

This Draft is distributed to the ECSS community for Public Review.

Start of Public Review: 22 June 2023

End of Public Review: 8 September 2023

**DISCLAIMER (for drafts)**

This document is an ECSS Draft Standard. It is subject to change without any notice and may not be referred to as an ECSS Standard until published as such.

**ECSS Secretariat**

**ESA-ESTEC**

**Requirements & Standards Section**

**Noordwijk, The Netherlands**

**Foreword**

This Standard is one of the series of ECSS Standards intended to be applied together for the management, engineering, product assurance and sustainability in space projects and applications. ECSS is a cooperative effort of the European Space Agency, national space agencies and European industry associations for the purpose of developing and maintaining common standards. Requirements in this Standard are defined in terms of what shall be accomplished, rather than in terms of how to organize and perform the necessary work. This allows existing organizational structures and methods to be applied where they are effective, and for the structures and methods to evolve as necessary without rewriting the standards.

This Standard has been prepared by the Working Group, reviewed by the ECSS Executive Secretariat and approved by the ECSS Technical Authority.

**Disclaimer**

ECSS does not provide any warranty whatsoever, whether expressed, implied, or statutory, including, but not limited to, any warranty of merchantability or fitness for a particular purpose or any warranty that the contents of the item are error-free. In no respect shall ECSS incur any liability for any damages, including, but not limited to, direct, indirect, special, or consequential damages arising out of, resulting from, or in any way connected to the use of this Standard, whether or not based upon warranty, business agreement, tort, or otherwise; whether or not injury was sustained by persons or property or otherwise; and whether or not loss was sustained from, or arose out of, the results of, the item, or any services that may be provided by ECSS.

Published by: ESA Requirements and Standards Section

 ESTEC, P.O. Box 299,

 2200 AG Noordwijk

 The Netherlands

Copyright: 2023© by the European Space Agency for the members of ECSS

Change log

|  |  |
| --- | --- |
|  | Change log for Draft development |
| Previous steps |  |
|  | WG Draft received from WG on 1 May 2023. |
|  | Final check and edit between ECSS Secretariat and convenor completed 24 May 2023 |
| ECSS-Q-ST-80-10C DIR124 May 2023 | Parallel Assessment for the release for Public Review25 May – 13 June 2023NOTE: Draft was released for Public Review at TA82 |
| Current step |  |
| ECSS-Q-ST-80-10C DIR124 May 2023 | Public Review22 June – 8 September 2023(taking into account the summer break) |
| Next steps |  |
| DIR + impl. DRRs | Draft with implemented DRRs |
| DIR + impl. DRRs | DRR Feedback |
| DIA | TA Vote for publication |
| DIA | Preparation of document for publication (including DOORS transfer for Standards) |
|  | Publication |
|  | Change log for published Standard (to be updated by ES before publication) |
|  | First issue |

Table of contents

[Change log 3](#_Toc138231131)

[Introduction 7](#_Toc138231132)

[1 Scope 8](#_Toc138231133)

[2 Normative references 9](#_Toc138231134)

[3 Terms, definitions and abbreviated terms 10](#_Toc138231135)

[3.1 Terms from other standards 10](#_Toc138231136)

[3.2 Terms specific to the present standard 11](#_Toc138231137)

[3.3 Abbreviated terms 15](#_Toc138231138)

[3.4 Nomenclature 15](#_Toc138231139)

[4 Security in Space Systems Lifecycles Principles 17](#_Toc138231140)

[4.1 Security Design and Operations Principles 17](#_Toc138231141)

[4.1.1 Overview 17](#_Toc138231142)

[4.1.2 Need-to-Know 17](#_Toc138231143)

[4.1.3 Least Privilege 17](#_Toc138231144)

[4.1.4 Defence-in-Depth 17](#_Toc138231145)

[4.1.5 Separation of Duties 18](#_Toc138231146)

[4.1.6 Attack Surface Reduction 18](#_Toc138231147)

[4.1.7 Fail Secure 18](#_Toc138231148)

[4.1.8 Domain Separation 19](#_Toc138231149)

[4.1.9 Redundancy 19](#_Toc138231150)

[4.1.10 Secure Evolvability / Agility 19](#_Toc138231151)

[4.2 Organisation of this Standard 19](#_Toc138231152)

[4.3 Tailoring of this Standard 20](#_Toc138231153)

[5 Requirements 21](#_Toc138231154)

[5.1 Organisation 21](#_Toc138231155)

[5.1.1 Organisational Structure 21](#_Toc138231156)

[5.1.2 Information Security Management Plan 21](#_Toc138231157)

[5.1.3 Personnel 22](#_Toc138231158)

[5.1.4 Personnel Authorisation and Training 23](#_Toc138231159)

[5.1.5 Accounting and Authorisation 24](#_Toc138231160)

[5.2 Mission Security 24](#_Toc138231161)

[5.2.1 Mission Security Policy 24](#_Toc138231162)

[5.2.2 Mission Security Requirements 25](#_Toc138231163)

[5.2.3 Security Monitoring and Incident Handling 26](#_Toc138231164)

[5.3 System Security Engineering 26](#_Toc138231165)

[5.3.1 System Security Engineering Requirements 26](#_Toc138231166)

[5.3.2 Supply Chain requirements 28](#_Toc138231167)

[5.3.3 System Security Engineering Plan 30](#_Toc138231168)

[5.4 Security Assessment During Space Systems Lifecycle 30](#_Toc138231169)

[5.4.1 Security Risk Management 30](#_Toc138231170)

[5.4.2 Software Vulnerability Analysis and Testing 34](#_Toc138231171)

[5.4.3 Security Audits 35](#_Toc138231172)

[5.4.4 Vulnerability Management 35](#_Toc138231173)

[5.4.5 Penetration Testing 36](#_Toc138231174)

[Annex A (informative) Security Documents 37](#_Toc138231175)

[Annex B (informative) Common Threats Applicable to Space Missions Affecting Security 40](#_Toc138231176)

[B.1 Data Corruption / Modification 40](#_Toc138231177)

[B.2 Denial-of-Service 40](#_Toc138231178)

[B.3 Ground System Loss 41](#_Toc138231179)

[B.4 Interception of Data 41](#_Toc138231180)

[B.5 Jamming 41](#_Toc138231181)

[B.6 Masquerade 42](#_Toc138231182)

[B.7 Replay Attack 42](#_Toc138231183)

[B.8 Software Threats 42](#_Toc138231184)

[B.9 Unauthorized Access 43](#_Toc138231185)

[B.10 Supply Chain Threats 43](#_Toc138231186)

[B.11 Other Threats with an Impact to Security 44](#_Toc138231187)

[B.12 Summary 45](#_Toc138231188)

[Bibliography 50](#_Toc138231189)

**Figures**

[Figure 5‑1: Indicative Supply chain challenges 29](#_Toc138231190)

[Figure 5‑2: Indicative Security Risk Management Process 31](#_Toc138231191)

[Figure 5‑3: Example of an Incremental Security Analysis to be Iteratively Derived at each Project Lifecycle Phase 32](#_Toc138231192)

[Figure A-1 : Security Documents to be produced. 37](#_Toc138231193)

[Figure A-2 : Typical Security Documents to be produced per phase. 38](#_Toc138231194)

**Tables**

[Table A-1 : Document requirements list (DRL) 39](#_Toc138231195)

[Table B-1 : Security Mechanisms to Counter Threats, Mitigations and Contingencies 46](#_Toc138231196)

Introduction

Security is a broad domain, affecting people, processes, and technologies. Application of security within all parts of an organisation and its activities are necessary for a coherent and structured approach to security. Security needs to apply to the system(s) to be operated, the systems used to enable security, the facilities to host and provide the global context, and the processes and methods used. Security must evolve and vary depending upon the threats and security risks, phase of the activity, regulations, the resources, and mechanisms selected to host and share the assets. On top of this, security is needed to be addressed when choosing the design, implementation aspects, resulting vulnerabilities, and the resources used to develop, operate, maintain, and dispose of the system.

