ISO27001 for Ground Segment Security

Mr. L. N. Swamy Siram[1]
VEGA Space GmbH, 64293 Darmstadt, Germany

This paper presents an overview of application of the ISO27001 standard for securing ground segment which is crucial for spacecraft operations. The purpose of this paper is to provide guidance for successful alignment of space business processes with ISO27001 standard and to present solutions for typical space industry problems in implementing risk mitigation measures. The scope of this paper is limited to the ground segment security only, space segment security is considered out of scope.

Each space mission varies with security requirements and in-orbit duration depending on its mission objectives, but all missions of an organization use some common ground segment infrastructure which is shared across several missions for cost efficiency. Risk mitigation measures and strategies that protect each mission's assets whilst benefitting from using shared infrastructure are presented in this paper. The solution allows missions with High, Medium or Low security requirements to co-exist and interoperate without compromising security.

In order to assign qualitative values to Confidentiality, Integrity and Availability requirements of the ground segment assets, a risk assessment methodology must be designed with security primitives based on mission operations. Such a methodology that suits space industry is developed. Problems related to patch management, certificate & key management, event correlation, malware and business continuity & disaster recovery are addressed.

Based on the experiences of the author in security standardization efforts, solutions provided in this paper would help ongoing and future security improvement activities in space organizations.

[1] ~~Ground Facilities Security Suppo~~rt Engineer, ICT Security Specialist, Swamy.Siram@vegaspace.com, Mobile: +49 17684260221

Table of Contents

I. Introduction

Compliance to ISO 27001 standard ensures that a continuous security improvement process is established and the resulting Information Security Management System (ISMS) fits with the organizational business needs.

Managed Information Security is not just about protecting infrastructure against computer hacking or viruses, but it has to cover all business processes of an organization. Good governance and a mature business model that avoids gaps in terms of security responsibilities are crucial for security of an organization's assets. To be able to protect the ground segment from a variety of threat categories, the ISO 27001 controls that cover different organizational units (not just IT department) need to be implemented to provide a comprehensive security protection against the risks posed by these threats.

Table 1. ISO 27001 controls coverage for various threat categories

Threat Category	Threat Samples	Related ISO 27001 Controls
Maligning organization's Image	System abuse, illegal implementations, disregard to organization's objectives	A.5 Security policy
Deviations in quality of service from service provider	Power, WAN issues	A.6 Organization of Information security
Unacceptable use of assets/Information leakage	Governance gaps, Sensitive documents on Internet	A.7 Asset management
Human Errors or failures	Misconfiguration, operator errors	A.8 Human Resource Security
Social Engineering/ Deliberate Acts of Information extortion	Blackmail of information exposure / disclosure	A.8 Human Resource Security
Deliberate Acts of Interception (theft)	Illegal confiscation of equipment or information	A.8 Human Resource Security
Deliberate Acts of sabotage / vandalism (physical attacks)	Destruction of systems / information	A.9 Physical and Environmental Security
Deliberate software attacks	Malware, Replay, Denial of service, Hacking, Traffic Analysis	A.10 Communications and Operations Management
Deliberate Acts or espionage or trespass	Unauthorized Access and/or data collection	A.11 Access control
Technical software failures or errors	Bugs, code problems, unknown loopholes	A.12 Information Systems Acquisition Development and Maintenance
Technological Obsolence	Antiquated or outdated Operating Systems/ Hardware/Technologies	A.12 Information Systems Acquisition Development and Maintenance
Technical hardware failures or errors	Equipment failures / errors	A.14 Business Continuity Management
Forces of nature	Heavy Snow, Wind, Fire, flood, earthquake, lightening	A.14 Business Continuity Management
Link Jamming	Radio Frequency Interference	A.15 Compliance (Legal, Policies, Standards, Technical Compliance, Audits)
Compromise to Intellectual Property	Invalid license, Piracy, Copyright infringements	A.15 Compliance (Legal, Policies, Standards, Technical Compliance, Audits)
All threat categories above	All threat samples above	In spite of all controls above, incidents might still happen which requires: A.13 Information security incident management

The mapping of typical threat categories with ISO 27001 controls that cover the risks originating from them in Table 1 depicts the need for addressing security in a comprehensive manner organization-wide. For example, 'document classification, labeling and handling' or 'compliance to the policy' are tasks that everyone in the organization have to perform. It is important for management to understand the ISO 27001 standard and its linkage to different business processes. If an organization is willing to initiate an ISO 27001 compliance project, it is strongly advised that the management involved attends ISO 27001 training at project inception. The training would help in few necessary compliance aspects that brings 'Top-Down' approach and also avoids questions like "If there is fire or power failure in control center, why is it linked to Security"? Or "If mission critical applications have software bugs, is it not taken care by software development team, why is it reflected as a security risk?"

The answer to these frequently asked questions is that any risk that has an impact on confidentiality, integrity and availability of an information asset, is considered as an information security risk, but the treatment of that risk can be addressed by existing business processes (e.g. Facility management in case of fire or power failure, Software development supplier in case of bug fixing). The ISO 27001 compliance initiative does not mandate creation of parallel processes to existing business processes, but it only complements them closing gaps if any.

The second part of this paper provides some guidelines to streamline business processes for the operation of a typical ground segment in a secure manner. The third part of this paper defines different classes of missions and guidelines for their efficient use of shared infrastructure without compromising security. The fourth part of this paper describes an example risk management methodology followed by the last part that provides some solutions for typical ground segment problems in achieving security improvement whilst complying to ISO 27001 standard.

II. Ground Segment Business Process Alignment to ISO 27001 Standard

A. Governance Model

Without a robust governance model, the risks identified cannot be mitigated. Before a process can be improved, the existing process needs to be clearly understood, defined and documented. Develop a robust governance model for the services offered within the defined ISMS scope that clearly specifies responsible persons for implementation of relevant ISO 27001 controls. The required steps to achieve this would include:

A.1) Collect documentation referring to existing business processes
A.2) With management support, obtain resources for business process review with existing process responsible
A.3) Define and document existing business processes into a business model
A.4) Ensure budget lines and existing organizational responsibilities are reflected in the model
A.5) Review related ISO 27001 controls for each process and agree on items that require existing process improvement. Related ISO 27001 control objectives and controls for a sample ground segment business model are provided in last column of Table 2. For additional guidance refer to ISO/IEC 27002:2005.
A.6) For each business process, ensure that the Service Provider(s) (Internal or Third Parties) involved are identified.
A.7) Ensure the customer base for each of the services is documented
A.8) Review the governance model to identify any gaps in processes & process responsible
A.9) Present the draft governance model to the customers, process responsible and service providers. Conduct workshops to increase awareness of the different parties involved and their responsibilities in running the organization and providing the services.
A.10) Keep the governance model up-to-date with feedback received, with changes in the ground segment, service portfolio, customer coverage, process responsible and any changes in their roles & responsibilities.

Table 2. Ground Segment Business Processes Alignment to ISO 27001

Process Category	Process groups	Typical Ground Segment Business Processes	Related ISO 27001 Control Objectives & Controls
Governance Processes	Service Strategy	Enterprise Governance	A.5, A.5.1.1, A.5.1.2
		Strategy & Objective Management	A.5, A.5.1.1, A.5.1.2
		Organization and management structures	A.6
		Capacity & Demand Management	A.10.3.1
		Financial Management	A.6.1.1
		QMS	Synergy with ISMS framework
		ISMS	All
		Technical compliance (Standards /Regulations)	A.15.2
	Continual Service Improvement	Performance Measurement	A.10.3.1
		Performance Reporting	A.10.3.1
		Training and Education	A.8.2.2
		Knowledge Management	A.8.2.2
Operational Processes	Service Design	Risk Management	All
		Business Continuity Management	A.14
		Maintenance and Engineering Concepts	A9.2.4, A.14.1.4, A.12
		Operations Concepts	A.12
		Infrastructure Requirements Management	A.12.1
		Operations Requirements Management	A.12.1
		External TT&C Services	A.6.2.2
		Setup and Management of Industrial Support	A.6.2
		Setup and Management of Organizations internal interfaces	A.6.2
	Service Transition	Inventory Management	A.7
		Asset Management	A.7
		Access Control	A.11
		Spares, Repairs and Calibration	A.9.2, A.10.3.2, A.12.5.1
		Packaging, Handling, Storage and Transportation	A.9.2.7
		Testing, Verification and Validation	A.12.2, A.14.1.5
		Maintenance	A.9.2.4, A.12
		Obsolescence Management	A.7, A.9.2.4, A.12
		Change, Configuration & Release Management	A.6, A.8.3, A.10.1.2, A.12.5
		Planning & Scheduling of Tracking Stations and Control Centers	A.10.3, A.10.3.1
	Service Operations	Control Center Helpdesk	A.10, A.11.2
		Incident Management	A.13
		Anomaly Management	A.13
		Problem Management	A.6, A.8.2.2, A.9.2.4, A.10.1.1,A.10.1.4, A.10.2.2, A.10.3.1, A.10.10, A.12.2.2, A.12.6.1, A.15.2.1

By the end of defining this governance model, the responsibilities of the ground segment services & infrastructure at control center and remote ground stations should be clearly understood. The responsibilities for mission operations, internal and external interfaces, infrastructure maintenance & operations for both hardware and software (including operating system and application software), should be clearly defined.

