The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

SECURITY GUIDE FOR MISSION PLANNERS

INFORMATIONAL REPORT

CCSDS 350.7-G-2

GREEN BOOK

April 2019

The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

SECURITY GUIDE FOR MISSION PLANNERS

INFORMATIONAL REPORT

CCSDS 350.7-G-2

GREEN BOOK
April 2019

AUTHORITY

Issue:	Informational Report, Issue 2
Date:	April 2019
Location:	Washington, DC, USA

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and reflects the consensus of technical panel experts from CCSDS Member Agencies. The procedure for review and authorization of CCSDS Reports is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4).

This document is published and maintained by:

CCSDS Secretariat
National Aeronautics and Space Administration
Washington, DC, USA
Email: secretariat@mailman.ccsds.org

FOREWORD

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Report is therefore subject to CCSDS document management and change control procedures, which are defined in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4). Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be sent to the CCSDS Secretariat at the email address indicated on page i.

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People's Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.
- UK Space Agency/United Kingdom.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
- Chinese Academy of Sciences (CAS)/China.
- China Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- Electronics and Telecommunications Research Institute (ETRI)/Korea.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand.
- Hellenic National Space Committee (HNSC)/Greece.
- Hellenic Space Agency (HSA)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- Mohammed Bin Rashid Space Centre (MBRSC)/United Arab Emirates.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- South African National Space Agency (SANSA)/Republic of South Africa.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- Swiss Space Office (SSO)/Switzerland.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 350.7-G-1	Security Guide for Mission Planners, Informational Report, Issue 1	November 2010	Original issue, superseded
CCSDS 350.7-G-2	Security Guide for Mission Planners, Informational Report, Issue 2	April 2019	Current issue – Annex A has been updated to align with the revised controls in ISO/IEC 27001:2013. – Figures have been updated to reflect additional security-related CCSDS documentation. – A new discussion of resilience has been added in A4.1.

CONTENTS

1 INTRODUCTION

1.1 PURPOSE

This Guide is intended to provide guidance to mission planners in developing the management, operational, and technical security controls appropriate to the value of their system and the information processed in it.

1.2 SCOPE

The information contained in this report is not part of any CCSDS Recommended Standard. In the event of conflict between any CCSDS Recommended Standard and the material presented herein, the CCSDS Recommended Standard is the controlling specification.

Other CCSDS Recommended Standards and 'Green Book' informational reports listed in 1.6, 'References', provide more detail on particular aspects of assessing risks and implementing technical security measures.

1.3 RATIONALE

The purpose of this guide is to introduce the reader to best practices in information security, and to provide a structured process flow and templates to help ensure security aspects pertinent to space systems are not overlooked.

To date, space missions have implemented a wide variety of generally mission-specific protections for space systems and data. Information security best practices have only recently been defined and agreed upon as recognized standards across industries and national boundaries. As space systems become increasingly interconnected with ground-based IT networks, including the Internet, it becomes more important to provide an integrated approach to addressing both the security concerns traditionally understood by space systems designers, and those more typical of IT environments.

1.4 DOCUMENT STRUCTURE

This document is organized as follows:

Section 2 provides an introduction to security.

Section 3 describes the security planning process from policy definition through risk assessment and security control selection, to architecture and requirements.

Section 4 presents an introduction to common security controls and describes some controls specific to space data systems.

Annex A provides a sample template for performing security planning that incorporates the ISO 27000 series of security controls, tailored for applicability to the lifecycle and operational environment of many space data systems.

1.5 DEFINITIONS

Definitions for the security terminology applicable to this and other CCSDS documents are provided in reference [20].

1.6 REFERENCES

The following documents are referenced in this Report. At the time of publication, the editions indicated were valid. All documents are subject to revision, and users of this Report are encouraged to investigate the possibility of applying the most recent editions of the documents indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS documents.

[1] *Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 1: Introduction and General Model*. 3rd ed.. International Standard, ISO/IEC 15408-1:2009. Geneva: ISO, 2009.

[2] *Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 2: Security Functional Components*. 3rd ed. International Standard, ISO/IEC 15408-2:2008. Geneva: ISO, 2008.

[3] *Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 3: Security Assurance Components*. 3rd ed. International Standard, ISO/IEC 15408-3:2008. Geneva: ISO, 2008.

[4] *Information Technology—Security Techniques—Security Requirements for Cryptographic Modules*. 2nd ed. International Standard, ISO/IEC 19790:2012. Geneva: ISO, 2012.

[5] *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*. 5th ed. International Standard, ISO/IEC 27000:2018. Geneva: ISO, 2018.

[6] *Information Technology—Security Techniques—Information Security Management Systems—Requirements*. 2nd ed. International Standard, ISO/IEC 27001:2013. Geneva: ISO, 2013.

[7] *Information Technology—Security Techniques—Code of Practice for Information Security Controls*. 2nd ed. International Standard, ISO/IEC 27002:2013. Geneva: ISO, 2013.

[8] *Information Technology—Security Techniques—Information Security Management Systems—Guidance*. 2nd ed. International Standard, ISO/IEC 27003:2017. Geneva: ISO, 2017.

[9] *Information Technology—Security Techniques—Information Security Management—Monitoring, Measurement, Analysis and Evaluation*. 2nd ed. International Standard, ISO/IEC 27004:2016. Geneva: ISO, 2016.

[10] *Information Technology—Security Techniques—Information Security Risk Management*. 3rd ed. International Standard, ISO/IEC 27005:2018. Geneva: ISO, 2018.

[11] *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. Rev. 1 (Updated 6/5/2014). National Institute of Standards and Technology Special Publication 800-37 Rev. 1. Gaithersburg, Maryland: NIST, February 2010.

[12] *Security and Privacy Controls for Federal Information Systems and Organizations*. Rev. 4 (Updated 1/22/2015). National Institute of Standards and Technology Special Publication 800-53 Rev. 4. Gaithersburg, Maryland: NIST, April 2013.

[13] *Guide for Mapping Types of Information and Information Systems to Security Categories*. Rev. 1. National Institute of Standards and Technology Special Publication SP 800-60 Vol. 1 Rev. 1. Gaithersburg, Maryland: NIST, August 2008.

