

IT-Grundschatz profile for  
the operation of UAS  
Volume 1: UAS  
operating category "Open"

## Content

Content.....	2
1. Introduction .....	4
1.1 Formal aspects.....	5
1.2 Disclaimer .....	5
2. Management Summary .....	6
2.1. Target group .....	6
2.2. Objective.....	6
2.3. Tasks of the management level.....	6
3. Definition of the scope of application .....	7
4. Delimitation of the information network .....	8
4.1. Components of the information network .....	8
4.2. Objects not included.....	8
5. Reference architecture .....	9
5.1. Business processes and applications.....	9
5.2. IT-Systems.....	11
5.3. Networks and network components.....	11
5.4. Infrastructure: Rooms and buildings .....	11
5.5. Infrastructure: Vehicles .....	12
5.6. Dealing with deviations .....	12
5.7. Components in relation to the target objects in the information network.....	13
6. Determining the need for protection .....	15
6.1. Risk assessment .....	17
6.2. Preparation of the risk analysis .....	18
7. Requirements to be met and measures to be implemented .....	19
7.1. Selection of process modules.....	19
7.2. Selection of system modules.....	22
7.3. Access controls .....	24
8. Residual risk assessment.....	25
9. Application notes .....	26
10. Supporting information.....	27

Appendix 1 - Building blocks/system components .....	28
Appendix 2 - Elementary hazards.....	29
Appendix 3 - Definitions of terms .....	31
Appendix 4 - Abbreviations .....	32

# 1. Introduction

In addition to flight safety requirements, the operation of unmanned aircraft systems (UAS) also places demands on information security. As flying computer networks, they are in need of protection because corrupted firmware updates, a failure of the communication infrastructure or manipulated databases can cause the vehicle to misbehave, making it a danger to people and the environment. The protection of data and secure communication with the company's internal network therefore require a closer look at information security. Information security in UAS must be considered from two perspectives: firstly, from the perspective of the UAS as a participant in air traffic and secondly, from the perspective of the mobile end device and data storage device.

In principle, this IT-Grundschutz<sup>1</sup> profile is intended to relieve those involved of this burden and clarify the important questions regarding information security when operating UAS using a reference architecture. In particular, the following questions should be addressed: How can suitable information security measures be taken to prevent interference with safe flight operations? How can risks to a connected network be averted? Data protection aspects, such as data collection for the operation of the drone and the processing of image data from the air in compliance with data protection regulations, are subject to the relevant legal provisions and are not covered by the basic IT protection profile.

There are many reasons to deal with information security when operating UAS. The most important is probably to avoid personal injury and damage to property due to inadequate information security. This IT-Grundschutz profile is suitable for transferring processes that have been established for the conventional IT landscape to the operation of UAS. Where this is not possible, individual modules have been developed. The IT-Grundschutz profile can also serve as an element for a risk analysis for submission to aviation authorities.

---

<sup>1</sup> The term "IT-Grundschutz" represents the basis for information security by recommending practical methods for appropriately protecting information in general. The combination of the IT-Grundschutz methodologies for basic, core and standard safeguards and the IT-Grundschutz Compendium outlines security requirements for establishing an information security management system (ISMS) in different operational environments, which ultimately facilitates the secure handling of information. IT-Grundschutz can be used by small and medium-sized companies (SME) as well as large organisations to establish a management system for information security. However, successful implementation of the IT-Grundschutz Profile requires that an organisational unit (IT operations) is established to set up, operate, monitor and maintain internal IT. The objective of IT-Grundschutz is to enable organisations to attain an adequate level of protection for all their information. The IT-Grundschutz Methodology is characterised by a holistic approach. By implementing a suitable combination of standard organisational, personnel-related, infrastructural, and technical security requirements, it is possible to attain a security level that is adequate for the relevant protection needs and appropriate for protecting information relevant to the organization.

## 1.1 Formal aspects

Aspekt	Beschreibung
<b>Title</b>	IT-Grundschutz profile for the operation of UAS Volume 1: UAS operating category "open"
<b>Authorship</b>	Jens Fehler (Mediator Consult) Kai Lothar John (GLVI) Marco Müller-ter Jung, LL.M. (Grant Thornton Rechtsanwaltsge- sellschaft mbH) Harald Rossol (b.r.m. IT & Aerospace) Markus Rossol (b.r.m. IT & Aerospace) Corinna Schmitt (University of the Federal Armed Forces Munich) Burkhard Wrenger (TH OWL)
<b>Publisher</b>	UAV DACH e.V.
<b>Version</b>	1.1
<b>Revision cycle</b>	After the release of version 1.0, a biennial review is planned.
<b>Confidentiality</b>	This document may be distributed in unmodified form.

