Cybersecurity in a PSAP

A Practical Approach

In this case study document, PSAPs can explore concrete examples of how to make their systems more secure.

Cybersecurity in a PSAP

Version: 1

Publication date: 16/05/2020

Status of the document: APPROVED

EENA
European Emergency Number Association
EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
T: +32/2.534.97.89
E-mail: info@eena.org

Authors that contributed to this document:

This document was written by members of EENA.

Author

Henning Schmidtpott – Integrated Control Centre, Freiburg, Germany

Contributors

Cristina Lumbreras – EENA

Daniel Gilles – Federal Office for Information Security (BSI), Germany

Rose Michael - EENA

LEGAL DISCLAIMER:

This document is authored by EENA staff members with contributions from individual members of EENA and represents the views of EENA. This document does not represent the views of individual members of EENA, or any other parties.

This document is published for information purposes only and it does not declare to be a statement or interpretation of EU law or the national law of EU Member States. This document is entirely without prejudice to the views of relevant national statutory authorities and their legal functions and powers, whether under EU law or the national law of their Member State. Accordingly, under no circumstances may reliance be placed upon this document by any parties in compliance or otherwise with any applicable laws. Neither may reliance be placed upon this document in relation to the suitability or functionality of any technical specifications, or any other matters discussed in it. Legal advice, technical advice and other advice as relevant, may be sought as necessary.

EXECUTIVE SUMMARY

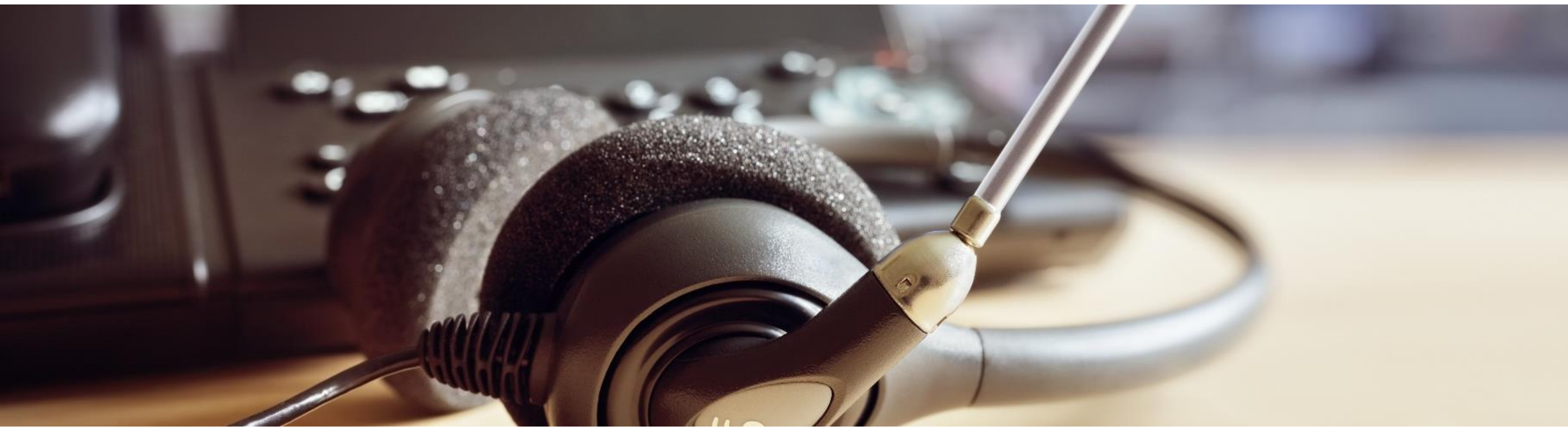
As our lives become more and more connected and as we become increasingly reliant on technology, cybersecurity should always be taken into account. Emergency services organisations are by no means exempt and Public Safety Answering Points (PSAPs) need to actions to ensure the continuity of service of the emergency numbers.

This document aims to help PSAPs to do this by providing a case study of a concrete approach, demonstrating how their systems can be made safer and resistant against cyber-attacks. The document is built on EENA's document *Cybersecurity – Guidelines and Best Practices for Emergency Services* and the recommended approach of the *German Federal Office for Information Security (BSI) IT-Grundschutz*.

The case study document is split into several different sections. In the first part, the formal frame conditions are set. In the second part, the reference architecture of a typical PSAP is specified and the protection requirements for the different objects are identified. In the third part, the measures to be implemented are determined. Both requirements and measures correspond to BSI IT-Grundschutz. The standard protection of IT-Grundschutz is compatible with ISO 27001 certification.

Cybersecurity should always be considered as a priority and emergency services are by no means exempt from cyber-attacks.

This case study aims to help Public Safety Answering Points with concrete examples of how they could approach the challenge of making systems safer and more resistant to cyber-attacks.



1 | SCOPE

Target audience

This document aims to assist decision-makers of information technology in PSAPs, industrial solution providers offering products and planning offices for PSAPs.

Protection requirements

Operational readiness of PSAPs must be guaranteed permanently. Correctness and confidentiality of the processed data must be emphasised. The aims of IT security, confidentiality, availability and integrity must be achieved far in excess of the usual quality. So, the level of cyber security protection of a PSAP has to be above the Standard Protection of the BSI IT-Grundschutz.

IT-Grundschutz procedure

BSI IT Grundschutz is a management system for information security, covering technical, organisational, infrastructural and personnel aspects. It is available for free for all users at the *BSI Website*.

BSI IT-Grundschutz offers three approaches: Basis Protection, Standard Protection and Core Protection. Depending of the chosen approach, the requirements in the modules must be implemented. The requirements in this document correspond to at least the Standard Protection of BSI- Standard 200-2. Furthermore, it is recommended to implement some requirements of the higher protection approach.

Compatibility with other standards

By implementing the Standard Protection, compatibility with ISO 27001 is given.

Framework

The *General Data Protection Regulation* is considered.