[14] "CIS Controls." CIS Center for Internet Security. https://www.cisecurity.org/controls/.

[15] IT Governance Institute. *COBIT 4.1*. Rolling Meadows, Illinois: ISACA, 2007.

[16] *Commercial Aircraft Information Security Concepts of Operation and Process Framework*. ARINC Report 811. Annapolis, Maryland: ARINC, 2005.

[17] *The Application of Security to CCSDS Protocols*. Issue 3. Report Concerning Space Data System Standards (Green Book), CCSDS 350.0-G-3. Washington, D.C.: CCSDS, March 2019.

[18] *Security Threats against Space Missions*. Issue 2. Report Concerning Space Data System Standards (Green Book), CCSDS 350.1-G-2. Washington, D.C.: CCSDS, December 2015.

[19] *CCSDS Guide for Secure System Interconnection*. Issue 2. Report Concerning Space Data System Standards (Green Book), CCSDS 350.4-G-2. Washington, D.C.: CCSDS, April 2019.

[20] *Information Security Glossary of Terms*. Issue 2. Recommendation for Space Data System Practices (Magenta Book), CCSDS 350.8-M-2. Forthcoming.

[21] *Security Architecture for Space Data Systems*. Issue 1. Recommendation for Space Data System Practices (Magenta Book), CCSDS 351.0-M-1. Washington, D.C.: CCSDS, November 2012.

2 OVERVIEW

2.1 TARGET AUDIENCE

This document is intended to provide the mission planner, program manager, and/or engineering lead with a basic understanding of the strategy, purpose, and process flow of integrating security early into the development of a space system.

2.2 SECURITY CONCEPTS

The objective of system security planning is to improve the protection of information and information system resources to ensure sustained mission success and continuity. Both space systems information and equipment are subject to a variety of threats (natural, accidental, and deliberate) and require varying degrees of protection depending upon the nature of the mission and the value of physical and informational assets.

2.3 SECURITY MANAGEMENT

Each organization should develop, document, and implement an organization-wide program to provide information security for the information and information systems that support the operations and assets of that organization. ISO/IEC 27000 (reference [5]), which provides a broad overview of information security management, calls this program an Information Security Management System (ISMS).

According to ISO/IEC 27000:

> Information security is achieved through the implementation of an applicable set of controls, selected through the chosen risk management process and managed using an ISMS, including policies, processes, procedures, organizational structures, software, and hardware to protect the identified information assets. These controls need to be specified, implemented, monitored, reviewed, and improved as necessary, to ensure the specific security and business objectives of the organization are met. Relevant information security controls are expected to be integrated seamlessly with an organization's business processes.

3 SECURITY PLANNING

3.1 INTRODUCTION

The objective of a security plan is to provide, in one place, an assessment, updated on an ongoing basis, of the present status of the system's security protections and risks. The security plan is essential to informing management decisions and establishing accountability for the development and maintenance of security protections.

Every mission should have a security plan and undergo a risk assessment. This guide is directed toward the development and use of the mission's security plan.

The security plan should either include or reference applicable system policies, security architecture, and operating procedures. These are discussed in more detail in references [17] and [21]. It should also include or reference a risk assessment that matches the threats to the system (and its assets) with known vulnerabilities that could be exploited to carry out an attack or otherwise cause adverse events. Where known vulnerabilities are found to match existent threats, the risk assessment determines the potential impacts of each to the system, as discussed in reference [18].

