DATA ITEM DESCRIPTION

1. DID NAME: -
2. TITLE: SECURITY RISK MANAGEMENT PLAN
3. DESCRIPTION AND INTENDED USE

The Security Risk Management Plan (SRMP) is used to identify and track threats to Information and Communications (ICT) security and cyber security, the associated risk assessments, the risk treatment options, and the existing and proposed risk controls associated with a Security System-of-Interest (SSoI) (eg, the Mission System), including during development, Verification and Validation (V&V), commissioning, operation and support, so that Defence is able to understand the level of risk exposure posed by the system. The Approved governing plan (eg, Materiel System Security Management Plan (MSSMP) or In‑Service Security Management Plan (ISSMP)) provides the plan and associated processes for managing the risks associated with ICT security and cyber security, while the SRMP addresses only the risk assessment aspects of ICT/cyber-security risk management for the Targets of Security Assessment (ToSAs) for a SSoI. This includes the Digitally Enabled Systems and Equipment (DESE) within each SSoI.

Note: This DID has been written on the basis that all ToSAs for a SSoI will be addressed within a single SRMP (including when the ToSA and the SSoI are one and the same). Where this is not the case, such as may occur for larger Mission Systems (eg, aircraft or ship), the requirements of the DID should be interpreted in the context of the set of SRMPs and associated ToSAs. The ToSAs are either identified in the Approved governing plan or in the System Security Plan(s) (SSP(s)) for a SSoI.

The SRMP serves two purposes:

during the design and implementation phases for a SSoI, it provides a supporting artefact for the design process, describing the risk assessment and proposed risk treatments for the identified threats, to demonstrate that the ICT/cyber-security controls are suitable and sufficient and the SSoI is likely to be assessed to be As Secure As Reasonably Practicable (ASARP); and

during the Security Authorisation assessment phases for a SSoI, it provides a consolidated reference or summary of the risk basis underpinning the ICT/cyber-security controls that have or have not been implemented, and is one of the artefacts for obtaining the required Security Authorisations for ICT security and cyber security.

The Contractor uses the SRMP:

to document the ICT/cyber-security threats and associated risk assessments for a SSoI;

to document the risk-treatment options and associated plans, the existing and proposed risk controls, the controls not implemented and not proposed to be implemented, and the residual risk exposure;

to advise the Commonwealth and the ICT and cyber Security Authorisation assessor(s) of the ICT/cyber-security threat and risk assessments associated with a SSoI/ToSA during the design, implementation and assessment phases; and

as one of the ICT/cyber-security artefacts to provide assurance to the Commonwealth that the Contractor’s ICT/cyber-security activities will enable the Security Outcomes for a SSoI to be achieved, particularly to demonstrate that the SSoI/ToSA is ASARP.

The Commonwealth uses the SRMP:

to understand, assess and manage ICT/cyber-security risks associated with a SSoI, including to review the Contractor’s controls for the identified risks and to assist with evaluating whether or not the residual risk is acceptable;

to understand and evaluate the Contractor’s approach to meeting the ICT/cyber-security requirements of the Contract as part of the system security program, including to understand the Commonwealth’s involvement in the Contractor’s ICT/cyber-security program;

as an input to its own planning, including to identify any actions arising from the system security program that need to be undertaken by the Commonwealth with regard to the implementation of a SSoI; and

as one of the suite of ICT/cyber-security artefacts provided to the relevant security authorities as part of obtaining the required ICT and cyber Security Authorisations for a SSoI.

1. INTER-RELATIONSHIPS

The SRMP is subordinate to the following data items, where these data items are required under the Contract:

Systems Engineering Management Plan (SEMP);

Contractor Engineering Management Plan (CEMP);

Materiel System Security Management Plan (MSSMP);

In‑Service Security Management Plan (ISSMP);

System Safety Program Plan (SSPP); and

In-service Materiel Safety Plan (IMSP).

The SRMP inter-relates with the following data items, where these data items are required under the Contract:

System Specification (SS) for each different type of SSoI;

the security-related data items required under the Contract (other than those identified under clause 4.1); and

the safety-related data items (eg, Hazard Log and Safety Case Report (SCR) or Materiel Safety Assessment (MSA)).