2 | SPECIFICATION OF INFORMATION DOMAIN

The information domain indicates the associated components of the general institution or of a specific scope of application. In a first step, the information domain must be specified by defining the relevant and not relevant parts for cyber security in PSAPs considered in this paper.

2.1 COMPONENTS OF INFORMATION DOMAIN

The following table shows the technical parts of the information domain supporting the processes within a PSAP considered in this paper.

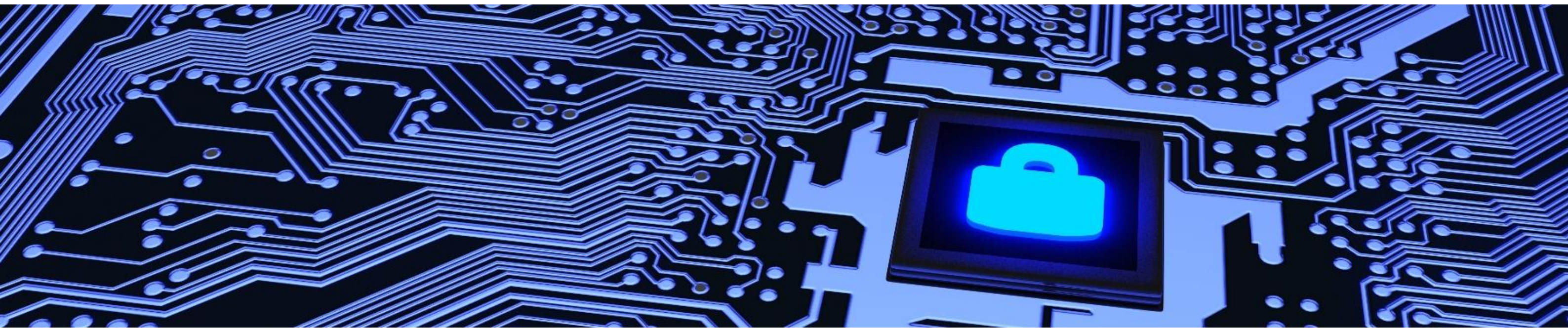
Identifier	Objects of information domain
ID1	Processes
ID2	Applications
ID3	Buildings and rooms
ID4	IT systems
ID5	Communication and networks

2.2 COMPONENTS NOT CONSIDERED

Not considered in this document is the broadcasting system. The broadcasting system is an independent system with interfaces to the Computer Aided Dispatch (CAD) and Integrated Communication Control Systems (ICCS) in the PSAP and it needs to be considered separately.

The protection of the external telecommunication connections is the responsibility of the network operators. The PSAPs can't intervene in this domain or take any provisions. For this reason, the telecommunication connections are not part of this document.

Mobile apps are also not included in this document. CAD or ICCS systems in the PSAPs may have interfaces to receive or send information by apps. Nevertheless, the security of the app itself is not the responsibility of the PSAP as it must be seen as a third-party application.



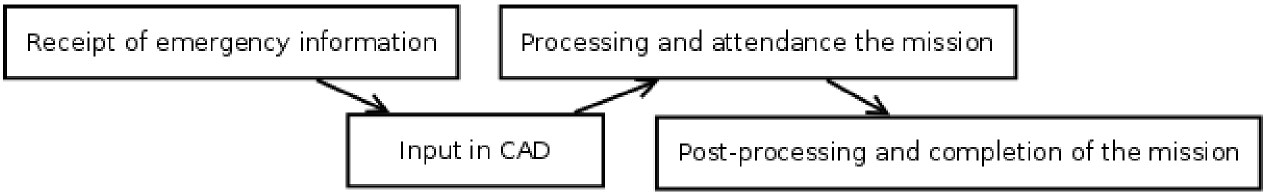
3 | REFERENCE ARCHITECTURE

The reference architecture includes buildings and rooms in which the PSAP operates, the communication links, the networks and the components required for them. In addition, all of the involved IT systems, the applications used and the processes running in the PSAPs are listed in the reference architecture.

It is possible that the reference architecture differs from the actual existing architecture of a PSAP. The handling of such deviations is described in Section 3.7.

3.1 | PROCESSES

The operation of a PSAP is subdivided into different processes, which are relevant for implementing the BSI IT-Grundschutz. These processes are defined in this section. The core processes are the receipt of the incoming emergency information and the input in the CAD, the processing and attendance of the mission, as well as the post-processing and completion of the mission (see Figure 1).


Receipt of emergency information
Processing and attendance the mission
Input in CAD
Post-processing and completion of the mission

Core processes in a PSAP

In the following table, the processes to be carried out in the PSAP are subdivided into sub-processes and provided with an identifier.

Identifier	Process of information domain
P1.1	Information receipt by phone call
P1.2	Information receipt by telefax
P1.3	Information receipt by email
P1.4	Information receipt by broadcast
P1.5	Information receipt by Web
P1.6	Information receipt by automatic fire alarm systems
P1.7	Information receipt by eCall
P2.1	Input in CAD manually
P2.2	Input in CAD automatically
P3.1	Dispatch
P3.2	Alarm
P3.3	Control
P3.4	Documentation
P4.1	Transmit data to third parties
P4.2	Archiving
P5.1	Receiving data by email and on USB storage (master data management)
P5.2	Input of data in CAD and ICCS (master data management)
P6	Conferences and training

3.2 | APPLICATIONS

In addition to the processes, the information domain also includes the applications that support optimal processing of the processes. In a PSAP, these are in particular the CAD and the ICCS. The e-mail client and the web browser are also important components. All the applications are listed in the following table with an identifier. The right-hand column indicates which processes are supported by the applications.

Identifier	Applications of information domain	Supported processes
A1	CAD	P1.6, P1.7, P2, P3, P4, P5.2
A2	ICCS	P1.1, P1.4, P1.7, P3, P5.2
A3	Webbrowser	P1.5, P3, P5
A4	Email client	P1.3, P5.1
A5	Hazardous material information systems	P2.1, P3
A6	PDF-Viewer	P2.1, P3, P5
A7	Office-Products	P5.1
A8	File depot, network drive	P4, P5

3.3 | IT SYSTEMS

In addition to the applications, the IT systems required for operating the applications are also part of the information domain. These include, for example, operating systems, or the hardware provided for this purpose. Components that affect network connections are considered separately in section 3.4.