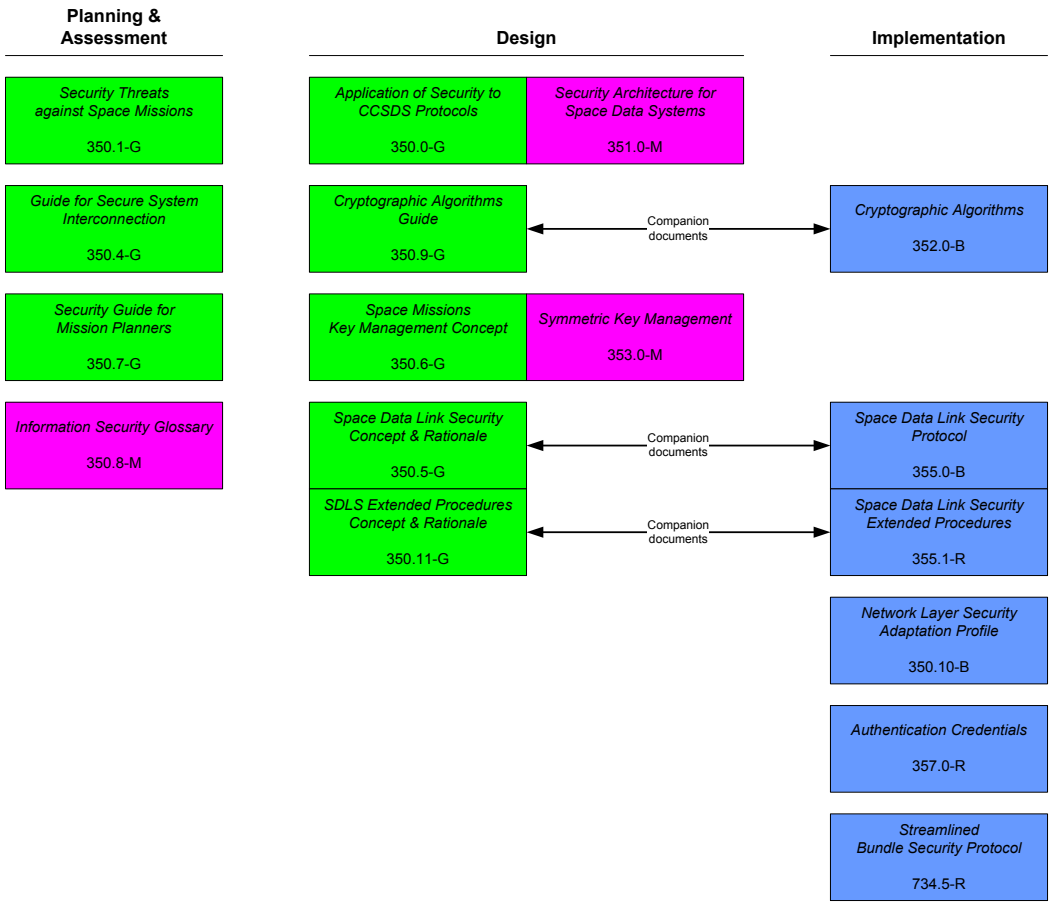

Figure 3-1: CCSDS Security Document Tree

Figure 3-1 depicts the logical organization of existing CCSDS security-related documentation. Some documents may still be in the review stage. Figure 3-2 depicts how these documents have evolved from a single 'Green Book' to a more fully-developed security framework and core suite of security recommendations to the mission designer. Areas of potential future CCSDS work are tentatively outlined, but unofficial as of this time.

Figure 3-2: Evolution of CCSDS Security Framework

3.2 SECURITY POLICY

A system's security policy is its 'concept of operations' with respect to security. It outlines how the system (which may be either considered broadly as a combination of infrastructure, multiple hardware and software components, and the individuals operating and maintaining them, or considered narrowly as a particular component in isolation) is intended to operate, and what action is to be taken when it operates outside its intended parameters.

Every mission should define a security policy as an element of its overall mission concept definition. The mission security policy must be observant of any higher-level organization security policies but must clearly state:

a) the classification and therefore level of protection of all the information (e.g., telemetry, telecommand, software, and ground systems data) associated with the mission, both live and archived;

b) the roles of those who have access to the system;

c) the integrity requirements of the system; and

d) the availability requirements of the system.

A well-considered security policy should precede system-requirements definition; it will help to minimize the risk of unforeseen security problems later in implementation.

3.3 INFORMATION CATEGORIZATION

In order to select appropriate security controls, organizations must clearly understand the criticality and sensitivity of the information that will be handled by the system according to the criteria of confidentiality, availability, and integrity. Systems may handle several different data types, each with different attributes. An example of information criticality and sensitivity categories applicable to various systems may be found in reference [13].

Military or dual-use systems are usually subject to national security classification regulations that override organizational discretion in categorizing information. Civil systems may be bound by other laws and policies (e.g., export and copyright restrictions) controlling the handling of specific information types. Organizations should identify their system's operational availability and integrity requirements for the information that may be unaddressed by legal and national-security requirements pertaining to information confidentiality.

3.4 THREAT ASSESSMENT

A threat assessment must consider the mission type and the information security threats to that mission. It is important to consider all parts of the mission architecture during all phases of the mission, as the threats relevant to the mission will change as the mission progresses. For a more detailed discussion of mission threat assessment, see reference [18].

It should be noted that the threat assessment will use the outputs of the Security Policy and Security Interconnection documents to help identify attack vectors and the value of the data and assets to be protected.

3.5 SECURITY REQUIREMENTS AND CONTROLS

3.5.1 GENERAL

Organizations must adopt a set of security controls and a process to implement and manage those controls in order to protect their information and information systems. The controls selected or planned must be documented in system requirements documentation.

Security requirements derive from security policy as well as functional system requirements that affect security. It is important to keep the two concepts separate; while requirements

mandate system capabilities, policy mandates the uses of those capabilities. For example, to reject commands that fail authentication is a policy; to build a capability that can authenticate commands is a requirement. Avoid placing security policy statements into requirements documents. Requirements should state the capabilities needed to implement the security policy.

Similarly, avoid placing 'negative' security requirements into requirements documents (i.e., expressing a requirement that something should *not* occur). Such requirements are difficult to test for compliance. It is commonplace within IT to encounter systems that pass all functional testing and yet have obvious, easily exploited security flaws. This is usually explainable by functional tests that prove what the system does, and not what it does not do.

Security controls provide the mapping from requirements and policy to system design and operations. Most security controls belong to one of three basic classes: *protective*, *detective*, or *reactive*. Protective controls are measures designed to prevent a negative event from occurring. Detective controls aim to inform the organization about an event. Reactive controls are 'after the fact' measures to restore the system to nominal operation and/or collect forensic information about the nature and extent of the event. (It should be noted that current trends in IT security monitoring, event correlation, and automated incident response do lessen the practical ability to distinguish between these three classes of controls in an IT implementation.)

Organizations must also maintain a mission system's security controls throughout the lifetime of the mission, as described below in section 3.6.4.

3.5.2 USE OF STANDARDS

Security must be an integral part of the overall system design. Security flaws are often subtle, and the most troublesome security design flaws arise from unintended effects of interactions between components in a system. Unlike programming errors, such vulnerabilities cannot be easily remedied. It is advantageous to employ proven and well-known standards in security designs.

This is particularly true in the field of cryptographic mechanisms. Algorithms that have been subjected to peer review by the cryptographic community are, in general, more mathematically robust and less likely to contain hidden weaknesses.

3.6 SECURITY PLAN

3.6.1 GENERAL

Each organization should develop a system security plan that references or provides a summary of the system security requirements, describes the security controls in place or planned for meeting those requirements, and describes the results of the risk assessment of

the system. The plan should also detail organizational decisions regarding what is to be done about any discrepancies, including whether to accept risk or proceed as is.

The purpose of the system security plan is to provide an overview of the system security requirements, and to describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and the expected behavior of all individuals who access the system. Additional information may be included in the plan, and the format may be organized according to organizational needs, so long as the major sections described in this document are adequately covered and readily identifiable.

3.6.2 SYSTEM DEFINITION

A security plan may have multiple subsystems or subordinate systems that inherit their policies and/or controls. The mission planner should include both space and ground elements in defining security for the early stages of planning, although each element should have its own security plan as development progresses toward implementation.

A security plan should generally describe resources under the same direct management control. When a complex system includes interacting elements under different management control (e.g., spacecraft and ground systems), the elements should be described separately, and interactions between them should be carefully noted. Additionally, there must be assurance that any shared resources (e.g., organizational processes, networks, and physical facilities) are adequate for the highest criticality and sensitivity handled.