The objective of this standard is to ensure a systematic and consistent consideration and implementation of a secure lifecycle for space systems.

As mentioned at the beginning, security is a broad domain covering many different aspects, technological, engineering or process related, etc. Therefore, this standard is intended to be accompanied by a set of handbooks or even additional security standards focused on specific security aspects.

# Scope

This standard provides requirements on the implementation of security in space systems, and requirements on the processes implemented during their lifecycle. This means ensuring the correct implementation of required security functionality in the system (e.g., implementation of an Information Security Management System in the ground segment); and also ensuring reasonable security of the lifecycle itself (e.g., ensuring reasonable management of design information). Space systems include manned and unmanned spacecraft, launchers, payloads, experiments and their associated ground equipment and facilities. Specifically, in the scope of this document are the Space Segment, Ground Segment, Launch Segment, and Support Segment, as defined in ECSS-S-ST-00-01, during their whole lifecycle (from definition, design, development, to operation and decommission).

This standard considers the wide variety of security aspects that must be examined during the lifetime of a space system, including potential certification needs, allowing a tailoring to adapt to specific missions and services. It also considers the interaction between security of the system and its lifecycle, and the corporate security of the organisations involved. This standard is applicable to unclassified missions and projects, and used or tailored, as needed, abiding by national and inter-governmental rules for classified governmental security projects. Corporate security is usually specific to each organisation and may be constrained by national regulations or standards. Therefore, this standard avoids imposing unnecessary constraints that conflict with corporate security of the organisations involved in the lifecycle.

A security risk assessment should support the identification of sensitive information as well as the corresponding required protective security marking and measures.

This standard interfaces with space engineering and management, which are addressed in the Engineering (-E) and Management (-M) branches of the ECSS System.

This standard may be tailored for the specific characteristics and constraints of a space project in conformance with ECSS-S-ST-00.

# Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this ECSS Standard. For dated references, subsequent amendments to, or revision of any of these publications do not apply. However, parties to agreements based on this ECSS Standard are encouraged to investigate the possibility of applying the more recent editions of the normative documents indicated below. For undated references, the latest edition of the publication referred to applies.

|  |  |
| --- | --- |
| ECSS-S-ST-00-01 | ECSS system — Glossary of terms |
| ECSS-E-ST-40C | Space Engineering – Software  |
| ECSS-Q-ST-80 | Space Product Assurance – Software Product Assurance |
| ECSS-Q-ST-10 | Product assurance management |

# Terms, definitions and abbreviated terms

## Terms from other standards

1. For the purpose of this Standard, the terms and definitions from ECSS-S-ST-00-01 apply, in particular for the following terms:
	1. Acceptance
	2. Analysis
	3. Assurance
	4. Audit
	5. Component
	6. Conformance
	7. Contract
	8. COTS
	9. Customer
	10. Design
	11. Development
	12. Element
	13. Fail Safe
	14. Firmware
	15. Ground segment
	16. Incident
	17. Launch segment
	18. Lifecycle
	19. Lifetime
	20. Mission
	21. Process
	22. Product
	23. Project
	24. Requirements
	25. Space missions
	26. Space segment
	27. Space system
	28. Spacecraft
	29. Subsystem
	30. Supplier
	31. Support segment
	32. Support system
	33. System
	34. Tailoring
	35. Validation
	36. Verification
	37. Waiver

## Terms specific to the present standard

In this sub-section the terms specific to this standard are defined. As potential sources, various creditable ones have been considered (ISO, CCSDS, NIST, IETF, ESA Security Directives). The ones used were chosen on their suitability for the intended purpose of this document (and if needed modified) and not following any specific “hierarchy” in the adoption.

1. authenticity

property of being genuine and able to be verified and trusted

[IETF RFC 4949]

1. authentication

process of verifying the identity or other attributes claimed by or assumed of a user, process, or device, or to verify the source and integrity of data

[CCSDS 350.8-M-2]

1. An authentication process consists of two basic steps: 1) Identification step: Presenting the claimed attribute value (e.g., a user identifier) to the authentication subsystem. 2) Verification step: Presenting or generating authentication information (e.g., a value signed with a private key) that acts as evidence to prove the binding between the attribute and that for which it is claimed (see IETF RFC 4949).
2. availability

property of a system or a system resource being accessible and usable upon demand by an authorised entity, according to performance specifications for the system or the system resource

[IETF RFC 4949]

1. confidentiality

property that information is not made available or disclosed to unauthorized individuals, entities, or processes, i.e., to any unauthorized system entity

[CCSDS 350.8-M-2]

1. cyber disaster

cyber incident that results in an extended cyber damage, making the eradication of the artefacts that lead to the cyber incident and the recovery of the affected system extremely difficult by the typical incident handling means and procedures

1. cyber incident

occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies

[NIST SP 800-53 Rev. 5]

1. fuzzing

test or automated software testing method that injects invalid, malformed, or unexpected inputs into a system to reveal software defects and vulnerabilities

1. incident handling

mitigation of violations of security policies and recommended practices

[NIST 800-61 Rev. 2]

1. The term incident response is synonymous.
2. information security

measures that implement and assure security services in information systems, including in computer systems (COMPUSEC) and in communication systems (COMSEC)

[IETF RFC 4949]

1. information security management system

set of policies, procedures and other controls involving people, processes, and technology for systematically managing an organization’s information security

1. penetration testing

test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system

[NIST SP 800-53, NIST SP 800-95]

1. protective marking

means used to associate a set of security attributes with objects in a human-readable form to enable organizational, process-based enforcement of information security policies, national laws and regulations

* 1. 1 The terms security marking and protective security marking are synonymous.
	2. 2 Adapted from NIST SP 800-53.
1. security risk owner

person or entity with the accountability and authority to set the security risk appetite, accepting risk treatment plans and residual risks for an activity

* 1. 1 The security risk owner is defined by the customer or mission owner and agreed with the project. Risks are formally accepted by the next higher-level responsibility within the customer/supplier chain.
	2. 2 The term risk owner is used as the short form of security risk owner.
	3. 3 Adapted from ISO 27005:201422.
1. security controls

management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information

[CCSDS 350.8-M-2]

1. security risk

function of the impact of an occurrence and the likelihood of that impact’s occurrence

* 1. 1 Security risk may be considered qualitatively (e.g., low/medium/high) or quantitatively according to organizational needs:
	Security Risk = Likelihood × Impact.
	2. 2 Adapted from CCSDS 350.7-G-2.
1. security audit

systematic and independent review and examination of a system’s records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.

[NIST SP-800-82]

1. security monitoring

automated process of collecting and analysing indicators of potential security threats, then triaging these threats with appropriate action

1. security risk analysis

systematic use of information to identify item or activity having a potential for a consequence and to estimate the risk

[ENISA, ISO/IEC Guide 73]

1. security risk appetite

pre-defined type and level of security risk that, on a broad level, the organisation, program and project are willing to accept in order to meet its objectives

1. security risk assessment

process of comparing the estimated risk against given risk criteria to determine the significance of risk

[ISO/IEC Guide 73]

1. security risk identification

process to find, list and characterize elements of risk

[ISO/IEC Guide 73]

1. security risk management

The process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options.