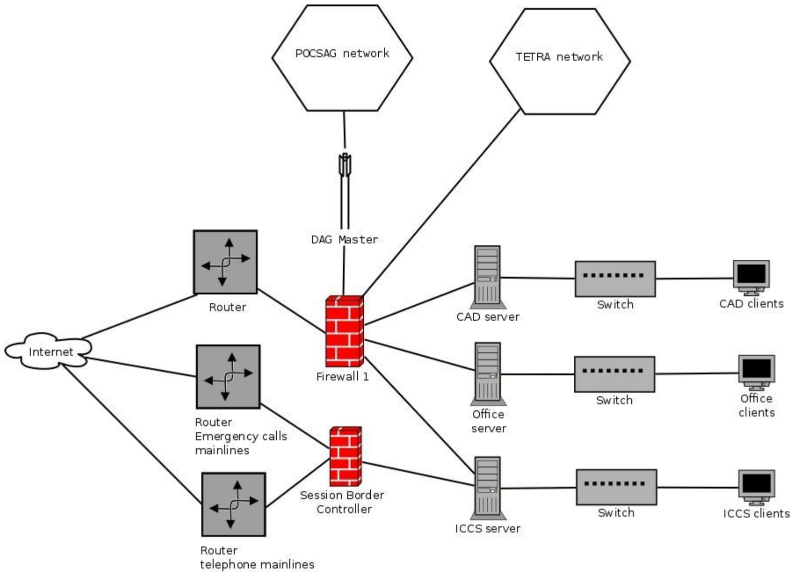
Identifier	IT systems of information domain	Depending objects
S1.1	Operating systems for clients	A1, A2, A3, A4, A5, A6, A7, A8
S1.2	Operating systems for servers	A1, A2
S2.1	Server	A1, A2
S2.2	Virtualisation platforms	A1, A2
S3	Workstation clients	A1, A2, A3, A4, A5, A6, A7, A8
S4	Fax machine	P1.2
S5	Printer and scanner	A1, A6, A7

3.4 | COMMUNICATION LINKS AND NETWORK

Applications and systems of the PSAP are integrated in various networks. Even if the number and structure of the networks cannot be generalised in detail, it is assumed that the architecture is at least similar in many control centres. The operation of the networks requires active and passive network components.

Identifier	Networks of information domain	Depending objects
N1	CAD network	A1, S1, S2, S3, S5
N2	ICCS network	A2, S1, S2, S3, S5
N3	Office network	A3, A4, A5, A6, A7, A8, S1, S2, S3, S5
N4	Network to Internet Service Provider	A1, A2, A3, A4
N5.1	Router	N1, N2, N3
N5.2	Switches	N1, N2, N3
N5.3	Firewalls	N1, N2, N3
N5.4	Session Border Controller	N2
N6	Cable and patch panels	N1, N2, N3
N7	Alerting POCSAG network	A1

3.5 | NETWORK DIAGRAM



3.6 | BUILDINGS AND ROOMS

Not only do the information technology components play a major role in information security, but the security of the buildings and rooms in which the PSAP operates must also be taken into account. This does not only apply to the dispatching room, where the emergency calls are received and the rescue services are dispatched. The rooms where servers and other technology are housed must be considered, as well as the office space for administrative employees.

Identifier	Rooms of information domain	Depending objects
R1	Dispatching room	P1, P2, P3, S3, S4, S5
R2	Computer centre	S2
R3.1	Management office rooms	S3, S4, S5
R3.2	Master data management office	P5, S3, S4, S5
R3.3	System administrator office	S3, S4, S5
R4	Telecommunication network room	N2, N4
R5	Archive room	P4
R6	Conference- and training room	P6

3.7 | HANDLING DIFFERENCES

If the information domain to be protected differs from the reference architecture, the additional or non-existent objects must be documented. These objects must be allocated to suitable components of the BSI IT-Grundschutz Compendium. The derived requirements must be adjusted depending on the protection requirements.

4 | PROTECTION REQUIREMENTS

The BSI IT-Grundschutz Compendium provides modules giving application-specific recommendations for the implementation of IT-Grundschutz.

First, the protection requirements of the processes, applications, IT systems and communication links must be defined. Afterwards, the relevant modules must be identified and an adaptation of the requirements to the corresponding target group must be carried out. The result of adapting the requirements may mean that all or only certain requirements of the module are relevant for information security in emergency response centres. Also, requirements can be considered as completely irrelevant. The relevance of the measures listed in the requirements must also be identified.

4.1 | HANDLING DIFFERENCES

When determining the protection requirements, the implications of violating the basic objectives of information security, confidentiality, integrity, or availability are fundamental. These effects are considered below. The BSI names various scenarios to which damage can relate. This considers the damage scenarios listed in table 4.

Violations of laws, regulations or contracts (DS1) may be present, for example, if the PSAP is not ready for operation and thus cannot fulfil its tasks (DS4). At the same time, this can lead to impairments to the personal integrity of the caller (DS3) if the person is not helped on time. Infringements of data protection laws also fall under damage scenario 1. The transmission of confidential information, via callers or patients to unauthorized persons, also constitutes an impairment of the informational right of self-determination of the persons seeking help (DS2). All these cases can also have financial consequences for the PSAP due to claims for damages by the victims (DS6).

For the citizens, a high level of confidence in the work of the PSAP is fundamental. Being helped in an emergency gives people a feeling of safety. Due to a negative external effect (DS5), this certainty can be lost. The same applies to the own personnel of the PSAP or the affiliated rescue organisations with a negative interior effect. These effects can occur, for example, due to defaults and associated negative media coverage.