When this process alignment is completed, the ISMS processes can be perceived by everyone in the organization as a complementary process to existing business processes but not competing or parallel processes that does not

converge with reality on the ground. If that is not the case, the management should re-enforce the priorities or could put the ISMS activity on hold until the business processes are mature enough for such standardization.

Aligning the business processes to ISO 27001 controls helps ISMS implementations:

a. To be cost effective
b. Minimizes changes to organization
c. Reduces Δ implementations, no re-invention of the wheel (e.g. runs on existing procedures for change control, incident/anomaly management etc.)
d. Obtains support from people who run day-to-day business
e. Risks can be effectively managed
f. Security requirements can be addressed in normal ground segment engineering processes
g. Security becomes part of work culture

In the next sections, guidelines for aligning important business processes that improve security in the ground segment i.e. for Security Requirements Engineering, Asset Management, Change, Configuration & Release Management and Incident Management are provided.

B. Security Requirements Engineering in Ground Segment Definition

As part of Ground Segment Definition process, Ground segment customer requirements document (GSCRD), Mission description document (MDD), Mission operations concept document (MOCD), Space–to–ground interface control document (draft) (SGICD) documents are provided as input for ground segment requirements engineering. As an output of this requirements engineering process, the ground segment requirements document (GSRD) is generated as an elaboration of the requirements of the GSCRD.

In each ISMS cycle, risk assessment is conducted for operational ground segment infrastructure & services. Security measures that are defined to mitigate the identified risks or to reduce the risks to acceptable levels are stated as security requirements in Ground Segment Requirements Document (GSRD) for further implementation. The sub-system suppliers in turn would engineer implementation plans that fulfill these requirements. After implementation, security procedures are produced and used in routine mission operations by respective operations teams of each ground segment sub-system.

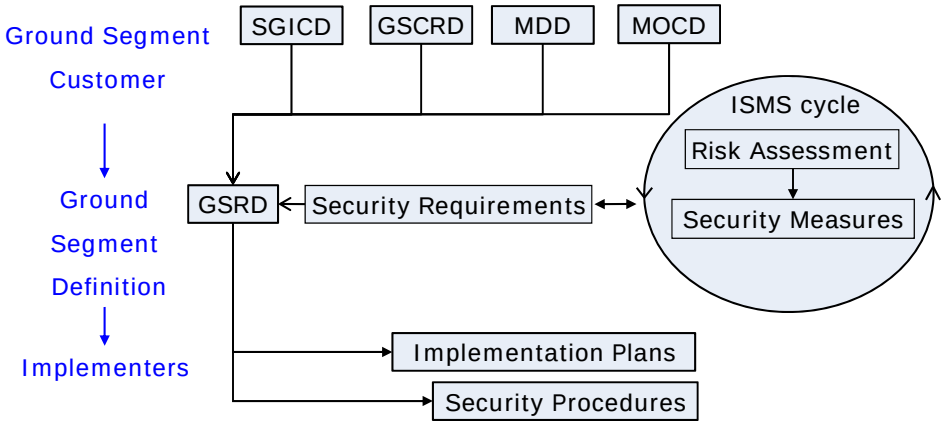

Figure 1. ISMS Link with Ground Segment Requirements Engineering

An example set of such security requirements that can be fed into GSRD are:

a. The inventory of all assets shall be maintained
b. Customer Mission security requirements from MDD, MOCD, GSCRD, and SGICD shall be addressed.
c. Documents and data shall be categorized to a suitable classification level, labeled and handled according to the level of protection required by that classification category
d. All operational roles shall have a prime and backup person nominated to ensure that the responsibilities can be carried out even in case of the absence of the prime responsible.

e. Sufficient physical security measures shall be put in place to ensure unauthorized users do not obtain physical access to the hardware
f. Communication protocols and ports shall comply with Implementation of Network Security Policies. Policy waivers shall be approved only after security assessment and for a limited period.
g. All software used shall have valid licenses and they shall be maintained in the inventory
h. Data and document distribution shall be controlled by the respective data and document owner
i. Release of media, hardware and equipment outside the Ground Segment premises for maintenance or repair or product evaluation shall be controlled
j. Proper means provided by the organization shall be followed when information and media needs to be destroyed
k. Only authorized removable media shall be used, personal devices shall not be used. These removable drives shall not be used prior to virus-scan and confirmation that the device is free from malware
l. Different privileges shall be configured for different roles (e.g. system administration, software maintenance, hardware maintenance, application administration, application user, mission operations team, ground operations team, flight dynamics team, mission exploitation team, simulations officer(s), QA, etc.)
m. User access shall be implemented based on mission operational requirements
n. In case of adverse use of the system or application, the identity of the user shall be traceable
o. The computer systems and applications shall log events which are monitored to ensure acceptable use and in case of incident handling
p. In addition, include specific requirements that treat the risks in the defined organization's ISMS Scope.
q. Security procedures that fulfill the above security requirements shall be prepared for their use by various sub-system operations teams
r. Auditing shall be performed to inspect that the security requirements are met and the evidence records shall be submitted to the ISMS team
s. The requirements and their corresponding implementations shall be reflected in the Statement of Applicability (SoA) of the defined ISMS Scope.

C. Asset Management

To build robust security for a ground segment, proper asset management is essential.

Asset ownership and responsibility of an asset for e.g. in terms of system administration, system management, change control, access control is crucial for the protection of the asset.

All organizations need to have a tool for effective management of assets and inventory. To address security aspects, the following typical requirements need to be implemented in the existing asset management tool for security management. The tool should be able to:

C.1) Identify & Implement user friendly method (e.g. a search function) to be able to identify computer systems in the Inventory

C.2) Search assets based on Supplier. This should help in identifying the organization responsible for the system administration of every computer system or network device. The organization owning the root/administrative privileges of the system ultimately owns the responsibility for system administration and the system security.

C.3) Include parameters listed below for network & system administration

a. Operating System
b. Patch level/Service Pack
c. Antivirus tool/product
d. Data backup/Spares
e. System responsible prime
f. System responsible backup
g. IP Address (for a system, multiple IPs should be able to be registered)
h. Hostname
i. Domain
j. MAC Address (for a system, multiple MACs should be able to be registered)
k. Subnet Address
l. Catalyst Location
m. Name

n. Drop ID
o. Speed
p. Duplex
q. Rack/ Patch Number
r. VLAN
s. Aliases

C.4) Register all software inventory:
a. Software Name,
b. Version,
c. Description,
d. Vendor,
e. Licenses (number of licenses that the key provides)
i. Copies (number of assets that have the given key assigned to the given application)
ii. Balance (=Licenses – Copies)
f. Installed on systems (computer systems list)

C.5) Includes fields for each inventory item for Obsolescence Management
a. Reliability
b. Availability
c. Maintainability
d. Supportability
e. Built Date
f. Installed Date
g. Market Availability
h. End-of-life Date
i. End-of-support Date
j. End-of-Service Date
k. Condition
l. Spares Situation
m. Comments
n. Impact
o. Work-around

C.6) Ensure obsolescence management process is linked with ground segment engineering (both sustaining and evolution)

C.7) Include inventory of all units in the organization, without any gaps.

C.8) Include classification level of each asset. Especially if the ground segment is used to operate High secure missions (III.A1.a). The access rules to the inventory & configuration of the assets should be based on the selected classification level. Based on the classification level, appropriate information handling rules for e.g. Personal Security Clearances, Encryption etc. needs to be adopted.

D. Change, Configuration & Release Management

Include security assessment in existing change, configuration and release management processes of the organization. The following procedure can be adopted to in the decision making process of a change request to keep the operational security overheads to the minimum:

D.1) The impact to security of the asset for which a change is being proposed needs to be assessed by the user requesting the change.

D.2) The change control board will take a decision whether to approve the change or reject the change based on the review of the risk assessment provided by the user. In situations when approvers require expert support for security assessment, they request the support from security experts for further assessment. Otherwise, the board can make a decision at this step which leads to step D.5).

D.3) The security experts analyses the input provided by the user, the board and provides the expert assessment briskly to ensure that delay in approval process (due to security assessment) is kept to minimum.

D.4) Based on the assessment, the approvers take a decision

D.5) The next task follows. I.e. either implementation (if decision is 'Approved') or update/withdrawal of the change request (if decision is 'Rejected').

Higher the efforts spent in security engineering process, lower the efforts that would be required to control operational security risks in change, configuration and release management.

E. Incident Management

What should an operator at ground station or at the control center do when a critical system is hit with a system compromise or virus infection or if there is WAN failure or if there is power failure or fire or a strike or vandalism etc.? No typical information security policies or security controls will guarantee total protection of ground segment information, information systems, services, networks or people. After controls have been implemented, residual weaknesses are likely to remain that may make information security ineffective and thus information security incidents possible. The following processes need to be followed to manage information security incidents.

