The Federal Office for Information Security (BSI) as a Major Player for Cybersecurity in Civil Aviation

Cybersecurity in Civil Aviation

Hendrik Dibbern

Head of Division W 32 – Cybersecurity at Airports

Hamburg Aerospace Lecture Series, October, 09th 2025

Federal Office for Information Security

Bundesamt für Sicherheit in der Informationstechnik (BSI)

https://doi.org/10.5281/zenodo.17722957

Hamburg Aerospace Lecture Series
Hamburger Luft- und Raumfahrtvorträge

RAeS Hamburg in cooperation with the DGLR, VDI, ZAL & HAW invites you to a lecture

The Federal Office for Information Security (BSI) as a Major Player for Cybersecurity in Civil Aviation

Hendrik Dibbern, MSSc
Head of Division Cybersecurity at Airports, BSI

Date: **Thursday 9 October 2025, 18:00**
Location: **HAW Hamburg, Berliner Tor 5, Hörsaal 01.10** (in-person only!)

The German "Federal Office for Information Security", in German: "**Bundesamt für Sicherheit in der Informationstechnik**" (**BSI**) is the German federal cybersecurity authority. During the last several years, it has been playing an increasingly larger role in the national air safety network. It acts as a cooperative partner together with different aviation organizations.

Hendrik Dibbern will describe the role of the BSI in the field of Cybersecurity in Aviation. The BSI works in a field of tension between supervision and cooperation. It deals also with future regulations.

Author: Heidas, CC BY-SA, Wikimedia

2018 – 2020	*Master of Social Science (MSSc) in International Security and Law at University of Southern Denmark.*
2020	*Start of work at BSI in the area of Critical Infrastructure in the Transport Sector.*
Since 2023	*Head of Division Cybersecurity at Airports (Referatsleiter W32 – Cybersicherheit an Flughäfen).*

Hamburg Aerospace Lecture Series (AeroLectures): Jointly organized by DGLR, RAeS, ZAL, VDI and HAW Hamburg (aviation seminar). Information about current events is provided by means of an e-mail distribution list. Current lecture program, archived lecture documents from past events, entry in e-mail distribution list. All services via http://AeroLectures.de.

Topics

- Introduction of the German Federal Office for Information Security (BSI) and Division W 32

- Main tasks of Division W 32

- The current (Aviation) Cyber Threat Landscape

- Beyond regulating stakeholders: IT-Grundschutz Profil for Small- and Medium-Sized Airports

Introduction of the German Federal Office for Information Security (BSI) and Division W 32