The security plan should follow the functional organization of the system. The process of uniquely assigning information resources to an information system defines the security boundary for that system. The security boundary should take into account regulatory authority, trust relationships, supply chain, and line management authority.

3.6.3 RISK ASSESSMENT

The risk assessment uses the output of the threat assessment to assess the likelihood of any potential impact occurring. Risk assessment involves assessing system vulnerabilities that correspond to an identified threat. In the early stages of development, vulnerabilities may be theoretical in nature; in later stages, their exploitability in practice will be highly dependent upon implementation details.

Risk is a function of the impact of an occurrence and the likelihood of that impact's occurrence. Impact may be considered qualitatively (e.g., low/medium/high) or quantitatively (e.g., lost revenue due to outages) according to organizational needs.

The risk assessment should also identify, for each risk found, a mitigation strategy (to be prioritized and scheduled as the organization chooses) or a recommendation to accept the risk.

3.6.4 APPROVAL AND LIFE CYCLE

Organizational policy should clearly define who is responsible for approving the system security plan and who is responsible for authorizing the system to operate. By authorizing the system to operate, the manager accepts its associated risks.

Management authorization should be based on an assessment of management, operational, and technical controls. Since the system security plan establishes and documents the security controls, risk assessment, and risk mitigation actions or acceptance of residual risks, it should form the basis for the authorization.

The applicability and usefulness of the security controls originally implemented should be periodically re-evaluated as threats to the system change over time, and especially as system components are replaced or upgraded during normal maintenance. Security controls should be changed as appropriate to adapt to changes in their associated threats and specific vulnerabilities in system components. Where applicable, a periodic review of the system security plan should be used to renew the management authorization.

4 SECURITY CONTROLS FRAMEWORKS

4.1 INTRODUCTION

The purpose of a security controls framework is to provide a hierarchical grouping of related security concerns to guide the system owner in setting policy and aid in decomposing policy into more specific architectural and procedural requirements for implementation. A security controls framework makes it possible to assess whether and how the system meets its security objectives.

Most frameworks will recommend more stringent or less stringent controls based upon the predetermined criticality and sensitivity (with respect to confidentiality, availability, and integrity) of the data types the system processes.

4.2 ISO/IEC 27000 SERIES

The ISO/IEC 27001 standard (reference [6]) identifies a security controls framework encompassing management, operational, and technical capabilities. The framework addresses the most common aspects of protecting the confidentiality, integrity, and availability of information and information systems. There are dozens of individual controls available in the ISO framework, which are organized according to the high-level groupings listed in table A-1. An overview of information security management may be found in ISO/IEC 27000 (reference [5]). The companion ISO/IEC documents numbered 27002-27005 (references [7]–[10]) provide accompanying implementation guidance.

4.3 OTHER FRAMEWORKS

In addition to ISO/IEC standards (and national standards derived from ISO/IEC), there are several widely used security controls frameworks used by private entities and government agencies. Among these are:

a) the National Institute for Standards and Technology (NIST) Risk Management Framework, used by United States civilian government agencies and defined in NIST Special Publications 800-37, 800-53, 800-60, et al. (references [11], [12], and [13]);

b) the ‘Top 20’ Critical Security Controls (reference [14]), published by the Center for Internet Security (CIS);

c) the Control Objectives for Information and related Technology (COBIT) (reference [15]) published by the Information Systems Audit and Control Association (ISACA); and,

d) the considerations found in ARINC Report 811 (reference [16]), *Commercial Aircraft Information Security Concepts of Operation and Process Framework*.

4.4 SPECIAL CONSIDERATIONS FOR SPACE SYSTEMS

In addition to the security controls from a well-known IT security controls framework such as ISO 27001, there are organization-specific or system-specific security controls that may be locally defined. Some security concerns are particular to space systems and may not be clearly addressed in IT controls frameworks applicable to generic IT systems.

The template in Annex A includes some sample controls pertinent to space systems.

ANNEX A

MISSION SECURITY PLAN TEMPLATE

A1 INTRODUCTION

The following template is intended to aid the mission planner in understanding and applying recognized best practices in security. It takes the form of a document that would normally be compiled to satisfy organizational directives or a third-party security audit.

A2 GENERAL SYSTEM INFORMATION

A2.1 SYSTEM NAME

The system name and/or any unique reference identifier(s) the organization uses should be listed.

A2.2 SYSTEM OPERATIONAL STATUS

The operational status of the system should be indicated. If more than one status is selected, the part of the system covered under each status must be listed:

- Operational;
- Under Development;
- Major Modification.

A2.3 RESPONSIBLE INDIVIDUALS

A2.3.1 System Owner

This section should identify the individual with overall budgetary and management authority over the development and operation of the system. The person may be identified by title and agency, although it is preferable to include specific individual contact information (e.g., name, email address, and telephone number).

A2.3.2 Authorizing Official

This section should identify the individual designated by the organization to have the authority and responsibility to approve the fitness of the system for operation. This may be the system owner or another individual. The person may be identified by title and agency, although it is preferable to include specific individual contact information (e.g., name, email address, and telephone number).

A2.3.3 Assignment of Security Responsibility

This section should identify the individual with overall authority and responsibility for the security of the system. The person may be identified by title and agency, although it is preferable to include specific individual contact information (e.g., name, email address, and telephone number).

A2.3.4 Other Designated Contacts

This section should identify other key personnel, if applicable. The person may be identified by title and agency, although it is preferable to include specific individual contact information (e.g., name, email address, and telephone number).

A3 GENERAL SYSTEM DESCRIPTION

A3.1 DATA TYPES AND SENSITIVITY

The types of data the system processes and the sensitivity of each data type, with respect to confidentiality, integrity, and availability, must be listed. Data sensitivity will be highly specific to the customer or mission needs. For example, a satellite mission serving multiple customers may have some customers with low confidentiality needs and other customers whose data requires moderate or high confidentiality protections.