E.1) **Incident Management Processes:** The four main distinct processes for information security incident management are:

a. Plan and Prepare
b. Use
c. Review
d. Improve

i. **Plan and Prepare:**

a. Incident Management Policy: The target objectives of incident management e.g. zero tolerance policy, sanctions for deliberate actions, roles & responsibilities of the incident handling teams need to be defined in the incident management policy. The roles should be officially nominated.
b. Tools & Procedures: It is important that teams involved in incident management prepare necessary toolkits for incident management. The procedures to follow and instructions on how to use to the tools should be made available for both the operations teams at the control centre and for the operations teams at ground stations. Sufficient testing should be done on regular basis to keep the tools up-to-date to deal with old & latest vulnerabilities. With tools and procedures in place, should incidents happen; the organisation will be in a better position to handle the incidents. Negligence in this preparation stage could cause severe damage to mission operations and their recovery time.
c. Define incident severity scales and encompass them within operations team's responsibilities. The incident reporting and escalation procedures should be clearly documented and followed by all operational teams.
d. Users should be made aware of incident handling procedure through briefings and/or other mechanisms, its benefits and how to report an information security event. Appropriate training should be provided to personnel responsible for managing the information security Incident management procedure, decision makers involved in determining whether information security events are incidents, and those individuals involved in the investigation of incidents.
e. The incident handling procedure should be thoroughly tested by all parties involved in this procedure and kept up-to-date.

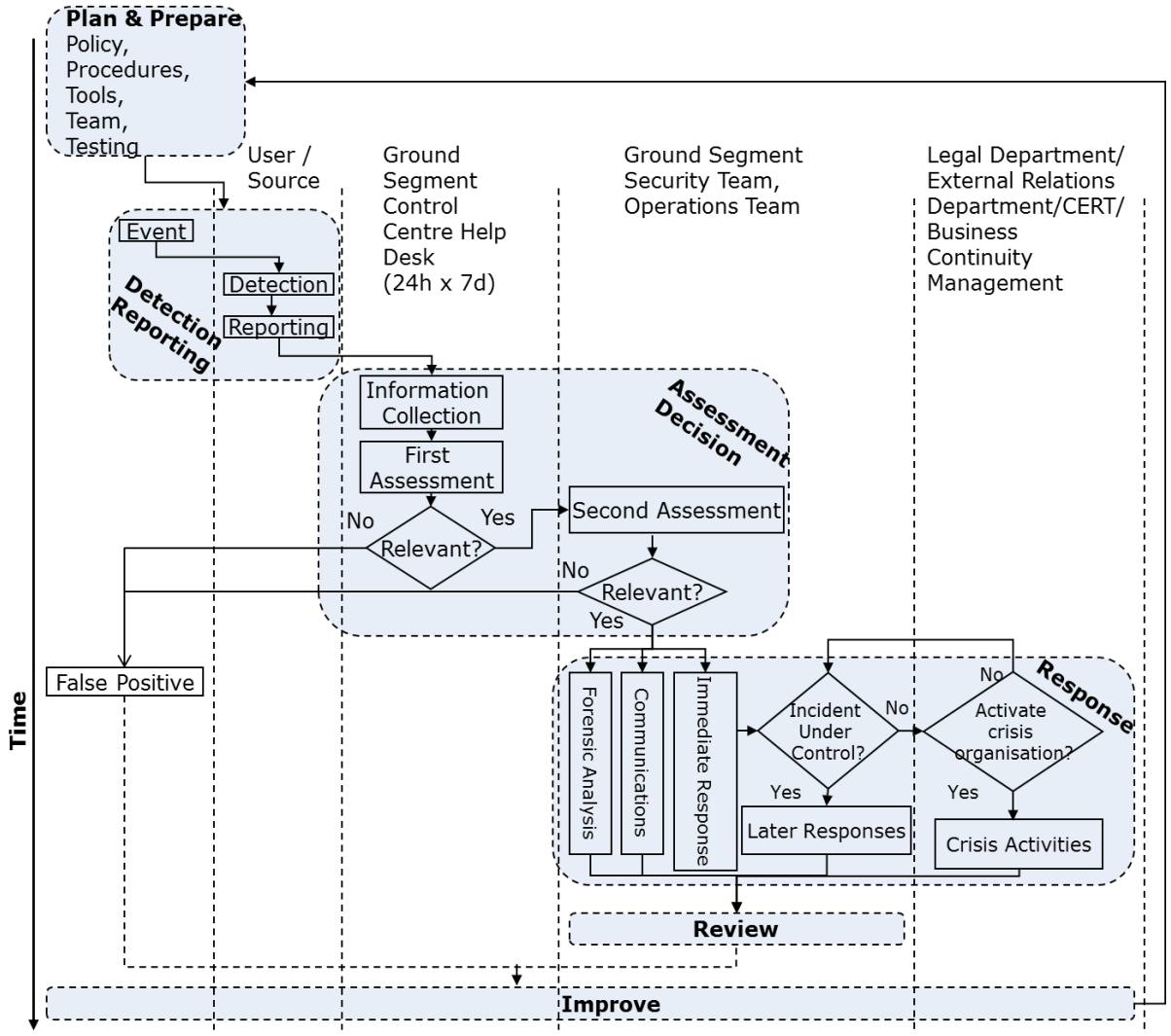

Figure 2. Information Security Event and Incident Flow Diagram

Information security events need to be monitored on a permanent basis. When an event turns out to be an incident[2], a pre-defined process as shown in Figure 2 will be handy.

ii. Use:

a. Event Detection & Reporting: Users or operational teams detects (by manual or automatic means) and reports the occurrence of information security events. Depending on the type of the incident e.g. physical security related, environment related or IT related etc., an appropriate reporting procedure is followed. Do not penalise the whistle blowers, instead encourage people to report incidents and reward them. It is always better those incidents are known from internal sources of the organisation than reading it in newspapers. When events are reported by external parties, communicate to them using organisation's official means and procedures.

[2] It should be noted that information security events could be the result of accidental or intentional attempts to breach information security controls, but in most cases an information security event alone does not imply that an attempt has really been successful and therefore doesn't need to have any implications on confidentiality, integrity and/or availability i.e. not all information security events should be categorized as information security incidents.

b. Event Assessment & Decision: Collect information associated with information security events, and does first assessment if the event is an incident or not. For example, a ground segment's security infrastructure could produce millions of events/day, not all are incidents. If it is a false positive, an incident is not raised. If the event is assessed as an incident, a ticket should be raised for operations teams to further assess and take appropriate actions.

c. Incident Response:
   1) Inform the relevant customer mission affected and assess the impact.
   2) Where information security incidents are under control, activities that may be required are conducted (for example, re-building compromised non-critical webserver).
   3) If information security incidents are not under control, 'crisis' activities (for example, a worm/virus spreading across Ground Segment and interrupting mission operations or activating failover procedures in cases of a disaster or major failure) are instigated. The respective organisational unit (e.g. Legal Department, External Relations Department, and Business Continuity Management Teams for recovery) shall be involved as appropriate.
   4) Communicate the incidents and relevant details thereof to internal and external people and/or organizations (This could include escalating for further assessments and/or decisions as required).
   5) Forensic analysis is conducted, the extent of forensics depends on the type incident and the damage caused. The forensic tool kits developed in "Plan and Prepare" phase will now be useful.
   6) All activities and decisions are properly logged for further analysis.
   7) Incidents are closed upon resolution. An incident report is prepared with the summary of all actions taken by all teams.

iii. **Review:** After information security incidents have been resolved, conduct the following review activities as necessary:

   a. Conducting further forensic analysis, if required.
   b. Identifying the lessons learnt from information security incidents and communicate for further processing.
   c. Identify improvements to security controls implementation.
   d. Identifying improvements to the information security incident management procedure as a whole, as a result of lessons learnt from reviews of the approach (for example, from review of the effectiveness of the processes, procedures, the reporting forms and/or the organizational structure).

iv. **Improve:** It is emphasized that the information security incident management processes are iterative, with regular improvements made to a number of information security elements in each ISMS cycle. These improvements will be proposed on the basis of reviews of the data on information security incidents and the responses to them, as well as trends over time.
   a. Measure security performance and effectiveness metrics
   b. Revise the existing information security risk analysis and input for management review
   c. Make improvements to the information security incident management procedures and its documentation.
   d. Initiate improvements to security, which may encompass the implementation of new and/or updated information security controls.

III. Shared Infrastructure

A.1) Mission Classes: Missions can be categorized into three different classes based on their Confidentiality (C), Integrity (I) and Availability (A) requirements. For example:

a. High Secure Missions: Missions that would need end-to-end TC/TM encryption. Typically these missions are critical for national infrastructure. E.g. Defense missions, Commercial missions, Missions handling classified information, etc.
b. Medium Secure Missions: Expensive missions that would need TC authentication or encryption but TM doesn't require end-to-end encryption. E.g. Navigation Satellites, Telecom Satellites etc.
c. Low Secure Missions: Research missions with un-encrypted TC/TM. E.g. Science Missions, Earth Observations missions etc.

Shared Infrastructure Concept: It is technically possible for missions with different classes use some elements of common infrastructure by following the guidelines below:

Policy compliance: Irrespective of which security class the missions belong to, the security requirements and their implementation of one class should not endanger the security of missions that belong to another class. Ground Segment preparation for each mission should ensure a harmonized approach according to organization's defined network security policies and industry standards. The common infrastructure service provider should ensure that the risks due to the use of shared infrastructure components are assessed and appropriate technical and procedural security controls are put in place. By policy, shared infrastructure component should be categorized to the highest level of classification level of the data processed/stored by that system and security controls are implemented according to that highest level.

Network Architecture: The key input for designing such a network architecture is the knowledge of network traffic matrix (assuming TCP/IP only networks: source, destination, port, protocol information) that is required for the operations of each mission. During design and validation phase of the ground segment, collect this information and test that the traffic matrix to be absolutely sure that none of the application's functionalities fail to work in operations especially if some functions are rarely used. The shared network infrastructure of an organization with high secure missions, can implement end-to-end network level encryption for their mission critical systems to avoid expensive re-development of mission critical applications. For encryption, use VPNs, SSL tunnels, etc. For network authentication and network access control, use port authentication. Segregate networks where common infrastructure components are not required. Isolate mission dedicated networks with different VLANs and manage security between the VLANs with Access Control Lists. Use tools that allow the mission operators to administer the ACLs effectively.

System Sandboxing: Build and use certificate-based encryption, signing and system access control solutions. Where a single system is used by missions with different security classes, ensure that shared logins are not used between missions. Ensure that operators obtain Personal Security Clearances of the highest classification level of the information processed/stored by that system. Sandbox application area, data area and system area for each mission class by jailing them and making it extremely difficult to hop between the mission classes.

Risk Monitoring: Monitor both network and systems closely on a daily basis, preferably by automatic means (e.g. File Integrity, Log Correlation tools etc.) to ensure that any policy violations are detected timely and actions are taken. Especially, the high secure missions cannot afford to have lax security due vulnerabilities introduced into the shared system by low secure missions or vice versa.

IV. Risk Management Methodology

Important principles in choosing a risk management methodology for the defined organization's ISMS Scope:

a. Keep the methodology 'Simple'. Risk assessment results should be consistent and reproducible.
b. Use existing risk management process of the organization to the extent possible
c. Select security primitives that are relevant for mission operations
d. Review the methodology with typical risk owners and management
e. Obtain management approval for the methodology and risk acceptance criteria. It should support management in decision making and investment planning based on risk prioritization.
f. The risk assessment tools should be easy to use in day-to-day operations
g. After implementation of risk treatment plans ensure status of residual risk is reviewed by management
h. Ensure information related to incidents/anomalies is accessible to roles who have the responsibility for risk identification & risk communication
i. Risks should be formally accepted only by risk owners. If a new risk is identified, it should be communicated to appropriate management level so that an action plan can be initiated immediately.
j. Ensure a level of independent review of Information Security in risk management

A sample risk management methodology is described in the next sections.

A. Sample Risk Management Methodology for a Ground Segment

Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication. It is conducted periodically throughout the life cycle of the ground segment service operations to ensure that new risks are adequately addressed. The roles and responsibilities for each step in the risk management are clearly defined in Table 3. There are several tools available for risk management in the market, but a simple excel sheet is used in this methodology.

Table 3. Roles & Responsibilities in Risk Management

Risk Management Task	Role	Responsibility
Risk Management methodology	ISMS Team	Preparation of the methodology Review
Risk Assessment	ISMS Team	Periodically conduct Risk Assessment Review of the Risk Assessment report
Risk Treatment	ISMS Team, Implementation Teams	Risk Treatment Plan Suggestions on Risk treatment options
Management Review & Approval	Management	Risk acceptance criteria Residual risk Acceptance Decision on Risk treatment options, Approval.
Risk Communication	ISMS Team	Reporting risks User interface Follow Escalation process
ISMS	ISMS Team	The output of this risk management process is taken as input for other ISMS processes

A.1) **Asset Identification:** Identify and list all the Ground Segment assets.

A.2) **Asset Valuation:** Asset Valuation is done based on the Table 4. The Asset values assigned shall be reviewed and agreed by the asset owners. A simple scale from 1 to 4 is assumed. Note that columns in the following table are not to be interpreted as mutually dependent.

The Asset Value (V) of an asset item is the maximum of values given for Confidential (C) or Integrity (I) or Availability (A). $V = \text{Max}\{C, I, A\}$.

Which means security is given priority for an asset even only if one of the C, I, A requirements is high (safe option). For e.g. a webserver on DMZ that is not used for mission operations could be of asset value 1. But mission control system could have an asset value of 4.

Table 4. Security Primitives for Asset Valuation

C,I,A Values	Confidentiality	Integrity	Availability
4	Information of highly sensitive nature whose unauthorized disclosure is either disadvantageous or harmful to the national interests of the organization	Non-recoverable loss of integrity that may have permanent effect on achieving mission objectives and organization's reputation.	Non-recoverable unavailability that directly affect achieving mission objectives and organization's reputation.
3	Information of sensitive nature whose unauthorized disclosure affects organization's reputation and needs additional security measures to protect access to it.	Recoverable loss of integrity of information that may affect achieving mission objectives temporarily.	Recoverable unavailability that may affect mission objectives.
2	Information of less sensitive nature whose unauthorized disclosure doesn't affect organization's reputation.	Recoverable loss of integrity of information that may not affect mission objectives.	Recoverable unavailability that may affect achieving mission objectives temporarily.
1	Information that can be disclosed to public.	Non-recoverable loss of integrity of information that may not affect mission objectives.	Unavailability may not affect mission objectives.

Without a level of aggregation in assets, the list would become unmanageable and difficult to review. So, for simplicity, the assets could be categorized into groups based on the similarities in the following criterion:

a. Type of function or services delivered by the asset
b. Asset owner
c. Classification/Confidentiality (C), Integrity (I) and Availability (A) requirements
d. Usability as Evidence Record for ISMS
e. Level of applicability of vulnerabilities and threats
f. Type of Risk Treatment Option & Risk Mitigation Procedure
g. Budget lines & relevance to organizational structure
h. Auditable

A.3) **Risk Identification:** Risk identification is the most important aspect of providing security for an organization. This responsibility is normally assigned to trusted, trained and experienced security engineers, who should be fully aware of the ground segment infrastructure & services, their vulnerabilities, news/events/incidents/anomalies that are happening and their role is crucial for identifying risks at an early stage before the threat causes serious damage to mission operations.

A.4) **Risk Evaluation:** A qualitative approach is chosen for Risk Evaluation for Ground Segment. This approach is chosen to suit the mission operations environment. The quantitative approach is not practical to attempt to execute without extensive input feed from all staff, a recognized automated tool and associated knowledge base including all financial details is a must. Even then, the exercise will be overly difficult to complete. On the other hand, the advantages with this qualitative approach are:

a. Calculations are intuitive, readily understood and executed
b. It is usually not necessary to determine the *monetary* (Euro) value of information (its availability, confidentiality and integrity).
c. It is not necessary to determine quantitative threat frequency and impact data.
d. It is not necessary to estimate the cost of recommended risk mitigation measures and calculate cost/benefit because the process is not quantitative.

e. A general indication of significant areas of risk that should be addressed is provided.

The following formula is used to calculate the qualitative risk:

Table 5. Risk Evaluation Formula

Risk (R) = Threat Level (T) x Impact (I_m) x Annual Rate of Occurrence (ARO) x Asset Value (V) i.e. $R = T \times I_m \times ARO \times V$, where T, Im, ARO, V are the risk factors. $NRV = R / R_m$, where R_m is the Maximum possible risk value.

Threat Level Analysis: Security threats to assets depend on the type of mission for which the services are provided. The purpose of the mission data, the system's deployment and access are important factors in threat analysis. Assign Threat levels for each asset in the defined ISMS scope based on the list of projects (missions) supported, their type (phase), connectivity, user base, organisation's own mission or 3rd party or Joint Mission and Mission category (Defence, Navigation, Research, etc.)

Table 6. Threat Level Definitions

Criteria	**Threat Level <0 – 1.0>**	**Comments**
No. of Projects		
support for 1 Project	0	Shared Infrastructure provides services to multiple missions. More missions supported, more is the threat
support for multiple Projects	0.1	
Network Connectivity		
Connected to secure networks	0	Threat level increases for systems with lesser level of protection provided by the network perimeter security.
Connected to External Networks (facing internet)	0.1	
User base, Application is accessible to		
Internal Users Only	0	Threat level increases with user remoteness. Less control over the user actions, more the threat.
Internal & External Users	0.1	
Used in Mission Phase		
System Definition Only (Phase O/A and B: Feasibility Study, Preliminary Design)	0	Threat level increases with the operational nature of the mission phase.
Ground Segment Implementation (Phase C and D: Detailed Design, Development, Validation)	0.1	
Mission Operations (Phase E and F: LEOP and Routine)	0.2	
Used by organisations mission/ 3rd Party (Reputation)		
Organisation's own Mission	0	Threat level increases when reputation is at stake for the organisation, 3rd party or even higher if it is for both (joint missions).
3rd Party Mission	0.1	
Joint Mission	0.2	
Mission Category		
science missions or meteorological satellites	0.1	Threat level increases with the purpose of mission data (research - less threat, applications - more threat), orbit used (Deep space - less threat, LEO - more threat) and risk to life
manned space flight	0.2	
navigation satellites or communications satellites	0.3	
Threat Level for the asset = ∑(chosen value for each of the above criteria)	Between [0 – 1]	

It is clearly seen that the threat levels are high for systems supporting multiple missions i.e. for shared infrastructure and are accessible to external users or on external network. Following criteria can be used in determining the threat levels:

Science missions risks are much less than those missions where life or infrastructure may be disrupted. In the case of science missions, while money was spent to gather the information, only the monetary investment and the data collection will be lost. Whereas in communications satellites, navigation satellites and human spaceflights, the loss of satellite systems would result not only in loss of investment Euros; there would also be the high potential for the loss of life, safety, and infrastructure. Failure of human space flight might result in loss of few lives, but failure of navigation or communication to a ship carrying thousands of people might depend on the signals from Navigation satellites or communication satellites and so are assigned with higher threat level than the human space flight.

For example, Threat level for SLE service provider is:

Table 7. Assigning threat levels to assets - an example

Criteria	**Threat Level <0 – 1.0>**	**Comments**
No. of Projects		
support for multiple Projects	0.1	Shared Infrastructure provides services to multiple missions. More missions supported, more is the threat
Network Connectivity		
Connected to secure networks	0	SLE service provider is normally located in relatively protected mission critical networks, so gets the value 0 for this criterion.
User base, Application is accessible to		
Internal & External Users	0.1	The SLE application is used by both internal users for organisations own missions or by external SLE clients for external missions, so gets a 0.1 value for this criterion.
Used in Mission Phase		
Mission Operations (Phase E and F: LEOP and Routine)	0.2	SLE is used for mission operations, so gets value 0.2 for this criterion.
Used by organisations mission/ 3rd Party (Reputation)		
Joint Mission	0.2	Can be used for own/3rd party or joint mission, so gets 0.2 value for this criterion.
Mission Category		
navigation satellites or communications satellites	0.3	SLE services can be used for any mission category, so gets 0.3 value for this criterion.
Threat Level for the asset 'SLE service provider' = ∑(values of all the above criteria)	(0.1+0+0.1 +0.2+0.2+ 0.3) = 0.9	SLE security is important considering the high threat level.

Impact Analysis: Impact level is chosen based on the potential damage to mission operations:

Table 8. Impact Level Definition

Impact Level	0	1	2	3	4	5
Result	No impact	Procedure change	Config change	Missed non-critical TM	Missing Radiometric measurements (Ranging,etc.)	Missing critical TM

Impact Level	6	7	8	9	10
Result	Missing non-critical Pass (TC&TM)	Missing Critical pass (TC&TM)	Safe Mode for ≤ 3 days	Safe Mode for >3 days	Loss of spacecraft

The risk factor's definition and their range of values are described in the table below:

Table 9. Risk Factors Definition and Value Range

Risk Factor	**Definition**	**Value Range**
Risk (R)	Combination of probability of an event and its consequence	[0 – 40]
Threat Level (T)	The probability of potential exploitation of an existing weakness or absence of security counter measure; i.e. potential exploitations of an existing vulnerability.	{0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1.0}
Impact (Im)	The result of an unwanted incident	{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10}
Annual Rate of Occurrence (ARO)	Probability of such a risk happening in one year. For instance, if an event definitely happens once in a year, then its value is 1. If an event is probable to happen once in 10 years, then the ARO value is 0.1	{0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 10}
Value (V)	Asset Value of the item. It indicates the importance of the asset in terms of Confidentiality, Integrity and Availability on a scale, 1 is least valuable and 4 is most valuable.	{1,2,3,4}
Normalised Risk Value (NRV)	NRV Risk on a scale of 0 to 1. Scaling allows consistency in Risk Valuation even if other risk factors and their ranges are changed in future.	[0 – 1]

Value Range:

a. The values of Threat and Annual Rate of Occurrence can be decimal values.
b. The Impact value is an Integer between 0 and 10. {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10}
c. The Asset Values (V) are 1 or 2 or 3or 4
d. With these possible value ranges, the maximum risk value is 40 and the minimum risk value is 0.
e. Normalised Risk Value (NRV) is between 0 and 1

A.5) **Risk Acceptance Criteria:** The risk acceptance criteria indicate up to which level management is willing to accept the risks. In the current risk assessment approach, this is the Normalized Risk Value (NRV), the value in the last column as shown in Table 8.

All risks below this NRV value are considered acceptable to management and no actions are required to be taken to mitigate these risks.

The risk acceptance criteria for the Ground Segment Information Security is:

a. All risks with NRV **< *0.20*** are acceptable.
b. All risks with NRV **≥ *0.20*** are treated.

This Risk Acceptance Criteria is subject to change according to the mission and security requirements and as decided by management.

It is often the case that the risk acceptance criteria value is increased if the budget allocated for security improvement is limited. In that case, the risk owners are knowingly and willingly accepting higher level of risks in This Risk Acceptance Criteria is subject to change according to the mission and security requirements and as decided by management.

It is often the case that the risk acceptance criteria value is increased if the budget allocated for security improvement is limited. In that case, the risk owners are knowingly and willingly accepting higher level of risks in their goal to achieve mission objectives which is the core business for the ground segment. For missions with strict security requirements, the risk acceptance criteria value is normally kept lower.

A.6) **Risk Treatment:** When the risks have been identified and assessed, the Risk Assessment Report is prepared as a summary of the risk assessment. Based on the risks, a Risk Treatment plan is prepared, which is to identify and evaluate the most appropriate action of how to deal with these risks. This decision shall be made based on the assets involved and the impacts on the mission. Another important input into this decision is the acceptable level of risk that has been identified by Risk Acceptance Criteria.

For the identified and assessed risks, there are four possible actions an organisation might want to take:

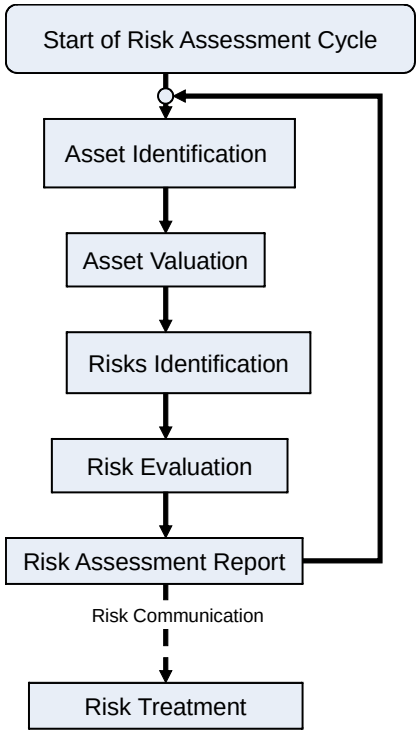

Figure 3. Risk assessment approach

a. Reducing Risks: Applying appropriate controls to reduce the risks

b. Accepting Risks: Knowingly and objectively accepting risks, providing they clearly satisfy the ISMS Policy and the criteria for risk acceptance

c. Avoiding Risks: Risk avoidance describes any action where assets are moved away from the threats (e.g. physical areas or mission processes). This can, for example, be achieved by:
   i. Not conducting certain mission activities (e.g. not processing "classified" information through shared infrastructure)
   ii. Moving assets away from an area of risk (e.g. moving a particular service management to a different service manager); or
   iii. Deciding not to process particularly sensitive information, e.g. with third parties, if sufficient protection cannot be guaranteed.

   When evaluating the option of risk avoidance, this needs to be balanced against mission and monetary needs. For example, it might be inevitable for the organisation to use the Internet because of mission demands, despite of all their concerns about hackers, and it might be not feasible from a mission operations point of view to move certain assets to a safer place. In such situations, one of the other options, i.e. risk reduction or risk transfer, should be considered.

d. Transferring Risks: Risk transfer might be the best option if it seems impossible to avoid the risk, and it is difficult, or too expensive, to achieve appropriate reduction of risk. For example, risk transfer can be achieved by taking out insurance to a value commensurate with the assessed asset values and related risks, taking also into account the importance for the ground segment service. Another possibility is to use third parties or outsourcing partners to handle some of the ground segment services if they are suitably equipped for doing so. In this case, care should be taken that all security requirements, control objectives and

controls are included in associated contracts to ensure that sufficient security will be in place. What should be kept in mind is that, in many cases, the ultimate responsibility for the security of the outsourced information and information processing facilities remains with the organisation.

For each of the risks, these options should be evaluated to identify the most suitable one. The results of this activity are documented, communicated to all parties involved and finalised in a risk treatment plan document.

A.7) **Selection of Controls:** In order to reduce the assessed risks within the scope of the ISMS being considered, appropriate and justified security controls should be identified and selected.