Identifier	Damage Scenario
DS1	Violations of laws, regulations or contracts
DS2	Impairment of the informational right of self-determination
DS3	Impaired personal integrity
DS4	Impairment of task fulfilment
DS5	Negative interior or exterior effect
DS6	Financial impacts

The damage scenarios are considered individually in the following sections for each of the basic objectives of information security. The damage impact can usually not be determined in detail in advance. For this reason, the IT-Grundschutz methodology of the BSI recommends defining three categories that classify the protection requirement. The three categories are normal, high or very high. Table v lists the categories, plus the damage impact. The damage impact can always refer to the PSAP itself or to the citizens seeking help.

Category	Recommended protection needs
Normal	The effects of damage for the PSAP or the citizens seeking help are limited and manageable.
High	The damage effects can considerably restrict the operation of the PSAP. For the citizens seeking for help, the consequences can be considerable.
Very high	The damage effects can shut down the operation of the PSAP. For people seeking help, there can be existential or life-threatening consequences.

When determining the protection requirements of an object specified in Section 4, it is always necessary to consider the processes or other objects for which this object is needed. If, for example, an object is used for a process whose protection requirement is very high, the protection requirement of the object considered must also be classified as very high.

4.1.1 | PROTECTION REQUIREMENTS FOR PROCESSES

For determining the protection requirements of the processes, the extent of damage to the respective process must be determined. First, every process defined in section 4.1 is examined concerning confidentiality. This is followed by an inquiry into integrity. Finally, the protection requirement for the availability of the individual processes is determined.

Protection requirements concerning confidentiality for processes		
Object	**Protection need**	**Reasons**
P1.1	very high	Processing of personal data with medical diagnosis (DS1, DS2, DS5, DS6).
P1.2	very high	Processing of personal data with medical diagnosis (DS1, DS2, DS5, DS6).
P1.3	normal	PSAPs usually don’t receive confidential data by email.
P1.4	very high	Processing of personal data with medical diagnosis (DS1, DS2, DS5, DS6).
P1.5	very high	Processing of personal data with medical diagnosis (DS1, DS2, DS5, DS6).
P1.6	normal	Only technical parameters are transmitted.
P1.7	normal	Only technical parameters are transmitted.
P2.1	very high	Processing of personal data with medical diagnosis (DS1, DS2, DS5, DS6).
P2.2	normal	Only technical parameters are processed.
P3	very high	Processing of personal data with medical diagnosis (DS1, DS2, DS5, DS6).
P4	very high	Processing of personal data with medical diagnosis (DS1, DS2, DS5, DS6).
P5	high	Processing of personal data (DS1, DS2, DS5, DS6).

Protection requirements concerning integrity for processes		
Object	**Protection need**	**Reasons**
P1, P2, P3, P5	very high	Life-threatening consequences by processing incorrect data or faulty behavior (DS1, DS3, DS4, DS5, DS6).
P4, P6	normal	Slight consequences by processing incorrect data or faulty behavior (DS1, DS6).

Protection requirements concerning availability for processes		
Object	**Protection need**	**Reasons**
P1.1, P1.2	very high	Life-threatening consequences by failure of emergency number 112 (DS1, DS3, DS4, DS5, DS6).
P1.3	normal	Slight consequences by failure of email, because emergency messages usually are not received by email (DS4, DS5).
P1.4	normal	Alternative ways of communication can be used (DS4, DS5).
P1.5	very high	Consequences increase if non phone emergency calls are received by web browser e.g. from an app (DS1, DS3, DS4, DS5, DS6).
P1.6	very high	High material damage possible (DS1, DS3, DS4, DS5, DS6).
P1.7	very high	Life-threatening consequences by failure of eCall receiver (SZ1, SZ3, SZ4, SZ5, SZ6).
P2, P3	very high	Life-threatening consequences by failure of CAD (DS1, DS3, DS4, DS5, DS6).
P4, P5	normal	Slight consequences as processes are not time critical (DS4, DS6).

4.1.2 | PROTECTION REQUIREMENTS FOR APPLICATIONS

The protection requirements for applications are based on the protection requirements of the processes that are supported by using the particular application. The maximum principle is considered and the highest protection requirements are inherited by the application. If the protection requirement for only part of the processes supported by the applications is classified as very high, then the protection requirement of the entire application must be rated as very high as well.

Protection requirements concerning confidentiality for applications		
Object	**Protection need**	**Reasons**
A1	very high	Very high protection requirements for P2.1, P3 und P4.
A2	very high	Very high protection requirements for P1.1, P1.4 und P3.
A3	very high	Very high protection requirements for P1.5 und P3.
A4	high	High protection requirements for P5.1.
A5	very high	Very high protection requirements for P2.1 und P3.
A6	very high	Very high protection requirements for P2.1 und P3.
A7	high	High protection requirements for P5.1.
A8	very high	Very high protection requirements for P4.

Protection requirements concerning integrity for applications		
Object	**Protection need**	**Reasons**
A1	very high	Very high protection requirements for P1.6, P1.7, P2, P3 und P5.2.
A2	very high	Very high protection requirements for P1.1, P1.4, P1.7, P3 und P5.2.
A3	very high	Very high protection requirements for P1.5, P3 und P5.
A4	very high	Very high protection requirements for P1.3 und P5.1.
A5	very high	Very high protection requirements for P2.1 und P3.
A6	very high	Very high protection requirements for P2.1, P3 und P5.
A7	very high	Very high protection requirements for P5.1.
A8	very high	Very high protection requirements for P5.

Protection requirements concerning availability for applications		
Object	**Protection need**	**Reasons**
A1	very high	Very high protection requirements for P1.6, P1.7, P2 und P3.
A2	very high	Very high protection requirements for P1.1, P1.7 und P3.
A3	very high	Very high protection requirements for P1.5 und P3.
A4	normal	Normal protection requirements for P1.3 und P5.1.
A5	very high	Very high protection requirements for P2.1 und P3.
A6	very high	Very high protection requirements for P2.1 und P3.
A7	normal	Normal protection requirements for P5.1.
A8	normal	Normal protection requirements for P5 und P5.

