Filling the Void – InfoSec in Space Operations

M. Rückert[1], M. Butkovic[2], E. Dölling[3], J. Eggleston[4], F. Flentge[5], J. Franks[6], D. Heinzer[7], M. Lugert[8], and M. Schmidt[9]
European Space Agency, Robert-Bosch-Str. 5, 64293 Darmstadt, Germany

S. Siram[10]
Vega Space GmbH, Darmstadt, Germany

Information is the most valuable asset of space missions and, as a space operations centre, ESOC is helping protect its confidentiality, integrity, and availability. Following international agreements, ESA has established agency-wide Security Directives that govern all aspects of security, including *Information Security*. Implementing these Directives in the frame of a ISO 27001 Information Security Management Systems is the subject of this paper. The content is threefold. First, we discuss ESOC's information security organization and how it is embedded in ESA's security organization. Second, we describe how this organization was created during an ongoing project. Third, we summarize lessons learned that, we believe, will ease definition and execution of similar projects elsewhere.

I. Introduction

Information is often the only return generated by space missions and it is obviously their most valuable asset – *are we doing enough to protect it…?*

In the past, space missions have focused their risk assessment mainly on the *availability* of information and infrastructure, making sure the spacecraft can be operated under virtually any circumstances. In the current threat landscape, this approach falls short as it does not address the equally important aspects of *confidentiality* and *integrity.*

Cyber-criminals have significantly evolved over the past decade. Driven by large criminal organizations or foreign intelligence, they are no longer looking for random targets, but mount direct, multi-staged attacks. They are, what is known as an Advanced Persistent Threat. and there is growing concern about their impact on critical infrastructure[1,2] The successful attack on RSA[3], compromising the SecurID tokens, specialized malware (Stuxnet/Duqu), and documented security incidents in "space"[4] are only the alarming tip of the iceberg.

At ESA, information security is addressed in the ESA Security Directives[5], based on regulations and agreements with the ESA member states. To facilitate their implementation, ESA's Space Operations Centre (ESOC) is running a project to establish an Information Security Management System (ISMS) according to the ISO 27001 standard[7], similar to independent efforts at other space agencies, such as DLR[10]. Our ISMS addresses the three dimensions: People, Processes, and Technology, to support a continuous improvement cycle and a challenging cultural change.

This paper contains a firsthand account of ESOC's approach of managing and breaking down this intricate task. It shows how we have defined manageable infrastructure layers and representative pilot initiatives without sacrificing the holistic operational strategy. In addition to management and formal certification aspects, it describes

[1] ICT Security Engineer, IT Dept., markus.rueckert@esa.int.
[2] Ground Operations Engineer, Mission Operations Dept., marko.butkovic@esa.int.
[3] Head of ESOC Informatics Evolution Section, IT Dept., ernesto.doelling@esa.int.
[4] Head of Product Maintenance and Support Section for Ground Data Systems Infrastructure, Ground Systems Engineering Dept., james.eggleston@esa.int.
[5] Software Engineer, Ground Systems Engineering Dept., felix.flentge@esa.int.
[6] Mission Operations IT Infrastructure Services Manager, Mission Operations Dept., jenny.franks@esa.int.
[7] ICT Engineer, IT Dept., danielle.heinzer@esa.int.
[8] Head of Ground Facilities Operations Division, Mission Operations Dept., manfred.lugert@esa.int.
[9] Head of Technical & Management Support Office, Mission Operations Dept., michael.schmidt@esa.int.
[10] Ground Facilities Security Support Engineer, Mission Operations Dept., swamy.siram@esa.int.

promising techniques for awareness and training campaigns as well as important lessons learned, specific to our common "space" culture.

We believe that especially these lessons learned in Section IV are useful for other organizations that are already implementing an Information Security Management System (ISMS) or plan to do so. Before we discuss these and our conclusions in Section V, we describe how ESOC is organizing information security in the form of three coordinated Information Security Management Systems in Section II. Here, we show how the three sub-systems are scoped, based on their business functions, to complement one another as follows. The 'Information Technology' layer mainly provides the computer and communications infrastructure, while the 'Mission Data Systems' layer develops and provides ground systems and related software. On top, the 'Ground Facilities' layer provides the actual implementation of operations services for space missions (tracking services, radiometric services, etc.). As shown in Sections II.B and III.B, the scope definition was one of the most challenging tasks as the layers provide services inter-layer as well as directly to space missions.

In addition, we discuss how these sub-systems are embedded in ESA's security organization with the ESA Security Directives as the governing element. In Section III, we focus the ongoing project to implement the Information Security Management (ISM) systems at ESOC. Its objective is obtain an ISO 27001:2005[7] certification for ESOC's Mission Operations Infrastructure.

II. ESOC's Information Security Organization

ESOC's information security organization is embedded in the ESA's directorate of Human Space Flight and Operations, where it addresses all aspects of information security in ESOC's Mission Operations Infrastructure (MOI). In the subsequent sections, we describe this organization in detail, explaining how it is embedded in ESA's security organization as well as how it is implemented and for which scope. Afterwards, we explain our approach to information security training and how we organize security as a continuous improvement process.

