DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-AEOA-V5.2

2. TITLE: APPLICATION FOR ENGINEERING ORGANISATION APPROVAL

3. DESCRIPTION AND INTENDED USE

3.1 The Application for Engineering Organisation Approval (AEOA) is a formal submission by the Contractor, to the Commonwealth, to demonstrate that it has the means to perform engineering activities that comply with specified ADF regulatory / assurance framework requirements.

3.2 The Contractor uses the AEOA to seek formal recognition of its engineering organisation by submitting evidence that the Contractor:

a. can, and will, sustain an engineering organisation that complies with the specified ADF regulatory / assurance framework requirements, to the extent that they apply to the engineering activities required under the Contract; and

b. will undertake the required engineering activities to approved standards, using competent and authorised individuals, who are acting as members of the complying engineering organisation.

3.3 The Commonwealth uses the AEOA, to assess the Contractor’s capability and readiness to apply the specified ADF regulatory / assurance framework requirements to the engineering activities required under the Contract.

4. INTER-RELATIONSHIPS

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

a. Contractor Engineering Management Plan (CEMP);

b. Systems Engineering Management Plan (SEMP); and

c. Configuration Management Plan (CMP).

5. APPLICABLE DOCUMENTS

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

AAP 8000.011	Defence Aviation Safety Regulations (DASR)
ANP3411-0101	Naval Materiel Assurance Publication
LMSM	Land Materiel Safety Manual

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

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

6.1.2 When the Contract has specified delivery of other data items that contains aspects of the required information, the AEOA shall summarise these aspects and refer to the other data items.

6.1.3 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.

6.1.4 All documents provided as part of the AEOA shall be controlled documents.

6.2 Specific Content

6.2.1 Aerospace - Application for Design / Production Organisation Approval

6.2.1.1 Where the Contractor is required to comply with the DASR, as applicable to the scope of work under the Contract, the AEOA shall include:

a. for design activities, a completed *DASR Form 80 - Application for Military Design Organisation Approval*, supported by a *Design Organisation Exposition* (DOE) addressing the requirements of DASR 21.A.243; and/or

b. for production activities, a completed *DASR Form 50 - Application for DASR 21 Production Organisation Approval*, supported by a *Production Organisation Exposition* (POE) addressing the requirements of DASR 21.A.143.

6.2.1.2 In meeting the requirements of clause 6.2.1.1 the AEOA shall, except where provided to the Commonwealth by other means, include the CEMP, SEMP and CMP, as applicable, and all other plans, procedures, and other documents referenced in the DOE and/or POE, as applicable.

6.2.2 Land - Application to demonstrate compliance with the LMSM

6.2.2.1 Where the Contractor is required to show compliance with the LMSM, as applicable to the scope of work under the Contract, the AEOA shall:

a. be released under the authority of the Contractor’s Senior Design Engineer for the program;

b. provide objective quality evidence to demonstrate that the Contractor possesses the engineering management systems, competent people, processes, data and other resources required to provide engineering management and design services consistent with applicable LMSM requirements identified in the Contract;

c. except where provided to the Commonwealth by other means, include the CEMP, SEMP and CMP, as applicable, and all other plans, procedures and related documents containing the objective quality evidence required by clause 6.2.2.1b; and

d. include a compliance matrix, showing how the Contractor’s engineering management system complies with LMSM requirements applicable to the engineering activities under the Contract.

6.2.3 Maritime – Application to demonstrate compliance with the Naval Materiel Assurance Publication

6.2.3.1 Where the Contractor is required to comply with the *Naval Materiel Assurance Publication*, as applicable to the scope of work under the Contract, the AEOA shall:

a. be released under the authority of the Contractor’s Senior Design Engineer for the program;

b. provide objective quality evidence to demonstrate that the Contractor possesses the engineering management systems, competent people, processes, data and other resources required to provide engineering management and design services in accordance with *Naval Materiel Assurance Publication* requirements (refer to ANP3411-0101 Chapter 6, paragraphs 6.24 and 6.28);

c. except where provided to the Commonwealth by other means, include the CEMP, SEMP and CMP, as applicable, and all other plans, procedures and related documents containing the objective quality evidence required by clause 6.2.3.1b; and

d. include a compliance matrix showing how the Contractor’s engineering management system complies with *Naval Materiel Assurance Publication* requirements applicable to the engineering activities under the Contract.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-MNT-AMOA-V5.2

2. TITLE: APPLICATION FOR MAINTENANCE ORGANISATION APPROVAL

3. DESCRIPTION AND INTENDED USE

3.1 The Application for Maintenance Organisation Approval (AMOA) is a formal submission by the Contractor, to the Commonwealth, to demonstrate that it has the means to perform Maintenance activities that comply with specified ADF regulatory / assurance framework requirements.