Our Stakeholders

State

Business

Civil society

Science

Prevention

Detection

Response

- Adoption of technical protection measures
- National IT Situation Centre
- Technical support and services
- CERT-Bund and MIRTs
- Advice and service centre
- Co-operation
- Alliance for Cyber Security
- CI Implementation Plan (UP KRITIS)
- Support in training and further education
- Technical guidelines
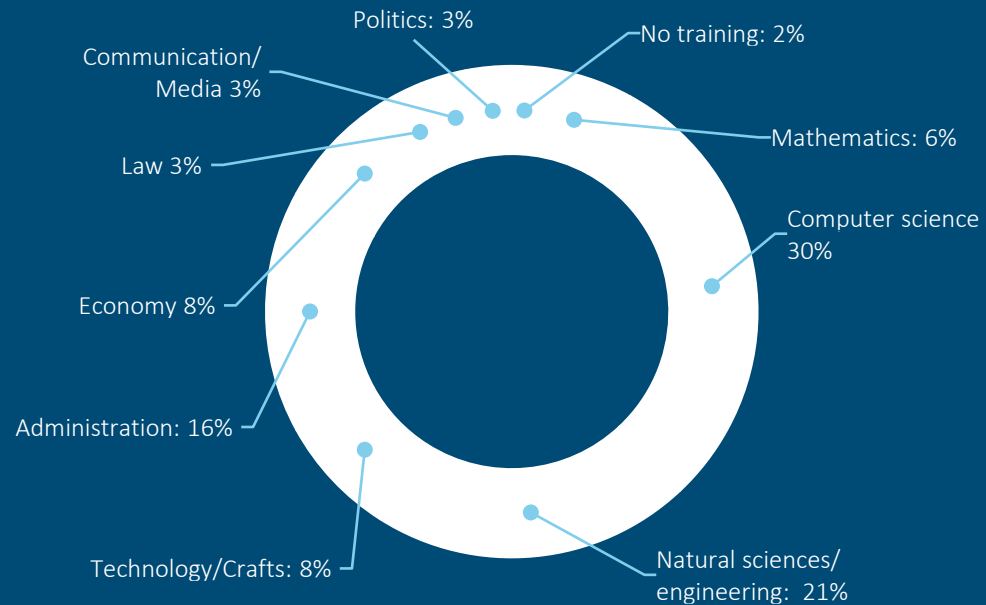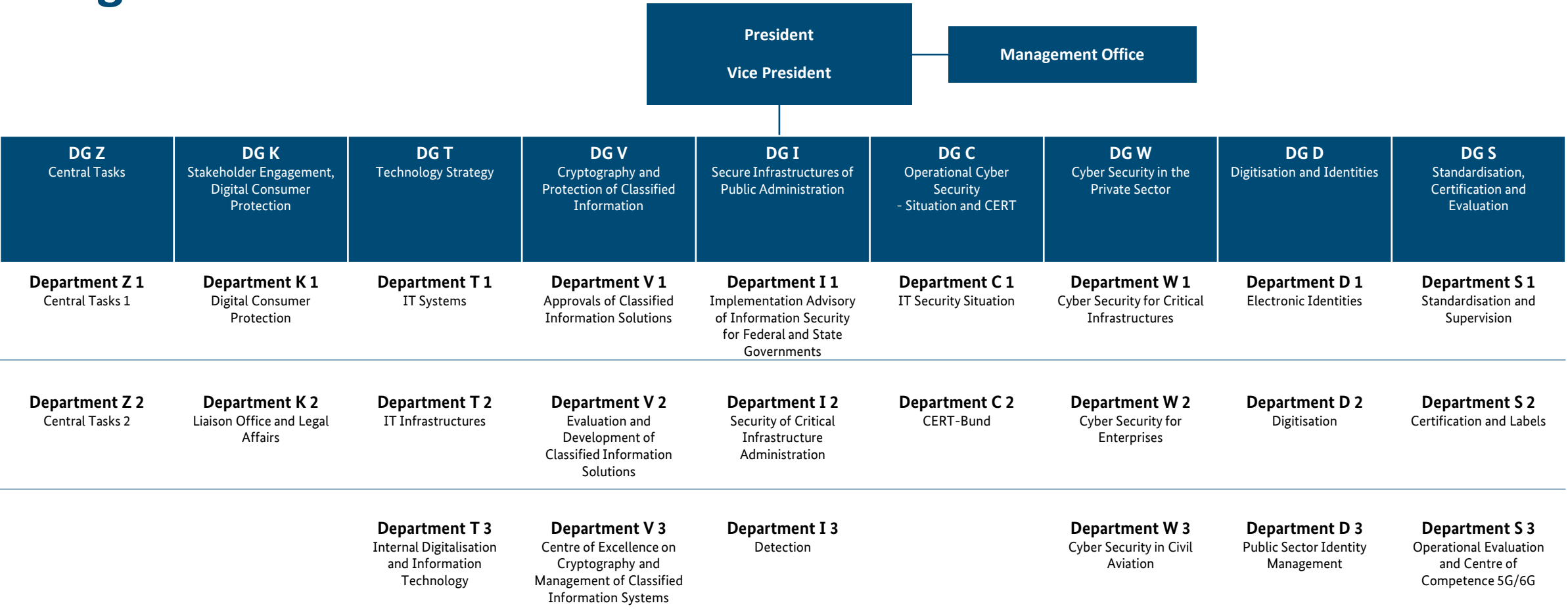- Certification
- IT security mark

Federal Office for Information Security

Foundation
1 January 1991

Hamburg

Berlin

Headquarter

Bonn

Freital

Brussels

Wiesbaden

Saarbrücken

Stuttgart

Federal Ministry of the Interior

Federal Office for Information Security

Jobs 2024

1,785

Politics: 3%

No training: 2%

Communication/ Media 3%

Law 3%

Mathematics: 6%

Computer science 30%

Economy 8%

Administration: 16%

Natural sciences/ engineering: 21%

Technology/Crafts: 8%

237 million Euro

Financial planning 2024

Version information: 30.06.2022

Main Tasks of the BSI

Cybersecurity basics and state of the art

Institutional co-operation

Technologies

Research funding

Manufacturers and products

Operators and business

Classified information

Security Operations

Digital consumer protection

IT security of the federal government

Federal Office
for Information Security

Organisation of the BSI

President

Vice President

Management Office

DG Z	DG K	DG T	DG V	DG I	DG C	DG W	DG D	DG S
Central Tasks	Stakeholder Engagement, Digital Consumer Protection	Technology Strategy	Cryptography and Protection of Classified Information	Secure Infrastructures of Public Administration	Operational Cyber Security – Situation and CERT	Cyber Security in the Private Sector	Digitisation and Identities	Standardisation, Certification and Evaluation
Department Z 1 Central Tasks 1	**Department K 1** Digital Consumer Protection	**Department T 1** IT Systems	**Department V 1** Approvals of Classified Information Solutions	**Department I 1** Implementation Advisory of Information Security for Federal and State Governments	**Department C 1** IT Security Situation	**Department W 1** Cyber Security for Critical Infrastructures	**Department D 1** Electronic Identities	**Department S 1** Standardisation and Supervision
Department Z 2 Central Tasks 2	**Department K 2** Liaison Office and Legal Affairs	**Department T 2** IT Infrastructures	**Department V 2** Evaluation and Development of Classified Information Solutions	**Department I 2** Security of Critical Infrastructure Administration	**Department C 2** CERT-Bund	**Department W 2** Cyber Security for Enterprises	**Department D 2** Digitisation	**Department S 2** Certification and Labels
		Department T 3 Internal Digitalisation and Information Technology	**Department V 3** Centre of Excellence on Cryptography and Management of Classified Information Systems	**Department I 3** Detection		**Department W 3** Cyber Security in Civil Aviation	**Department D 3** Public Sector Identity Management	**Department S 3** Operational Evaluation and Centre of Competence 5G/6G