4.1.3 | PROTECTION REQUIREMENTS FOR IT SYSTEMS

The protection requirements for the IT systems of a PSAP depend on the applications that are installed on or connected to the IT systems. According to the maximum principle, the protection requirement must again be at least as high as for these applications.

Protection requirements concerning confidentiality for IT systems		
Object	**Protection need**	**Reasons**
S1.1	very high	Very high protection requirements for A1, A2, A3, A5, A6, A8
S1.2	very high	Very high protection requirements for A1, A2
S2	very high	Very high protection requirements for A1, A2
S3	very high	Very high protection requirements for A1, A2, A3, A5, A6, A8
S4	very high	Very high protection requirements for P1.2
S5	very high	Very high protection requirements for A1, A6

Protection requirements concerning integrity for IT systems		
Object	**Protection need**	**Reasons**
S1.1	very high	Very high protection requirements for A1, A2, A3, A4, A5, A6, A7, A8
S1.2	very high	Very high protection requirements for A1, A2
S2	very high	Very high protection requirements for A1, A2
S3	very high	Very high protection requirements for A1, A2, A3, A4, A5, A6, A7, A8
S4	very high	Very high protection requirements for P1.2
S5	very high	Very high protection requirements for A1, A6, A7

Protection requirements concerning availability for IT systems		
Object	**Protection need**	**Reasons**
S1.1	very high	Very high protection requirements for A1, A2, A3, A5, A6
S1.2	very high	Very high protection requirements for A1, A2
S2	very high	Very high protection requirements for A1, A2
S3	very high	Very high protection requirements for A1, A2, A3, A5, A6
S4	very high	Very high protection requirements for P1.2
S5	very high	Very high protection requirements for A1, A6

4.1.4 | PROTECTION REQUIREMENTS FOR COMMUNICATION LINKS AND NETWORKS

Many applications and IT systems used in the PSAP transmit and receive data via the networks and components defined in Section 4.4. The protection requirements of the networks and components thus depend on the protection requirements of the applications and IT systems that transmit and receive data via these networks

Protection requirements concerning confidentiality for networks		
Object	**Protection need**	**Reasons**
N1	very high	Very high protection requirements for A1
N2	very high	Very high protection requirements for A2
N3	very high	Very high protection requirements for A3, A5, A6, A8
N4	very high	Very high protection requirements for N1, N2 und N3
N5	very high	Very high protection requirements for N1, N2 und N3
N6	very high	Very high protection requirements for A1

Protection requirements concerning integrity for networks		
Object	**Protection need**	**Reasons**
N1	very high	Very high protection requirements for A1
N2	very high	Very high protection requirements for A2
N3	very high	Very high protection requirements for A3, A5, A6, A7, A8
N4	very high	Very high protection requirements for N1, N2 und N3
N5	very high	Very high protection requirements for N1, N2 und N3
N6	very high	Very high protection requirements for A1

Protection requirements concerning availability for networks		
Object	**Protection need**	**Reasons**
N1	very high	Very high protection requirements for A1
N2	very high	Very high protection requirements for A2
N3	very high	Very high protection requirements for A3, A5, A6
N4	very high	Very high protection requirements for N1, N2 und N3
N5	very high	Very high protection requirements for N1, N2 und N3
N6	very high	Very high protection requirements for A1

4.1.5 | PROTECTION REQUIREMENTS FOR BUILDINGS AND ROOMS

The determination of protection requirements for rooms depends on the IT systems installed in the room and the processes that are carried out in these rooms. The higher their need for protection, the higher the need for protection for the room. When determining the protection requirement, the amount of systems installed in the room must also be considered.

Protection requirements concerning confidentiality for buildings and rooms		
Object	**Protection need**	**Reasons**
R1	very high	Very high protection requirements for P1, P2, P3, S3, S4, S5
R2	very high	Very high protection requirements for S2
R3	very high	Very high protection requirements for S3, S4, S5 und P5
R4	very high	Very high protection requirements for N2
R5	very high	Very high protection requirements for P4
R6	normal	Normal protection requirements for P6

Protection requirements concerning integrity for buildings and rooms		
Object	**Protection need**	**Reasons**
R1	very high	Very high protection requirements for S3, S4, S5
R2	very high	Very high protection requirements for S2
R3	very high	Very high protection requirements for S3, S4, S5
R4	very high	Very high protection requirements for N2
R5	very high	Normal protection requirements for P4
R6	normal	Normal protection requirements for P6

Protection requirements concerning availability for buildings and rooms		
Object	**Protection need**	**Reasons**
R1	very high	Very high protection requirements for P1, P2 und P3
R2	very high	Very high protection requirements for S2
R3	normal	Using alternative room is possible
R4	very high	Very high protection requirements for N2
R5	very high	Normal protection requirements for P4
R6	normal	Normal protection requirements for P6

4.2 | MEASURES

After having determined the protection requirements of the processes, applications, IT systems and communication networks in the last section, the next step is to identify the relevant modules and adapt the requirements to the corresponding target group. The result of adapting the requirements may mean that all or only certain requirements of the module are relevant for information security in PSAPs. Likewise, requirements can be considered completely irrelevant. The relevance of the measures listed in the requirements must also be identified. In addition, specifications for implementing the requirements of the blocks are described.