3.2 The Contractor uses the AMOA to seek formal recognition of its Maintenance organisation by submitting evidence that the Contractor:

a. can, and will, sustain a Maintenance organisation that complies with the specified ADF regulatory / assurance framework requirements, to the extent that they apply to the Maintenance activities required under the Contract; and

b. will undertake the required Maintenance activities to approved standards, using competent and authorised individuals, who are acting as members of the complying Maintenance organisation.

3.3 The Commonwealth uses the AMOA, to assess the Contractor's capability and readiness to apply the specified ADF regulatory / assurance framework requirements to the Maintenance activities required under the Contract.

4. INTER-RELATIONSHIPS

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

a. Maintenance Management Plan (MMP); and

b. Configuration Management Plan (CMP).

5. APPLICABLE DOCUMENTS

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

AAP 8000.011	Defence Aviation Safety Regulations (DASR)
ANP3411-0101	Naval Materiel Assurance Publication
LMSM	Land Materiel Safety Manual

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

6.1.2 When the Contract has specified delivery of other data items that contains aspects of the required information, the AMOA shall summarise these aspects and refer to the other data items.

6.1.3 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.

6.1.4 All documents provided as part of the AMOA shall be controlled documents.

6.2 Specific Content

6.2.1 Aerospace - Application for Maintenance Organisation Approval

6.2.1.1 Where the Contractor is required to comply with the DASR, as applicable to the scope of work under the Contract, the AMOA shall include:

a. a completed DASR Form 2 – 'Application for DASR 145 and DASR M Subpart G Approval', for the DASR 145 requirements (only); and

b. a *Maintenance Organisation Exposition* (MOE), addressing the requirements of DASR 145.A.70.

6.2.1.2 In meeting the requirements of clause 6.2.1.1, the AMOA shall, except where provided to the Commonwealth by other means, include the MMP and all plans, procedures, and other documents referenced in the MOE.

6.2.2 Land - Application to demonstrate compliance with the LMSM

6.2.2.1 Where the Contractor is required to show compliance with the LMSM, as applicable to the scope of work under the Contract, the AMOA shall:

a. be released under the authority of the Contractor's Senior Maintenance Manager for the program;

b. provide objective quality evidence to demonstrate that the Contractor possesses the Maintenance management systems, competent people, processes, data and other resources required to provide Maintenance Services consistent with the applicable LMSM requirements identified in the Contract;

c. except where provided to the Commonwealth by other means, include the MMP and CMP, as applicable, and all other plans, procedures, and related documents containing the objective quality evidence required by clause 6.2.2.1b; and

d. include a compliance matrix showing how the Contractor's Maintenance management system complies with LMSM requirements applicable to the Maintenance activities under the Contract.

6.2.3 Maritime - Application to demonstrate compliance with Naval Materiel Assurance Publication

6.2.3.1 Where the Contractor is required to comply with the *Naval Materiel Assurance Publication*, as applicable to the scope of work under the Contract, the AMOA shall:

a. be released under the authority of the Contractor's Senior Maintenance Manager for the program;

b. provide objective quality evidence to demonstrate that the Contractor possesses the Maintenance management systems, competent people, processes, data and other resources required to provide Maintenance Services in accordance with *Naval Materiel Assurance Publication* requirements;

c. except where provided to the Commonwealth Representative by other means, include the MMP and CMP, as applicable, and all other plans, procedures and related documents containing the objective quality evidence required by clause 6.2.3.1b; and

d. include a compliance matrix showing how the Contractor's Maintenance management system complies with *Naval Materiel Assurance Publication* requirements applicable to the Maintenance activities under the Contract.

DATA ITEM DESCRIPTION

1. DID NUMBER: DID-SSM-ISSMP-V5.2

2. TITLE: IN-SERVICE SECURITY MANAGEMENT PLAN

3. DESCRIPTION AND INTENDED USE

3.1 The In-Service Security Management Plan (ISSMP) describes the Contractor's plan for meeting the system security requirements for the in-service phase for those products that are Products Being Supported (or will become Products Being Supported under an associated or linked Contract (Support) when this data item is being developed under a Contract (Acquisition)) and that:

a. could be susceptible to security vulnerabilities that may affect the Commonwealth's security obligations and compliance requirements (as would be determined by a competent contractor acting reasonably in making such a determination);

b. are the subject of, or included within the scope of, a Security Authorisation, including in relation to physical security, Emanation Security (EMSEC), Information and Communications Technology (ICT) security, cyber security, and personnel security (but, for personnel security, only in relation to Contractor Personnel operating, or maintaining or upgrading a Security System-of-Interest (SSoI) or an associated Target of Evaluation (ToE)); and/or

c. are required by the Contractor to undertake the system security services (eg, Software such as Splunk®).

