84
11.7 7. Tools and Systems . . . 84
11.8 8. Approval . . . 84

12 Policy: Access Control and Permissions 85
12.1 1. Purpose and Objectives . . . 85
12.2 2. Scope . . . 85
12.3 3. Principles . . . 85
12.4 4. Responsibilities . . . 86
12.5 5. Derived Guidelines and Standards . . . 86
12.6 6. Evidence and Control . . . 86
12.7 7. Consequences of Violations . . . 86
12.8 8. Approval . . . 86

13 Guideline: IAM Joiner Mover Leaver and Recertification 88
13.1 1. Purpose and Reference . . . 88
13.2 2. Scope . . . 88
13.3 3. Mandatory Requirements (MUST) . . . 88
13.4 4. Recommended Requirements (SHOULD) . . . 89
13.5 5. Process and Implementation . . . 89
13.6 6. Evidence . . . 89
13.7 7. Exceptions . . . 89
13.8 8. Training and Awareness . . . 89
13.9 9. Review and Update . . . 89
13.1010. Approval . . . 90

14 Policy: Authentication and MFA 91
14.1 1. Purpose and Objectives . . . 91
14.2 2. Scope . . . 91

14.3 3. Principles . . . 91
14.4 4. Responsibilities . . . 92
14.5 5. Derived Guidelines and Standards . . . 92
14.6 6. Evidence and Control . . . 92
14.7 7. Consequences of Violations . . . 92
14.8 8. Approval . . . 92

15 Guideline: Password MFA and Session Rules 94
15.1 1. Purpose and Reference . . . 94
15.2 2. Scope . . . 94
15.3 3. Mandatory Requirements (MUST) . . . 94
15.4 4. Recommended Requirements (SHOULD) . . . 95
15.5 5. Process and Implementation . . . 95
15.6 6. Evidence . . . 95
15.7 7. Exceptions . . . 95
15.8 8. Training and Awareness . . . 95
15.9 9. Review and Update . . . 95
15.1010. Approval . . . 96

16 Policy: Asset and Inventory Management 97
16.1 1. Purpose and Objectives . . . 97
16.2 2. Scope . . . 97
16.3 3. Principles . . . 97
16.4 4. Responsibilities . . . 98
16.5 5. Derived Guidelines and Standards . . . 98
16.6 6. Evidence and Control . . . 98
16.7 7. Consequences of Violations . . . 98
16.8 8. Approval . . . 98

17 Guideline: Asset Lifecycle Tagging and Disposal 100
17.1 1. Purpose and Reference . . . 100
17.2 2. Scope . . . 100
17.3 3. Mandatory Requirements (MUST) . . . 100
17.4 4. Recommended Requirements (SHOULD) . . . 101
17.5 5. Process and Implementation . . . 101
17.6 6. Evidence . . . 101
17.7 7. Exceptions . . . 101
17.8 8. Training and Awareness . . . 101
17.9 9. Review and Update . . . 101
17.1010. Approval . . . 102

18 Policy: Configuration and Hardening 103
18.1 1. Purpose and Objectives . . . 103
18.2 2. Scope . . . 103
18.3 3. Principles . . . 103
18.4 4. Responsibilities . . . 104
18.5 5. Derived Guidelines and Standards . . . 104
18.6 6. Evidence and Control . . . 104

18.7 7. Consequences of Violations . . . 104
18.8 8. Approval . . . 104

19 Guideline: Security Baselines and Deviation Management 106
19.1 1. Purpose and Reference . . . 106
19.2 2. Scope . . . 106
19.3 3. Mandatory Requirements (MUST) . . . 106
19.4 4. Recommended Requirements (SHOULD) . . . 107
19.5 5. Process and Implementation . . . 107
19.6 6. Evidence . . . 107
19.7 7. Exceptions . . . 107
19.8 8. Training and Awareness . . . 107
19.9 9. Review and Update . . . 107
19.1010. Approval . . . 108

20 Policy: Patch and Vulnerability Management 109
20.1 1. Purpose and Objectives . . . 109
20.2 2. Scope . . . 109
20.3 3. Principles . . . 109
20.4 4. Responsibilities . . . 110
20.5 5. Derived Guidelines and Standards . . . 110
20.6 6. Evidence and Control . . . 110
20.7 7. Consequences of Violations . . . 110
20.8 8. Approval . . . 110

21 Guideline: Scans Patching and Exploitation Response 112
21.1 1. Purpose and Reference . . . 112
21.2 2. Scope . . . 112
21.3 3. Mandatory Requirements (MUST) . . . 112
21.4 4. Recommended Requirements (SHOULD) . . . 113
21.5 5. Process and Implementation . . . 113
21.6 6. Evidence . . . 113
21.7 7. Exceptions . . . 113
21.8 8. Training and Awareness . . . 113
21.9 9. Review and Update . . . 113
21.1010. Approval . . . 114

22 Policy: Logging Monitoring and Detection 115
22.1 1. Purpose and Objectives . . . 115
22.2 2. Scope . . . 115
22.3 3. Principles . . . 115
22.4 4. Responsibilities . . . 116
22.5 5. Derived Guidelines and Standards . . . 116
22.6 6. Evidence and Control . . . 116
22.7 7. Consequences of Violations . . . 116
22.8 8. Approval . . . 116

23 Guideline: Log Standards SIEM UseCases and Retention 118
23.1 1. Purpose and Reference . . . 118

23.2 2. Scope . . . 118
23.3 3. Mandatory Requirements (MUST) . . . 118
23.4 4. Recommended Requirements (SHOULD) . . . 119
23.5 5. Process and Implementation . . . 119
23.6 6. Evidence . . . 119
23.7 7. Exceptions . . . 119
23.8 8. Training and Awareness . . . 119
23.9 9. Review and Update . . . 119
23.1010. Approval . . . 120

24 Policy: Incident Management 121
24.1 1. Purpose and Objectives . . . 121
24.2 2. Scope . . . 121
24.3 3. Principles . . . 121
24.4 4. Responsibilities . . . 122
24.5 5. Derived Guidelines and Standards . . . 122
24.6 6. Evidence and Control . . . 122
24.7 7. Consequences of Violations . . . 122
24.8 8. Approval . . . 122

25 Guideline: Incident Response Escalation and Forensics 124
25.1 1. Purpose and Reference . . . 124
25.2 2. Scope . . . 124
25.3 3. Mandatory Requirements (MUST) . . . 124
25.4 4. Recommended Requirements (SHOULD) . . . 125
25.5 5. Process and Implementation . . . 125
25.6 6. Evidence . . . 125
25.7 7. Exceptions . . . 125
25.8 8. Training and Awareness . . . 125
25.9 9. Review and Update . . . 125
25.1010. Approval . . . 126

26 Policy: Cryptography and Key Management 127
26.1 1. Purpose and Objectives . . . 127
26.2 2. Scope . . . 127
26.3 3. Principles . . . 127
26.4 4. Responsibilities . . . 128
26.5 5. Derived Guidelines and Standards . . . 128
26.6 6. Evidence and Control . . . 128
26.7 7. Consequences of Violations . . . 128
26.8 8. Approval . . . 128

27 Guideline: Encryption Key Rotation and Certificates 130
27.1 1. Purpose and Reference . . . 130
27.2 2. Scope . . . 130
27.3 3. Mandatory Requirements (MUST) . . . 130
27.4 4. Recommended Requirements (SHOULD) . . . 131
27.5 5. Process and Implementation . . . 131

27.6 6. Evidence . . . 131
27.7 7. Exceptions . . . 131
27.8 8. Training and Awareness . . . 131
27.9 9. Review and Update . . . 131
27.1010. Approval . . . 132

28 Policy: Secure Software Development 133
28.1 1. Purpose and Objectives . . . 133
28.2 2. Scope . . . 133
28.3 3. Principles . . . 133
28.4 4. Responsibilities . . . 134
28.5 5. Derived Guidelines and Standards . . . 134
28.6 6. Evidence and Control . . . 134
28.7 7. Consequences of Violations . . . 134
28.8 8. Approval . . . 134

29 Guideline: Secure SDLC Code Reviews SAST DAST Secrets 136
29.1 1. Purpose and Reference . . . 136
29.2 2. Scope . . . 136
29.3 3. Mandatory Requirements (MUST) . . . 136
29.4 4. Recommended Requirements (SHOULD) . . . 137
29.5 5. Process and Implementation . . . 137
29.6 6. Evidence . . . 137
29.7 7. Exceptions . . . 137
29.8 8. Training and Awareness . . . 137
29.9 9. Review and Update . . . 137
29.1010. Approval . . . 138

30 Policy: Change and Release Management 139
30.1 1. Purpose and Objectives . . . 139
30.2 2. Scope . . . 139
30.3 3. Principles . . . 139
30.4 4. Responsibilities . . . 140
30.5 5. Derived Guidelines and Standards . . . 140
30.6 6. Evidence and Control . . . 140
30.7 7. Consequences of Violations . . . 140
30.8 8. Approval . . . 140

31 Guideline: Change Approvals and Security Checks 142
31.1 1. Purpose and Reference . . . 142
31.2 2. Scope . . . 142
31.3 3. Mandatory Requirements (MUST) . . . 142
31.4 4. Recommended Requirements (SHOULD) . . . 143
31.5 5. Process and Implementation . . . 143
31.6 6. Evidence . . . 143
31.7 7. Exceptions . . . 143
31.8 8. Training and Awareness . . . 143
31.9 9. Review and Updates . . . 143

31.1010. Approval . . . 144

32 Policy: Supplier and Outsourcing Management 145
32.1 1. Purpose and Objectives . . . 145
32.2 2. Scope . . . 145
32.3 3. Principles . . . 145
32.4 4. Responsibilities . . . 146
32.5 5. Derived Guidelines and Standards . . . 146
32.6 6. Evidence and Control . . . 146
32.7 7. Consequences of Violations . . . 146
32.8 8. Approval . . . 146

33 Guideline: Third Party Risk Assessment and Contract Clauses 148
33.1 1. Purpose and Reference . . . 148
33.2 2. Scope . . . 148
33.3 3. Mandatory Requirements (MUST) . . . 148
33.4 4. Recommended Requirements (SHOULD) . . . 149
33.5 5. Process and Implementation . . . 149
33.6 6. Evidence . . . 149
33.7 7. Exceptions . . . 149
33.8 8. Training and Awareness . . . 149
33.9 9. Review and Updates . . . 149
33.1010. Approval . . . 150

34 Policy: Data Protection and Data Handling 151
34.1 1. Purpose and Objectives . . . 151
34.2 2. Scope . . . 151
34.3 3. Principles . . . 151
34.4 4. Responsibilities . . . 152
34.5 5. Derived Guidelines and Standards . . . 152
34.6 6. Evidence and Control . . . 152
34.7 7. Consequences of Violations . . . 152
34.8 8. Approval . . . 152

35 Guideline: Data Classification Labeling and Disclosure 154
35.1 1. Purpose and Reference . . . 154
35.2 2. Scope . . . 154
35.3 3. Mandatory Requirements (MUST) . . . 154
35.4 4. Recommended Requirements (SHOULD) . . . 155
35.5 5. Process and Implementation . . . 155
35.6 6. Evidence . . . 155
35.7 7. Exceptions . . . 155
35.8 8. Training and Awareness . . . 155
35.9 9. Review and Updates . . . 155
35.1010. Approval . . . 156

36 Policy: Backup and Recovery 157
36.1 1. Purpose and Objectives . . . 157
36.2 2. Scope . . . 157

36.3 3. Principles . . . 157
36.4 4. Responsibilities . . . 158
36.5 5. Derived Guidelines and Standards . . . 158
36.6 6. Evidence and Control . . . 158
36.7 7. Consequences of Violations . . . 158
36.8 8. Approval . . . 158

37 Guideline: Backup Restore and Regular Tests 160
37.1 1. Purpose and Reference . . . 160
37.2 2. Scope . . . 160
37.3 3. Mandatory Requirements (MUST) . . . 160
37.4 4. Recommended Requirements (SHOULD) . . . 161
37.5 5. Process and Implementation . . . 161
37.6 6. Evidence . . . 161
37.7 7. Exceptions . . . 161
37.8 8. Training and Awareness . . . 161
37.9 9. Review and Updates . . . 161
37.1010. Approval . . . 162

38 Policy: Network and Communication Security 163
38.1 1. Purpose and Objectives . . . 163
38.2 2. Scope . . . 163
38.3 3. Principles . . . 163
38.4 4. Responsibilities . . . 164
38.5 5. Derived Guidelines and Standards . . . 164
38.6 6. Evidence and Control . . . 164
38.7 7. Consequences of Violations . . . 164
38.8 8. Approval . . . 164

39 Guideline: Segmentation Firewalling VPN and Admin Access 166
39.1 1. Purpose and Reference . . . 166
39.2 2. Scope . . . 166
39.3 3. Mandatory Requirements (MUST) . . . 166
39.4 4. Recommended Requirements (SHOULD) . . . 167
39.5 5. Process and Implementation . . . 167
39.6 6. Evidence . . . 167
39.7 7. Exceptions . . . 167
39.8 8. Training and Awareness . . . 167
39.9 9. Review and Updates . . . 167
39.1010. Approval . . . 168

40 Policy: Endpoint and Mobile Security 169
40.1 1. Purpose and Objectives . . . 169
40.2 2. Scope . . . 169
40.3 3. Principles . . . 169
40.4 4. Responsibilities . . . 170
40.5 5. Derived Guidelines and Standards . . . 170
40.6 6. Evidence and Control . . . 170

40.7 7. Consequences of Violations . . . 170
40.8 8. Approval . . . 170

41 Guideline: MDM EDR Device Compliance and Remote Work 172
41.1 1. Purpose and Reference . . . 172
41.2 2. Scope . . . 172
41.3 3. Mandatory Requirements (MUST) . . . 172
41.4 4. Recommended Requirements (SHOULD) . . . 173
41.5 5. Process and Implementation . . . 173
41.6 6. Evidence . . . 173
41.7 7. Exceptions . . . 173
41.8 8. Training and Awareness . . . 173
41.9 9. Review and Updates . . . 173
41.1010. Approval . . . 174

42 Policy: Physical Security 175
42.1 1. Purpose and Objectives . . . 175
42.2 2. Scope . . . 175
42.3 3. Principles . . . 175
42.4 4. Responsibilities . . . 176
42.5 5. Derived Guidelines and Standards . . . 176
42.6 6. Evidence and Control . . . 176
42.7 7. Consequences of Violations . . . 176
42.8 8. Approval . . . 176

43 Guideline: Access Visitors and Equipment Protection 178
43.1 1. Purpose and Reference . . . 178
43.2 2. Scope . . . 178
43.3 3. Mandatory Requirements (MUST) . . . 178
43.4 4. Recommended Requirements (SHOULD) . . . 179
43.5 5. Process and Implementation . . . 179
43.6 6. Evidence . . . 179
43.7 7. Exceptions . . . 179
43.8 8. Training and Awareness . . . 179
43.9 9. Review and Updates . . . 179
43.1010. Approval . . . 180

44 Policy: Exception Process and Risk Acceptance 181
44.1 1. Purpose and Objectives . . . 181
44.2 2. Scope . . . 181
44.3 3. Principles . . . 181
44.4 4. Responsibilities . . . 182
44.5 5. Derived Guidelines and Standards . . . 182
44.6 6. Evidence and Control . . . 182
44.7 7. Consequences of Violations . . . 182
44.8 8. Approval . . . 182

45 Guideline: Exceptions Risk Waiver and Review 184
45.1 1. Purpose and Reference . . . 184

45.2 2. Scope . . . 184
45.3 3. Mandatory Requirements (MUST) . . . 184
45.4 4. Recommended Requirements (SHOULD) . . . 185
45.5 5. Process and Implementation . . . 185
45.6 6. Evidence . . . 185
45.7 7. Exceptions . . . 185
45.8 8. Training and Awareness . . . 185
45.9 9. Review and Updates . . . 185
45.1010. Approval . . . 186

46 Training and Awareness – Program **187**
46.1 1. Purpose and Objectives . . . 187
46.2 2. Target Groups . . . 187
46.3 3. Training Catalog . . . 187
46.4 4. Effectiveness Measurement . . . 188
46.5 5. Training Materials . . . 188
46.6 6. Communication and Awareness Campaigns . . . 189
46.7 7. Approval . . . 189

47 Internal Audit Program (Template) **190**
47.1 1. Purpose and Objectives . . . 190
47.2 2. Audit Approach . . . 190
47.3 3. Audit Plan . . . 190
47.4 4. Audit Checkpoints . . . 191
47.5 5. Audit Process . . . 191
47.6 6. Audit Report Template . . . 191
47.7 7. Findings Categorization . . . 191
47.8 8. Approval . . . 192

48 Management Review – Template **193**
48.1 1. Participants, Period, Scope . . . 193
48.2 2. Inputs for Management Review . . . 193
48.3 3. Outputs and Decisions . . . 194
48.4 4. Summary and Conclusion . . . 195
48.5 5. Approval . . . 195

49 Non-Conformities and Corrective Actions **196**
49.1 1. Purpose and Objectives . . . 196
49.2 2. Sources for Non-Conformities . . . 196
49.3 3. Process . . . 197
49.4 4. Findings Register . . . 197
49.5 5. Categorization and Response Times . . . 198
49.6 6. Reporting . . . 198
49.7 7. Lessons Learned . . . 198
49.8 8. Approval . . . 198

50 Appendix: Evidence Register **200**
50.1 1. Purpose and Objectives . . . 200
50.2 2. Evidence Register . . . 200

50.3 3. Evidence Categories . . . 202
50.4 4. Retention Periods . . . 203
50.5 5. Access Control . . . 203
50.6 6. Review and Updates . . . 203
50.7 7. Approval . . . 203

51 Appendix: Asset Inventory (Template) 205
51.1 1. Purpose and Objectives . . . 205
51.2 2. Maintenance Note . . . 205
51.3 3. Asset Categories . . . 205
51.4 4. Asset Register . . . 206
51.5 5. NetBox Integration . . . 206
51.6 6. Asset Lifecycle Management . . . 207
51.7 7. Responsibilities (RACI) . . . 207
51.8 8. Asset Tagging . . . 208
51.9 9. Reporting . . . 208
51.1010. Approval . . . 208

52 Appendix: Data Flows and Interfaces (Template) 209
52.1 1. Purpose and Objectives . . . 209
52.2 2. Data Flow Register . . . 209
52.3 3. Interface Register . . . 210
52.4 4. External Interfaces and Third Parties . . . 211
52.5 5. Data Flow Diagrams . . . 211
52.6 6. Data Categories . . . 211
52.7 7. Encryption Requirements . . . 212
52.8 8. Cross-Border Data Transfer . . . 212
52.9 9. Responsibilities (RACI) . . . 213
52.1010. Change Management . . . 213
52.1111. Approval . . . 213

53 Appendix: Network Plan and Zone Model (Template) 214
53.1 1. Purpose and Objectives . . . 214
53.2 2. High-Level Network Plan . . . 214
53.3 3. Network Zones and Segmentation . . . 214
53.4 4. Trust Boundaries and Firewall Rules . . . 215
53.5 5. Network Devices . . . 216
53.6 6. VLANs . . . 216
53.7 7. Administrative Access . . . 217
53.8 8. Network Monitoring . . . 217
53.9 9. Network Diagrams . . . 218
53.1010. Site Connectivity (WAN) . . . 218
53.1111. Cloud Integration . . . 218
53.1212. Responsibilities (RACI) . . . 218
53.1313. Change Management . . . 219
53.1414. Approval . . . 219

54 Appendix: Terms and Abbreviations 220

54.1 1. Purpose 220
54.2 2. Terms 220
54.3 3. Abbreviations 224
54.4 4. BSI-Specific Terms 226
54.5 5. Approval 226

Chapter 1

Information Security Policy (Top Management)

Document ID: 0010
Document Type: Policy/Policy
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

1.1 1. Purpose and Objectives

The Information Security Policy of **AdminSend GmbH** defines the strategic objectives and principles for the protection of information and IT systems.

1.1.1 1.1 Information Security Objective

AdminSend GmbH commits to establishing information security as an integral part of corporate management. The objective is the appropriate protection of all information assets from threats and risks.

[TODO: Add specific security objectives of the organization]

1.1.2 1.2 Protection Values

The information security of **AdminSend GmbH** is based on the following protection goals:

- **Confidentiality:** Protection against unauthorized disclosure of information
- **Integrity:** Protection against unauthorized modification of information
- **Availability:** Ensuring the availability of information and systems
- **Authenticity:** Ensuring the authenticity and credibility of information

- **Traceability:** Ensuring the traceability of actions

1.2 2. Scope

1.2.1 2.1 Organization and Locations

This policy applies to:

- **Organization:** AdminSend GmbH
- **Locations:** {{ meta.organization.locations }}
- **Executive Management:** Max Mustermann
- **Information Security Officer (ISB):** Thomas Weber

1.2.2 2.2 Information Domains in Scope

[TODO: Define the information domains within scope]

Examples: - IT infrastructure and networks - Business applications and databases - Cloud services and external service providers - Mobile devices and remote workplaces

1.2.3 2.3 Exceptions

[TODO: Document explicit exceptions from the scope]

1.3 3. Principles

1.3.1 3.1 Risk-Based Approach

AdminSend GmbH pursues a risk-based approach to information security according to BSI Standard 200-3. Security measures are implemented based on a systematic risk analysis and assessment.

1.3.2 3.2 Responsibilities and Resources

Executive management ensures that: - Clear responsibilities for information security are defined - Sufficient resources (personnel, budget, time) are provided - Information security is considered in all business processes

1.3.3 3.3 Continuous Improvement

The Information Security Management System (ISMS) is continuously monitored, assessed, and improved. Regular reviews and audits ensure effectiveness.

1.3.4 3.4 Commitment to Compliance

AdminSend GmbH commits to compliance with: - Legal and regulatory requirements (GDPR, IT Security Act, etc.) - Contractual obligations towards customers and partners - Internal guidelines and standards - BSI IT-Grundschutz requirements

1.4 4. Responsibilities

1.4.1 4.1 Top Management / Executive Management

Responsible: Max Mustermann (max.mustermann@adminsend.de)

Executive management bears overall responsibility for information security and: - Approves the information security policy - Provides resources - Promotes security culture - Monitors ISMS performance

1.4.2 4.2 Information Security Officer (ISO)

Responsible: Thomas Weber (thomas.weber@adminsend.de)

The ISO is responsible for: - Coordination of the ISMS - Advising executive management - Monitoring security measures - Conducting risk analyses - Incident management coordination

1.4.3 4.3 IT Management

Responsible: Anna Schmidt (anna.schmidt@adminsend.de)

IT management is responsible for: - Implementation of technical security measures - Operation of secure IT systems - Patch and vulnerability management - Technical incident response

1.4.4 4.4 Information Domain Managers

[TODO: Define responsible persons for specific information domains]

1.4.5 4.5 All Employees

All employees are obligated to: - Comply with security guidelines - Report security incidents - Participate in training - Handle information responsibly

1.5 5. Communication and Enforcement

1.5.1 5.1 Communication of the Policy

This policy is communicated through: - Publication on the intranet - Training and awareness programs - Onboarding of new employees - Regular reminders and updates

1.5.2 5.2 Consequences of Violations

Violations of this policy may result in the following measures: - Warning - Disciplinary measures - Employment law consequences - Criminal prosecution (in case of serious violations)

1.6 6. Review and Update

This policy is reviewed and updated at least annually or in case of significant changes.