The modules of the category Industrial IT are not listed from the outset due to their lack of relevance for the operation of PSAPs

Module		**Relevant?**	**Reason (if not relevant)**
ISMS: Information Security Management Systems			
ISMS.1	Security Management	Yes	
ORP: Organisation and Personnel			
ORP.1	Organisation	Yes	
ORP.2	Personell	Yes	
ORP.3	Awareness and Training	Yes	
ORP.4	Identity and Access Management	Yes	
ORP.5	Comliance Management	Yes	
CON: Concepts			
CON.1	Crypto Concept	Yes	
CON.2	Data Protection	Yes	
CON.3	Backup Concept	Yes	
CON.4	Selection and Use of Standard Software	Yes	

CON.5	Development and Use of Generic Applications	Yes	
CON.6	Deleting and Destroying	Yes	
CON.7	Information Security on Trips Abroad	No	PSAPs usually work local only
OPS: Operation			
OPS.1.1.2	Proper IT Administration	Yes	
OPS.1.1.3	Patch and Change Management	Yes	
OPS.1.1.4	Protection Against Malware	Yes	
OPS.1.1.5	Logging	Yes	
OPS.1.1.6	Software Tests and Approvals	Yes	
OPS.1.2.2	Archiving	Yes	
OPS.1.2.3	Exchange of Information and Storage Media	Yes	
OPS.1.2.4	Teleworking	No	Employees of PSAPs usually work in the PSAP rooms.
OPS.2.1	Outsourcing for Customers	Yes	
OPS.2.2	Cloud Usage	No	Operation of IT systems in PSAPs usually is in local rooms.
OPS.2.4	Remote Maintenance	Yes	
OPS.3.1	Outsourcing for Third Parties	No	PSAPs usually don’t deliver IT services for third parties.
DER: Detection and Reaction			
DER.1	Detecting Security-Relevant Events	Yes	
DER.2.1	Security Incident Handling	Yes	
DER.2.2	Provisions for IT Forensics	Yes	
DER.2.3	Clean-Up of Extensive Security Incidents	Yes	
DER.3.1	Audits and Revisions	Yes	
DER.3.2	Audits Based on the BSI “Guideline for IS Audits”	Yes	
DER.4	Business Continuity Management	Yes	

The following table lists the system modules. Here it is crucial whether the module is relevant to a specific component defined in Section 3.

Module		**Relevant?**	**Reason (if not relevant)**
APP: Applications			
APP.1.1	Office Products	Yes	
APP.1.2	Web Browsers	Yes	
APP.1.4	Mobile Applications (Apps)	No	For apps to alert the connected organizations or emergency apps, the respective operators and users are responsible.
APP.2.1	General Directory Service	No	Especially in smaller PSAPs, a user administration is performed purely at the level of CAD and ICCS.
APP.2.2	Active Directory	No	see APP.2.1
APP.2.3	OpenLDAP	No	see APP.2.1
APP.3.1	Web Applications	No	Own web applications are usually not required.
APP.3.2	Web servers	No	For the operation of the PSAP usually not necessary.
APP.3.3	File Servers	Yes	
APP.3.4	Samba	No	For the operation of the PSAP usually not necessary.
APP.3.6	DNS Servers	No	DNS can usually be operated as a subprocess on routers or firewalls in PSAPs.
APP.4.2	SAP ERP System	No	Usually not available in PSAPs.
APP.4.3	Relational Database Systems	Yes	Used by CAD and ICCS.
APP.4.6	SAP ABAP Programming	No	Usually not available in PSAPs.
APP.5.1	General Groupware	Yes	
APP.5.2	Microsoft Exchange and Outlook	No	Not mandatory, unless Exchange / Outlook is used. Take account to use alternative e-mail clients (for example Thunderbird, Lotus Notes, Groupwise).
SYS: IT Systems			
SYS.1.1	General Server	Yes	
SYS.1.2	Windows Server 2012	No	Not mandatory for the operation of the PSAP.
SYS.1.3	Unix Servers	No	Not mandatory for the operation of the PSAP.
SYS.1.5	Virtualisation	No	Not mandatory for the operation of the PSAP.
SYS.1.7	IBM Z-System	No	Usually not available in PSAPs.
SYS.1.8	Storage Solutions	No	For the operation of the applications in the PSAP usually not required, since storage media can be connected directly to the server.

SYS.2.1	General Client	Yes	
SYS.2.2.2	Windows 8.1 Clients	No	Use of other Windows operating systems is possible.
SYS.2.2.3	Windows 10 Clients	Yes	
SYS.2.3	Unix Clients	No	Usually not available, as CAD and ICCS clients mostly require Windows.
SYS.2.4	MacOS Clients	No	Usually not available, as CAD and ICCS clients mostly require Windows.
SYS.3.1	Laptops	No	Not required for operation of the PSAP.
SYS.3.2.1	General Smartphones and Tablets	No	Usually not available in PSAPs.
SYS.3.2.2	Mobile Device Management (MDM)	No	Not required for operation of the PSAP.
SYS.3.2.3	iOS (for Enterprise)	No	Usually not available in PSAPs.
SYS.3.2.4	Android	No	Usually not available in PSAPs.
SYS.3.3	Mobile Telephones	No	Usually not available in PSAPs.
SYS.3.4	Mobile Storage Media	Yes	
SYS.4.1	Printers, Copiers, and All-in-One Devices	Yes	
SYS.4.3	Embedded Systems	No	Usually not available in PSAPs.
SYS.4.4	General IoT Devices	No	Usually not available in PSAPs.
NET: Networks and Communication			
NET.1.1	Network Architecture and Design	Yes	
NET.1.2	Network Management	Yes	
NET.2.1	WLAN Operation	No	Not required for the operation of the PSAP, since only fixed local workplaces are used.
NET.2.2	WLAN Usage	No	see NET.2.1
NET.3.1	Router and Switches	Yes	
NET.3.2	Firewall	Yes	
NET.3.3	VPN	Yes	
NET.4.1	Telecommunications Systems	Yes	
NET.4.2	VoIP	Yes	
NET.4.3	Fax Machines and Fax Servers	Yes	
INF: Infrastructure			
INF.1	Generic Building	Yes	
INF.2	Data Centre/Server Room	Yes	
INF.3	Cabling	Yes	
INF.4	IT Cabling	Yes	
INF.6	Storage Media Archives	Yes	
INF.7	Office Workplace	Yes	

INF.8	Working from Home	No	The employees of a PSAP usually work exclusively in the offices of the PSAP.
INF.9	Mobile Workplace	No	Deviant, mobile workstations can be used in some PSAPs, e.g. in vehicles of the squad leader.
INF.10	Meeting, Event, and Training Rooms	Yes	

4.3 | GENERAL RELEVANT MODULES

In the next step, the requirements of the relevant modules are checked. If necessary, they are adapted to the framework conditions in PSAPs. Listed are basic and standard requirements. If the requirements for increased protection requirements also must be fulfilled for individual components, these are named separately.