A. Governance

ESA coordinates security centrally through the ESA Security Office, taking legal and regulatory requirements as well as existing agreements among the ESA Member States into account. Figure 1 illustrates the involved policy and implementation elements, which can be described as follows.

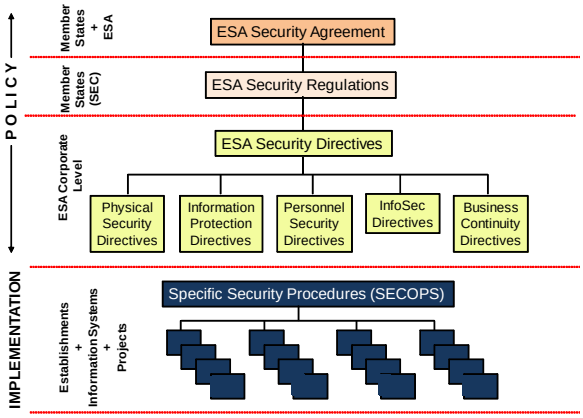

Figure 1. ESA's Information Security Governance.

The *ESA Security Agreement*, approved by the ESA Council and by the Parliaments of the Member States, establishes the general principles among the Parties to ensure a common degree of security for the protection and exchange of classified information.

The *ESA Security Regulations*, approved by ESA Council, provide a legal and technical framework to establish at ESA a system for handling classified information and to adequately protect it.

ESA has translated the Security Regulations into the *ESA Security Directives* which cover the following security areas (often referred to as the *Five Pillars of Security*) for both classified and unclassified information: Physical Security, Information Protection, Personnel Security, Communications and Information Systems Security (INFOSEC), and Business Continuity Management.

The ESA Security Directives provide rules, procedures and guidelines, to ensure conformity of application and correct implementation of the Security Regulations to the fullest extent across the Agency. For each system, e.g., a business unit or a facility, more detailed processes and procedures are addressed in the Security Operating Procedures (SECOPS), which build upon these standards and take into account local or system-specific conditions.

The organisation that manages the ESA security policy and its implementation aspects comprises a number of bodies and key roles. The approach of the ESA security implementation is consistent with that of other International Organisations, such as the European Union.

The ESA Security Committee (SEC) advises the ESA Council and the Director General on all issues relating to the security of Classified Information.

The ESA Director General shall in consultation with the ESA Security Committee ensure the implementation of the ESA Security Regulations within ESA through the issuing of the necessary directives and address security issues referred to him by the ESA Security Office (ESO), by NSAs or DSAs.

The ESA Security Office is responsible for the coordination, control and supervision of the implementation of the ESA security measures.

The Head of Establishment is the highest local authority at an ESA Establishment for security matters and is responsible for the implementation of the Security Directives within his area of responsibility – particularly for physical security. For this purpose, each Establishment or ESA site shall have a Site Security Officer who shall be responsible for the detailed implementation of security within the site.

ESA Directors shall establish a security structure within the organisational unit concerned wherever this is dictated by the nature of an ESA Programme, Project or activity. A *Security Officer* shall be appointed and charged with the implementation of the security within any Programme, Project or organizational unit. For specific aspects related to the security of Communications and Information Systems (CIS), a *Project/System Security Officer (PSSO)* shall be appointed.

The Mission Operations Infrastructure (MOI) domain, which is the subject of this paper, is under the responsibility of the Director of Human Spaceflight and Operations and therefore security is implemented at this level, in close cooperation with the ESA Security Office, the ESOC Site Security Officer for physical security aspects, the Site Security Officers at ESA tracking station sites, local security services, and other complementary corporate security services, e.g., the ESACERT.

B. Scope and Status

When describing the scope of our information security organization, it is important to understand that ESOC's management decided not to have one single ISMS for the entire MOI domain, but rather to break the scope down into three well-defined sub-systems. These are organized according to existing expert domains: Information Technology (IT), Ground Facilities (GNDF), and Mission Data Systems (DS). The rationale is to exploit as much of the expert knowledge as possible at the level of ISMS Managers. See Figure 2 for an overview of the MOI security organization and of the key roles in these expert domains[11].

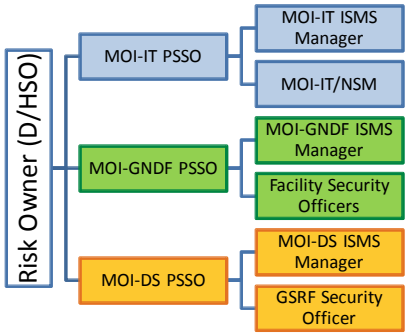

Figure 2. MOI Information Security Organization.

This separation implies a strong need for coordination and collaboration across these sub-systems, which is mainly achieved by means of a center-wide Business Continuity Management System (BCMS) and by linking ISMS documented procedures with existing QMS procedures.

Technically speaking, the combined scope of our three ISM systems encompasses all common and shared infrastructure services that ESOC provides to internal as well as external space missions under its multi-mission model. Examples are computer and communication systems engineering and operation during routine as well as critical mission phases; ESA Tracking Station (ESTRACK) utilization; and Software development of generic ground infrastructure.