The aim of control selection is to reduce risks to a level that is acceptable for the organisation. This selection shall be supported by the results of the risk assessment, for example, the vulnerabilities with associated threats indicate where protection may be needed, and what form it should take. Especially for the purpose of certification, the selection (or otherwise) of the controls is to be documented in the Statement of Applicability.

Already implemented controls can be re-examined in terms of cost comparisons, including maintenance, with a view to removing or improving them if they are not effective enough. Here it should be noted that sometimes it is more expensive to remove an inappropriate control than to leave it in place, and may be add another control and/or gradually phasing out and decommission the old one. This is a continuous process, so previous risk assessment reports shall be included and reviewed in each cycle.

A.8) **Management Approval:** Management shall approve the risk treatment plan, provide sufficient resources and prioritise implementation of the risk treatment plan. The rapid implementation of the approved risk treatment plan is crucial for improving the security standards of a ground segment. As part of the management review, residual risks need to be formally accepted by management. Residual risks are the perceived risks remaining after the risk treatment process or risks that were below the risk acceptance criteria.

Upon management approval, the output from the Risk Management process is fed into the continuous ISMS life cycle.

A.9) **Risk Management Examples:**

Table 10. Risk Management Examples

Risk Description	**Threat Description**	**Threat Level (T)**	**Impact (Im)**	**Vulnerability Description**	**ARO**	**Asset Value (V)**	**NRV (R/ Rm)**
MissionX_ASSET # 00001: SLE Service provider authentication information							
Disruption in TC/TM	Unauthorised use of equipment during scheduled pass	0.9	7	Failure of access controls	0.5	4	0.315
Failure of communication to prime Ground Station	Operator Error	0.9	2	Missed training	0.5	4	0.09

Example 1: For an asset “SLE service provider authentication information”, due to failure of access controls likely to happen once in two years, the authentication information for SLE connectivity is disclosed and if it was abused by an external hacker who obtains unauthorized SLE connection that denies legitimate connectivity for a scheduled critical pass which resulted in disruption of TC/TM of a spacecraft, the normalised risk value for this event is calculated to be 0.315, which is above the risk acceptance criteria (0.2). That means this risk needs to be treated. The risk treatment option for example could be to communicate SLE authentication information to partners is an encrypted E-mail, not in clear text.

Example 2: For the same asset "SLE service provider authentication information", if the spacecraft operator misses a training session likely to happen once in two years, that results in operator error of the configuration file which impacts only the prime ground station and upon realising the configuration error, the operator re-configured the job to use backup station that resulted only in communication failure to the primary ground station, the normalised risk value for this event is calculated to be 0.09, which is below the risk acceptance criteria (0.2). That means this risk is acceptable and no actions need to be initiated.

V. Solutions for Typical Problems

Typical challenges for ground segment security are:

a. Remoteness of Ground Stations and data dissemination networks
b. Sites located globally (local vs central monitoring, time zones)
c. Issues with cross-agency support, integration, release management (global customer base, different standard implementations)
d. Reaction Time is low (pass durations)
e. Critical nature of operations (especially during critical maneuvers and emergency support)
f. Long duration missions (obsolescence management)
g. Difficult to fully replicate a ground segment for validation purposes (limited simulators)

With these known challenges, continuous efforts to find technical solutions are necessary. Few technological guidelines are provided in the next sections:

A. Patch Management

If proper vulnerability assessment and patch management is not done, the systems become inherently weak and when perimeter security fails to prevent the threats, the systems could be compromised by attackers. Without appropriate patch management the risks posed by software vulnerabilities needs to be well managed. Where possible, by patching, if not, by other workarounds. Unpatched and vulnerable systems are a significant risk to the ground segment. Either risk mitigation measures or risk reduction measures can be implemented to ensure operations are not disrupted:

a. Review & Improve vulnerability assessment and patch management practises
b. Obtain latest security vulnerability and patch information from vendors, online vulnerability databases and other resources as appropriate.
c. Assess the impact of these vulnerabilities on the data system
d. For the mission applications in development:
    i. The data system's design shall ensure that the applications can be gracefully patched (both Operating System and application patches) and maintained without major impact on operations.
e. For mission applications in operations:
    i. Where possible, patch the system vulnerabilities after (mini-)validation in test environment and then rollout into operational systems. Ensure co-ordinated effort amongst all the 3 software layers i.e the core application, COTS and Operating System Baselines managing the risk due to identified vulnerabilities by patching.

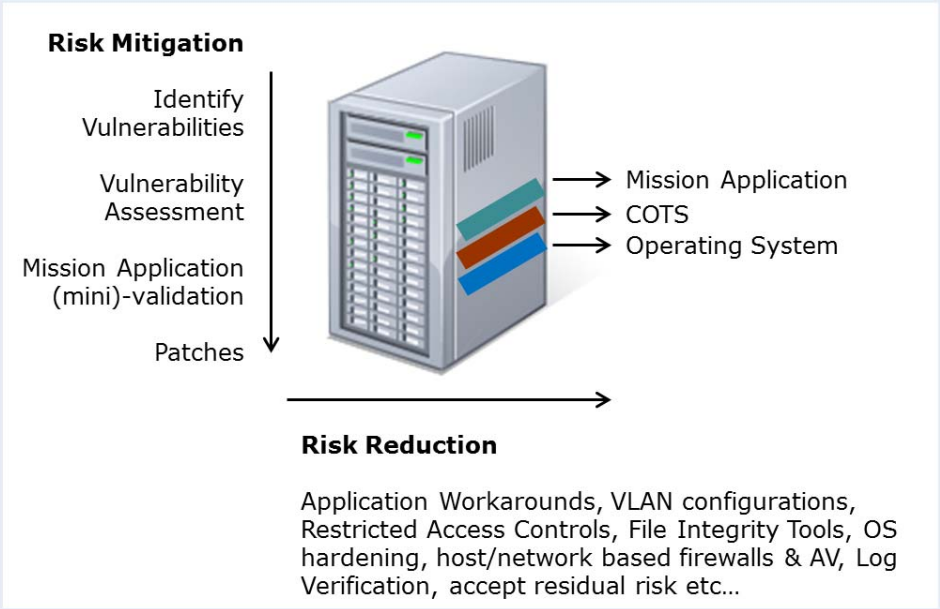

Figure 4. Patch and Vulnerability management

ii. Where the system cannot be patched, implement workarounds and reduce the residual risk to acceptable levels. Application level workarounds, operating system level and network level controls like improved VLAN configurations, Access control Lists, File Integrity tools, OS hardening, host/network based firewalls, Log Verification etc., can bring defence-in-depth where exploitation of the vulnerability becomes extremely difficult.

B. Certificate & Key Management

Certificate & electronic key management is a must for High and Medium Secure mission classes (III.A.1.a, b). Few guidelines are provided to engineer certificate services solution:

The following essential elements should be addressed in defining certificate management solution:

a. Legal and Regulatory requirements with respect to hosting nations of the ground segment shall be identified and complied with for key management solutions.
a. Users that work with technical workstation or an authorised personal device
b. Use of certificates by groups, functional entities, shared mail accounts (to avoid misuse, additional risks in not being able to identify end-user needs to be addressed)
c. Certificate Expiry and Renewal
d. Certificate Backup and Recover to and from Certificate Archive
e. Certificate Revocation
f. Support for master key escrow by Master Key Controllers
g. Multi-factor authentications can be defined to allow users and functional entities/groups to be equipped with a public trusted certificate.

When users join, leave or move within the organisation, their certificates needs to be revoked. Certificate revocation is an extremely important capability, as this is the primary means by which user certificates are removed from the Certificate Services solution. Revoked certificates should be placed on a certificate revocation list (CRL), which is then distributed through a public directory (typically the same directory as the valid public key certificates). It is important to note that merely publishing a CRL is not sufficient; the appropriate application security software (authentication module either on the server or independent) must verify whether a certificate is still valid by checking the CRL. Certificate revocation is also necessary when a user loses their private key material, or such material is otherwise compromised, stolen.

For high secure environments, certificate services solution would need following components, but depending on the specific mission application requirements, few components can be merged.