3.2 The Contractor uses the ISSMP to:

a. define, manage and monitor the Contractor's system security and related activities for the in-service phase and to demonstrate how the associated security objectives applicable to the in-service phase will be achieved, including managing any Security Authorisations that will require periodic revalidation during the in-service phase;

b. ensure that those parties (including the Commonwealth and Subcontractors) performing system security activities during the in-service phase understand their respective responsibilities, the processes to be used, and the time-frames involved, including in relation to:

(i) responding to cyber incidents;

(ii) ensuring business continuity and disaster recovery; and

(iii) continuous monitoring; and

c. demonstrate that it has the capability and capacity to meet its system security responsibilities for the SSoIs / ToEs and other security-related Support System Products during the in-service phase.

3.3 The Commonwealth uses the ISSMP:

a. to understand and evaluate the Contractor's approach for meeting the system security requirements of the Contract for the in-service phase;

b. to gain assurance that the Contractor has a sound system security program in place that complies with applicable Government and Defence security requirements and policies and that will satisfy the objectives of the program;

c. to plan the integration of the Contractor's system security activities for the in-service phase with the Commonwealth's security activities, particularly in relation to interacting with the respective security authorities;

d. as an input into the Commonwealth's own planning, particularly in relation to liaising with the applicable security authorities for each SSoI; and

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

4. INTER-RELATIONSHIPS

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

a. Support Services Management Plan (SSMP).

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

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

b. Materiel System Security Management Plan (MSSMP) governing the acquisition phase; and

c. the plans and Engineering Change Proposal(s) (ECP(s)) associated with any Major Changes.

5. APPLICABLE DOCUMENTS

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

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

Governing Security Documents	(see the Glossary for the definition of this term)
ANP4605	Navy Cyberworthiness
	National Institute of Standards and Technology (NIST), 'Cybersecurity Framework (CSF)', Version 2.0, February 26, 2024
AS/NZS ISO 31000:2018	Risk Management – Principles and Guidelines
NIST SP 800-30	Guide for Conducting Risk Assessments, Revision 1, September 2012
NIST SP 800-37	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2, December 2018
NIST SP 800-53A	Assessing Security and Privacy Controls in Information Systems and Organizations: Building Effective Assessment Plans, Revision 5, January 2022
	ACSC Publication, 'Strategies to Mitigate Cyber Security Incidents', February 2017
	ACSC Publication, 'Strategies to Mitigate Cyber Security Incidents – Mitigation Details', February 2017
	ACSC Publication, 'Guidelines for System Monitoring', September 2023
	ACSC Publication, 'Guidelines for Security Documentation', September 2023
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection – Information security management systems – Requirements

ISO/IEC 27032:2023	Cybersecurity – Guidelines for internet security
ISA/IEC 62443 series	Security for Industrial Automation and Control Systems
AS/NZS HB 231: 2004	Information Security Risk Management Guidelines
Defence ICT/Cyber SCRM Framework	The Defence ICT/Cyber Procurement Supply Chain Risk Management Framework, October 2020
SCRM Procurement Tool	ICT/Cyber Procurement Supply Chain Risk Assessment (SCRA) Tool, version 1.0, April 2021
Form XP 188	Security Report

6. PREPARATION INSTRUCTIONS

6.1 Generic Format and Content

6.1.1 The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled 'General Requirements for Data Items'.

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

6.1.3 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.

6.2 Specific Content

Note: References to 'Contract' in this DID mean the Contract (Support) when this data item is being developed under an acquisition contract.

6.2.1 Overview

6.2.1.1 The ISSMP shall provide an overview of the security-related Services for each SSoI to be provided under the Contract, including:

a. defining the scope and purpose of the ISSMP;

b. describing the scope and objectives of the system security program for the in-service phase, including:

(i) providing an overview of each SSoI and, if applicable, each ToE, and identifying other applicable Support System Products from a security perspective; and

(ii) providing an overview of any shared responsibilities for system security between the Contractor and the Commonwealth (eg, in relation to responding to cyber incidents, ensuring business continuity and disaster recovery, and continuous monitoring);

c. identifying and describing the nature and significance of the security risks and threats that will be managed through the ISSMP; and

d. describing any constraints, assumptions and risks associated with the program.