Next Review: {{ meta.document.next_review }}

1.7 7. Approval

Role	Name	Date	Approval
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI Standard 200-1: Management Systems for Information Security (ISMS) - BSI Standard 200-2: IT-Grundschutz Methodology - BSI Standard 200-3: Risk Analysis Based on IT-Grundschutz - BSI IT-Grundschutz Compendium

ewpage

Chapter 2

ISMS Organization, Roles and Responsibilities

Document ID: 0020
Document Type: Foundation Document
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

2.1 1. ISMS Organization

2.1.1 1.1 ISMS Owner/Sponsor

Responsible: Max Mustermann (max.mustermann@adminsend.de)

The ISMS Owner bears overall responsibility for the Information Security Management System and ensures that: - Sufficient resources are provided - The information security policy is approved - Strategic decisions on information security are made - The ISMS is integrated into business processes

2.1.2 1.2 Information Security Officer (ISO)

Responsible: Thomas Weber (thomas.weber@adminsend.de)

The ISO is the central coordination point for all information security activities: - Coordination and management of the ISMS - Advising executive management and departments - Conducting risk analyses and security assessments - Monitoring the implementation of security measures - Reporting to executive management - Coordination of security incidents - Conducting awareness measures

2.1.3 1.3 ISMS Team / Information Security Committee

The ISMS Team supports the ISO in implementing the ISMS:

Role	Name	Area of Responsibility
ISO (Lead)	Thomas Weber	Overall ISMS coordination
IT Management	Anna Schmidt	Technical security measures
Data Protection Officer	[TODO]	Data protection interface
BCM Manager	[TODO]	Business Continuity
Risk Manager	[TODO]	Risk management
HR Representative	[TODO]	Personnel and awareness topics
Legal/Compliance	[TODO]	Legal requirements

Meeting Frequency: [TODO: e.g. monthly, quarterly]

2.1.4 1.4 Interfaces to Other Areas

2.1.4.1 1.4.1 IT Service Management (ITSM)

Contact: Anna Schmidt

Interfaces: - Change Management: Security assessment of changes - Incident Management: Security incidents - Problem Management: Security vulnerabilities - Configuration Management: Asset inventory

2.1.4.2 1.4.2 Data Protection

Contact: [TODO: Data Protection Officer]

Interfaces: - Record of processing activities (ROPA) - Data Protection Impact Assessment (DPIA) - Technical and organizational measures (TOM) - Reporting of data breaches

2.1.4.3 1.4.3 Business Continuity Management (BCM)

Contact: [TODO: BCM Manager]

Interfaces: - Business Impact Analysis (BIA) - IT Disaster Recovery Plans - Emergency exercises and tests - Crisis management

2.1.4.4 1.4.4 Risk Management

Contact: [TODO: Risk Manager]

Interfaces: - Enterprise-wide risk management - Risk register and assessment - Risk reporting - Risk acceptance decisions

2.1.4.5 1.4.5 Internal Audit

Contact: [TODO: Internal Audit]

Interfaces: - ISMS audits - Compliance reviews - Follow-up of audit findings - Reporting to management

2.2 2. Roles and Responsibilities

2.2.1 2.1 Information Domain Manager

Role: Responsible for a specific information domain (e.g. business application, IT system)

Tasks: - Definition of the information domain scope - Conducting structure analysis - Protection needs assessment - Modeling and module assignment - Coordination of measure implementation - Monitoring the security of the information domain

[TODO: Designate specific information domain managers]

2.2.2 2.2 Asset Owner / System Owner

Role: Responsible for specific assets or IT systems

Tasks: - Classification and assessment of assets - Definition of security requirements - Approval of access rights - Monitoring asset usage - Decision on decommissioning

[TODO: Define asset owners for critical systems]

2.2.3 2.3 Measure/Control Owner

Role: Responsible for implementing specific security measures

Tasks: - Implementation of assigned security measures - Documentation of implementation - Evidence of effectiveness - Continuous monitoring and improvement

[TODO: Assignment of measure owners]

2.2.4 2.4 Administrators / Operators

Role: Technical implementation and operation of IT systems

Tasks: - Configuration and hardening of systems - Patch and update management - Monitoring and logging - Backup and recovery - Incident response (technical)

Responsible: Anna Schmidt (IT Management)

2.2.5 2.5 All Employees

Role: Users of IT systems and information

Tasks: - Compliance with security guidelines - Reporting security incidents - Participation in training - Responsible handling of information - Protection of access credentials

2.3 3. RACI Matrix for BSI IT-Grundschutz Processes

Activity	Executive Management	ISO	IT Management	Information Domain Managers	Departments	Internal Audit
Structure Analysis	I	A	C	R	C	I

Activity	Executive Management	ISO	IT Management	Information Domain Managers	Departments	Internal Audit
Protection Needs Assessment	A	C	C	R	C	I
Modeling (Module Assignment)	I	A	C	R	C	I
Basic Security Check	I	A	C	R	C	I
Risk Analysis (BSI 200-3)	A	R	C	C	C	I
Measure Planning	A	R	C	C	C	I
Measure Implementation	I	C	R	R	R	I
Effectiveness Review	I	A	C	R	C	I
ISMS Audit	I	C	C	C	C	R/A
Management Review	A	R	C	I	I	C
Incident Management	I	A	R	C	C	I
Awareness Training	I	A	C	C	R	I
Documentation	I	A	R	R	C	I

2.4 4. Escalation Paths

2.4.1 4.1 Operational Escalation

1. **Level 1:** Information Domain Managers / System Owner
2. **Level 2:** ISO / IT Management
3. **Level 3:** Executive Management

2.4.2 4.2 Security Incidents

1. **Report:** All Employees → ISO / IT Management
2. **Assessment:** ISO / IT Management

3. **Escalation (for Major Incidents):** Executive Management
4. **External Reporting (if required):** BSI, Data Protection Authority, Law Enforcement

2.5 5. Communication and Reporting

2.5.1 5.1 Regular Reports

Report	Frequency	Creator	Recipient
ISMS Status Report	Monthly	ISO	Executive Management, ISMS Team
Security Incidents	Monthly	ISO	Executive Management
Risk Dashboard	Quarterly	ISO	Executive Management
Management Review	Annually	ISO	Executive Management
Audit Results	After Audit	Internal Audit	Executive Management, ISO

2.5.2 5.2 Ad-hoc Communication

- **Security Incidents:** Immediate report to ISO
- **Critical Vulnerabilities:** Immediate report to ISO and IT Management
- **Compliance Violations:** Report to ISO and Legal/Compliance

2.6 6. Resources and Budget

[TODO: Define budget and resources for ISMS activities]

- **ISMS Budget:** [TODO]
- **Personnel Resources:** [TODO]
- **External Support:** [TODO]
- **Tools and Systems:** [TODO]

2.7 7. Review and Update

This organizational structure is reviewed and updated at least annually or in case of significant changes.

Next Review: {{ meta.document.next_review }}

References: - BSI Standard 200-1: Management Systems for Information Security (ISMS) - BSI Standard 200-2: IT-Grundschutz Methodology - BSI IT-Grundschutz Compendium

ewpage

Chapter 3

Document Control and Document Register

Document ID: 0030
Document Type: Process/Foundation
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

3.1 1. Purpose and Scope

This document describes document control for the Information Security Management System (ISMS) of **AdminSend GmbH**. It defines processes for creation, review, approval, distribution, modification, and archiving of ISMS documents.

3.1.1 1.1 Scope

This document control applies to all ISMS-relevant documents: - Policies - Guidelines and process descriptions - Security concepts and risk analyses - Work instructions and checklists - Protocols and evidence

3.2 2. Storage and Access

3.2.1 2.1 Official Storage Location

Primary Storage Location: [TODO: e.g. SharePoint, Confluence, DMS]

Responsible: IT Operations Manager

All ISMS documents are stored centrally in: - **Path:** [TODO: e.g. /ISMS/Documentation/] - **Backup:** [TODO: Backup strategy] - **Versioning:** Automatic versioning enabled

3.2.2 2.2 Access Control (RBAC)

Access to ISMS documents is role-based:

Role	Read	Write	Approve	Delete
Executive Management				
ISO				
ISMS Team				
Information Domain Managers		(own documents)		
All Employees	(public documents)			

3.2.3 2.3 Classification and Protection Need

Classification	Description	Access	Examples
Public	No confidentiality	All Employees	Awareness material
Internal	Internal use only	All Employees	Policies, guidelines
Confidential	Restricted access	ISMS Team, Authorized	Risk analyses, security concepts
Strictly Confidential	Highest confidentiality	Executive Management, ISO	Incident reports, audit findings

3.2.4 2.4 Emergency Access

In emergencies (e.g. ISO unavailable), the following persons have access to all ISMS documents: - **Executive Management:** Max Mustermann - **IT Management:** Anna Schmidt - **Deputy ISO:** [TODO]

3.3 3. Document Lifecycle

3.3.1 3.1 Creation

Process: 1. **Initiation:** Need is identified (ISO, ISMS Team, Department) 2. **Creation:** Author creates document based on template 3. **Quality Assurance:** Peer review by ISMS Team 4. **Approval:** Approval by responsible role (see approval matrix)

Responsible: Document author, ISO (coordination)

3.3.2 3.2 Review and Approval

3.3.2.1 3.2.1 Approval Matrix

Document Type	Creator	Reviewer	Approver
Policies	ISO	ISMS Team	Executive Management
Guidelines	ISO, Department	ISMS Team	ISO

Document Type	Creator	Reviewer	Approver
Security Concepts	Information Domain Managers	ISO	ISO
Work Instructions	Department	ISO	IT Management
Risk Analyses	ISO	ISMS Team	Executive Management

3.3.2.2 3.2.2 Review Intervals

Document Type	Review Interval	Responsible
Policies	Annually	ISO
Guidelines	Annually	ISO
Security Concepts	Annually or upon changes	Information Domain Managers
Work Instructions	Annually	Department
Risk Analyses	Annually or upon significant changes	ISO

Additional Review Triggers: - Significant changes in IT infrastructure - New legal requirements - Security incidents - Audit findings - Organizational changes

3.3.3 3.3 Versioning

Versioning Scheme: - **Major Version (X.0):** Significant content changes, new approval required - **Minor Version (X.Y):** Minor adjustments, editorial changes

Example: - Version 1.0: Initial approval - Version 1.1: Minor adjustments - Version 2.0: Major revision

3.3.4 3.4 Distribution and Communication

Distribution Process: 1. Document approval 2. Publication in central storage location 3. Notification of affected stakeholders (email, intranet) 4. Training/awareness (if required) 5. Acknowledgment of receipt (for critical documents)

Responsible: ISO

3.3.5 3.5 Change Management

Process for Changes: 1. **Change Request:** Initiator submits change request to ISO 2. **Assessment:** ISO assesses change need and impacts 3. **Approval:** Approval by responsible role 4. **Implementation:** Author updates document 5. **Review:** Review by ISMS Team 6. **Approval:** Approval according to approval matrix 7. **Distribution:** Communication of changes

3.3.6 3.6 Archiving and Deletion

Archiving: - Old versions are archived for [TODO: e.g. 5 years] - Archived documents are write-protected - Access only for ISO and Audit

Deletion: - Documents are deleted after retention period expires - Deletion according to data protection and compliance requirements - Deletion log is maintained

Responsible: ISO

3.4 4. Document Register

Document	ID	Owner	Status	Version	Last Updated	Next Review
Information Security Policy	0010	Thomas Weber	{{ meta.document.status }}	1.0.0	{{ meta.document.last_updated }}	{{ meta.document.next_revie
ISMS Organization, Roles and RACI	0020	Thomas Weber	{{ meta.document.status }}	1.0.0	{{ meta.document.last_updated }}	{{ meta.document.next_revie
Document Control	0030	Thomas Weber	{{ meta.document.status }}	1.0.0	{{ meta.document.last_updated }}	{{ meta.document.next_revie
[TODO: Add additional documents]						

3.5 5. Change Log

Version	Date	Change	Author	Approver	Status
0.1	{{ meta.document.last_updated }}	First draft	IT Operations Manager	-	Draft
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

3.6 6. Quality Assurance

3.6.1 6.1 Document Quality

All ISMS documents must meet the following quality criteria: - **Completeness:** All required content present - **Correctness:** Content accurate and current - **Comprehensibility:** Clearly and understandably formulated - **Consistency:** Consistent with other ISMS documents - **Traceability:** Changes documented traceably

3.6.2 6.2 Document Templates

Templates exist for all document types with: - Standardized header (metadata) - Structure specifications - Placeholders for variable content - Notes for authors

Template Storage Location: [TODO: e.g. /ISMS/Templates/]

3.7 7. Training and Awareness

All document authors and ISMS Team members are trained in: - Document control process - Use of templates - Versioning and change management - Classification and protection needs

Responsible: ISO

3.8 8. Monitoring and Improvement

The document control process is regularly monitored: - **Metrics:** Number of documents, review compliance, change rate - **Review:** Annual review of the process - **Improvement:** Continuous optimization based on feedback

Next Review: {{ meta.document.next_review }}

References: - BSI Standard 200-1: Management Systems for Information Security (ISMS) - BSI Standard 200-2: IT-Grundschutz Methodology

ewpage

Chapter 4

Scope and Information Domain (Boundaries)

Document ID: 0040
Document Type: Foundation Document
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

4.1 1. Purpose and Objectives

This document defines the scope of the Information Security Management System (ISMS) of **AdminSend GmbH** and delineates the information domain. The clear definition of scope is the foundation for all further IT-Grundschutz activities (structure analysis, protection needs assessment, modeling).

4.2 2. Scope Definition

4.2.1 2.1 Organizational Units and Locations

Organization: AdminSend GmbH

Locations in Scope:

Location	Address	Type	Employees	In Scope
{{ meta.organization.primary_location }}	[TODO]	Main location	[TODO]	

Location	Address	Type	Employees	In Scope
[TODO: Additional locations]	[TODO]	[TODO]	[TODO]	/

Organizational Units in Scope: - Executive Management - IT Department - [TODO: Additional departments]

4.2.2 2.2 Business Processes and Services

Critical Business Processes in Scope:

Process	Description	Criticality	Owner	In Scope
[TODO: Process 1]	[TODO]	High/Medium/Low	[TODO]	
[TODO: Process 2]	[TODO]	High/Medium/Low	[TODO]	

IT Services in Scope:

Service	Description	Users	Service Owner	In Scope
[TODO: Service 1]	[TODO]	[TODO]	Anna Schmidt	
[TODO: Service 2]	[TODO]	[TODO]	Anna Schmidt	

4.2.3 2.3 IT Infrastructure

IT Systems in Scope:

4.2.3.1 2.3.1 On-Premise IT

Category	Systems	Quantity	In Scope
Servers	{{ netbox.device.servers }}	[TODO]	
Network	{{ netbox.device.network }}	[TODO]	
Storage	{{ netbox.device.storage }}	[TODO]	
Clients	Workstations, Laptops	[TODO]	
Mobile Devices	Smartphones, Tablets	[TODO]	

4.2.3.2 2.3.2 Cloud Services

Cloud Service	Provider	Type (IaaS/PaaS/SaaS)	In Scope
[TODO: Cloud Service 1]	[TODO]	[TODO]	
[TODO: Cloud Service 2]	[TODO]	[TODO]	

4.2.3.3 2.3.3 OT/IoT (if applicable)

OT/IoT System	Description	Location	In Scope
[TODO: OT System 1]	[TODO]	[TODO]	/

4.2.4 2.4 Applications and Data

Business Applications in Scope:

Application	Type	Criticality	Data Classification	In Scope
[TODO: Application 1]	[TODO]	High/Medium/Low	Confidential/Internal	
[TODO: Application 2]	[TODO]	High/Medium/Low	Confidential/Internal	

Data Types in Scope: - Personal data (GDPR-relevant) - Trade secrets - Customer data - Financial data - [TODO: Additional data types]

4.3 3. Information Domain Boundaries

4.3.1 3.1 In Scope

The following elements are in scope of the ISMS:

1. **Infrastructure:**
   - All servers and network components at location {{ meta.organization.primary_location }}
   - [TODO: Additional infrastructure]
2. **Applications:**
   - All business-critical applications
   - [TODO: Specific applications]
3. **Data:**
   - All personal data
   - All business data classified as “Confidential” or higher
   - [TODO: Additional data]
4. **People:**
   - All employees of AdminSend GmbH
   - External service providers with access to scope systems
   - [TODO: Additional groups]
5. **Processes:**
   - All IT operations processes
   - All business-critical processes
   - [TODO: Additional processes]

4.3.2 3.2 Out of Scope

The following elements are NOT in scope of the ISMS:

Element	Justification	Risk Assessment	Interfaces to Scope
[TODO: Out-of-Scope Element 1]	[TODO: Justification]	[TODO: Risk]	[TODO: Interfaces]
[TODO: Out-of-Scope Element 2]	[TODO: Justification]	[TODO: Risk]	[TODO: Interfaces]

Important: Even out-of-scope elements must be assessed for their risks to the scope, especially when interfaces exist.

4.3.3 3.3 Justification of Boundaries

[TODO: Explain the reasons for the chosen scope boundaries]

Examples of justifications: - Focus on critical business processes - Resource constraints (phased expansion planned) - External responsibility (e.g. outsourced processes) - Low criticality

4.4 4. Interfaces and Dependencies

4.4.1 4.1 External Service Providers

Service Provider	Service	Criticality	Contractual Arrangements	Security Requirements
[TODO: Provider 1]	[TODO]	High/Medium/Low	[TODO: Contract available]	[TODO: SLA, Certifications]
[TODO: Provider 2]	[TODO]	High/Medium/Low	[TODO: Contract available]	[TODO: SLA, Certifications]

4.4.2 4.2 Critical Interfaces

Interfaces between Scope and Out-of-Scope:

Interface	From (Scope)	To (Out-of-Scope)	Data Flow	Security Measures
[TODO: Interface 1]	[TODO]	[TODO]	[TODO]	[TODO: Encryption, Firewall, etc.]
[TODO: Interface 2]	[TODO]	[TODO]	[TODO]	[TODO]

Interfaces to External Partners:

Information Domain Diagram

Figure 4.1: Information Domain Diagram

Partner	Purpose	Data Types	Security Measures
[TODO: Partner 1]	[TODO]	[TODO]	[TODO]
[TODO: Partner 2]	[TODO]	[TODO]	[TODO]

4.4.3 4.3 Dependencies

Critical Dependencies of the Scope:

Dependency	Type	Impact of Failure	Mitigation Measures
Internet Connection	External Infrastructure	[TODO]	[TODO: Redundancy, Backup line]
Power Supply	External Infrastructure	[TODO]	[TODO: UPS, Emergency power]
[TODO: Additional dependencies]	[TODO]	[TODO]	[TODO]

4.5 5. Information Domain Diagram

Diagram Legend: - **Green Line:** Scope boundary (in ISMS) - **Red Line:** Out-of-scope boundary - **Blue Arrows:** Data flows - **Yellow Symbols:** Critical interfaces

[TODO: Create an information domain diagram]

4.6 6. Scope Changes

4.6.1 6.1 Change Process

Scope changes require: 1. **Request:** Formal change request to ISO 2. **Assessment:** Assessment of impacts (risks, resources, compliance) 3. **Approval:** Approval by executive management 4. **Implementation:** Update of all affected documents 5. **Communication:** Information to all stakeholders

Responsible: Thomas Weber (ISO)

4.6.2 6.2 Scope Review

The scope is regularly reviewed: - **Frequency:** Annually or upon significant changes - **Triggers:** New business processes, IT systems, locations, regulatory requirements - **Responsible:** ISO

Next Review: {{ meta.document.next_review }}

4.7 7. Documentation and Evidence

The following documents and evidence are maintained for the scope: - This scope document - Information domain diagram - Asset inventory (see Appendix 0710) - Data flow diagrams (see Appendix 0720) - Contracts with external service providers - Scope change logs

4.8 8. Approval

Role	Name	Date	Approval
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ data.document.approval_status }}
ISO	Thomas Weber	{{ meta.document.approval_date }}	{{ data.document.approval_status }}

References: - BSI Standard 200-1: Management Systems for Information Security (ISMS) - BSI Standard 200-2: IT-Grundschutz Methodology (Chapter 4: Scope Definition) - BSI IT-Grundschutz Compendium

ewpage

Chapter 5

Structure Analysis (Template)

Document ID: 0050
Document Type: Methodology Artifact
Reference Framework: BSI IT-Grundschutz (BSI Standard 200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

5.1 1. Objective and Purpose

The structure analysis systematically captures the structure of the information domain of **AdminSend GmbH**. It forms the basis for: - Protection needs assessment (Document 0060) - Modeling and module assignment (Document 0070) - Basic security check (Document 0080) - Risk analysis (Document 0090)

Responsible: Thomas Weber (ISO)

5.2 2. Approach and Methodology

5.2.1 2.1 Data Sources

The following data sources are used for the structure analysis:

Data Source	Type	Responsible	Currency
CMDB/Asset Inventory	System	Anna Schmidt	[TODO]
Network Documentation	Document	Anna Schmidt	[TODO]
Architecture Diagrams	Document	Anna Schmidt	[TODO]
Service Provider Contracts	Document	[TODO]	[TODO]
Stakeholder Interviews	Primary Source	Thomas Weber	[TODO]

5.2.2 2.2 Granularity

The structure analysis is performed at the following granularity levels:

- **Business Processes:** Process level (not activity level)
- **Applications:** Application system level (not module level)
- **IT Systems:** Logical systems (servers, databases, storage)
- **Networks:** Network segments and zones
- **Rooms:** Locations and critical rooms (data center, server room)

5.2.3 2.3 Execution

Timeline: - **Start:** [TODO] - **Data Collection:** [TODO: e.g. 2 weeks] - **Validation:** [TODO: e.g. 1 week] - **Completion:** [TODO]

Participants: - ISO: Thomas Weber - IT Management: Anna Schmidt - Information Domain Managers: [TODO] - Departments: [TODO]

5.3 3. Structure Register

5.3.1 3.1 Business Processes and Services

ID	Process/Service	Owner	Description	Criticality	Dependencies	Applications
P-001	[TODO: Process 1]	[TODO]	[TODO]	High/Medium/Low	[TODO]	[TODO: A-001, A-002]
P-002	[TODO: Process 2]	[TODO]	[TODO]	High/Medium/Low	[TODO]	[TODO]
P-003	[TODO: Process 3]	[TODO]	[TODO]	High/Medium/Low	[TODO]	[TODO]

Total Number of Processes: [TODO]