ISMS.1 Security Management	
Requirements	ISMS.1.A1 - A15
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	A4: Depending on the size of the PSAP, the Information Security Officer may also perform other functions in a uniform manner.
	A10: When creating a safety concept, it is advisable to start with the areas of the PSAP that require the highest level of protection. Subsequently, the security concept can be supplemented with additional areas.

ORP.1 Organisation	
Requirements	ORP.1.A1 - A13
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	ORP.1.A12 If an impairment of the operation of the PSAP is unavoidable, maintenance and repair work shall, if possible, be carried out at times of the day in which fewer operations can be expected (for example at night).

ORP.2 Personnel	
Requirements	ORP.2.A1 - A10
Implementation guidelines	The requirements must be met in an appropriate way.

ORP.3 Awareness and Training	
Requirements	ORP.3.A1 - A8
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	ORP.3.A4 Training centres for fire brigade and rescue service can be included in the training and advanced training for PSAP call taker and dispatchers.

ORP.4 Identity and Access Management	
Requirements	ORP.4.A1 - A19
Implementation guidelines	The requirements must be met in an appropriate way.

ORP.5 Compliance Management	
Requirements	ORP.5.A1 - A8
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	ORP.5.A1 The personnel of the PSAP must have quick access to the documentation of the specifications.
	ORP.5.A3 In addition to the decisive points in the data protection laws (GDPR and national laws), this also includes parts of the legislation on security and the penal code for the personnel of the PSAP.

CON.1 Crypto Concept	
Requirements	CON.1.A1 - A6
Implementation guidelines	The requirements must be met in an appropriate way.

CON.2 Data Protection	
Requirements	CON.2.A1
Implementation guidelines	The requirements must be met in an appropriate way.

CON.3 Backup Concept	
Requirements	CON.3.A1 - A12
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	CON3.A.3 The rules governing the duration of storing emergency calls in the laws must be observed.
	CON.3.A12 As a geographically remote storage location a defined replacement PSAP can be determined.

CON.4 Selection and Use of Standard Software	
Requirements	CON.4.A1 - A9
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	The requirements of this module can, for example, be related to office applications, web browsers or PDF viewers. For CAD and ICCS, CON.5 should be used.

CON.5 Development and Use of Generic Applications	
Requirements	CON.5.A1 - A10
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	The requirements of this module can be referred to CAD and ICCS.

CON.6 Deleting and Destroying	
Requirements	CON.6.A1 - A8
Implementation guidelines	The requirements must be met in an appropriate way.

OPS.1.1.2 Proper IT Administration	
Requirements	OPS.1.1.2.A1 - A13
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	OPS.1.1.2.A1 Even if the activities of the administration are carried out by dispatchers in personal union, it is important to pay attention to role separation. The dispatcher should not be logged in with administration rights.

OPS.1.1.3 Patch and Change Management	
Requirements	OPS.1.1.3.A1 - A11
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	OPS.1.1.3.A7 The availability of the support should be guaranteed at and immediately after the installation of patches. An installation before weekends, holidays or appointments, which can be expected many events, should be avoided.
	OPS.1.1.3.A9 If possible, changes can first be tested on a training system before they are transferred to the production system.

OPS.1.1.4 Protection Against Malware	
Requirements	OPS.1.1.4.A1 - A9
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	OPS.1.1.4.A5 In order to avoid functional restrictions, the selection of the virus protection program should be agreed with the manufacturers of CAD and ICCS.

OPS.1.1.5 Logging	
Requirements	OPS.1.1.5.A1 - A10
Implementation guidelines	The requirements must be met in an appropriate way.

OPS.1.1.6 Software Tests and Approvals	
Requirements	OPS.1.1.6.A1 - A13
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	OPS.1.1.6.A11 The use of separate test system instances of CAD and ICCS is recommended.

OPS.1.2.2 Archiving	
Requirements	OPS.1.2.2.A1 - A19
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	OPS.1.2.2.A9 When changing the CAD, care must be taken to retain access to the events of the old system.

OPS.1.2.3 Exchange of Information and Storage Media	
Requirements	OPS.1.2.3.A1 - A12
Implementation guidelines	The requirements must be met in an appropriate way.

OPS.2.1 Outsourcing for Customers	
Requirements	OPS.2.1.A1 - A15
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	This module concerns a PSAP, for example, when outsourcing the IT administration to an external service provider.

OPS.2.4 Remote Maintenance	
Requirements	OPS.2.4.A1 - A20
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	The module is relevant if external IT service providers or manufacturers of CAD and ICCS carry out maintenance work remotely in the control center.
	OPS.2.4.A14 In order to be able to solve also problems with the Internet access, a dedicated Internet access is recommended for external remote maintenance.

DER.1 Detecting Security-Relevant Events	
Requirements	DER.1.A1 - A13
Implementation guidelines	The requirements must be met in an appropriate way.

DER.2.1 Security Incident Handling	
Requirements	DER.2.1.A1 - A18
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	DER.2.1.A6 Commissioning the replacement PSAP can be considered.

DER.2.2 Provisions for IT Forensics	
Requirements	DER.2.2.A1 - A12
Implementation guidelines	The requirements must be met in an appropriate way.

DER.2.3 Clean-Up of Extensive Security Incidents	
Requirements	DER.2.3.A1 - A8
Implementation guidelines	The requirements must be met in an appropriate way.

DER.3.1 Audits and Revisions	
Requirements	DER.3.1.A1 - A27
Implementation guidelines	The requirements must be met in an appropriate way.

DER.3.2 Audits Based on the BSI "Guideline for IS Audits"	
Requirements	DER.3.2.A1 - A22
Implementation guidelines	The requirements must be met in an appropriate way.

4.4 | RELEVANT MODULES FOR SPECIFIC OBJECTS

The following listed modules only affect the specified target objects. Usually the basic and standard requirements must be fulfilled. If the requirements for increased protection requirements are also to be fulfilled for individual components, these are named separately.