6.2.1.2 The ISSMP shall provide a list of key stakeholders involved with the system security program for the Contract, including:

a. System Owner;

b. Security Authorisation authorities; and

c. where DESE supported under the Contract is either integrated into, or installed onto, Defence systems and platforms, the in-service agencies responsible for managing and supporting those systems and platforms.

6.2.1.3 The ISSMP shall describe the mechanisms by which the general requirements for security documentation, as set out in the Information Security Manual (ISM), will be satisfied, including (for example):

a. Control ISM-0188: “Security documentation is reviewed at least annually and includes a ‘current as at [date]’ or equivalent statement”; and

b. Control ISM-1602: “Security documentation, including notification of subsequent changes, is communicated to all stakeholders”.

6.2.2 System Security Organisation and Roles

6.2.2.1 The ISSMP shall describe the organisations and the roles of the organisations involved with the system security program for the Contract, including:

a. within the Contractor’s organisation;

b. Subcontractors, including original equipment manufacturers; and

c. Associated Parties, including Defence agencies, regulatory authorities and other Commonwealth Contractors, as applicable.

6.2.2.2 The ISSMP shall identify the technical / design support network of organisations, including:

a. identifying the Subcontractors and other companies, which provide technical advice for security activities; and

b. describing the nature and scope of the technical advice to be provided.

6.2.2.3 The ISSMP shall identify the qualifications and training required by persons filling any Key Staff Positions for the system security program for the Contract.

6.2.2.4 The ISSMP shall provide details of the Contractor’s security team that is dedicated to the provision of security-related Services for each SSoI / ToE, including numbers and skills.

6.2.3 System Security Risk Management

6.2.3.1 The ISSMP shall describe the risk management processes to be applied to the Contractor’s system security program for the Contract, cross-referring to the risk management elements of the Approved SSMP[1] and the applicable elements of the Approved ADF regulatory / assurance plans as appropriate, including:

a. the processes to be used to identify system security risks;

Note to drafters: The following clause refers to the CASG Risk Management Product Matrix included at Annex A to this DID. This enables a 5x5 matrix to be employed for the purposes of project or product risk management using the Predict! tool. The Security Authorisation process, however, requires the use of a 6x6 matrix in accordance with the DSPF. Drafters should amend the following clause and Annex A to suit their contract-management circumstances (ie, to select a risk matrix that will result in the least work for the contract-management team, either translating into the DSPF 6x6 matrix if the CASG matrix is retained, or translating into Predict! if the following clause and Annex A are amended to incorporate the DSPF matrix).

b. the processes to be used for analysing, assessing and evaluating system security risks, including the specific assessment criteria to be used, cross-referring to the CASG Risk Management Product Risk Matrix at Annex A in relation to assessing risks to security and cyber;

c. the risk register(s) to be used for recording each system security risk (eg, Security Risk Management Plan (SRMP) and Cyber Supply Chain Risk Plan (CSCRP)), including its attributes, evaluation and treatment(s);

d. the processes to be used to determine the specific risk treatment strategies to be employed, particularly the application of risk controls (eg, as per the ISM); and

e. the mechanisms to be used to keep the Commonwealth Representative apprised of any changes to system security risks.

6.2.3.2 The ISSMP shall describe how security requirements will be incorporated into the Contractor’s supply chains to address cyber security supply chain risks (eg, using the ICT/Cyber Procurement SCRA Tool in accordance with the Defence ICT/Cyber SCRM Framework), cross-referring to any CSCRP required under the Contract.

[1] An Approved SSMP is unlikely to exist if the ISSMP is developed under an acquisition contract.

6.2.4 System Security Program Activities – General

Note: In relation to security monitoring and testing, clause 6.2.7 of this DID provides additional requirements that the ISSMP must address.

6.2.4.1 The ISSMP shall describe the Contractor's processes for undertaking the security-related Services for the SSoIs, as required by the Contract, including:

a. an overview of the methodology to be employed to achieve the objectives, outcomes and requirements set out in clause 3 of this DID;

b. describing how the applicable standards and other documents, referred to under clause 5, will be adapted to the Contractor's system security program; and

c. describing how each of the system security requirements set out in the Contract will be undertaken, including when and by whom, and the processes and tools to be employed.