Based on the above-mentioned information security governance, the main applicable document for establishing an ISMS is the ESA Security Directives. In addition to policy aspects, it contains applicable security controls and best practices in the form of *INFOSEC directives*. At present, we use these directives instead of ISO 27002[14] to write the mandatory Statement of Applicability. In the future, we intend to generalize our approach, taking both ISO 27002 and ESA's INFOSEC directives into account. In particular, this will be a requirement for obtaining an external ISO 27001 certification, which we currently planned for 2013.

In the meantime, in preparation of this goal, our ISM systems are already run according to ISO 27001 requirements and they are completing individual, full PDCA cycles. In order to fine-tune documentation and processes, we undergo regular internal audits and management reviews, providing evidence of our commitment to

[11] Each domain ISMS is driven by an ISMS Manager, who is supported by 'operational' roles that handle the day-to-day business. Their roles can be briefly described as follows The MOI-IT Network Security Manager (MOI-IT/NSM) approves change requests with a security impact and follow-up on security incidents. The Facility Security Officers are responsible for information security in the various operational facilities (Operational Control Center, Tracking Stations, etc.). The Ground Segment Reference Facility (GSRF) Security Officer is responsible for information security in the ESOC's Ground Segment test facility.

continuous improvement. The goal is to complete a full cycle in each sub-system, incl. management review and internal audit before undergoing an external certification audit. The intentional, staggered implementation schedule (1. MOI-IT; 2. MOI-GNDF; 3. MOI-DS) allowed for MOI-GNDF and MOI-DS to benefit from the lessons learned during MOI-IT ISMS implementation, which is completing a full cycle at the time of writing this document.

C. Running of an ISMS

While information security can be organized in many ways, ESOC's management is adopting the well-established ISO 27001[7] standard in its current version of 2005 and augmenting it with elements from the ESA Security Directives. The ISO standard specifies the requirements for creating and maintaining an Information Security Management System (ISMS). This formal, process oriented approach is aligned with other management system norms, such as Quality Management according to ISO 9001[6]. In consequence, an ISMS runs in four phases: Plan, Do, Check, and Act, forming the PDCA cycle (cf. Figure 3). We augment this framework with two elements required as per the ESA Security Directives: the *System-specific Security Requirements Statement (SSRS)* and the *Security Operating Procedures (SECOPS)*. Security requirements for the system, or sub-system in our case, are systematically identified in the SSRS and they need to be taken into account in all business processes. These requirements may originate from legal obligations, the risk assessment of the sub-system, or they are injected from other business units according to their needs. In all cases, we record the origin and regularly review the adequacy of the requirement. Based on the SSRS, each sub-system documents their information security procedures in the SECOPS. Here, each procedure specifies trigger, input, output, and records, as well as the addressed requirement.

Figure 3. The PCDA Cycle.

In general, an ISMS is composed of many procedures and processes as shown in Table 1. Some of elements are quite formal and help demonstrate normative compliance, e.g., documents and records management. The remaining processes, such as training and control implementation, are driven by the central element of ISO 27001 – the assessment of information security risks.

Phase	Key Processes
Plan	Definition of scope Definition of objectives and certification targets Risk assessment Security policy development Financial planning
Do	Implementation of security policy Application of new controls Process integration and constant monitoring Evaluation of performance indicators Training
Check	Auditing Review of incidents Review effectiveness of established controls Identification of non-conformances Identification of new and changed risks
Act	Analysis of target failures and their cause Corrective and preventive action Review risk analysis and act upon changed risks

Table 1. Phases of the PDCA Cycle.

To this end, each of our ISM systems annually reviews and updates their risk assessment, highlighting changes, required funding, and conclusions to senior management. The assessment takes customer requirements and expectations into account, and it analyses business processes with their supporting assets in a top-down fashion. The analysis focuses on assets, tangible and intangible, and their vulnerabilities, i.e., a weakness that can be exploited by a threat. Only threats with an impact on *Confidentiality*, *Integrity*, or *Availability* (C-I-A) of assets are taken into account. When the estimated impact is combined with a projected probability of occurrence as a second dimension, we arrive at a risk value. This risk value is normalized for ease of exposition and comparability across the three subsystems. As a result, we work with normalized risk values (NRV) in the range [0,1], which are presented to the risk owner along with risk mitigation proposals[12] for all risks above a certain threshold.

[12] Risks may either be consciously accepted, avoided, transferred, reduced, or temporarily monitored.

Once approved and adequate funding is provided, we execute the risk treatment plan with procedural (SECOPS) and technical controls, which typically affects the three dimensions: *People*, *Processes*, and *Technology* (PPT), i.e., also taking operational constraints and the, potentially adverse, operational impact into account. The execution concludes with the verification of the intended control objective, i.e., verifying the effectiveness of the control to mitigate the underlying risk (see Section E). To sum up, the process of systematic risk identification is crucial as the entire ISMS cycle is driven by risks and virtually every action can be traced back to an originating risk.