For illustrative purposes only, a hypothetical spacecraft should be considered. Example data types (and sensitivity levels) would likely include:

- Spacecraft telecommands (low confidentiality, high integrity, high availability);
- Spacecraft telemetry (high confidentiality, high integrity, low availability); and,
- Data relay or rebroadcast data (low confidentiality, low integrity, moderate availability).

A3.2 SYSTEM CRITICALITY

The types of data listed in section A3.1 above should be used to establish an overall criticality for the system that will influence default protections for components within the system's security boundary.

A3.3 SYSTEM ENVIRONMENT

A general technical description of the system must be provided, and the primary hardware, software, and communications components must be identified.

A4 SYSTEM INTERCONNECTIONS

A4.1 INFORMATION SHARING

Interconnected systems and system identifiers should be listed when appropriate. The system, name, organization, and system type (major application or general support system) must be provided. If there is a formal agreement to interconnect on file, the date of said agreement, data types exchanged, certification or accreditation status, and the authorizing official(s), it should be indicated.

A4.2 RELATED LAWS/REGULATIONS/POLICIES

Laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system must be listed.

A5 SECURITY CONTROLS

A5.1 GENERAL

An appropriate security control baseline must be selected. Then, a thorough description of how all security controls in the applicable baseline are being implemented, or are planned to be implemented, must be provided. The description should contain: 1) the security control title; 2) how the security control is being implemented or is planned to be implemented; 3) any scoping guidance that has been applied and what type of consideration; and 4) indication of whether the security control is a common control and who is responsible for its implementation.

A5.2 SPACE SYSTEM SECURITY CONTROLS

A5.2.1 General

As described in 4.4, many of the ISO 27001 and related security controls from reference [6] may not be directly applicable in a space environment. Generic information technology frameworks commonly omit many concerns common to a space mission environment and include many concerns pertinent to a generic information technology system not applicable to a space mission environment. The security controls listed below in table A-1 are a set of controls that have been tailored to the most common needs of space systems, ground operations systems, and development facilities for spacecraft or ground systems. Each of these controls, numbered and grouped according to their related ISO 27001 subject areas (A.5, A.6, A.7, …), either reference existing ISO 27001 controls that are also applicable to space missions or list objectives specific to space missions that are absent from ISO 27001. These may be selected according to organizational needs to establish policies and system requirements or recommend countermeasures to probable risks. These controls may also be used to augment other controls if compliance with other control frameworks is required by law or policy.

A5.2.2 Plan for the Whole Mission

The security controls implemented for a particular system should take into consideration the entire duration of the mission including pre- and post-flight periods. While different security controls may be appropriate for implementation during different mission phases, the overall selection of security controls for a mission should ensure that one phase's protections (e.g., for confidentiality of proprietary data) are not nullified by vulnerabilities left unmitigated during other phases.

The mission planner should evaluate the applicability of each of the controls below in table A-1 to the mission needs and objectives. Where certain controls are considered inappropriate, the plan should document those reasons. Where certain controls are considered necessary for a mission, even if not recommended below, the plan should include them and document the reasons. Some controls that have not been provided in previous space missions may need to be provided in future ones due to the changes in system capabilities and the threat environment.

A5.2.3 Plan for Resilience

Security controls implemented for space systems and ground operations systems should particularly take into consideration a mission's need for overall *resilience*: the system's capability to quickly respond to, and effectively recover from, adverse events. Designing for resilience includes contingency planning that anticipates specific potential events. However, generalized system resilience (and availability assurance) is optimized when feedback-response capabilities are included in the system architecture and concept of operations. For example, component redundancy is commonly implemented to recover from anticipated or known failure modes, but additional measures may be needed to withstand/operate through unknown failure modes.

A minimum nominal ('mission success criteria') operational capability should be defined in the mission requirements, so that a system can be architected to optimize the return to a steady state after unknown contingencies within a survivable time frame.

Cyber-attack threats in particular are appropriately defended against by security controls and policies/procedures that plan for contingency scenarios, including, for example, potential real-time operational decisions to:

- shut off or degrade system capabilities;
- isolate networks for cyber-attack containment; and/or
- operate throughout the absence of normal indicators of system integrity.

Table A-1: Security Controls for Space Systems

Control Number	Security Control Objective	Development Systems	Ground Operations Systems	Space Systems
A.5 Information security policies				
A.5.1 Management direction for information security Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.				
A.5.1.MP1	The ISO 27001 controls: – A.5.1.1 Policies for information security – A.5.1.2 Review of the policies for information security should be satisfied for all facilities and systems affiliated with a mission.	•	•	•
A.5.1.MP2	Security controls should give highest priority to the safe operation of the spacecraft and the safety of the occupants in the case of manned spacecraft.		•	•
A.5.1.MP3	Space systems should provide security controls to mitigate the safety risks to bystanders at expected launch and landing areas.		•	•
A.5.1.MP4	Security controls for space systems should be designed so as not to inhibit mission accomplishment. A mission that places a higher priority on avoiding a security breach than on accomplishing the mission objectives should clearly state so in the mission security policy.		•	•
A.5.1.MP5	Security controls for space systems should be designed to be suitable for operations and maintenance throughout the duration of the mission, to the extent known. For example, selection of cryptographic methods should take into account the increasing computational resources available to potential attackers that may render current methods obsolete, as time passes. This may be addressed by anticipating a means of upgrading spacecraft flight software and providing reserve capacity to accommodate upgrades.			•
A.6 Organization of information security				
A.6.1 Internal organization Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.				
A.6.1.MP1	The ISO 27001 controls: – A.6.1.1 Information security roles and responsibilities – A.6.1.3 Contact with authorities – A.6.1.4 Contact with special interest groups – A.6.1.5 Information security in project management should be satisfied for all facilities and systems affiliated with a mission.	•	•	•
A.6.1.MP2	The ISO 27001 control: – A.6.1.2 Segregation of duties should be satisfied for all development and ground operations facilities.	•	•	
A.6.2 Mobile devices and teleworking Objective: To ensure the security of teleworking and use of mobile devices.				
A.6.2.MP1	The ISO 27001 controls: – A.6.2.1 Mobile device policy – A.6.2.2 Teleworking should be satisfied for all development and ground operations facilities.	•	•	