6.2.4.2 The ISSMP shall describe any simulation and other tools, instruments, items of equipment, Software, test facilities and any other major elements that will be required to satisfy the security requirements of the Contract.

6.2.4.3 The ISSMP shall contain a high-level schedule indicating key activities, events and milestones for the system security program for the Contract, including in relation to physical security, EMSEC, ICT security and cyber security.

6.2.5 Incident Response Plan

Note: A security incident is a suspicious approach, event or action (whether deliberate, reckless, negligent or accidental) that:

a. fails to meet the expected outcomes of Defence security as outlined in the DSPF;

b. compromises Defence's protective security arrangements; and

c. results in (or has the potential to result in) loss, damage, harm or disclosure to Defence information, assets and/or personnel.

6.2.5.1 The ISSMP shall document the Contractor's plan for responding to security incidents ('**Incident Response Plan**') pertaining to each SSoI, including:

a. the roles and responsibilities of all personnel (Commonwealth, Contractor and Subcontractors) during an incident, including:

(i) system users, system support staff, system administrators, etc based on the incident type;

(ii) the identification of the position that will have ultimate responsibility for the operational management of an incident; and

(iii) the authorised methods of communication between the various parties, particularly between the Commonwealth and the Contractor and between the Contractor and its Subcontractors;

b. the authorities within the Contractor's organisation responsible for initiating:

(i) a formal (administrative) investigation; and

(ii) a police investigation of an incident;

c. the minimum level of Training for investigators, users and system administrators (eg, Cert IV in Forensics and Security Investigations);

d. guidelines on what situations and scenarios constitute an incident;

e. the goals and objectives of the incident response based on incident type;

f. the types of incidents likely to be encountered and the expected response to each type (eg, malware, system intrusion, data compromise, and unauthorised system change), including the processes for threat containment and eradication for each incident type;

g. the steps necessary to ensure the availability of critical systems during an incident;

h. management of the vulnerability exploited within the compromised system elements;

i. system contingency measures and/or relationships to other response processes and procedures to ensure the continued safety and operational effectiveness of the SSoI;

Note: In accordance with DSPF Principle 77, "Once the risk of immediate harm has been effectively managed, a Security Report must be submitted to SICC [Security Incident Coordination Centre] via the Security Report within 24 hours of the incident occurrence or discovery". A copy of this report is also to be provided to the Commonwealth Representative at the same time, including any supporting information.

j. incident reporting mechanisms, including both internally (eg, using a Form XP 188) and externally to relevant operational authorities (eg, the Australian Cyber Security Centre) and including those parties that need to be informed in the event of a security incident;

k. criteria for investigation into a security incident involving external entities (eg, as could be requested from a law enforcement agency, the Australian Cyber Security Centre or other relevant authority); and

l. the steps necessary to ensure the integrity of evidence for use in investigation.

6.2.5.2 The Incident Response Plan shall detail the management of, and contents of, the Incident Register to be used to capture the necessary details associated with each security incident, including fields to allow the tracking of the following information:

a. the date the incident was discovered;

b. the date the incident occurred;

c. a description of the incident, including the people and locations involved;

d. the action taken;

e. lessons identified;

f. to whom the incident was reported; and

g. whether or not any further investigations were undertaken.

6.2.5.3 The Incident Response Plan shall describe the intervals and process for testing incident response and recovery capability, and for confirming that the plan remains fit for purpose.

6.2.6 Business Continuity and Disaster Recovery Plan

6.2.6.1 The ISSMP shall document the Contractor's plan for ensuring the continued operation of each SSoI (or critical elements thereof) in response to either:

a. a security incident or a series of security incidents that have a high likelihood of compromising Defence operations involving the SSoI; or

b. a disaster that would compromise Defence operations involving the SSoI,

('**Business Continuity and Disaster Recovery Plan**' or '**BCDRP**')

Note: Different elements of an SSoI may involve different considerations in relation to business continuity and/or disaster recovery. Where applicable, the BCDRP should identify these differences so that it is clear exactly what will occur for the different elements in relation to business continuity and disaster recovery.