In addition to the systematic, but rather static, analysis of risks, our ISM systems employ a measurement programme for effectiveness and efficiency of the deployed controls as well of as of the training campaigns. These information are valuable input for ESOC's bi-annual management review of ISMS and QMS, where we report the status of the ISMS to ESOC's management to seek feedback and guidance. This report summarized the outcome of the measurement programme, as well as problem areas, significant risks, and improvement suggestions (e.g., a policy change).

The management review is only one part of the Check phase, where the ESOC's management reviews the ISM systems internally. Another element of this phase is the internal audit, where qualified auditors in ESA assess the compliance of the individual ISM systems against the ISO 27001 requirements. These audits may conclude with non-conformances and observations, which are addressed in a plan for implementing corrective and preventive actions.

In the future, we intend to complement this phase with an external surveillance audit that is performed by an accredited certification authority.

D. Training

Following the above-mentioned concept of sub-system ISM systems, the training and awareness campaigns are planned, designed, and conducted in the individual expert domains. This ensures adequacy and relevance of the presented material. In addition to covering the ESA Security Directives and information security management, we focus on general awareness topics (e.g., the password lifecycle) and the address system-specific Security Operating Procedures (SECOPS) as a central element. This mixture of generic, transferable topics and specific procedures allows for the training to be beneficial for a majority of attendees that have mixed backgrounds and education.

The objective of the training sessions is primarily to enable personnel to fulfill their security responsibilities in their organizational role and the selected topics are driven by the risk profile identified in the sub-system ISMS.

The awareness level and success factor of the initiatives is controlled through the use of questionnaires and by including the results in the measurement programme (cf. Sections B and E). Conducting the campaigns twice a year has proven to be a reasonable trade-off.

In addition, the ESA Security Office and ESACERT provide all ESA staff with a series of educational courses to become acquainted with protection measures against typical information security threats. Their focus is on risks in the ESA corporate environment, i.e., their material is highly transferable, also to other companies and even to the use of IT equipment at home. Hence, central and local training efforts nicely complement one another.

E. Continuous Improvement

Information Security is a very dynamic field, both on the attack side and on the defense side. This requires constant monitoring of changes in the organization and its environment – including the Internet.

Thus, a continuous security improvement process is required to maintain and increase the protection of the MOI information from all possible threats. This process comprises four central tools: audits, control checks, incident review, and measurement.

1. Audits

Internal and statutory audits assist management in assessing the adequacy of procedures and controls. The MOI is periodically reviewed by the ESA Security Office and planned to be externally reviewed by a certification authority. These audits are coordinated with the ESOC's Quality Office. For each reported non-conformance or observation, the related risk is assessed and a corrective action is proposed. The corrective actions plan is followed up by the ISMS managers.

2. Control Check

Auditors focus on compliance with the normative requirements and are unable to verify each and every procedural and technical control, which is why it is the responsibility of the security organization itself to ensure the effectiveness of the employed controls.

The specific target used to determine whether a control is operating effectively is called the *control objective*; we perform a *verification of control objectives* after control implementation and whenever indicators suggest a re-

evaluation. Access control procedures, for example, can be tested by verifying that all access rights of former personnel have been duly revoked and that the required records (clearance form) exist.

3. Review of security incidents

MOI is monitored 24h/7d. Whenever an event turns out to be a security incident, it is handled following assessment and escalation procedures. A rapid escalation, even of suspected incidents is performed. After information security incidents have been supposedly resolved, the situation is reviewed to confirm the accuracy of the original conclusions and measures taken, which may trigger further analysis. In any case, noteworthy lessons learned are communicated to the affected ISMS Managers for identifying control improvements.

4. Measurement

Performance metrics and indicators measure the effectiveness of the ISMS management and of established security controls. Starting with a small set of indicators, the MOI ISM systems are constantly reviewing and fine-tuning the measurement programme, aligned with ISO 27004[9], in order to tailor it to the organizational needs. These indicators are reported, in aggregated form, during the management reviews. The ISMS Managers take improvement actions either in the same ISMS cycle or in the next ISMS cycle depending on their feasibility and budgetary constraints.

III. Establishing Information Security Management Systems

The first activities related to the implementation of ESA Security Directives with a view to the Mission Operations Infrastructure (MOI) started in 2009, with a pilot activity concentrating on an already flying space mission. Results thereof and a proposal for follow-up work were presented to the ESOC's management, which approved the execution of a security assessment of the Mission Operations Infrastructure (MOI) overall, and requested a plan for implementing mitigation measures. These activities were concentrated in the project "Security Directives Implementation Project for Mission Operations Infrastructure" (SDIP for MOI). The project started in early in 2010, and is expected to finish by the end of 2013.

The following sections summarize project requirements, strategy, team building aspects, and the main stakeholders.

A. Requirements

The project was confronted with requirements from various internal and external sources. The main ESA-internal source of requirements stems from the INFOSEC chapter of the ESA Security Directives. Moreover, these Directives were an vital input to defining the scope of the project as it allows the project to focus on information security and leave the equally important aspects of physical security, personnel security, and information protection in general to other business units with the corresponding mandate.

Further input for requirements come from ESA's policies and regulation, as well as from the Staff Rules and from an ESA management perspective, the requirement is to secure and further improve ESOC's reputation as a trustworthy partner for Member States, international partners, and Industry.