Control Number	Security Control Objective	Development Systems	Ground Operations Systems	Space Systems
A.7 Human resource security				
A.7.1 Prior to employment Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.				
A.7.1.MP1	The ISO 27001 controls: – A.7.1.1 Screening – A.7.1.2 Terms and conditions of employment should be satisfied for all facilities and systems affiliated with a mission.	●	●	●
A.7.2 During employment Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.				
A.7.2.MP1	The ISO 27001 controls: – A.7.2.1 Management responsibilities – A.7.2.2 Information security awareness, education, and training – A.7.2.3 Disciplinary process should be satisfied for all facilities and systems affiliated with a mission.	●	●	●
A.7.3 Termination or change of employment Objective: To protect the organization's interests as part of the process of changing or terminating employment.				
A.7.3.MP1	The ISO 27001 control: – A.7.3.1 Termination responsibilities should be satisfied for all facilities and systems affiliated with a mission.	●	●	●
A.8 Asset management				
A.8.1 Responsibility for assets Objective: To identify organizational assets and define appropriate protection responsibilities.				
A.8.1.MP1	The ISO 27001 controls: – A.8.1.1 Inventory of assets – A.8.1.2 Ownership of assets – A.8.1.3 Acceptable use of assets – A.8.1.4 Return of assets should be satisfied for all development and ground operations facilities.	●	●	
A.8.2 Information classification Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.				
A.8.2.MP1	The ISO 27001 controls: – A.8.2.1 Classification of information – A.8.2.2 Labelling of information – A.8.2.3 Handling of assets should be satisfied for all facilities and systems affiliated with a mission.	●	●	●
A.8.3 Media handling Objective: To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.				
A.8.3.MP1	The ISO 27001 controls: – A.8.3.1 Management of removable media – A.8.3.2 Disposal of media – A.8.3.3 Physical media transfer should be satisfied for all development and ground operations facilities.	●	●	

Control Number	Security Control Objective	Development Systems	Ground Operations Systems	Space Systems
A.9 Access control				
A.9.1 Business requirements of access control Objective: To limit access to information and information processing facilities.				
A.9.1.MP1	The ISO 27001 controls: – A.9.1.1 Access control policy – A.9.1.2 Access to networks and network services should be satisfied for all development and ground operations facilities. These controls should be satisfied for all space systems in which networking protocols are used, particularly where mobile or ad hoc networking is enabled.	•	•	•
A.9.2 User access management Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.				
A.9.2.MP1	The ISO 27001 controls: – A.9.2.1 User registration and deregistration – A.9.2.2 User access provisioning – A.9.2.3 Management of privileged access rights – A.9.2.4 Management of secret authentication information of users – A.9.2.5 Review of user access rights – A.9.2.6 Removal or adjustment of access rights should be satisfied for all development and ground operations facilities. These controls should also be satisfied for manned space systems if there is a need to attribute crew actions to particular individuals.	•	•	•
A.9.3 User responsibilities Objective: To make users accountable for safeguarding their authentication information.				
A.9.3.MP1	The ISO 27001 control: – A.9.3.1 Use of secret authentication information should be satisfied for all ground operations facilities. This control should be satisfied for manned space systems if there is a need to attribute crew actions to particular individuals.		•	•
A.9.4 System and application access control Objective: To prevent unauthorized access to systems and applications.				
A.9.4.MP1	The ISO 27001 controls: – A.9.4.1 Information access restriction – A.9.4.2 Secure log-on procedures – A.9.4.3 Password management system – A.9.4.4 Use of privileged utility programs – A.9.4.5 Access control to program source code should be satisfied for all development and ground operations facilities.	•	•	
A.9.6.MP2	Space systems should provide an isolated computing environment for critical vehicle control functions, separate from that used for other in-flight computing functions. Separation may be achieved through various means, such as dedicated physical processing units, hypervisors, or other functional partitioning in hardware and software (e.g. ARINC 653). Regardless of implementation, the objective is that critical functions should not be vulnerable to disruption due to a failure or breach in non-critical functions.			•

Control Number	Security Control Objective	Development Systems	Ground Operations Systems	Space Systems
A.10 Cryptography				
A.10.1 Cryptographic controls Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information.				
A.10.1.MP1	The ISO 27001 controls: – A.10.1.1 Policy on the use of cryptographic controls – A.10.1.2 Key management should be satisfied for all facilities and systems affiliated with a mission.	●	●	●
A.10.1.MP2	Space systems and ground systems should provide cryptographic authentication in order to protect telecommands. Keyed authentication should be used so that the receiving end can verify the identity of the source and the data integrity of the telecommand.	●	●	●
A.10.1.MP3	Space systems and ground systems should provide for encryption in order to ensure the confidentiality (where required by policy) of telecommands, telemetry, audio, and video data.	●	●	●
A.10.1.MP4	Space systems and ground systems should use cryptographic components (including software, where appropriate) that have been validated for correctness by an external third party according to recognized criteria (e.g., Common Criteria, references [1]–[3], or ISO/IEC 19790, reference [4]).	●	●	●
A.10.1.MP5	Space systems and ground systems should protect cryptographic keys used for telecommands and telemetry against key recovery by unauthorized parties.	●	●	●
A.11 Physical and environmental security				
A.11.1 Secure areas Objective: To prevent unauthorized physical access, damage, and interference to the organization's information and information processing facilities.				
A.11.1.MP1	The ISO 27001 controls: – A.11.1.1 Physical security perimeter – A.11.1.2 Physical entry controls – A.11.1.3 Securing offices, rooms, and facilities – A.11.1.4 Protecting against external and environmental threats – A.11.1.5 Working in secure areas – A.11.1.6 Delivery and loading areas should be satisfied for all development and ground operations facilities.	●	●	
A.11.2 Equipment Objective: To prevent loss, damage, theft, or compromise of assets and interruption to the organization's operations.				
A.11.2.MP1	The ISO 27001 controls: – A.11.2.1 Equipment siting and protection – A.11.2.2 Supporting utilities – A.11.2.3 Cabling security – A.11.2.4 Equipment maintenance should be satisfied for all ground operations facilities with telecommanding capability.		●	
A.11.2.MP2	The ISO 27001 controls: – A.11.2.1 Equipment siting and protection – A.11.2.4 Equipment maintenance should be satisfied for all spacecraft processing facilities. Spacecraft and spacecraft components should be protected against unauthorized modification during pre-flight handling and storage.	●		