5.3.2 3.2 Applications

ID	Application	Owner	Purpose	User Group	Interfaces	Hosting	Criticality
A-001	[TODO: App 1]	[TODO]	[TODO]	[TODO]	[TODO]	On-Prem/Cloud/SaaS	High/Medium/Low
A-002	[TODO: App 2]	[TODO]	[TODO]	[TODO]	[TODO]	On-Prem/Cloud/SaaS	High/Medium/Low
A-003	[TODO: App 3]	[TODO]	[TODO]	[TODO]	[TODO]	On-Prem/Cloud/SaaS	High/Medium/Low

Total Number of Applications: [TODO]

Hosting Distribution: - On-Premise: [TODO] - Cloud (IaaS/PaaS): [TODO] - SaaS: [TODO]

5.3.3 3.3 IT Systems and Components

ID	System/Component	Type	Owner	Location/Region	Operation	IP Address	Notes
S-001	{{ netbox.device.server_001 }}	Server	Anna Schmidt	{{ meta.organization.primary_location }}	Internal	{{ netbox.ip_address.server_001 }}	[TODO]
S-002	[TODO: System 2]	Database	Anna Schmidt	[TODO]	Internal/External	[TODO]	[TODO]
S-003	[TODO: System 3]	Storage	Anna Schmidt	[TODO]	Internal/External	[TODO]	[TODO]
S-004	[TODO: System 4]	Firewall	Anna Schmidt	[TODO]	Internal	[TODO]	[TODO]

Total Number of IT Systems: [TODO]

System Types: - Servers: [TODO] - Databases: [TODO] - Storage: [TODO] - Network Components: [TODO] - Security Components: [TODO] - Clients: [TODO]

5.3.4 3.4 Networks and Communication

ID	Network/Zone	Purpose	Segmentation	Internet Access	VLAN ID	Operator	Security Zone
N-001	Management Network	Administration	Yes	No	{{ netbox.vlan.management }}	Anna Schmidt	High Security
N-002	Production Network	Business Applications	Yes	Yes (filtered)	[TODO]	Anna Schmidt	Secure
N-003	DMZ	External Services	Yes	Yes	[TODO]	Anna Schmidt	Medium
N-004	Guest WLAN	Guests	Yes	Yes (isolated)	[TODO]	Anna Schmidt	Low

Total Number of Network Segments: [TODO]

Security Zones: - High Security (Management, critical systems): [TODO] - Secure (Production systems): [TODO] - Medium (DMZ, external interfaces): [TODO] - Low (Guest network): [TODO]

5.3.5 3.5 Rooms and Locations

ID	Location/Room	Type	Protection Measures	Access	Operator	Criticality
R-001	{{ meta.organization.primary_location }}	Main Location	[TODO]	Access Control	AdminSend GmbH	High

ID	Location/Room	Type	Protection Measures	Access	Operator	Criticality
R-002	Data Center	Server Room	Climate Control, Fire Protection, Access Control	Authorized	AdminSend GmbH	High
R-003	[TODO: Room 3]	[TODO]	[TODO]	[TODO]	[TODO]	Medium/Low

Total Number of Locations: [TODO]
Total Number of Critical Rooms: [TODO]

5.3.6 3.6 External Service Providers and Cloud Providers

ID	Service Provider	Service	Criticality	Contract	Certifications	Location	Notes
D-001	[TODO: Provider 1]	[TODO: Service]	High/Medium/Low	[TODO: Contract No.]	[TODO: ISO 27001, etc.]	[TODO]	[TODO]
D-002	[TODO: Provider 2]	[TODO: Service]	High/Medium/Low	[TODO]	[TODO]	[TODO]	[TODO]

Total Number of Service Providers: [TODO]

5.3.7 3.7 Personnel and Roles

Role	Name	Area of Responsibility	Contact	Deputy
Executive Management	Max Mustermann	Overall Responsibility	max.mustermann@adminsend.de	[TODO]
ISO	Thomas Weber	ISMS Coordination	thomas.weber@adminsend.de	[TODO]
IT Management	Anna Schmidt	IT Operations	anna.schmidt@adminsend.de	[TODO]
[TODO: Additional Roles]	[TODO]	[TODO]	[TODO]	[TODO]

5.4 4. Dependencies and Interfaces

5.4.1 4.1 Internal Dependencies

Network Diagram

Figure 5.1: Network Diagram

Application Architecture

Figure 5.2: Application Architecture

From (Source)	To (Target)	Type	Criticality	Notes
[TODO: System A]	[TODO: System B]	Data Flow	High/Medium/Low	[TODO]
[TODO: Application X]	[TODO: Database Y]	Data Access	High/Medium/Low	[TODO]

5.4.2 4.2 External Interfaces

Interface	Partner/Provider	Direction	Data Types	Protocol	Security Measures
[TODO: Interface 1]	[TODO]	Inbound/Outbound/Bidirectional	[TODO]	[TODO]	[TODO: VPN, TLS, etc.]
[TODO: Interface 2]	[TODO]	Inbound/Outbound/Bidirectional	[TODO]	[TODO]	[TODO]

5.5 5. Diagrams and Visualizations

5.5.1 5.1 Network Diagram

[TODO: Create a network diagram with all segments and zones]

5.5.2 5.2 Application Architecture

[TODO: Create a diagram of the application landscape]

5.5.3 5.3 Data Flow Diagram

[TODO: Create a data flow diagram for critical processes]

5.6 6. Validation and Quality Assurance

5.6.1 6.1 Validation Process

The structure analysis is validated by: 1. **Review by IT Management:** Anna Schmidt 2. **Review by Information Domain Managers:** [TODO] 3. **Comparison with CMDB/Inventory:** [TODO: Date] 4. **Approval by ISO:** Thomas Weber

Data Flow Diagram

Figure 5.3: Data Flow Diagram

5.6.2 6.2 Completeness Check

Category	Number Captured	Completeness	Notes
Business Processes	[TODO]	[TODO: %]	[TODO]
Applications	[TODO]	[TODO: %]	[TODO]
IT Systems	[TODO]	[TODO: %]	[TODO]
Networks	[TODO]	[TODO: %]	[TODO]
Rooms	[TODO]	[TODO: %]	[TODO]
Service Providers	[TODO]	[TODO: %]	[TODO]

5.7 7. Update and Maintenance

The structure analysis is updated when: - New IT systems or applications - Changes in network architecture - New service providers or cloud services - Organizational changes - At least annually as part of ISMS review

Responsible: Thomas Weber (ISO)
Next Review: {{ meta.document.next_review }}

5.8 8. Approval

Role	Name	Date	Approval
ISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI Standard 200-2: IT-Grundschutz Methodology (Chapter 5: Structure Analysis) - BSI IT-Grundschutz Compendium

ewpage

Chapter 6

Protection Needs Assessment (Template)

Document ID: 0060
Document Type: Methodology Artifact
Reference Framework: BSI IT-Grundschutz (BSI Standard 200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

6.1 1. Objective and Purpose

The protection needs assessment systematically determines the protection requirements for business processes, information, applications, and IT systems of **AdminSend GmbH**. It forms the basis for: - Selection of appropriate security measures - Prioritization of security investments - Risk analysis (Document 0090) - Compliance evidence

Responsible: Thomas Weber (ISB)

6.2 2. Protection Needs Categories and Criteria

6.2.1 2.1 Protection Objectives

The protection needs assessment is conducted for the following protection objectives:

6.2.1.1 2.1.1 Confidentiality

Protection against unauthorized disclosure of information.

Category	Description	Damage Examples
Normal	Limited negative impacts	Minor impairment, internal embarrassment
High	Considerable negative impacts	Violation of laws, significant financial damage, reputational damage
Very High	Existential impacts	Existential threat, catastrophic reputational damage, criminal consequences

6.2.1.2 2.1.2 Integrity

Protection against unauthorized modification of information.

Category	Description	Damage Examples
Normal	Limited negative impacts	Correctable errors, minor impact on business processes
High	Considerable negative impacts	Significant business process disruptions, financial losses, compliance violations
Very High	Existential impacts	Critical business process failures, existential financial damage

6.2.1.3 2.1.3 Availability

Ensuring the availability of information and systems.

Category	Description	Tolerable Downtime	Damage Examples
Normal	Limited negative impacts	$>$ 24 hours	Minor productivity losses, inconveniences
High	Considerable negative impacts	4-24 hours	Significant productivity losses, customer complaints, financial losses
Very High	Existential impacts	$<$ 4 hours	Critical business process failures, massive financial losses, existential threat

6.2.1.4 2.1.4 Authenticity (Optional)

Ensuring the genuineness and credibility of information.

Category	Description	Damage Examples
Normal	Limited negative impacts	Minor doubts about authenticity, correctable
High	Considerable negative impacts	Significant legal or financial consequences
Very High	Existential impacts	Existential legal or financial consequences

6.2.1.5 2.1.5 Accountability (Optional)

Ensuring the traceability of actions.

Category	Description	Damage Examples
Normal	Limited negative impacts	Difficult troubleshooting, minor compliance risks
High	Considerable negative impacts	Compliance violations, difficult incident investigation
Very High	Existential impacts	Severe compliance violations, impossible incident investigation

6.2.2 2.2 Assessment Scale

Assessment Criteria: - Legal and regulatory requirements (GDPR, IT Security Act, etc.) - Contractual obligations - Business criticality - Financial impacts - Reputational risks - Personal data - Trade secrets

6.3 3. Protection Needs Assessment

6.3.1 3.1 Business Processes

Process ID	Process	Owner	C	I	A	Justification	Overall Protection Need
P-001	[TODO: Process 1]	[TODO]	Normal/High/Very High	Normal/High/Very High	Normal/High/Very High	[TODO: Justification]	[TODO: Maximum Principle]
P-002	[TODO: Process 2]	[TODO]	Normal/High/Very High	Normal/High/Very High	Normal/High/Very High	[TODO]	[TODO]
P-003	[TODO: Process 3]	[TODO]	Normal/High/Very High	Normal/High/Very High	Normal/High/Very High	[TODO]	[TODO]

Total Number of Processes: [TODO]
Distribution: - Normal: [TODO] - High: [TODO] - Very High: [TODO]

6.3.2 3.2 Information and Data

Info ID	Information/Data Type	Process	C	I	A	Justification	Overall Protection Need
I-001	Personal Data (GDPR)	[TODO]	High	High	Normal	GDPR requirements	High
I-002	Trade Secrets	[TODO]	Very High	High	Normal	Competitive advantage	Very High
I-003	Financial Data	[TODO]	High	Very High	High	Legal requirements	Very High
I-004	[TODO: Additional Data]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Total Number of Information Types: [TODO]

6.3.3 3.3 Applications

Application ID	Application	Process	C	I	A	Justification	Overall Protection Need
A-001	[TODO: Application 1]	P-001	[TODO]	[TODO]	[TODO]	Inherited from Process P-001	[TODO]
A-002	[TODO: Application 2]	P-002	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
A-003	[TODO: Application 3]	P-003	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Total Number of Applications: [TODO]

6.3.4 3.4 IT Systems and Components

System ID	System/Component	Application	C	I	A	Justification	Overall Protection Need
S-001	{{ netbox.device.server_001 }}	A-001	[TODO]	[TODO]	[TODO]	Inherited from Application A-001	[TODO]
S-002	[TODO: System 2]	A-002	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
S-003	[TODO: System 3]	A-003	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Total Number of IT Systems: [TODO]

6.3.5 3.5 Networks

Network ID	Network/Zone	Systems	C	I	A	Justification	Overall Protection Need
N-001	Management Network	S-001, S-002	Very High	Very High	High	Critical administrative access	Very High
N-002	Production Network	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
N-003	DMZ	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Total Number of Networks: [TODO]

6.3.6 3.6 Rooms and Locations

Room ID	Room/Location	Systems	C	I	A	Justification	Overall Protection Need
R-001	Data Center	All critical servers	Very High	Very High	Very High	Hosting critical systems	Very High
R-002	{{ meta.organization.primary_location }}	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Total Number of Rooms: [TODO]

6.4 4. Protection Needs Inheritance and Dependencies

6.4.1 4.1 Inheritance Principle

Protection needs are inherited according to the **Maximum Principle**:

```
Business Process
    ↓ (inherits protection need)
Information
    ↓ (inherits protection need)
Applications
    ↓ (inherits protection need)
IT Systems
    ↓ (inherits protection need)
Networks, Rooms
```

Example: - Process P-001 has protection need "Very High" for confidentiality - Application A-001 supports Process P-001 - → Application A-001 inherits protection need "Very High" for confidentiality - Server S-001 hosts Application A-001 - → Server S-001 inherits protection need "Very High" for confidentiality

6.4.2 4.2 Inheritance Table

From (Source)	To (Target)	Inherited Protection Need	Justification
P-001	A-001	C: Very High, I: High, A: High	Application supports critical process
A-001	S-001	C: Very High, I: High, A: High	Server hosts critical application
[TODO]	[TODO]	[TODO]	[TODO]

6.4.3 4.3 Exceptions and Justifications

Exceptions to the Maximum Principle:

Object	Expected Protection Need	Actual Protection Need	Justification	Approved By
[TODO: Object]	[TODO]	[TODO]	[TODO: Justification for deviation]	Thomas Weber

Important: Exceptions must be documented and approved.

6.4.4 4.4 Cumulative Effects

When a system hosts multiple applications with different protection needs, the **Maximum Principle** applies:

System	Application 1	Application 2	Application 3	Resulting Protection Need
S-001	C: High	C: Very High	C: Normal	C: Very High (Maximum)
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

6.5 5. Validation and Quality Assurance

6.5.1 5.1 Validation Process

The protection needs assessment is validated by:

1. **Review by Process Owners:** Confirmation of business criticality
2. **Review by IT Management:** Anna Schmidt - Technical feasibility
3. **Review by Legal/Compliance:** Legal requirements
4. **Review by Data Protection:** GDPR compliance
5. **Approval by ISB:** Thomas Weber

6.5.2 5.2 Consistency Check

Check Criterion	Status	Comments
All processes assessed	[TODO: /]	[TODO]
All applications assessed	[TODO: /]	[TODO]
All IT systems assessed	[TODO: /]	[TODO]
Inheritance consistent	[TODO: /]	[TODO]
Exceptions documented	[TODO: /]	[TODO]
Justifications complete	[TODO: /]	[TODO]

6.6 6. Impact on Security Measures

6.6.1 6.1 Measures by Protection Need

Protection Need	Exemplary Measures
Normal	Standard security measures, basic hardening, standard backup
High	Enhanced security measures, encryption, MFA, extended monitoring, redundant systems
Very High	Maximum security measures, end-to-end encryption, hardware tokens, 24/7 monitoring, high availability, disaster recovery

6.6.2 6.2 Prioritization of Measures

Security measures are prioritized according to: 1. **Very High Protection Need:** Highest priority 2. **High Protection Need:** High priority 3. **Normal Protection Need:** Normal priority

6.7 7. Documentation and Evidence

The following documents and evidence are maintained: - This protection needs assessment document - Assessment workshop protocols - Process owner approvals - Exception approvals - Change logs

6.8 8. Update and Maintenance

The protection needs assessment is updated when: - New business processes or applications are introduced - Significant changes to existing processes occur - New legal requirements emerge - Security incidents occur - At least annually as part of the ISMS review

Responsible: Thomas Weber (ISB)
Next Review: {{ meta.document.next_review }}

6.9 9. Approval

Role	Name	Date	Approval
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI Standard 200-2: IT-Grundschutz Methodology (Chapter 6: Protection Needs Assessment) - BSI IT-Grundschutz Compendium

ewpage

Chapter 7

Modeling: Module Assignment (Template)

Document ID: 0070
Document Type: Methodology Artifact
Reference Framework: BSI IT-Grundschutz (BSI Standard 200-2, IT-Grundschutz Compendium)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

7.1 1. Objective and Purpose

The modeling assigns appropriate IT-Grundschutz modules to the objects of the information domain of **AdminSend GmbH**. It forms the basis for: - Basic security check (Document 0080) - Identification of requirements to be implemented - Systematic security measure planning

Responsible: Thomas Weber (ISB)

Important: This document only references modules. The complete module texts are located in the BSI IT-Grundschutz Compendium and are not copied.

7.2 2. IT-Grundschutz Modules: Overview

7.2.1 2.1 Module Structure

The BSI IT-Grundschutz Compendium organizes modules into the following layers:

Layer	Abbreviation	Description	Examples
ISMS	ISMS	Security Management	ISMS.1 Security Management
Organization and Personnel	ORP	Organizational Processes	ORP.1 Organization, ORP.3 Awareness and Training
Conception and Approaches	CON	Concepts and Methods	CON.1 Crypto Concept, CON.3 Data Backup Concept
Operations	OPS	IT Operations Processes	OPS.1.1.2 Proper IT Administration
Detection and Response	DER	Incident Management	DER.1 Detection of Security-Relevant Events
Systems	SYS	IT Systems	SYS.1.1 General Server, SYS.2.1 General Client
Applications	APP	Application Software	APP.1.1 Office Products, APP.3.1 Web Applications
IT Systems	NET	Networks and Communication	NET.1.1 Network Architecture and Design, NET.3.1 Routers and Switches
Industrial IT	IND	OT/ICS Systems	IND.1 Operational and Control Technology

7.2.2 2.2 Assignment Logic

Principles: 1. **Completeness:** All relevant objects receive module assignments 2. **Appropriateness:** Modules match the object type and protection need 3. **No Redundancy:** Each module is assigned only once per object 4. **Granularity:** Assignment at a meaningful abstraction level

Approach: 1. Adopt objects from structure analysis (Document 0050) 2. Identify suitable modules from IT-Grundschutz Compendium 3. Document assignment 4. Validation by IT management and ISB

7.3 3. Module Assignment

7.3.1 3.1 ISMS and Organization (ISMS, ORP)

Object ID	Object	Object Class	Assigned Modules	Justification	Owner
ORG-001	AdminSend GmbH	Organization	ISMS.1 Security Management	Overall organization	Thomas Weber
ORG-001	AdminSend GmbH	Organization	ORP.1 Organization	Organizational structure	Thomas Weber
ORG-001	AdminSend GmbH	Organization	ORP.2 Personnel	Personnel management	[TODO: HR]
ORG-001	AdminSend GmbH	Organization	ORP.3 Awareness and Training	Awareness program	Thomas Weber
ORG-001	AdminSend GmbH	Organization	ORP.4 Identity and Access Management	IAM processes	Anna Schmidt
ORG-001	AdminSend GmbH	Organization	ORP.5 Compliance Management (Requirements Management)	Compliance	[TODO]

7.3.2 3.2 Conception and Approaches (CON)

Object ID	Object	Object Class	Assigned Modules	Justification	Owner
CON-001	Crypto Concept	Concept	CON.1 Crypto Concept	Encryption strategy	Thomas Weber
CON-002	Data Backup Concept	Concept	CON.3 Data Backup Concept	Backup strategy	Anna Schmidt
CON-003	Deletion Concept	Concept	CON.6 Deletion and Destruction	Data deletion	Thomas Weber
CON-004	Patch and Change Management	Concept	CON.7 Information Security on Business Trips	[TODO: if applicable]	[TODO]
CON-005	Software Development	Concept	CON.8 Software Development	[TODO: if applicable]	[TODO]

7.3.3 3.3 Operations (OPS)

Object ID	Object	Object Class	Assigned Modules	Justification	Owner
OPS-001	IT Operations	Operations Process	OPS.1.1.2 Proper IT Administration	IT administration	Anna Schmidt
OPS-002	Patch Management	Operations Process	OPS.1.1.3 Patch and Change Management	Patch process	Anna Schmidt
OPS-003	Protection Against Malware	Operations Process	OPS.1.1.4 Protection Against Malware	Malware protection	Anna Schmidt
OPS-004	Data Backup	Operations Process	OPS.1.1.5 Logging	Logging	Anna Schmidt
OPS-005	Software Tests	Operations Process	OPS.1.1.6 Software Tests and Releases	[TODO: if applicable]	[TODO]
OPS-006	Outsourcing	Operations Process	OPS.2.1 Outsourcing for Customers	[TODO: if applicable]	[TODO]
OPS-007	Cloud Usage	Operations Process	OPS.2.2 Cloud Usage	Cloud services	Anna Schmidt

7.3.4 3.4 Detection and Response (DER)

Object ID	Object	Object Class	Assigned Modules	Justification	Owner
DER-001	Detection	Process	DER.1 Detection of Security-Relevant Events	SIEM, Monitoring	Anna Schmidt
DER-002	Incident Management	Process	DER.2.1 Handling of Security Incidents	Incident response	Thomas Weber
DER-003	Forensics	Process	DER.2.2 Preparation for IT Forensics	[TODO: if applicable]	[TODO]
DER-004	Audits	Process	DER.3.1 Audits and Reviews	Internal audit	[TODO]

7.3.5 3.5 Applications (APP)

Object ID	Object	Object Class	Assigned Modules	Justification	Owner
A-001	[TODO: Application 1]	Application	APP.1.1 Office Products	[TODO: if office application]	[TODO]
A-002	[TODO: Application 2]	Application	APP.3.1 Web Applications	[TODO: if web application]	[TODO]
A-003	[TODO: Application 3]	Application	APP.3.2 Web Server	[TODO: if web server]	Anna Schmidt
A-004	[TODO: Application 4]	Application	APP.3.3 File Server	[TODO: if file server]	Anna Schmidt
A-005	[TODO: Application 5]	Application	APP.3.6 DNS Server	[TODO: if DNS]	Anna Schmidt
A-006	[TODO: Application 6]	Application	APP.4.3 Relational Database Systems	[TODO: if database]	Anna Schmidt
A-007	[TODO: Application 7]	Application	APP.5.1 General Groupware	[TODO: if groupware]	[TODO]
A-008	[TODO: Application 8]	Application	APP.5.2 Microsoft Exchange and Outlook	[TODO: if Exchange]	Anna Schmidt

7.3.6 3.6 IT Systems (SYS)

Object ID	Object	Object Class	Assigned Modules	Justification	Owner
S-001	{{ net-box.device.server_001 }}	Server	SYS.1.1 General Server	General server	Anna Schmidt
S-002	[TODO: Linux Server]	Server	SYS.1.3 Server under Linux and Unix	Linux server	Anna Schmidt
S-003	[TODO: Windows Server]	Server	SYS.1.2.3 Windows Server	Windows server	Anna Schmidt
S-004	[TODO: Virtualization]	Virtualization	SYS.1.5 Virtualization	VMware/Hyper-V	Anna Schmidt
S-005	[TODO: Container]	Container	SYS.1.6 Containerization	Docker/Kubernetes	Anna Schmidt

Object ID	Object	Object Class	Assigned Modules	Justification	Owner
S-006	[TODO: Storage]	Storage	SYS.1.8 Storage Solutions	SAN/NAS	Anna Schmidt
S-007	[TODO: Client]	Client	SYS.2.1 General Client	Workstations	Anna Schmidt
S-008	[TODO: Windows Client]	Client	SYS.2.2.3 Clients under Windows	Windows clients	Anna Schmidt
S-009	[TODO: macOS Client]	Client	SYS.2.4 Clients under macOS	macOS clients	Anna Schmidt
S-010	[TODO: Mobile Device]	Mobile	SYS.3.2.1 General Smartphones and Tablets	Mobile devices	Anna Schmidt
S-011	[TODO: IoT]	IoT	SYS.4.4 General IoT Device	[TODO: if IoT]	[TODO]