Table 1: Overview of formal aspects

## 1.2 Disclaimer

This document has been prepared with the utmost care but makes no claim to completeness or accuracy. The authors have no influence on the use of this IT-Grundschutz profile by users and are also not aware of the individual requirements for their security concepts, so that they naturally cannot assume any liability for the effects on the legal position of the parties.

## 2. Management Summary

### 2.1. Target group

This IT-Grundschutz profile is aimed at all organizations, authorities and companies in which UAS are used as part of the "open" operating category. It is intended in particular for those responsible in management and IT administration, as well as those specialist departments in which UAS are used.

### 2.2. Objective

The IT-Grundschutz profile defines requirements in terms of IT-Grundschutz in order to secure the confidentiality, integrity and availability of the processed data. The operation of UAS is exemplified by the processes

- GP1: Flight operations with the sub-processes
  - Launch preparations,
  - Start,
  - Flight,
  - Landing,
  - Decommissioning.
- GP2: Maintenance and repair with the sub-processes
  - Replacing or updating the mechanical drive components,
  - Updating the flight operations software,
  - Update of all other software components according to the manufacturer's specifications,
  - Analysis of the system files (log files).

### 2.3. Tasks of the management level

The application of this IT-Grundschutz profile in the context of flight operations with UAS is part of a safety concept and can serve as an element of the approval or authorization of aviation operations in accordance with the relevant guidelines and regulations.

The authors recommend that organizations wishing to make use of UAS services use this IT-Grundschutz profile as a basis for commissioning appropriate service providers. The requirements formulated here should be included in the terms of contract.

### 3. Definition of the scope of application

The requirements listed in this IT-Grundschutz profile are recommendations from UAV DACH e.V. for UAS operators. They cover the requirements of the "standard protection" of BSI Standard 200-2.

The implementation of standard security is compliant with ISO 27001.

The requirements set out in this IT-Grundschutz profile also take into account parts of the provisions of the GDPR, the BDSG, the TTDSG, the TMG, in particular Section 13 TMG, and for U-Space service providers also Annex III of Implementing Regulation 2021/664 for U- Space.

It should be noted that at the time of publication of this IT-Grundschutz profile, all EU cybersecurity certificates from ENISA (see Art. 8, 48 ff of Regulation EU 2019/881 (Cybersecurity Act)) are still under construction. This IT-Grundschutz profile is therefore designed for self-implementation and, if the certificates are available, for a self-assessment of conformity by the manufacturer or user of the UAS. Therefore, within the framework of the trustworthiness classification according to the European schemes<sup>2</sup> of ENISA pursuant to Art. 53 of the Cybersecurity Act, it would be possible to achieve at most the trustworthiness level "low". For the further levels "medium" and "high", however, audits by accredited independent third parties would be required.

---

<sup>2</sup> Drones are likely to be classified as an ICT product under Art. 2 No. 12 of the Cybersecurity Act, but in any case - depending on the design of the drone - the installed components (video and photo camera, microphones, network connection to U-space service providers, etc.). The scheme "Cybersecurity Certification: EUCC Scheme V1.1.1" (under construction), which deals with ICT products, must be observed. Furthermore, the scheme "EUCC - Cloud Services Scheme" may have to be observed if U-Space service providers are to be regarded as cloud service providers within the meaning of Art. 2 No. 13 Cybersecurity Act.

## 4. Delimitation of the information network

### 4.1.Components of the information network

The information network includes all components and procedures at a UAS operator that are necessary for flight operations, including maintenance and repair (see reference architecture, see section 5.).

### 4.2.Objects not included

Components that are not directly related to flight operations and procedures that go beyond flight operations, such as order processing, invoicing, etc., are not taken into account.

Users of UAS services should use this IT-Grundschutz profile as a basis for selecting appropriate service providers. The requirements formulated here should be included in the contractual conditions.



## 5. Reference architecture

The information network considered by the IT-Grundschatz profile contains all the key mobile and stationary objects of the Unmanned Aircraft System (UAS) that are essential for operation in the context of the business processes described below. A schematic representation of the information network can be found in Figure 1<sup>3</sup>.