[ENISA Glossary]

1. Security risk management is implemented at each level of the customer‐supplier network.
2. security sensitivity

measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection

[NIST SP 800-12, 800-30]

1. Sensitivity is used as the short form of security sensitivity.
2. source code review

examination of source code to discover hidden vulnerabilities, design flaws, and verify if key security controls are implemented

1. threat

circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service

1. Adapted from NIST SP 800-30, 800-53, and 800-128
2. vulnerability

flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy

[IETF RFC 4949]

1. vulnerability assessment

systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation

[CCSDS 350.8-M-2]

## Abbreviated terms

For the purpose of this Standard, the abbreviated terms and symbols from ECSS-S-ST-00-01 and the following apply:

|  |  |
| --- | --- |
| Abbreviation | Meaning |
| AR | Acceptance Review |
| CDR | Critical Design Review |
| COTS | Commercial Off the Shelf |
| FOSS | Free and Open Source Software |
| INFOSEC | Information Security |
| ISMP | Information Security Management Plan |
| ISMS | Information Security Management System |
| MGT | Management file |
| ORR | Operational Readiness Review |
| OSS | Open Source Software |
| PDR | Preliminary Design Review |
| QR | Qualification Review |
| SRR | System Requirements Review |

## Nomenclature

The following nomenclature applies throughout this document:

1. The word “shall” is used in this Standard to express requirements. All the requirements are expressed with the word “shall”.
2. The word “should” is used in this Standard to express recommendations. All the recommendations are expressed with the word “should”.
3. It is expected that, during tailoring, recommendations in this document are either converted into requirements or tailored out.
4. The words “may” and “need not” are used in this Standard to express positive and negative permissions, respectively. All the positive permissions are expressed with the word “may”. All the negative permissions are expressed with the words “need not”.
5. The word “can” is used in this Standard to express capabilities or possibilities, and therefore, if not accompanied by one of the previous words, it implies descriptive text.
6. In ECSS “may” and “can” have completely different meanings: “may” is normative (permission), and “can” is descriptive.
7. The present and past tenses are used in this Standard to express statements of fact, and therefore they imply descriptive text.

# Security in Space Systems Lifecycles Principles

## Security Design and Operations Principles

### Overview

Design and operations principles are presented together because most of them affect both the design of the system and how its maintenance and operations can be organised.

During design and operation of any system, the following principles apply.

### Need-to-Know

Need-to-Know (NTK) is the principle according to which a positive determination is made by the issuer of the information that a prospective recipient has a requirement for access to, knowledge of, or possession on information in order to perform tasks or services in the scope of the contract programme, project or activity.

### Least Privilege

Least privilege is the principle that a security architecture is designed so that each entity is granted the minimum system resources and authorisations that the entity needs to perform its function.

[Source: NIST 800-53 Rev.5].

### Defence-in-Depth

Defence-in-depth is an information security strategy integrating people, technology, and operations capabilities to establish multiple countermeasures in a layered or stepwise manner to achieve the security objectives. The application of this principle involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another.

[Source: NISTIR 8183].

These layers shall include at a minimum:

1. Prevention: security measures aimed at impeding or blocking an attack on the system.
2. Detection: security measures aimed at discovering the occurrence of an attack on the system.
3. Resilience: security measures aimed at limiting impact of an attack to a minimum set of information or assets and preventing further damage, and
4. Recovery: security measures aimed at regaining a secure situation for the System if it is compromised.

This principle focuses on maximising the complexity of an attack for the adversary and encourages the use of redundancy in defences, where security is not dependent on only one security feature working.

### Separation of Duties

Separation of duties is the principle that no user should be given enough privileges to misuse the system on their own. Separation of duties can be enforced either statically (by defining conflicting roles, i.e., roles which cannot be executed by the same user) or dynamically (by enforcing the control at access time). An example of dynamic separation of duty is the two-person rule.

[Source: NIST SP 800-192].

An example of application of this principle is to require two different physical persons to authorise an operation so as this to take place. Another example is to allocate critical but interdependent roles to different persons, e.g., a domain controller administrator to be a different person from a database administrator, or a crypto custodian to be a different person than a crypto operator.

### Attack Surface Reduction

This principle refers to the reduction of the total reachable and (potentially) exploitable services, applications, assets, resources, etc. to the bare minimum required for the function of the system, subsystem, or component. Attack surface reduction refers to all the measures that can be taken so as to achieve the final objective, from applying appropriate boundary controls (e.g. network and host firewalls by minimising access to the bare minimum ports) to completely removing services, applications, any kind of software and functionalities that do not strictly needed for fulfilling the mission requirements.

This principle is also known as the principle of minimalism.

### Fail Secure

Fail secure is a principle that refers to a mode of termination of system functions that prevents loss of secure state when a failure occurs or is detected in the system (but the failure still might cause damage to some system resource or system entity)

[Source: IETF RFC 4949].

1. Fail Secure is not the same with Fail Safe, which is a design feature or practice that, in the event of a specific type of failure, inherently responds in a way that can cause only minimal or no harm to other equipment, to the environment or to people.

### Domain Separation

Domains with distinctly different protection needs are physically or logically Separated. The separation of domains enables enhanced control and, therefore, protection of system function and the flow of data. Control relative to separated domains limits the extent to which an entity or domain is influenced by or is able to influence some other entity or domain, thereby enhancing the protection of a domain. This is achieved through the control of information flow and data between domains as well as control over the use of a system capability between domains.

[Source: NIST SP 800-160v1r1, Annex E].

### Redundancy

The system design delivers the required capability by replication of system functions or elements. Redundancy employs multiples of the same system elements, data and control flows, or paths to avoid single points of failure. Redundancy requires a strategy for how multiple system elements are used individually or in combination (e.g., load-balancing, fail-over, concurrently, backup, etc.)

[Source: NIST SP 800-160v1r1, Annex E].

### Secure Evolvability / Agility

The principle of secure evolvability states that a system should be developed to facilitate the maintenance of its security properties when there are changes to its functionality structure, interfaces, and interconnections (i.e., system architecture) or its functionality configuration (i.e., security policy enforcement).

[Source: NIST 800-160, appendix F].

## Organisation of this Standard

This standard is organised in four main parts:

* Organisation (i.e. personnel, Information Security Management Plan, organisational structure of involved entities).
* Mission Security
* System Security Engineering
* Security Assessment during Space Systems Lifecycle.

The documentation collecting the expected output of the requirements of the current document is summarised in Annex A.

Each requirement of this Standard is identified by a hierarchical number, plus a letter if necessary (e.g. 5.3.1.5, bullet a). For each requirement, the associated output is given in the “Expected Output” section. With each output, the destination file of the output is indicated in brackets, together with the corresponding document DRD (after a comma) and review(s) (after a semicolon). When no DRD is defined for an Expected Output, and/or the Expected Output is not to be provided at any specific milestone review, then the corresponding sections of that Expected Output are replaced by dashes.

## Tailoring of this Standard

The general information and requirements for the selection and tailoring of applicable standards are defined in ECSS-S-ST-00.

# Requirements

## Organisation

### Organisational Structure

An organisational structure of personnel required to ensure security in space systems, projects and missions during their whole lifecycle shall be defined.

In this organisational structure the responsibilities, the authority, the tasks and the interrelation of personnel who manage, perform and verify work affecting security in space systems lifecycle shall be defined.

This organisational structure shall include at a minimum a Security Manager and a Security Internal Auditor.

The Security Manager and the Security Internal Auditor shall perform their duties without prejudice due to their functional hierarchy in their entity.

The interfaces with any external or internal entity involved in a project or a mission and their responsibilities in respect to the project or mission shall be defined and documented.

The organisational structure shall be incorporated into the Security Management Plan.

1. Security Management Plan [MGT; Proposal, KOM, SRR, and updated when needed]

### Information Security Management Plan

Each entity participating by any means to any space project, programme, or mission, shall develop, document, and implement an organization-wide plan to provide security for the information, information and communication systems and facilities that support the operations and assets of that organization.