Fortunately, these internal aspects already take many of the external factors, such as legal and regulatory requirements, into account. These are particularly important because ESA is bound to international regulations, its convention and Hosting Nation Agreements and Treaties.

On the technical side, the controls resulting from the ISMS processes need to take the critical nature of space operations into account, where security controls must be validated and not conflict with the exceptional availability constraints of a space operations center. Instead, these security controls shall actively support a safe conduct of critical support phases, by preventing serious security incidents from happening.

B. Objectives, and Strategy

To address the above requirements, the main objective of the SDIP for MOI project is to ensure proper management of information security risks in the MOI. In order to achieve this, the project

- bootstraps a continuous improvement cycle, by creating ISM systems;
- implements mitigation measures for immediate security risks; and
- obtains a certification of the ISM systems against the ESA Security Directives (internal) and ISO 27001[13] standards (external).

As an outcome of the project, a common infrastructure, methods, and culture are established, which creates a reliable and trustworthy basis for a broad customer base and international cross-support.

[13] ~~The ISO27001 certification was a~~dded to the project objectives in 2011.

For facilitating the implementation of the project, two key strategies were devised: 1. Split the scope into manageable domains, aligned with existing organizational structures; 2. Allow the resulting sub-systems to run in parallel threads at their individual pace and exchange knowledge and lessons learned frequently.

The resulting sub-systems were designed after an initial in-depth analysis of information security risks in the MOI that may affect flying missions. ESOC's multi-mission model allows space missions to inject their requirements into the MOI, but they typically use existing services. The MOI sub-systems, IT (MOI-IT), Mission Data Systems (MOI-DS), and Ground Facilities (MOI-GNDF), provide services directly to the mission and to one another as depicted in Figure 4. All our sub-systems build upon and rely on the strong physical security concept at ESOC.

While a clearly layered structure would ease both exposition and management, the existing organizational structures with their different maturity levels in terms of information security called for this more complex scope breakdown. Furthermore, running the ISMS implementation[14] for each sub-system in parallel with a temporal offset, allowed MOI-GNDF and MOI-DS to take advantage of the lessons learned of the MOI-IT ISMS implementation.

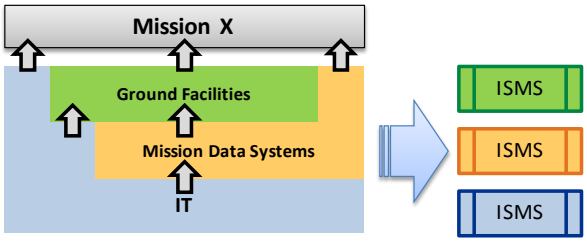

Figure 4. MOI ISMS Sub-systems and Service Provision.

The project will conclude as soon as all three ISM systems are established and internally as well as externally certified against ISO 27001. Afterwards, running these continuous improvement cycles will be part of the normal business activities.

All of these decisions were influenced by the outcome of an elaborate pilot phase, where a flying space mission was analysed regarding their information security posture as compared to their needs. This included an assessment of the impact of implementing identified security controls. Since the majority of risks were identified to be treatable in the infrastructure, the decision was to focus on ESOC's infrastructure services. As a consequence, ESOC's multi-mission model ensures that all customers equally benefit from these improvements. Afterwards, mission-specific aspects need to be treated during the preparation of the mission, based on a mission-specific information security risk assessment.

In support of continued service provision to space missions, the SDIP project is actively supporting the formalization of a Business Continuity Management System (BCMS) that is well-coordinated with the infrastructure ISM systems. This system effectively bridges the gap between common infrastructure protection and dedicated mission-specific information security procedures.

C. Team Building

The project work is being carried out with a small core team, as shown in Figure 5, which is largely aligned with the resulting security organization (see Figure 2). Depending on the tasks to be implemented, the core team is augmented by experts within the Mission Operations and Engineering departments. The core team key roles are as follows.

1. *Project manager*

The project manage is responsible for the overall execution of the project, including financial matters, securing strong management support, and interfacing with all stakeholders. He is coordinating the three ISM systems for the duration of the project to harmonize their output and to exploit synergies.

2. *ISMS Manager*

For each sub-system, the designated ISMS Manager is in charge of implementing an ISMS according to the agreed scope. They remain responsible for their ISMS after the end of the project.

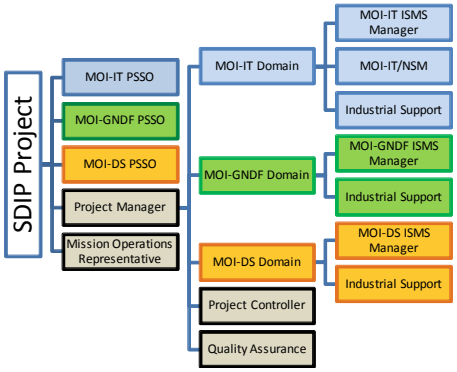

Figure 5. SDIP Core Team.