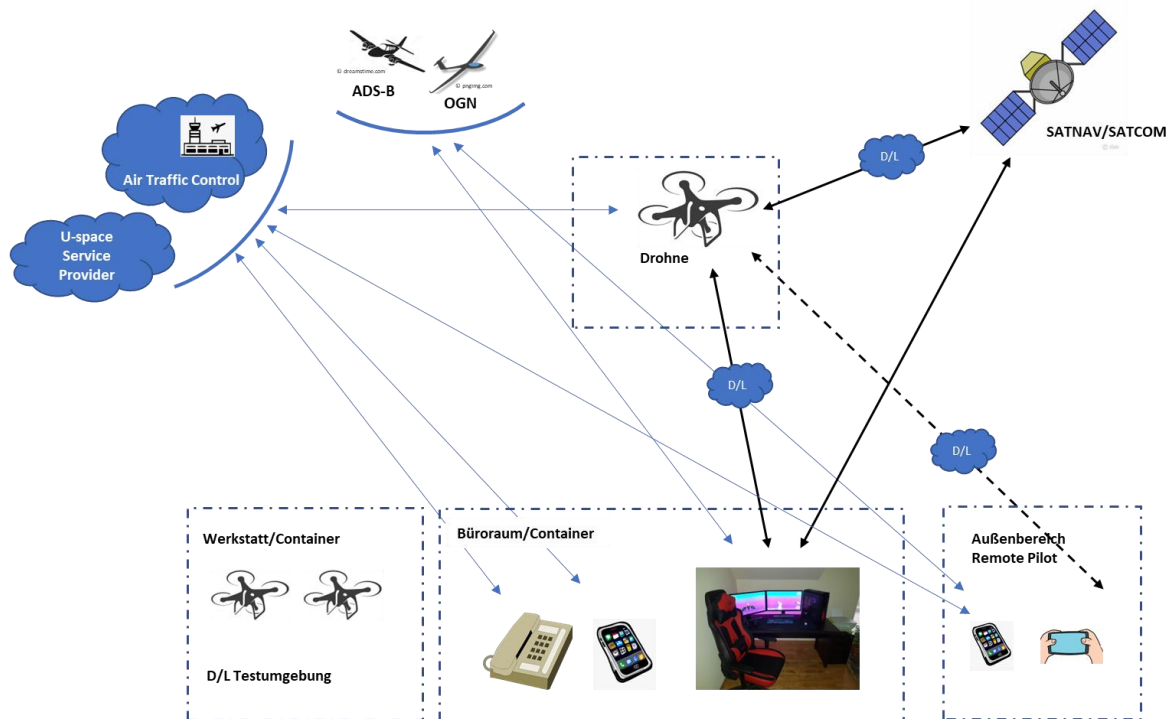


Figure 1: Schematic representation of the reference architecture.

The need for protection relates to the elements and components shown, in particular buildings and rooms, computer networks and communication, IT systems and business processes/applications. Communication takes place between different end devices, such as desktop computers, laptops, tablets and control computers. Different communication methods are used for this. The security requirements must be checked individually by each institution.

### 5.1. Business processes and applications

The IT-Grundschatz profile under consideration relates to the business processes

- GP1: Flight operations
- GP2: Maintenance and repair

These business processes are examples of different sub-aspects and protection goals and can be replaced by the organization's specific business processes.

<sup>3</sup> The current version of the graphic can be obtained via the following link: [https://uavdach.sharepoint.com/:p/r/teams/FGIT-Sicherheit/Freigegebene Dokumente/IT-Grundschatzprofil/20220301-Drohnen-IT-GSProfil\\_v2.pptx?d=w397d4f3e1d334cda915ed31e179d116c&csf=1&web=1&e=LWo-NAC](https://uavdach.sharepoint.com/:p/r/teams/FGIT-Sicherheit/Freigegebene%20Dokumente/IT-Grundschatzprofil/20220301-Drohnen-IT-GSProfil_v2.pptx?d=w397d4f3e1d334cda915ed31e179d116c&csf=1&web=1&e=LWo-NAC)

GP1 includes the commissioning of the UAS, its take-off, flight, landing and subsequent de-commissioning, as well as activities directly associated with the flight, such as flight preparation.

For GP1, therefore, the setup of the UAS at or near the launch site, the mechanical, electrical and electronic tests and self-tests to be carried out before the launch and the communication link between the subcomponents of the UAS must be taken into account. After take-off, further tests of the UAS and its payload, the automatic or manual monitoring of the flight corridor and the system status as well as the flight progress must be taken into account. After landing, further (self-) tests, documentation and backup of the flight data as well as further mechanical and electronic tests are carried out. Payload data may also need to be backed up.