Categories of BSI Tasks

Overview of the Individual Tasks

Security Operations

- Situation centre and situation
- IT Crisis Response Centre
- Incident support (CERT and MIRT)
- National Cyber Defence Centre (NCAZ)
- Cyber defence
- Vulnerability management

Operators and Business

- KRITIS support
- Support for providers of digital services
- Support for Big Businesses
- NIS II support
- Sector support

- Support for SMEs
- Security networks
- Investment restrictions
- Maturity assessment and certification

Main tasks of Division W 32
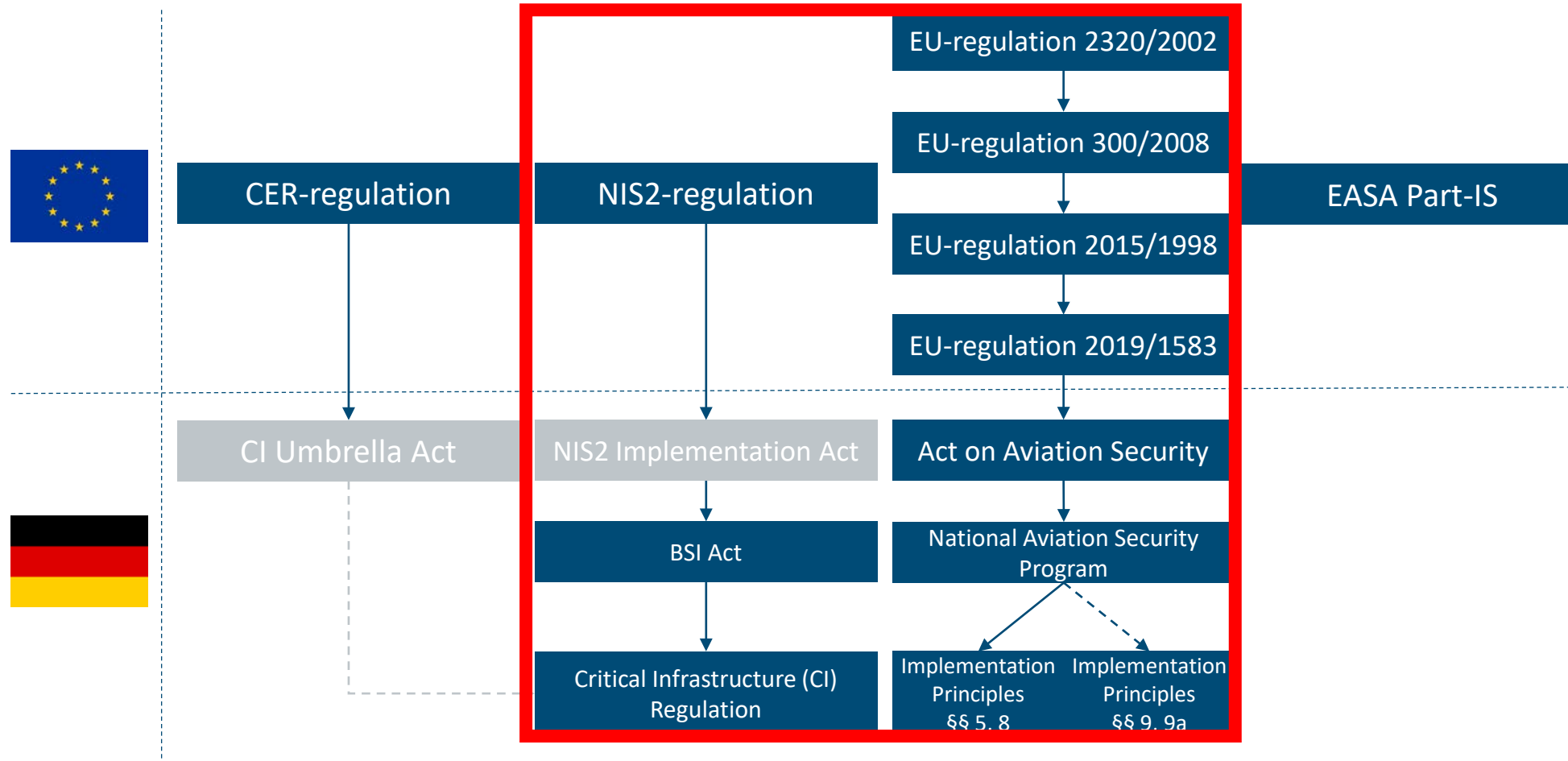
Main Regulations that lay the Foundation for our Work