1. Information Security Management Plan [MGT; Proposal, KOM, SRR, and updated when needed]
	1. 1 Example of facilities include factories, test centres, and other.
	2. 2 The set of information, information and communication systems and facilities is, typically known as Information Security Management System (ISMS).

An ISMP shall follow the functional organization of the ISMS.

The process of uniquely assigning information resources to an information system shall define the security boundary for that system.

The security boundary shall take into account regulatory authority, trust relationships, and line management authority.

1. [Source: CCSDS 350.7-G-2, para. 3.6.2 (mod)].

An ISMP shall describe resources under the same direct management control.

Process as well as project/mission data and information shall be handled and protectively marked in compliance with the international or national applicable Security Controls Frameworks standards.

1. This includes project/mission data and information shared with subcontractors.

Access to assets and information shall be given, based on the “Need-To-Know (NTK)” principle and its related sensitivity.

1. Information Security Management Plan [MGT; Proposal, KOM, SRR, and updated when needed]

### Personnel

#### Security Manager

The organisation or entity shall appoint a Security Manager responsible for managing the implementation of security requirements in the scope of the activities under the responsibility of this organisation or entity.

The Security Manager shall be trained for the role.

The Security Manager shall be responsible for conducting at least the following tasks:

Establishment of implementation plans for security policies and security requirements.

Support to the implementation of the necessary security measures and of the security risk mitigations.

Supervision and monitoring of the performance of all security related planned tasks.

1. Examples of such tasks are vulnerability assessments, risk assessments, application of needed asset sensitivity, protective marking, security controls, and other.

Reporting of the status of all security related tasks, as well as of the security posture of the system that falls under the responsibility of her/his entity.

Promotion of Information Security (INFOSEC) within her/his entity.

The responsibilities of the Security Manager shall be defined in the Security Management Plan.

1. Security Management Plan [MGT; KOM, SRR, and updated when needed]

#### Security Internal Auditor

The organisation or entity shall appoint a Security Internal Auditor responsible for conducting security audits in the perimeter of this organisation or entity.

The Security Internal Auditor shall be trained for the role.

The Security Internal Auditor shall carry out the security auditing activities impartially and independently from the execution of the Security Manager.

The Security Auditor shall be independent from the team implementing or controlling the security measures.

The Security Internal Auditor shall have direct reporting line to the high-level management of the project or mission.

The Security Internal Auditor shall not be part of the internal organisation that manages the execution of the project (operations or development) or mission.

The Security Internal Auditor shall be responsible for conducting at least the following tasks:

Planning and implementation of security audits in the perimeter of her/his area of responsibility.

Evaluation of the level of compliance of the Information Security Management System (ISMS) of her/his entity, of the implementation of the security requirements, and of the security measures that have been put in place.

Providing independent feedback and report on a regular basis (at least every six months) on the effectiveness of Information Security Management Plan (ISMP), security measures, and their application.

The Security Internal Auditor shall always be granted access to the information required to perform her/his duties.

The responsibilities of the Security Internal Auditor shall be defined in the Security Management Plan.

1. Security Management Plan [MGT; KOM, SRR, and updated when needed]

### Personnel Authorisation and Training

All personnel shall be appropriately authorised, security trained & briefed based on their responsibilities, role and function.

Personnel authorisation and training shall be periodically refreshed also depending on role, and function and changes in threat and risk.

Security awareness briefings shall be periodically organised for all personnel.

The personnel authorisation requirements and their training plan shall be included in the Security Management Plan

1. Security Management Plan [MGT; KOM, SRR, and updated when needed]

### Accounting and Authorisation

Any equipment and resource shall be accounted and authorised prior to use within a space project or mission.

1. Equipment includes hardware, software, firmware and their configuration.

Processes and tools shall be in place to detect and address unauthorized equipment, personnel use or access.

The processes and tools to be used to address accounting and authorisation requirements shall be defined at the beginning of the project or mission and checked throughout the complete lifecycle.

Access to assets and information shall be given, based on the “Need-To-Know (NTK)” principle and the sensitivity of the asset.

The processes and tools to be used for accounting and authorisation shall be included in the Security Management Plan.

1. Security Management Plan [MGT; KOM, SRR, and updated when needed]

## Mission Security

### Mission Security Policy

Every mission shall define a Mission Security Policy as an element of its overall mission concept definition.

The Mission Security Policy shall outline how the space system is intended to operate, and what action are taken when it operates outside its intended parameters.

The Mission Security Policy shall be observant of any higher-level organization.

The Mission Security Policy shall clearly state:

The sensitivity and therefore the required level of protection of all the information associated with the mission, both live and archived, during the whole lifecycle of the mission;

the protective marking to applied to information and assets;

the roles of those who have access to the system(s) operating the mission;

the confidentiality, integrity requirements of the mission, and,

the availability requirements of the mission.

* 1. 1 [Source: CCSDS 350.7-G-2, para. 3.2]
	2. 2 Information associated with the mission includes, but is not limited to, telemetry, telecommand structure and their contents, software, and ground systems data, and personal data.

Where a complex system includes interacting elements under different management control, those elements shall be described separately.

1. Elements under different management control can be spacecrafts, ground segment, or other.

Interactions between elements under different management control shall be documented.

Any shared resources shall be approved by the relevant authorities for the highest sensitivity level of the resources and information managed.

* 1. 1 [Source: CCSDS 350.7-G-2, para. 3.6.2 (mod)].
	2. 2 Shared resources can be organizational processes, networks, physical facilities, and other.
1. Mission Security Policy [TS; KOM, SRR, PDR, CDR; updated when needed]

### Mission Security Requirements

All communication links (telemetry, telecommand, mission specific) shall, at a minimum, be protected with cryptographic authentication and integrity mechanisms sufficient for the sensitivity of the information and asset and accompanied by the required documented procedures.

1. The outcome of a security risk analysis can be used to support non-cryptographic alternative controls on the telemetry link where a mission risk owner has a high-risk appetite and low levels of residual risk.

A mission level security risk analysis shall be used to assess the need of encryption of the various communication links.

Measures shall be put in place to support detection of unauthorised interference.

A mission level security risk analysis shall assess the need and feasibility of encryption, authentication, integrity protection and detection controls regarding systems and information in transport, at rest and in-use with assessment of physically separated entities, data-flows and third party access.

The operator shall take technical and organizational measures that prevent unauthorized persons access to the installations, operating rooms for the commanding of the spacecraft as well as to the equipment and services for receiving, processing and storing the data appropriate for the sensitivity of the asset and information.

The operator shall ensure adequate security screening and (where appropriate) clearance of persons who have access to the facilities for commanding a spacecraft or to the facilities for receiving, processing and storing the data of a spacecraft, any accessing other relevant information or physical assets based on the assets security sensitivity.

The measures and procedures ensuring the implementation of these requirements shall be part of the Mission Security Policy.

Mission security requirements shall be captured in the Mission Security Policy

1. Mission Security Policy [TS; KOM, SRR, PDR, CDR; updated when needed]

### Security Monitoring and Incident Handling

Each mission and each of its systems shall be continuously monitored in terms of security for intrusion detection purposes from a Security Operations Centre (SOC).

Security monitoring capability shall cover the whole perimeter of a mission or a system.

Security monitoring shall be able to detect all possible types of attacks with support of cyber threat intelligence.

Incident handling capability shall be incorporated into the security monitoring capability of the mission.

Incident handling processes, procedures and response performances shall be agreed by the mission owner.

Incident handling capability shall include a Security Incident Response Team, capable of being developed rapidly to handle a cyber incident.

Measures and plans shall be put in place to respond and recover in case of major incidents.