7.3.7 3.7 Networks and Communication (NET)

Object ID	Object	Object Class	Assigned Modules	Justification	Owner
N-001	Network Architecture	Network	NET.1.1 Network Architecture and Design	Overall network	Anna Schmidt
N-002	Network Management	Network	NET.1.2 Network Management	Network monitoring	Anna Schmidt
N-003	[TODO: Routers/Switches]	Network Component	NET.3.1 Routers and Switches	Network devices	Anna Schmidt
N-004	[TODO: Firewall]	Security Component	NET.3.2 Firewall	Perimeter protection	Anna Schmidt
N-005	[TODO: VPN]	Security Component	NET.3.3 VPN	Remote access	Anna Schmidt
N-006	[TODO: WLAN]	Network	NET.2.1 WLAN Operations	Wireless network	Anna Schmidt
N-007	[TODO: Email]	Communication	NET.4.1 TLS Encryption	[TODO: if applicable]	Anna Schmidt

7.3.8 3.8 Industrial IT (IND) - Optional

Object ID	Object	Object Class	Assigned Modules	Justification	Owner
IND-001	[TODO: OT System]	OT/ICS	IND.1 Operational and Control Technology	[TODO: if OT in scope]	[TODO]
IND-002	[TODO: ICS Component]	OT/ICS	IND.2.1 General ICS Component	[TODO: if ICS in scope]	[TODO]

7.3.9 3.9 Rooms and Infrastructure (INF)

Object ID	Object	Object Class	Assigned Modules	Justification	Owner
R-001	Data Center	Room	INF.2 Data Center and Server Room	Critical server room	[TODO: Facility]
R-002	{{ meta.organization.primary_location }}	Building	INF.1 General Building	Main location	[TODO: Facility]
R-003	[TODO: Office Room]	Room	INF.8 Home Office	[TODO: if home office]	[TODO]

7.4 4. Summary and Statistics

7.4.1 4.1 Assignment Statistics

Module Layer	Number of Assigned Modules	Number of Affected Objects
ISMS	[TODO]	[TODO]
ORP (Organization and Personnel)	[TODO]	[TODO]
CON (Conception)	[TODO]	[TODO]
OPS (Operations)	[TODO]	[TODO]
DER (Detection and Response)	[TODO]	[TODO]
APP (Applications)	[TODO]	[TODO]
SYS (Systems)	[TODO]	[TODO]
NET (Networks)	[TODO]	[TODO]
IND (Industrial IT)	[TODO]	[TODO]
INF (Infrastructure)	[TODO]	[TODO]
Total	**[TODO]**	**[TODO]**

7.4.2 4.2 Completeness Check

Object Type	Number of Objects	Number with Module Assignment	Completeness
Processes	[TODO]	[TODO]	[TODO: %]
Applications	[TODO]	[TODO]	[TODO: %]
IT Systems	[TODO]	[TODO]	[TODO: %]
Networks	[TODO]	[TODO]	[TODO: %]
Rooms	[TODO]	[TODO]	[TODO: %]

7.4.3 4.3 Open Items

ID	Object	Issue	Responsible	Deadline
[TODO]	[TODO]	[TODO: No suitable module found]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO: Unclear assignment]	[TODO]	[TODO]

7.5 5. Validation and Quality Assurance

7.5.1 5.1 Validation Process

The module assignment is validated by: 1. **Review by IT Management:** Anna Schmidt - Technical correctness 2. **Review by Information Domain Responsible:** Completeness 3. **Comparison with IT-Grundschutz Compendium:** Currency of modules 4. **Approval by ISB:** Thomas Weber

7.5.2 5.2 Quality Criteria

Criterion	Status	Comments
All objects have module assignments	[TODO: /]	[TODO]
Modules are current (IT-Grundschutz Compendium Edition [TODO])	[TODO: /]	[TODO]
Assignments are comprehensibly justified	[TODO: /]	[TODO]
No redundancies	[TODO: /]	[TODO]
Owners are named	[TODO: /]	[TODO]

7.6 6. Next Steps

After completing the modeling, the following steps follow: 1. **Basic Security Check (Document 0080):** Target-actual comparison for all assigned modules 2. **Risk Analysis (Document 0090):** For objects with increased protection needs or non-modelable risks 3. **Measure Planning (Document 0100):** Implementation planning of identified requirements

7.7 7. Update and Maintenance

The module assignment is updated when: - New IT systems or applications are introduced - Changes in IT architecture occur - New edition of IT-Grundschutz Compendium is released - At least annually as part of the ISMS review

Responsible: Thomas Weber (ISB)
Next Review: {{ meta.document.next_review }}

7.8 8. Approval

Role	Name	Date	Approval
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI Standard 200-2: IT-Grundschutz Methodology (Chapter 7: Modeling) - BSI IT-Grundschutz Compendium (current edition) - BSI IT-Grundschutz Compendium: https://www.bsi.bund.de/grundschutz-kompendium

ewpage

Chapter 8

Basic Security Check / Gap Analysis (Template)

Document ID: 0080
Document Type: Methodology Artifact
Reference Framework: BSI IT-Grundschutz (BSI Standard 200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

8.1 1. Objective and Purpose

The basic security check systematically assesses the extent to which the IT-Grundschutz requirements modeled for the information domain of **AdminSend GmbH** have been implemented. It forms the basis for: - Identification of security gaps - Prioritization of measures - Measure planning (Document 0100) - Compliance evidence

Responsible: Thomas Weber (ISB)

8.2 2. Approach and Methodology

8.2.1 2.1 Data Sources

The following sources are used for the basic security check:

Data Source	Type	Responsible	Usage
Interviews with stakeholders	Primary source	Thomas Weber	Process and organizational requirements

Data Source	Type	Responsible	Usage
Configuration evidence	Technical	Anna Schmidt	Technical requirements
Policies and guidelines	Document	Thomas Weber	Organizational requirements
Tickets and change records	System	Anna Schmidt	Implementation evidence
Logs and monitoring data	System	Anna Schmidt	Operational requirements
Audit reports	Document	[TODO: Internal Audit]	External validation

8.2.2 2.2 Assessment Logic

Fulfillment Levels:

Status	Abbreviation	Description	Criteria
Fulfilled	F	Requirement fully implemented	All aspects of the requirement are implemented and evidenced
Partially Fulfilled	P	Requirement partially implemented	Essential aspects implemented, but gaps exist
Not Fulfilled	N	Requirement not implemented	Requirement not or only minimally implemented
Not Applicable	N/A	Requirement not relevant	Requirement does not apply to organization
Not Assessed	-	Not yet reviewed	Assessment pending

8.2.3 2.3 Sample Size

Review Depth: - **Critical Requirements (Protection Need "Very High"):** 100% review - **Important Requirements (Protection Need "High"):** 50% sample - **Standard Requirements (Protection Need "Normal"):** 25% sample

Review Methods: - Document review - Configuration review - Interviews - Technical tests (samples)

8.2.4 2.4 Execution

Timeline: - **Start:** [TODO] - **Data Collection:** [TODO: e.g., 4 weeks] - **Assessment:** [TODO: e.g., 2 weeks] - **Validation:** [TODO: e.g., 1 week] - **Completion:** [TODO]

Participants: - ISB: Thomas Weber - IT Management: Anna Schmidt - Information Domain Responsible: [TODO] - Departments: [TODO]

8.3 3. Basic Security Check: Results

8.3.1 3.1 ISMS and Organization (ISMS, ORP)

Module	Requirement (Short)	Object	Status	Evidence	Finding	Measure	Owner	Target Date
ISMS.1	Security policy created	AdminSend GmbH	F	Document 0010	-	-	Thomas Weber	-
ISMS.1	ISMS organization defined	AdminSend GmbH	F	Document 0020	-	-	Thomas Weber	-
ISMS.1	Resources provided	AdminSend GmbH	P	Budget evidence	Budget insufficient	Increase budget	Max Mustermann	[TODO]
ORP.1	Roles and responsibilities defined	AdminSend GmbH	F	Document 0020	-	-	Thomas Weber	-
ORP.2	Onboarding of new employees	AdminSend GmbH	P	HR process	No security training in onboarding	Integrate security training	[TODO: HR]	[TODO]
ORP.3	Awareness program	AdminSend GmbH	N	-	No awareness program exists	Establish awareness program	Thomas Weber	[TODO]
ORP.4	IAM process	AdminSend GmbH	P	IAM guideline	Recertification missing	Implement recertification process	Anna Schmidt	[TODO]

8.3.2 3.2 Conception and Approaches (CON)

Module	Requirement (Short)	Object	Status	Evidence	Finding	Measure	Owner	Target Date
CON.1	Crypto concept created	Crypto concept	N	-	No crypto concept exists	Create crypto concept	Thomas Weber	[TODO]

Module	Requirement (Short)	Object	Status	Evidence	Finding	Measure	Owner	Target Date
CON.3	Data backup concept created	Backup concept	F	Backup documentation	-	-	Anna Schmidt	-
CON.3	Backup tests performed	Backup process	P	Test protocols	Tests not regular	Establish quarterly backup tests	Anna Schmidt	[TODO]
CON.6	Deletion concept created	Deletion concept	N	-	No deletion concept exists	Create deletion concept	Thomas Weber	[TODO]

8.3.3 3.3 Operations (OPS)

Module	Requirement (Short)	Object	Status	Evidence	Finding	Measure	Owner	Target Date
OPS.1.1.2	Administration concept	IT-Administration	P	Admin guideline	Privileged Access Management missing	Implement PAM solution	Anna Schmidt	[TODO]
OPS.1.1.3	Patch process established	Patch management	F	Patch documentation	-	-	Anna Schmidt	-
OPS.1.1.3	Patch SLAs defined	Patch management	P	SLA document	Critical patches > 30 days	Reduce SLA to 7 days	Anna Schmidt	[TODO]
OPS.1.1.4	Malware protection implemented	All systems	F	Antivirus solution	-	-	Anna Schmidt	-
OPS.1.1.5	Logging activated	All systems	P	Log configuration	Central log collection missing	Implement SIEM	Anna Schmidt	[TODO]
OPS.2.2	Cloud security concept	Cloud services	N	-	No cloud security concept	Create cloud security concept	Thomas Weber	[TODO]

8.3.4 3.4 Detection and Response (DER)

Module	Requirement (Short)	Object	Status	Evidence	Finding	Measure	Owner	Target Date
DER.1	Detection established	Monitoring	P	Monitoring tools	SIEM missing	Implement SIEM	Anna Schmidt	[TODO]
DER.2.1	Incident response process	Incident management	P	IR guideline	No incident response exercises	Establish annual IR exercise	Thomas Weber	[TODO]
DER.2.2	Forensics preparation	Forensics	N	-	No forensics preparation	Create forensics concept	Thomas Weber	[TODO]

8.3.5 3.5 Applications (APP)

Module	Requirement (Short)	Object	Status	Evidence	Finding	Measure	Owner	Target Date
APP.3.1	Secure web application development	[TODO: Web application]	P	SDLC process	SAST/DAST missing	Integrate security testing	[TODO]	[TODO]
APP.3.2	Web server hardening	[TODO: Web server]	F	Hardening checklist	-	-	Anna Schmidt	-
APP.4.3	Database hardening	[TODO: Database]	P	DB configuration	Encryption at rest missing	Activate TDE	Anna Schmidt	[TODO]

8.3.6 3.6 IT Systems (SYS)

Module	Requirement (Short)	Object	Status	Evidence	Finding	Measure	Owner	Target Date
SYS.1.1	Server hardening	{{ netbox.device.server_001 }}	F	Hardening baseline	-	-	Anna Schmidt	-
SYS.1.3	Linux hardening	[TODO: Linux server]	P	CIS Benchmark	Not all CIS controls implemented	Complete CIS implementation	Anna Schmidt	[TODO]

Module	Requirement (Short)	Object	Status	Evidence	Finding	Measure	Owner	Target Date
SYS.1.5	Virtualization security	[TODO: VMware]	P	VMware configuration	Network segmentation insufficient	Implement microsegmentation	Anna Schmidt	[TODO]
SYS.2.1	Client hardening	Workstations	P	GPO configuration	BitLocker not comprehensive	Activate BitLocker on all clients	Anna Schmidt	[TODO]
SYS.3.2.1	Mobile device management	Mobile devices	N	-	No MDM exists	Implement MDM solution	Anna Schmidt	[TODO]

8.3.7 3.7 Networks and Communication (NET)

Module	Requirement (Short)	Object	Status	Evidence	Finding	Measure	Owner	Target Date
NET.1.1	Network segmentation	Network architecture	P	Network diagram	Segmentation insufficient	Implement microsegmentation	Anna Schmidt	[TODO]
NET.1.2	Network monitoring	Network management	F	Monitoring tools	-	-	Anna Schmidt	-
NET.3.1	Router/switch hardening	Network devices	P	Configuration evidence	SNMP v3 not everywhere	SNMP v3 comprehensive	Anna Schmidt	[TODO]
NET.3.2	Firewall ruleset	Firewall	F	Firewall rules	-	-	Anna Schmidt	-
NET.3.3	VPN security	VPN	P	VPN configuration	MFA for VPN missing	Implement MFA for VPN	Anna Schmidt	[TODO]
NET.2.1	WLAN security	WLAN	F	WLAN configuration	-	-	Anna Schmidt	-

8.3.8 3.8 Infrastructure (INF)

Module	Requirement (Short)	Object	Status	Evidence	Finding	Measure	Owner	Target Date
INF.1	Building security	{{ meta.organization.primary_location }}	P	Security concept	Visitor management insufficient	Visitor management system	[TODO: Facility]	[TODO]
INF.2	Data center security	Data center	F	DC documentation	-	-	[TODO: Facility]	-

8.4 4. Summary and Statistics

8.4.1 4.1 Fulfillment Statistics

Module Layer	Total	Fulfilled (F)	Partial (P)	Not Fulfilled (N)	N/A	Fulfillment Rate
ISMS	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
ORP	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
CON	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
OPS	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
DER	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
APP	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
SYS	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
NET	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
INF	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
Total	**[TODO]**	**[TODO]**	**[TODO]**	**[TODO]**	**[TODO]**	**[TODO: %]**

Overall Fulfillment Rate: [TODO: %]

8.4.2 4.2 Critical Gaps (Priority 1)

ID	Requirement	Object	Risk	Measure	Owner	Target Date
GAP-001	[TODO: Critical gap 1]	[TODO]	Very high	[TODO]	[TODO]	[TODO]
GAP-002	[TODO: Critical gap 2]	[TODO]	Very high	[TODO]	[TODO]	[TODO]

8.4.3 4.3 Quick Wins (Priority 2)

ID	Requirement	Object	Effort	Benefit	Measure	Owner	Target Date
QW-001	[TODO: Quick win 1]	[TODO]	Low	High	[TODO]	[TODO]	[TODO]
QW-002	[TODO: Quick win 2]	[TODO]	Low	High	[TODO]	[TODO]	[TODO]

8.4.4 4.4 Medium-Term Measures (Priority 3)

ID	Requirement	Object	Effort	Measure	Owner	Target Date
MF-001	[TODO: Medium-term measure 1]	[TODO]	Medium	[TODO]	[TODO]	[TODO]
MF-002	[TODO: Medium-term measure 2]	[TODO]	Medium	[TODO]	[TODO]	[TODO]

8.5 5. Management Summary

8.5.1 5.1 Overall Assessment

Fulfillment Rate: [TODO: %]

Assessment: - [TODO: Summary assessment of security level] - [TODO: Main findings] - [TODO: Critical action areas]

8.5.2 5.2 Top 5 Findings

1. **[TODO: Finding 1]:** [TODO: Description and impact]
2. **[TODO: Finding 2]:** [TODO: Description and impact]
3. **[TODO: Finding 3]:** [TODO: Description and impact]
4. **[TODO: Finding 4]:** [TODO: Description and impact]
5. **[TODO: Finding 5]:** [TODO: Description and impact]

8.5.3 5.3 Resource Requirements

Estimated Effort for Measure Implementation: - **Person-days:** [TODO] - **Budget:** [TODO] - **External Support:** [TODO] - **Timeframe:** [TODO]

8.5.4 5.4 Dependencies

Measure	Dependency	Impact	Mitigation
[TODO: Measure 1]	[TODO: Dependency]	[TODO]	[TODO]
[TODO: Measure 2]	[TODO: Dependency]	[TODO]	[TODO]

8.6 6. Next Steps

1. **Measure Planning (Document 0100):** Detailed planning of identified measures
2. **Risk Analysis (Document 0090):** For objects with increased protection needs or non-modelable risks
3. **Management Presentation:** Presentation of results to executive management
4. **Measure Implementation:** Start of implementation of prioritized measures

8.7 7. Update and Maintenance

The basic security check is repeated: - After completion of significant measures - When significant changes occur in IT infrastructure - At least annually as part of the ISMS review

Responsible: Thomas Weber (ISB)
Next Check: {{ meta.document.next_review }}

8.8 8. Approval

Role	Name	Date	Approval
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI Standard 200-2: IT-Grundschutz Methodology (Chapter 8: Basic Security Check) - BSI IT-Grundschutz Compendium

ewpage

Chapter 9

Risk Analysis (BSI Standard 200-3) – Template

Document ID: 0090
Document Type: Methodology Artifact
Reference Framework: BSI IT-Grundschutz (BSI Standard 200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

9.1 1. Objective and Trigger

The risk analysis according to BSI Standard 200-3 identifies and assesses risks for **AdminSend GmbH** that are not covered by IT-Grundschutz modules.

Responsible: Thomas Weber (ISB)

Triggers for Risk Analysis: - High or very high protection need (see Document 0060) - Special threat situation (e.g., targeted attacks) - Deviations from IT-Grundschutz requirements - New technologies without suitable modules - External requirements (customers, regulation)

[TODO: Document specific triggers for this risk analysis]

9.2 2. Risk Objects and Scope

Affected Objects:

Object ID	Object	Type	Protection Need	Justification for Risk Analysis
[TODO]	[TODO]	Process/Application/System	Very high	[TODO]

Object ID	Object	Type	Protection Need	Justification for Risk Analysis
[TODO]	[TODO]	Process/Application/System	Very high	[TODO]

Interfaces and Providers: - [TODO: Document external interfaces and service providers]

9.3 3. Threats, Vulnerabilities and Scenarios

9.3.1 3.1 Threat Catalog

Threat ID	Threat	Category	Description
T-001	Targeted Cyber Attacks	External	APT attacks on critical systems
T-002	Ransomware	External	Encryption of critical data
T-003	Insider Threat	Internal	Abuse of privileged access
T-004	DDoS Attacks	External	Availability impairment
T-005	Supply Chain Attacks	External	Compromise via suppliers
[TODO]	[TODO]	[TODO]	[TODO]

9.3.2 3.2 Vulnerability Catalog

Vulnerability ID	Vulnerability	Object	Description
V-001	Insufficient Segmentation	Network	Missing microsegmentation
V-002	Missing MFA	VPN Access	Password-only authentication
V-003	Outdated Software	[TODO: System]	End-of-life software in use
[TODO]	[TODO]	[TODO]	[TODO]

9.3.3 3.3 Risk Scenarios

Scenario ID	Scenario	Threat	Vulnerability	Affected Object
S-001	Ransomware attack on production systems	T-002	V-001, V-002	[TODO: Production system]
S-002	Data theft by insider	T-003	V-002	[TODO: Database]

Scenario ID	Scenario	Threat	Vulnerability	Affected Object
S-003	DDoS on public services	T-004	[TODO]	[TODO: Web server]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

9.4 4. Risk Assessment

9.4.1 4.1 Assessment Scale

Likelihood:

Level	Description	Frequency
1 - Very Low	Unlikely	< 1x in 10 years
2 - Low	Rare	1x in 5-10 years
3 - Medium	Occasional	1x in 1-5 years
4 - High	Probable	1x per year
5 - Very High	Very probable	Multiple times per year

Impact (Damage Level):

Level	Description	Financial Impact	Business Impact
1 - Very Low	Negligible	< 10,000 €	No significant impairment
2 - Low	Limited	10,000 - 50,000 €	Minor impairment
3 - Medium	Considerable	50,000 - 250,000 €	Noticeable impairment
4 - High	Severe	250,000 - 1,000,000 €	Significant impairment
5 - Very High	Catastrophic	> 1,000,000 €	Existential threat

Risk Matrix:

Likelihood	Impact 1	Impact 2	Impact 3	Impact 4	Impact 5
5 - Very High	Medium	High	High	Very High	Very High
4 - High	Medium	Medium	High	High	Very High
3 - Medium	Low	Medium	Medium	High	High
2 - Low	Low	Low	Medium	Medium	High
1 - Very Low	Low	Low	Low	Medium	Medium

9.4.2 4.2 Risk Acceptance Criteria

Risk Level	Treatment	Approval Required
Very High	Must be treated	Executive Management
High	Should be treated	ISB

Risk Level	Treatment	Approval Required
Medium	Can be treated	ISB
Low	Can be accepted	Information Domain Responsible

9.5 5. Risk Register

Risk ID	Object	Scenario	Threat	Vulnerability	Existing Measures	Likelihood	Impact	Risk (Before)	Treatment	Additional Measure	Owner	Deadline	Risk (After)
R-001	[TODO]	S-001	T-002	V-001, V-002	Antivirus, Backup	4	5	Very High	Mitigate	Microsegmentation, MFA	Anna Schmidt	[TODO]	Medium
R-002	[TODO]	S-002	T-003	V-002	Logging, IAM	3	4	High	Mitigate	PAM, DLP	Anna Schmidt	[TODO]	Low
R-003	[TODO]	S-003	T-004	[TODO]	Firewall	3	3	Medium	Mitigate	DDoS Protection	Anna Schmidt	[TODO]	Low
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Risk Treatment Options: - **Mitigate:** Implement additional measures - **Avoid:** Eliminate risk source - **Transfer:** Transfer risk to third parties (insurance, outsourcing) - **Accept:** Consciously accept risk (with approval)

9.6 6. Risk Assessment: Summary

Risk Distribution (Before Treatment): - Very High: [TODO] - High: [TODO] - Medium: [TODO] - Low: [TODO]

Risk Distribution (After Treatment): - Very High: [TODO] - High: [TODO] - Medium: [TODO] - Low: [TODO]

Top 5 Risks: 1. [TODO: Risk 1] 2. [TODO: Risk 2] 3. [TODO: Risk 3] 4. [TODO: Risk 4] 5. [TODO: Risk 5]

9.7 7. Approval and Risk Acceptance

9.7.1 7.1 Risk Owners

Risk ID	Risk	Risk Owner	Acceptance	Date
R-001	[TODO]	Max Mustermann	Accepted after measure implementation	[TODO]

Risk ID	Risk	Risk Owner	Acceptance	Date
R-002	[TODO]	Thomas Weber	Accepted after measure implementation	[TODO]

9.7.2 7.2 Management Approval

Role	Name	Date	Approval
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

9.8 8. Update and Maintenance

The risk analysis is updated when: - Significant changes in the threat landscape occur - New vulnerabilities or security incidents emerge - Changes to the information domain occur - At least annually as part of the ISMS review