Aviation Security
(§§ 5, 8 Aviation Security Act)

Critical Infrastructures
(BSI Act / NIS2)

Airports (§ 8)

Authorities (§ 5)

Airlines

Logistics

Big Airports

ANSPs*

*ANSP: Air Navigation Service Provider

Federal Office
for Information Security

What We Do on a Daily Basis

Stakeholders

Registration

Regular Audits
→ "State-of-the-Art"-
ISMS/BCMS/IDS

Reporting of Security Deficiencies and Security Incidents

BSI

Information of Stakeholders with regard to Vulnerabilities and Attacks/Threats

Support of Stakeholders during Security Incidents

Registrations, Audit Evidence, Monitoring of Security Deficiencies

Federal Office
for Information Security

The current (Aviation) Cyber Threat Landscape

Reported Incidents in 2024 and 2025 (as of September, 30th)
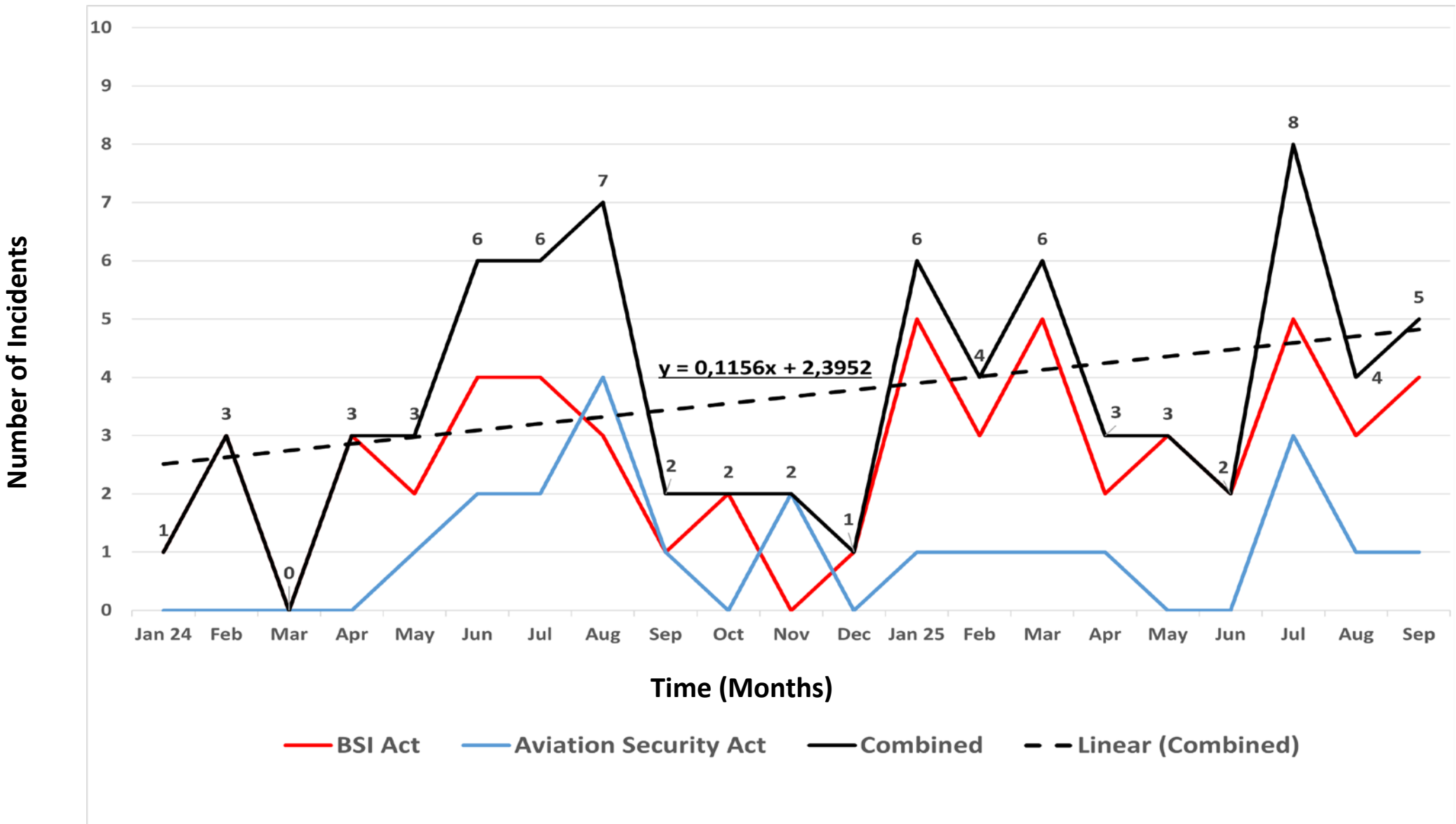
Linear equation shown on chart: $y = 0{,}1156x + 2{,}3952$

Legend: BSI Act — Aviation Security Act — Combined — Linear (Combined)

X-axis: Time (Months)
Y-axis: Number of Incidents

Beyond regulating stakeholders: IT-Grundschutz-profil for Small- and Medium-Sized Airports

What is an IT-Grundschutz Profil?