The measures and plans to be put in place to respond and recover in case of major incidents shall be verified periodically.

Security monitoring and incident handling capability may be outsourced.

1. Security Monitoring and Incident Handling Plan [SF; SRR, PDR, CDR, and updated when needed]

## System Security Engineering

### System Security Engineering Requirements

System security engineering shall be incorporated from the very beginning of a project or mission as part of the whole system engineering for any kind of project or mission.

Security requirements shall be derived from mission security policy and security risk treatment plan, as well as from functional system requirements with implications to security.

 The security requirements shall be incrementally extended and derived based on the mission phase and level of the project customer-supplier.

In order to select appropriate security controls, organizations shall categorize the information to be handled by the system according to the criteria of Confidentiality, Availability, and Integrity.

1. National security regulations as well as other laws (e.g., export, personal sensitive data and copyright restrictions) controlling the handling of specific information types override organizational discretion in categorizing information.

Security controls from the following categories shall be put in place:

Controls and measures designed to prevent a negative security event from occurring (preventive controls);

Controls and measures that aim to inform the organization about potential security events (detective controls);

Controls are ’after the incident’ measures to minimise impact, restore the system to nominal operation and/or collect forensic information about the nature and extent of the event (responsive controls).

The applicability and usefulness of the security controls originally implemented shall be periodically re-evaluated and adapted:

As threats and risks to the system change over time;

when system components are replaced, upgraded or their sensitivity levels are changed;

as specific vulnerabilities are identified;

and when the risk appetite is modified.

Together with the system architecture, a system security architecture shall be compiled, incorporating the security controls to be put in place.

The system security architecture shall be compiled adhering to the principles defined in Clause 4.1.

The system security architecture shall be driven by a mission/system security risk analysis including asset and information sensitivity.

The system security architecture shall incorporate the technical capabilities required to apply business continuity and disaster recovery plan including cyber disasters such as malware pandemic.

The system design shall address or mitigate the security risks identified in the security risk analysis performed at the beginning of the project or mission by proposing for implementation the required security controls and taking into account the available risk treatment plans.

For each system, a security obsolescence plan shall be defined specifying the requirements for support by the vendors of each component for security patches, fixes and security certifications (if applicable).

The security obsolescence plan shall be agreed with the risk owner and maintained during the system lifetime.

For each system a patching policy for all software and firmware shall be defined, applicable during the whole lifecycle of the mission.

Each system shall be designed and developed in a way to be capable of applying the defined patching policy.

The patching policy shall include at a minimum:

Which patches to be applied.

How frequently to be applied.

Patches to be applied during security maintenance shall be tested and verified in terms of their authenticity.

 For secure software development, ECSS-Q-ST-80 and ECSS-E-ST-40 shall be followed.

The supplier shall define and apply guidelines for secure configuration of all the services, sub-systems and components in a system.

System security engineering requirements shall be included in the system security engineering plan.

1. System Security Engineering Plan [TS; SRR, PDR, CDR, QR]

### Supply Chain requirements

The supplier shall define and implement processes and technical measures to ensure and verify at any phase of the project the authenticity of a service, component or a subsystem across the whole supply chain.

* 1. 1 Supply chain also includes services provided by third parties such as contractors and sub-contractors.
	2. 2 In Figure 5‑1 an example of a supply chain and of corresponding potential security issues is given.



Figure ‑: Indicative Supply chain challenges

Supplier shall implement product assurance requirements considering ECSS-Q-ST-10.

The security requirements which have been derived in the frame of the project shall be flown-down to the relevant suppliers of security sensitive products and considering also ECSS-Q-ST-80C Rev.1 and ECSS-E-ST-40 if the supplies contain software modules.

The supplier shall assess potential vendors, taking into account the criticality and sensitivity of the product or service to determine if they:

Provide products and components, or sub-components, sourced through original equipment manufacturers or authorized resellers with clear and traceable bill of materials with appropriate integrity and authenticity measures.

Have previously incurred significant malicious network intrusions, data breaches, loss of client data, or intellectual property.

Have an adequately mature cyber security organisation, appropriate certifications and qualifications.

1. Example for an organisation include ISO27001 ISMS certification and for a product Common Criteria Product evaluation.

Provide services and products compliant to national regulations.

1. Examples include Export Control, Personal Information and the location of the organisation/service.

The customer shall define the supplier privacy and security requirements based on the criticality and sensitivity of the asset, resource or services to be provided by the supplier.

The supplier shall provide a statement of compliance with supporting credible evidence.

Supply chain management and requirements shall be defined and implemented at each level of the customer‐supplier network.

Supply chain management and requirements shall be defined in Supply Chain Management Plan.

1. Supply Chain Management Plan [MGT; Proposal/KOM, SRR, PDR, CDR, QR, AR]

### System Security Engineering Plan

Each supplier shall develop a System Security Engineering Plan that references or provides:

A summary of the system security requirements,

The system security controls in place and how it is planned for meeting the system security requirements,

A complete list of the inventory up to component level including each COTS and OSS with a detail versioning.

A cyber disaster recovery plan, and

A plan for source code analysis, security audits, vulnerability assessments and penetration tests to ensure that products are delivered to meet specified security requirements.

A system may have multiple subsystems or subordinate systems; a system security engineering plan shall include them in their scope.

The system security engineering plan shall include in its scope everything that falls in the responsibility of the specific mission, project, or contract,

Organizational policy shall clearly define who is responsible for approving the system security engineering plan.

1. [Source: CCSDS 350.7-G-2, para. 3.6.4 (mod)]

The system security engineering plan shall be subject to review during the major project review milestones.

1. [Source: CCSDS 350.7-G-2, para. 3.6.4 (mod)].
2. System Security Engineering Plan [TS; SRR, PDR, CDR, QR]

## Security Assessment During Space Systems Lifecycle

### Security Risk Management

A security risk owner shall be defined by the customer or the mission owner who is the responsible party to accept and agree on security risks and treatments.

1. Mission Security Policy [TS; KOM, SRR, PDR, CDR; updated when needed]

The pre-defined acceptable security risk level shall be agreed by the risk owner.

1. The pre-defined acceptable security risk is called “risk appetite”.
2. Mission Security Policy [TS; KOM, SRR, PDR, CDR; updated when needed]

At the beginning of each project or mission a security risk management process shall be defined.

1. Security Risk Analysis [SF; SRR, PDR, CDR, QR, AR, ORR]
2. An indicative Security risk management process is given in Figure 5‑2 and an example of its application along a project’s lifecycle in Figure 5‑3.



Figure ‑: Indicative Security Risk Management Process



\* In this example, the higher-level context and low level assessments are shown as parallel activities present in later phases to support different stakeholder and reporting needs, but this is not always necessary.

Figure ‑: Example of an Incremental Security Analysis to be Iteratively Derived at each Project Lifecycle Phase

At the beginning of each project or mission a preliminary security risk assessment shall be performed.

The preliminary risk assessment shall consider at least the following:

The type of the mission and the information security threats to that mission.

All parts of the mission and system architecture during all phases of the mission/project, as the relevant threats may change during their lifecycle.

The preliminary risk assessment shall use the outputs of the Mission Security Policy and system interconnections as identified in the system architecture to help identify attack vectors, sensitivity, and the value of the information and assets to be protected.

The security risk assessment shall be performed at each level in the customer-supplier network.

The security risk assessment shall be refined and updated at least at each major milestone and when there is a major design change or new vulnerabilities are identified.

1. New vulnerabilities can be identified during development, operations, and in general during the mission or system lifecycle via penetration tests, risks assessments, security audits, etc.

The security risk assessment shall incorporate all known vulnerabilities existing along all stages of the components (HW, SW, Firmware) supply chain and/or development.