Responsible: Thomas Weber (ISB)
Next Review: {{ meta.document.next_review }}

References: - BSI Standard 200-3: Risk Analysis based on IT-Grundschutz - BSI IT-Grundschutz Compendium

ewpage

Chapter 10

Security Concept and Action Plan

Document ID: 0100
Document Type: Plan/Control Document
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

10.1 1. Target Vision and Strategy

10.1.1 1.1 Security Objectives

AdminSend GmbH pursues the following strategic security objectives:

1. **[TODO: Objective 1]:** [TODO: Description]
2. **[TODO: Objective 2]:** [TODO: Description]
3. **[TODO: Objective 3]:** [TODO: Description]

10.1.2 1.2 Priorities

Prioritization by: - Criticality (protection need) - Risk level - Compliance requirements - Quick wins (effort vs. benefit) - Dependencies

10.1.3 1.3 Architectural Guardrails

Security Architecture Principles: - Defense in Depth (multi-layered security) - Zero Trust (Verify explicitly, Least privilege, Assume breach) - Secure by Design - Privacy by Design - [TODO: Additional principles]

10.2 2. Measure Catalog

10.2.1 2.1 Measures from Basic Security Check

Measure ID	Source	Description	Priority	Owner	Effort (PD)	Budget	Target Date	Dependencies	Status
M-001	Basic Check (GAP-001)	[TODO: Critical measure 1]	P1 - Critical	Thomas Weber	[TODO]	[TODO]	[TODO]	-	Open
M-002	Basic Check (QW-001)	[TODO: Quick win 1]	P2 - High	Anna Schmidt	[TODO]	[TODO]	[TODO]	-	Open
M-003	Basic Check	[TODO: Measure 3]	P3 - Medium	[TODO]	[TODO]	[TODO]	[TODO]	M-001	Open
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

10.2.2 2.2 Measures from Risk Analysis

Measure ID	Source	Description	Priority	Owner	Effort (PD)	Budget	Target Date	Dependencies	Status
M-101	Risk Analysis (R-001)	[TODO: Risk mitigation 1]	P1 - Critical	Anna Schmidt	[TODO]	[TODO]	[TODO]	-	Open
M-102	Risk Analysis (R-002)	[TODO: Risk mitigation 2]	P2 - High	Anna Schmidt	[TODO]	[TODO]	[TODO]	-	Open
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

10.2.3 2.3 Strategic Measures

Measure ID	Description	Priority	Owner	Effort (PD)	Budget	Target Date	Status
M-201	SIEM Implementation	P1 - Critical	Anna Schmidt	[TODO]	[TODO]	[TODO]	Open
M-202	Zero Trust Architecture	P2 - High	Anna Schmidt	[TODO]	[TODO]	[TODO]	Open

Measure ID	Description	Priority	Owner	Effort (PD)	Budget	Target Date	Status
M-203	Security Awareness Program	P2 - High	Thomas Weber	[TODO]	[TODO]	[TODO]	Open
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

10.3 3. Measure Prioritization

10.3.1 3.1 Priority 1 - Critical (Immediate)

Measure ID	Description	Owner	Target Date	Dependencies
M-001	[TODO]	[TODO]	[TODO]	-
M-101	[TODO]	[TODO]	[TODO]	-
M-201	[TODO]	[TODO]	[TODO]	-

Count: [TODO]
Total Effort: [TODO] PD
Total Budget: [TODO] €

10.3.2 3.2 Priority 2 - High (Short-term, 0-6 months)

Measure ID	Description	Owner	Target Date	Dependencies
M-002	[TODO]	[TODO]	[TODO]	-
M-102	[TODO]	[TODO]	[TODO]	M-001
M-202	[TODO]	[TODO]	[TODO]	M-201

Count: [TODO]
Total Effort: [TODO] PD
Total Budget: [TODO] €

10.3.3 3.3 Priority 3 - Medium (Medium-term, 6-12 months)

Measure ID	Description	Owner	Target Date	Dependencies
M-003	[TODO]	[TODO]	[TODO]	M-001
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Count: [TODO]
Total Effort: [TODO] PD
Total Budget: [TODO] €

10.3.4 3.4 Priority 4 - Low (Long-term, > 12 months)

Measure ID	Description	Owner	Target Date	Dependencies
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Count: [TODO]
Total Effort: [TODO] PD
Total Budget: [TODO] €

10.4 4. Roadmap

10.4.1 4.1 Quarter 1 (Q1 {{ meta.document.year }})

Focus: Close critical security gaps

Measure ID	Description	Owner	Status
M-001	[TODO]	[TODO]	Planned
M-101	[TODO]	[TODO]	Planned

10.4.2 4.2 Quarter 2 (Q2 {{ meta.document.year }})

Focus: Quick wins and basic security

Measure ID	Description	Owner	Status
M-002	[TODO]	[TODO]	Planned
M-201	[TODO]	[TODO]	Planned

10.4.3 4.3 Quarter 3 (Q3 {{ meta.document.year }})

Focus: Strategic measures

Measure ID	Description	Owner	Status
M-202	[TODO]	[TODO]	Planned
M-203	[TODO]	[TODO]	Planned

10.4.4 4.4 Quarter 4 (Q4 {{ meta.document.year }})

Focus: Consolidation and optimization

Measure ID	Description	Owner	Status
M-003	[TODO]	[TODO]	Planned
[TODO]	[TODO]	[TODO]	Planned

10.5 5. Resource Planning

10.5.1 5.1 Personnel Resources

Role	Effort (PD)	Availability	Gap
ISB	[TODO]	[TODO]	[TODO]
IT Management	[TODO]	[TODO]	[TODO]
IT Administrators	[TODO]	[TODO]	[TODO]
External Consultants	[TODO]	[TODO]	[TODO]
Total	**[TODO]**	**[TODO]**	**[TODO]**

10.5.2 5.2 Budget

Category	Budget	Usage
Software Licenses	[TODO] €	SIEM, PAM, EDR, etc.
Hardware	[TODO] €	Firewalls, servers, etc.
External Services	[TODO] €	Consulting, implementation
Training	[TODO] €	Awareness, technical training
Other	[TODO] €	[TODO]
Total	**[TODO] €**	

10.5.3 5.3 External Support

Service Provider	Service	Effort	Budget	Period
[TODO: Provider 1]	[TODO]	[TODO] PD	[TODO] €	[TODO]
[TODO: Provider 2]	[TODO]	[TODO] PD	[TODO] €	[TODO]

10.6 6. Dependencies and Risks

10.6.1 6.1 Critical Dependencies

Measure	Dependency	Impact	Mitigation
M-202 (Zero Trust)	M-201 (SIEM)	Delay	Parallel planning
[TODO]	[TODO]	[TODO]	[TODO]

10.6.2 6.2 Implementation Risks

Risk	Likelihood	Impact	Mitigation	Owner
Resource shortage	High	Delay	External support	Thomas Weber
Budget cut	Medium	Prioritization	Focus on P1 measures	Max Mustermann

Risk	Likelihood	Impact	Mitigation	Owner
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

10.7 7. Success Measurement

10.7.1 7.1 Success Criteria

Criterion	Target	Measurement
Measure implementation	100% P1 measures by [TODO]	Action plan tracking
IT-Grundschutz fulfillment	> 80% by [TODO]	Basic security check
Risk reduction	No “Very High” risks	Risk register
[TODO]	[TODO]	[TODO]

10.7.2 7.2 Milestones

Milestone	Date	Criterion	Status
M1: Critical gaps closed	[TODO]	All P1 measures implemented	Planned
M2: Basic security achieved	[TODO]	80% fulfillment rate	Planned
M3: Strategic measures implemented	[TODO]	SIEM, Zero Trust productive	Planned
M4: IT-Grundschutz certification	[TODO]	Certification received	Planned

10.8 8. Governance and Control

Control Committee: ISMS Team (see Document 0020)

Regular Meetings: - **Weekly:** Measure status update (ISB, IT Management) - **Monthly:** ISMS team meeting (progress, escalations) - **Quarterly:** Management review (Executive Management)

Reporting: See Document 0110 (Implementation Control and KPIs)

10.9 9. Approval

Role	Name	Date	Approval
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Role	Name	Date	Approval
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI Standard 200-2: IT-Grundschutz Methodology - Document 0080: Basic Security Check - Document 0090: Risk Analysis

ewpage

Chapter 11

Implementation Control, Reporting and KPIs

Document ID: 0110
Document Type: Control Document
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

11.1 1. Control Model

11.1.1 1.1 Governance Structure

ISMS control operates on three levels:

Level	Committee	Frequency	Participants	Focus
Strategic	Management Review	Annually	Executive Management, ISB, IT Management	Strategic direction, resources
Tactical	ISMS Team Meeting	Monthly	ISB, IT Management, Information Domain Responsible	Measure planning, risks
Operational	Measure Status Update	Weekly	ISB, IT Management, Measure Owners	Implementation progress

11.1.2 1.2 Regular Meetings

Weekly - Measure Status Update: - **Schedule:** [TODO: e.g., Monday 10:00] - **Duration:** 30 minutes - **Participants:** ISB, IT Management, current measure owners - **Agenda:** Status of ongoing measures, blockers, escalations

Monthly - ISMS Team Meeting: - **Schedule:** [TODO: e.g., first Thursday of month, 14:00] - **Duration:** 2 hours - **Participants:** ISMS Team (see Document 0020) - **Agenda:** - KPI review - Measure progress - New risks and incidents - Compliance updates - Decisions and escalations

Quarterly - Management Review: - **Schedule:** [TODO: e.g., last Friday of quarter] - **Duration:** 1 hour - **Participants:** Executive Management, ISB, IT Management - **Agenda:** - ISMS performance (KPIs) - Measure implementation - Risk dashboard - Budget and resources - Strategic decisions

Annually - Management Review (comprehensive): - **Schedule:** [TODO: e.g., Q4] - **Duration:** Half day - **Participants:** Executive Management, ISB, IT Management, ISMS Team - **Agenda:** See Document 0140 (Management Review Template)

11.1.3 1.3 Reporting Channels

Report	Frequency	Creator	Recipient	Tool/Format
Measure Status	Weekly	ISB	IT Management	[TODO: Ticketing system]
ISMS Status Report	Monthly	ISB	Executive Management, ISMS Team	[TODO: Dashboard/PDF]
Security Incidents	Monthly	ISB	Executive Management	[TODO: Incident tool]
Risk Dashboard	Quarterly	ISB	Executive Management	[TODO: GRC tool]
Management Review	Annually	ISB	Executive Management	Presentation

11.2 2. Key Performance Indicators (KPIs)

11.2.1 2.1 Measure Implementation

KPI	Definition	Target	Source	Frequency	Owner
Action Plan Fulfillment	% completed measures vs. planned	100%	Action Plan (Document 0100)	Monthly	Thomas Weber
P1 Measure Fulfillment	% completed P1 measures	100% in [TODO] months	Action Plan	Weekly	Thomas Weber
Measure Delay	Average delay in days	< 14 days	Action Plan	Monthly	Thomas Weber

KPI	Definition	Target	Source	Frequency	Owner
Budget Compliance	% used budget vs. planned	100% ± 10%	Financial Controlling	Monthly	Max Mustermann

11.2.2 2.2 IT-Grundschutz Compliance

KPI	Definition	Target	Source	Frequency	Owner
IT-Grundschutz Fulfillment Rate	% fulfilled requirements	> 80%	Basic Security Check (Document 0080)	Quarterly	Thomas Weber
Critical Gaps	Number of unfulfilled P1 requirements	0	Basic Security Check	Monthly	Thomas Weber
Module Coverage	% modeled modules with target-actual comparison	100%	Modeling (Document 0070)	Quarterly	Thomas Weber

11.2.3 2.3 Risk Management

KPI	Definition	Target	Source	Frequency	Owner
Risk Exposure	Number of "Very High" risks	0	Risk Register (Document 0090)	Monthly	Thomas Weber
Risk Reduction	% reduced risks vs. identified	> 80%	Risk Register	Quarterly	Thomas Weber
Risk Acceptance Rate	% accepted risks (without measures)	< 10%	Risk Register	Quarterly	Thomas Weber

11.2.4 2.4 Patch and Vulnerability Management

KPI	Definition	Target	Source	Frequency	Owner
Patch Compliance	% systems with current patches	> 95%	Patch Management Tool	Monthly	Anna Schmidt
Critical Patches (SLA)	% critical patches within SLA (7 days)	100%	Patch Management Tool	Weekly	Anna Schmidt

KPI	Definition	Target	Source	Frequency	Owner
Vulnerability Remediation	Average time to remediation (days)	< 30 days (High), < 90 days (Medium)	Vulnerability Scanner	Monthly	Anna Schmidt
Open Vulnerabilities	Number of open vulnerabilities (Critical/High)	< 10	Vulnerability Scanner	Weekly	Anna Schmidt

11.2.5 2.5 Backup and Recovery

KPI	Definition	Target	Source	Frequency	Owner
Backup Success Rate	% successful backups	> 99%	Backup System	Daily	Anna Schmidt
Backup Test Rate	% successful restore tests	100%	Test Protocols	Quarterly	Anna Schmidt
Recovery Time Actual (RTA)	Actual recovery time	< RTO	Test Protocols	Quarterly	Anna Schmidt

11.2.6 2.6 Incident Management

KPI	Definition	Target	Source	Frequency	Owner
Security Incidents	Number of security incidents	Decreasing trend	Incident Management System	Monthly	Thomas Weber
Mean Time to Detect (MTTD)	Average detection time	< 24 hours	SIEM	Monthly	Anna Schmidt
Mean Time to Respond (MTTR)	Average response time	< 4 hours (Critical)	Incident Management System	Monthly	Thomas Weber
Incident Closure Rate	% closed incidents within SLA	> 95%	Incident Management System	Monthly	Thomas Weber

11.2.7 2.7 Awareness and Training

KPI	Definition	Target	Source	Frequency	Owner
Training Rate	% employees with awareness training	100%	HR System	Quarterly	Thomas Weber
Phishing Test Success Rate	% employees passing phishing test	> 90%	Phishing Simulation	Quarterly	Thomas Weber
Security Champion Rate	Number of security champions per department	Min. 1 per department	ISMS Team	Annually	Thomas Weber

11.2.8 2.8 Access Management

KPI	Definition	Target	Source	Frequency	Owner
Privileged Account Compliance	% privileged accounts with MFA	100%	IAM System	Monthly	Anna Schmidt
Access Review Compliance	% completed access recertifications	100%	IAM System	Quarterly	Anna Schmidt
Orphaned Accounts	Number of orphaned accounts	0	IAM System	Monthly	Anna Schmidt

11.3 3. KPI Dashboard

11.3.1 3.1 Traffic Light Status

KPI Category	Current Value	Target	Status	Trend
Measure Implementation	[TODO: %]	100%	/ /	/→/
IT-Grundschutz Compliance	[TODO: %]	> 80%	/ /	/→/
Risk Management	[TODO]	0 “Very High”	/ /	/→/
Patch Compliance	[TODO: %]	> 95%	/ /	/→/
Backup Success Rate	[TODO: %]	> 99%	/ /	/→/
Security Incidents	[TODO]	Trend	/ /	/→/
Awareness Training	[TODO: %]	100%	/ /	/→/

Traffic Light Logic: - **Green:** Target achieved or exceeded - **Yellow:** Target not achieved, but acceptable (< 10% deviation) - **Red:** Target significantly missed (> 10% deviation), escalation required

11.3.2 3.2 Trend Analysis

[TODO: Insert diagrams and trend visualizations]

11.4 4. Escalation Rules

11.4.1 4.1 Escalation Levels

Level	Trigger	Escalate to	Response Time	Actions
Level 1	KPI for 1 month	IT Management	1 week	Root cause analysis, corrective actions
Level 2	KPI or for 2 months	ISB	3 days	Escalation meeting, review resources
Level 3	KPI for 1 month	Executive Management	Immediate	Management decision, release resources

11.4.2 4.2 Escalation Process

1. **Identification:** KPI deviation detected
2. **Analysis:** Root cause analysis by owner
3. **Escalation:** Escalation according to level
4. **Actions:** Define and implement corrective actions
5. **Monitoring:** Close monitoring until target achievement
6. **Lessons Learned:** Documentation and process improvement

11.5 5. Reporting Templates

11.5.1 5.1 Monthly ISMS Status Report

Report Structure: 1. **Executive Summary:** Overall status (1 page) 2. **KPI Dashboard:** Traffic light status and trends 3. **Measure Progress:** Top 10 measures 4. **Security Incidents:** Summary 5. **Risks:** Top 5 risks 6. **Escalations:** Open escalations 7. **Next Steps:** Planned activities

11.5.2 5.2 Quarterly Risk Dashboard

Report Structure: 1. **Risk Heatmap:** Visualization of all risks 2. **Top 10 Risks:** Detailed description 3. **Risk Reduction:** Progress since last quarter 4. **New Risks:** Identified new risks 5. **Risk Acceptance:** Accepted risks with justification

11.5.3 5.3 Annual Management Review

Report Structure: See Document 0140 (Management Review Template)

11.6 6. Continuous Improvement

11.6.1 6.1 Improvement Process

PDCA Cycle: 1. **Plan:** Define objectives and KPIs 2. **Do:** Implement measures 3. **Check:** Measure and evaluate KPIs 4. **Act:** Derive improvement actions

11.6.2 6.2 Lessons Learned

After each major incident or project: 1. **Retrospective:** What went well? What didn't? 2. **Root Cause Analysis:** Identify causes 3. **Improvement Actions:** Define concrete actions 4. **Documentation:** Document lessons learned 5. **Communication:** Share insights

11.7 7. Tools and Systems

Tool/System	Purpose	Owner	Status
[TODO: GRC Tool]	Risk management, compliance	Thomas Weber	[TODO]
[TODO: Ticketing System]	Measure tracking	Anna Schmidt	[TODO]
[TODO: SIEM]	Security monitoring	Anna Schmidt	[TODO]
[TODO: Vulnerability Scanner]	Vulnerability management	Anna Schmidt	[TODO]
[TODO: Dashboard Tool]	KPI visualization	Thomas Weber	[TODO]

11.8 8. Approval

Role	Name	Date	Approval
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI Standard 200-1: Management Systems for Information Security (ISMS) - BSI Standard 200-2: IT-Grundschutz Methodology

ewpage

Chapter 12

Policy: Access Control and Permissions

Document ID: 0200
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

12.1 1. Purpose and Objectives

This policy defines the principles for access control and permissions at **AdminSend GmbH**.

Responsible: Thomas Weber (ISB)

[TODO: Add specific objectives]

12.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

12.3 3. Principles

[TODO: Define strategic principles for access control and permissions]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

12.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Policy compliance	All

12.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0210:** Guideline: IAM Joiner Mover Leaver and Recertification - [TODO: Additional guidelines and standards]

12.6 6. Evidence and Control

Evidence/Documentation: - [TODO: Define required evidence] - Examples: Configuration evidence, logs, audit reports

Review Interval: - This policy is reviewed annually or when significant changes occur - **Next Review:** {{ meta.document.next_review }}

12.7 7. Consequences of Violations

Violations of this policy may result in the following actions: - Warning - Disciplinary measures - Employment law consequences - Criminal prosecution (for serious violations)

12.8 8. Approval

Role	Name	Date	Approval
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - BSI Standards 200-1, 200-2, 200-3 - Document 0210: Guideline: IAM Joiner Mover Leaver and Recertification

ewpage

Chapter 13

Guideline: IAM Joiner Mover Leaver and Recertification

Document ID: 0210
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

13.1 1. Purpose and Reference

This guideline implements **Policy 0200: Policy: Access Control and Permissions** and defines specific requirements for IAM processes.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

13.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

13.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

13.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

13.5 5. Process and Implementation

13.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

13.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

13.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

13.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (ISB)

13.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

13.9 9. Review and Update

This guideline is reviewed regularly: - **Frequency:** Annually or when significant changes occur - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

13.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - Document 0200: Policy: Access Control and Permissions

ewpage

Chapter 14

Policy: Authentication and MFA

Document ID: 0220
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

14.1 1. Purpose and Objectives

This policy defines the principles for authentication and MFA at **AdminSend GmbH**.

Responsible: Thomas Weber (ISB)

[TODO: Add specific objectives]

14.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

14.3 3. Principles

[TODO: Define strategic principles for authentication and MFA]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

14.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Policy compliance	All

14.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0230:** Guideline: Password MFA and Session Rules - [TODO: Additional guidelines and standards]

14.6 6. Evidence and Control

Evidence/Documentation: - [TODO: Define required evidence] - Examples: Configuration evidence, logs, audit reports

Review Interval: - This policy is reviewed annually or when significant changes occur - **Next Review:** {{ meta.document.next_review }}

14.7 7. Consequences of Violations

Violations of this policy may result in the following actions: - Warning - Disciplinary measures - Employment law consequences - Criminal prosecution (for serious violations)

14.8 8. Approval

Role	Name	Date	Approval
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - BSI Standards 200-1, 200-2, 200-3 - Document 0230: Guideline: Password MFA and Session Rules

ewpage

Chapter 15

Guideline: Password MFA and Session Rules

Document ID: 0230
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

15.1 1. Purpose and Reference

This guideline implements **Policy 0220: Policy: Authentication and MFA** and defines specific requirements for password and MFA requirements.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

15.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

15.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

15.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

15.5 5. Process and Implementation

15.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

15.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

15.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

15.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (ISB)

15.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

15.9 9. Review and Update

This guideline is reviewed regularly: - **Frequency:** Annually or when significant changes occur - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

15.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - Document 0220: Policy: Authentication and MFA

ewpage

Chapter 16

Policy: Asset and Inventory Management

Document ID: 0240
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

16.1 1. Purpose and Objectives

This policy defines the principles for asset management at **AdminSend GmbH**.

Responsible: Thomas Weber (ISB)

[TODO: Add specific objectives]

16.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

16.3 3. Principles

[TODO: Define strategic principles for asset management]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

16.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Policy compliance	All

16.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0250:** Guideline: Asset Lifecycle Tagging and Disposal - [TODO: Additional guidelines and standards]

16.6 6. Evidence and Control

Evidence/Documentation: - [TODO: Define required evidence] - Examples: Configuration evidence, logs, audit reports

Review Interval: - This policy is reviewed annually or when significant changes occur - **Next Review:** {{ meta.document.next_review }}

16.7 7. Consequences of Violations

Violations of this policy may result in the following actions: - Warning - Disciplinary measures - Employment law consequences - Criminal prosecution (for serious violations)

16.8 8. Approval

Role	Name	Date	Approval
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - BSI Standards 200-1, 200-2, 200-3 - Document 0250: Guideline: Asset Lifecycle Tagging and Disposal

ewpage

Chapter 17

Guideline: Asset Lifecycle Tagging and Disposal

Document ID: 0250
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

17.1 1. Purpose and Reference

This guideline implements **Policy 0240: Policy: Asset and Inventory Management** and defines specific requirements for asset lifecycle.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

17.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

17.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

17.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

17.5 5. Process and Implementation

17.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

17.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

17.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

17.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (ISB)

17.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

17.9 9. Review and Update

This guideline is reviewed regularly: - **Frequency:** Annually or when significant changes occur - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

17.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - Document 0240: Policy: Asset and Inventory Management

ewpage

Chapter 18

Policy: Configuration and Hardening

Document ID: 0260
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

18.1 1. Purpose and Objectives

This policy defines the principles for system hardening at **AdminSend GmbH**.