- **"baseline protection profile" based on the BSI IT-Grundschutz (State of the Art in Information Security)**

- **Information Security Template for users (from users)**

- **the usage of an IT-Grundschutz Profil is not a BSI requirement but a <u>recommendation</u>**

<u>Core content:</u>
- a list of relevant targets (business processes, applications, IT systems and rooms);
- a determination of the required protection level for the relevant processes and applications;
- an assignment of the appropriate and existing IT-Grundschutz modules to the target objects (modeling)
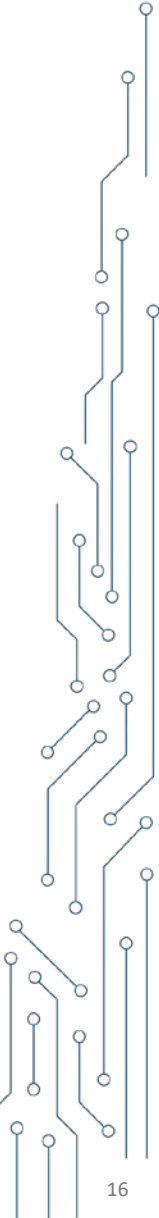
Participants in the working group

Besides BSI employees, staff of the following airports was involved:

Münster/ Osnabrück Airport (FMO)	**Dortmund Airport (DTM)**	**Hahn Airport (HHN)**	**Nuremberg Airport (NUE)**	**Karlsruhe/ Baden-Baden Airport (FKB)**	**Memmingen Airport (FMM)**

Standard Protection procedure

Steps included in IT-Grundschutz Profil for small and medium airports

Specification of the scope
- Organisation
- Infrastructure
- IT Systems
- Applications
- ~~Employees~~

Structure Analysis
Status quo Analysis

Defining Protection Needs

Modelling
(selection and adaption of requirements)

IT-Grundschutz Check (Part 1)
(gap analysis)

Risk Analysis

Consolidation

IT-Grundschutz Check (Part 2)

Implementation of Safeguards

Maintenance and Continuous Improvement

Core Protection

Normal protection requirements

Standard Protection

Basic Protection
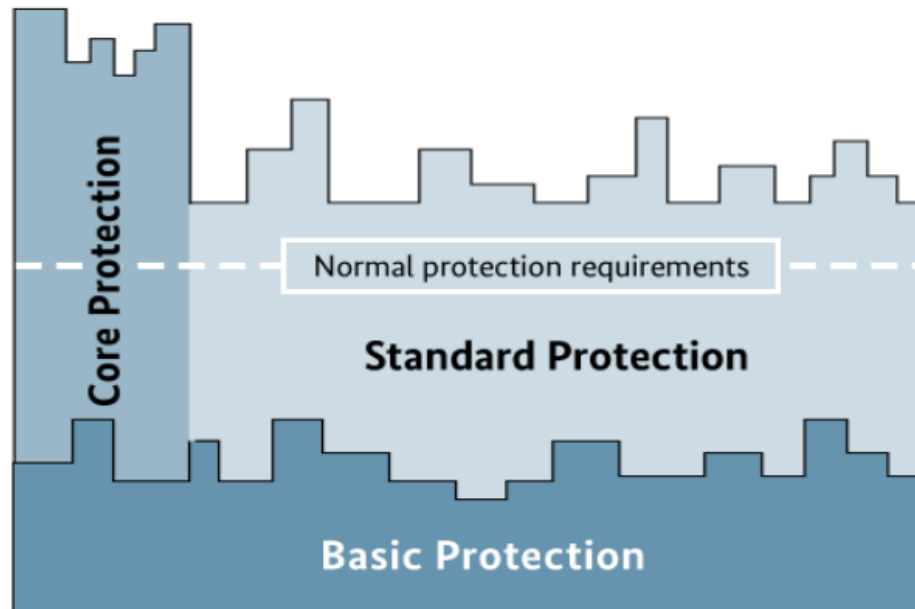
Structural Analysis
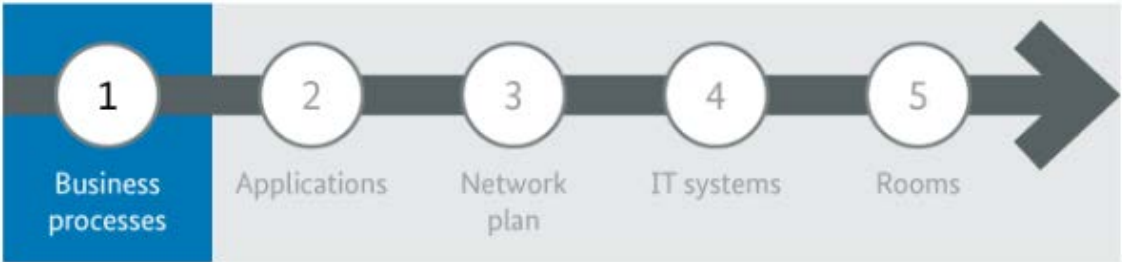
| Identifier	Security processes and description
P1.1	Airport
P1.1.1	ID card management: administration and issuing of ID cards for employees, suppliers or visitors to the airport for identification and access authorisation
P1.1.2	Boarding pass control: checking passengers' boarding passes before they enter the security checkpoint and boarding area