6.2.6.2 The BCDRP shall:

a. identify the management structures and the roles and responsibilities of applicable personnel (Commonwealth, Contractor and Subcontractors) associated with business continuity and/or disaster management and recovery, including the relationships with incident response management;

b. identify the critical services, functions and assets associated with each SSoI in the context of Defence operations, cross-referring to the Business Impact Levels (BILs) in the Security Classification and Categorisation Guide (SCCG) at Attachment J to the Contract;

c. categorise the identified elements according to their priority for maintaining continuity of operations and/or for recovery after a disaster;

d. define the maximum acceptable outage time for the critical services and functions and the associated recovery time objective in the context of the maximum acceptable outage time;

e. describe credible scenarios that could cause a system interruption, such as a natural disaster, civil disturbance, major ICT failure or major cyberattack;

f. describe the strategies for maintaining business continuity in response to the identified scenarios and in the context of the prioritised services, functions and assets;

g. describe the strategies for disaster management and recovery in the context of the identified scenarios, the prioritised services, functions and assets, and the recovery time objectives;

h. describe the processes to be implemented to ensure that personnel are prepared for potential system disruptions that could compromise Defence operations using the SSoI, including, for example, the conduct of business continuity and disaster recovery exercises and testing;

i. describe the processes for activating and managing the business continuity and/or disaster management and recovery mechanisms and activities, including:

    (i) identifying the likely triggers;

    (ii) describing the potential requirements for relocating systems, equipment, personnel and other items during a disaster, including ensuring the safety of personnel as the highest priority;

    (iii) describing the associated internal and external communications;

    (iv) describing the coordination with other interested parties throughout a disruption; and

    (v) describing the likely temporary arrangements to be implemented during a disruption;

j. describe the systems, processes and personnel necessary to return business / mission activities from the temporary measures adopted during the disruption to normal operations;

k. describe the processes for data backup and recovery to ensure that minimal data is lost in the event of an interruption to the SSoI and the SSoI can be recovered within the required timeframes, including the use of remote locations for data backup, testing backup and restoration processes, and security considerations for the data backups;

l. describe any other elements of the BCDRP (eg, employee contact lists, vital records, and alternate site operations, resources and transportation); and

m. describe the implementation and maintenance of communication and warning procedures, including those necessary to manage the incident response and coordination with other interested parties throughout a disruption.

6.2.6.3 The BCDRP shall describe the processes for maintaining capabilities and response readiness, such as table top exercises, and for confirming that the plan remains fit for purpose.

Note to drafters: The following requirements may not be applicable to any SSoI or to the Contractor's responsibilities under a Contract. If not applicable, the following clauses should be deleted and replaced with 'Not Used', and other clauses that reference continuous monitoring should also be amended.

6.2.7 Continuous Monitoring Plan

Note: The requirements of this clause are broader than the ISM requirements for a continuous monitoring plan.

6.2.7.1 The ISSMP shall document the Contractor’s plan for undertaking continuous monitoring of each SSoI (or applicable element thereof) during the in-service phase, to proactively identify, prioritise and respond to security Issues (eg, vulnerabilities) (‘**Continuous Monitoring Plan**’), including:

a. identifying the management structures and the roles and responsibilities of applicable personnel (Commonwealth, Contractor and Subcontractors) associated with continuous monitoring of each SSoI, including the relationships with incident response management and business continuity and disaster recovery management;

b. describing the use of agencies and websites that provide advice of known vulnerabilities, such as the ACSC Alerts and the Known Exploited Vulnerabilities (KEV) catalogue at www.cisa.gov/known-exploited-vulnerabilities-catalog;

c. describing the use of automated system event logging tools and processes (if applicable), as described in the ACSC Guidance Document, ‘Guidelines for System Monitoring’, to assist with the identification of security vulnerabilities and security incidents, including:

(i) describing how the system event logging systems and processes have been implemented;

(ii) identifying the system events to be logged and the associated event details to be captured;

(iii) describing the mechanisms for security vulnerability / incident identification and reporting based on the logged system events (eg, automatically to the system administrator and/or system security manager within particular timeframes); and

(iv) management of the event log, including protection, retention, and auditing;

d. in addition to any automated system event processes, describing the types of intermittent monitoring and testing activities to be employed (eg, vulnerability assessments, vulnerability scans and penetration tests), including the likely nature and scope of these activities and the timeframes for conducting them;

e. describing the analysis and investigation activities to be undertaken when potential or actual security Issues (eg, vulnerabilities) are identified, including the stakeholders to be consulted and the report(s) to be provided to the Commonwealth;

f. describing the processes to be employed to prioritise the implementation of mitigations, taking into account the cost of mitigations and the implications for Defence operations, other Contract work, the health and safety of personnel, and the environment; and

g. describing how the mitigation work will be implemented and managed, particularly when configuration changes are required.

Annex:

A. CASG Risk Management Product Risk Matrix

DID-ENG-MGT-MSS
MP - Annex A Risk M