Responsible: Thomas Weber (ISB)

[TODO: Add specific objectives]

18.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

18.3 3. Principles

[TODO: Define strategic principles for system hardening]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

18.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Policy compliance	All

18.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0270:** Guideline: Security Baselines and Deviation Management - [TODO: Additional guidelines and standards]

18.6 6. Evidence and Control

Evidence/Documentation: - [TODO: Define required evidence] - Examples: Configuration evidence, logs, audit reports

Review Interval: - This policy is reviewed annually or when significant changes occur - **Next Review:** {{ meta.document.next_review }}

18.7 7. Consequences of Violations

Violations of this policy may result in the following actions: - Warning - Disciplinary measures - Employment law consequences - Criminal prosecution (for serious violations)

18.8 8. Approval

Role	Name	Date	Approval
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - BSI Standards 200-1, 200-2, 200-3 - Document 0270: Guideline: Security Baselines and Deviation Management

ewpage

Chapter 19

Guideline: Security Baselines and Deviation Management

Document ID: 0270
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

19.1 1. Purpose and Reference

This guideline implements **Policy 0260: Policy: Configuration and Hardening** and defines specific requirements for security baselines.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

19.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

19.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

19.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

19.5 5. Process and Implementation

19.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

19.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

19.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

19.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (ISB)

19.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

19.9 9. Review and Update

This guideline is reviewed regularly: - **Frequency:** Annually or when significant changes occur - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

19.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - Document 0260: Policy: Configuration and Hardening

ewpage

Chapter 20

Policy: Patch and Vulnerability Management

Document ID: 0280
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

20.1 1. Purpose and Objectives

This policy defines the principles for patch management at **AdminSend GmbH**.

Responsible: Thomas Weber (ISB)

[TODO: Add specific objectives]

20.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

20.3 3. Principles

[TODO: Define strategic principles for patch management]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

20.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Policy compliance	All

20.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0290:** Guideline: Scans Patching and Exploitation Response - [TODO: Additional guidelines and standards]

20.6 6. Evidence and Control

Evidence/Documentation: - [TODO: Define required evidence] - Examples: Configuration evidence, logs, audit reports

Review Interval: - This policy is reviewed annually or when significant changes occur - **Next Review:** {{ meta.document.next_review }}

20.7 7. Consequences of Violations

Violations of this policy may result in the following actions: - Warning - Disciplinary measures - Employment law consequences - Criminal prosecution (for serious violations)

20.8 8. Approval

Role	Name	Date	Approval
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - BSI Standards 200-1, 200-2, 200-3 - Document 0290: Guideline: Scans Patching and Exploitation Response

ewpage

Chapter 21

Guideline: Scans Patching and Exploitation Response

Document ID: 0290
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

21.1 1. Purpose and Reference

This guideline implements **Policy 0280: Policy: Patch and Vulnerability Management** and defines specific requirements for vulnerability management.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

21.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

21.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

21.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

21.5 5. Process and Implementation

21.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

21.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

21.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

21.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (ISB)

21.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

21.9 9. Review and Update

This guideline is reviewed regularly: - **Frequency:** Annually or when significant changes occur - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

21.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - Document 0280: Policy: Patch and Vulnerability Management

ewpage

Chapter 22

Policy: Logging Monitoring and Detection

Document ID: 0300
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

22.1 1. Purpose and Objectives

This policy defines the principles for logging and monitoring at **AdminSend GmbH**.

Responsible: Thomas Weber (ISB)

[TODO: Add specific objectives]

22.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

22.3 3. Principles

[TODO: Define strategic principles for logging and monitoring]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

22.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Policy compliance	All

22.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0310:** Guideline: Log Standards SIEM UseCases and Retention - [TODO: Additional guidelines and standards]

22.6 6. Evidence and Control

Evidence/Documentation: - [TODO: Define required evidence] - Examples: Configuration evidence, logs, audit reports

Review Interval: - This policy is reviewed annually or when significant changes occur - **Next Review:** {{ meta.document.next_review }}

22.7 7. Consequences of Violations

Violations of this policy may result in the following actions: - Warning - Disciplinary measures - Employment law consequences - Criminal prosecution (for serious violations)

22.8 8. Approval

Role	Name	Date	Approval
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - BSI Standards 200-1, 200-2, 200-3 - Document 0310: Guideline: Log Standards SIEM UseCases and Retention

ewpage

Chapter 23

Guideline: Log Standards SIEM UseCases and Retention

Document ID: 0310
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

23.1 1. Purpose and Reference

This guideline implements **Policy 0300: Policy: Logging Monitoring and Detection** and defines specific requirements for SIEM and log management.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

23.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

23.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

23.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

23.5 5. Process and Implementation

23.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

23.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

23.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

23.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (ISB)

23.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

23.9 9. Review and Update

This guideline is reviewed regularly: - **Frequency:** Annually or when significant changes occur - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

23.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - Document 0300: Policy: Logging Monitoring and Detection

ewpage

Chapter 24

Policy: Incident Management

Document ID: 0320
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

24.1 1. Purpose and Objectives

This policy defines the principles for incident management at **AdminSend GmbH**.

Responsible: Thomas Weber (ISB)

[TODO: Add specific objectives]

24.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

24.3 3. Principles

[TODO: Define strategic principles for incident management]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

24.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Policy compliance	All

24.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0330:** Guideline: Incident Response Escalation and Forensics - [TODO: Additional guidelines and standards]

24.6 6. Evidence and Control

Evidence/Documentation: - [TODO: Define required evidence] - Examples: Configuration evidence, logs, audit reports

Review Interval: - This policy is reviewed annually or when significant changes occur - **Next Review:** {{ meta.document.next_review }}

24.7 7. Consequences of Violations

Violations of this policy may result in the following actions: - Warning - Disciplinary measures - Employment law consequences - Criminal prosecution (for serious violations)

24.8 8. Approval

Role	Name	Date	Approval
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - BSI Standards 200-1, 200-2, 200-3 - Document 0330: Guideline: Incident Response Escalation and Forensics

ewpage

Chapter 25

Guideline: Incident Response Escalation and Forensics

Document ID: 0330
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

25.1 1. Purpose and Reference

This guideline implements **Policy 0320: Policy: Incident Management** and defines specific requirements for incident response process.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

25.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

25.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

25.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

25.5 5. Process and Implementation

25.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

25.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

25.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

25.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (ISB)

25.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

25.9 9. Review and Update

This guideline is reviewed regularly: - **Frequency:** Annually or when significant changes occur - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

25.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - Document 0320: Policy: Incident Management

ewpage

Chapter 26

Policy: Cryptography and Key Management

Document ID: 0340
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

26.1 1. Purpose and Objectives

This policy defines the principles for cryptography at **AdminSend GmbH**.

Responsible: Thomas Weber (ISB)

[TODO: Add specific objectives]

26.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

26.3 3. Principles

[TODO: Define strategic principles for cryptography]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

26.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Policy compliance	All

26.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0350:** Guideline: Encryption Key Rotation and Certificates - [TODO: Additional guidelines and standards]

26.6 6. Evidence and Control

Evidence/Documentation: - [TODO: Define required evidence] - Examples: Configuration evidence, logs, audit reports

Review Interval: - This policy is reviewed annually or when significant changes occur - **Next Review:** {{ meta.document.next_review }}

26.7 7. Consequences of Violations

Violations of this policy may result in the following actions: - Warning - Disciplinary measures - Employment law consequences - Criminal prosecution (for serious violations)

26.8 8. Approval

Role	Name	Date	Approval
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - BSI Standards 200-1, 200-2, 200-3 - Document 0350: Guideline: Encryption Key Rotation and Certificates

ewpage

Chapter 27

Guideline: Encryption Key Rotation and Certificates

Document ID: 0350
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

27.1 1. Purpose and Reference

This guideline implements **Policy 0340: Policy: Cryptography and Key Management** and defines specific requirements for encryption and key management.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

27.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

27.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

27.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

27.5 5. Process and Implementation

27.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

27.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

27.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

27.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (ISB)

27.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

27.9 9. Review and Update

This guideline is reviewed regularly: - **Frequency:** Annually or when significant changes occur - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

27.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - Document 0340: Policy: Cryptography and Key Management

ewpage

Chapter 28

Policy: Secure Software Development

Document ID: 0360
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

28.1 1. Purpose and Objectives

This policy defines the principles for secure software development at **AdminSend GmbH**.

Responsible: Thomas Weber (ISB)

[TODO: Add specific objectives]

28.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

28.3 3. Principles

[TODO: Define strategic principles for secure software development]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

28.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Policy compliance	All

28.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0370:** Guideline: Secure SDLC Code Reviews SAST DAST Secrets - [TODO: Additional guidelines and standards]

28.6 6. Evidence and Control

Evidence/Documentation: - [TODO: Define required evidence] - Examples: Configuration evidence, logs, audit reports

Review Interval: - This policy is reviewed annually or when significant changes occur - **Next Review:** {{ meta.document.next_review }}

28.7 7. Consequences of Violations

Violations of this policy may result in the following actions: - Warning - Disciplinary measures - Employment law consequences - Criminal prosecution (for serious violations)

28.8 8. Approval

Role	Name	Date	Approval
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - BSI Standards 200-1, 200-2, 200-3 - Document 0370: Guideline: Secure SDLC Code Reviews SAST DAST Secrets

ewpage

Chapter 29

Guideline: Secure SDLC Code Reviews SAST DAST Secrets

Document ID: 0370
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

29.1 1. Purpose and Reference

This guideline implements **Policy 0360: Policy: Secure Software Development** and defines specific requirements for Secure SDLC.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

29.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

29.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

29.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

29.5 5. Process and Implementation

29.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

29.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

29.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

29.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (ISB)

29.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

29.9 9. Review and Update

This guideline is reviewed regularly: - **Frequency:** Annually or when significant changes occur - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

29.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz Compendium - Document 0360: Policy: Secure Software Development

ewpage

Chapter 30

Policy: Change and Release Management

Document ID: 0380
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

30.1 1. Purpose and Objectives

This policy defines the principles for Change Management at **AdminSend GmbH**.

Responsible: Thomas Weber (CISO)

[TODO: Add specific objectives]

30.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

30.3 3. Principles

[TODO: Define the strategic principles for Change Management]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

30.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Compliance with policy	All

30.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0390:** Guideline: Change Approvals and Security Checks - [TODO: Additional guidelines and standards]

30.6 6. Evidence and Control

Evidence/Records: - [TODO: Define required evidence] - Examples: Configuration records, logs, audit reports

Review Interval: - This policy is reviewed annually or upon significant changes - **Next Review:** {{ meta.document.next_review }}

30.7 7. Consequences of Violations

Violations of this policy may result in the following measures: - Warning - Disciplinary action - Employment law consequences - Criminal prosecution (for serious violations)

30.8 8. Approval

Role	Name	Date	Approval
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Document 0390: Guideline: Change Approvals and Security Checks

ewpage

Chapter 31

Guideline: Change Approvals and Security Checks

Document ID: 0390
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

31.1 1. Purpose and Reference

This guideline implements **Policy 0380: Policy: Change and Release Management** and defines specific requirements for the Change Process.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

31.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

31.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

31.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

31.5 5. Process and Implementation

31.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

31.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

31.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

31.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (CISO)

31.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

31.9 9. Review and Updates

This guideline is reviewed regularly: - **Frequency:** Annually or upon significant changes - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

31.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - Document 0380: Policy: Change and Release Management

ewpage

Chapter 32

Policy: Supplier and Outsourcing Management

Document ID: 0400
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

32.1 1. Purpose and Objectives

This policy defines the principles for Supplier Management at **AdminSend GmbH**.

Responsible: Thomas Weber (CISO)

[TODO: Add specific objectives]

32.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

32.3 3. Principles

[TODO: Define the strategic principles for Supplier Management]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

32.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Compliance with policy	All

32.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0410:** Guideline: Third Party Risk Assessment and Contract Clauses - [TODO: Additional guidelines and standards]

32.6 6. Evidence and Control

Evidence/Records: - [TODO: Define required evidence] - Examples: Configuration records, logs, audit reports

Review Interval: - This policy is reviewed annually or upon significant changes - **Next Review:** {{ meta.document.next_review }}

32.7 7. Consequences of Violations

Violations of this policy may result in the following measures: - Warning - Disciplinary action - Employment law consequences - Criminal prosecution (for serious violations)

32.8 8. Approval

Role	Name	Date	Approval
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Document 0410: Guideline: Third Party Risk Assessment and Contract Clauses

ewpage

Chapter 33

Guideline: Third Party Risk Assessment and Contract Clauses

Document ID: 0410
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

33.1 1. Purpose and Reference

This guideline implements **Policy 0400: Policy: Supplier and Outsourcing Management** and defines specific requirements for Third-Party Risk Management.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

33.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

33.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

33.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

33.5 5. Process and Implementation

33.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

33.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

33.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

33.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (CISO)

33.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

33.9 9. Review and Updates

This guideline is reviewed regularly: - **Frequency:** Annually or upon significant changes - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

33.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - Document 0400: Policy: Supplier and Outsourcing Management

ewpage

Chapter 34

Policy: Data Protection and Data Handling

Document ID: 0420
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

34.1 1. Purpose and Objectives

This policy defines the principles for Data Protection at **AdminSend GmbH**.

Responsible: Thomas Weber (CISO)

[TODO: Add specific objectives]

34.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

34.3 3. Principles

[TODO: Define the strategic principles for Data Protection]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

34.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Compliance with policy	All

34.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0430:** Guideline: Data Classification Labeling and Disclosure - [TODO: Additional guidelines and standards]

34.6 6. Evidence and Control

Evidence/Records: - [TODO: Define required evidence] - Examples: Configuration records, logs, audit reports

Review Interval: - This policy is reviewed annually or upon significant changes - **Next Review:** {{ meta.document.next_review }}

34.7 7. Consequences of Violations

Violations of this policy may result in the following measures: - Warning - Disciplinary action - Employment law consequences - Criminal prosecution (for serious violations)

34.8 8. Approval

Role	Name	Date	Approval
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Document 0430: Guideline: Data Classification Labeling and Disclosure

ewpage

Chapter 35

Guideline: Data Classification Labeling and Disclosure

Document ID: 0430
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

35.1 1. Purpose and Reference

This guideline implements **Policy 0420: Policy: Data Protection and Data Handling** and defines specific requirements for Data Classification.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

35.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

35.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

35.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

35.5 5. Process and Implementation

35.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

35.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

35.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

35.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (CISO)

35.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

35.9 9. Review and Updates

This guideline is reviewed regularly: - **Frequency:** Annually or upon significant changes - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

35.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - Document 0420: Policy: Data Protection and Data Handling

ewpage

Chapter 36

Policy: Backup and Recovery

Document ID: 0440
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

36.1 1. Purpose and Objectives

This policy defines the principles for Backup and Recovery at **AdminSend GmbH**.

Responsible: Thomas Weber (CISO)

[TODO: Add specific objectives]

36.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

36.3 3. Principles

[TODO: Define the strategic principles for Backup and Recovery]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

36.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Compliance with policy	All

36.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0450:** Guideline: Backup Restore and Regular Tests - [TODO: Additional guidelines and standards]

36.6 6. Evidence and Control

Evidence/Records: - [TODO: Define required evidence] - Examples: Configuration records, logs, audit reports

Review Interval: - This policy is reviewed annually or upon significant changes - **Next Review:** {{ meta.document.next_review }}

36.7 7. Consequences of Violations

Violations of this policy may result in the following measures: - Warning - Disciplinary action - Employment law consequences - Criminal prosecution (for serious violations)

36.8 8. Approval

Role	Name	Date	Approval
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Document 0450: Guideline: Backup Restore and Regular Tests

ewpage

Chapter 37

Guideline: Backup Restore and Regular Tests

Document ID: 0450
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

37.1 1. Purpose and Reference

This guideline implements **Policy 0440: Policy: Backup and Recovery** and defines specific requirements for the Backup Process.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

37.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

37.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

37.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

37.5 5. Process and Implementation

37.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

37.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

37.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

37.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (CISO)

37.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

37.9 9. Review and Updates

This guideline is reviewed regularly: - **Frequency:** Annually or upon significant changes - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

37.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - Document 0440: Policy: Backup and Recovery

ewpage

Chapter 38

Policy: Network and Communication Security

Document ID: 0460
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

38.1 1. Purpose and Objectives

This policy defines the principles for Network Security at **AdminSend GmbH**.

Responsible: Thomas Weber (CISO)

[TODO: Add specific objectives]

38.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

38.3 3. Principles

[TODO: Define the strategic principles for Network Security]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

38.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Compliance with policy	All

38.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0470:** Guideline: Segmentation Firewalling VPN and Admin Access - [TODO: Additional guidelines and standards]

38.6 6. Evidence and Control

Evidence/Records: - [TODO: Define required evidence] - Examples: Configuration records, logs, audit reports

Review Interval: - This policy is reviewed annually or upon significant changes - **Next Review:** {{ meta.document.next_review }}

38.7 7. Consequences of Violations

Violations of this policy may result in the following measures: - Warning - Disciplinary action - Employment law consequences - Criminal prosecution (for serious violations)

38.8 8. Approval

Role	Name	Date	Approval
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Document 0470: Guideline: Segmentation Firewalling VPN and Admin Access

ewpage

Chapter 39

Guideline: Segmentation Firewalling VPN and Admin Access

Document ID: 0470
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

39.1 1. Purpose and Reference

This guideline implements **Policy 0460: Policy: Network and Communication Security** and defines specific requirements for Network Segmentation.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

39.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

39.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

39.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

39.5 5. Process and Implementation

39.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

39.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

39.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

39.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (CISO)

39.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

39.9 9. Review and Updates

This guideline is reviewed regularly: - **Frequency:** Annually or upon significant changes - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

39.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - Document 0460: Policy: Network and Communication Security

ewpage

Chapter 40

Policy: Endpoint and Mobile Security

Document ID: 0480
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

40.1 1. Purpose and Objectives

This policy defines the principles for Endpoint Security at **AdminSend GmbH**.

Responsible: Thomas Weber (CISO)

[TODO: Add specific objectives]

40.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

40.3 3. Principles

[TODO: Define the strategic principles for Endpoint Security]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

40.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Compliance with policy	All

40.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0490:** Guideline: MDM EDR Device Compliance and Remote Work - [TODO: Additional guidelines and standards]

40.6 6. Evidence and Control

Evidence/Records: - [TODO: Define required evidence] - Examples: Configuration records, logs, audit reports

Review Interval: - This policy is reviewed annually or upon significant changes - **Next Review:** {{ meta.document.next_review }}

40.7 7. Consequences of Violations

Violations of this policy may result in the following measures: - Warning - Disciplinary action - Employment law consequences - Criminal prosecution (for serious violations)

40.8 8. Approval

Role	Name	Date	Approval
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Document 0490: Guideline: MDM EDR Device Compliance and Remote Work

ewpage

Chapter 41

Guideline: MDM EDR Device Compliance and Remote Work

Document ID: 0490
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

41.1 1. Purpose and Reference

This guideline implements **Policy 0480: Policy: Endpoint and Mobile Security** and defines specific requirements for Mobile Device Management.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

41.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

41.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

41.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

41.5 5. Process and Implementation

41.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

41.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

41.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

41.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (CISO)

41.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

41.9 9. Review and Updates

This guideline is reviewed regularly: - **Frequency:** Annually or upon significant changes - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

41.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - Document 0480: Policy: Endpoint and Mobile Security

ewpage

Chapter 42

Policy: Physical Security

Document ID: 0500
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

42.1 1. Purpose and Objectives

This policy defines the principles for Physical Security at **AdminSend GmbH**.

Responsible: Thomas Weber (CISO)

[TODO: Add specific objectives]

42.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

42.3 3. Principles

[TODO: Define the strategic principles for Physical Security]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

42.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Compliance with policy	All

42.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0510:** Guideline: Access Visitors and Equipment Protection - [TODO: Additional guidelines and standards]

42.6 6. Evidence and Control

Evidence/Records: - [TODO: Define required evidence] - Examples: Configuration records, logs, audit reports

Review Interval: - This policy is reviewed annually or upon significant changes - **Next Review:** {{ meta.document.next_review }}

42.7 7. Consequences of Violations

Violations of this policy may result in the following measures: - Warning - Disciplinary action - Employment law consequences - Criminal prosecution (for serious violations)

42.8 8. Approval

Role	Name	Date	Approval
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Document 0510: Guideline: Access Visitors and Equipment Protection

ewpage

Chapter 43

Guideline: Access Visitors and Equipment Protection

Document ID: 0510
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

43.1 1. Purpose and Reference

This guideline implements **Policy 0500: Policy: Physical Security** and defines specific requirements for Access Controls.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

43.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

43.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

43.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

43.5 5. Process and Implementation

43.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

43.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

43.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

43.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (CISO)

43.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

43.9 9. Review and Updates

This guideline is reviewed regularly: - **Frequency:** Annually or upon significant changes - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

43.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - Document 0500: Policy: Physical Security

ewpage

Chapter 44

Policy: Exception Process and Risk Acceptance

Document ID: 0520
Document Type: Policy (abstract)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

44.1 1. Purpose and Objectives

This policy defines the principles for Exception Process at **AdminSend GmbH**.

Responsible: Thomas Weber (CISO)

[TODO: Add specific objectives]

44.2 2. Scope

This policy applies to: - All employees of AdminSend GmbH - All IT systems and applications - All locations: {{ meta.organization.locations }} - External service providers with system access

Exceptions: - Exceptions are only possible through the exception process (Document 0520) - [TODO: Document specific exceptions]

44.3 3. Principles

[TODO: Define the strategic principles for Exception Process]

Example Principles: 1. **Principle 1:** [TODO] 2. **Principle 2:** [TODO] 3. **Principle 3:** [TODO]

44.4 4. Responsibilities

Role	Responsibility	Name
Policy Owner	Overall responsibility for policy	Thomas Weber
Implementation Responsible	Technical implementation	Anna Schmidt
Control/Audit	Monitoring compliance	[TODO: Internal Audit]
All Employees	Compliance with policy	All

44.5 5. Derived Guidelines and Standards

This policy is implemented through: - **Guideline 0530:** Guideline: Exceptions Risk Waiver and Review - [TODO: Additional guidelines and standards]

44.6 6. Evidence and Control

Evidence/Records: - [TODO: Define required evidence] - Examples: Configuration records, logs, audit reports

Review Interval: - This policy is reviewed annually or upon significant changes - **Next Review:** {{ meta.document.next_review }}

44.7 7. Consequences of Violations

Violations of this policy may result in the following measures: - Warning - Disciplinary action - Employment law consequences - Criminal prosecution (for serious violations)

44.8 8. Approval

Role	Name	Date	Approval
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Executive Management	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Document 0530: Guideline: Exceptions Risk Waiver and Review

ewpage

Chapter 45

Guideline: Exceptions Risk Waiver and Review

Document ID: 0530
Document Type: Guideline/Standard (concrete)
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

45.1 1. Purpose and Reference

This guideline implements **Policy 0520: Policy: Exception Process and Risk Acceptance** and defines specific requirements for Exception Management.