Extract from table 8 in the IT-Grundschutz Profil for small and medium airports
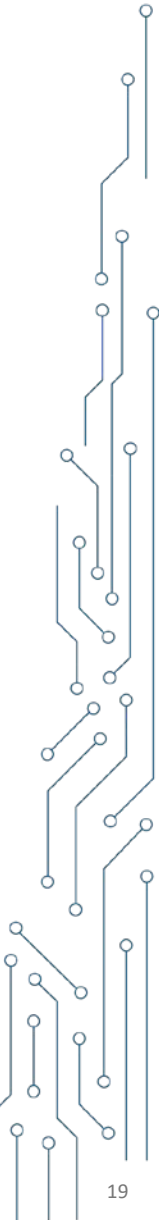
Structural Analysis
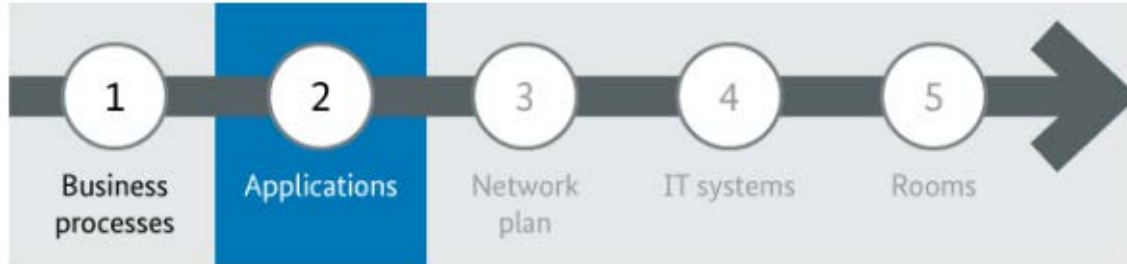
Identifier	Applications in the information network	Supported processes
A1	Airport Operational Database (AODB)	P3.1.3, P3.1.4, P3.1.5, P3.2.1, P3.4.3 – P3.4.10, P3.5.1, P3.5.2, P7.1.5, P7.2.1, P7.2.18, P7.2.19
A2	ID card management system	P1.1.1, P1.1.7
A3	Access control system	P1.1.1, P1.1.7, P1.1.8

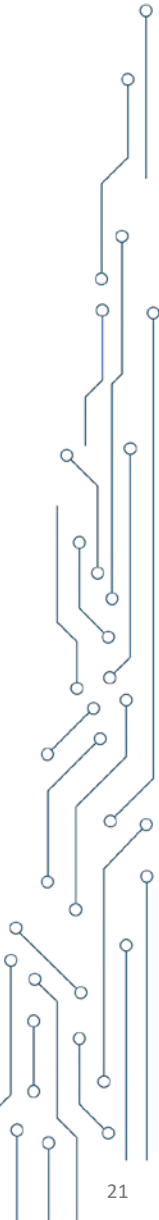Extract from table 9 in the IT-Grundschutzprofil for small and medium airports

Structural Analysis
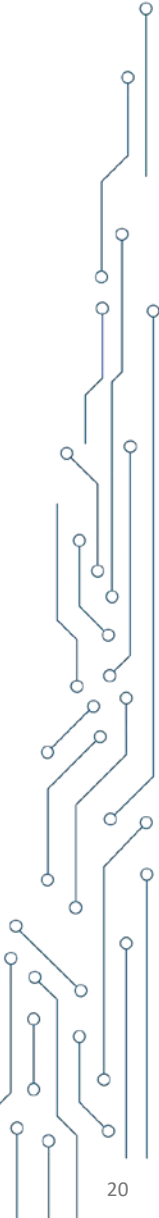
1	2	3	4	5
Business processes	Applications	Network plan	IT systems	Rooms
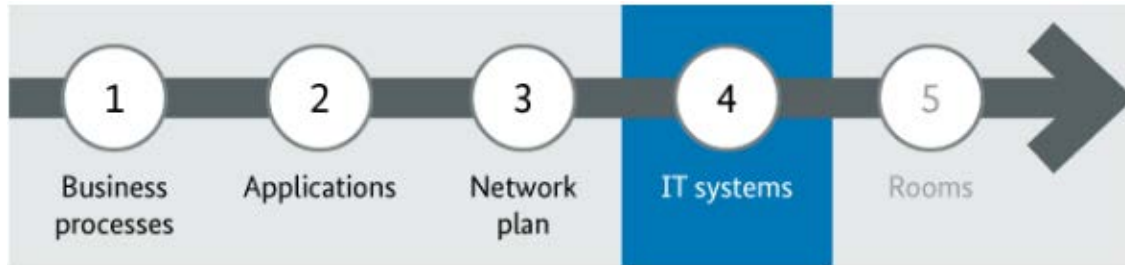
Identifier	IT systems in the information network	Supported applications
S1	**File management and access**	
S1.1	File server (file system)	A29
S2	**Authentication and access control**	
S2.1	Authentication server (AD)	all applications that include AD rights administration
S2.2	Multi-factor authentication server	all applications when accessed via RDP/VPN (remote access) or external service
S2.3	Video surveillance server	A4
S2.4	Certification server	A1
S2.5	Access control server	A2, A3