APP.1.1 Office Products	
Targets	S3
Requirements	APP.1.1.A1 - A14
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	A9: A suitable format for the distribution of documents that does not need to be processed by the recipient is, for example, the PDF format.

APP.1.2 Web Browsers	
Targets	P1.5, A3
Requirements	In addition to the basic and standard requirements, APP.1.2.A12 has to be fulfilled.
Implementation guidelines	The requirements must be met in an appropriate way.

APP.3.3 File servers	
Targets	A8, N3
Requirements	APP.3.3.A1 - A11
Implementation guidelines	The requirements must be met in an appropriate way.

APP.4.3 Relational Database Systems	
Targets	A1, A2
Requirements	APP.4.3.A1 - A20
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	APP.4.3.A10 The selection of the database system for CAD and ICCS must be made in consultation with the manufacturers.

APP.5.1 General Groupware	
Targets	A4, N3
Requirements	APP.5.1.A1 - A19
Implementation guidelines	The requirements must be met in an appropriate way.

SYS.1.1 General Server	
Targets	S1.2, S2.1
Requirements	SYS.1.1.A1 - A25
Implementation guidelines	The requirements must be met in an appropriate way.

SYS.2.1 General Client	
Targets	S1.1, S3
Requirements	SYS.2.1.A1 - A27
Implementation guidelines	The requirements must be met in an appropriate way.

SYS.2.2.3 Windows 10 Clients	
Targets	S1.1
Requirements	SYS.2.2.3.A1 - A20
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	SYS.2.2.3.A4 These connections can be blocked, for example, in the firewall.

SYS.3.4 Mobile Storage Media	
Targets	P5.1
Requirements	SYS.3.4.A1 - A7
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	SYS.3.4.A4 By using a data lock with anti-virus software, security can be increased.

SYS.4.1 Printers, Copiers, and All-in-One Devices	
Targets	P4.1, P4.2, P5.1
Requirements	SYS.4.1.A1 - A19
Implementation guidelines	The requirements must be met in an appropriate way.

NET.1.1 Network Architecture and Design	
Targets	N1, N2, N3, N4, N6
Requirements	NET.1.1.A1 - A27
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	NET.1.1.A23 The separation of CAD, ICCS and office network increases the security level.

NET.1.2 Network Management	
Targets	N1, N2, N3, N4
Requirements	NET.1.2.A1 - A29
Implementation guidelines	The requirements must be met in an appropriate way.

NET.3.1 Router and Switches	
Targets	N1, N2, N3, N4, N5
Requirements	NET.3.1.A1 - A23
Implementation guidelines	The requirements must be met in an appropriate way.

NET.3.2 Firewall	
Targets	N1, N2, N3, N4, N5
Requirements	NET.3.2.A1 - A24
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	NET.3.2.A15 If the network is segmented by two firewalls, it is important to procure the firewalls from different manufacturers. This reduces the chances of an attacker exploiting the same vulnerability in both products.

NET.3.3 VPN	
Targets	N1
Requirements	NET.3.3.A1 - A13
Implementation guidelines	The requirements must be met in an appropriate way.

NET.4.1 Telecommunications Systems	
Targets	A2
Requirements	NET.4.1.A1 - A16
Implementation guidelines	The requirements must be met in an appropriate way.

NET.4.2 VoIP	
Targets	A2, N2
Requirements	NET.4.2.A1 - A13
Implementation guidelines	The requirements must be met in an appropriate way.
Hints	NET.4.2.A1 Compliance with the technical guidelines of the country must be taken into account when planning the use of VoIP.

NET.4.3 Fax Machines and Fax Servers	
Targets	S4
Requirements	NET.4.3.A1 - A10
Implementation guidelines	The requirements must be met in an appropriate way.

INF.1 Generic Building	
Targets	R1, R2, R3, R4, R5, R6
Requirements	INF.1.A1 - A20
Implementation guidelines	The requirements must be met in an appropriate way.

INF.2 Data Centre/Server Room	
Targets	R2
Requirements	INF.2.A1 - A20
Implementation guidelines	The requirements must be met in an appropriate way.

INF.3 Cabling	
Targets	R1, R2, R3, R4, R6
Requirements	INF.3.A1 - A12
Implementation guidelines	The requirements must be met in an appropriate way.

INF.4 IT Cabling	
Targets	N6
Requirements	INF.4.A1 - A11
Implementation guidelines	The requirements must be met in an appropriate way.

INF.6 Storage Media Archives	
Targets	R2, R3, R5
Requirements	INF.6.A1 - A8
Implementation guidelines	The requirements must be met in an appropriate way.

INF.7 Office Workplace	
Targets	R1, R3
Requirements	INF.7.A1 - A7
Implementation guidelines	The requirements must be met in an appropriate way.

INF.10 Meeting, Event, and Training Rooms	
Targets	R6
Requirements	INF.10.A1 - A8
Implementation guidelines	The requirements must be met in an appropriate way.

There are objects that cannot be adequately modelled using the existing modules of IT-Grundschutz. These must be considered separately.

The connection to the ISP (N4) has a very high protection requirement in all three protection goals. The PSAP has no influence on the achieved security level of the ISP.

There is no module for the alarm network N7 which suitably maps the requirements for the protection requirement of this component. Since this network has a very high protection requirement in all three protection objectives, the risks must also be considered separately.

5 | DIRECTIONS FOR USE

The identified requirements must be integrated into the overall safety concept and implemented over the course of the planned realization.

The BSI recommends carrying out the requirements of the blocks in a defined order. This ensures that the basic risks are covered early. The following modules should be implemented first:

- ISMS security management
- ORP.1 to ORP.4 from ORP organisation and personnel
- CON.3 and CON.6 from CON concepts and procedures
- All modules from OPS.1.1 core IT operation

6 | SUPPORTING INFORMATION

More detailed information on the individual requirements can be found in the implementation notes of the individual modules of *IT-Grundschutz*.

Another helpful document is the *EENA Guidelines and Best Practices for Emergency Services*.