Responsible: Anna Schmidt (IT Management)

[TODO: Add specific objectives]

45.2 2. Scope

Systems/Platforms: - [TODO: Define affected systems] - Examples: Active Directory, cloud platforms, applications

Target Groups: - IT administrators - System owners - [TODO: Additional target groups]

45.3 3. Mandatory Requirements (MUST)

[TODO: Define mandatory requirements]

Example MUST Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO] 3. **Requirement 3:** [TODO]

45.4 4. Recommended Requirements (SHOULD)

[TODO: Define recommended requirements]

Example SHOULD Requirements: 1. **Requirement 1:** [TODO] 2. **Requirement 2:** [TODO]

45.5 5. Process and Implementation

45.5.1 5.1 Process Steps

[TODO: Define the process]

Example Process: 1. **Request:** [TODO] 2. **Approval:** [TODO] 3. **Implementation:** [TODO] 4. **Review:** [TODO]

45.5.2 5.2 Tooling and Systems

Tools Used: - [TODO: Tool 1] - [TODO: Tool 2]

Responsible: Anna Schmidt

45.6 6. Evidence

Required Evidence: - [TODO: Evidence 1] - [TODO: Evidence 2]

Retention Period: [TODO: e.g., 3 years]

45.7 7. Exceptions

Exceptions to this guideline are only possible through the **Exception Process (Document 0520)**.

Exception Request to: Thomas Weber (CISO)

45.8 8. Training and Awareness

[TODO: Define training requirements]

Target Group: [TODO]
Frequency: [TODO]
Responsible: Thomas Weber

45.9 9. Review and Updates

This guideline is reviewed regularly: - **Frequency:** Annually or upon significant changes - **Responsible:** Anna Schmidt - **Next Review:** {{ meta.document.next_review }}

45.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium - Document 0520: Policy: Exception Process and Risk Acceptance

ewpage

Chapter 46

Training and Awareness – Program

Document ID: 0600
Document Type: Program
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

46.1 1. Purpose and Objectives

The training and awareness program of **AdminSend GmbH** ensures that all employees have the required security knowledge.

Responsible: Thomas Weber (CISO)

46.2 2. Target Groups

Target Group	Number	Specific Requirements
All Employees	[TODO]	Basic Awareness
IT Administrators	[TODO]	Technical Security, Privileged Access
Developers	[TODO]	Secure Coding, SDLC
Management	[TODO]	Security Strategy, Risk Management
External Service Providers	[TODO]	Relevant Security Requirements

46.3 3. Training Catalog

Training	Target Group	Frequency	Duration	Content	Evidence	Owner
Information Security Fundamentals	All	Annually	1h	Policies, Phishing, Passwords, Incident Reporting	LMS Certificate	Thomas Weber
Onboarding Security	New Employees	Upon Entry	30min	Fundamentals, Policies	Attendance List	HR
Phishing Simulation	All	Quarterly	10min	Phishing Recognition	Click Rate	Thomas Weber
Admin Training	IT Admins	Annually	4h	Privileged Access, Hardening, Logging	Attendance List	Anna Schmidt
Secure Coding	Developers	Annually	8h	OWASP Top 10, SAST/DAST	Attendance List	Anna Schmidt
[TODO: Additional Training]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

46.4 4. Effectiveness Measurement

46.4.1 4.1 Metrics (KPIs)

KPI	Target	Measurement	Frequency
Training Rate	100%	% Employees with Current Training	Quarterly
Phishing Test Success Rate	> 90%	% Employees Recognizing Phishing	Quarterly
Quiz Success Rate	> 80%	% Passed Final Tests	After Training

46.4.2 4.2 Feedback and Improvement

- **Feedback Surveys:** After each training
- **Lessons Learned:** From security incidents
- **Continuous Improvement:** Annual program review

46.5 5. Training Materials

Available Materials: - E-Learning Modules (LMS) - Presentations - Checklists and Quick Reference Guides - Posters and Infographics - Newsletters and Intranet Articles

Storage Location: [TODO: e.g., Intranet/Training Portal]

46.6 6. Communication and Awareness Campaigns

Regular Activities: - Monthly Security Newsletter - Quarterly Awareness Campaigns (Topics: Phishing, Passwords, etc.) - Security Champions Program - Annual Security Awareness Month

46.7 7. Approval

Role	Name	Date	Approval
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
HR	[TODO]	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI Standard 200-1: ISMS - BSI IT-Grundschutz-Kompendium: ORP.3 Awareness and Training

ewpage

Chapter 47

Internal Audit Program (Template)

Document ID: 0610
Document Type: Program/Template
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

47.1 1. Purpose and Objectives

The internal audit program of **AdminSend GmbH** ensures the effectiveness of the ISMS.

Responsible: [TODO: Internal Audit]

47.2 2. Audit Approach

Principles: - **Risk-based:** Focus on critical areas - **Independent:** Auditors are independent from audited area - **Scope-related:** Audits cover the entire ISMS scope - **Systematic:** Structured audit process

47.3 3. Audit Plan

Period	Audit Topic	Criteria	Auditor	Auditee	Status	Result	Actions
Q1 {{ meta.document.year }}	Basic Security Check Sample	Policies, Guidelines, Evidence	[TODO]	Anna Schmidt	Planned	-	-

Period	Audit Topic	Criteria	Auditor	Auditee	Status	Result	Actions
Q2 {{ meta.document.year }}	Risk Management Process	Document 0090, Risk Register	[TODO]	Thomas Weber	Planned	-	-
Q3 {{ meta.document.year }}	Incident Management	Document 0320/0330, Incident Logs	[TODO]	Anna Schmidt	Planned	-	-
Q4 {{ meta.document.year }}	Document Control	Document 0030, Document Register	[TODO]	Thomas Weber	Planned	-	-

47.4 4. Audit Checkpoints

Standard Checks: - Are documents current and approved? - Is evidence available and traceable? - Is the action status plausible? - Are deviations documented and addressed? - Are processes lived (not just documented)?

47.5 5. Audit Process

1. **Planning:** Audit scope, criteria, schedule
2. **Preparation:** Document review, checklists
3. **Execution:** Interviews, sampling, inspections
4. **Reporting:** Audit report with findings
5. **Follow-up:** Tracking of corrective actions

47.6 6. Audit Report Template

Structure: 1. Executive Summary 2. Audit Scope and Criteria 3. Audit Methodology 4. Findings (Categorized: Critical/High/Medium/Low) 5. Positive Observations 6. Recommendations 7. Action Plan

47.7 7. Findings Categorization

Category	Description	Response Time
Critical	Severe deviation, high risk	Immediately
High	Significant deviation	30 days
Medium	Improvement potential	90 days
Low	Minor deviation	180 days

47.8 8. Approval

Role	Name	Date	Approval
Internal Audit	[TODO]	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI Standard 200-1: ISMS - BSI IT-Grundschutz-Kompendium: DER.3.1 Audits and Reviews

ewpage

Chapter 48

Management Review – Template

Document ID: 0620
Document Type: Evidence/Template
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

48.1 1. Participants, Period, Scope

Date: [TODO]
Location: [TODO]
Duration: [TODO]

Participants: - Executive Management: Max Mustermann - CISO: Thomas Weber - IT Management: Anna Schmidt - [TODO: Additional participants]

Information Domain(s): [TODO: See Document 0040]

48.2 2. Inputs for Management Review

48.2.1 2.1 Action Plan Status

Action Implementation: [TODO: % completed]
Critical Actions: [TODO: Status]
Delays: [TODO: Description and reasons]

Reference: Document 0100 (Action Plan)

48.2.2 2.2 Audit and Check Results

Internal Audits: [TODO: Summary]
Basic Security Check: [TODO: Compliance level]
External Audits: [TODO: if conducted]

Reference: Document 0610 (Audit Program), Document 0080 (Basic Check)

48.2.3 2.3 Security Incidents and Lessons Learned

Number of Incidents: [TODO]
Critical Incidents: [TODO: Description]
Lessons Learned: [TODO: Insights]
Preventive Measures: [TODO]

Reference: Document 0320/0330 (Incident Management)

48.2.4 2.4 Context Changes

Technology: - [TODO: New systems, cloud migration, etc.]

Organization: - [TODO: Restructuring, new locations, etc.]

Suppliers: - [TODO: New service providers, contract changes]

Legal Requirements: - [TODO: New laws, regulations]

48.2.5 2.5 Risk Situation and Top Risks

Risk Exposure: [TODO: Number of "Very High"/"High" risks]
Top 5 Risks: [TODO: See Document 0090]
New Threats: [TODO]

Reference: Document 0090 (Risk Analysis)

48.2.6 2.6 KPI Performance

IT-Grundschutz Compliance Level: [TODO: %]
Patch Compliance: [TODO: %]
Training Rate: [TODO: %]
Additional KPIs: [TODO]

Reference: Document 0110 (KPIs)

48.3 3. Outputs and Decisions

48.3.1 3.1 Policy and Objectives Adjustment

Decision: [TODO: Adjust policy? Yes/No]
Justification: [TODO]
New Security Objectives: [TODO]

Responsible: Max Mustermann

48.3.2 3.2 Resources and Investments

Budget Adjustment: [TODO: Increase/Decrease]
Personnel Resources: [TODO: Additional positions?]
External Support: [TODO]

Responsible: Max Mustermann

48.3.3 3.3 Risk Acceptances

Accepted Risks: [TODO: Risk IDs]
Justification: [TODO]
Validity Period: [TODO]

Responsible: Max Mustermann

48.3.4 3.4 Improvement Actions

Action	Description	Owner	Target Date	Priority
[TODO]	[TODO]	[TODO]	[TODO]	High/Medium/Low

48.3.5 3.5 Scope Changes

Scope Extension: [TODO: New systems/locations]
Scope Reduction: [TODO: if applicable]

Reference: Document 0040 (Scope)

48.4 4. Summary and Conclusion

Overall ISMS Assessment: [TODO: Effective/Needs Improvement]
Key Findings: [TODO]
Next Steps: [TODO]

48.5 5. Approval

Role	Name	Date	Signature
Executive Management	Max Mustermann	[TODO]	[TODO]
CISO	Thomas Weber	[TODO]	[TODO]

References: - BSI Standard 200-1: ISMS (Management Review) - All ISMS Documents (0010-0630)

ewpage

Chapter 49

Non-Conformities and Corrective Actions

Document ID: 0630
Document Type: Process/Template
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

49.1 1. Purpose and Objectives

This process ensures that deviations from ISMS requirements are systematically captured, addressed, and their effectiveness verified.

Responsible: Thomas Weber (CISO)

49.2 2. Sources for Non-Conformities

Non-conformities can be identified through: - Internal Audits (Document 0610) - Basic Security Check (Document 0080) - Security Incidents (Document 0320/0330) - Penetration Tests and Vulnerability Scans - Policy Violations - Management Review (Document 0620) - External Audits

49.3 3. Process

49.3.1 3.1 Capture

Step 1: Identification and Documentation - Non-conformity is identified - Finding is recorded in the Findings Register (see Section 4) - Categorization: Critical/High/Medium/Low

Responsible: Identifying person (Auditor, CISO, etc.)

49.3.2 3.2 Root Cause Analysis

Step 2: Root Cause Analysis - Why did the non-conformity occur? - Which processes/controls failed? - Is this an isolated case or systemic problem?

Methods: - 5-Why Analysis - Fishbone Diagram - Process Analysis

Responsible: CISO, affected area manager

49.3.3 3.3 Define Action

Step 3: Define Corrective Action - Immediate action (fix symptom) - Corrective action (fix cause) - Preventive action (prevent recurrence)

Responsible: CISO, Action Owner

49.3.4 3.4 Implementation

Step 4: Implement Action - Action is implemented - Progress is tracked - Implementation documentation

Responsible: Action Owner

49.3.5 3.5 Effectiveness Check

Step 5: Effectiveness Check - Was the non-conformity resolved? - Is the cause eliminated? - Have no new problems emerged?

Methods: - Follow-up Audit - Sampling - KPI Monitoring

Responsible: CISO, Internal Audit

49.3.6 3.6 Closure

Step 6: Closure - Effectiveness confirmed - Finding closed - Lessons Learned documented

Responsible: CISO

49.4 4. Findings Register

Finding ID	Source	Date	Description	Category	Root Cause	Action	Owner	Due	Status	Effectiveness Verified On
F-001	Audit Q1	[TODO]	[TODO]	High	[TODO]	[TODO]	[TODO]	[TODO]	Open	-
F-002	Basic Check	[TODO]	[TODO]	Medium	[TODO]	[TODO]	[TODO]	[TODO]	In Progress	-
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Status Values: - **Open:** Newly identified - **In Analysis:** Root cause analysis ongoing - **In Progress:** Action being implemented - **Effectiveness Check:** Action implemented, verification pending - **Closed:** Effectiveness confirmed

49.5 5. Categorization and Response Times

Category	Description	Response Time	Escalation
Critical	Severe deviation, high risk	Immediately	Executive Management
High	Significant deviation	7 days	CISO
Medium	Improvement potential	30 days	Area Manager
Low	Minor deviation	90 days	Area Manager

49.6 6. Reporting

Monthly: - Number of open findings (by category) - Overdue findings - Closed findings

Quarterly: - Trend analysis - Top finding categories - Effectiveness of corrective actions

Responsible: Thomas Weber
Recipients: Executive Management, ISMS Team

49.7 7. Lessons Learned

After closing critical or recurring findings: 1. **Retrospective:** What went well? What didn't? 2. **Process Improvement:** Adjustment of processes/controls 3. **Documentation:** Document lessons learned 4. **Communication:** Share insights (Awareness)

49.8 8. Approval

Role	Name	Date	Approval
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI Standard 200-1: ISMS (Non-conformities and Corrective Actions) - Document 0610: Internal Audit Program

ewpage

Chapter 50

Appendix: Evidence Register

Document ID: 0700
Document Type: Appendix/Template
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

50.1 1. Purpose and Objectives

The evidence register of **AdminSend GmbH** provides a central overview of all evidence documenting the implementation of security measures, policies, and guidelines.

Responsible: Thomas Weber (CISO)

50.2 2. Evidence Register

Evidence ID	Topic/Measure	Description	Document Type	Location/Link	Owner	Retention Period	Last Review	Next Review	Status
E-001	Patch Compliance	Monthly Patch Status Report	Report	[TODO: SharePoint/CMDB]	Anna Schmidt	3 years	[TODO]	[TODO]	Current
E-002	Backup Tests	Quarterly Restore Tests	Test Protocol	[TODO]	Anna Schmidt	3 years	[TODO]	[TODO]	Current

Evidence ID	Topic/Measure	Description	Document Type	Location/Link	Owner	Retention Period	Last Review	Next Review	Status
E-003	Training Records	Attendance Lists Security Awareness	Attendance List	[TODO: LMS]	Thomas Weber	5 years	[TODO]	[TODO]	Current
E-004	Audit Reports	Internal Audit Reports	Audit Report	[TODO]	Internal Audit	10 years	[TODO]	[TODO]	Current
E-005	Risk Acceptances	Documented Risk Acceptances	Approval Document	[TODO]	Max Mustermann	5 years	[TODO]	[TODO]	Current
E-006	Vulnerability Scans	Monthly Vulnerability Scan Reports	Scan Report	[TODO: Vulnerability Management Tool]	Thomas Weber	2 years	[TODO]	[TODO]	Current
E-007	Penetration Tests	Annual Pentest Reports	Pentest Report	[TODO]	Thomas Weber	5 years	[TODO]	[TODO]	Current
E-008	Incident Documentation	Incident Reports and Postmortems	Incident Report	[TODO: ITSM]	Anna Schmidt	3 years	[TODO]	[TODO]	Current
E-009	Change Approvals	Change Approvals with Security Review	Change Record	[TODO: ITSM]	Anna Schmidt	2 years	[TODO]	[TODO]	Current
E-010	Access Logs	Privileged Access Logs	Log Archive	[TODO: SIEM]	Thomas Weber	1 year	[TODO]	[TODO]	Current

Evidence ID	Topic/Measure	Description	Document Type	Location/Link	Owner	Retention Period	Last Review	Next Review	Status
E-011	Supplier Assessments	Third-Party Risk Assessments	Assessment Report	[TODO]	Thomas Weber	3 years	[TODO]	[TODO]	Current
E-012	Management Review	Annual Management Review Minutes	Minutes	[TODO]	Max Mustermann	10 years	[TODO]	[TODO]	Current
E-013	Basic Security Check	BSI Basic Check Results	Gap Analysis	[TODO]	Thomas Weber	3 years	[TODO]	[TODO]	Current
E-014	Protection Needs Assessment	Documented Protection Needs	Assessment	[TODO]	Thomas Weber	5 years	[TODO]	[TODO]	Current
E-015	Emergency Exercises	BCM/DR Test Protocols	Test Protocol	[TODO]	Thomas Weber	3 years	[TODO]	[TODO]	Current
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

50.3 3. Evidence Categories

50.3.1 3.1 Technical Evidence

- Scan Reports (Vulnerability, Compliance)
- Log Data and SIEM Evaluations
- Backup Protocols
- Patch Status Reports
- Configuration Documentation

50.3.2 3.2 Organizational Evidence

- Policies and Guidelines (approved)
- Training Records
- Audit Reports
- Management Review Minutes
- Risk Acceptances

50.3.3 3.3 Process Evidence

- Incident Reports
- Change Records
- Problem Management Documentation
- Test Protocols (DR, Backup, etc.)

50.3.4 3.4 Compliance Evidence

- Certificates (ISO, BSI, etc.)
- External Audit Reports
- Penetration Tests
- Data Protection Impact Assessments (DPIA)

50.4 4. Retention Periods

Document Type	Retention Period	Legal Basis
Audit Reports	10 years	Commercial Law
Training Records	5 years	Evidence Requirement
Incident Reports	3 years	Best Practice
Log Data	1 year (Standard), 3 years (Critical Systems)	GDPR, BSI
Risk Acceptances	5 years	Evidence Requirement
Contracts (Suppliers)	Contract Duration + 3 years	Commercial Law

50.5 5. Access Control

Access to Evidence: - **CISO:** Full Access - **Internal Audit:** Full Access (Read) - **Executive Management:** Full Access - **Area Managers:** Access to Own Evidence - **External Auditors:** Temporary Read Access (after approval)

Storage Locations: - Central Document Repository: [TODO: e.g., SharePoint, Confluence] - ITSM System: [TODO: e.g., ServiceNow, Jira] - SIEM/Log Management: [TODO] - CMDB: [TODO]

50.6 6. Review and Updates

Regular Review: - **Quarterly:** Completeness Check - **Annually:** Retention Period Review - **During Audits:** Check Availability and Currency

Responsible: Thomas Weber

50.7 7. Approval

Role	Name	Date	Approval
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI Standard 200-1: ISMS (Documentation) - BSI Standard 200-2: IT-Grundschutz Methodology (Evidence Management) - All ISMS Documents (0010-0630)

ewpage

Chapter 51

Appendix: Asset Inventory (Template)

Document ID: 0710
Document Type: Appendix/Template
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

51.1 1. Purpose and Objectives

The asset inventory of **AdminSend GmbH** documents all IT assets within the ISMS scope.

Responsible: Anna Schmidt

51.2 2. Maintenance Note

Recommendation: This inventory should be maintained in a CMDB (Configuration Management Database) or Asset Management Tool. This document serves as a template/export format.

CMDB System: [TODO: e.g., ServiceNow, Device42, NetBox]
Storage Location: {{ netbox.url }} or [TODO]

51.3 3. Asset Categories

51.3.1 3.1 Hardware Assets

- Servers (physical, virtual)
- Network Devices (routers, switches, firewalls)

- Storage Systems
- Endpoints (laptops, desktops, mobile devices)
- IoT Devices

51.3.2 3.2 Software Assets

- Operating Systems
- Applications (commercial, open source, custom development)
- Databases
- Middleware

51.3.3 3.3 Data Assets

- Databases
- File Servers/Shares
- Cloud Storage
- Backup Media

51.3.4 3.4 Services

- IT Services (internal, external)
- Cloud Services (SaaS, PaaS, IaaS)

51.4 4. Asset Register

Asset ID	Name	Type	Category	Owner	Location	Protection Need (C/I/A)	Lifecycle Status	Manufacturer	Model	Serial Number	Acquisition Date	EOL Date	Notes
{{ netbox.device.id }}	{{ netbox.device.name }}	Server	Hardware	Anna Schmidt	{{ netbox.site.name }}	[TODO]	Production	{{ netbox.device.manufacturer }}	{{ netbox.device.model }}	{{ netbox.device.serial }}	[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Protection Need Categories: - **Normal:** Standard protection need - **High:** Elevated protection need - **Very High:** Critical protection need

Lifecycle Status: - **Planning:** In procurement - **Development:** In development/configuration - **Production:** In production operation - **Maintenance:** In maintenance/support - **Decommissioned:** Shut down - **Disposal:** Scheduled for disposal

51.5 5. NetBox Integration

NetBox Instance: {{ netbox.url }}

Available Data from NetBox: - Devices: {{ netbox.device.name }}, {{ netbox.device.type }}, {{ netbox.device.role }} - Sites: {{ netbox.site.name }}, {{ netbox.site.region }} - IP Addresses: {{

netbox.ipaddress.address }} - VLANs: {{ netbox.vlan.name }}, {{ netbox.vlan.id }} - Racks: {{ netbox.rack.name }}, {{ netbox.rack.location }}

Synchronization: [TODO: Automatic/Manual, Frequency]

51.6 6. Asset Lifecycle Management

51.6.1 6.1 Procurement

- Asset is recorded (Status: Planning)
- Protection need is determined
- Owner is assigned

51.6.2 6.2 Commissioning

- Asset is configured and hardened
- Asset is transferred to production (Status: Production)
- Monitoring is activated

51.6.3 6.3 Operation

- Regular updates and patches
- Monitoring and maintenance
- Changes are documented (Change Management)

51.6.4 6.4 Decommissioning

- Asset is shut down (Status: Decommissioned)
- Data is securely deleted
- Asset is disposed of (Status: Disposal)

Reference: Document 0250 (Asset Lifecycle)

51.7 7. Responsibilities (RACI)

Activity	IT Management	Asset Owner	CMDB Admin	CISO
Record Asset	A	R	I	I
Determine Protection Need	A	C	I	R
Update Asset	I	R	A	I
Asset Review (annual)	A	R	C	C
Asset Disposal	A	R	I	C

Legend: - **R** = Responsible (Execution responsibility) - **A** = Accountable (Overall responsibility) - **C** = Consulted - **I** = Informed

51.8 8. Asset Tagging

Tagging Schema: - **Environment:** Production, Staging, Development, Test - **Criticality:** Critical, High, Medium, Low - **Owner:** Area manager - **Compliance:** ISO27001, BSI, GDPR, etc. - **Backup:** Yes/No - **DR:** Yes/No