GP2 contains all maintenance and repair work that must be carried out in order to maintain operational safety. GP2 includes all sub-processes that must be carried out between flights of the UAS in order to maintain operational safety. This includes checking and, if necessary, repairing, replacing information-processing components, updating the flight operations software, e.g. the firmware or system software of the central control computer in the UAS, and updating all other software components in accordance with the manufacturer's specifications. Some of these tasks must be carried out after or before each flight, while others are subject to specific manufacturer specifications.

In addition to the GP1 and GP2 business processes, the information network includes other applications that support the tasks to be performed. The following table provides an overview of the typical applications of the information network.

Abbreviation	Name of the software
A01	Flight planning software
A02	Map software
A03	Maintenance software
A04	Flight-Control-Software
A05	Ground-Control-Software
A06	Flight-Data-Recorder <sup>4</sup>
A07	Payload control
A08	Control of additional tasks
A09	Configuration-management-software

*Table 2: Typical applications in the information network*

---

<sup>4</sup> The flight data recorder is a technical component of the drone and, in terms of the IT-Grundschatz profile, represents a variable that is beyond the control of the user. The measures for IT-Grundschatz are the responsibility of the respective drone manufacturer.

## 5.2.IT-Systems

In addition to the business processes and applications, the IT systems must also be considered in the information network.

The following table provides an overview of the typical IT systems in the information network:

Abbreviation	Name of the IT system
C01	Desktop computer
C02	Laptop
C03	Tablet or smartphone
S01	Server
D01	Flight-controller
D02	Companion-computer

Table 3: Typical IT systems in the information network

## 5.3.Networks and network components

The information network is characterized by heterogeneous networks. In addition to wired networks, radio networks such as WLAN/IEEE 802.11 for local communication, mobile radio standards, IEEE 802.15.4 and specific long-range and satellite communication links are used for communication between the drone in the air and the controlling ground station. In detail, these are usually the data connection between the drone and the ground control station (telemetry and telecommand), connections between the drone and other aircraft (ADS-B, OGN) and/or connections between the ground control station and other air traffic participants (USSP, ANSP, etc.).

The following table provides an overview of the typical network components in the information network:

Abbreviation	Name of the network component
NET01	Active components Wired organizational network
NET02	Active components wireless organization network
NET03	Interface between organizational and data network
NET04	On-board network of the drone
NET05	Active components of the drone to ground control station connection

Table 4: Typical network components in the information network

## 5.4.Infrastructure: Rooms and buildings

Components of the information network can be housed in a building, in a vehicle (see section 5.5 below), outside buildings or vehicles and in the drone. These infrastructure components

may need to be treated differently from an information security perspective. For this reason, a distinction is made here and in the next subsection between mobile and stationary infrastructure objects.

The following table provides an overview of the typical stationary infrastructure components in the information network:

Abbreviation	Name of the room or building
R01	General room, access-controlled
R02	Control station/ground control station
R03	Hall, workshop area
R04	Laboratory
R05	Server room
R06	Outdoor area, access-controlled
R07	Flight test and demonstration area
R08	Public space

*Table 5: Typical infrastructure components in the information network*

## 5.5. Infrastructure: Vehicles

UAS are not usually operated at the UAS operator's headquarters. As a rule, the transportation of UAS must therefore be taken into account.

The following table provides an overview of the typical mobile infrastructure components in the information network:

Abbreviation	Name of the mobile infrastructure component
F01	Transport vehicle for UA or UAS
F02	Operation Vehicle
UA01	Unmanned Aircraft/Drone

*Table 6: Typical mobile infrastructure components in the information network*

In many cases, F01 and F02 are identical, i.e. transportation and operational support take place in one vehicle.

## 5.6. Dealing with deviations

If the information network to be protected deviates from the reference architecture described in this chapter, the additional target objects must be documented as part of the structural analysis. Suitable components of the IT-Grundschutz compendium must be assigned to these target objects.

Target objects from this IT-Grundschutz profile that do not occur in the information network to be protected do not need to be taken into account.

### 5.7.Components in relation to the target objects in the information network

The following table assigns the components to the target objects in the information network. This relationship provides the framework for selecting the relevant building blocks for the respective organization applying the IT-Grundschutz profile:

Component	To be applied to target object
A01 Flight planning software	GP1
A02 Card software	GP1
A03 Maintenance software	GP2
A04 Flight control software	GP1
A05 Ground control software	GP1
A06 Flight-Data-Recorder	GP1
A07 Payload-control	GP1
A08 Control of additional tasks	GP1
A09 Configuration management software	GP2
C01 Desktop computer	A01, A03, A05, A07, A08, A09
C02 Laptop	A01, A03, A05, A07, A08, A09
C03 Tablet	A01, A03, A05, A07, A08, A09
S01 Server	A02
D01 Flight-Controller	A04
D02 Companion-Computer	A07, A08
NET01 Wired network	C01, C02, S01
NET02 Wireless network	C01, C02, C03
NET03 Interfaces Nw/Dat.	C01, C02, C03, S01, D01, D02
NET04 On-board network	D01, D02
NET05 Drone ground control station	C01, C02, C03, D01, D02
R01 General room, access-controlled	C01, C02, C03, NET01, NET03
R02 Control station/ground control station	C01, C02, C03
R03 Hall, workshop area	C01, C02, C03, D01, D02
R04 Laboratory	C01, C02, C03, D01, D02
R05 Server room	S01
R06 Outdoor area, access-controlled	C02, C03, D01, D02
R07 Flight test and demonstration area	C02, C03, D01, D02
R08 Public space	C02, C03, D01, D02
F01 Transport vehicle	D01, D02
F02 Operation Vehicle	C01, C02, C03, S01
UA01 Unmanned Aircraft	D01, D02

*Tabelle 7: Modules to be applied*

## 6. Determining the need for protection

The protection requirements for the processes, applications, IT and communication systems and infrastructure components identified as part of the structural analysis must first be determined. The basis for this is the impact that violations of the basic values of information security (confidentiality, integrity and availability) would have. Suitable contacts for determining protection requirements are, for example, the respective process owners or the data owner of the data processed in the respective process. The need for protection generally depends on the scope of all data processed in the processes. The procedure for determining the need for protection is described in detail in BSI Standard 200-2 (see section 8.2). The BSI baseline protection specifies various scenarios to which damage can relate. These are listed in the following table:

Identifier	Damage scenario
SZ1	Violations of laws, regulations or contracts
SZ2	Impairment of the informal right to self-determination
SZ3	Impairment of personal integrity
SZ4	Impairment of the fulfillment of tasks
SZ5	Negative internal or external impact
SZ6	Financial impact

*Table 8: Potential damage scenarios*

The specific effects and possible damage scenarios can vary depending on the application. The following table lists possible examples of damage scenarios:

Identifier	Examples of damage scenarios
SZ1	Altered or incomplete data can lead to violations of laws and regulations (e.g. flight within an unauthorized flight area) or to violations of contracts with business partners (e.g. video recording not in the agreed flight area).
SZ2	<p>Personal data of employees or business partners or sensitive company data becomes accessible to the public or unauthorized third parties without authorization.</p> <p>Company-critical or confidential data becomes accessible to the public or unauthorized third parties without authorization. This can lead to financial disadvantages.</p>
SZ3	Incomplete or faulty data transmission or the transmission of maliciously modified data leads to incorrect control of the UAS, incorrect decisions in the process sequence (flight operations or maintenance/repair) and, as a result, to accidents with personal injury.
SZ4	<p>Incomplete or maliciously modified data transmission leads to an interruption of flight operations (GP1), video recording (GP1) or faulty maintenance or repair of the UAS (GP2) and thus to restricted or failed task fulfillment.</p> <p>If part of the information network is not available or only available to a limited extent, flight operations will be aborted or video recording will be terminated, thus limiting the fulfillment of tasks.</p>
SZ5	<p>Restricted or aborted flight operations (GP1) or incomplete video recording (GP1) lead to damage to the company's image and loss of trust.</p> <p>Incomplete or faulty maintenance and repair leads to damage to the company's image and loss of trust.</p>
SZ6	<p>An incomplete flight operation (GP1) or an incomplete video recording (GP1) leads to service or process failures or costs for the re-execution of the process.</p> <p>Incorrect flight operation resulting in damage leads to additional costs. Incorrect or incomplete maintenance and repairs lead to additional material and personnel costs.</p>

Table 9: Examples of damage scenarios

The impact of damage cannot be determined in advance. For this reason, the BSI's IT- Grundschutz methodology recommends classification into three categories - normal, high and very high - in connection with the determination of protection requirements. The following table lists the categories, supplemented by the generic damage effects. The effects can relate to components, the company or affected third parties:



Category	Effect of damage
normal	The impact of the damage is limited and manageable.
high	The effects of damage can be considerable.
Very high	The effects of damage can be life-threatening or even life-threatening.

*Table 10: Examples of the NB for protection requirement categories*

If considerable, life-threatening or life-threatening effects are identified in a damage scenario, the affected basic value is classified as high or very high in the protection requirement, in all other cases as normal. The protection requirement determined for each basic value is then passed on to the application layer, followed by further steps for the IT systems, networks, premises and infrastructure objects.