Extract from table 10 in the IT-Grundschutzprofil for small and medium airports

Structural Analysis
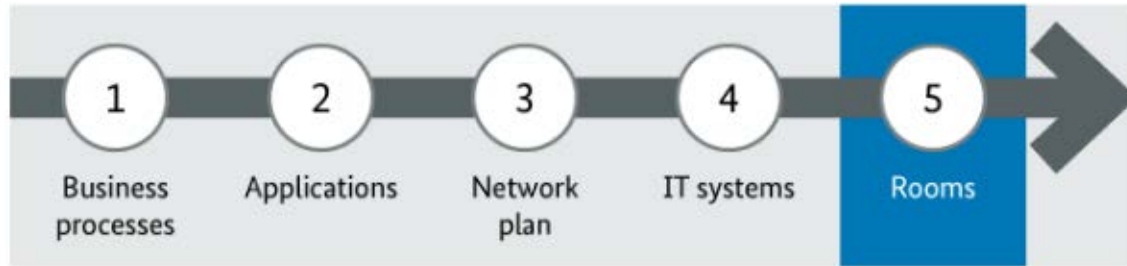
Identifier	Area, building or room
R01	Traffic control centre
R02	Distribution rooms (network)
R03	Server rooms/data centres (1,2,3) Combinations of these (on-site, external)

Extract from table 11 in the IT-Grundschutzprofil for small and medium airports

Determination of protection requirements

Category
normal
high
very high

Extract from table 12 in the IT-Grundschutz

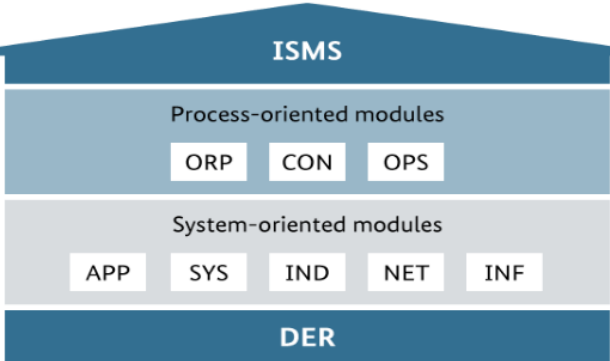| Process name	SG Confidentiality	SG Integrity	SG Availability
Security processes			
Airport			
P1.1.1 ID card management	high (Processing and storage of personal data)	high (all authorised persons identify themselves with the ID card and may be granted access to sensitive areas)	high (in the event of failure, no new ID cards can be issued or existing ones are blocked)

Extract from table 13 in the IT-Grundschutzprofil for small and medium airports

Modelling

ID	Module	Relevant	Target objects	Note
APP	**Applications**			
APP.1.1	Office products	Yes	A29, A31	
APP.1.2	Web browsers	Yes	S5.12, S5.13	
APP.1.4	Mobile applications (Apps)	Yes	A31, S5.13	apps are used by airport employees (e.g. on the apron, baggage handling)
APP.2.1	General directory services	Yes	A29, cf. SYS.1.1	

Extract from table 16 in the IT-Grundschutzprofil for small and medium airports

IT-Grundschutz-Compendium

Final Draft, 1 February 2022

ISMS

Process-oriented modules

ORP CON OPS

System-oriented modules

APP SYS IND NET INF

DER

Goal: Support compliance with the following regulations

Aviation Security

IR (EU) 2015/1998
(IR (EU) 2019/1583)