* 1. 1 [source: CCSDS 350.7-G-2, para. 3.6.3 (mod)]
	2. 2 In the early stages of development, vulnerabilities can be theoretical in nature; in later stages, they can be highly dependent upon implementation details.
	3. 3 Vulnerability along the component supply chain can enable gateways for future threats or they can cause “residuals” that can develop under certain circumstances into threats.

Security risk assessment of a mission shall include as a minimum the following:

Launch site and facilities.

Manufacturing, Assembly, Integration and Test facilities.

Ground Segment

Space Segment

User Segment

Security risk assessment of a system/subsystem shall cover all its perimeter, including its interfaces with external systems/subsystems in line with the security scope agreed with the risk owner.

For each risk found, the security risk assessment shall also identify and propose a mitigation strategy, including a risk treatment plan (to be prioritized and scheduled).

Where identified security risk mitigation strategies conflict with other types of risk, most notably safety, environmental risk and dependability they shall be agreed with the risk owner(s).

The proposed risk treatment plan shall include the risk treatments and measures to address, at least, the identified security risks above the risk appetite.

1. Security risk analysis and Security risk treatment plan [SF; SRR, PDR, CDR, QR, AR, ORR].

The risk treatment plan shall define the security risk treatment(s) and plan for implementation that includes as a minimum:

The security risks with their associated criticality.

Proposed treatments for the risk with rationale for selection.

Plan for implementation of the treatments.

Residual risk assessment after treatment, defined in line with the implementation plan.

1. Security Risk Treatments include: Accept/Retain, Avoid, Transfer, Share, Mitigate/Modify.

Where a residual risk is present that is above the risk appetite for a release of the product/system, the risk shall be supported by a security waiver that presents a risk balance case justifying why the residual risk and risk treatment plan can be acceptable to the risk owner.

1. Project constraints such as cost, schedule, safety, operability can be valid justification for the risk owner, often as temporary treatments.

The risk treatment plan and security waivers shall be presented and approved by the risk owner.

The communication and ranking of security risks and treatments for incorporation into the overall project risk management process shall be agreed by the risk owner.

1. The principles and requirements for integrated risk management on a space project are defined in ECSS-M-ST-80.

At each major milestone, the acceptance of the associated risks, security waivers and related risk treatment plans shall be considered to decide whether to authorise the completion for that phase.

1. Temporary authorisation can be permitted based on the completion of risk treatment plans as authorised by the risk owner.

The applicable security handing and processing constraints shall be respected during the whole security risk management process (including the communication and processing of risk assessments, risk treatment plans and security waivers).

1. Information Security Management Plan [MGT; Proposal, KOM, SRR, and updated when needed] and Mission Security Policy [TS; KOM, SRR, PDR, CDR; updated when needed]

The security analysis, associated security risks and risk treatment plans shall be monitored, reviewed, updated systematically and periodically throughout the entire system lifecycle ensuring their continued consistency with each other and their validity.

1. Security risk analysis and security risk treatment plan (updated) [SF; SRR, PDR, CDR, QR, AR, ORR]

The security risk analysis shall include supply chain risks.

### Software Vulnerability Analysis and Testing

At the end of each software development, a source code review and analysis shall be performed to ensure the product is in conformance to security coding policies and is free from known vulnerabilities and malicious code.

1. Source code review and analysis can include static, dynamic code analysis, runtime analysis, etc.

The vulnerabilities identified during the source code review shall be fixed before qualification.

An additional source code review shall be performed to confirm the fixes.

Fuzzing testing shall ensure the product is free from known vulnerabilities at the time of design and product delivery.

The security risk analysis shall be updated based on the not fixed vulnerabilities and the risk management process shall be followed.

1. Security vulnerability analysis and testing report [SF; QR, AR].

For the not fixed vulnerabilities, the risk management process shall be followed.

### Security Audits

The Security Internal Auditor shall perform internal security audits at intervals defined at the system security engineering plan.

The customer shall have the capability to request additional security audits on the organization and mission during the system lifecycle.

The security risk analysis shall be updated based on findings of the security audits.

1. Security audits report [SF; QR, AR, ORR].

### Vulnerability Management

For each system a vulnerability management policy shall be defined.

The vulnerability management policy shall include at least the following:

The vulnerability scoring methodology to be used to assess the severity of the identified vulnerabilities.

The sources (“feeds”) of known vulnerabilities applicable to the system.

A mechanism/methodology to automatically correlate the system inventory with known vulnerabilities on COTS and FOSS used in the system (passive vulnerability assessment).

The importance of the system and information assets in terms of Confidentiality, Integrity and Availability (known as Security Sensitivity of the assets).

Passive and active vulnerability assessments shall be performed during development, as part of the qualification, before acceptance and during operation.

1. Active vulnerability assessment can be performed using a vulnerability assessment using a tool, ideally using authenticated scanning to the systems to be assessed.

The security risk analysis shall be updated based on the identified vulnerabilities.

1. Vulnerability assessment report [SF; QR, AR, ORR].

The risk management process shall be followed for the identified vulnerabilities.

### Penetration Testing

Independent penetration tests shall be performed during development, as part of the qualification, before acceptance and during operation.

Independent means that the penetration testers shall not have been involved in the design, development or implementation of the system(s).

The level of independence of the penetration testing team shall be agreed with the customer.

1. Level of independence can depend on whether the penetration testing team comes from an external company or agency, or whether it is an internal team independent from the development team, etc.

The penetration testing team shall have appropriate skills and qualifications to undertake the activity in line with the sensitivity of the assets to be tested.

The penetration testing team (also known as red team) shall replicate the potential adversarial threat to a given mission to assess vulnerability and to detect weaknesses.

The security risk analysis shall be updated based on the vulnerabilities identified during the penetration test.

1. Penetration testing report [SF; QR, AR, ORR].

The risk management process shall be followed for the identified vulnerabilities.

1. (informative)
Security Documents

This annex defines the structure of the security documents to be produced, as depicted in Figure A-1:



: Security Documents to be produced.

In Figure A-2 the correspondence of the produced documents to the phases are depicted.



: Typical Security Documents to be produced per phase.

Table A-1 represents the document requirements list, identifying the software documentation to be produced in accordance with the requirements defined in this Standard.

: Document requirements list (DRL)

| Related file | DRL item(e.g. Plan, document, file, report, form, matrix) | KOM | SRR | PDR | CDR | QR | AR | ORR |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| MGT | Information Security Management Plan | ****** | ****** |  |  |  |  |  |
| Security Management Plan | ****** | ****** |  |  |  |  |  |
| Supply Management Plan | ****** | ****** | ****** | ****** | ****** | ****** |  |
| TS | Mission Security Policy | ****** | ****** | ****** | ****** |  |  |  |
| System Security Engineering Plan |  | ****** | ****** | ****** | ****** |  |  |
| SF | Security Risk Analysis |  | ****** | ****** | ****** | ****** | ****** | ****** |
| Security Audits |  |  |  |  | ****** | ****** | ****** |
| Security Vulnerability Analysis and Testing Report |  |  |  |  | ****** | ****** |  |
| Vulnerability Assessment Reports |  |  |  |  | ****** | ****** | ****** |
| Penetration Testing Reports |  |  |  |  | ****** | ****** | ****** |
| Security Risk Treatment Plan |  | ****** | ****** | ****** | ****** | ****** | ****** |
| Security Monitoring and Incident Handling Management Plan | ****** | ****** | ****** | ****** |  |  |  |

1. (informative)
Common Threats Applicable to Space Missions Affecting Security
	1. Data Corruption / Modification

Data Corruption/Modification refers to the intentional or non-intentional alteration of data, whether being communicated or at rest. Data corruption/modification always implies a breach of data integrity. Data could be corrupted at rest, in transit, or during processing, at its original source, final destination, or anywhere in between.