The user must determine the specific protection requirements on a case-by-case basis using the IT-Grundschutz profile.

## 6.1. Risk assessment

Even if all requirements are implemented, one hundred percent security cannot be achieved. Both the users of the IT-Grundschutz profile and the decision-makers must be aware of this. Due to the special features of flight operations with drones, a risk analysis must always be carried out.

There are no suitable modules in the IT-Grundschutz compendium, particularly for the target objects UAS/drone and possibly the ground control station, meaning that a risk analysis is absolutely necessary until further notice. The risk analysis procedure in accordance with BSI Standard 200-3 is recommended. This BSI standard already lists 47 elementary hazards, which are explained in more detail in the IT baseline protection compendium. These hazards should be the starting point for creating the hazard overview and should be supplemented as necessary.

The following steps are carried out as part of the risk analysis:

- create a hazard overview,
- carry out a risk assessment,
- determine the risk treatment,
- Consolidation of the extended security measures with the results of the IT-Grundschutz check.

This ensures that higher-value security measures defined as part of the risk analysis are also applied to objects with normal protection requirements, if this makes sense. It should be noted that aspects of flight safety are considered separately as part of flight safety management. They are therefore not part of this IT-Grundschutz profile.

## 6.2.Preparation of the risk analysis

The table associated with this profile serves as the basis for preparing the risk analysis and determining the risk potential of the applications for which this IT-Grundschutz profile is used. Risk matrix. The table can be obtained as an additional file from the BSI website, right next to this profile.

## 7. Requirements to be met and measures to be implemented

The BSI's IT-Grundschutz compendium provides process and system modules that specify application-related requirements for the implementation of IT-Grundschutz.

### 7.1. Selection of process modules

The overarching process modules must be applied to every information network. These deal with security aspects that apply equally to large parts of the information network.

#### **ISMS: Security management**

ID	Building block	relevant	Reason (if not relevant)
ISMS.1	Security management	Yes	

Table 11: ISMS layer

#### **ORP: Organisation and personnel**

ID	Building block	relevant	Reason (if not relevant)
ORP.1	Organization	Yes	
ORP.2	Personnel	Yes	
ORP.3	Raising awareness and training on information security	Yes	
ORP.4	Identity and Authorization management	Yes	
ORP.5	Compliance management	Yes	

Table 12: ORP layer

**CON: Concept and procedure**

ID	Building block	relevant	Reason (if not relevant)
CON.1	Crypto concept	Yes	Defined by CE procedures as part of the procurement of drones. Not subject to the influence of the user.
CON.2	Data protection	Yes	
CON.3	Data backup concept	Yes	
CON.4	(omitted)		(intentionally left blank)
CON.5	(omitted)		(intentionally left blank)
CON.6	Delete and destroy	Yes	Defined by the manufacturer as part of the CE procedure. Not subject to the influence of the user.
CON.7	Information security when traveling abroad	No	Not within the scope; conceptually irrelevant
CON.8	Software development	No	No software development in the information network
CON.9	Exchange of information	ja	
CON.10	Development of web applications	No	No development of web applications in the information society

*Table 13: CON layer*

## **OPS: Operation**

<b>ID</b>	<b>Building block</b>	<b>relevant</b>	<b>Reason (if not relevant)</b>
OPS.1.1.1	General IT operations	Yes	Fulfillment of basic requirements, i.e. definition of roles and authorizations as well as definition of tasks and responsibilities, otherwise depending on relevance for drone operation.
OPS.1.1.2	Ordnungsgemäße IT-Administration	Yes	
OPS.1.1.3	Patch- und Änderungsmanagement	Yes	
OPS.1.1.4	Schutz vor Schadprogrammen	Yes	
OPS.1.1.5	Protokollierung	Yes	
OPS.1.1.6	Software-Tests und Freigaben	Yes	Limited according to manufacturer's specifications
OPS.1.1.7	Systemmanagement	Yes	
OPS.1.2.1			(intentionally left blank)
OPS.1.2.2	Archivierung	Yes	
OPS.1.2.3			(intentionally left blank)
OPS.1.2.4	Telearbeit	No	not applicable
OPS.1.2.5	Fernwartung	Yes	Restricted according to manufacturer's specifications
OPS.1.2.6	NTP-Zeitsynchronisation	Yes	
OPS.2.1	Outsourcing für Kunden	No	Not considered here, conceptually irrelevant
OPS.2.2	Cloud-Nutzung	Yes	(depending on configuration)
OPS.3.1	Outsourcing für Dienstleister	Yes	(depending on the application scenario)