Control Number	Security Control Objective	Development Systems	Ground Operations Systems	Space Systems
A.11.2.MP3	The ISO 27001 controls: – A.11.2.5 Removal of assets – A.11.2.6 Security of equipment off premises – A.11.2.7 Secure disposal or reuse of equipment should be satisfied for all development and ground operations facilities.	●	●	
A.11.2.MP4	The ISO 27001 controls: – A.11.2.8 Unattended user equipment – A.11.2.9 Clear desk and clear screen policy should be satisfied for all ground operations facilities.		●	
A.11.2.MP5	Ground operations systems should provision for trajectory prediction and object tracking in order to predict potential collisions of the spacecraft with other objects.		●	
A.11.2.MP6	Space systems should consider provisioning a collision avoidance capability.			●
A.12 Operations security				
A.12.1 Operational procedures and responsibilities Objective: To ensure correct and secure operations of information processing facilities.				
A.12.1.MP1	The ISO 27001 controls: – A.12.1.1 Documented operating procedures – A.12.1.2 Change management – A.12.1.3 Capacity management should be satisfied for all facilities and systems affiliated with a mission.	●	●	●
A.12.1.MP2	The ISO 27001 control: – A.12.1.4 Separation of development, testing, and operational environments should be satisfied for all development and ground operations facilities. Systems should be designed to minimize access to operational components for purposes other than direct mission integration and operations (e.g., by providing data replication for indirect/offline mission support).	●	●	
A.12.2 Protection from malware Objective: To ensure that information and information processing facilities are protected against malware.				
A.12.2.MP1	The ISO 27001 control: – A.12.2.1 Controls against malware should be satisfied for all development and ground operations facilities. This control should be satisfied for space systems in which network protocols are used, depending upon the processing capabilities (onboard applications, network stack, etc.) of the spacecraft.	●	●	●
A.12.3 Backup Objective: To protect against loss of data.				
A.12.3.MP1	The ISO 27001 control: – A.12.3.1 Information backup should be satisfied for all development and ground operations facilities.	●	●	
A.12.4 Logging and monitoring Objective: To record events and generate evidence.				
A.12.4.MP1	The ISO 27001 controls: – A.12.4.1 Event logging – A.12.4.2 Protection of log information – A.12.4.3 Administrator and operator logs should be satisfied for all facilities and systems affiliated with a mission. NOTE: Telemetry is the normal means of recording spacecraft events.	●	●	●

Control Number	Security Control Objective	Development Systems	Ground Operations Systems	Space Systems
A.12.4.MP2	All telecommand activity should be logged. NOTE: Space systems may be unable to provide onboard logging of certain hardware-decoded, 'essential' commands.	●	●	●
A.12.4.MP3	The ISO 27001 control: – A.12.4.4 Clock synchronization should be satisfied for all ground operations systems.		●	
A.12.4.MP4	Space systems and ground systems should provide time synchronization capabilities in order to provide accurate situational awareness for coordinating operations. Spacecraft telemetry should provide an indication of spacecraft internal time. Ground systems should calibrate the time reported in spacecraft telemetry and monitor the deviation of spacecraft internal clocks from ground-based time, accounting for expected transmission delays in receipt of telemetry.		●	●
A.12.5 Control of operational software Objective: To ensure the integrity of operational systems.				
A.12.5.MP1	The ISO 27001 control: – A.12.5.1 Installation of software on operational systems should be satisfied for all facilities and systems affiliated with a mission.	●	●	●
A.12.5.MP2	Space systems should provide the capability to detect modifications to onboard software. The implementation should provide a means to check hashes or signatures for installed software components and data loads, to verify their integrity against known-good values in run time and/or report these signatures in telemetry.			●
A.12.6 Technical vulnerability management Objective: To prevent exploitation of technical vulnerabilities.				
A.12.6.MP1	The ISO 27001 control: – A.12.6.1 Management of technical vulnerabilities – A.12.6.2 Restrictions on software installation should be satisfied for all facilities and systems affiliated with a mission. Security controls should be reviewed periodically for obsolescence and the discovery of technical vulnerabilities. The system's security policy should define the frequency of reviews.	●	●	●
A.12.7 Information systems audit considerations				
A.12.7.MP1	The ISO 27001 controls: – A.12.7.1 Information systems audit controls should be satisfied for all development and ground operations facilities.	●	●	
A.13 Communications security				
A.13.1 Network security management Objective: To ensure the protection of information in networks and its supporting information processing facilities.				
A.13.1.MP1	The ISO 27001 controls: – A.13.1.1 Network controls – A.13.1.2 Security of network services – A.13.1.3 Segregation in networks should be satisfied for all development and ground operations facilities. This control should be satisfied for space systems where network protocols are used.	●	●	●
A.13.1.MP2	Space systems should provide segregation between critical vehicle communications and other in-flight communications or networking. Reference [16] describes one potential architecture for providing such segregation.			●