Possible Mission Impact: Corruption might be a result of software failures or bugs, hardware failures, use of unauthorized software, or active attempts to change/modify data to deny its use. A corrupted spacecraft command could result in catastrophic loss if either no action occurred (e.g., command is discarded) or the wrong action was taken onboard a spacecraft. For example, if a navigation manoeuvre burn command were corrupted, the spacecraft might end up in an unusable orbit, miss an encounter with a comet/planet/asteroid, or be destroyed.

Applicable to: Space Segment, Ground Segment, Space-Link Communication

Reference: CCSDS 350.1-G-3, para. 3.4.2 (mod.)

* 1. Denial-of-Service

Denial-of-service attacks could occur in several ways: consumption of resources (e.g., communication bandwidth, processor bandwidth, disk space, memory), disruption of system/network configurations (e.g., routing changes), disruption of state information (e.g., persistent network connection resets), disruption of network components (e.g., router or switch crashes), or obstruction/destruction of communications paths. High powered lasers could blind sensors or destroy solar cells. High powered microwaves could cause CPU restarts, disruption of electronics, or memory errors.

Possible Mission Impact: Denial-of-service attacks could prevent authorized access to resources, both in space and on the ground. Ground systems and their networks could be greatly affected by loss of system availability, which could result in an inability to control a mission or obtain data from a mission.

Applicable to: Space Segment, Ground Segment

Reference: CCSDS 350.1-G-3, para. 3.4.6

* 1. Ground System Loss

A successful exploitation of a vulnerability through a physical/cyber-attack might disable the ground facility and directly affect the operation of the mission and the services provided. An attack might also take physical control of the facility to take control of the spacecraft without technically attacking the facility’s systems. Environmental factors might also result in the loss of a ground facility. Tornados, hurricanes, tsunamis, flooding, or other weather-related factors could result in physical damage to the facilities or the loss of electrical power to the ground station.

Possible Mission Impact: The loss of a ground system might result in the loss of data, loss of access to data in a timely manner, degradation or loss of spacecraft commanding, or loss of the entire mission.

Applicable to: Ground Segment

Reference: CCSDS 350.1-G-3, para. 3.4.3

* 1. Interception of Data

Possible Mission Impact: If the data is not encrypted, or is encrypted using weak algorithms or implementations, interception of data may result in the loss of data confidentiality and data privacy. In addition to those entities authorized for the data, non-authorized entities may also gain access. The interception of data could also result in masquerade or replay attacks.

Applicable to: Space Segment, Ground Segment, Space-Link Communication

Reference: CCSDS 350.1-G-3, para. 3.4.4

* 1. Jamming

An attack that attempts to interfere with the reception of broadcast communications. [IETF RFC 4949, Internet Security Glossary, Version 2].

Denial of communications to and from spacecraft could be accomplished by interfering with the RF signal. This can be achieved by injecting noise, by transmitting on the same frequency from another source, Electromagnetic Pulse (EMP), high powered microwave, or overpowering the original source. Optical sensors could be blinded and solar arrays damaged by lasers.

[Source: CCSDS 350.1-G-3, para. 3.4.5]

Possible Mission Impact: The interference can result in link loss and loss of mission control. Spacecraft commanding as well as the ability to receive science or engineering data from the spacecraft could be blocked. In addition, authorized access to system resources can be blocked, possibly delaying time-critical operations on both the ground and in space.

Applicable to: Space Segment, Ground Segment, Space-Link Communications

Reference: CCSDS 350.1-G-3, para. 3.4.5

* 1. Masquerade

A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity. [IETF RFC 4949, Internet Security Glossary, Version 2] [also used in NIST standards].

Authentication of an entity’s true identity is crucial for applying access control policies. When access control policies are being enforced, certain entities are allowed to perform specific actions while other entities may be denied. Access controls can be rendered useless if entities disguise their true identity or can masquerade as another entity. The lack of authentication can affect all space communications.

Possible Mission Impact: If an instrument operator masquerades as a spacecraft operator, incorrect spacecraft bus health and status actions might result in a loss of the mission. Likewise, if an external entity can masquerade as a spacecraft operator; unauthorized commands could be transmitted to the spacecraft resulting in damage, data loss, or loss of a mission.

Applicable to: Space Segment, Ground Segment

Reference: CCSDS 350.1-G-3, para. 3.4.7

* 1. Replay Attack

An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by a third party who intercepts the data and retransmits it, possibly as part of a masquerade attack. [Source: IETF RFC 4949, Internet Security Glossary, Version 2]

For example, transmissions to or from a spacecraft or between ground system computers can be intercepted, recorded, and played back at a later time.

Possible Mission Impact: If the recorded data were a command set from the ground to the spacecraft and they are re-transmitted to their originally intended destination, they might be acted upon, potentially for a second time. If the replayed commands are not rejected, they could result in a duplicate spacecraft operation such as a manoeuvre burn or a spacecraft reorientation with the result that a spacecraft is in an unintended orientation (e.g., tumbling, antenna pointed in the wrong direction, solar arrays pointed away from the sun, or the reset of critical onboard parameters).

Applicable to: Space Segment, Ground Segment, Space-Link Communications

Reference: CCSDS 350.1-G-3, para. 3.4.8

* 1. Software Threats

Users, system operators, and programmers often make mistakes that can result in security problems. Users or administrators can install unauthorized or un-vetted software, which might contain bugs, viruses, spyware, or which might simply result in system instability. System operators might configure a system incorrectly resulting in security weaknesses. Programmers may introduce logic or implementation errors which could result in system vulnerabilities or instability /reliability. Weaknesses may be discovered after a mission is operational, which external threat agents might attempt to exploit to inject instructions, software, or configuration changes.

Possible Mission Impact: Software threats could result in loss of data, loss of spacecraft control, unauthorized spacecraft control, or loss of mission.

Applicable to: Space Segment, Ground Segment

Reference: CCSDS 350.1-G-3, para. 3.4.9

* 1. Unauthorized Access

Access control policies based on strong authentication provide a means by which only authorized entities are allowed to perform system actions, while all others are prohibited.

“Weakness of an asset or control that can be exploited by one or more threats.” Acc. To [ISO27K, (3.77)]

“Vulnerability weakness in the TOE that can be used to violate the SFRs in some environment.” Acc. To [CC Part 1-17, Section 4.5 ‘Terms and definitions related to the AVA class’])

Possible Mission Impact: An access control breech would allow an unauthorized entity the ability to take control of a ground system or a ground system network, shut down a ground system, upload unauthorized commands to a spacecraft, obtain unauthorized data, contaminate archived data, or completely shut down a mission. If weak access controls are in place, unauthorized access might be obtained. Interception of data might result in unauthorized access because identities, identifiers, or passwords might be obtained. Social engineering could be employed to obtain identities, identifiers, passwords, or other technical details permitting unauthorized access.

Applicable to: Space Segment, Ground Segment:

Reference: CCSDS 350.1-G-3, para. 3.4.10

* 1. Supply Chain Threats

Software and hardware originate from various sources. Some of the sources are domestic, and some are not. Some are vetted, trusted sources, whereas some are not.

Chain-of-custody, even from vetted sources, is required to ensure that only genuine hardware and software, in full compliance with requirements and specifications, is delivered and integrated. Trust shall be validated and re-validated as the supply chain may have access to sensitive materials that require protection.

Resources, services and facilities with their logistical elements contribute to the supply chain that are specific for each project with resulting risks and threats that need to be considered and addressed. Resources such as cloud services utilise a shared responsibility model. Outsourced suppliers or workforce providing services require strong contractual coverage minimising risks associated with the loss of direct control by the project.