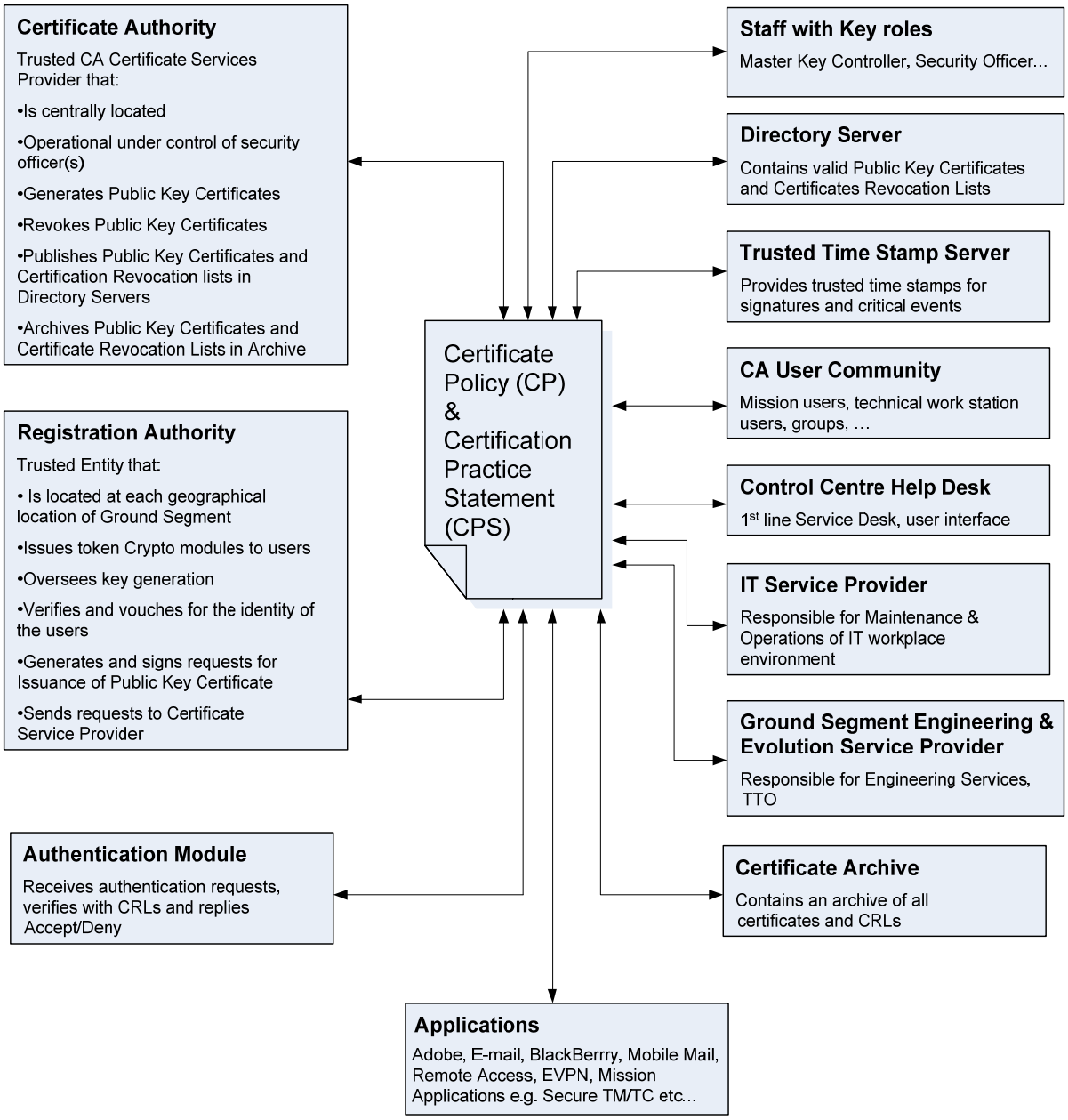

Figure 5. Certificate Services Components

A.10) **User enrolment:** The following essential elements should be addressed in defining a solution for ground segment wide user enrolment

a. The user is sufficiently validated before offering the services
b. Means for the users to establish trust in the CA service provider are presented
c. Effective communication from control centre help desk
d. Friendly and easy to use user interface
e. Documentation including user manuals, FAQ
f. Training aspects for users and for CA administrators & relevant M&O teams

Options for Automated central certificate storage (e.g. in LDAP directory, Active Directory etc.) that allows seamless use of the certificates by various applications (Adobe, E-mail applications, Blackberry, mission applications etc.) in a secure manner shall be analysed. If possible integrate directory services with certificate services solution.

Private CA Certificates: Access to applications that are critical for day-to-day secure mission operations needs to be highly available at all times. When such access is disrupted due to integration of certificate based authentication, it would not help the missions cause. The risk of using completely outsourced CA Certification Services using Public Certificate Authorities is that when their services are not available, mission applications become un-accessible. However, Strict SLAs with service provider and offline authentication could reduce this risk but this is design option that needs to be further analysed. On the other hand, an organisation's own private Sub-CA (whose root CA is signed by public CA) delivering certificate based authentication services would be a better option.

Secure Private Key Management: The private key is the most sensitive component of the public key cryptography. Theft of private key means that the user can be impersonated in electronic communications, documents or transactions. Besides risk of fraud, there is the cost of recovery. If the private key of the organisation's CA were lost or stolen, all the certificates in the hierarchy that have been signed by that CA are invalid and would need to be reissued. When deployed organisation-wide, this can be an onerous task, and the security of a private key is paramount. To mitigate this risk, Hardware Storage Modules (HSM) for e.g. like Smart cards, peripherals, modules, PCMCIA cards can be used.

Application Access Control: A fully functional access control system is vital in order to successfully enable an existing legacy mission application to support Certificate Services Integration. There are some central functionalities and features required in the solution:

a. X.509 Certificate-based access control
b. Single sign-on capabilities for login information
c. Multiprotocol revocation control
d. LDAP support for access to data integrity configuration parameters and authentication information in a directory server
e. Support for hardware cryptographic accelerators and key storage

Figure 6 illustrates the access control aspect of a fully certificate services enabled system, with optional means of authentication.

Access Control Server: Typically a SSL gateway with extended PKI capabilities to be used by any client-server application to achieve strong encryption, revocation control and PKI-based access control. TLS/SSL provides a platform for a generic SSL server-side tunnel that can be applied to any static TCP protocol.

Single Sign-On: The single sign-on (SSO) feature allows a user to log onto the network once and gain access to all authorised services such as web portals, E-mail, some mission applications etc. The SSO feature acts as middleware between users and applications; for instance, the SSO performs a certificate based authentication and authorisation for that user and then via LDAP provides username/password logon to an application. SSO improves reliability and performance, since the SSO system can log on faster with fewer errors than a user can. SSO improves productivity, since users don't have to go through logon sequences. It can be implemented at various security levels, based on the type of authentication, without modifying the back-end applications.

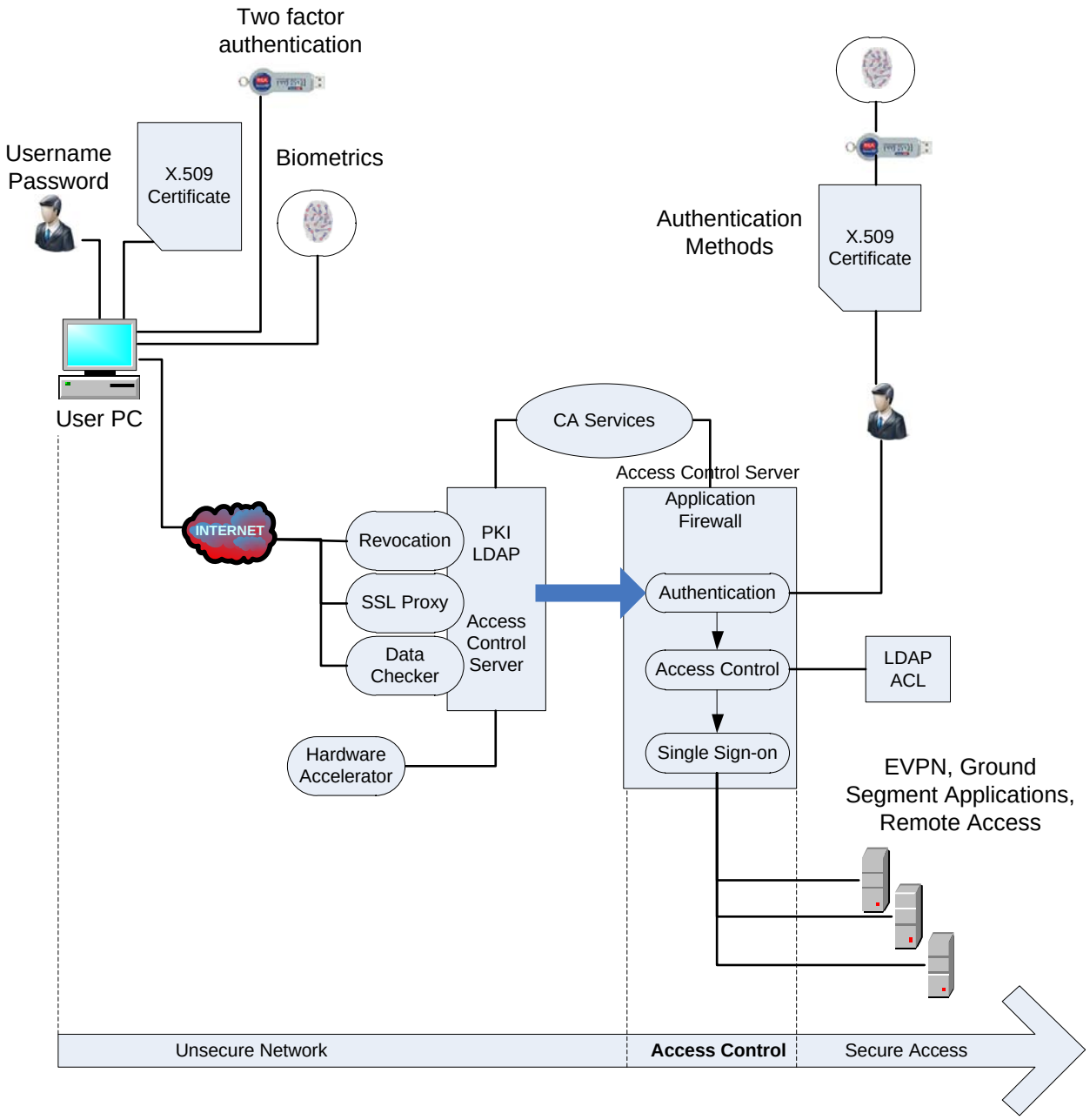

Figure 6. Client-Server components for Certificate based Access Control System

Digital Signature Verification Server: It contains the digital signature, the certificate, the revocation control time stamp, the transaction time stamp and the data both before and after signing. It fulfils digital signing requests; enforce time limits on the transactions. Implementing digital signing functionality as a separate module makes it easier to integrate functionality with legacy applications.

