SpaceOps Workshop

The security policy at DLR/GSOC based on the ISO 27001

Martin Pilgram – DLR/GSOC

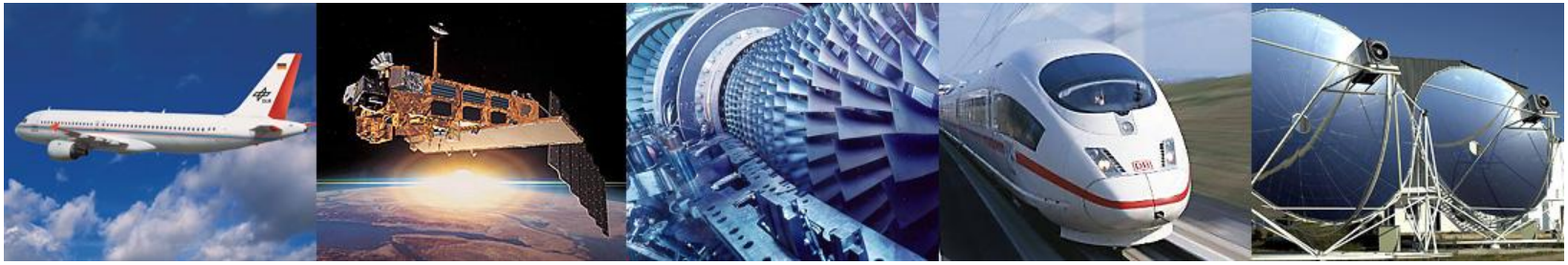
The security policy at GSOC (German Space Operation Center)based on the ISO 27001 - Overview

- GSOC – one part of DLR
- Security for space missions
- GSOCs approach to ISO 27001
- The Information Security Management System (ISMS) build up in GSOC
- Specific aspects of the ISMS and their implementation
- Interaction with other security concepts
- Lessons learned

DLR: Guiding Principles – Vision

- DLR – one of Europe's leading public research institutions, setting trends in its aeronautics, space, transport and energy business areas
- DLR – in its space agency function, a force that shapes European space activities
- DLR – the umbrella organisation for the most effective and efficient project management agencies and offices

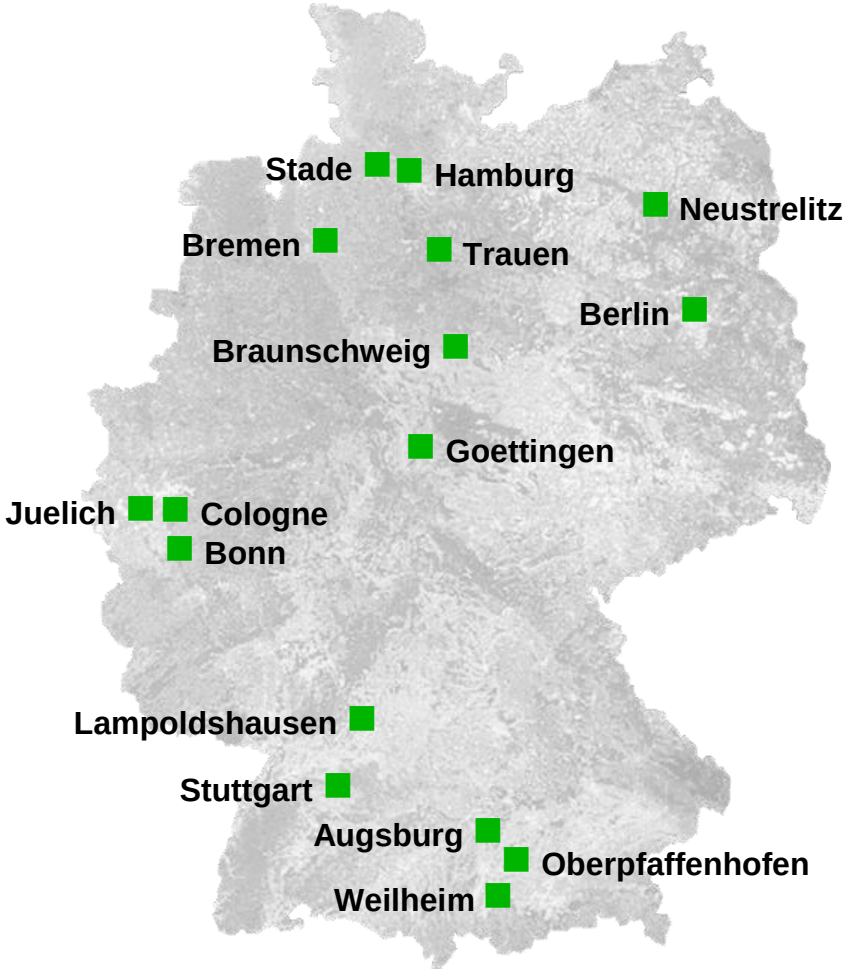
Aeronautics | **Space Research and Technology** | **Transport** | **Energy** | **Space Administration** | **Project Management Agency**