[14] I.e., assessment of assets and risks; proposal of risk treatment options; management review and approval; prioritized implementation of processes and controls; certification

3. *MOI-IT/NSM*

Being responsible for the secure operation and maintenance of all systems and networks provided by MOI-IT, the MOI-IT/NSM closely supports the MOI-IT ISMS Manager in the implementation of technical controls and procedures. This key role will also remain after project closure.

4. *Industrial Support*

To support the ISMS Managers, each sub-system is relies on experienced technical experts. In particular, they are supporting the complex task of conducting a risk assessment, which often requires an external, unbiased view.

5. *Project System Security Officers (PSSO)*

The PSSOs are overseeing all information security aspects in their respective domain and they are responsible for implementing the ESA Security Directives therein. In the project, they also act as interfaces to senior management as well as supporters of reviews and audits.

6. *Mission Operations Representative*

Representing the needs of ESOC's customers, space mission, he challenges the proposed structures and controls regarding their acceptability and sustainability. He also plays a coordinating role, promoting information security and running surveys and reviews with selected space missions. This includes the documentation of existing centre-wide Business Continuity Processes in the frame of a BCMS, which can be seen as an overarching system to provide requirements to the individual ISM systems.

D. Stakeholders

Identifying stakeholders in a project is key for its success. Within the 'SDIP for MOI' project, the following stakeholders have been identified.

1. *Senior Management*

The *Director* of Human Spaceflight and Operations is the main project stakeholder, at the top of the security organisation, and responsible of risk management within his directorate. His support is vital in the review process and ensures that the project receives funding during the implementation phase.

The support of the *Department Heads* for Mission Operations and Engineering is crucial for the project. They enforce policies and foster the implementation of security improvements within their departments. In addition, they can effectively sensitize all managers in their departments as well as their peers in the Director's management team. A key driver for them is the strategic importance of information security for securing extending and ESOC's customer base.

2. *ISMS Implementers*

3. *The aforementioned separation of the scope into three sub-systems requires several divisions within the ESOC to closely collaborate. Thus, support of the division management is required to ensure manpower, information, and funding for local activities is adequately provided. This includes the staff and contractors working on the implementation of procedures and work instructions. Only with their support and with an understanding of their needs, information security can be successful. Mission Operations Ground Segment Managers (GSM)*

As key users of the MOI, the GSMs represent the user community, for which the ISMS is implemented. Their support is required to ensure feedback during the risk assessment phase, and also during the implementation for evaluating the operational impact of ISMS products. They are represented in the core project team (Mission Operations Representative in Figure 5).

4. *ESA INFOSEC Officer*

Being responsible for the coordination, control and supervision of the implementation of the ESA Security Directives, he reviews, authorises, and certifies the output of the project at planned intervals. The project requires his support as an internal auditor and for overall guidance.

5. *Site Security Officers*

Link to the physical security at ESOC and Tracking Station sites. As the SDIP for MOI project scope only deals with INFOSEC, the support of the Site Security Officers is required to ensure to internal/external auditors that the MOI ISMS has properly linked all physical security requirements.

6. *Quality Manager*

The QMS Manager is in charge of the Quality Assurance organisation within ESOC, the project requires the support of the quality manager in order to facilitate the integration of the ISMS inside the QMS framework and coordinate the external audit process.

7. *SDIP Core Team*

The core team (cf. Figure 5) as with any project, is instrumental to the success of the project, that the team members accept their roles and responsibilities and support the accurate and timely provision of project deliverables.

IV. Lessons Learned

Based on our experience with implementing ISM systems in a space operations centre, we summarize noteworthy lessons learned and recommendations in the subsequent sections. These lessons are based on a survey that included various stakeholders of the SDIP for MOI project and the results are presented from three different perspectives: project management, infrastructure user, and ISMS Managers.

A. Project Perspective

The layered strategy for the SDIP for MOI project simplifies the definition of the work breakdown structure and its gradual implementation, but it also brings a number of challenges to be managed.

1. Definition of Scope

The boundaries of each ISMS have occasionally been confused with the boundaries of the ESA internal organisation. This created a number of conflicting situations and potential misunderstandings within the project, which in principle could have left major gaps between the ISM systems. As a counter-measure, the demarcation lines between the ISM systems were changed several times, requiring an update of the ISMS documentation and of the implementation plans. Defining the scope 'top-down' from the beginning, based on business processes, may have helped to avoid these changes.

2. Resource Allocation

The activities in each domain started in parallel, with the MOI-IT layer being the pioneer, leading the way for the others. The level of resources required by the project, especially in the area of ISO 27001 industrial support was underestimated. This created a strong competition for resources, which did not serve to the overall benefit of the project. As of the increase of the external resource level from one to three experts, the implementation of each ISMS is proceeding according to schedule. However, the growing project team created a new challenge, namely, ensuring that all products from the project follow the same guidelines to provide a unified view of the ISM systems for internal and external auditors.

3. Integration with Quality Management

With the initial goal of achieving compliance with the ESA Security Directives, the project mainly focussed on risk assessment and control implementation. The scope extension to comply with ISO 27001 required a change of focus, away from technical control and towards documented procedures and processes. These overlap with existing Quality Management structures at ESOC and a common set of documented procedures (cf. ISO 27001, clauses 4.3.2, 4.3.3, 6, 7, and 8) offers valuable synergies. As a consequence, several project products had to be amended to align with existing QMS procedures. We recommend considering QMS already in early phases of the ISMS implementation, also because the ISMS itself may be subject of QMS audits.

4. Extrapolation of Pilot Phase to the entire MOI

The extrapolation of the flying spacecraft mission (pilot ISMS) assessment results to the entire MOI was done to estimate the financial and operational impact. This in-depth exercise was very useful to identify space mission specific and common risks. In addition, it led to the important conclusion of focussing on the common infrastructure elements to the benefit of all supported space missions. However, it must be said that mission-specific risks matter and that they need to be addressed according to the mission's own security requirements.

B. Infrastructure User Perspective

The lessons learned from the perspective of the user representative, i.e., the Mission Operations Representative (cf. Section C) can be summarized as follows.

1. Early Involvement

Involving a user representative as a key stakeholder from the beginning was appreciated by all parties.

2. Integration with Business Continuity

The integration of our ISM systems with a centre-wide BCMS was considered only after establishing the ISM systems. In consequence, the individual domains were addressing disaster recovery and related aspects differently. For a consistent business continuity plan, we recommend the definition of a business continuity plan before addressing this aspect in the ISM systems.

3. Reduction of Operational Impact

Information security is often seen as an additional burden and even as an obstacle. Instead of requiring individual teams to produce documents and reports, the SDIP project is delivering them examples and templates for requirements documents (SSRS) and procedures (SECOPS). This successfully increased the receptiveness of the affected teams and avoids duplicate work packages.

C. MOI-IT Perspective

During the ISMS implementation and after completing one PDCA cycle, the MOI-IT domain encountered the following main challenges.

1. Scheduling and Definition of Awareness Campaigns

Improving the security awareness of staff is a key factor to successfully secure the MOI-IT infrastructure and services. Obviously, in a space operations centre, work priorities are assigned to support the eleven flying missions and various missions in preparation. As a consequence, it was and still is very difficult to schedule large training campaigns that also include shift workers. Furthermore, it is difficult to define a training scope that is sufficiently broad and specific enough to the audience with their diverse background. To this end, two measures have been devised. First, recording of the training on video so that it can be replayed at any time that is convenient for the individual. Second, using *simulated incidents* (e.g., a virus outbreak) as a means to challenge all participants in their actual roles. The latter concept also preempts an otherwise typical response of saying that *"Nothing happened in my area of responsibility in the last 10 years, why should I change my way of working now?"*

2. Changing established Operating Procedures

In addition to technical controls, the ISMS typically affects established procedures to align them with the identified requirements (see SSRS and SECOPS in Section II.C). Changing too much in the first iteration, however, puts the support of information security at risks. By changing too little, the identified requirements may not be met. In our case, a good balance was to leave 80% of existing procedures largely unmodified and to significantly change or introduce the remaining 20%. This allows the ISMS management to focus on the problem areas that have been identified previously during staff interviews.

3. Setting up a Measurement Programme

We see measuring of information security performance as a key success factor for maintaining an ISMS. An initial set of metrics, based on what can be easily measured, did not yield the expected results and insights. Also, it did not provide us with indicators or an early warning system for failing or inadequate security controls. As a counter-measure we are running a study with external experts to guide the selection, design, and implementation of meaningful metrics according to ISO 27004[9], focusing on a broad coverage of controls in ISO 27002 and on how to report the outcome to the different interest groups (ISMS Manager, Management Review, etc.).

4. Impact Assessment in Change Management

Assessing the impact on the overall security of the mission operation networks and the systems therein is an integral part of the in-depth information security strategy of the MOI. Whenever a change to the MOI-IT infrastructure constitutes an exception to established policies, the originator is asked to provide a business justification and the expected expiration date of the exception. This process does not always work smoothly and our recommendation is to train the "requestors" of significant changes in how to specify policy exceptions and also how to avoid them.

D. MOI-GNDF Perspective

After having completed the internal audit of the MOI-GNDF ISMS, the following implementation challenges were identified in the Ground Facilities domain.

1. Business Process Model

The security initiatives taken were initially perceived as a standalone project, which would not bring the expected change without reviewing the whole business process. Significant efforts were spent in reviewing and enhancing the existing business process model with the responsible individuals. This in-depth review was instrumental to achieve a robust integration of existing business processes with information security aspects.

2. Inter-dependencies of ISM Systems

The aforementioned split into three expert domain ISM systems naturally results in dependencies in the implementation plans. With MOI-GNDF depending on other business units for the implementation of controls, the plans were too optimistic. As a result, we recommend keeping a close eye on these dependencies to spot schedule slippages as early as possible.

3. Security Training

In addition to the training challenges discussed in Section C, in the Ground Facilities domain, the participation in the security awareness campaigns was not ideal and revealed, once more, the challenging task of brining cultural change to address information security. Communicating the importance of the training events via the appropriate management level and by making the attendance mandatory, we observed an increase in both attendance and awareness. This holds in particular for staff working in remote locations, such as Ground Stations. Also, making information security training part of existing training events is considered a valuable synergy.

4. Security in Outsourcing Contracts

Injecting information security requirements in outsourcing contracts, especially in existing ones, is not trivial. The approach at ESOC was to nominate "security representatives" on both sides to coordinate the update of contracts and agreements, i.e., SLAs and NDA. These security representatives would then address all security matters related to that external interface in day-to-day operations.

E. MOI-DS Perspective

Being the third domain to start with the ISMS implementation, the MOI-DS domain was able to largely benefit from the other ISM systems and their lessons learned. However, the specific area of software development of large mission data systems has various pitfalls and challenges to address.

1. Heterogeneity

The MOI-DS domain includes over 200 staff and contractors working in several different units and two departments (ESA's 2nd organization level). It covers both software development and operational services, such as provision of flight dynamics and navigation data. The initial risk assessment was done on a system and service level by technical documentation review, consultancy from data system experts and asking standardised questions to the responsible Technical Officers. One of the main problems of this approach has been that systems and services have been mainly considered in isolation and that different interpretations of the questions lead to different answers. There is a large difference if a system is considered either without its deployment or with the knowledge of the actual deployment in mind. For example, the availability of a system processing telecommands could be considered extremely important if there is only one such system and the spacecraft design requires the daily uplink of telecommands. If both a redundant deployment scenario and a spacecraft design is taken into account which stores command timelines for several days, the assessment of the availability of the system will be considered much less critical.

In the future, the assessment will be based on the critical business processes and associated assets instead. In addition, the standardized questionnaire will be changed and tailored to the individual process areas.

2. Detailed Vulnerability Assessment

Even for small software products, it is very difficult to assess technical vulnerabilities in detail. When it comes to "big" mission data systems, the challenge becomes enormous, requiring a lot of manual intervention. Even though such penetration tests have been executed over the past years, conducting them for *all* data systems is considered disproportional. Instead, focussing on the most exposed software products helps and to address the remaining systems via a security-enhanced software development life-cycle. This includes a vulnerability scanner that works on the source code level.

V. Conclusion

Taking the above lessons learned into account, the core take-home message should be to focus on the people (stakeholder, operations teams, etc.) with the aim of making them receptive for information security concepts. While the technical part is a challenge by itself, it is the people within the organization who determine their effectiveness. Although this might sound straightforward, it is very difficult to achieve in a complex work environment. Based on our experience, a helpful tool to sensitize the affected staff is to conduct an awareness campaign *before* implementing new technical and procedural controls. Otherwise, once awareness campaigns are mixed with training on specific procedures, discussions on the utility of procedural details may divert the attention away from the actual goal of raising the overall alertness regarding fundamental principles of information security.

In addition to the lessons described in Section IV, we recommend to pay attention to the rather informal comments and observations received from the auditors, even though they do not constitute actionable non-conformances. In fact, they help in avoiding non-conformances in the future.

Appendix A

Acronym List

BCMS	Business Continuity Management System
BCP	Business Continuity Plan
DS	(Mission) Data Systems
DSA	Designated Security Authority
ESACERT	ESA Computer and Communications Emergency Response Team
ESO	ESA Security Office
GNDF	Ground Facilities
GSM	Ground Segment Manager
ICT	Information and Communication Technology
INFOSEC	Information Security
ISM	Information Security Management
ISMS	Information Security Management System
IT	Information Technology
MOI	Mission Operations Infrastructure
NSA	National Security Authority
PDCA	Plan-Do-Check-Act
QMS	Quality Management System
SDIP	Security Directives Implementation Project

Acknowledgments

The authors would like to thank all staff and contractors at ESOC, who have worked hard on the definition and implementation of the ISM systems. We continue to count on their support and commitment to a continuous improvement process. Furthermore, we are indebted to our ESA Security Office for guidance and support throughout the entire implementation.

References

[1] The US-China Economic and Security Review Commission, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" [Online Report], URL: http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf [cited October 2009]

[2] The US-China Economic and Security Review Commission, 2011 "Report to Congress" [Online Report], URL: http://www.uscc.gov/annual_report/2011/annual_report_full_11.pdf [cited November 2011]

[3] RSA, "Open Letter to RSA Customers" [Online Press Release], URL http://www.rsa.com/node.aspx?id=3872 [cited 17/03/2011]

[4] Tal Dekel Ram Levi , "Space Security Capabilities and Trends" [Presentation], URL: http://www.unidir.ch/pdf/conferences/pdf-conf1033.pdf , Presentation, Space Security Conference 2011

[5] European Space Agency (ESA), "ESA Security Directives", 2008

[6] ISO 9000:2008, Quality management systems – Requirements, International Standard

[7] ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements, International Standard

[8] ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management , International Standard

[9] ISO/IEC 27004:2009, Information technology – Security techniques – Information security management – Measurement, International Standard

[10] German Aerospace Center (DLR), "First time in the branch of spaceflight control centers: Accredited Information Security in accordance with ISO 27001", URL: http://www.dlr.de/rb/en/desktopdefault.aspx/tabid-4769/5005_read-32189 [cited 19/09/2011]