1. APPLICABLE DOCUMENTS

The following documents form a part of this DID to the extent specified herein:

Note to drafters: Amend the following list of Applicable Documents to suit the requirements of the Contract. Do not include documents that are included within the ‘Governing Security Documents’.

|  |  |
| --- | --- |
| 1. Governing Security Documents | 1. (see the Glossary for the definition of this term) |
| 1. NIST CSF 2.0 | 1. National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), Version 2.0, February 26, 2024 |
| 1. NIST SP 800-30 | 1. Guide for Conducting Risk Assessments, Revision 1, September 2012 |
| 1. NIST SP 800-37 | 1. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2, December 2018 |
| 1. NIST SP 800-53 | 1. Security and Privacy Controls for Information Systems and Organizations, Revision 5, September 2020 |
| 1. NIST SP 800-53A | 1. Assessing Security and Privacy Controls in Information Systems and Organizations, Revision 5, January 2022 |
| 1. NIST SP 800-82 | 1. Guide to Operational Technology Security, Revision 3, September 2023 |
| 1. ISA/IEC 62433 series | 1. Security for Industrial Automation and Control Systems |
| 1. ISO/IEC 27005:2022 | 1. Information security, cybersecurity and privacy protection – Guidance on managing information security risks |

1. Preparation Instructions
   1. Generic Format and Content

Subject to clause 6.1.2, the data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

Where a SRMP is required for an ICT Security Authorisation, the format and content requirements for the SRMP shall comply with any template for a SRMP issued by Defence in addition to the content requirements set out in clauses 6.1.3 to 6.1.7 and clause 6.2 of this DID.

Note to drafters: The SRMP implements the risk processes defined in the Approved governing plan. Attention is drawn to the Note to drafters in the MSSMP and ISSMP DIDs, which highlights the implications associated with the selection of either the CASG 5x5 matrix or the PSPF 6x6 matrix as the basis for these risk processes.

The SRMP shall be consistent with and, where applicable, comply with the Governing Security Documents. The SRMP shall accord with the risk management framework documented in the Approved governing plan (eg, SEMP, MSSMP or ISSMP), as applicable.

Where the Approved governing plan identifies that more than one SRMP will be developed to address the ToSAs within an SSoI, each SRMP shall identify the full scope of ToSAs and the associated SRMPs for the SSoI, including the relationships between them (if any).

While early versions of the SRMP for a SSoI may contain threats and risk assessments for one or more components of, or ToSAs for, a SSoI, the final version of the SRMP for a SSoI shall contain the complete set of threats and associated risk assessments for all ToSAs within the SSoI.

When the Contract has specified delivery of another data item that contains aspects of the required information, the SRMP should summarise these aspects and refer to the other data item.

The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

* 1. Specific Content – Part 1
     1. Executive Summary

The SRMP shall include a system-level summary of the SRMP, including:

an overview of the ToSAs and the SSoI being assessed;

a brief description of the risk-assessment process that has been undertaken, cross-referring to the Approved governing plan, as appropriate;

a summary table of the threats considered alongside the severity of risk exposures associated with these threats; and

the significant conclusions of the SRMP.

* + 1. Scope

The SRMP shall define the scope of the threat and risk assessment that has been undertaken, identifying the SSoI, the ToSAs addressed by the SRMP, the associated SSP(s), and the SSoI assets under threat.

The SRMP shall identify the stakeholders associated with the SSoI and the ToSAs, including the System Owner, project sponsor, acquirer, user, developer, support agencies, and the relevant authorities for each different type of required Security Authorisation.

The SRMP shall identify any assumptions and constraints associated with the threat and risk assessments conducted for the ToSAs and/or the SSoI, including any factors relating to the SRMP which are assumed but not confirmed and which have constrained the assessment of security risk for the ToSAs/SSoI.

* + 1. Threat and Risk Assessment

The threat and risk assessment elements of the SRMP shall describe how the Applicable Documents listed at clause 5 have been utilised to ensure that the SRMP will achieve the purposes and required outcomes set out in clause 3.

The SRMP shall describe the threat identification and modelling methodology applied (eg, attack trees, MITRE ATT&CK® framework, STRIDE[[1]](#footnote-1) threat model, context analysis, operational scenario analysis, or a combination of methodologies), including the use of threat intelligence sources and reporting.

Note: In addressing the following requirement, the SRMP only needs to address the most applicable threats relevant to the SSoI (or element thereof) and its operating context. The analysis should be informed by both cyber threat intelligence reporting and knowledge of the SSoI design and the associated operational and support concepts.

The SRMP shall identify and describe the threats applicable to the scope of the assessment addressed through the SRMP, including identifying the risk threat profile that will help to predict potential future attacks and/or attack trends applicable to the SSoI.