DLR: Locations and employees

7400 employees across
32 institutes and facilities at
- 16 sites.

Offices in Brussels, Paris, Tokyo and Washington.



DLR Space Operations Facilities

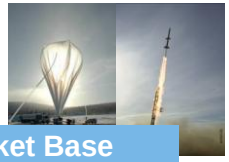
- Microgravity User Support Center Cologne

-German Space Operations Center Oberpfaffenhofen

- European Astronaut Center Cologne

-Galileo Control Center -Oberpfaffenhofen

-Ground Station Weilheim



-Mobile Rocket Base -Oberpfaffenhofen

- Satellite Operations

- Astronaut Training

- Spaceflight Technologies

- Human Spaceflight - Missions

- Sounding Rockets

- Ground Stations & Communications

Security for space missions

Space segment

To fulfill security requirements for up- and downlink the satellite has to support this functionality on board. This may include e.g. authentication or crypto mechanisms for securing the up- and downlink.

Ground segment

Beside the support of the implemented on board features ground operations has to deal with both:

- ❑ Providing a secured infrastructure
- ❑ Operate the satellite using this infrastructure in a secured manor.

Ground segment interoperability

is limited today to the use of a provided crypto unit and the exchange of crypto keys and ISAs (Interconnection Security Agreement) for general support.

Guidelines:

- ❑ ***Security Threats against Space Missions.*** **CCSDS 350.1-G-1**
- ❑ ***CCSDS Guide for Secure System Interconnection.*** **CCSDS 350.4-G-1**
- ❑ ***Security Guide for Mission Planners.*** **CCSDS 350.7-G-1**

Security requirements for the ground segment

TerraSAR-X (security against sabotage)

Because of *US International Traffic in Arms Regulations* (ITAR) regulations some kind of security for the use of US sensors in TSX satellites was required. This triggered the SatDSiG (Satellite Data Security Act). With this act government aims to:

- prevent tampering with commands for remote sensing satellites,
- protect sensitive remote sensing data against uncontrolled proliferation and misuse.

SATCOM (security against classified items, military systems)

GSOC is operating the communication satellites of Germany's armed forces. This is done in a fully separated network.

Upcoming missions

Will combine military and non-military parts. To save money and to benefit from the infrastructure already used for other missions, a security baseline has to be provided.

Our way to ISO 27001

Freedom of science and research

Commercial business

We learned that establishing an Information Security Management System (ISMS) is not a word by word implementation of a given standard but a may be practicable steering instrument for efficient planning, doing, controlling and acting information security.

To fulfill security requirements first for TSX and then also for future missions GSOC decided in 2007 to go for an ISMS (ISO 27001).

As being already ISO 9001 certified it was decided to build up the ISMS as part of an integrated management system.

A Project-Centric Approach

As TerraSAR-X (TSX) brought up the need for a security management this project was selected as basis for certification.

- This approach should minimize the effort to be done to get the ISMS set up.
- It includes all TSX specific systems as well as all general purpose operational environment (network, servers,…)

But it didn‘t touch project specific items of any other mission.

ISMS – the new approach

past:
hardening systems to protect the kept information

today:
analysis the protection requirements of information to harden the entities where the information is located.

The result might be the same but the view is different!

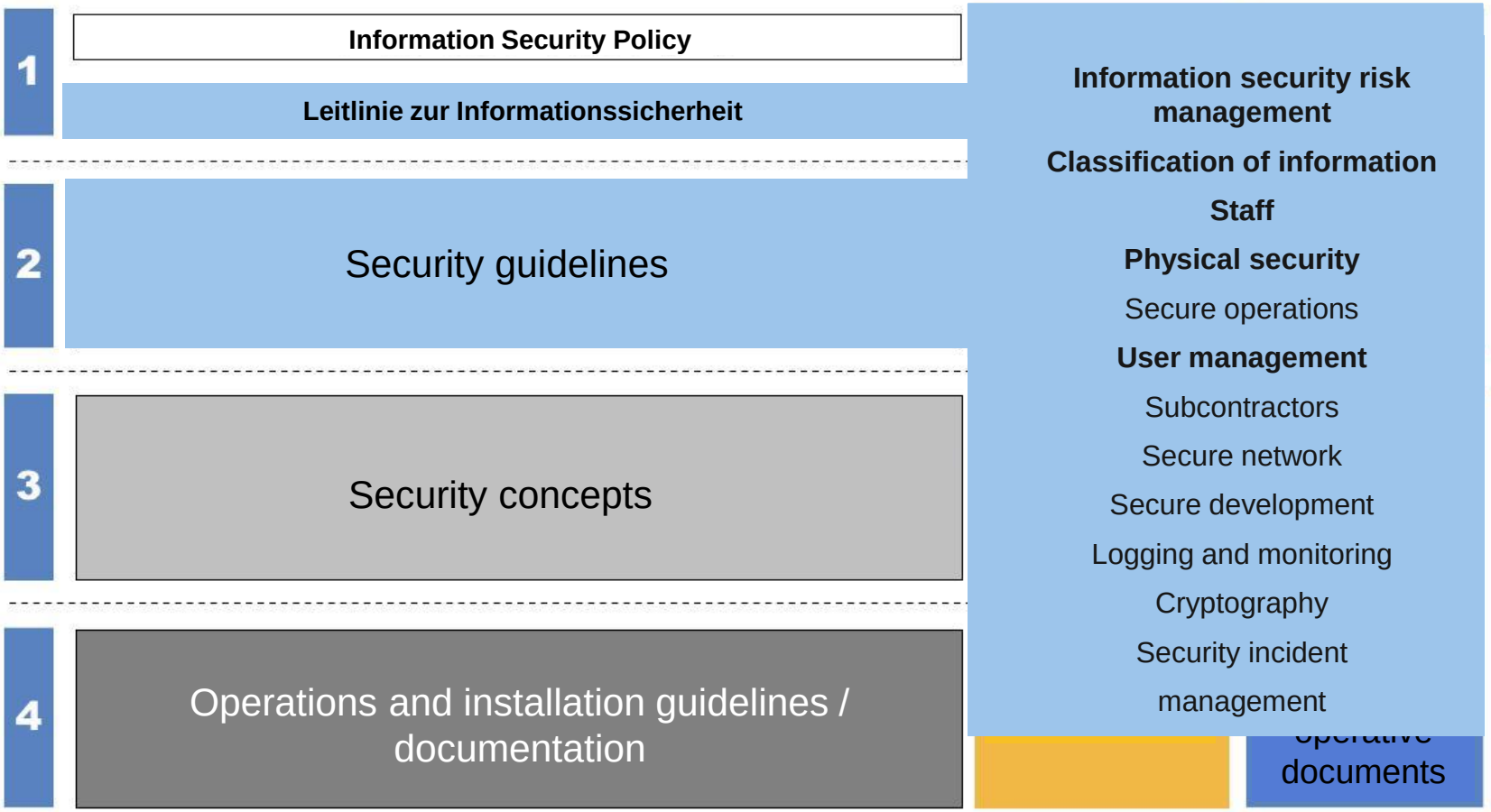
Definition

Information security includes

1. the organizational regulations (processes, structures, rules and instructions) the personal arrangements (communication, training, awareness)
2. the three core areas of technical security: IT security, physical security and security regulations/law.

<table>
<tr><td colspan="3">Information security</td></tr>
<tr><td colspan="3">organisational security</td></tr>
<tr><td colspan="3">personal security</td></tr>
<tr><td colspan="3">technical security</td></tr>
<tr><td>IT security</td><td>physical security</td><td>security regulations/law</td></tr>
</table>

Structure of our ISMS Documentation



Risk Management

Risk analyzes

- for all critical items the risk has to be analyzed on the basis of effects and occurrence probability.
- Three categories for the effects have to be analyzed: Quality/Security, Cost and Time.
- Based on these analyzes the critical items are classified as low, medium or high risk items.

Risk handling

- look for avoidance, reducing, acceptance and transfer of the risk
- analyze the effectiveness of the risk handling based on the requirement that the remaining risk is acceptable
- at least once a year a risk report has to be generated for a project
- define how to deal with the remaining risk

Information Classification

- All information created, stored or processed by GSOC projects shall be classified
- Classification of external data has to be kept
- The classification imposes restrictions in regard to:
  Access, Storage, Duplication, Publication, Transmission, Retention, Destruction

1	Offen
2	Intern / Internal-Use-Only
3	Vertraulich / Confidential
4	Verschlusssache (VS)

	1	2	3	4		
ESA	ESA Unclassified	ESA Unclassified	ESA Unclassified	ESA Restricted	ESA Confidential	ESA Secret
Germany				VS-NfD	VS-confidential	secret
DLR		normal	confidential/ high	VS-NfD/ very high	VS-confidential/ very high	secret/ very high
GSOC	open	internal	confidential	VS-NfD	VS-confidential	secret

Physical security

	Definition of the zones Description	**Examples**
0 white	**Uncontrolled Area** Acessible freely by everybody	Public domain, surroundings of DLR like streets etc.
1 gray	**Controlled Area** Acessible freely by employees; others become controlled and recorded	DLR site OP
2 green	**Area only for employees and visitors** Controlled access for employees and third party; third party has to register and to be accompanied or have a permission	GSOC foyer
3 yellow	**Area only for a certain group of employees** Other employees have to have a concrete task and a permission or be accompanied; third party has to be known, accompanied and fulfilling a concrete task	Offices, meeting rooms
4 red	**Security Zone** Zone has to be secured and controlled at any time; access only for a certain group of employees having a concrete task; employees registered; third party registered, known and accompanied personally	Control rooms, server rooms

Password Handling as Part of User Management

The ISMS gives a very detailed description on the handling of passwords, which includes requirements for:

- structure of a password (e.g. length),
- duration of validity,
- differentiation between user and admin passwords,
- storage of passwords, and
- how a new password has to vary from an old one.

But it is hard to control, how the user store their passwords, how they change their passwords if the system is not supporting the policy,….

The policy has to follow technology trends:

- longer passwords,
- other methods of authentication.

User Awareness Training

One of the certification audits showed deficiencies concerning the awareness training of the employees.

Based on these observation awareness trainings were improved

- General awareness lesson (once a year, mandatory for everyone in GSOC)
- Information Security is now integral part of group meetings (also for contractors) and it is taking into account the special involvement of the people of this group (e.g. special training for operators)
- Our training is now based on lessons or questionnaires.

Open issue: how to meter the success of the training.

ISMS measures

like in every management system you have to show that your performance is increasing over the time. Therefore you have to generate measurements to show this performance. These measures could be:

- Number of employees attending the awareness training
- Number of risks remaining
- Number of vulnerabilities in the used OS
- Number of rejected accesses at your firewalls
- Number of viruses deleted in your system
- Number of wrong logins

Interaction with other security concepts

DLR security

GSOC as part of DLR has to follow DLR rules. On the other side GSOC is certified based on its ISMS. Therefore DLR should be close contact with GSOC when introducing new rules which contradict the ISMS.

BSI catalogue

At least in Germany, especially requirements for military missions are still based on the so called BSI (Federal Office for Information Security) catalogues. They are much more concrete and more applicable to an office environment than for a „real-time“ environment. For interaction a cross-referencing is necessary.

Interaction between different ISMS

As the ISMS is more or less only a framework for how to organize security the concrete implementation could be different. Therefore it might not be easy to generate a general security concept are based on different ISMS.

New Projects

New projects have to be defined on the basis of the ISMS, this includes

- Information classification for the project,
- Risk analysis based on the information classification,
- Check for compliance with our multimission environment,
- A responsible for QA and Security has to be defined.

Lessons Learned

A valuable set of documents is only one part of on ISMS

- You have to update the documents regularly
- You have to live the documentation
- Implementations should support the security requirements and give the user the feeling to do it easier the right way.
- You must be able to control the implementation of your security requirements
- Not all employees are talking German

Conclusion

GSOC will decide in July 2013 how to proceed with ISO 27001.

As TerrarSAR-X is ending over the next years a new candidate-project has to be picked and the question will be beside the selection:

Is the approach generating too much overhead for the projects, or

is the approach the base level for information security a space operation center has to agree on.

The system we established to be ISO 27001 certified, gives us a framework to handle information security in a lot of areas, which were not set up before.