Table 14: OPS layer

### **DER: Detection and reaction**

ID	Building block	relevant	Reason (if not relevant)
DER.1	Detection of safety-relevant events	Yes	
DER.2.1	Handling of security incidents	Yes	
DER.2.2	Provision for IT forensics	Yes	Aviation safety/accident investigation
DER.2.3	Cleaning up far-reaching Security incidents	Yes	
DER.3.1	Audits and reviews	Yes	Recommendation: continuous improvement process Implement with the drone user
DER.3.2	Revision on the basis of the IS revision guidelines	No	Only prescribed for federal authorities
DER.4	Business Continuity Management	Yes	In conjunction with manufacturer

*Tabelle 15: DER-layer*

## 7.2. Selection of system modules

The system modules are listed in the following tables. The decisive factor here is whether the respective module is relevant for a specific component of the information network under consideration here. It should be noted that system components of the INF layer in the Open category (UAS Open) are generally not part of the information network of this IT- Grundschatz profile.

**APP: Applications**

ID	Building block	Target objects	relevant	Reason (if not relevant)
APP.1.1	Office products		No	not part of the information network
APP.1.2	Web-browser	C01, C02, C03, S01	Yes (if applicable)	
APP.1.4	Mobile Applications		Yes (if applicable)	
APP.2.1	General directory service		Yes (if applicable)	
APP.3.1	Web applications		Yes (if applicable)	
APP.3.2	Webserver		Yes	
APP.3.3	File server	C01, C02, C03	Yes	
APP.3.4	DNS server		No	not part of the information network
APP.4.2	SAP-ERP system		No	not part of the information network
APP.4.3	Relational database system		No	not part of the information network
APP.4.6	SAP-ABAP-programming		No	not part of the information network
APP.5.2	Microsoft Exchange and Outlook		No	not part of the information network
APP.5.3	General e-mail client and server		No	not part of the information network
APP.6	General software		Yes	
APP.7	Development of customized software		No	There is no development of software in the information network.

Table 16: APP layer

## **SYS: IT Systems**

ID	Building block	Target objects	relevant	Reason (if not relevant)
SYS.1.1	General server	S01	Yes	
SYS.2.1	General Client	C01	Yes	
SYS.3.1	Laptops	C02, C03	Yes	
SYS.4.3	Embedded systems	D01, D02	Yes	
SYS.4.4	General IoT device			

*Table 17: SYS layer*

The building blocks of the **IND: Industrial IT**, **NET: Networks and Communication** and **INF: Infrastructure layers** are not currently considered in this profile. They must be considered and modeled individually by the users as part of the security process.

### **7.3.Access controls**

Data may be subject to regulations, so it must be ensured that access is appropriately limited and can be documented. At the same time, easy maintenance should be made possible. The models often implemented here are IBAC, RBAC and ABAC or hybrid variants of these 3 models.



## 8. Residual risk assessment

Flight operations with unmanned aerial vehicles in the open category do not currently require a general residual risk assessment if the principles of this IT-Grundsatz profile are adhered to.

## 9. Application notes

The identified requirements must be integrated into the overall security concept and implemented. The PDCA cycle (Plan, Do, Check, Act), i.e. a recurring process of planning, implementation, review and adjustment, has proven its worth in order to continuously maintain the desired level of security.

## 10. Supporting information

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

Specific information on implementing the requirements of Section 13 TMG can be found in the BSI publication "Absicherung von Telemediendiensten nach Stand der Technik".

In addition, the relevant national and international regulations and rules for flight operations with unmanned aircraft apply.

## Appendix 1 - Building blocks/system components

Abbreviation	Designation
A01	Flight planning software
A02	Card software
A03	Maintenance software
A04	Flight control software
A05	Ground control software
A06	Logbook/Flight Data Recorder
A07	Payload control
A08	Control of additional tasks
A09	Configuration management software
C01	Desktop computer
C02	Laptop
C03	Tablet
S01	Server
D01	Flight controller of the UA
D02	Companion computer
NET01	Active components Wired company network
NET02	Active components wireless company network
NET03	Interface between company and data network
NET04	OnBoard network of the UA
R01	Access-controlled room (Access controls are specific to the institution and the risk situation and must be adapted individually. Ideally, all rooms and areas should be access-controlled).
R02	Control station (ground control station)
R03	Hall, workshop area
R04	Laboratory
R05	Server room
R06	Outdoor area, access-controlled
R07	Flight test and demonstration area
R08	Public space
F01	Transport vehicle for UA or UAS
F02	Operation Vehicle
UA01	Unmanned Aircraft/Drone

Table 18: Modules/system components

## Appendix 2 - Elementary hazards

Abbreviation	Designation
G 0.1	Fire
G 0.2	Unfavorable climatic conditions
G 0.3	Water
G 0.4	Contamination Dust Corrosion
G 0.5	Natural disasters
G 0.6	Disasters in the surrounding area
G 0.7	Major events in the surrounding area
G 0.8	Failure or malfunction of the power supply
G 0.9	Failure or disruption of communication networks
G 0.10	Failure or disruption of supply networks
G 0.11	Failure or disruption of service providers
G 0.12	Electromagnetic interference radiation
G 0.13	Interception of compromising radiation
G 0.14	Spying on information (espionage)
G 0.15	Eavesdropping
G 0.16	Theft of devices, data carriers or documents
G 0.17	Loss of devices, data carriers and documents
G 0.18	Planning errors or lack of adaptation
G 0.19	Disclosure of sensitive information
G 0.20	Information or products from an unreliable source
G 0.21	Manipulation of hardware and software
G 0.22	Manipulation of information
G 0.23	Unauthorized intrusion into IT systems
G 0.24	Destruction of devices or data carriers
G 0.25	Failure of devices or systems
G 0.26	Malfunction of devices or systems
G 0.27	Lack of resources
G 0.28	Software vulnerabilities or errors
G 0.29	Violation of laws or regulations
G 0.30	Unauthorized use or administration of devices and systems
G 0.31	Incorrect use or administration of devices and systems
G 0.32	Misuse of authorizations

G 0.33	Staff absence
G 0.34	Assault
G 0.35	Coercion, extortion or corruption
G 0.36	Identity theft
G 0.37	Denial of actions
G 0.38	Misuse of personal data
G 0.39	Malicious programs
G 0.40	Prevention of services (denial of service)
G 0.41	Sabotage
G 0.42	Social engineering
G 0.43	Importing messages
G 0.44	Unauthorized entry into premises
G 0.45	Data loss
G 0.46	Loss of integrity of sensitive information
G 0.47	Harmful side effects of IT-based attacks

*Table 19: Elementary hazards*

## Appendix 3 - Definitions of terms

Term	Definition
Information security	Comprehensive term for all elements related to the collection, use and storage of data, including information technology.
Basic protection	A state that achieves a level of security through a suitable combination of organizational, personnel, infrastructural and technical security requirements that is appropriate and sufficient for the respective protection requirements in order to protect institution-relevant information. BSI-IT Grundschutz compendium Chapter 1.2).
Increased protection requirements	The protection requirement describes the level of protection that is sufficient and appropriate for the business processes, the information processed and the information technology used. Scenario-related peculiarities may arise that require a specific risk analysis irrespective of the protection requirement category and may result in selective or temporary measures.
Risk analysis	Name of the complete process to assess (identify, assess and evaluate) and treat risks. (BSI-IT-Grundschutz Glossary).
Organization network	The IT and communication network of the respective aviation company.
Data network	Digital storage services outside the organizational network, e.g. cloud.
Unmanned Aircraft Systems	In this IT-Grundschutz profile, the internationally standardized generic term is used uniformly. It includes all system designations and subcategories that denote unmanned aerial systems, such as drone, Remotely Piloted Aircraft System (RPAS), etc. In this context, the term Unmanned Aircraft (UA) refers to the flying element of the system. The term Unmanned Aerial Vehicle (UAV) is outdated and should no longer be used.

Table 20: Definitions of terms

## Appendix 4 - Abbreviations

Abbreviation	Term
ABAC	Attribute Based Access Control
ADS-B	Automatic Dependent Surveillance - Broadcast
ANSP	Air Navigation Service Provider
BDSG	Bundesdatenschutzgesetz (Federal Data Protection Act)
DNS	Domain Name System
GDPR	General Data Protection Regulation
GP	Geschäftsprozess (Business process)
IBAC	Identity Based Access Control
IT	Information technology
JARUS	Joint Authorities for Rulemaking on Unmanned aircraft Systems
OGN	Open Glider Network
RBAC	Role Based Access Control
SAP ABAP	Advanced Business Application Programming (SAP product)
SAP ERP	Enterprise Resource Planning (SAP product)
TMG	Telemediengesetz (Telemedia Act)
TTDSG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (Act on Data Protection and the Protection of Privacy in Telecommunications and Telemedia)
UAS	Unmanned Aircraft System
USSP	U-Space Service Provider

Table 21: Abbreviations