The SRMP shall address ICT/cyber-security risks in relation to:

confidentiality, integrity and availability of systems and data; and

the cyber-security functions of Identify, Protect, Detect, Respond and Recover (as these terms are defined in NIST CSF 2.0).

For each identified threat, the SRMP shall include the following information:

threat title and unique identifier;

threat description, including threat type and characteristics, including the causes of the threat (ie, what needs to occur for the threat to eventuate);

threat source(s) (ie, the sources (malicious or otherwise) likely to realise the threat, including the actors or agencies behind the threat (if known));

asset(s) affected (ie, which systems, subsystems and assets identified in the ‘scope’ section are vulnerable to the threat), including any potential downstream or upstream implications for other systems that interact with, or interface to, the SSoI/ToSA;

overview (ie, a short description of how the threat sources and affected assets link to the threat for the ToSAs/SSoI, including how the threat accesses or compromises the system, subsystem or asset, or what circumstances, phases or locations does the threat present itself);

likelihood of occurrence;

consequence of realisation in terms of confidentiality, integrity and availability of systems and data, and the impacts of these consequences on the mission, safe operation of the ToSAs/SSoI, information security, or some other function or combination of functions;

Notes:

1. The information provided in response to the following requirement will evolve as the design and implementation of the ToSA/SSoI progresses (ie, as a control to be implemented becomes an existing control).
2. The Approved SSP will identify the publications from which the controls have been derived, which will include the ISM and DSPF and any complementary publications (eg, NIST SP 800-82 or ISA-62443 series) agreed by the Commonwealth.

controls to be incorporated, including:

existing controls (ie, the controls already implemented in the ToSA/SSoI);

other controls that the Contract intends to implement, either fully or partially;

other available controls that the Contractor does not intend to implement (either fully or partially),

as set out in the associated SSP(s), including the Contractor’s assessment as to whether the controls are effective at managing the threats/risks to the SSoI;

resultant risk exposure;

treatment option (ie, acceptance, reduction, transfer or avoidance);

treatment recommendation(s);

residual likelihood of occurrence after the identified treatment recommendations, which involve implementation actions, have been implemented;

residual consequence of realisation after the identified treatment recommendations, which involve implementation actions, have been implemented; and

residual risk exposure.

For all threats that affect the safe operation and/or support of the SSoI, the risk assessments and associated controls for these threats shall be entered into the Hazard Log element of the SCR/MSA, and managed in accordance with the Approved SSPP. The SRMP shall identify the specific ICT/cyber threats and risk assessments that are being managed through the system safety program.

The SRMP shall propose security controls for each risk for which the risk-treatment option is to reduce the likelihood and/or reduce the consequence.

* 1. Specific Content – Part 2

Note: During the Security Authorisation assessment phases for a SSoI, the following elements of the SRMP will provide input information for the Plan Of Action and Milestones (POAM), which will be developed by the Commonwealth as one of the required artefacts for obtaining the Security Authorisations for ICT security and cyber security.

* + 1. Risk Treatment Planning

The SRMP shall set out the Contractor’s risk-treatment plan for each risk for which the risk-treatment option is to either:

reduce the likelihood and/or reduce the consequence; or

avoid the risk, but a change to the design of the SSoI is required to enable such avoidance to occur,

with the aim of demonstrating that these risk-treatment plans, once implemented, will be sufficient to ensure that the SSoI will be ASARP.

Each risk-treatment plan shall include:

the position responsible;

a brief description of the required scope of work;

the envisaged schedule for implementation, including the associated milestones;

the likely resources;

the envisaged cost; and

any other relevant information (eg, implementation risks and Verification activities).

* + 1. Residual Risk Exposure

The SRMP shall record whether the residual risk exposure associated with each threat has been accepted by the Commonwealth in support of:

if applicable, ICT Security Authorisation for the SSoIs (or elements thereof); and

cyber Security Authorisation for the SSoIs (or elements thereof).

The record of risk acceptance required under clause 6.3.2.1 shall include:

the Contractor’s risk acceptance authority by title and organisation, and date of acceptance;

the Commonwealth authority’s concurrence or non-concurrence, as applicable, by title and organisation, and date of risk acceptance; and

identification details for the signed risk acceptance document(s).

1. [STRIDE](https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN) is an acronym for six threat categories: Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of service and Elevation of privileges [↑](#footnote-ref-1)