Example (Cloud Resources):

```
Environment: Production
Criticality: High
Owner: Anna Schmidt
Compliance: ISO27001, BSI
Backup: Yes
DR: Yes
```

51.9 9. Reporting

Regular Reports: - **Monthly:** Asset Inventory Overview - **Quarterly:** EOL Report (Assets approaching End-of-Life) - **Annually:** Complete Asset Review

Responsible: Anna Schmidt

51.10 10. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium: OPS.1.1.1 General IT Operations - BSI IT-Grundschutz-Kompendium: OPS.1.2.2 Archiving - Document 0050: Structure Analysis - Document 0060: Protection Needs Assessment - Document 0250: Asset Lifecycle

ewpage

Chapter 52

Appendix: Data Flows and Interfaces (Template)

Document ID: 0720
Document Type: Appendix/Template
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

52.1 1. Purpose and Objectives

The documentation of data flows and interfaces of **AdminSend GmbH** supports: - Protection Needs Assessment (Document 0060) - Risk Analysis (Document 0090) - Crypto Concept (Document 0340/0350) - Data Protection Compliance (Document 0420/0430)

Responsible: Thomas Weber (CISO), Anna Schmidt (IT Management)

52.2 2. Data Flow Register

Data Flow ID	Source	Destination	Data Types	Protection Need (C/I/A)	Transport Path	Encryption	Storage	Provider/Third Country	Owner	Legal Basis	Note
DF-001	Web Server ({{ net-box.device.name }})	Database Server	Customer Data (personal)	Very High/High/High	{{ net-box.vlan.name }} (internal)	TLS 1.3	Encrypted (AES-256)	Internal	Anna Schmidt	GDPR Art. 6(1)(b)	[TODO]
DF-002	Backup Server	Cloud Storage (AWS S3)	Backup Data	High/High/High	Internet (VPN)	TLS 1.3 + AES-256	Encrypted (AES-256)	AWS (EU-West-1)	Anna Schmidt	GDPR Art. 28	[TODO]
DF-003	Employee (Remote)	VPN Gateway	Business Data	High/High/Normal	Internet	IPsec/IKEv2	N/A	Internal	Anna Schmidt	-	[TODO]
DF-004	ERP System	Payment Gateway	Payment Data	Very High/Very High/High	Internet (HTTPS)	TLS 1.3	Not Stored	Payment Provider (EU)	Anna Schmidt	PCI-DSS	[TODO]
DF-005	SIEM	Log Archive	Log Data	Normal/High/Normal	{{ net-box.vlan.name }} (Management)	TLS 1.2	Encrypted	Internal	Thomas Weber	-	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

52.3 3. Interface Register

Interface ID	System A	System B	Protocol	Port	Authentication	Encryption	Data Direction	Frequency	Owner	Note
IF-001	Web Server	Database	PostgreSQL	5432	Certificate	TLS 1.3	Bidirectional	Permanent	Anna Schmidt	[TODO]
IF-002	ERP	CRM	REST API	443	OAuth 2.0	TLS 1.3	Bidirectional	Real-time	Anna Schmidt	[TODO]
IF-003	Monitoring	SIEM	Syslog	514	Certificate	TLS 1.2	Unidirectional	Permanent	Thomas Weber	[TODO]
IF-004	AD	LDAP Clients	LDAPS	636	Kerberos	TLS 1.2	Bidirectional	On-Demand	Anna Schmidt	[TODO]
IF-005	Backup Server	Cloud Storage	S3 API	443	API Key	TLS 1.3	Unidirectional	Daily	Anna Schmidt	[TODO]

Interface ID	System A	System B	Protocol	Port	Authentication	Encryption	Data Direction	Frequency	Owner	Note
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

52.4 4. External Interfaces and Third Parties

Third Party	Service	Data Types	Protection Need	Location/Third Country	Contract	Data Protection Agreement	Owner	Note
AWS	Cloud Hosting (EC2, S3)	Business Data, Backup	High/High/High	EU (Frankfurt, West-1	[TODO: Contract Number]	Yes (Art. 28 GDPR)	Anna Schmidt	[TODO]
Microsoft	Office 365	Email, Documents	High/High/Normal	EU	[TODO]	Yes	Anna Schmidt	[TODO]
Payment Provider	Payment Processing	Payment Data	Very High/Very High/High	EU	[TODO]	Yes	Anna Schmidt	PCI-DSS certified
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Reference: Document 0400/0410 (Supplier and Outsourcing Management)

52.5 5. Data Flow Diagrams

Storage Location: `diagrams/dataflows.png` or [TODO: Confluence/SharePoint]

Recommended Diagrams: 1. **High-Level Data Flow:** Overview of all main data flows 2. **Detailed Data Flows:** Per critical system/service 3. **External Data Flows:** All data flows to third parties 4. **Personal Data:** GDPR-relevant data flows

Tools: [TODO: e.g., Lucidchart, Draw.io, Visio]

52.6 6. Data Categories

52.6.1 6.1 Personal Data (GDPR)

- Customer Data (name, address, email, etc.)
- Employee Data (HR data)
- Special Categories (Art. 9 GDPR): [TODO: if applicable]

52.6.2 6.2 Business Data

- Contracts
- Financial Data
- Trade Secrets
- Strategic Documents

52.6.3 6.3 Technical Data

- Log Data
- Monitoring Data
- Configuration Data

52.6.4 6.4 Public Data

- Marketing Materials
- Public Website Content

52.7 7. Encryption Requirements

Data Type	Protection Need	Transport Encryption	Storage Encryption	Key Management
Personal Data	Very High	TLS 1.3 (min. TLS 1.2)	AES-256	HSM/KMS
Business Data	High	TLS 1.3 (min. TLS 1.2)	AES-256	KMS
Log Data	Normal	TLS 1.2	Optional	KMS
Public Data	Normal	TLS 1.2	Not Required	-

Reference: Document 0340/0350 (Cryptography and Key Management)

52.8 8. Cross-Border Data Transfer

Data Transfer to Third Countries:

Destination Country	Data Types	Legal Basis	Safeguards	Approval	Note
USA	[TODO]	Standard Contractual Clauses (SCC)	[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Reference: Document 0420/0430 (Data Protection)

52.9 9. Responsibilities (RACI)

Activity	IT Management	CISO	Data Protection Officer	Business Unit
Document Data Flows	A	C	C	R
Determine Protection Need	A	R	C	C
Implement Encryption	R	C	I	I
Review Third-Party Contracts	C	C	R	A
Annual Review	A	R	C	C

Legend: - **R** = Responsible (Execution responsibility) - **A** = Accountable (Overall responsibility) - **C** = Consulted - **I** = Informed

52.10 10. Change Management

Changes to Data Flows: - New data flows must be documented before commissioning - Changes to existing data flows require change ticket - Security-relevant changes require CISO approval

Reference: Document 0380/0390 (Change Management)

52.11 11. Approval

Role	Name	Date	Approval
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Data Protection Officer	[TODO]	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI Standard 200-2: IT-Grundschutz Methodology (Structure Analysis) - BSI IT-Grundschutz-Kompendium: CON.1 Crypto Concept - Document 0050: Structure Analysis - Document 0060: Protection Needs Assessment - Document 0090: Risk Analysis - Document 0340/0350: Cryptography and Key Management - Document 0420/0430: Data Protection

ewpage

Chapter 53

Appendix: Network Plan and Zone Model (Template)

Document ID: 0730
Document Type: Appendix
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

53.1 1. Purpose and Objectives

The documentation of network architecture and zone model of **AdminSend GmbH** serves: - Structure Analysis (Document 0050) - Risk Analysis (Document 0090) - Network Security (Document 0460/0470) - Incident Response (Document 0320/0330)

Responsible: Anna Schmidt (IT Management)

53.2 2. High-Level Network Plan

Storage Location: `diagrams/network-highlevel.png` or [TODO: Confluence/SharePoint]

Representation: - All network zones - Firewalls and trust boundaries - Main connections (Internet, WAN, VPN) - Critical systems

Tools: [TODO: e.g., Lucidchart, Draw.io, Visio]

53.3 3. Network Zones and Segmentation

Zone ID	Zone Name	Description	Trust Level	Access Control	Responsible	Note
Z-001	Internet	Public Internet	Untrusted	Firewall (Deny All)	Anna Schmidt	[TODO]
Z-002	DMZ	Demilitarized Zone (Web Server, Mail Gateway)	Low Trust	Firewall (Whitelist)	Anna Schmidt	[TODO]
Z-003	Internal LAN	Internal Corporate Network	Trusted	Firewall (Default Allow)	Anna Schmidt	{{ net-box.vlan.name }}
Z-004	Server VLAN	Production Servers	High Trust	Firewall (Whitelist)	Anna Schmidt	{{ net-box.vlan.name }}
Z-005	Database VLAN	Database Servers	High Trust	Firewall (Strict Whitelist)	Anna Schmidt	{{ net-box.vlan.name }}
Z-006	Management VLAN	Management Network (Monitor-ing, Backup, Admin)	High Trust	Firewall (Strict Whitelist)	Anna Schmidt	{{ net-box.vlan.name }}
Z-007	Guest WiFi	Guest WLAN	Untrusted	Captive Portal, Firewall	Anna Schmidt	[TODO]
Z-008	VPN	Remote Access (VPN)	Trusted (after authentica-tion)	VPN Gateway, MFA	Anna Schmidt	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

53.4 4. Trust Boundaries and Firewall Rules

53.4.1 4.1 Trust Boundaries

Definition: Trust boundaries are borders between network zones with different trust levels.

Main Boundaries: 1. **Internet DMZ:** Firewall with strict rules (only HTTP/HTTPS inbound) 2. **DMZ Internal LAN:** Firewall with whitelist (only defined connections) 3. **Internal LAN Server VLAN:** Firewall with whitelist 4. **Server VLAN Database VLAN:** Firewall with strict whitelist (only DB ports) 5. **Management VLAN All Zones:** Firewall with strict whitelist (only admin access)

53.4.2 4.2 Firewall Rules (Example)

Rule ID	Source	Destination	Service/Port	Action	Justification	Owner
FW-001	Internet	DMZ (Web Server)	HTTPS (443)	Allow	Public web access	Anna Schmidt
FW-002	DMZ (Web Server)	Server VLAN (App Server)	HTTPS (8443)	Allow	Backend communication	Anna Schmidt
FW-003	Server VLAN (App Server)	Database VLAN (DB Server)	PostgreSQL (5432)	Allow	Database access	Anna Schmidt
FW-004	Management VLAN	All Zones	SSH (22), RDP (3389)	Allow	Admin access	Anna Schmidt
FW-005	Guest WiFi	Internet	HTTP/HTTPS (80/443)	Allow	Internet access for guests	Anna Schmidt
FW-006	Guest WiFi	Internal LAN	All	Deny	Isolation from internal network	Anna Schmidt
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Reference: Document 0460/0470 (Network Security)

53.5 5. Network Devices

Device ID	Type	Model	Location	IP Address	Management IP	Role	Owner	Note
{{ netbox.device.id }}	{{ netbox.device.type }}	{{ netbox.device.model }}	{{ netbox.site.name }}	{{ netbox.ipaddress.address }}	[TODO]	{{ netbox.device.role }}	Anna Schmidt	[TODO]
[TODO]	Firewall	[TODO]	[TODO]	[TODO]	[TODO]	Perimeter Firewall	Anna Schmidt	[TODO]
[TODO]	Switch	[TODO]	[TODO]	[TODO]	[TODO]	Core Switch	Anna Schmidt	[TODO]
[TODO]	Router	[TODO]	[TODO]	[TODO]	[TODO]	Internet Router	Anna Schmidt	[TODO]

NetBox Integration: {{ netbox.url }}

53.6 6. VLANs

VLAN ID	VLAN Name	Network (CIDR)	Gateway	Description	Zone	Note
{{ net-box.vlan.id }}	{{ net-box.vlan.name }}	[TODO: e.g., 10.0.10.0/24]	[TODO]	[TODO]	[TODO]	[TODO]
[TODO]	Management	[TODO]	[TODO]	Management Network	Z-006	[TODO]
[TODO]	Servers	[TODO]	[TODO]	Production Servers	Z-004	[TODO]
[TODO]	Database	[TODO]	[TODO]	Database Servers	Z-005	[TODO]

53.7 7. Administrative Access

53.7.1 7.1 Bastion/Jump Hosts

Bastion Host: [TODO: Hostname/IP]
Purpose: Central access point for administrative access to production systems
Authentication: MFA (Multi-Factor Authentication)
Protocols: SSH, RDP
Logging: All access is logged (SIEM)

Reference: Document 0200/0210 (Access Control)

53.7.2 7.2 Remote Admin

VPN Gateway: [TODO: Hostname/IP]
Authentication: MFA (Multi-Factor Authentication)
Protocol: IPsec/IKEv2 or OpenVPN
Access: Only for authorized administrators
Logging: All VPN connections are logged

Reference: Document 0470 (VPN and Admin Access)

53.7.3 7.3 Break-Glass Access

Emergency Access: [TODO: Description]
Activation: Only in emergencies (documented)
Monitoring: Immediate notification upon use

Reference: BCM Document (Emergency Access)

53.8 8. Network Monitoring

Monitoring Tools: - **SIEM:** [TODO: e.g., Splunk, ELK] - **Network Monitoring:** [TODO: e.g., Nagios, Zabbix, PRTG] - **Flow Analysis:** [TODO: e.g., NetFlow, sFlow]

Monitored Metrics: - Bandwidth utilization - Firewall logs - Anomalies (e.g., port scans, DDoS) - VPN connections

Reference: Document 0300/0310 (Logging and Monitoring)

53.9 9. Network Diagrams

Available Diagrams: 1. **High-Level Network Plan:** Overview of all zones and main connections 2. **Detailed Network Plan:** All devices, VLANs, IP addresses 3. **Firewall Topology:** All firewalls and trust boundaries 4. **WAN Topology:** Site connectivity (if applicable) 5. **Cloud Integration:** Connections to cloud providers (AWS, Azure, etc.)

Storage Location: `diagrams/` or [TODO: Confluence/SharePoint]

53.10 10. Site Connectivity (WAN)

If applicable:

Site	Connection Type	Bandwidth	Provider	Backup Connection	Encryption	Note
{{ net-box.site.name }}	[TODO: e.g., MPLS, VPN]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

53.11 11. Cloud Integration

Cloud Providers:

Provider	Service	Connection Type	Encryption	Region	Note
AWS	EC2, S3, RDS	VPN (Site-to-Site)	IPsec	EU-West-1	[TODO]
Azure	[TODO]	ExpressRoute	[TODO]	West Europe	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Reference: Document 0400/0410 (Suppliers and Cloud Security)

53.12 12. Responsibilities (RACI)

Activity	IT Management	Network Admin	CISO	Firewall Admin
Maintain Network Plan	A	R	I	C
Change Firewall Rules	A	C	C	R
VLAN Configuration	A	R	I	I
Network Monitoring	A	R	C	I
Annual Review	A	R	C	C

Legend: - **R** = Responsible (Execution responsibility) - **A** = Accountable (Overall responsibility) - **C** = Consulted - **I** = Informed

53.13 13. Change Management

Changes to Network Architecture: - All changes require change ticket - Security-relevant changes require CISO approval - Network plan must be updated after changes

Reference: Document 0380/0390 (Change Management)

53.14 14. Approval

Role	Name	Date	Approval
IT Management	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium: NET.1.1 Network Architecture and Design - BSI IT-Grundschutz-Kompendium: NET.1.2 Network Management - BSI IT-Grundschutz-Kompendium: NET.3.2 Firewall - Document 0050: Structure Analysis - Document 0090: Risk Analysis - Document 0460/0470: Network Security

ewpage

Chapter 54

Appendix: Terms and Abbreviations

Document ID: 0740
Document Type: Appendix
Reference Framework: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Classification: internal
Last Updated: {{ meta.document.last_updated }}
Next Review: {{ meta.document.next_review }}

54.1 1. Purpose

This document defines central terms and abbreviations used in the ISMS documentation of **AdminSend GmbH**.

54.2 2. Terms

54.2.1 A

Asset
Valuable item (e.g., hardware, software, data, processes) that is of value to the organization and must be protected.

Authentication
Process of verifying the identity of a user, system, or application.

Authorization
Process of granting access rights to resources after successful authentication.

Availability
Property that information and systems are available and usable when needed.

54.2.2 B

Backup
Copy of data that can be used for recovery in case of data loss.

Basic Security Check
Verification of the implementation of BSI IT-Grundschutz requirements (target-actual comparison).

Building Block (Baustein)
Modular security requirements in the BSI IT-Grundschutz Compendium applied to specific target objects (e.g., servers, applications).

BSI
Federal Office for Information Security (Germany - Bundesamt für Sicherheit in der Informationstechnik).

54.2.3 C

CIA Triad
Confidentiality, Integrity, Availability – the three fundamental principles of information security.

CMDB
Configuration Management Database – database for managing IT assets and their configurations.

Confidentiality
Property that information is only accessible to authorized persons.

54.2.4 D

Data Protection
Protection of personal data from misuse (legal framework: GDPR).

DMZ
Demilitarized Zone – network segment between internal network and Internet hosting publicly accessible services.

DSGVO/GDPR
General Data Protection Regulation (EU Regulation 2016/679).

54.2.5 E

Encryption
Conversion of data into an unreadable form to ensure confidentiality.

Endpoint
End device (e.g., laptop, desktop, smartphone) connected to the network.

54.2.6 F

Firewall
Security system for controlling network traffic between different network segments.

54.2.7 G

Gap Analysis
Comparison between target state (requirements) and actual state (implementation) to identify gaps.

54.2.8 H

Hardening
Hardening of systems by removing unnecessary services, applying security patches, and configuring according to best practices.

HSM
Hardware Security Module – specialized hardware for secure management of cryptographic keys.

54.2.9 I

IAM
Identity and Access Management – management of user identities and access rights.

Incident
Security incident that affects the confidentiality, integrity, or availability of information.

Information Domain (Informationsverbund)
Defined set of processes, information, IT systems, people, and rooms considered within the ISMS.

Integrity
Property that information is complete, correct, and unchanged.

ISB/CISO
Information Security Officer (ISB - Informationssicherheitsbeauftragter) / Chief Information Security Officer.

ISMS
Information Security Management System – systematic approach to managing information security.

ISO 27001
International standard for information security management systems.

54.2.10 K

KMS
Key Management System – system for managing cryptographic keys.

KPI
Key Performance Indicator – metric for measuring performance/effectiveness.

54.2.11 L

Least Privilege
Principle that users receive only the minimally necessary access rights.

Logging
Recording of events and activities in systems for traceability and analysis.

54.2.12 M

MFA
Multi-Factor Authentication – authentication with at least two independent factors (e.g., password + token).

Modeling (Modellierung)
Assignment of BSI building blocks to target objects in the information domain.

54.2.13 N

NetBox
Open-source tool for managing network and datacenter infrastructure (IPAM, DCIM).

54.2.14 P

Patch
Software update to fix security vulnerabilities or errors.

Penetration Test
Simulated attack on systems to identify security vulnerabilities.

Policy
High-level guideline defining security objectives and principles.

54.2.15 R

RACI
Responsibility Assignment Matrix: Responsible, Accountable, Consulted, Informed – model for clarifying responsibilities.

Risk Analysis
Systematic identification, assessment, and treatment of risks.

Risk Acceptance
Conscious decision to accept an identified risk (without further measures).

RTO
Recovery Time Objective – maximum tolerable downtime of a system/process.

RPO
Recovery Point Objective – maximum tolerable data loss (time period).

54.2.16 S

Protection Need (Schutzbedarf)
Assessment of asset criticality regarding confidentiality, integrity, and availability (Normal, High, Very High).

SIEM
Security Information and Event Management – system for central collection and analysis of security events.

SoA
Statement of Applicability – declaration of applicability of security measures (ISO 27001).

Structure Analysis (Strukturanalyse)
Capture and documentation of IT infrastructure and processes in the information domain.

54.2.17 T

TLS
Transport Layer Security – cryptographic protocol for secure data transmission.

Trust Boundary
Border between network segments with different trust levels.

54.2.18 V

VLAN
Virtual Local Area Network – logical segmentation of a physical network.

Vulnerability
Weakness in a system that can be exploited by attackers.

54.2.19 Z

Zero Trust
Security model assuming that no user or system is trustworthy by default.

54.3 3. Abbreviations

Abbreviation	Meaning
AD	Active Directory
AES	Advanced Encryption Standard
API	Application Programming Interface
AV	Antivirus
AWS	Amazon Web Services
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BSI	Federal Office for Information Security (Germany)
C/I/A	Confidentiality / Integrity / Availability
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
CRM	Customer Relationship Management
DAST	Dynamic Application Security Testing
DB	Database
DCIM	Data Center Infrastructure Management
DDoS	Distributed Denial of Service

Abbreviation	Meaning
DMZ	Demilitarized Zone
DNS	Domain Name System
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DSGVO	General Data Protection Regulation (German)
EDR	Endpoint Detection and Response
EOL	End of Life
ERP	Enterprise Resource Planning
GDPR	General Data Protection Regulation
HR	Human Resources
HSM	Hardware Security Module
HTTP/HTTPS	Hypertext Transfer Protocol (Secure)
IAM	Identity and Access Management
IDS/IPS	Intrusion Detection/Prevention System
IoT	Internet of Things
IP	Internet Protocol
IPAM	IP Address Management
IPsec	Internet Protocol Security
ISB	Information Security Officer (German)
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITSM	IT Service Management
KMS	Key Management System
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
LMS	Learning Management System
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MPLS	Multiprotocol Label Switching
NAC	Network Access Control
NDA	Non-Disclosure Agreement
OS	Operating System
PaaS	Platform as a Service
PCI-DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
RACI	Responsible, Accountable, Consulted, Informed
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SAST	Static Application Security Testing
SCC	Standard Contractual Clauses
SDLC	Software Development Lifecycle
SIEM	Security Information and Event Management

Abbreviation	Meaning
SLA	Service Level Agreement
SoA	Statement of Applicability
SOC	Security Operations Center
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer (deprecated, see TLS)
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

54.4 4. BSI-Specific Terms

BSI Standard 200-1
Management Systems for Information Security (ISMS)

BSI Standard 200-2
IT-Grundschutz Methodology

BSI Standard 200-3
Risk Analysis Based on IT-Grundschutz

IT-Grundschutz Compendium
Collection of building blocks with security requirements for various target objects

Building Block (Baustein)
Modular security requirements in the IT-Grundschutz Compendium (e.g., APP.3.1 Web Applications, SYS.1.1 General Server)

Basic Requirements (Basis-Anforderungen)
Minimum requirements that must be implemented for basic protection

Standard Requirements (Standard-Anforderungen)
Requirements for standard protection (beyond basic)

Requirements for Increased Protection Needs
Additional requirements for assets with high or very high protection needs

54.5 5. Approval

Role	Name	Date	Approval
CISO	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

References: - BSI IT-Grundschutz-Kompendium: Glossary - ISO 27000: Information security management systems – Overview and vocabulary - All ISMS Documents (0010-0630)

ewpage