Authentication to access the Remotes Access Services (EVPN): The certificate based authentication works very well with several COTS EVPN solutions and which can provide even three factor authentications or more.

Authentication to access the workplace (physical and virtual): With integration of the CA certificate services and the Directory services, this task can also be achieved with low complexity.

Authentication to access the Mission Applications: Similar to digital signing solution, this one is also of high complexity as it involves several legacy applications and their support for certificate based authentication needs to be verified. The integration of certificate based authentication into web-based applications should be relatively simple. Other applications will need to be studied before estimating their complexity.

Based on the chosen certificate services components and their configuration, prepare a Certification Policy and Certification Practice Statement (CP&CSP) that makes it an essential infrastructure component of a secure ground segment.

C. Event Correlation

It is not humanly possible to conduct manual log verification of all systems in the ground segment daily. Several log correlation solutions are available in the market to help in this aspect. Evaluate various technologies, their limitations and their suitability for operational environment of the ground segment.

a. Obtain configuration information of logging mechanisms on existing systems
b. Define strategy for implementation
c. Send all logs to server; do not filter on the client systems. If bandwidth between ground stations and control center is an issue, select distributed log server architectures that ensure local processing before clogging the WAN link.
d. Logic should be decided on the log correlation server not on client
e. Introduce intelligence into the tool with mission operations experience
f. Provide consoles at grounds stations and at control centers so that operators can be timely alerted
g. Reduce false positives before deployment of technical solution into operations. Too many alerts means that M&O teams would disregard alerts.
h. Ensure acoustic alarms for critical events

This solution if implemented correctly would improve not only security but also the performance of the ground segment services to its customers as symptoms of anomalies can be detected early and actions can be taken before the events become problems.

D. Malware

Due to increased network based applications, Malware (Viruses, Worms, Trojans, etc.) have reached not only ground segment but also space segment. Malware has been well known problem for every organization and ground segment is no exception. In addition to technical solutions, procedures that ensure office etiquette are a must to fight against this constant menace.

Deploy multi-faceted antivirus solutions that include both host-based central antivirus solutions and network based antivirus solutions. Especially due to the nature of ground segment operations and the challenges in this environment, not every system can be patched and kept up-to-date. There could be mission applications/devices where antivirus software cannot even be installed. In such cases, a network based antivirus solution would provide sufficient protection.

Some additional guidelines to protect the ground segment from malware are:

a. Do not run day-to-day operations with system administrative privileges
b. Control use of removable media (e.g. USB stick, USB hard drives etc.)
c. Strictly enforce Internet usage policies
d. Avoid use of personal media
e. Request virus-free certification prior to connecting third party devices into your network
f. Control propagation of malware from general corporate network into Missions Critical Networks or vice versa
g. Test tools for recovery and rescue
h. Ensure security policies are respected in design, engineering and deployment
i. Keep signatures up-to-date. Verify & troubleshoot issues for systems that do not receive latest signatures

j. Select different client policies to minimize impact on the system performance for systems running mission critical applications
k. Ensure signatures are also updated during mission Freeze periods
l. If central solution cannot deliver signature updates, obtain the latest signatures by Live update or by manual intervention.
m. Reporting false positives, issues if any to AV vendor
n. In spite of all the above controls, incidents might still happen, keep your incident management procedures ready.

E. Business Continuity & Disaster Recovery

It is often difficult to answer questions like; do we need a back-up control center? If so, to what extent do we need to build the infrastructure in the backup center? What is my ground segment Recovery Time Objective (RTO)? What is my ground segment Recovery Point Objective (RPO)? In case of my customer spacecraft emergency, within how many minutes do I have to re-plan my ground station scheduling and for how long does this customer might need my ground station as a backup, etc.?

These kind of questions can only be answered by reviewing the customer mission's business continuity requirements and their mission planning. Some guidelines are provided below:

a. Obtain the ground segment business continuity requirements from customer point of view for running mission operations and define the scope and BCM Policy for that ground segment.
b. Conduct Business Impact Analysis of the ground segment based on these customer requirements and plan for implementations if any.
c. Prepare or Update existing Contingency Recovery Plans and procedures.
d. Conducting tests/drills, which could even be table top exercises where experts meet and do a dry run of typical scenarios and analyze the effectiveness of the procedures.
e. Produce evidence records for the ISO 27001 audits.
f. Review, Improve and then next cycle starts.

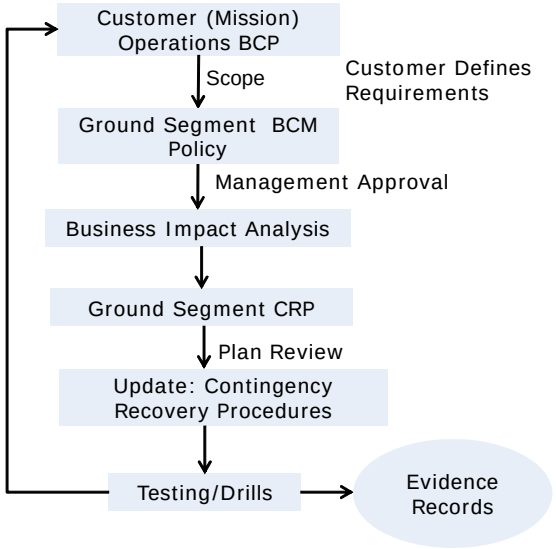

Figure 7. Ground Segment BCP Process

VI. Conclusion

Adopting ISO 27001 standard to secure ground segment would definitely prove to be beneficial to mission operations. It will establish a continuous security improvement process with Plan-Do-Check-Act life cycle. It is not just a one-off project implementation of fixing a specific security vulnerability in the organization but once the ISMS is operational, it becomes part of day-to-day work culture of everyone in the organization. Security incidents might still happen, but customers and end users of the ground segment can be confident that a mature process is in place to control any damage that could be caused by these incidents and to briskly recover mission operations to normal state.

Appendix A
Acronym List

A	Availability
ACL	Access Control List
BCM	Business Continuity Management
BCP	Business Continuity Plan
C	Confidentiality
CA	Certificate Authority
CERT	Computer Emergency Response Team
COTS	Commercial Off-The-Shelf
CP	Certification Policy
CPS	Certification Practice Statement
CRP	Contingency Recovery Plan
FAQ	Frequently Asked Questions
GSCRD	Ground Segment Customer Requirements Document
GSRD	Ground Segment Requirements Document
I	Integrity
IDPS	Intrusion Detection and Prevention System
ISMS	Information Security Management System
MDD	Mission Description Document
MOCD	Mission Operations Concept Document
M&O	Maintenance & Operations
QA	Quality Assurance
QMS	Quality Management System
SGICD	Space-to-Ground Interface Control Document
SLE	Space Link Extension
SoA	Statement of Applicability

Appendix B
Glossary

Information security event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
Information security incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

Acknowledgments

Author thanks his family, Alexandra Sokolowski (VEGA), Paul Bearman (VEGA), Elias Taylor (Thorn SDS), Marko Butkovic (ESA), Manfred Lugert (ESA) for their support.

References

[1]CCSDS Security Threats against Space Missions, Informational Report, CCSDS 350.1-G-1, Green Book, October 2006.

[2]ISO/IEC 27000:2009(E) ISO/IEC 27000 Information technology - Security techniques - Information security management systems — Overview and vocabulary

[3]ISO/IEC 27001:2005(E) Information security management systems - Requirements

[4]ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management

[5]ISO/IEC 27003:2010 Information technology - Security techniques - Information security management system implementation guide

[6]ISO/IEC 27004:2009 Information technology - Security techniques - Information security management -- Measurement

[7]ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management

[8]ECSS-P-001B, ECSS Glossary of terms, 14 July 2004

[9]ECSS-E-ST-70-31C, ECSS, Space Engineering, Ground systems and operations - Monitoring and control data definition, 31 July 2008

[10]ECSS-E-ST-70C, ECSS, Space Engineering, Ground systems and operations, 31 July 2008