Control Number	Security Control Objective	Development Systems	Ground Operations Systems	Space Systems
A.13.2 Information transfer Objective: To maintain the security of information transferred within an organization and with any external entity.				
A.13.2.MP1	The ISO 27001 controls: – A.13.2.1 Information transfer policies and procedures – A.13.2.2 Agreements on information transfer – A.13.2.3 Electronic messaging – A.13.2.4 Confidentiality or nondisclosure agreements should be satisfied for all facilities and systems affiliated with a mission. Sample processes and templates for documenting such agreements are described in reference [19]. This control should be satisfied for space systems in which third-party services (e.g., data relay services) are used.	●	●	●
A.13.2.MP2	Consideration should be given to employing security controls that facilitate the use of cross-support within the mission's security policy. For example, the communications architecture may need to anticipate the possible occasional use of other organizations' RF ground stations.	●	●	●
A.14 System acquisition, development, and maintenance				
A.14.1 Security requirements of information systems Objective: To ensure information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems that provide services over public networks.				
A.14.1.MP1	The ISO 27001 control: – A.14.1.1 Information security requirements analysis and specification – A.14.1.2 Securing application services on public networks – A.14.1.3 Protecting application services transactions should be satisfied for all facilities and systems affiliated with a mission.	●	●	●
A.14.2 Security in development and support processes Objective: To ensure information security is designed and implemented within the development lifecycle of information systems.				
A.14.2.MP1	The ISO 27001 controls: – A.14.2.1 Secure development policy – A.14.2.2 System change control procedures – A.14.2.3 Technical review of applications after operating platform changes – A.14.2.4 Restrictions on changes to software packages – A.14.2.5 Secure system engineering principles – A.14.2.6 Secure development environment – A.14.2.7 Outsourced development – A.14.2.8 System security testing – A.14.2.9 System acceptance testing should be satisfied for all facilities and systems affiliated with a mission.	●	●	●
A.14.2.MP2	Space systems should detect the loss, resequencing, or attempted replay of received telecommands.			●
A.14.2.MP3	Space systems should provide the capability to authorize execution of individual telecommands according to a defined time window.			●
A.14.2.MP4	Ground systems should detect the loss or data corruption of received telemetry.		●	

Control Number	Security Control Objective	Development Systems	Ground Operations Systems	Space Systems
A.14.3 Test data Objective: To ensure the protection of data used for testing.				
A.14.3.MP1	The ISO 27001 controls: – A.14.3.1 Protection of test data should be satisfied for all facilities and systems affiliated with a mission.	●	●	●
A.14.3.MP2	Systems should restrict the dissemination of detailed spacecraft ground test procedures and configurations.	●	●	●
A.14.3.MP3	Spacecraft ground test configurations should validate the correct operation of security controls for spacecraft communications (especially for telecommands and telemetry).	●	●	●
A.15 Supplier relationships				
A.15.1 Information security in supplier relationships Objective: To ensure protection of the organization's assets that is accessible by suppliers.				
A.15.1.MP1	The ISO 27001 controls: – A.15.1.1 Information security policy for supplier relationships – A.15.1.2 Addressing security within supplier agreements – A.15.1.3 Information and communication technology supply chain should be satisfied for all facilities and systems affiliated with a mission.	●	●	●
A.15.2 Supplier service delivery management Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.				
A.15.2.MP1	The ISO 27001 controls: – A.15.2.1 Monitoring and review of supplier services – A.15.2.2 Managing changes to supplier services should be satisfied for all systems. This control should be satisfied for space systems where third-party services are used, for example, for data relay.	●	●	●
A.16 Information security incident management				
A.16.1 Management of information security incidents and improvements Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.				
A.16.1.MP1	The ISO 27001 controls: – A.16.1.1 Responsibilities and procedures – A.16.1.2 Reporting information security events – A.16.1.3 Reporting information security weaknesses – A.16.1.4 Assessment of and decision on information security events – A.16.1.5 Response to information security incidents – A.16.1.6 Learning from information security incidents – A.16.1.7 Collection of evidence should be satisfied for all facilities and systems affiliated with a mission.	●	●	●
A.16.2.MP2	Space systems should have a policy for handling recovery/disposal of flight hardware and/or debris.			●

Control Number	Security Control Objective	Development Systems	Ground Operations Systems	Space Systems
A.17 Information security aspects of business continuity management				
A.17.1 Information security continuity Objective: Information security continuity shall be embedded in the organization's business continuity management systems.				
A.17.1.MP1	The ISO 27001 controls: – A.17.1.1 Planning information security continuity – A.17.1.2 Implementing information security continuity – A.17.1.3 Verify, review, and evaluate information security continuity should be satisfied for all facilities and systems affiliated with a mission. Space systems and ground systems should ensure security controls are reestablished following a recovery from a failure or an interruption of communications.	●	●	●
A.17.1.MP2	Space systems operating in a 'safe mode', or in a degraded capacity where security controls may be nonfunctioning, should permit only a limited set of telecommands until the system is returned to nominal operations.			●
A.17.2 Redundancies Objective: To ensure availability of information processing facilities.				
A.17.2.MP1	The ISO 27001 control: – A.17.2.1 Availability of information processing facilities should be satisfied for all facilities and systems affiliated with a mission. Space systems and ground systems should define availability requirements, and provide redundancy in systems and/or components as necessary to meet the defined availability levels.	●	●	●
A.18 Compliance				
A.18.1 Compliance with legal and contractual requirements Objective: To avoid breaches of security requirements and breaches of legal, statutory, regulatory, or contractual obligations related to information security.				
A.18.1.MP1	The ISO 27001 controls: – A.18.1.1 Identification of applicable legislation and contractual requirements – A.18.1.2 Intellectual property rights – A.18.1.3 Protection of records – A.18.1.4 Privacy and protection of personally identifiable information – A.18.1.5 Regulation of cryptographic controls should be satisfied for all facilities and systems affiliated with a mission. The mission security policy should define which are the applicable laws, regulations, and policies for the mission.	●	●	●
A.18.1.MP2	Missions having international scope should provide for the operation of cryptographic controls in accordance with export/import restrictions and national laws. The mission security policy should define which are the applicable laws, regulations, and policies for the mission.	●	●	●
A.18.2 Information security reviews Objective: To ensure that information security is implemented and operated in accordance with organizational policies and procedures.				
A.18.2.MP1	The ISO 27001 control: – A.18.2.1 Independent review of information security should be satisfied for all facilities and systems affiliated with a mission. A review conducted using a separate internal branch of the organization may suffice in certain cases, if no qualified external organization can be obtained to conduct the review.	●	●	●
A.18.2.MP2	The ISO 27001 controls: – A.18.2.2 Compliance with security policies and standards – A.18.2.3 Technical compliance review should be satisfied for all facilities and systems affiliated with a mission.	●	●	●