Aviation Safety EASA Part-IS

DR (EU) 2022/1645
IR (EU) 2023/203

NIS 2
Directive (EU) 2022/2555

Planned extensions and revisions

- Module "Baggage conveying and sorting system (or conveyor belts in general)"
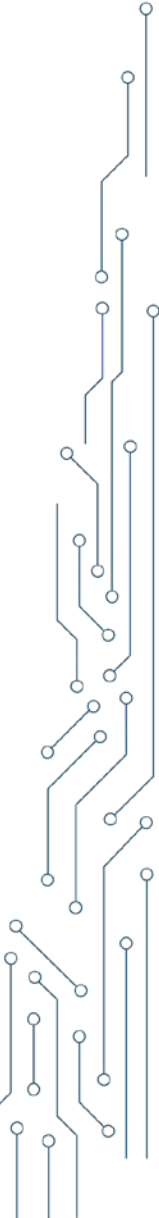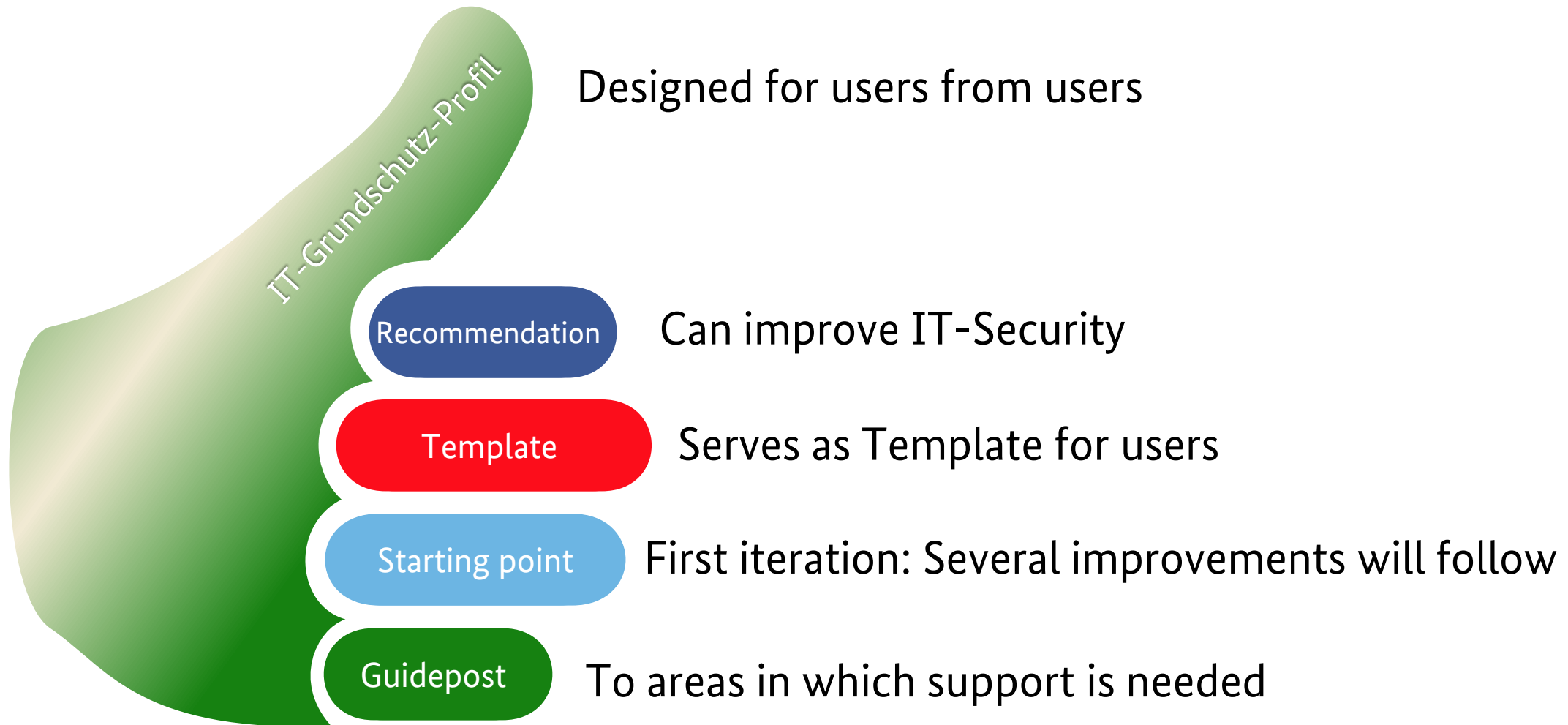
- Module „Baggage Screening System"

- Revision of the IT-Grundschutzprofil within the next 2 years
- Transfer into Grundschutz++

- Research Project „EvalGSP-KMF"

Summary

IT-Grundschutz-Profil

Designed for users from users

Recommendation — Can improve IT-Security

Template — Serves as Template for users

Starting point — First iteration: Several improvements will follow

Guidepost — To areas in which support is needed

Take-Home-Message

Thank you!

Let's keep in touch!

High threat level

Challenges ahead

Prevention is key!

Hendrik Dibbern
Head of Division W32 – Cybersecurity at Airports

lusi@bsi.bund.de
Phone: +49 228 9582-6916
Mobile: +49 160 92085258

Federal Office for Information Security (BSI)
Godesberger Allee 87, 53175 Bonn

www.bsi.bund.de

Follow us:

Image: © AdobeStock/Nirut