Transport of equipment and supplies can be affected and disrupted by threats such as access to parts, fuel, even labour shortages or access to rare raw materials. Considering may be necessary if the transport is being made on sensitive or critical assets and potential impacts in case of disruption, destruction, loss or access and leakage of sensitive information.

Finally, hardware and software might be tainted because it could contain hidden, malicious capabilities, since might not be produced by the claimed manufacturer and be counterfeit.

Possible Mission Impact: Supply chain disruption could result in genuine parts being unavailable, thereby resulting in the potential use of counterfeit parts. If trust is not verified, counterfeit hardware or software could be delivered and used on a mission without anyone’s knowledge. The hardware or software may contain malicious circuits or malicious code that could result in unintended mission consequences. The hardware or software might allow unauthorized access to the system or it might prohibit authorized access. It might send telemetry or observation data to an unauthorized entity. It might ignore authentic commands. Some of these scenarios could result in mission loss. Partners in the supply chain may expose or provide access to sensitive materials, cause disruption or delays to the availability of schedule critical elements. Connected suppliers with security weaknesses could be compromised and used to impact the availability of support services or to launch attacks on Agencies, systems, and missions. In addition, the mission may be seriously impacted by hardware or software that do not have all of the specified capabilities of the genuine hardware or software. The tainted hardware or software may lead to premature failure. The mission may be impacted by additional, hidden capabilities contained in the counterfeit hardware/software such as transmitting data to unauthorized and unintended destinations, intermittent system instability, damage to other system components, or other undesirable system effects that could lead to mission loss.

Applicable to: Space Segment, Ground Segment

Reference: CCSDS 350.1-G-3, para. 3.4.11/3.4.12

* 1. Other Threats with an Impact to Security

Threats such as human accidental or intentional, Physical threats such as kinetic attacks on satellites (kinetic weapon such as a missile, or laser to blind or damage the vehicle or to manipulate a satellites orbit) or a space based platform, perhaps a hijacked satellite.

For satellites or ground systems with high value information, they may be targeted by ‘characterisation’ missions to eavesdrop or monitor the capabilities of the assets (whether on-ground or in-space).

Environmental threats such as geomagnetic storms, solar radiation, radio blackouts, satellite or debris conjunction events. Earth based environmental threats may include weather events (storms, rain, snow, lightning) as well as facilities such as flooding, electrical power disruption.

Possible Mission Impact: These threats can range from mildly disruptive, temporary denial of a command link or service, through to the release of unauthorised information and potentially the destruction of a mission or the ground facilities.

Applicable to: Launch Segment, Space Segment, Ground Segment, Space-Link Communication, Supply Segment.

* 1. Summary

The following table summarises the recommended security measures to counter threat the most relevant threats for space systems [source: CCSDS 350.1-G-3, para. 5.8]. An exhaustive list of threats (but not specific to space missions) can be found in NIST Special Publication 800-30, appendix E.

: Security Mechanisms to Counter Threats, Mitigations and Contingencies

| Threat | Security Mechanisms to Counter Threat | Threat Mitigations | Threat Contingencies |
| --- | --- | --- | --- |
| Data corruption | * Data integrity schemes (hashing, check values, digital signatures)
* Resilient hardware
 | * Secure data backups
 | * Verify integrity of backups
* Hold offsite copies of critical data for cyber disaster scenarios
 |
| Ground facility physical attack | * Guards
* Gates
* Access control
 | * Alternate ground facilities
 | * Failover or hot standby to alternate site
 |
| Interception(Eavesdropping) | * Protection of traffic via encryption, frequency hopping, spread spectrum
* Protection of archive & distribution systems via encryption
 | * Use secure transmission
 | * Use hardened transmission facilities
 |
| Jamming | * Multiple uplink paths
* Multiple access points
* Frequency hopping, spread spectrum
 | * Legislation
* Monitoring
* Interdiction
* Reporting
 | * Have alternate frequencies or transmission facilities available
* Provide resilience for outages (e.g. PNT local clocks, alternate sources)
 |
| Denial-of-Service (DoS) | * Firewalls
* Routers
* Switches
* Intrusion Prevention Systems
* Private, segregated networks
* Encryption & authentication
* ISP ‘edge’ support
 | * Access control lists
* Rate limiting
* ‘expect’ scripting
* Service screening
 | * Safe Mode
* Fault detection and isolation
 |
| Masquerade / Spoofing | * Strong authentication
* Access control scheme
* Vetting of staff
* No use of open networks
 | * Strong authentication
* Session tokens
* Behaviour
* Timestamps
 | * Intrusion Detection Systems
* Intrusion Prevention Systems
 |
| Replay | * Data integrity schemes (e.g., authenticated command counter, timestamps)
 | * Sequence numbers
* One-time passwords
* Session tokens (nonces)
* Timestamps
* Challenge-response
 | * Intrusion Detection Systems
* Intrusion Prevention Systems
 |
| Software Threats | * Acceptance testing
* System evaluation (e.g., IVV, code analysis)
* COTS product use
* Continuous threat monitoring, continuous risk management
* Run-time security monitoring
* Auditing
* Software partitioning (trusted computing base)
* Supply chain confidence
* Data Leak Protection
 | * Secure software development methodologies
* Security monitoring
 | * Develop multiple, independent implementations from the same specification for higher assurance platforms
 |
| Unauthorized Access | * Encryption of TT&C and mission data
* Authentication/authorization of commands
* No use of open networks
* Access control in control centre
* Access control in cross support network
* Access control in control and dissemination systems
* Accountability of access
* Multiple access paths
* Auditing & accounting
* Non-repudiation
* Authentication tokens (e.g. smart cards)
* Access controls; flight,
* flight-to-ground, on-ground
* Access controls using data
* and service segregation
* Apply security hardening and
* least privilege principals
* Vetting of staff
 | * Strong authentication – Session tokens (nonces)
* One-time passwords
* Multi-factor authentication
* Security monitoring
 | * Intrusion Detection Systems
* Intrusion Prevention Systems
 |
| Tainted Components (hardware/software) | * Supply chain confidence
* Authenticity of components
* Vetted component suppliers
* Vetted component production
* Analysis of component functionality
* Multi-vendor component components
 | * Diverse hardware purchasing
* Blind buy purchasing
* Random IVV testing
 | * Resource utilization monitoring
* Intrusion detection
* Intrusion prevention
* Vetted back-up hardware stocks
 |
| Supply Chain | * Supply chain confidence
* Vetted/trusted sources
* chain of custody evidence
* contract and performance penalties
 | * Multiple, vetted
* sources (non-reliance on a single source)
* Strong chain of custody documentation
 | * Accumulation of:
	+ parts enabling
	+ emergency
	+ reaction
 |

Bibliography

|  |  |
| --- | --- |
| CCSDS 350.1-G-2 | Security Threats against Space Missions |
| CCSDS 350.8-M-2 | Security Guide for Mission Planners |
| CCSDS 350.8-M-2 | Information Security Glossary of Terms |
| ESA-REG-004 | ESA Security Regulations |
| IETF RFC 4949 | Internet Security Glossary, Version 2 |
| ISO/IEC 27000 | Information technology — Security techniques — Information security management systems |
| ISO/IEC 27001 | Information Security Management |
| ISO/IEC 27005 | Information security, cybersecurity and privacy protection — Guidance on managing information security risks |
| NIST SP 800-30 | Guide for Conducting Risk Assessments |
| NIST SP 800-53 Rev.5 | Computer Security Incident Handling Guide |
| NIST SP.800-160, Volume 2 | Developing Cyber Resilient Systems – A Systems Security Engineering Approach |
| NIST SP 800-161, Rev. 1 | Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations |