ShipRight
Linked Supporting Services

Procedure for the Assessment of Cyber Security for Ships and Ships Systems

September 2019

Lloyd's Register

Document History	
Date:	Notes:
September 2019	First release

Section 1
Introduction

1.1 General

1.1.1

(a) This procedure details the Lloyd's Register assessment criteria for the assessment and assignment of cyber security descriptive notes as referenced in the *LR Procedure for Assignment of Digital Descriptive Notes for Autonomous and Remote Access Ships* for systems on board vessels classed by LR.

(b) This *ShipRight Procedure* has been developed to provide an independent assessment of ship-owners, Operators and managers approach to effectively manage the cyber security risks in a connected, integrated and internet enabled environment. The cyber risks presented through both onboard and shore-based support services could impact the safety and functions of a vessel due to the ability to perform passive and offensive actions from anywhere on the globe. Threats from organised criminals, pirates, opportunists, insiders and even nation states now need to be considered.

(c) Considerations at both the design and build stage of a ship also need to be considered with the operating procedures. It is recognised that vessels in operation may not have been built with all these considerations in mind and that operating environments can be very diverse with, in some cases, many parties involved. The LR ShipRight cyber procedures have been created within this mind and provide four levels of maturity across eight domain areas to allow for a baseline standard to be reached along side setting a desired future position that is appropriate for the risks faced.

(d) This *ShipRight Procedure* provides an independent assessment of the maturity of cyber security measures that have been implemented, and are being maintained, to provide effective cyber security and information assurance that the risks from a cyber attack affecting the safety of the ship have been reduced to an acceptable level.

Contents

Contents

Section 1
Cyber security descriptive notes

1.1 General

1.1.1

(a) The cyber security descriptive notes have the format as detailed in the *Lloyd's Register Procedure for Assignment of Digital Descriptive Notes for Autonomous and Remote Access Ships*.

(b) The assignment of the cyber security descriptive notes indicates that the systems identified within the scope of the assessment have been assessed in accordance with this *ShipRight Procedure*. The descriptive notes indicate both the scope of the assessment carried out and the level of cyber security maturity determined during the assessment.

(c) The assigned level of cyber security maturity will be determined based on the lowest level demonstrated during the assessment across the eight cyber security domains.

Contents

Contents

Section 1
Cyber security assessment

1.1 General

1.1.1

(a) Modern ship's operating environments are changing with the adoption of cloud services, internet of things, connectivity and increasing automation. This can present a complex threat surface where many parties are responsible for meeting the cyber risks presented. Increasing needs to use specialist on shore-based parties to support the operational functions on board and to provide crew and passengers Internet facilities require opening up the on board networks to remote users and service providers.

(b) For each assessment a clear scope needs to be documented at the outset, communicated with network diagrams and signed off by the owners. This will be regularly reviewed and updated.

1.2 Cyber security domains

1.2.1

(a) Cyber security is a complex, emerging and developing risk area for connected ships and ships systems. LR has established eight cyber security risk areas (hereafter referred to as domains) that are considered in this *ShipRight Procedure* when assessing cyber security maturity:

(i) **Asset management** (data/physical/logical/environmental controls);

(ii) **Authentication and authorisation** (identification management/role-based access management/remote access/user privileges/third party access);

(iii) **Secure networks and systems** (secure architecture/perimeter security/segregation/configuration/patching/encryption);

(iv) **Cyber policy** (documented policy);

(v) **Physical access** (physical security);

(vi) **Security awareness** (training/testing);

(vii) **Detect and respond** (analysis/investigation/discovery/incident response planning and testing/business continuity planning and testing);

(viii) **Assurance** (penetration testing/vulnerability testing/crises management/third party management/risk management).

(b) These domains form a framework within which are referenced the indicator areas of the *Lloyd's Register Cyber Security Framework* (LR CSF). For example, LR CSF Indicator Area No.4: Defined Roles & Responsibilities is considered within the authentication and authorisation domain in this procedure, and each indicator area details the necessary outcomes/controls and required evidence and testing to demonstrate that the control is in place, and consequently that the outcome can be measured.

(c) Each domain heading in this *ShipRight Procedure* details the required evidence to be submitted and required outcomes during the assessment of that evidence for each cyber security maturity level in the domain.

(d) In this *ShipRight Procedure*, each domain is divided across four levels of cyber security maturity that are based on the security levels identified in the *IEC 62443* industry standard:

Lloyd's Register procedure for the assessment of cyber security for ships and ships systems	IEC 62443
Established	Security level 1 (SL 1)
Enhanced	Security level 2 (SL 2)
Accomplished	Security level 3 (SL 3)
Optimised	Security level 4 (SL 4)

Contents

Contents

Section 1
Outcomes

1.1 Outcomes

1.1.1

(a) All assets relevant to the secure operation of the fleet are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date.

(b) You have assigned responsibility for managing the physical assets.

1.1.2

(a) You have identified and catalogued all the data important to the operation of the ship, or that would assist an attacker. You know who has access to this important data.

(b) You maintain a current understanding of the location, quantity and quality of data important to the operation of the ship.

Section 2
Asset and data inventory

2.1 Controls

2.1.1 Assets and/or data that are associated with facilities and/or areas that store, process and/or transmit critical information must be identified and documented; this inventory must be kept up-to-date.

2.1.2 Mappings:

- ISO 27002: Section 8.1.1
- IEC 62443-3
    - SR 3.4 – Software and information integrity
    - SR 3.4 RE 1 – Automated notification about integrity violations
    - SR 7.8 – Control system component inventory

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how you verified that the policy for controlling storage and maintenance of all assets associated with facilities and/or areas that store, process and/or transmit critical information requires periodic media inventories.

(b) Provide evidence how you verified that the documented inventory is kept current.

Section 3
Asset and data ownership

3.1 Controls

3.1.1 Assets and/or data documented in the inventory must have an identified Owner, responsible for the management of the asset and/or data from creation to disposal.

3.1.2 Mappings:

- ISO 27002: Section 8.1.2

3.2 Required evidence and testing

3.2.1 Provide evidence how the usage policies and procedures define ways to accurately determine the Owner, contact information and purpose of critical information and any assets associated with facilities and/or areas that store, process and/or transmit critical information.

Section 4
Asset and data usage

4.1 Controls

4.1.1 Policies and procedures for the acceptable use of critical information and any assets associated with facilities and/or areas that store, process and/or transmit critical information must be documented and implemented.

4.1.2 Mappings:

- ISO 27002: Section 8.1.3

4.2 Required evidence and testing

4.2.1 Provide evidence how you verified that usage policies and procedures define ways to accurately determine the Owner, contact information and purpose of critical information and any assets associated with facilities and/or areas that store, process and/or transmit critical information.

Section 5
Asset and data classification

5.1 Controls

5.1.1 All organisational assets and/or data must be classified; this classification must take account of any legal requirements and must include the value, criticality and sensitivity of this asset and/or data, if the confidentiality and integrity of the asset and/or data is compromised.

5.1.2 Mappings:

- ISO 27002: Section 8.2.1

5.2 Required evidence and testing

5.2.1 Provide evidence how you verified that all data and any assets associated with facilities and/or areas that store, process and/or transmit critical information is classified so that the value, criticality and sensitivity of the data and/or asset can be determined.

Section 6
Asset and data labelling

6.1 Controls

6.1.1 Asset and/or data labelling procedures must be developed and implemented; these procedures will be defined by the data classification policy.

6.1.2 Mappings:

- ISO 27002: Section 8.2.2

6.2 Required evidence and testing

6.2.1 Provide evidence how the asset and/or data labelling accurately determined the Owner, contact information and purpose of the asset and/or data.

Section 7
Asset and data handling

7.1 Controls

7.1.1 Asset and/or data handling procedures must be developed and implemented; these procedures will be defined by the data classification policy.

7.1.2 Mappings:

- ISO 27002: Section 8.2.3

7.2 Required evidence and testing

7.2.1 Provide evidence how you verified the following:

(a) access controls supported the protection requirements as determined by the asset and/or data classification;
(b) list of authorised recipients of assets and/or data was maintained and managed;
(c) protection of copies (whether temporary or permanent) was consistent with the protection afforded to the original data set;
(d) storage of assets that store, process and/or transmit critical information followed manufacturers' guidelines; and
(e) copies clearly indicate the authorised recipient.

Section 8
Asset and data removal

8.1 Controls

8.1.1 Authorisation is required before any equipment, information or software is removed from either a shored-based and/or ship-based facility and/or area that stores, processes and/or transmits critical information.

8.1.2 Mappings:

- ISO 27002: Section 11.2.5

8.2 Required evidence and testing

8.2.1 Provide evidence how employees and external third parties are authorised to remove assets from facilities and/or areas that store, process and/or transmit critical information.

Section 9
Security of assets and data taken off-site

9.1 Controls

9.1.1 Risk-based security controls must in place before any asset that stores, processes and/or transmits critical information is taken off-site (whether a shored-based or a ship-based facility).

9.1.2 Mappings:

- ISO 27002: Section 11.2.6

9.2 Required evidence and testing

9.2.1 Provide evidence how risk-based controls were defined before any asset that stores, processes and/or transmits critical information was taken off-site.

Contents

Contents

Section 1
Outcomes

1.1 Outcomes

1.1.1

(a) All assets relevant to the secure operation of the fleet are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date.
(b) You have assigned responsibility for managing the physical assets.

1.1.2

(a) You have identified and catalogued all the data important to the operation of the ship, or that would assist an attacker. You know who has access to this important data.
(b) You maintain a current understanding of the location, quantity and quality of data important to the operation of the ship.
(c) You take steps to remove or minimise unnecessary copies or unneeded historic data.
(d) You maintain a current understanding of the data links used to transmit data that is important to the ships operation.

Section 2
Asset and data inventory

2.1 Controls

2.1.1 *See Ch 4, 2.1 Controls*

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how you verified that the policy for controlling storage and maintenance of all assets associated with facilities and/or areas that store, process and/or transmit critical information requires periodic media inventories.
(b) Provide evidence how you verified that a list of assets associated with facilities and/or areas that store, process and/or transmit critical information is maintained and includes a description of their function/purpose.
(c) Provide evidence how you verified that the documented inventory is kept current.
(d) Provide evidence how you verified the asset inventory accurately recorded the Owner, contact information and purpose of critical information and any assets associated with facilities and/or areas that store, process and/or transmit critical information.

Section 3
Asset and data ownership

3.1 Controls

3.1.1 *See Ch 4, 3.1 Controls*

3.2 Required evidence and testing

3.2.1

(a) Provide evidence how the usage policies and procedures defined ways to accurately determine the Owner, contact information and purpose of critical information and any assets associated with facilities and/or areas that store, process and/or transmit critical information.

(b) Provide evidence how the asset Owner correctly

(i) listed the asset on the inventory,

(ii) classified the asset,

(iii) and defined the asset's access controls.

(c) Provide evidence how the asset Owner provided appropriate controls to protect the asset.

(d) Provide evidence how the asset Owner periodically reviewed

(i) access controls,

(ii) and classification of asset.

(e) Provide evidence how the asset Owner followed organisational procedures for the removal and disposal of any assets under their management.

Section 4
Asset and data usage

4.1 Controls

4.1.1 *See Ch 4, 4.1 Controls*

4.2 Required evidence and testing

4.2.1

(a) Provide evidence how you verified that usage policies and procedures define ways to accurately determine the Owner, contact information and purpose of critical information and any assets associated with facilities and/or areas that store, process and/or transmit critical information.

(b) Provide evidence how you verified that usage policies and procedures defined acceptable locations for facilities and/or areas that store, process and/or transmit critical information.

(c) Provide evidence how you verified that usage policies and procedures define acceptable uses for any assets associated with facilities and/or areas that store, process and/or transmit critical information.

Section 5
Asset and data classification

5.1 Controls

5.1.1 *See Ch 4, 5.1 Controls*

5.2 Required evidence and testing

5.2.1 *See Ch 4, 5.2 Required evidence and testing*

Section 6
Asset and data labelling

6.1 Controls

6.1.1 *See Ch 4, 6.1 Controls*

6.2 Required evidence and testing

6.2.1 *See Ch 4, 6.2 Required evidence and testing*

Section 7
Asset and data handling

7.1 Controls

7.1.1 *See Ch 4, 7.1 Controls*

7.2 Required evidence and testing

7.2.1 *See Ch 4, 7.2 Required evidence and testing*

Section 8
Asset and data removal

8.1 Controls

8.1.1 *See Ch 4, 8.1 Controls*

8.2 Required evidence and testing

8.2.1

(a) Provide evidence how employees and external third parties are authorised to remove assets from facilities and/or areas that store, process and/or transmit critical information.

(b) Provide evidence how you verified that employees and external third parties are authorised to remove assets.

(c) Provide evidence how the removal of assets is managed, e.g. how long the asset can be removed, how the return of the asset is verified and recorded and how the identity, role and affiliation of individuals (who are authorised to remove the asset) are documented.

(d) Provide evidence how you verified the removal of assets is managed.

Section 9
Security of assets and data taken off-site

9.1 Controls

9.1.1 *See Ch 4, 9.1 Controls*

9.2 Required evidence and testing

9.2.1

(a) Provide evidence how risk-based controls were defined before any asset that stores, processes and/or transmits critical information was taken off-site.

(b) Provide evidence how you verified that the risk-based controls were implemented.

Contents

Contents

Section 1 Outcomes

1.1 Outcomes

1.1.1

(a) All assets relevant to the secure operation of the fleet are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date.
(b) You have assigned responsibility for managing the physical assets.
(c) Dependencies on supporting infrastructure (e.g. power, cooling, etc.) are recognised and recorded.
(d) Assets are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.

1.1.2

(a) You have identified and catalogued all the data important to the operation of the ship, or that would assist an attacker. You know who has access to this important data.
(b) You maintain a current understanding of the location, quantity and quality of data important to the operation of the ship.
(c) You take steps to remove or minimise unnecessary copies or unneeded historic data.
(d) You maintain a current understanding of the data links used to transmit data that is important to the ships operation.

1.1.3 Data in transit

(a) You have identified and suitably protected all the data links that carry data important to the operation of the ship.
(b) You apply appropriate physical or technical means to protect data that travels over an untrusted carrier, with justified confidence in the robustness of the protection applied.

1.1.4 Data at rest

(a) You have only necessary copies of this data. Where data is transferred to less secure systems, the data is provided with limited detail and/or as a read-only copy.
(b) You have applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion.
(c) If cryptographic protections are used you apply suitable technical and procedural means, and you have justified confidence in the robustness of the protection applied.
(d) Necessary historic or archive data is suitably secured in storage.

Section 2
Asset and data inventory

2.1 Controls

2.1.1 *See Ch 4, 2.1 Controls*

2.2 Required evidence and testing

2.2.1 *See Ch 5, 2.2 Required evidence and testing*

Section 3
Asset and data ownership

3.1 Controls

3.1.1 *See Ch 4, 3.1 Controls*

3.2 Required evidence and testing

3.2.1 *See Ch 5, 3.2 Required evidence and testing*

Section 4
Asset and data usage

4.1 Controls

4.1.1 *See Ch 4, 4.1 Controls*

4.2 Required evidence and testing

4.2.1 *See Ch 5, 4.2 Required evidence and testing*

Section 5
Asset and data classification

5.1 Controls

5.1.1 *See Ch 4, 5.1 Controls*

5.2 Required evidence and testing

5.2.1 *See Ch 4, 5.2 Required evidence and testing*

Section 6
Asset and data labelling

6.1 Controls

6.1.1 *See Ch 4, 6.1 Controls*

6.2 Required evidence and testing

6.2.1 *See Ch 4, 6.2 Required evidence and testing*

Section 7
Asset and data handling

7.1 Controls

7.1.1 *See Ch 4, 7.1 Controls*

7.2 Required evidence and testing

7.2.1 *See Ch 4, 7.2 Required evidence and testing*

Section 8
Asset and data removal

8.1 Controls

8.1.1 *See Ch 4, 8.1 Controls*

8.2 Required evidence and testing

8.2.1 *See Ch 5, 8.2 Required evidence and testing*

Section 9
Security of assets and data taken off-site

9.1 Controls

9.1.1 *See Ch 4, 9.1 Controls*

9.2 Required evidence and testing

9.2.1 *See Ch 5, 9.2 Required evidence and testing*

Section 10
Management of portable assets

10.1 Controls

10.1.1 Procedures for the management of any portable assets (including removable media such as USB drives) that are used to store, process and/or transmit data must be developed and implemented; these procedures must be defined by the asset and/or data classification. (Maps to ISO 27002: Sections 8.3.1; 10.1; 13.2).

10.1.2 Procedures for the secure disposal of any portable assets (including removable media such as USB drives) that are used to store, process and/or transmit data must be developed and implemented; these procedures must be defined by the asset and/or data classification. (Maps to ISO 27002: Section 8.3.2).

10.1.3 Procedures for the protection of any portable assets during transit (including removable media such as USB drives) that are used to store, process and/or transmit data from unauthorised access, misuse and/or corruption must be developed and implemented; these procedures must be defined by the asset and/or data classification. (Maps to ISO 27002: Section 8.3.3).

10.2 Required evidence and testing

10.2.1

(a) Provide evidence how you verified that the policy and procedures for the management of portable media (including removable media such as USB drives) stipulates that

  (i) appropriate authorisation is required before such portable assets can be used to store and/or transfer critical/sensitive information,
  (ii) all portable assets are periodically reviewed and documented,
  (iii) and that this inventory includes the asset Owner, contact details and a record of the critical/sensitive information currently and previously stored.

  Note If encryption is used to protect critical/sensitive information held on a portable assets and/or removable media, then provide evidence how you verified that it is encrypted (using an industry recognised strong cryptographic algorithm).

(b) Provide evidence how you verified that the use of portable assets (including removable media such as USB drives) to store and/or transfer critical/sensitive information requires appropriate authorisation.

(c) Provide evidence how you verified that any critical/sensitive information held on a portable asset is encrypted (using an industry recognised strong cryptographic algorithm).

(d) Provide evidence how you verified that all portable assets are periodically reviewed and documented.

(e) Provide evidence how you verified that the inventory includes the asset Owner, contact details and a record of the critical/sensitive information currently and previously stored.

(f) Provide evidence how you verified that the asset destruction policy and procedures (including portable assets) stipulates that

  (i) there must be a reasonable assurance that hard-copy materials cannot be reconstructed when destroyed;
  (ii) containers used for storing materials prior to their destruction are secured;
  (iii) and critical/sensitive information held on electronic assets is rendered unrecoverable.

(g) Provide evidence how you verified that hard-copy materials cannot be reconstructed when they are destroyed.

(h) Provide evidence how you verified that containers used for storing materials prior to their destruction are secured.

(i) Provide evidence how you verified that critical/sensitive information held on electronic assets is rendered unrecoverable.

(j) Provide evidence how procedures for protecting portable assets

  (i) include controls for physically securing all assets
  (ii) and that these controls are defined by the asset and/or data classification. (NB: Portable assets include, but are not limited to mobile phones, laptops, removable electronic media such as USB drives, paper reports and faxes that contain, process and/or transmit data.)

(k) Provide evidence how

  (i) a policy controls the distribution of all portable assets,
  (ii) the policy covers all distributed assets (including those assets distributed to internal individuals),
  (iii) and includes the asset and/or data classification.

(l) Provide evidence how you verified that all portable assets (containing critical/sensitive information) sent outside of a shore-based and/or ship-based facility are logged and sent via a secure delivery method that can be tracked.

(m) Provide evidence how you verified that management authorisation is obtained whenever any portable asset (containing critical/sensitive information) is moved from a secured area (including those assets distributed to internal individuals).

Section 11
Protection from environmental threats and hazards

11.1 Controls

11.1.1 Facilities and/or areas that store, process and/or transmit critical information must be sited and protected to reduce the risks from environmental threats and hazards. (Maps to ISO 27002: Section 11.2.1.)

11.2 Required evidence and testing

11.2.1

(a) Provide evidence how procedures for protecting portable assets

  (i) include controls for physically securing all assets;
  (ii) and that these controls are defined by the asset and/or data classification. (NB: Portable assets include, but are not limited to mobile phones, laptops, removable electronic media such as USB drives, paper reports and faxes that contain, process and/or transmit data.)

(b) Provide evidence how a

  (i) policy controls the distribution of all portable assets;
  (ii) the policy covers all distributed assets (including those assets distributed to internal individuals);
  (iii) and includes the asset and/or data classification.

(c) Provide evidence how you verified that all portable assets (containing critical/sensitive information) sent outside of a shore-based and/or ship-based facility are logged and sent via a secure delivery method that can be tracked.

(d) Provide evidence how you verified that management authorisation is obtained whenever any portable asset (containing critical/sensitive information) is moved from a secured area (including those assets distributed to internal individuals).

(e) Provide evidence how you verified that facilities and/or areas that store, process and/or transmit critical information were positioned so that the risk of such information being viewed by unauthorised individuals was reduced.

(f) Provide evidence how you verified that the impact of physical and environmental threats (e.g. theft, fire, explosives, smoke, water [or water supply failure], dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism, etc.) upon facilities and/or areas that store, process and/or transmit critical information was minimised.

(g) Provide evidence how you verified that guidelines for eating, drinking and smoking in proximity to facilities and/or areas that store, process and/or transmit critical information had been established.

(h) Provide evidence how you verified that environmental conditions (e.g. temperature, humidity, etc.) were monitored, and how alerts for conditions that could adversely affect the operation of facilities and/or areas that store, process and/or transmit critical information were generated and acted upon.

(i) Provide evidence how you verified that usage policies and procedures defined acceptable locations for facilities and/or areas that store, process and/or transmit critical information.

Section 12
Asset maintenance

12.1 Controls

12.1.1 To ensure their continued availability and integrity system components that store, process and/or transmit critical information must be correctly maintained. (Maps to ISO 27002: Section 11.2.4.)

12.2 Required evidence and testing

12.2.1

(a) Provide evidence how you verified documented policies and procedures include the requirement to

  (i) maintain a list of system components that store, process and/or transmit critical information;
  (ii) periodically inspect such system components looking for tampering or substitution;

(iii) train personnel to be aware of suspicious behaviour and to report tampering or substitution of system components.

(b) Provide evidence how you verified that the list of system components that store, process and/or transmit critical information includes the

(i) make and model;
(ii) location of the system component;
(iii) and serial number.

(c) Provide evidence how you verified the list is accurate and up-to-date.

(d) Provide evidence how you confirmed that the list is updated when system components are added, relocated, decommissioned, etc.

(e) Provide evidence how you verified that documented procedures include

(i) procedures for inspecting system components;
(ii) and the frequency of such inspections.

(f) Identify the individual who confirmed that

(i) personnel are aware of procedures for inspecting system components;
(ii) and all system components are periodically inspected for evidence of tampering and substitution.

(g) Provide evidence how you verified that individuals are aware of tampering or replacement of system components, including

(i) verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot system components;
(ii) not to install, replace or return system components without verification;
(iii) to be aware of suspicious behaviour around system components (e.g. attempts to unplug or open devices);
(iv) and reporting suspicious behaviour and indications of system component tampering or substitution to appropriate personnel (e.g. duty officer, security officer, etc.)

Section 13
Return of assets

13.1 Controls

13.1.1 The termination of any employment, contract and/or agreement must include a process for returning all previously issued physical and electronic assets and/or data. (Maps to ISO 27002: Section 8.1.4.)

13.2 Required evidence and testing

13.2.1

(a) Provide evidence how at the termination of any employment, contract and/or agreement all previously issued physical and electronic assets were returned or deactivated.

Section 14
Secure disposal or reuse of assets

14.1 Controls

14.1.1 Critical information and licensed software must be either removed from the asset or securely overwritten before the asset is either disposed or reused. (Maps to ISO 27002: Section 11.2.7.)

14.2 Required evidence and testing

14.2.1

(a) Provide evidence how the organisation ensures that storage media destined for disposal or reuse does not contain critical information.

(b) Provide evidence how you verified that critical information on storage media destined for disposal or reuse is rendered unrecoverable.

Section 15
Encrypt transmission of critical/sensitive data over untrusted networks

15.1 Controls

15.1.1 Policies and procedures detailing cryptographic controls used to protect critical/sensitive information during transmission over open, public networks must be developed and implemented. (Maps to ISO 27002: Sections 10.1 and 13.2.)

15.2 Required evidence and testing

15.2.1

(a) Provide evidence how you confirmed the documented policies and procedures detailed

  (i) all the locations where critical/sensitive data is transmitted over open, public networks;
  (ii) and all the security protocols and strong cryptography used at those locations.

(b) Provide evidence how the system configurations confirmed

  (i) that only trusted keys and/or certificates were accepted;
  (ii) the security protocol does not support insecure versions or configurations;
  (iii) and that an appropriate encryption strength was being used.

(c) Provide evidence how you verified that all critical/sensitive data is encrypted with strong cryptography during inbound and outbound transmissions.

(d) If wireless networks are used to transmit critical/sensitive data and/or connected to facilities and/areas that store, process and/or transmit critical/sensitive data, then provide evidence how you verified

  (i) that industry recognised strong encryption for authentication and transmission was implemented;
  (ii) and that weak encryption (such as WEP, SSL) was not used for authentication and transmission.

Contents

Contents

Section 1
Outcomes

1.1 Outcomes

1.1.1

(a) All assets relevant to the secure operation of the fleet are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date.
(b) You have assigned responsibility for managing the physical assets.
(c) Dependencies on supporting infrastructure (e.g. power, cooling, etc.) are recognised and recorded.
(d) Assets are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.

1.1.2

(a) You have identified and catalogued all the data important to the operation of the ship, or that would assist an attacker. You know who has access to this important data.
(b) You maintain a current understanding of the location, quantity and quality of data important to the operation of the ship.
(c) You take steps to remove or minimise unnecessary copies or unneeded historic data.
(d) You maintain a current understanding of the data links used to transmit data that is important to the ships operation.
(e) You understand the context, limitations and dependencies of your important data.
(f) You understand the impact on your ships operation and safety of all relevant scenarios, including unauthorised data access, modification or deletion, or when authorised users are unable to appropriately access this data.
(g) You validate these impact statements regularly, e.g. annually.

1.1.3 Data in transit

(a) You have identified and suitably protected all the data links that carry data important to the operation of the ship.
(b) You apply appropriate physical or technical means to protect data that travels over an untrusted carrier, with justified confidence in the robustness of the protection applied.

1.1.4 Data at rest

(a) You have only necessary copies of this data. Where data is transferred to less secure systems, the data is provided with limited detail and/or as a read-only copy.
(b) You have applied suitable physical or technical means to protect this important stored data from unauthorised access, modification or deletion.
(c) If cryptographic protections are used you apply suitable technical and procedural means, and you have justified confidence in the robustness of the protection applied.
(d) Necessary historic or archive data is suitably secured in storage.

Section 2
Asset and data security impact assessments

2.1 Controls

2.1.1 Security impact assessments relating to the loss of confidentiality, integrity and availability of data and/or assets that store, process and/or transmit critical/sensitive data must be developed; these security impact assessments must be undertaken by a competent individual of the organisation's executive, and reviewed and revalidated either

(a) annually;
(b) and/or when assets are upgraded and/or data is reclassified.

(Maps to ISO 27002: Section 17.)

2.2 Required evidence and testing

2.2.1

(a) Identify the competent individual interviewed who undertook the security impact assessments.
(b) Provide evidence how you verified their competence to undertake these security impact assessments.
(c) Provide evidence how the security impact assessments were reviewed and revalidated.
(d) Provide evidence how the security impact assessments were
    (i) documented,
    (ii) in use
    (iii) and disseminated to all affected parties.
(e) Provide evidence how you verified the individual has an understanding of how the loss of confidentiality, integrity and availability of data and/or assets that store, process and/or transmit critical/sensitive data would impact on the organisation.

Section 3
Asset and data inventory

3.1 Controls

3.1.1 *See Ch 4, 2.1 Controls*

3.2 Required evidence and testing

3.2.1

(a) Describe how you verified that the policy for controlling storage and maintenance of all assets associated with facilities and/or areas that store, process and/or transmit critical information requires periodic media inventories.

(b) Describe how you verified that a list of assets associated with facilities and/or areas that store, process and/or transmit critical information is maintained and includes a description of their function/purpose.

(c) Describe how you verified that the documented inventory is kept current.

(d) Describe how you verified the asset inventory accurately recorded the Owner, contact information and purpose of critical information and any assets associated with facilities and/or areas that store, process and/or transmit critical information.

■ *Section 4*
Asset and data ownership

4.1 Controls

4.1.1 *See Ch 4, 3.1 Controls*

4.2 Required evidence and testing

4.2.1 *See Ch 5, 3.2 Required evidence and testing*

■ *Section 5*
Asset and data usage

5.1 Controls

5.1.1 *See Ch 4, 4.1 Controls*

5.2 Required evidence and testing

5.2.1 *See Ch 5, 4.2 Required evidence and testing*

■ *Section 6*
Asset and data classification

6.1 Controls

6.1.1 *See Ch 4, 5.1 Controls*

6.2 Required evidence and testing

6.2.1 *See Ch 4, 5.2 Required evidence and testing*

■ *Section 7*
Asset and data labelling

7.1 Controls

7.1.1 *See Ch 4, 6.1 Controls*

7.2 Required evidence and testing

7.2.1 *See Ch 4, 6.2 Required evidence and testing*

Section 8
Asset and data handling

8.1 Controls

8.1.1 *See Ch 4, 7.1 Controls*

8.2 Required evidence and testing

8.2.1 *See Ch 4, 7.2 Required evidence and testing*

Section 9
Asset and data removal

9.1 Controls

9.1.1 *See Ch 4, 8.1 Controls*

9.2 Required evidence and testing

9.2.1 *See Ch 5, 8.2 Required evidence and testing*

Section 10
Security of assets and data taken off-site

10.1 Controls

10.1.1 *See Ch 4, 9.1 Controls*

10.2 Required evidence and testing

10.2.1 *See Ch 5, 9.2 Required evidence and testing*

Section 11
Management of portable assets

11.1 Controls

11.1.1 *See Ch 6, 10.1 Controls*

11.2 Required evidence and testing

11.2.1 *See Ch 6, 10.2 Required evidence and testing*

Section 12
Protection from environmental threats and hazards

12.1 Controls

12.1.1 *See Ch 6, 11.1 Controls*

12.2 Required evidence and testing

12.2.1 *See Ch 6, 11.2 Required evidence and testing*

Section 13
Asset maintenance

13.1 Controls

13.1.1 *See Ch 6, 12.1 Controls*

13.2 Required evidence and testing

13.2.1 *See Ch 6, 12.2 Required evidence and testing*

Section 14
Return of assets

14.1 Controls

14.1.1 *See Ch 6, 13.1 Controls*

14.2 Required evidence and testing

14.2.1 *See Ch 6, 13.2 Required evidence and testing*

Section 15
Secure disposal or reuse of assets

15.1 Controls

15.1.1 *See Ch 6, 14.1 Controls*

15.2 Required evidence and testing

15.2.1 *See Ch 6, 14.2 Required evidence and testing*

Section 16
Encrypt transmission of critical/sensitive data over untrusted networks

16.1 Controls

16.1.1 *See Ch 6, 15.1 Controls*

16.2 Required evidence and testing

16.2.1 *See Ch 6, 15.2 Required evidence and testing*

Contents

Contents

Section 1
Outcomes

1.1 Outcomes

1.1.1

(a) Necessary roles and responsibilities for the security of networks and information systems supporting essential services have been identified. These are reviewed periodically to ensure they remain fit for purpose.
(b) Appropriately capable and knowledgeable staff fill those roles and are given the time, authority and resources to carry out their duties.
(c) There is clarity on who in your organisation has overall accountability for the security of the networks and information systems supporting your essential service.
(d) Privileged access (e.g. to systems controlling critical functions or system administration) is carried out with separate accounts that are closely managed.
(e) All remote users are controlled with appropriate access for their job role.
(f) Remote access requirements are protected with multi-factor authentication (MFA) and logged.

Section 2
Defined roles and responsibilities

2.1 Controls

2.1.1 The organisation must develop and document an access control policy. The policy must be regularly reviewed and must be developed in accordance with organisation's business and cyber security requirements.

2.1.2 Mappings:

- ISO 27002: 9.1.1
- IEC 62443-3
    - SR 1.1 – Human user identification and authentication
    - SR 1.1 RE 1 – Unique identification and authentication
    - SR 2.1 RE 2 – Permission mapping to roles
    - SR 7.6 – Network and security configuration settings

2.1.3 The organisation must ensure the existence of defined access requirements for each role. These access requirements must include:

(a) system components and data resources that each role needs to access for their job function;
(b) level of privilege required (for example, user, administrator, etc.) for accessing resources.

2.1.4 Mappings:

- ISO 27002: 9.1.2

- IEC 62443-3
    - SR 2.1 – Authorisation enforcement
    - SR 2.1 RE 1 – Authorisation enforcement for all users
    - SR 2.1 RE 2 – Permission mapping to roles

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how you verified that access is generally forbidden unless expressly permitted.
(b) Provide evidence how you verified that each role had defined access needs and assigned privileges.
(c) Provide evidence how access is restricted to those least privileges necessary to perform job responsibilities.
(d) Provide evidence how you verified that documented formal approval (either electronically or in writing) is required for all access (including the specific privileges required).
(e) Provide evidence how access rights are periodically reviewed.
(f) Provide evidence how you verified that roles having privileged access are reviewed every 6 months.
(g) Provide evidence how you verified that the removal (i.e. terminated users, change of job responsibilities) of access rights is formally documented.

2.2.2

(a) Provide evidence how you verified that access requirements are defined and include:
    (i) system components and data resources that each role needs to access for their job function;
    (ii) identification of privilege necessary for each role to perform their job function.
(b) Provide evidence how you verified that privileges assigned are based on that individual's job classification and function.
(c) Provide evidence how you verified that access rights are periodically reviewed.
(d) Provide evidence how individuals receive training appropriate to their organisational roles and responsibilities.
(e) Provide evidence how you verified that the training received was appropriate to the individuals' organisational role and responsibilities.

Section 3
Privileged access rights

3.1 Controls

3.1.1 The organisation must restrict and control the allocation and use of privileged access rights.

3.1.2 Mappings:

- ISO 27002: 9.2.3
- IEC 62443-3
    - SR 2.1 – Authorisation enforcement
    - SR 2.1 RE 1 – Authorisation enforcement for all users
    - SR 2.1 RE 2 – Permission mapping to roles
    - SR 2.1 RE 4 – Dual approval

3.2 Required evidence and testing

3.2.1

(a) Provide evidence how the organisation defined the privileged access rights associated with each system and/or process.
(b) Provide evidence how you verified individuals were allocated the appropriate privileged access rights for each system and/or process.
(c) Provide evidence how (e.g. need-to-use; event-by-event, etc.) the organisation allocated (e.g. least privilege necessary to perform their job function, etc.) privileged access rights to individuals.
(d) Provide evidence how the organisation authorises and documents the allocation of privileged access rights.

(e) Provide evidence how you verified that privileged access rights are assigned to separate and unique user ID(s).

Section 4
Remote user access

4.1 Controls

4.1.1 The organisation must ensure all access to data/systems/services is controlled by a secure log-on procedures.

4.1.2 Mappings:

- ISO 27002: 9.4.2
- IEC 62443-3
    - SR 1.13 – Access via untrusted networks
    - SR 1.13 RE 1 – Explicit access request approval
    - SR 2.6 – Remote session termination

4.2 Required evidence and testing

4.2.1

(a) Provide evidence how you verified that insecure remote user access commands are not available for non-console access.
(b) Provide evidence how the organisation manages remote access granted to service providers.
(c) Provide evidence how you verified the organisation secures all remote access to the organisation's infrastructure using MFA.

Section 5
Secure log-on procedures

5.1 Controls

5.1.1 The organisation must ensure all access to data/systems/services is controlled by a secure log-on procedures.

5.1.2 Mappings:

- ISO 27002: 9.4.2
- IEC 62443-3
    - SR 1.1 – Human user identification and authentication
    - SR 1.1 RE 1 – Unique identification and authentication
    - SR 1.1 RE 2 – Multifactor authentication for untrusted networks
    - SR 1.1 RE 3 – Multifactor authentication for all networks
    - SR 1.2 – Software process and device identification and authentication
    - SR 1.2 RE 1 – Unique identification and authentication
    - SR 1.6 – Wireless access management
    - SR 1.6 RE 1 – Unique identification and authentication
    - SR 1.7 – Strength of password-based authentication
    - SR 1.7 RE 1 – Password generation and lifetime restrictions for human users
    - SR 1.7 RE 2 – Password lifetime restrictions for all users
    - SR 1.10 – Authenticator feedback
    - SR 1.11 – Unsuccessful login attempts

5.2 Required evidence and testing

5.2.1

(a) Provide evidence how you verified that all individuals (including service providers) use a unique ID to access organisational data/systems/services.

(b) Provide evidence how you verified that assigned unique ID(s) only has access privileged rights as detailed in authorisation documentation.

(c) Provide evidence how you verified that access privileged rights for individuals that leave the organisation are immediately revoked.

(d) Provide evidence how you verified that inactive user accounts are disabled.

(e) Provide evidence how you verified that remote access granted to service providers

  (i) is monitored when in use;

  (ii) and is disabled when not in use.

(f) Provide evidence how you verified the organisation restricts repeated access attempts.

(g) Provide evidence how you verified the lockout duration is active.

(h) Provide evidence how you verified the session idle time is active.

(i) Provide evidence how you verified the authentication process not only requires a unique ID, but also additional authentication methods.

(j) Provide a description of the strong cryptography used to guarantee all authentication methods are unreadable during transmission and storage.

(k) Provide evidence how you verified strong cryptography is used to guarantee all authentication methods are unreadable during transmission and storage.

(l) Provide evidence how the organisation confirms the user identity before modifying their authentication credentials.

(m) Provide evidence how you verified the organisation confirms the user identity before modifying their authentication credentials.

(n) Provide evidence how you verified that any passwords/passphrases used have complexity and strength at least equivalent to recognised industry best practice.

(o) Provide evidence how you verified that any reset passwords/passphrases for each user cannot be the same as any previous passwords/passphrases used by the same user.

(p) Provide evidence how you verified

  (i) that first-time passwords/passphrases for new users;

  (ii) and reset passwords/passphrases for existing users, are set to a unique value for each user and changed after first use.

(q) Provide evidence how you verified that group/shared/generic authentication credentials are not used.

(r) Provide evidence how you verified the organisation secures all non-console administrative access to the organisation's infrastructure using MFA.

(s) Provide evidence how you verified that all authentication methods (e.g. physical/logical security tokens, smart cards, etc.), are assigned to an individual, named and unique account.

(t) Provide evidence how you verified that all authentication methods (e.g. physical/logical security tokens, smart cards, etc.), are not assigned to multiple accounts.

Contents

Contents

Section 1 Outcomes

1.1 Outcomes

(a) Necessary roles and responsibilities for the security of networks and information systems supporting essential services have been identified. These are reviewed periodically to ensure they remain fit for purpose.
(b) Appropriately capable and knowledgeable staff fill those roles and are given the time, authority and resources to carry out their duties.
(c) There is clarity on who in your organisation has overall accountability for the security of the networks and information systems supporting your essential service.
(d) Privileged access (e.g. to systems controlling critical functions or system administration) is carried out with separate accounts that are closely managed.
(e) You regularly review privileged access rights and always update privileges as part of your joiners, movers and leavers process.
(f) Privileged access is only granted on devices owned and managed by your organisation.
(g) The list of system administrators is regularly reviewed, e.g. every 6 months.
(h) All remote users are controlled with appropriate access for their job role.
(i) Remote access requirements are protected with MFA and logged.

Section 2 Defined roles and responsibilities

2.1 Controls

2.1.1 *See Ch 8, 2.1 Controls*

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how you verified that access is generally forbidden unless expressly permitted.
(b) Provide evidence how you verified that each role had defined access needs and assigned privileges.
(c) Provide evidence how access is restricted to those least privileges necessary to perform job responsibilities.
(d) Provide evidence how you verified that documented formal approval (either electronically or in writing) is required for all access (including the specific privileges required).
(e) Provide evidence how access rights are periodically reviewed.
(f) Provide evidence how you verified that roles having privileged access are reviewed every 6 months.
(g) Provide evidence how you verified that the removal (i.e. terminated users, change of job responsibilities) of access rights is formally documented.

2.2.2

(a) Provide evidence how you verified that access requirements are defined and include:

(i) system components and data resources that each role needs to access for their job function;
(ii) identification of privilege necessary for each role to perform their job function.

(b) Provide evidence how you verified that privileges assigned are based on that individual's job classification and function.
(c) Provide evidence how you verified that access rights are periodically reviewed.
(d) Provide evidence how you verified that roles having privileged access are reviewed every 6 months.
(e) Provide evidence how individuals receive training appropriate to their organisational roles and responsibilities.
(f) Provide evidence how you verified that the training received was appropriate to the individuals' organisational role and responsibilities.

Section 3
Privileged access rights

3.1 Controls

3.1.1 *See Ch 8, 3.1 Controls*

3.2 Required evidence and testing

3.2.1

(a) Provide evidence how the organisation defined the privileged access rights associated with each system and/or process.
(b) Provide evidence how you verified individuals were allocated the appropriate privileged access rights for each system and/or process.
(c) Provide evidence how (e.g. need-to-use event-by-event, etc.) the organisation allocated (e.g. least privilege necessary to perform their job function, etc.) privileged access rights to individuals.
(d) Provide evidence how the organisation authorises and documents the allocation of privileged access rights.
(e) Provide evidence how you verified that privileged access rights are only granted after the authorisation process is completed.
(f) Provide evidence how the organisation restricts (e.g. defined expiry requirements for) privileged access rights.
(g) Provide evidence how you verified that access rights are periodically reviewed.
(h) Provide evidence how you verified that roles having privileged access are reviewed every 6 months.
(i) Provide evidence how you verified that privileged access rights are assigned to separate and unique user ID(s).

Section 4
Remote user access

4.1 Controls

4.1.1 The organisation must ensure all access to data/systems/services is controlled by a secure log-on procedures. (Maps to ISO 27002: 9.4.2.)

4.1.2 Maturity assessment:

- Does the organisation ensure remote access granted to service providers

(i) is monitored when in use;
(ii) and is disabled when not in use.

4.2 Required evidence and testing

4.2.1 *See Ch 8, 4.2 Required evidence and testing*

Section 5
Secure log-on procedures

5.1 Controls

5.1.1 The organisation must ensure all access to data/systems/services is controlled by a secure log-on procedures. (Maps to ISO 27002: 9.4.2.)

5.1.2 Maturity assessment:

- Does the organisation monitor for inactive user accounts?
- Does the organisation provide

(i) guidance on selecting/protecting authentication credentials?
(ii) instructions to reset authentication credentials, if a compromise of the credentials is suspected?

5.2 Required evidence and testing

5.2.1 *See Ch 8, 5.2 Required evidence and testing*

Contents

Contents

Authentication and Authorisation Domain (Accomplished)

Section 1 Outcomes

1.1 Outcomes

1.1.1

(a) Necessary roles and responsibilities for the security of networks and information systems supporting essential services have been identified. These are reviewed periodically to ensure they remain fit for purpose.

(b) Appropriately capable and knowledgeable staff fill those roles and are given the time, authority and resources to carry out their duties.

(c) There is clarity on who in your organisation has overall accountability for the security of the networks and information systems supporting your essential service.

(d) Privileged access (e.g. to systems controlling critical functions or system administration) is carried out with separate accounts that are closely managed.

(e) You regularly review privileged access rights and always update privileges as part of your joiners, movers and leavers process.

(f) Privileged access is only granted on devices owned and managed by your organisation.

(g) The list of system administrators is regularly reviewed, e.g. every 6 months.

(h) All privileged access to your networks and information systems requires strong authentication, such as two-factor/hardware authentication, or additional real-time security monitoring.

(i) Where you don't already issue temporary, time-bound rights for privileged access and external third-party support access, you are migrating to access control that supports this functionality.

(j) Activity by privileged users is routinely validated.

(k) Only individually authenticated and authorised users can connect to or access your networks or information systems. Both logical and physical access require this individual authentication and authorisation.

(l) User access to all your networks and information systems are limited to the minimum necessary.

(m) You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, when you individually authenticate and authorise all remote access to all your networks and information systems.

(n) The list of individuals with access to all your networks and systems supporting the critical functions are reviewed on a regular basis, e.g. annually.

(o) The list of users with access to critical networks and systems is reviewed on a regular basis, e.g. every 6 months.

(p) Your joiners, leavers and movers process ensures that, in addition to when people change roles, user permissions are reviewed regularly.

(q) All access is logged and monitored.

(r) You regularly review access logs and correlate this data with other access records and expected activity.

(s) Attempts by unauthorised users to connect to your systems are alerted, promptly assessed and investigated where relevant.

(t) All remote users are controlled with appropriate access for their job role.

(u) Remote access requirements are protected with MFA and logged.

Section 2
Defined roles and responsibilities

2.1 Controls

2.1.1 *See Ch 8, 2.1 Controls*

2.2 Required evidence and testing

2.2.1 *See Ch 9, 2.2 Required evidence and testing*

Section 3
Privileged access rights

3.1 Controls

3.1.1 *See Ch 8, 3.1 Controls*

3.2 Required evidence and testing

3.2.1

(a) Provide evidence how the organisation defined the privileged access rights associated with each system and/or process.
(b) Provide evidence how you verified individuals were allocated the appropriate privileged access rights for each system and/or process.
(c) Provide evidence how (e.g. need-to-use; event-by-event, etc.) the organisation allocated (e.g. least privilege necessary to perform their job function, etc.) privileged access rights to individuals.
(d) Provide evidence how the organisation authorises and documents the allocation of privileged access rights.
(e) Provide evidence how you verified that privileged access rights are only granted after the authorisation process is completed.
(f) Provide evidence how the organisation restricts (e.g. defined expiry requirements for) privileged access rights.
(g) Provide evidence how you verified that access rights are periodically reviewed.
(h) Provide evidence how you verified that roles having privileged access are reviewed every 6 months.
(i) Provide evidence how you verified that privileged access rights are assigned to separate and unique user ID(s).
(j) Provide evidence how the organisation verifies that individuals assigned privileged access rights are competent to perform the duties allocated to those privileged access rights.
(k) Provide evidence how the organisation validates the activity of individuals assigned privileged access rights when performing duties allocated to those privileged access rights.
(l) Provide evidence how the organisation prevents the creation of unauthorised privileged access rights.

Section 4
Account/RBAC provisioning and management

4.1 Controls

4.1.1 The organisation must ensure that individuals can only access those networks and services for which they have been granted authorisation. The organisation must implement a formal user access provisioning and management process.

4.1.2 Maturity assessment:

- Does the organisation verify that any access granted is consistent with the access control policies?
- Does the organisation require multi-factor authorisation for all remote and/or privileged access requests?
- Does the organisation regularly review access logs and correlate this data with other access records and expected activity?
- Does the organisation investigate all attempts by unauthorised users to connect to organisational data/systems/services?
- Are authentication and authorisation requirements regularly assessed and improvements identified?

4.1.3 Mappings:

- ISO 27002: 9.1.2
- ISO 27002: 9.2.2
- IEC 62443-3
    - SR 1.3 – Account management
    - SR 1.3 RE 1 – Unified account management
    - SR 1.4 – Identifier management
    - SR 2.1 – authorisation enforcement
    - SR 2.1 RE 1 – authorisation enforcement for all users
    - SR 2.1 RE 2 – Permission mapping to roles

4.2 Required evidence and testing

4.2.1

(a) Provide evidence how you verified that the organisation maintains a central record of granted access rights.
(b) Provide evidence how you verified the central access rights record was kept current and up-to-date.
(c) Provide evidence how unique user ID(s) are allocated to individual users.
(d) Provide evidence how the organisation manages access rights for those individuals who
    (i) change organisational roles;
    (ii) or leave the organisations.
(e) Provide evidence how you verified the procedures for managing access rights of individuals who
    (i) change organisational roles;
    (ii) or leave the organisation were in place and active.
(f) Provide evidence how you verified shared and/or generic user ID(s) were not in use.
(g) Provide evidence how and when the organisation reviews access rights.
(h) Provide evidence how the organisation records and monitors all access requests to organisational data/systems/services.
(i) Provide evidence how the organisation is alerted when unauthorised users attempt to connect to organisational data/systems/services.
(j) Provide evidence how you verified that the organisation is alerted when unauthorised users attempt to connect to organisational data/systems/services.
(k) Provide evidence how the organisation responds to these alerts.

■ *Section 5*
Remote user access

5.1 Controls

5.1.1 *See Ch 9, 4.1 Controls*

5.2 Required evidence and testing

5.2.1 *See Ch 8, 4.2 Required evidence and testing*

■ *Section 6*
Secure log-on procedures

6.1 Controls

6.1.1 *See Ch 9, 5.1 Controls*

Authentication and Authorisation Domain (Accomplished)

6.2 Required evidence and testing

6.2.1 *See Ch 8, 5.2 Required evidence and testing*

Contents

Contents

Section 1
Outcomes

1.1 Outcomes

1.1.1

(a) Necessary roles and responsibilities for the security of networks and information systems supporting essential services have been identified. These are reviewed periodically to ensure they remain fit for purpose.

(b) Appropriately capable and knowledgeable staff fill those roles and are given the time, authority and resources to carry out their duties.

(c) There is clarity on who in your organisation has overall accountability for the security of the networks and information systems supporting your essential service.

(d) Privileged access (e.g. to systems controlling critical functions or system administration) is carried out with separate accounts that are closely managed.

(e) You regularly review privileged access rights and always update privileges as part of your joiners, movers and leavers process.

(f) Privileged access is only granted on devices owned and managed by your organisation.

(g) The list of system administrators is regularly reviewed, e.g. every 6 months.

(h) All privileged access to your networks and information systems requires strong authentication, such as two-factor/hardware authentication, or additional real-time security monitoring.

(i) Where you don't already issue temporary, time-bound rights for privileged access and external third-party support access, you are migrating to access control that supports this functionality.

(j) Activity by privileged users is routinely validated.

(k) You record and store all privileged user sessions for offline analysis and investigation.

(l) Only individually authenticated and authorised users can connect to or access your networks or information systems. Both logical and physical access require this individual authentication and authorisation.

(m) User access to all your networks and information systems are limited to the minimum necessary.

(n) You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, when you individually authenticate and authorise all remote access to all your networks and information systems.

(o) The list of individuals with access to all your networks and systems supporting the critical functions are reviewed on a regular basis, e.g. annually.

(p) The list of users with access to critical networks and systems is reviewed on a regular basis, e.g. every 6 months.

(q) Your joiners, leavers and movers process ensures that, in addition to when people change roles, user permissions are reviewed regularly.

(r) All access is logged and monitored.

(s) You regularly review access logs and correlate this data with other access records and expected activity.

(t) Attempts by unauthorised users to connect to your systems are alerted, promptly assessed and investigated where relevant.

(u) You use additional authentication mechanisms, such as two-factor or hardware-backed certificates, for all systems that operate or support critical functions.
(v) You have an auditable, robust procedure to verify each user and issue minimum required access rights.
(w) Dedicated devices are used for privileged actions (such as administration or accessing the essential service's network and information systems). These devices are not used for directly browsing the web or accessing email.
(x) You have obtained independent or professional assurance of the security of third-party networks, or you only allow third-party devices / networks dedicated to supporting your systems to connect.
(y) You perform device identity management which is cryptographically backed, and only allow known devices to access systems.
(z) You perform regular scans to detect unknown devices and investigate any findings.
(aa) All remote users are controlled with appropriate access for their job role.
(ab) Remote access requirements are protected with MFA and logged.

Section 2
Defined roles and responsibilities

2.1 Controls

2.1.1 *See Ch 8, 2.1 Controls*

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how you verified the role-based access control is based on individual's job classification and function.
(b) Provide evidence how you verified that access is generally forbidden unless expressly permitted.
(c) Provide evidence how you verified that each role had defined access needs and assigned privileges.
(d) Provide evidence how access is restricted to those least privileges necessary to perform job responsibilities.
(e) Provide evidence how you verified that documented formal approval (either electronically or in writing) is required for all access (including the specific privileges required).
(f) Provide evidence how access rights are periodically reviewed.
(g) Provide evidence how you verified that roles having privileged access are reviewed every 6 months.
(h) Provide evidence how you verified that the removal (i.e. terminated users, change of job responsibilities) of access rights is formally documented.

2.2.2

(a) Provide evidence how you verified that access requirements are defined and include:
    (i) system components and data resources that each role needs to access for their job function;
    (ii) identification of privilege necessary for each role to perform their job function.
(b) Provide evidence how you verified that privileges assigned are based on that individual's job classification and function.
(c) Provide evidence how you verified that access rights are periodically reviewed.
(d) Provide evidence how you verified that roles having privileged access are reviewed every 6 months.
(e) Provide evidence how individuals receive training appropriate to their organisational roles and responsibilities.
(f) Provide evidence how you verified that the training received was appropriate to the individuals' organisational role and responsibilities.

Section 3
Privileged access rights

3.1 Controls

3.1.1 *See Ch 8, 3.1 Controls*

3.2 Required evidence and testing

3.2.1

(a) Provide evidence how the organisation defined the privileged access rights associated with each system and/or process.
(b) Provide evidence how you verified individuals were allocated the appropriate privileged access rights for each system and/or process.
(c) Provide evidence how (e.g. need-to-use event-by-event, etc.) the organisation allocated (e.g. least privilege necessary to perform their job function, etc.) privileged access rights to individuals.
(d) Provide evidence how the organisation authorises and documents the allocation of privileged access rights.
(e) Provide evidence how you verified that privileged access rights are only granted after the authorisation process is completed.
(f) Provide evidence how the organisation restricts (e.g. defined expiry requirements for) privileged access rights.
(g) Provide evidence how you verified that access rights are periodically reviewed.
(h) Provide evidence how you verified that roles having privileged access are reviewed every 6 months.
(i) Provide evidence how you verified that privileged access rights are assigned to separate and unique user ID(s).
(j) Provide evidence how the organisation verifies that individuals assigned privileged access rights are competent to perform the duties allocated to those privileged access rights.
(k) Provide evidence how the organisation validates the activity of individuals assigned privileged access rights when performing duties allocated to those privileged access rights.
(l) Provide evidence how the organisation records and stores the activity of individuals assigned privileged access rights when performing duties allocated to privileged access rights.
(m) Provide evidence how the organisation prevents the creation of unauthorised privileged access rights.

Section 4
Account/RBAC provisioning and management

4.1 Controls

4.1.1 *See Ch 10, 4.1 Controls*

4.2 Required evidence and testing

4.2.1

(a) Provide evidence how the organisation's role-based access control (RBAC) links access rights with individuals' organisational role and responsibilities.
(b) Provide evidence how you verified that authorisation from the data/system/network service Owner is required prior to access being granted.
(c) Provide evidence how the organisation verifies that the access granted is consistent with the access control policies.
(d) Provide evidence how the organisation ensures access rights are not granted prior to the completion of the authorisation process.
(e) Provide evidence how you verified that the organisation maintains a central record of granted access rights.
(f) Provide evidence how you verified the central access rights record was kept current and up-to-date.
(g) Provide evidence how unique user ID(s) are allocated to individual users.
(h) Provide evidence how the organisation manages access rights for those individuals who
    (i) change organisational roles;
    (ii) or leave the organisation.
(i) Provide evidence how you verified the procedures for managing access rights of individuals who
    (i) change organisational roles;
    (ii) or leave the organisation were in place and active.
(j) Provide evidence how you verified shared and/or generic user ID(s) were not in use.
(k) Provide evidence how and when the organisation reviews access rights.
(l) Provide evidence how the organisation records and monitors all access requests to organisational data/systems/services.

(m) Provide evidence how the organisation is alerted when unauthorised users attempt to connect to organisational data/systems/services.

(n) Provide evidence how you verified that the organisation is alerted when unauthorised users attempt to connect to organisational data/systems/services.

(o) Provide evidence how the organisation responds to these alerts.

Section 5
Controlled access

5.1 Controls

5.1.1 The organisation must ensure that any feature (i.e. system administration privileges) or facility (i.e. system utility programs) that can override system or application controls are managed and controlled.

5.1.2 Mappings:

- ISO 27002: 9.4
- IEC 62443-3
  - SR 1.5 – Authenticator management
  - SR 1.5 RE 1 – Hardware security for software process identity credentials
  - SR 1.8 – Public key infrastructure (PKI) certificates
  - SR 1.9 – Strength of public key authentication
  - SR 1.9 RE 1 – Hardware security for public key authentication
  - SR 1.12 – System use notification
  - SR 2.1 RE 3 – Supervisor override
  - SR 2.5 – Session lock

5.2 Required evidence and testing

5.2.1

(a) Provide evidence how system functionality required to access critical data and/or systems that store, process and/or transmit critical data is restrict to only that which is necessary.

(b) Provide evidence how you verified that system functionality required to access critical data and/or systems that store, process and/or transmit critical data is restrict to only that which is necessary.

(c) Provide evidence how you verified that the organisation maintains and implement policies and procedures to manage service providers with whom critical data is shared, or that could affect the security of critical data.

(d) Provide evidence how you verified that service providers with remote access to the organisation's infrastructure use MFA.

(e) Provide evidence how you verified that the organisation maintains written agreements that includes an acknowledgement that service providers are responsible for the security of critical data the service providers stores, processes and/or transmits on behalf of the organisation, or to the extent that the service provider could impact on the security of the organisation's facilities that store, process and/or transmit critical data.

(f) If the service provider is able to offer an information security accreditation (i.e. ISO 27001), then provide evidence how the organisation maintains a programme to monitor service providers' certification status.

(g) Provide evidence how you verified that physical and/or logical controls ensure only the intended account and/or device can gain access to data/systems/services.

(h) Provide evidence how the organisation is alerted when unauthorised devices are used to connect to organisational data/systems/services.

(i) Provide evidence how you verified that the organisation is alerted when unauthorised devices attempt to connect to organisational data/systems/services.

(j) Provide evidence how the organisation responds to these alerts.

Section 6
Remote user access

6.1 Controls

6.1.1 *See Ch 9, 4.1 Controls*

6.2 Required evidence and testing

6.2.1 *See Ch 8, 4.2 Required evidence and testing*

Section 7
Secure log-on procedures

7.1 Controls

7.1.1 *See Ch 9, 5.1 Controls*

7.2 Required evidence and testing

7.2.1 *See Ch 8, 5.2 Required evidence and testing*

Contents

Contents

Section 1
Outcomes

1.1 Outcomes

1.1.1

(a) Network boundaries are clearly defined with entry points being secured to provide security, filtering and visibility of information coming into and leaving the network.

Section 2
Network perimeter security

2.1 Controls

2.1.1 As part of organisation's network security management programme, appropriate network controls to manage the security of network services must be in place.

2.1.2 Mappings:

- ISO 2002: 13
- IEC 62443-3
    - SR 2.2 – Wireless use control
    - SR 2.2 RE 1 – Identify and report unauthorised wireless devices
    - SR 3.1 – Communication integrity
    - SR 3.2 – Malicious code protection
    - SR 3.2 RE 1 – Malicious code protection on entry and exit points
    - SR 3.2 RE 2 – Central management and reporting for malicious code protection
    - SR 5.2 – Zone boundary protection
    - SR 5.2 RE 1 – Deny by default, allow by exception
    - SR 5.2 RE 2 – Island mode
    - SR 5.2 RE 3 – Fail close
    - SR 5.3 – General purpose person-to-person communication restrictions
    - SR 7.1 – Denial of service protection
    - SR 7.1 RE 1 – Manage communication loads
    - SR 7.1 RE 2 – Limit DoS effects to other systems or networks
    - SR 7.2 – Resource management
    - SR 7.6 – Network and security configuration settings

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how you verified the organisation has a formal process for approving all network connections/configurations.

(b) Provide evidence how you verified all network connections/configurations were approved.

(c) Provide evidence how you verified the organisation has a formal process for approving all changes to network connections/configurations.

(d) Provide evidence how you verified all changes to network connections/configurations were approved.

(e) Provide evidence how the organisation documents network connections/configurations.

(f) Provide evidence how you verified that documented network connections/configurations are

  (i) up-to-date;

  (ii) and include all connections/configurations.

(g) Provide evidence how the organisation documents the data flow across the organisation's networks.

(h) Provide evidence how you verified that documented data flow diagrams are

  (i) up-to-date;

  (ii) and include all connections/configurations.

(i) Provide evidence how you verified that the management of network components/connections/configurations included a formal description of groups, roles and responsibilities.

(j) Provide evidence how the organisation provides a justification and approval for all network services, protocols and ports being used.

(k) Provide evidence how the organisation justified and approved the use of those network services, protocols and ports that are considered insecure.

Contents

Contents

Section 1
Outcomes

1.1 Outcomes: network perimeter security

1.1.1

(a) Network boundaries are clearly defined with entry points being secured to provide security, filtering and visibility of information coming into and leaving the network.
(b) Appropriate tools and technologies are used to mitigate threats that face the network and environment.
(c) Technologies at the perimeter protect internal systems from unauthorised access.

1.2 Outcomes: network segregation

1.2.1

(a) Techniques and tools are used to split the network into different segments in order to reduce the scope of any particular segment.
(b) Network configurations are reviewed, documented and tested to ensure that they effective and secure.
(c) Different segments in the network should have clearly defined boundaries with access controlled by perimeter utilities.

1.3 Outcomes: secure configuration and patching

1.3.1

(a) You have identified, documented and actively manage the assets that need to be carefully configured to maintain the security of the ship's operational service.
(b) All platforms conform to your secure, consistent baseline build or latest known good configuration version for that environment.
(c) You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.

Section 2
Network perimeter security

2.1 Controls

2.1.1 *See Ch 12, 2.1 Controls*

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how you verified the organisation has a formal process for approving and testing all network connections/ configurations.
(b) Provide evidence how you verified all network connections/configurations were
    (i) approved;

(ii) and tested.

(c) Provide evidence how you verified the organisation has a formal process for approving and testing all changes to network connections/configurations.

(d) Provide evidence how you verified all changes to network connections/configurations were

(i) approved;

(ii) and tested.

(e) Provide evidence how the organisation documents network connections/configurations.

(f) Provide evidence how you verified that documented network connections/configurations are

(i) up-to-date;

(ii) and include all connections/configurations.

(g) Provide evidence how the organisation documents the data flow across the organisation's networks.

(h) Provide evidence how you verified that documented data flow diagrams are

(i) up-to-date;

(ii) and include all connections/configurations.

(i) Provide evidence how you verified that the management of network components/connections/configurations included a formal description of groups, roles and responsibilities.

(j) Provide evidence how the organisation provides a justification and approval for all network services, protocols and ports being used.

(k) Provide evidence how the organisation justified and approved the use of those network services, protocols and ports that are considered insecure.

(l) Provide evidence how you verified network connections/configurations only allowed necessary and approved network traffic.

(m) Provide evidence how the organisation secures and synchronises network configurations.

(n) Provide evidence how you verified that network configurations were secured and synchronised.

(o) Provide evidence how the organisation ensures facilities that store, process and/or transmit critical data does not have a direct connection to the Internet.

(p) Provide evidence how you verified that facilities that store, process and/or transmit critical data do not have a direct connection to the Internet.

(q) Provide evidence how the organisation ensures inbound connections to an internal network only originate from an established session.

(r) Provide evidence how you verified all inbound connections (not associated with an established session) to an internal network were prohibited.

(s) Provide evidence how the organisation ensures private IP addresses and routing information are not disclosed.

(t) Provide evidence how you verified that private IP addresses and routing information are not disclosed.

(u) Provide evidence how the organisation protects all portable computing devices (that are used within data facilities to access services that store, process and/or transmit critical data) when connected to the Internet outside of such facilities.

(v) Provide evidence how you verified that security configurations protecting such portable computing devices were

(i) defined and documented;

(ii) actively running;

(iii) and cannot be altered/disabled by users.

■ *Section 3*
Network segregation

3.1 Controls

3.1.1 The organisation must use network segmentation to manage and control the security of networks that store, process and/or transmit critical data.

3.1.2 Mappings:

- ISO 27002: 13

- IEC 62443-3
  - SR 3.2 – Malicious code protection
  - SR 3.2 RE 1 – Malicious code protection on entry and exit points
  - SR 3.2 RE 2 – Central management and reporting for malicious code protection
  - SR 5.1 – Network segmentation
  - SR 5.1 RE 1 – Physical network segmentation
  - SR 5.1 RE 2 – Independence from non-control system networks
  - SR 5.1 RE 3 – Logical and physical isolation of critical networks
  - SR 7.6 – Network and security configuration settings

3.2 Required evidence and testing

3.2.1

(a) Provide evidence how the organisation uses network segregation to isolate groups and users.
(b) Provide evidence how the organisation
  (i) documents;
  (ii) reviews;
  (iii) and tests network segregation controls.
(c) Provide evidence how the organisation ensures network segregations are effective and secure.
(d) Provide evidence how you verified the segmentation was functioning as intended by the organisation.
(e) Provide evidence for the security controls used to ensure the integrity of the segmentation systems.
(f) Provide evidence how you verified the security controls (used to ensure the integrity of the segmentation systems) were
  (i) defined and documented;
  (ii) and effective and secure.
(g) Provide evidence how you verified that penetration testing is used to confirm all segmentation systems are operational and effective.
(h) Provide evidence how you verified that penetration testing was performed after changes to the segmentation systems.

Section 4
Secure configuration and patching

4.1 Controls

4.1.1 The organisation should ensure that all systems are hardened and patched to a level that addresses the risk faced and in line with industry guidance. This will include a baseline system hardening policy as well as ongoing maintenance and patching procedures that may be adapted based on the likely threat impacts and value of the assets.

4.1.2 Mappings:

- ISO 27002: 12
- IEC 62443-3
  - SR 2.3 – Use control for portable and mobile devices
  - SR 2.3 RE 1 – Enforcement of security status of portable and mobile devices
  - SR 2.4 – Mobile code
  - SR 2.4 RE 1 – Mobile code integrity check
  - SR 2.5 – Session lock
  - SR 2.6 – Remote session termination
  - SR 2.7 – Concurrent session control
  - SR 3.2 – Malicious code protection
  - SR 3.2 RE 1 – Malicious code protection on entry and exit points
  - SR 3.2 RE 2 – Central management and reporting for malicious code protection

- SR 3.5 – Input validation
- SR 3.8 – Session integrity
- SR 3.8 RE 1 – Invalidation of session IDs after session termination
- SR 3.8 RE 2 – Unique session ID generation
- SR 3.8 RE 3 – Randomness of session IDs
- SR 3.9 – Protection of audit information
- SR 3.9 RE 1 – Audit records on write-once media
- SR 4.1 – Information confidentiality
- SR 4.2 – Information persistence
- SR 4.2 RE 1 – Purging of shared memory resources
- SR 5.3 – General purpose person-to-person communication restrictions
- SR 5.4 – Application partitioning
- SR 7.6 – Network and security configuration settings
- SR 7.6 RE 1 – Machine-readable reporting of current security settings
- SR 7.7 – Least functionality

4.2 Required evidence and testing

4.2.1

(a) Provide evidence how the organisation ensures that systems, networks and/or software are protected from known vulnerabilities.

(b) Provide evidence how you verified that all systems, networks and/or software are protected from known vulnerabilities.

(c) Provide evidence how you verified that vendor defaults for system components and other security controls were changed before being deployed.

(d) Provide evidence how you verified that default accounts for system components and other security controls were either removed or disabled.

(e) Provide evidence how you verified that configuration standards for all system and network components follow recognised industry hardening guidelines.

(f) Provide evidence how you verified that the configuration standards focus on all known security vulnerabilities.

(g) Provide evidence how you verified that configuration standards are

  (i) documented;
  (ii) kept up-to date;
  (iii) and in use.

(h) Provide evidence how the organisation only enables those services, protocols, ports and/or daemons as defined by the system's function.

(i) Provide evidence how you verified that only those services, protocols, ports and/or daemons (as defined by the system's function) are enabled.

(j) Provide evidence how you verified that any insecure services, protocols and/or daemons were protected with additional security controls.

(k) Provide evidence how you verified that security controls were protected from misuse.

(l) Provide evidence how you verified that all functionality not required was removed or disabled.

(m) Provide evidence for the encryption algorithms used to encrypt non-console administrative access.

(n) Provide evidence how you verified that non-console administrative access was encrypted using industry recognised strong encryption.

(o) Provide evidence how you verified that patching and configuration security policies and procedures were

  (i) documented;
  (ii) applied;
  (iii) and disseminated.

Contents

Contents

Secure Networks and Systems Domain (Accomplished)

Section 1
Outcomes

1.1 Outcomes: network perimeter security

1.1.1

(a) Network boundaries are clearly defined with entry points being secured to provide security, filtering and visibility of information coming into and leaving the network.
(b) Appropriate tools and technologies are used to mitigate threats that face the network and environment.
(c) Technologies at the perimeter protect internal systems from unauthorised access.
(d) As part of accounting, secure configurations are communicated and documented.

1.2 Outcomes: network segregation

1.2.1 *See Ch 13, 1.2 Outcomes: network segregation*

1.3 Outcomes: secure configuration and patching

1.3.1

(a) You have identified, documented and actively manage the assets that need to be carefully configured to maintain the security of the ship's operational service.
(b) All platforms conform to your secure, consistent baseline build or latest known good configuration version for that environment.
(c) You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.
(d) You regularly review and validate that your network and information systems have the expected, secured settings and configuration.
(e) Only permitted software can be installed and standard users cannot change settings that would impact security or business operation.

1.4 Outcomes: cryptographic security

1.4.1

(a) Cryptographic tools should be implemented appropriately in regards to security objectives.
(b) Cryptographic techniques should outline protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys.
(c) The responsibilities of those who manage and generate keys are clearly defined.

Section 2
Network: perimeter security

2.1 Controls

2.1.1 *See Ch 12, 2.1 Controls*

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how you verified the organisation has a formal process for approving and testing all network connections/configurations.

(b) Provide evidence how you verified all network connections/configurations were

  (i) approved;
  (ii) and tested.

(c) Provide evidence how you verified the organisation has a formal process for approving and testing all changes to network connections/configurations.

(d) Provide evidence how you verified all changes to network connections/configurations were

  (i) approved;
  (ii) and tested.

(e) Provide evidence how the organisation documents network connections/configurations.

(f) Provide evidence how you verified that documented network connections/configurations are

  (i) up-to-date;
  (ii) and include all connections/configurations.

(g) Provide evidence how the organisation documents the data flow across the organisation's networks.

(h) Provide evidence how you verified that documented data flow diagrams are

  (i) up-to-date;
  (ii) and include all connections/configurations.

(i) Provide evidence how the organisation follows industry recognised secure architecture principles (i.e. deploying a firewall at each Internet connection, deploying a firewall between a DMZ and an internal network, using segmentation to isolate different networks).

(j) Provide evidence how you verified the organisation

  (i) deploys a firewall at each Internet connection;
  (ii) deploys a firewall between a DMZ and an internal network;
  (iii) and isolates networks using segmentation.

(k) Provide evidence how you verified that the management of network components/connections/configurations included a formal description of groups, roles and responsibilities.

(l) Provide evidence how the organisation provides a justification and approval for all network services, protocols and ports being used.

(m) Provide evidence how the organisation justified and approved the use of those network services, protocols and ports that are considered insecure.

(n) Provide evidence how the organisation ensure that network connections/configurations are reviewed every 6 months.

(o) Provide evidence how you verified that organisation reviews network connections/configurations every 6 months.

(p) Provide evidence how you verified network connections/configurations only allowed necessary and approved network traffic.

(q) Provide evidence how the organisation secures and synchronises network configurations.

(r) Provide evidence how you verified that network configurations were secured and synchronised.

(s) Provide evidence how the organisation ensures facilities that store, process and/or transmit critical data does not have a direct connection to the Internet.

(t) Provide evidence how you verified that facilities that store, process and/or transmit critical data do not have a direct connection to the Internet.

(u) Provide evidence how the organisation ensures inbound connections to an internal network only originate from an established session.

(v) Provide evidence how you verified all inbound connections (not associated with an established session) to an internal network were prohibited.

(w) Provide evidence how the organisation ensures private IP addresses and routing information are not disclosed.

(x) Provide evidence how you verified that private IP addresses and routing information are not disclosed.

(y) Provide evidence how the organisation protects all portable computing devices (that are used within data facilities to access services that store, process and/or transmit critical data) when connected to the Internet outside of such facilities.

(z) Provide evidence how you verified that security configurations protecting such portable computing devices were

(i) defined and documented;
(ii) actively running;
(iii) and cannot be altered/disabled by users.

(aa) Provide evidence how you verified that network perimeter security policies and procedures were

(i) documented;
(ii) applied;
(iii) and disseminated.

Section 3
Network segregation

3.1 Controls

3.1.1 *See Ch 13, 3.1 Controls*

3.2 Required evidence and testing

3.2.1

(a) Provide evidence how the organisation uses network segregation to isolate groups and users.

(b) Provide evidence how the organisation

(i) documents;
(ii) reviews;
(iii) and tests network segregation controls.

(c) Provide evidence how the organisation ensures network segregations are effective and secure.

(d) Provide evidence how you verified the perimeter of each segregated network was defined and documented.

(e) Provide evidence how the organisation controls access between segregated network domains.

(f) Provide evidence how you verified the access controls on segregated network domains were effective and secure.

(g) Provide evidence for the criteria used to

(i) segregate the network into domains;
(ii) and define the access controls.

(h) Provide evidence how you verified the segmentation was functioning as intended by the organisation.

(i) Provide a description of the security controls used to ensure the integrity of the segmentation systems.

(j) Provide evidence how you verified the security controls (used to ensure the integrity of the segmentation systems) were

(i) defined and documented;
(ii) and effective and secure.

(k) Provide evidence how you verified that penetration testing is used to confirm all segmentation systems are operational and effective.

(l) Provide evidence how you verified that penetration testing was performed after changes to the segmentation systems.

Section 4
Secure configuration and patching

4.1 Required evidence and testing

4.1.1

(a) Provide evidence how the organisation ensures that systems, networks and/or software are protected from known vulnerabilities.

(b) Provide evidence how you verified that all systems, networks and/or software are protected from known vulnerabilities.

(c) Provide evidence how the change management procedures include documented approval for the deployment of security patches.

(d) Provide evidence how you verified that the deployment of security patches requires documented approval.

(e) Provide evidence how you verified that vendor defaults for system components and other security controls were changed before being deployed.

(f) Provide evidence how you verified that default accounts for system components and other security controls were either removed or disabled.

(g) Provide evidence how you verified that configuration standards for all system and network components follow recognised industry hardening guidelines.

(h) Provide evidence how you verified that the configuration standards focus on all known security vulnerabilities.

(i) Provide evidence how you verified that configuration standards are

  (i) documented;
  (ii) kept up-to date;
  (iii) and in use.

(j) Provide evidence how the organisation prevents the deployment on the same server of functionality requiring differing security levels.

(k) Provide evidence how you verified that the organisation has only implemented one primary function per server.

(l) Provide evidence how the organisation only enables those services, protocols, ports and/or daemons as defined by the system's function.

(m) Provide evidence how you verified that only those services, protocols, ports and/or daemons (as defined by the system's function) are enabled.

(n) Provide evidence how you verified that any insecure services, protocols and/or daemons were protected with additional security controls.

(o) Provide evidence how you verified that security controls were protected from misuse.

(p) Provide evidence how you verified that all functionality not required was removed or disabled.

(q) Provide a description of the encryption algorithms used to encrypt non-console administrative access.

(r) Provide evidence how you verified that non-console administrative access was encrypted using industry recognised strong encryption.

(s) Provide evidence how you verified that a record of hardware components and/or software applications is documented.

(t) Provide evidence how you verified the record

  (i) includes a description of the functionality for each component and/or application;
  (ii) and is up-to-date.

(u) Provide evidence how you verified that patching and configuration security policies and procedures were

  (i) documented;
  (ii) applied;
  (iii) and disseminated.

Section 5
Cryptographic security

5.1 Controls

5.1.1 The organisation must use a risk-based approach when developing cryptographic controls for protecting critical data.

5.1.2 Mappings:

- ISO 27002: 10
- IEC 62443-3
    - SR 1.8 – Public key infrastructure (PKI) certificates
    - SR 1.9 – Strength of public key authentication
    - SR 1.9 RE 1 – Hardware security for public key authentication
    - SR 3.1 – Communication integrity
    - SR 3.1 RE 1 – Cryptographic integrity protection
    - SR 4.1 – Information confidentiality
    - SR 4.1 RE 1 – Protection of confidentiality at rest or in transit via untrusted networks
    - SR 4.1 RE 2 – Protection of confidentiality across zone boundaries
    - SR 4.3 – Use of cryptography

5.2 Required evidence and testing

5.2.1

(a) Provide evidence how you verified the cryptographic architecture supports organisational security objectives.
(b) Provide evidence how you verified the cryptographic architecture was implemented
    (i) as defined by industry best practice and/or;
    (ii) as detailed in the vendor's documentation.
(c) Provide evidence how the organisation stores encryption keys.
(d) Provide evidence how you verified that encryption keys are stored securely.
(e) Provide evidence how the organisation documents the description of the cryptographic architecture.
(f) Provide evidence how you verified that the documented description details
    (i) algorithms, protocols and keys (key strength/expiry date) used;
    (ii) and key usage.
(g) Provide evidence how you verified the deployed encryption solution is mirrored by the documented description of cryptographic architecture.
(h) Provide evidence how access to encryption keys is restricted to those individuals with a documented need to access them.
(i) Provide evidence how you verified access to encryption keys is restricted.
(j) Provide evidence how the organisation stores keys used to encrypt/decrypt data.
(k) Provide evidence how you verified that encryption security policies and procedures were
    (i) documented;
    (ii) applied;
    (iii) and disseminated.
(l) Provide evidence how you verified that strong encryption is used to secure the transmission (over open public networks, including the use of end-user messaging technologies) of critical data.
(m) Provide evidence how you verified that strong encryption is used to guarantee authentication credentials are indecipherable during storage and transmission.

Contents

Contents

Section 1
Outcomes

1.1 Outcomes: network perimeter security

1.1.1 *See Ch 14, 1.1 Outcomes: network perimeter security*

1.2 Outcomes: network segregation

1.2.1

(a) Techniques and tools are used to split the network into different segments in order to reduce the scope of any particular segment.
(b) Network configurations are reviewed, documented and tested to ensure that they effective and secure.
(c) Different segments in the network should have clearly defined boundaries with access controlled by perimeter utilities.
(d) Wireless networks should be segregated from the rest of the network.

1.3 Outcomes: secure configuration and patching

1.3.1

(a) You have identified, documented and actively manage the assets that need to be carefully configured to maintain the security of the ship's operational service.
(b) All platforms conform to your secure, consistent baseline build or latest known good configuration version for that environment.
(c) You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.
(d) You regularly review and validate that your network and information systems have the expected, secured settings and configuration.
(e) Only permitted software can be installed and standard users cannot change settings that would impact security or business operation.
(f) If automated decision-making technologies are in use, their operation is well understood and decisions can be replicated.

1.4 Outcomes: cryptographic security

1.4.1

(a) Cryptographic tools should be implemented appropriately in regards to security objectives.
(b) Cryptographic techniques should outline protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys.
(c) The responsibilities of those who manage and generate keys are clearly defined.
(d) The impact of using cryptographic tools and encryption is clearly understood and evaluated.
(e) Assessment and selection of cryptographic technologies should be viewed as part of a larger risk management process.

Section 2
Network perimeter security

2.1 Controls

2.1.1 *See Ch 12, 2.1 Controls*

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how you verified the organisation has a formal process for approving and testing all network connections/configurations (including wireless network connections/configurations).

(b) Provide evidence how you verified all network connections/configurations were

  (i) approved;
  (ii) and tested.

(c) Provide evidence how you verified the organisation has a formal process for approving and testing all changes to network connections/configurations.

(d) Provide evidence how you verified all changes to network connections/configurations were

  (i) approved;
  (ii) and tested.

(e) Provide evidence how the organisation documents network connections/configurations.

(f) Provide evidence how you verified that documented network connections/configurations are

  (i) up-to-date;
  (ii) and includes all connections/configurations.

(g) Provide evidence how the organisation documents the data flow across the organisation's networks.

(h) Provide evidence how you verified that documented data flow diagrams are

  (i) up-to-date;
  (ii) and includes all connections/configurations.

(i) Provide evidence how the organisation follows industry recognised secure architecture principles (i.e. deploying a firewall at each Internet connection, deploying a firewall between a DMZ and an internal network, using segmentation to isolate different networks).

(j) Provide evidence how you verified the organisation

  (i) deploys a firewall at each Internet connection;
  (ii) deploys a firewall between a DMZ and an internal network;
  (iii) and isolates networks using segmentation.

(k) Provide evidence how you verified that the management of network components/connections/configurations included a formal description of groups, roles and responsibilities.

(l) Provide evidence how the organisation provides a justification and approval for all network services, protocols and ports being used.

(m) Provide evidence how the organisation justified and approved the use of those network services, protocols and ports that are considered insecure.

(n) Provide evidence how the organisation ensure that network connections/configurations are reviewed every 6 months.

(o) Provide evidence how you verified that organisation reviews network connections/configurations every 6 months.

(p) Provide evidence how you verified network connections/configurations only allowed necessary and approved network traffic.

(q) Provide evidence how the organisation secures and synchronises network configurations.

(r) Provide evidence how you verified that network configurations were secured and synchronised.

(s) Provide evidence how you verified that firewalls were deployed between wireless networks and facilities that store, process and/or transmit critical data.

(t) Provide evidence how you verified wireless network connections/configurations only allowed necessary and approved network traffic.

(u) Provide evidence how the organisation ensures facilities that store, process and/or transmit critical data does not have a direct connection to the Internet.

(v) Provide evidence how you verified that facilities that store, process and/or transmit critical data do not have a direct connection to the Internet.

(w) Provide evidence how the organisation ensures inbound connections to an internal network only originate from an established session.

(x) Provide evidence how you verified all inbound connections (not associated with an established session) to an internal network were prohibited.

(y) Provide evidence how the organisation ensures private IP addresses and routing information are not disclosed.

(z) Provide evidence how you verified that private IP addresses and routing information are not disclosed.

(aa) Provide evidence how the organisation protects all portable computing devices (that are used within data facilities to access services that store, process and/or transmit critical data) when connected to the Internet outside of such facilities.

(ab) Provide evidence how you verified that security configurations protecting such portable computing devices were

(i) defined and documented;
(ii) actively running;
(iii) and cannot be altered/disabled by users.

(ac) Provide evidence how you verified that network perimeter security policies and procedures were

(i) documented;
(ii) applied;
(iii) and disseminated.

Section 3
Network segregation

3.1 Controls

3.1.1 *See Ch 13, 3.1 Controls*

3.2 Required evidence and testing

3.2.1

(a) Provide evidence how the organisation uses network segregation to isolate groups and users.

(b) Provide evidence how the organisation

(i) documents;
(ii) reviews;
(iii) and tests network segregation controls.

(c) Provide evidence how the organisation ensures network segregations are effective and secure.

(d) Provide evidence how you verified that wireless networks are segregated from the rest of the network.

(e) Provide evidence how you verified the perimeter of each segregated network was defined and documented.

(f) Provide evidence how the organisation controls access between segregated network domains.

(g) Provide evidence how you verified the access controls on segregated network domains were effective and secure.

(h) Provide a description of the criteria used to

(i) segregate the network into domains;
(ii) and define the access controls.

(i) Provide evidence how you verified the segmentation was functioning as intended by the organisation.

(j) Provide a description of the security controls used to ensure the integrity of the segmentation systems.

(k) Provide evidence how you verified the security controls (used to ensure the integrity of the segmentation systems) were

(i) defined and documented;
(ii) and effective and secure.

(l) Provide evidence how you verified that penetration testing is used to confirm all segmentation systems are operational and effective.

(m) Provide evidence how you verified that penetration testing was performed after changes to the segmentation systems.

Section 4
Secure configuration and patching

4.1 Required evidence and testing

4.1.1

(a) Provide evidence how the organisation ensures that systems, networks and/or software are protected from known vulnerabilities.

(b) Provide evidence how you verified that all systems, networks and/or software are protected from known vulnerabilities.

(c) Provide evidence how the change management procedures include documented approval for the deployment of security patches.

(d) Provide evidence how you verified that the deployment of security patches requires documented approval.

(e) Provide evidence how you verified that vendor defaults for system components (including WiFi access points) and other security controls were changed before being deployed.

(f) Provide evidence how you verified that default accounts for system components (including WiFi access points) and other security controls were either removed or disabled.

(g) Provide evidence how you verified that configuration standards for all system and network components follow recognised industry hardening guidelines.

(h) Provide evidence how you verified that the configuration standards focus on all known security vulnerabilities.

(i) Provide evidence how you verified that configuration standards are

  (i) documented;
  (ii) kept up-to date;
  (iii) and in use.

(j) Provide evidence how the organisation prevents the deployment on the same server of functionality requiring differing security levels.

(k) Provide evidence how you verified that the organisation has only implemented one primary function per server.

(l) Provide evidence how the organisation only enables those services, protocols, ports and/or daemons as defined by the system's function.

(m) Provide evidence how you verified that only those services, protocols, ports and/or daemons (as defined by the system's function) are enabled.

(n) Provide evidence how you verified that any insecure services, protocols and/or daemons were protected with additional security controls.

(o) Provide evidence how you verified that security controls were protected from misuse.

(p) Provide evidence how you verified that all functionality not required was removed or disabled.

(q) Provide a description of the cryptographic algorithms used to encrypt non-console administrative access.

(r) Provide evidence how you verified that non-console administrative access was encrypted using industry recognised strong encryption.

(s) Provide evidence how you verified that a record of hardware components and/or software applications is documented.

(t) Provide evidence how you verified the record

  (i) includes a description of the functionality for each component and/or application;
  (ii) and is up-to-date.

(u) Provide evidence how you verified that patching and configuration security policies and procedures were

  (i) documented;
  (ii) applied;
  (iii) and disseminated.

Section 5
Cryptographic security

5.1 Controls

5.1.1 *See Ch 14, 5.1 Controls*

5.2 Required evidence and testing

5.2.1

(a) Provide evidence how you verified the cryptographic architecture supports organisational security objectives.

(b) Provide evidence how the organisation incorporated a risk management process to assess, select and manage the encryption technologies.

(c) Provide evidence how you verified the cryptographic architecture was implemented

  (i) as defined by industry best practice;

  (ii) and/or as detailed in the vendor's documentation.

(d) Provide evidence how the organisation stores encryption keys.

(e) Provide evidence how you verified that encryption keys are stored securely.

(f) Provide evidence how the organisation documents the description of the cryptographic architecture.

(g) Provide evidence how you verified that the documented description details

  (i) algorithms, protocols and keys (key strength/expiry date) used;

  (ii) and key usage.

(h) Provide evidence how you verified the deployed encryption solution is mirrored by the documented description of cryptographic architecture.

(i) Provide evidence how access to encryption keys is restricted to those individuals with a documented need to access them.

(j) Provide evidence how you verified access to encryption keys is restricted.

(k) Provide evidence how the organisation stores keys used to encrypt/decrypt data.

(l) Provide a description of the organisation's key management procedures.

(m) Provide evidence how you verified the key management procedures

  (i) generate strong encryption keys;

  (ii) secure the distribution of encryption keys;

  (iii) secure the storage of encryption keys;

  (iv) define the encryption keys cryptoperiod;

  (v) define when encryption keys must be retired/replaced;

  (vi) prevent the unauthorised substitution of encryption keys;

  (vii) and require a formal acknowledgment from key-custodian responsibilities.

(n) Provide evidence how you verified that encryption security policies and procedures were

  (i) documented;

  (ii) applied;

  (iii) and disseminated.

(o) Provide evidence how you verified that strong encryption is used to secure the transmission (over open public networks, including the use of end-user messaging technologies) of critical data.

(p) Provide evidence how you verified that strong encryption is used to guarantee authentication credentials are indecipherable during storage and transmission.

Contents

Contents

Section 1
Security policies

1.1 Outcomes

1.1.1

(a) Your organisation's cyber security policies and processes are developed to be practical, usable and appropriate for your ship's operational use, context, dependencies and technologies.

(b) Where your cyber security policies and processes place requirements on people, e.g. changes in behaviour or activity, this is practical and they can do what is expected.

(c) You review and improve policies and processes at suitably regular intervals to ensure they remain relevant to threats, the way people and systems work, adapt to lessons learned and remain appropriate and effective. This is in addition to reviews following a major cyber security incident.

(d) You document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance.

(e) Cyber security is embedded throughout these policies and processes and key performance indicators are reported to your executive management.

(f) Your cyber security policies and processes are effectively and appropriately communicated across all levels of the organisation.

(g) All staff are aware of their responsibilities under your service protection policies and processes.

(h) Suitable action is taken to correct significant single or aggregated breaches of cyber security policies and processes.

1.2 Controls

1.2.1 The organisation must ensure a set of cyber security policies

(a) are establish and published;

(b) have management approval;

(c) and are freely disseminated to all individuals (including contractors and relevant external service providers).

(Maps to ISO 27002:5.)

1.2.2 The organisation must ensure reviews of the cyber security policies are undertaken. (Maps to ISO 27002:5.)

1.3 Required evidence and testing

1.3.1

(a) Provide evidence how the organisation's cyber security policies define the way in which the organisation manages its cyber security objectives.

(b) Provide evidence how the organisation's cyber security policies define and manage all activities relating to cyber security (including assigning responsibilities for cyber security to specific roles).

(c) Provide evidence how you verified the assignment of cyber security responsibilities to specific roles was

  (i) current;

  (ii) active;

  (iii) and known to all relevant parties.

(d) Provide evidence how the organisation's cyber security policies take into account deviations and exceptions to the organisation's operational and cyber threat environment.

(e) Provide evidence how the organisation's cyber security policies take into account

  (i) the organisation's business strategy and operational environment;

  (ii) legal, regulatory and contractual obligations;

(iii) and current and projected risk-based cyber security threat models.

(f) Provide evidence how you verified the organisation's cyber security policies

(i) are established and published;
(ii) have senior management approval;
(iii) and are disseminated to all individuals (including contractors and relevant external service providers).

(g) Provide evidence how the organisation's cyber security policies

(i) make reference to topic specific cyber security requirements and procedures (e.g. authentication and authorisation, asset management, etc.).

(h) Provide evidence how these topic specific cyber security requirements and procedures support the organisation's cyber security policies.

(i) Provide evidence how these topic specific cyber security requirements and procedures are disseminated to all individuals (including contractors and relevant external service providers).

(j) Provide evidence how the dissemination of these topic specific cyber security requirements and procedures

(i) are readily accessible and understandable;
(ii) and form part of an organisational security awareness programme.

(k) Provide evidence how you verified the dissemination of these topic specific cyber security requirements and procedures

(i) are readily accessible and understandable;
(ii) and form part of an organisational security awareness programme.

(l) Provide evidence how the organisation deals with a single or aggregated breaches of cyber security policies and processes.

1.3.2

(a) Provide evidence how the organisation ensures the cyber security policies continue to be appropriate, effective and relevant.

(b) Provide evidence how the organisation conducted reviews of the cyber security policies.

(c) Provide evidence how you verified that reviews of the cyber security policies are undertaken

(i) at regular intervals;
(ii) after significant changes to the organisation's business strategy and operational environment;
(iii) after a cyber security incident;
(iv) and when the organisation's cyber security threat models are updated.

(d) Provide evidence how you verified senior management approval was required for any modification to the cyber security policies.

Contents

Contents

Section 1
Security policies

1.1 Outcomes

1.1.1 *See Ch 16, 1.1 Outcomes*

1.2 Controls

1.2.1 *See Ch 16, 1.2 Controls*

1.3 Required evidence and testing

1.3.1 *See Ch 16, 1.3 Required evidence and testing*

Contents

Contents

Section 1
Security policies

1.1 Outcomes

1.1.1 *See Ch 16, 1.1 Outcomes*

1.2 Controls

1.2.1 *See Ch 16, 1.2 Controls*

1.3 Required evidence and testing

1.3.1 *See Ch 16, 1.3 Required evidence and testing*

Contents

Contents

Section 1
Security policies

1.1 Outcomes

1.1.1

(a) Your organisation’s cyber security policies and processes are developed to be practical, usable and appropriate for your ship's operational use, context, dependencies and technologies.

(b) Where your cyber security policies and processes place requirements on people, e.g. changes in behaviour or activity, this is practical and they can do what is expected.

(c) You review and improve policies and processes at suitably regular intervals to ensure they remain relevant to threats, the way people and systems work, adapt to lessons learned and remain appropriate and effective. This is in addition to reviews following a major cyber security incident.

(d) You document your overarching security governance and risk management approach, technical security practice and specific regulatory compliance.

(e) Cyber security is embedded throughout these policies and processes and key performance indicators are reported to your executive management.

(f) Your cyber security policies and processes are effectively and appropriately communicated across all levels of the organisation.

(g) All staff are aware of their responsibilities under your service protection policies and processes.

(h) Suitable action is taken to correct significant single or aggregated breaches of cyber security policies and processes.

(i) Your systems are designed with 'guard rails', so that they remain secure even when user security policies and processes are not always followed.

(j) All your cyber security policies and processes are enacted.

(k) You regularly evaluate the correct application and security effectiveness of your service protection policies.

(l) Your cyber security policies and processes are integrated with other organisational policies and processes, including HR assessments of individuals' trustworthiness.

1.2 Controls

1.2.1 *See Ch 16, 1.2 Controls*

1.3 Required evidence and testing

1.3.1

(a) Provide evidence how the organisation’s cyber security policies define the way in which the organisation manages its cyber security objectives.

(b) Provide evidence how the organisation’s cyber security policies define and manage all activities relating to cyber security (including assigning responsibilities for cyber security to specific roles).

(c) Provide evidence how you verified the assignment of cyber security responsibilities to specific roles was

  (i) current;

  (ii) active;

  (iii) and known to all relevant parties.

(d) Provide evidence how the organisation’s cyber security policies take into account deviations and exceptions to the organisation’s operational and cyber threat environment.

(e) Provide evidence how the organisation’s cyber security policies take into account

  (i) the organisation’s business strategy and operational environment;

  (ii) legal, regulatory and contractual obligations;

(iii) and current and projected risk-based cyber security threat models.

(f) Provide evidence how you verified the organisation's cyber security policies

(i) are established and published;
(ii) have senior management approval;
(iii) and are disseminated to all individuals (including contractors and relevant external service providers).

(g) Provide evidence how the organisation's cyber security policies

(i) make reference to topic specific cyber security requirements and procedures (e.g. authentication and authorisation, asset management, etc.).

(h) Provide evidence how these topic specific cyber security requirements and procedures support the organisation's cyber security policies.

(i) Provide evidence how these topic specific cyber security requirements and procedures are disseminated to all individuals (including contractors and relevant external service providers).

(j) Provide evidence how the dissemination of these topic specific cyber security requirements and procedures

(i) are readily accessible and understandable;
(ii) and form part of an organisational security awareness programme.

(k) Provide evidence how you verified the dissemination of these topic specific cyber security requirements and procedures

(i) are readily accessible and understandable;
(ii) and form part of an organisational security awareness programme.

(l) Provide evidence how the organisation deals with a single or aggregated breaches of cyber security policies and processes.

(m) Provide evidence how the organisation ensures technical security controls reduce the consequences of a single or aggregated breaches of cyber security policies and processes.

(n) Provide evidence how you verified the organisation's technical security controls reduce the consequences of a single or aggregated breaches of cyber security policies and processes.

(o) Provide evidence how the organisation's incident response testing includes breaches of cyber security policies and processes.

(p) Provide evidence how you verified testing of the organisation's incident response plan includes breaches of cyber security policies and processes.

(q) Provide evidence how all organisational policies and procedures make reference to the organisation's cyber security policies and procedures.

1.3.2

(a) Provide evidence how the organisation ensures the cyber security policies continue to be appropriate, effective and relevant.

(b) Provide evidence how the organisation conducted reviews of the cyber security policies.

(c) Provide evidence how you verified that reviews of the cyber security policies are undertaken

(i) at regular intervals;
(ii) after significant changes to the organisation's business strategy and operational environment;
(iii) after a cyber security incident;
(iv) and when the organisation's cyber security threat models are updated.

(d) Provide evidence how you verified senior management approval was required for any modification to the cyber security policies.

Contents

Contents

Physical and Environmental Security Domain (Established)

Section 1
Outcomes

1.1 Outcomes: physicial security procedures

1.1.1

(a) All secure areas/zones are protected by access controls that limit access on a role-based control.
(b) Logs and records are maintained of access to all secure areas and areas of control, server or communications equipment.

1.2 Outcomes: physicial security

1.2.1 The objective of physical and environment security is to prevent unauthorised physical access to the organisations' information and information processing facilities, and thereby reduce to an acceptable level the likelihood of an organisation's

(a) assets being lost, damaged, stolen and/or compromised;
(b) and operations being interrupted and/or compromised.

Section 2
Physical: security procedures

2.1 Controls

2.1.1 Security policies and operational procedures for restricting physical access to facilities and/or areas that store, process and/or transmit critical information must be documented, in use and known to all affected parties. (Maps to ISO 27002: Section 11.)

2.2 Required evidence and testing

2.2.1

(a) Identify the document reviewed to verify that security policies and operational procedures for restricting physical access to facilities and/or areas that store, process and/or transmit critical information are documented.
(b) Identify the responsible personnel interviewed who confirm that documented security policies and operational procedures for restricting physical access to facilities and/or areas that store, process and/or transmit critical information are
    (i) in use;
    (ii) and known to all affected parties.

Section 3
Physical security perimeters

3.1 Controls

3.1.1 Facilities and/or areas that store, process and/or transmit critical information must have a defined security perimeter, and be protected by defined physical security controls. (Maps to ISO 27002: Section 11.1.1.)

3.2 Required evidence and testing

3.2.1

(a) Provide evidence for the physical security perimeter and controls used.

(b) Provide evidence how you verified that the physical security perimeter and controls were in place.

(c) Provide evidence how the security perimeter and physical security controls restrict physical access to facilities and/or areas that store, process and/or transmit critical information.

Section 4
Physical entry controls

4.1 Controls

4.1.1 Individual access to facilities and/or areas that store, process and/or transmit critical information must be protected by appropriate entry controls to ensure only authorised personnel are allowed access. (Maps to ISO 27002: Section 11.1.2.)

4.2 Required evidence and testing

4.2.1

(a) Provide evidence how you verified that all physical authentication methods were returned or deactivated.

(b) Provide evidence how the documented authentication policies and procedures verified that

  (i) authentication mechanisms are assigned to an individual account and not shared among multiple accounts;

  (ii) and physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access.

(c) Identify the individual who confirmed that authentication mechanisms are assigned to an account and not shared among multiple accounts.

(d) Provide evidence how the system configuration settings and/or physical controls verified that implemented controls ensure only the intended account can use that mechanism to gain access.

(e) Provide evidence how you verified that access:

  (i) to facilities and/or areas that store, process and/or transmit critical information is authorised;

  (ii) is required for the individual's job function.

(f) Provide evidence how you verified that recently terminated employees do not have physical access to facilities and/or areas that store, process and/or transmit critical information.

(g) Provide evidence how you verified that procedures are defined for identifying and distinguishing between onsite personnel and visitors.

(h) Provide evidence how you verified

  (i) the use of visitor badges;

  (ii) that visitors are easily distinguishable from onsite personnel;

  (iii) and that visitor badges expire.

(i) Provide evidence how you verified that a log is used to record physical access to facilities and/or areas that store, process and/or transmit critical information.

Section 5
Securing offices, rooms and facilities

5.1 Controls

5.1.1 Physical access to publicly accessible network jacks, wireless access points, gateways, handheld devices, networking/communications hardware and telecommunication lines must be restricted. (Maps to ISO 27002: Section 11.1.3.)

5.2 Required evidence and testing

5.2.1

(a) Provide evidence how you verified that appropriate controls are in place to restrict access to publicly accessible network jacks.

(b) Provide evidence how you verified that physical access to wireless access points, gateways, handheld devices, networking/communications hardware and telecommunication lines is appropriately restricted.

(c) Provide evidence how you verified that a log is used to record physical access to networking/communications hardware and telecommunication lines.

Contents

Contents

Physical and Environmental Security Domain (Enhanced)

Section 1
Outcomes

1.1 Outcomes: physicial security procedures

1.1.1 *See Ch 20, 1.1 Outcomes: physicial security procedures*

1.2 Outcomes: physicial security

1.2.1 *See Ch 20, 1.2 Outcomes: physicial security*

Section 2
Physical security procedures

2.1 Controls

2.1.1 *See Ch 20, 2.1 Controls*

2.2 Required evidence and testing

2.2.1 *See Ch 20, 2.2 Required evidence and testing*

Section 3
Physical security perimeters

3.1 Controls

3.1.1 *See Ch 20, 3.1 Controls*

3.2 Required evidence and testing

3.2.1 *See Ch 20, 3.2 Required evidence and testing*

Section 4
Physical entry controls

4.1 Controls

4.1.1 *See Ch 20, 4.1 Controls*

4.2 Required evidence and testing

4.2.1 *See Ch 20, 4.2 Required evidence and testing*

■ *Section 5*
Securing offices, rooms and facilities

5.1 Controls

5.1.1 *See Ch 20, 5.1 Controls*

5.2 Required evidence and testing

5.2.1 *See Ch 20, 5.2 Required evidence and testing*

Contents

Contents

Physical and Environmental Security Domain (Accomplished)

Section 1
Outcomes

1.1 Outcomes: physicial security procedures

1.1.1

(a) All secure areas/zones are protected by access controls that limit access on a role-based control.
(b) Logs and records are maintained of access to all secure areas and areas of control, server or communications equipment.
(c) All access to the ship is controlled through physical controls (CCTV and/or badge readers) with logs maintained in a secure manner.
(d) All visitors are accompanied in all secure areas at all times.

1.2 Outcomes: physicial security

1.2.1 *See Ch 20, 1.2 Outcomes: physicial security*

Section 2
Physical security procedures

2.1 Controls

2.1.1 *See Ch 20, 2.1 Controls*

2.2 Required evidence and testing

2.2.1 *See Ch 20, 2.2 Required evidence and testing*

Section 3
Physical security perimeters

3.1 Controls

3.1.1 *See Ch 20, 3.1 Controls*

3.2 Required evidence and testing

3.2.1 *See Ch 20, 3.2 Required evidence and testing*

Section 4
Physical entry controls

4.1 Controls

4.1.1 *See Ch 20, 4.1 Controls*

4.2 Required evidence and testing

4.2.1

(a) Provide evidence how you verified that all physical authentication methods were returned or deactivated.

(b) Provide evidence how the documented authentication policies and procedures verified that

  (i) authentication mechanisms are assigned to an individual account and not shared among multiple accounts;

  (ii) and physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access.

(c) Identify the individual who confirmed that authentication mechanisms are assigned to an account and not shared among multiple accounts.

(d) Provide evidence how the system configuration settings and/or physical controls verified that implemented controls ensure only the intended account can use that mechanism to gain access.

(e) Provide evidence how you verified that access:

  (i) to facilities and/or areas that store, process and/or transmit critical information is authorised;

  (ii) is required for the individual's job function.

(f) Provide evidence how you verified that recently terminated employees do not have physical access to facilities and/or areas that store, process and/or transmit critical information.

(g) Provide evidence how you observed video cameras and/or access control mechanisms to be in place to monitor the entry/exit points to facilities and/or areas that store, process and/or transmit critical information.

(h) Provide evidence how video cameras and/or access control mechanisms are protected from tampering or disabling.

(i) Provide evidence how you verified the video cameras and/or access control mechanisms are active and recording access to facilities and/or areas that store, process and/or transmit critical information.

(j) Provide evidence how you verified that procedures (i.e. the identification process) are defined for identifying and distinguishing between onsite personnel and visitors.

(k) Provide evidence how the identification process

  (i) distinguishes between onsite personnel and visitors;

  (ii) considers changes to access requirements;

  (iii) revokes physical access to terminated onsite personnel;

  (iv) and manages expired visitor identification.

(l) Provide evidence how the identification process ensures that visitors must be authorised before they are granted access to, and escorted at all times within, facilities and/or areas that store, process and/or transmit critical information.

(m) Identify the individual who confirmed that visitors must be authorised before they are granted access to, and escorted at all times within, facilities and/or areas that store, process and/or transmit critical information.

(n) Provide evidence how you verified that access to the identification process is limited to authorised personnel.

(o) Provide evidence how the use of visitor badges verified that a physical token badge does not permit unescorted access to facilities and/or areas that store, process and/or transmit critical information.

(p) Provide evidence how you verified

  (i) the use of visitor badges;

  (ii) that visitors are easily distinguishable from onsite personnel;

  (iii) and that visitor badges expire.

(q) Provide evidence how you verified that visitors were asked to surrender their visitor badge upon departure or expiration.

(r) Provide evidence how you verified that a log is used to record physical access to facilities and/or areas that store, process and/or transmit critical information.

(s) Provide evidence how you verified that the log details the

(i) visitor's name;
(ii) firm represented;
(iii) and onsite personnel authorising physical access.

Section 5
Securing offices, rooms and facilities

5.1 Controls

5.1.1 *See Ch 20, 5.1 Controls*

5.2 Required evidence and testing

5.2.1 *See Ch 20, 5.2 Required evidence and testing*

Section 6
Securing delivery and loading areas

6.1 Controls

6.1.1 Delivery and loading areas must be isolated from facilities that store, process and/or transmit critical data. (Maps to ISO 27002: 11.1.6.)

6.2 Required evidence and testing

6.2.1

(a) Provide evidence how you verified that access to delivery and loading areas was restricted to authorised individuals.
(b) Provide evidence how the delivery and loading areas were isolated from those facilities that store, process and/or transmit critical data.
(c) Provide evidence
    (i) how delivered items were protected from tampering;
    (ii) and if tampering was discovered how it was reported.

Section 7
Securing cables

7.1 Controls

7.1.1 Cables used to transmit data or provide supporting services (e.g. power) must be protected from interception, interference and/or damage. (Maps to ISO 27002: 11.2.3.)

7.2 Required evidence and testing

7.2.1 Provide evidence how cables used to transmit data or provide supporting services (e.g. power) were protected from interception, interference and/or damage.

Contents

Contents

Physical and Environmental Security Domain (Optimised)

Section

Section 1
Outcomes

1.1 Outcomes: physicial security procedures

1.1.1 *See Ch 22, 1.1 Outcomes: physicial security procedures*

1.2 Outcomes: physicial security

1.2.1 *See Ch 20, 1.2 Outcomes: physicial security*

Section 2
Physical security procedures

2.1 Controls

2.1.1 *See Ch 20, 2.1 Controls*

2.2 Required evidence and testing

2.2.1 *See Ch 20, 2.2 Required evidence and testing*

Section 3
Physical security perimeters

3.1 Controls

3.1.1 *See Ch 20, 3.1 Controls*

3.2 Required evidence and testing

3.2.1 *See Ch 20, 3.2 Required evidence and testing*

Physical and Environmental Security Domain (Optimised)

Section 4
Physical entry controls

4.1 Controls

4.1.1 *See Ch 20, 4.1 Controls*

4.2 Required evidence and testing

4.2.1 *See Ch 22, 4.2 Required evidence and testing*

Section 5
Securing offices, rooms and facilities

5.1 Controls

5.1.1 *See Ch 20, 5.1 Controls*

5.2 Required evidence and testing

5.2.1 *See Ch 20, 5.2 Required evidence and testing*

Section 6
Securing delivery and loading areas

6.1 Controls

6.1.1 *See Ch 22, 6.1 Controls*

6.2 Required evidence and testing

6.2.1 *See Ch 22, 6.2 Required evidence and testing*

Section 7
Securing cables

7.1 Controls

7.1.1 *See Ch 22, 7.1 Controls*

7.2 Required evidence and testing

7.2.1 *See Ch 22, 7.2 Required evidence and testing*

Contents

Contents

Section 1
Awareness, education and training

1.1 Outcomes

1.1.1

(a) Your executive management clearly and effectively communicates the organisation's cyber security priorities and objectives to all staff.

(b) Your organisation displays positive cyber security attitudes, behaviours and expectations.

1.2 Controls

1.2.1 Employees of the organisation (including contractors) must undergo regular and relevant (as defined by their organisational roles and responsibilities) security awareness education and training. (Maps to ISO 27002: Section 7.2.2.)

1.2.2 Employees (including contractors) using mobile devices must be made aware of the additional risks associated with use of such devices. (Maps to ISO 27002: Section 6.2.)

1.2.3 Individuals with specific security breach response responsibilities must be given appropriate security awareness education and training. (Maps to ISO 27002: Section 12.2.)

1.2.4 Employees (including contractors) who manage supplier relationships must be given appropriate security awareness education and training. (Maps to ISO 27002: Section 15.)

1.3 Required evidence and testing

1.3.1

(a) Provide evidence how you verified the management’s commitment to information security.

(b) Provide evidence how policies and procedures verified that employees (including contractors) undergo security awareness education and training.

(c) Provide evidence how you verified that the security awareness education and training provided by the organisation to employees (including contractors) was relevant to their organisational roles and responsibilities.

(d) Provide evidence how the security awareness programme provides awareness to all employees (including contractors) about

  (i) individual accountability and responsibility for protecting the organisation’s data, in particular the security of data and facilities and/or areas that store, process and transmit critical/sensitive data;

  (ii) basic information security procedures (as defined by their roles and responsibilities);

  (iii) and resources for additional information and guidance.

(e) Provide evidence how you verified that employees (including contractors)

  (i) have completed the security awareness training;

  (ii) and are aware of the importance of information security.

1.3.2

(a) Provide evidence how addition information security awareness, education and training was provided to employees (including contractors) using mobile devices for work related activities.

(b) Provide evidence how such training was assessed for relevance to the employees (including contractors) normal mobile device and teleworking activities.

1.3.3

(a) Provide evidence how addition information security awareness, education and training was provided to individuals with specific security breach response responsibilities.

(b) Provide evidence how such training was assessed for relevance for those individuals with specific security breach response responsibilities.

(c) Provide evidence how the training and education programme

  (i) incorporated lessons learnt from previous security incidents;

  (ii) and included a means of assessing the attendees' level of understanding of information security at the course completion.

1.3.4

(a) Provide evidence how security awareness education and training is provided to those employees (including contractors) involved in acquisitions.

(b) Provide evidence how security awareness education and training is provided to those employees (including contractors) interacting with suppliers.

(c) Provide evidence how such security awareness education and training includes

  (i) supplier engagement procedures;

  (ii) and how the engagement is dependent on the level of supplier access to facilities and/or areas that store, process and/or transmit critical/sensitive data.

Contents

Contents

Section 1
Awareness, education and training

1.1 Outcomes

1.1.1

(a) Your executive management clearly and effectively communicates the organisation's cyber security priorities and objectives to all staff. Your organisation displays positive cyber security attitudes, behaviours and expectations.

(b) People in your organisation are positively recognised for bringing cyber security incidents and issues to light, not reprimanded or ignored.

(c) Individuals at all levels in your organisation routinely report concerns or issues about cyber security and are recognised for their contribution to keeping the organisation secure.

1.2 Controls

1.2.1 *See Ch 24, 1.2 Controls 1.2.1*

1.2.2 The organisation’s senior management must provide direction and support for cyber security. (Maps to ISO 27002: Section 5).

1.2.3 *See Ch 24, 1.2 Controls 1.2.2*

1.2.4 *See Ch 24, 1.2 Controls 1.2.3*

1.2.5 *See Ch 24, 1.2 Controls 1.2.4*

1.3 Required evidence and testing

1.3.1

(a) Provide evidence how you verified the management’s commitment to information security.

(b) Provide evidence how policies and procedures verified that employees (including contractors) undergo security awareness education and training.

(c) Provide evidence how you verified that the security awareness education and training provided by the organisation to employees (including contractors) was relevant to their organisational roles and responsibilities.

(d) Provide evidence how the security awareness programme provides awareness to all employees (including contractors) about

  (i) individual accountability and responsibility for protecting the organisation’s data, in particular the security of data and facilities and/or areas that store, process and transmit critical/sensitive data;

  (ii) basic information security procedures (as defined by their roles and responsibilities);

  (iii) and resources for additional information and guidance.

(e) Provide evidence how you verified that employees (including contractors)

  (i) have completed the security awareness training;

  (ii) and are aware of the importance of information security.

1.3.2

(a) Provide evidence how cyber security priorities are embedded within the organisation’s business-as-normal activities.

(b) Provide evidence how cyber security incidents are

  (i) reported;

  (ii) communicated to senior management;

  (iii) and how senior management responds to those reports.

1.3.3

(a) Provide evidence how addition information security awareness, education and training was provided to employees (including contractors) using mobile devices for work related activities.

(b) Provide evidence how such training was assessed for relevance to the employees (including contractors) normal mobile device and teleworking activities.

1.3.4

(a) Provide evidence how addition information security awareness, education and training was provided to individuals with specific security breach response responsibilities.

(b) Provide evidence how such training was assessed for relevance for those individuals with specific security breach response responsibilities.

(c) Provide evidence how the training and education programme

  (i) incorporated lessons learnt from previous security incidents;

  (ii) and included a means of assessing the attendees' level of understanding of information security at the course completion.

1.3.5

(a) Provide evidence how security awareness education and training is provided to those employees (including contractors) involved in acquisitions.

(b) Provide evidence how security awareness education and training is provided to those employees (including contractors) interacting with suppliers.

(c) Provide evidence how such security awareness education and training includes

  (i) supplier engagement procedures;

  (ii) and how the engagement is dependent on the level of supplier access to facilities and/or areas that store, process and/or transmit critical/sensitive data.

Contents

Contents

Section 1
Awareness, education and training

1.1 Outcomes

1.1.1

(a) Your executive management clearly and effectively communicates the organisation's cyber security priorities and objectives to all staff. Your organisation displays positive cyber security attitudes, behaviours and expectations.

(b) People in your organisation are positively recognised for bringing cyber security incidents and issues to light, not reprimanded or ignored.

(c) Individuals at all levels in your organisation routinely report concerns or issues about cyber security and are recognised for their contribution to keeping the organisation secure.

(d) Your management is seen to be committed to and actively involved in cyber security.

(e) Your organisation communicates openly about cyber security, with any concern being taken seriously.

(f) People across your organisation participate in cyber security activities and improvements, building joint ownership and bringing knowledge of their area of expertise.

(g) All people in your organisation, from executives to the most junior roles, follow appropriate cyber security training paths.

1.2 Controls

1.2.1 *See Ch 24, 1.2 Controls 1.2.1*

1.2.2 *See Ch 25, 1.2 Controls 1.2.2*

1.2.3 *See Ch 24, 1.2 Controls 1.2.2*

1.2.4 *See Ch 24, 1.2 Controls 1.2.3*

1.2.5 *See Ch 24, 1.2 Controls 1.2.4*

1.3 Required evidence and testing

1.3.1

(a) Provide evidence how you verified the management’s commitment to information security.

(b) Provide evidence how policies and procedures verified that employees (including contractors) undergo security awareness education and training.

(c) Provide evidence how you verified that the security awareness education and training provided by the organisation to employees (including contractors) was relevant to their organisational roles and responsibilities.

(d) Provide evidence how the security awareness programme provides awareness to all employees (including contractors) about

  (i) individual accountability and responsibility for protecting the organisation’s data, in particular the security of data and facilities and/or areas that store, process and transmit critical/sensitive data;

  (ii) basic information security procedures (as defined by their roles and responsibilities);

  (iii) and resources for additional information and guidance.

(e) Provide evidence how you verified that the documented security awareness training programme

  (i) provides multiple methods of communicating awareness and educating employees (including contractors);

  (ii) ensures that employees (including contractors) attend security awareness training when hired and annually thereafter;

  (iii) and requires employees (including contractors) to annually acknowledge (either in writing or electronically) that they have read and understand the information security policy.

(f) Provide evidence how you verified that employees (including contractors)

  (i) have completed the security awareness training;

  (ii) and are aware of the importance of information security.

(g) Provide evidence how the training and education programme

(i) incorporated lessons learnt from previous security incidents;

(ii) and included a means of assessing the attendees' level of understanding of information security at the course completion.

1.3.2

(a) Provide evidence how cyber security priorities are embedded within the organisation's business-as-normal activities.

(b) Provide evidence how cyber security incidents are

(i) reported;

(ii) communicated to senior management;

(iii) and how senior management responds to those reports.

1.3.3

(a) Provide evidence how addition information security awareness, education and training was provided to employees (including contractors) using mobile devices for work related activities.

(b) Provide evidence how such training was assessed for relevance to the employees (including contractors) normal mobile device and teleworking activities.

1.3.4

(a) Provide evidence how addition information security awareness, education and training was provided to individuals with specific security breach response responsibilities.

(b) Provide evidence how such training was assessed for relevance for those individuals with specific security breach response responsibilities.

(c) Provide evidence how the training and education programme

(i) incorporated lessons learnt from previous security incidents;

(ii) and included a means of assessing the attendees' level of understanding of information security at the course completion.

1.3.5

(a) Provide evidence how security awareness education and training is provided to those employees (including contractors) involved in acquisitions.

(b) Provide evidence how security awareness education and training is provided to those employees (including contractors) interacting with suppliers.

(c) Provide evidence how such security awareness education and training includes

(i) supplier engagement procedures;

(ii) and how the engagement is dependent on the level of supplier access to facilities and/or areas that store, process and/or transmit critical/sensitive data.

Contents

Contents

Section 1
Awareness education and training

1.1 Outcomes

1.1.1

(a) Your executive management clearly and effectively communicates the organisation's cyber security priorities and objectives to all staff. Your organisation displays positive cyber security attitudes, behaviours and expectations.

(b) People in your organisation are positively recognised for bringing cyber security incidents and issues to light, not reprimanded or ignored.

(c) Individuals at all levels in your organisation routinely report concerns or issues about cyber security and are recognised for their contribution to keeping the organisation secure.

(d) Your management is seen to be committed to and actively involved in cyber security.

(e) Your organisation communicates openly about cyber security, with any concern being taken seriously.

(f) People across your organisation participate in cyber security activities and improvements, building joint ownership and bringing knowledge of their area of expertise.

(g) All people in your organisation, from executives to the most junior roles, follow appropriate cyber security training paths.

(h) You track individuals' cyber security training and ensure that refresh update training is completed at suitable intervals.

(i) You routinely engage all people across your organisation on cyber security and evaluate that your cyber security training and awareness activities reach the widest audience effectively.

(j) Cyber security information and good practice guidance is easily and widely available. You know this is referenced and employed by people in your organisation.

1.2 Controls

1.2.1 *See Ch 24, 1.2 Controls 1.2.1*

1.2.2 *See Ch 25, 1.2 Controls 1.2.2*

1.2.3 *See Ch 24, 1.2 Controls 1.2.2*

1.2.4 *See Ch 24, 1.2 Controls 1.2.3*

1.2.5 *See Ch 24, 1.2 Controls 1.2.4*

1.3 Required evidence and testing

1.3.1

(a) Provide evidence how you verified the management's commitment to information security.

(b) Provide evidence how policies and procedures verified that employees (including contractors) undergo security awareness education and training.

(c) Provide evidence how you verified that the security awareness education and training provided by the organisation to employees (including contractors) was relevant to their organisational roles and responsibilities.

(d) Provide evidence how the security awareness programme provides awareness to all employees (including contractors) about

  (i) individual accountability and responsibility for protecting the organisation's data, in particular the security of data and facilities and/or areas that store, process and transmit critical/sensitive data;

  (ii) basic information security procedures (as defined by their roles and responsibilities);

  (iii) and resources for additional information and guidance.

(e) Provide evidence how you verified that the documented security awareness training programme

  (i) provides multiple methods of communicating awareness and educating employees (including contractors);

  (ii) ensures that employees (including contractors) attend security awareness training when hired and annually thereafter;

(iii) and requires employees (including contractors) to annually acknowledge (either in writing or electronically) that they have read and understand the information security policy.

(f) Provide evidence how you verified that employees (including contractors)

(i) have completed the security awareness training;
(ii) and are aware of the importance of information security.

(g) Provide evidence how additional training and education was provided to employees (including contractors) who move into new roles, with substantially different information security responsibilities.

(h) Provide evidence how the training and education programme

(i) incorporated lessons learnt from previous security incidents;
(ii) and included a means of assessing the attendees' level of understanding of information security at the course completion.

1.3.2

(a) Provide evidence how cyber security priorities are embedded within the organisation's business-as-normal activities.

(b) Provide evidence how cyber security incidents are

(i) reported;
(ii) communicated to senior management;
(iii) and how senior management responds to those reports.

(c) Provide evidence how the organisation engages with employees (including contractors) to ensure cyber security priorities are seen as part of the organisation's normal business activity.

(d) Provide evidence how the organisation provides additional information on recent cyber security alerts reported by either

(i) news media;
(ii) governmental guidance;
(iii) and/or vendor communications.

(e) Provide evidence how the organisation empowers their employees (including contractors) to participate in cyber security activities and improvements.

(f) Provide evidence how the organisation ensures that cyber security information and good practice guidance is referenced and employed by their employees (including contractors).

1.3.3

(a) Provide evidence how addition information security awareness, education and training was provided to employees (including contractors) using mobile devices for work related activities.

(b) Provide evidence how such training was assessed for relevance to the employees (including contractors) normal mobile device and teleworking activities.

1.3.4

(a) Provide evidence how addition information security awareness, education and training was provided to individuals with specific security breach response responsibilities.

(b) Provide evidence how such training was assessed for relevance for those individuals with specific security breach response responsibilities.

(c) Provide evidence how the training and education programme

(i) incorporated lessons learnt from previous security incidents;
(ii) and included a means of assessing the attendees' level of understanding of information security at the course completion.

1.3.5

(a) Provide evidence how security awareness education and training is provided to those employees (including contractors) involved in acquisitions.

(b) Provide evidence how security awareness education and training is provided to those employees (including contractors) interacting with suppliers.

(c) Provide evidence how such security awareness education and training includes

(i) supplier engagement procedures;

(ii) and how the engagement is dependent on the level of supplier access to facilities and/or areas that store, process and/or transmit critical/sensitive data.

Contents

Contents

Section 1
Outcomes

1.1 Outcomes: coverage and depth of detection capability (endpoint)

1.1.1

(a) You are able to monitor your network boundaries (public/private, OT/IT, secure/non-secure) effectively.
(b) You have coverage and depth detection which includes internal host-based monitoring.
(c) Your process for bringing new systems on line includes considerations for access to monitoring data sources.

1.2 Outcomes: business continuity

1.2.1

(a) You have business continuity and disaster recovery plans that have been tested for practicality, effectiveness and completeness.

Section 2
Coverage and depth of detection capability (endpoint)

2.1 Controls

2.1.1 The organisation must ensure that monitoring is undertaken recording

(a) all network/service/user activities;
(b) exceptions;
(c) faults and security events.

2.1.2 The organisation must ensure that all monitoring logs

(a) are stored securely and regularly reviewed;
(b) have restricted access with read-only access controls;
(c) and that all access is monitored and logged.

2.1.3 Mappings:

- ISO 27002: 12.4
- IEC 62443-3
    - SR 2.8 – Auditable events
    - SR 2.8 RE 1 – Centrally managed, system-wide audit trail
    - SR 2.9 – Audit storage capacity
    - SR 2.9 RE 1 – Warn when audit record storage capacity threshold reached
    - SR 2.12 – Non-repudiation
    - SR 2.12 RE 1 – Non-repudiation for all users
    - SR 5.1 – Network segmentation
    - SR 5.1 RE 1 – Physical network segmentation
    - SR 5.1 RE 2 – Independence from non-control system networks

- SR 5.1 RE 3 – Logical and physical isolation of critical networks

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how the organisation monitors network boundaries.
(b) Provide evidence how you verified all endpoints were monitored effectively.
(c) Provide evidence how you verified the monitored network boundaries aligned to network diagrams.
(d) Provide evidence how the organisation uses host-based monitoring to monitor activities within systems on internal networks.
(e) Provide evidence how you verified that host-based monitoring is used effectively.
(f) Provide evidence how you verified that monitored systems on internal networks aligned to network diagrams.
(g) Provide evidence how you verified monitoring procedures are updated to include alterations to network boundaries.

Section 3
Business continuity

3.1 Controls

3.1.1 The organisation must determine its requirements for the continuation and management of data/software/system cyber security during adverse conditions.

3.1.2 Mappings:

- ISO 27002: 17
- IEC 62443-3
    - SR 7.4 – Control system recovery and reconstitution

3.2 Required evidence and testing

3.2.1

(a) Provide evidence how the organisation has verified embedded cyber security continuity within business continuity and/or disaster recovery.
(b) Provide evidence how the organisation determined its cyber security continuity requirements.

Contents

Contents

Section 1
Outcomes

1.1 Outcomes: coverage and depth of detection capability (endpoint)

1.1.1

(a) You are able to monitor your network boundaries (public/private, OT/IT, secure/non-secure) effectively.
(b) You have coverage and depth detection which includes internal host-based monitoring.
(c) Your process for bringing new systems on line includes considerations for access to monitoring data sources.
(d) Your monitoring data provides sufficient detail to reliably detect security incidents that could affect your operational services.

1.2 Outcomes: business continuity

1.2.1

(a) You have business continuity and disaster recovery plans that have been tested for practicality, effectiveness and completeness.
(b) Appropriate use is made of different test methods, e.g. manual failover, table-top exercises or red-teaming.

Section 2
Coverage and depth of detection capability (endpoint)

2.1 Controls

2.1.1 *See Ch 28, 2.1 Controls*

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how the organisation monitors network boundaries.
(b) Provide evidence how you verified all endpoints were monitored effectively.
(c) Provide evidence how you verified the monitored network boundaries aligned to network diagrams.
(d) Provide evidence how the organisation uses host-based monitoring to monitor activities within systems on internal networks.
(e) Provide evidence how you verified that host-based monitoring is used effectively.
(f) Provide evidence how you verified that monitored systems on internal networks aligned to network diagrams.
(g) Provide evidence how you verified monitoring procedures are updated to include alterations to network boundaries.
(h) Provide evidence how you verified that monitoring data provided sufficient detail to detect security incidents.

Section 3
Business continuity

3.1 Controls

3.1.1 *See Ch 28, 3.1 Controls*

3.2 Required evidence and testing

3.2.1

(a) Provide evidence how you verified the organisation has embedded cyber security continuity within business continuity and/or disaster recovery.

(b) Provide evidence how the organisation determined its cyber security continuity requirements.

(c) Provide evidence how the organisation ensures continuity for cyber security will be in place during an adverse situation.

(d) Provide evidence how you verified the cyber security continuity requirements are in line with the organisation's threat models.

(e) Provide evidence how you verified the cyber security continuity requirements are updated

  (i) after being tested;

  (ii) in line with threat intelligence received;

  (iii) and/or when a new cyber security vulnerability is identified.

(f) Provide evidence how you verified testing of the cyber security continuity requirements is undertaken in line with recognised industry best practice.

Contents

Contents

Section 1 Outcomes

1.1 Outcomes: coverage and depth of detection capability (endpoint and network)

1.1.1

(a) You are able to monitor your network boundaries (public/private, OT/IT, secure/non-secure) effectively.
(b) You have coverage and depth detection which includes internal host-based monitoring.
(c) Your process for bringing new systems on line includes considerations for access to monitoring data sources.
(d) Your monitoring data provides sufficient detail to reliably detect security incidents that could affect your operational services.
(e) You are able to monitor user activity extensively in relation to your operational services.
(f) You can detect policy violations and have an agreed list of suspicious or undesirable behaviour.

1.2 Outcomes: analysis, investigation and discovery

1.2.1

(a) You are able to monitor and analyse traffic coming in and going out of your network.
(b) Your monitoring capability allows you to investigate suspicious traffic which can then be escalated or handed over to incident response as necessary.

1.3 Outcomes: incident management planning

1.3.1 The creation of incident management and response capabilities are driven by senior management as part of their understanding of risk management.

1.4 Outcomes response capability

1.4.1 Incident response follows documented procedures including evidence collection, use of communication channels, escalation, forensic tool use and chain of custody.

1.5 Outcomes: business continuity

1.5.1

(a) You have business continuity and disaster recovery plans that have been tested for practicality, effectiveness and completeness.
(b) Appropriate use is made of different test methods, e.g. manual failover, table-top exercises or red-teaming.
(c) You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.
(d) Your operational systems are segregated from other business and external systems by appropriate technical and physical means, e.g. separate network and system infrastructure with independent user administration.

1.6 Outcomes: data recovery

1.6.1 Suitable backups of all important data and information needed to recover critical systems are made, tested, documented and routinely reviewed.

Section 2
Coverage and depth of detection capability (endpoint and network)

2.1 Controls

2.1.1 *See Ch 28, 2.1 Controls*

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how the organisation monitors network boundaries.
(b) Provide evidence how you verified all endpoints were monitored effectively.
(c) Provide evidence how you verified the monitored network boundaries aligned to network diagrams.
(d) Provide evidence how the organisation uses host-based monitoring to monitor activities within systems on internal networks.
(e) Provide evidence how you verified that host-based monitoring is used effectively.
(f) Provide evidence how you verified that monitored systems on internal networks aligned to network diagrams.
(g) Provide evidence how you verified monitoring procedures are updated to include alterations to network boundaries.
(h) Provide evidence how you verified that monitoring data provided sufficient detail to detect security incidents.
(i) Provide evidence how the organisation monitors user activity.
(j) Provide evidence how you verified the organisation monitors user/service activity.
(k) Provide evidence how the organisation maintains a baseline (i.e. a minimum level of activity or starting point used for comparisons) of user/service activity.
(l) Provide evidence how the organisation uses this baseline user activity as part of their detection of suspicious/undesirable network policy violations.
(m) Provide evidence how the organisation regularly updates the baseline activity level.
(n) Provide evidence how the organisation maintains a record of suspicious/undesirable network activity for comparisons.

Section 3
Analysis, investigation and discovery

3.1 Controls

3.1.1 The organisation must ensure that all monitoring logs

(a) are stored securely and regularly reviewed;
(b) have restricted access with read-only access controls;
(c) and that all access is monitored and logged.

3.1.2 Mappings:

- ISO 27002: 12.4.2
- IEC 62443-3
    - SR 2.8 – Auditable events
    - SR 2.8 RE 1 – Centrally managed, system-wide audit trail
    - SR 2.11 – Timestamps
    - SR 2.11 RE 1 – Internal time synchronization
    - SR 2.11 RE 2 – Protection of time source integrity
    - SR 2.12 – Non-repudiation

- SR 2.12 RE 1 – Non-repudiation for all users
- SR 3.3 – Security functionality verification
- SR 3.3 RE 1 – Automated mechanisms for security functionality verification
- SR 3.3 RE 2 – Security functionality verification during normal operation
- SR 6.1 – Audit log accessibility
- SR 6.1 RE 1 – Programmatic access to audit logs
- SR 6.2 – Continuous monitoring

3.2 Required evidence and testing

3.2.1

(a) Provide evidence how the organisation's monitoring ties access to individuals and/or services.
(b) Provide evidence how you verified the organisation's monitoring ties access to individuals and/or services.
(c) Provide evidence how the organisation's monitoring is able reconstruct
    (i) all logical access requests (including requests to access audit logs and invalid access requests);
    (ii) all administrative privilege activities;
    (iii) initialising, stopping and pausing monitoring activities;
    (iv) and system level object creation/deletion.
(d) Provide evidence how you verified that organisation's monitoring is able reconstruct
    (i) all logical access requests (including requests to access audit logs and invalid access requests);
    (ii) all administrative privilege activities;
    (iii) initialising, stopping and pausing monitoring activities;
    (iv) and system level object creation/deletion.
(e) Provide evidence how the organisation's monitoring is able to reconstruct usage and/or changes to authentication and authorisation processes, specifically
    (i) privilege elevation;
    (ii) administrative privilege modification and/or deletion.
(f) Provide evidence how verified the organisation's monitoring is able to reconstruct usage and/or changes to authentication and authorisation processes, specifically
    (i) privilege elevation;
    (ii) and administrative privilege modification and/or deletion.
(g) Provide evidence how you verified the organisation's monitoring recorded for each network event the
    (i) user identification;
    (ii) date, time, type, source and target;
    (iii) and success and failure.
(h) Provide details of the time synchronisation services used by the organisation.
(i) Provide evidence how you verified that the organisation receives time settings from industry recognised sources.
(j) Provide evidence how you verified that
    (i) all systems have correct and consistent time;
    (ii) access to time data is restricted and logged;
    (iii) and access to time synchronisation services is restricted and logged.

■ *Section 4*
Incident management planning

4.1 Controls

4.1.1 The organisation must ensure that management responsibilities and procedures provide an immediate and successful response to security incidents. (Maps to ISO 27002: 16.1.1.)

4.2 Required evidence and testing

4.2.1

(a) Provide evidence how your organisation's incident management methodology

(i) is a product of senior management's risk management process;
(ii) ensures those responsible for response are competent;
(iii) and a clear chain of communication exists to facilitate effective decision making and contact to relevant parties.

(b) Provide evidence how you verified the organisation's incident management methodology ensures designated individuals

(i) are available to immediately respond to cyber security incidents;
(ii) and are periodically trained in the latest cyber security incident investigation techniques.

(c) Provide evidence how the organisation's incident management methodology takes into account the organisation's

(i) cyber security threat models;
(ii) and cyber security risk management strategy.

(d) Provide evidence how you verified that the organisation's incident management methodology takes into account the organisation's

(i) cyber security threat models;
(ii) and cyber security risk management strategy.

(e) Provide evidence how you verified the organisation's incident management methodology has procedures for monitoring alerts from system components with security capabilities.

■ *Section 5* Response capability

5.1 Controls

5.1.1 The organisation must ensure that any incident response actions follow documented incident response policies and procedures. (Maps to ISO 27002: 16.1.5.)

5.2 Required evidence and testing

5.2.1 Provide evidence how the organisation's incident response capability and procedures are based on industry-accepted practice (e.g. NIST SP800-800-61, etc.).

■ *Section 6* Business continuity

6.1 Controls

6.1.1 *See Ch 28, 3.1 Controls*

6.2 Required evidence and testing

6.2.1 *See Ch 29, 3.2 Required evidence and testing*

Section 7
Data recovery

7.1 Controls

7.1.1 The organisation must ensure the business continuity plans defines procedures for creating and testing data backups and software/system images.

7.1.2 Mappings:

- ISO 27002: 12.3
- IEC 62443-3
    - SR 7.3 – Control system backup
    - SR 7.3 RE 1 – Backup verification
    - SR 7.3 RE 2 – Backup automation
    - SR 7.4 – Control system recovery and reconstitution

7.2 Required evidence and testing

7.2.1

(a) Describe how the organisation's business continuity plans makes provision for data and software recovery.
(b) Describe how the organisation's business continuity plans details the recovery procedures.
(c) Describe how you verified the recovery procedures are based on the organisation's
    (i) business requirements;
    (ii) cyber security threat models;
    (iii) and a risk assessment of the data/software/system availability to the organisation's well-being.
(d) Describe how you verified the appropriateness of organisation's recovery procedures.
(e) Describe how you verified the recovery procedures were tested.
(f) Describe how you verified the recovery time was in line with the organisation's business continuity strategy.
(g) Describe how you verified the organisation's documented records of the data backups and software/system images were current and accurate.
(h) Describe how the organisation manages and controls the data/software/system replication process.

Contents

Contents

Section 1 Outcomes

1.1 Outcomes: coverage and depth of detection capability (endpoint, network and behaviour)

1.1.1

(a) You are able to monitor your network boundaries (public/private, OT/IT, secure/non-secure) effectively.
(b) You have coverage and depth detection which includes internal host-based monitoring.
(c) Your process for bringing new systems on line includes considerations for access to monitoring data sources.
(d) Your monitoring data provides sufficient detail to reliably detect security incidents that could affect your operational services.
(e) You are able to monitor user activity extensively in relation to your operational services.
(f) You can detect policy violations and have an agreed list of suspicious or undesirable behaviour.
(g) You have risk-assessed the impact of a network compromise to your operational services.
(h) You have aligned the detect and respond procedures to the impact of a network compromise.
(i) You have aligned detect and respond procedures with the organisation's threat models?

1.2 Outcomes: analysis, investigation and discovery

1.2.1

(a) You are able to monitor and analyse traffic coming in and going out of your network.
(b) Your monitoring capability allows you to investigate suspicious traffic which can then be escalated or handed over to incident response as necessary.
(c) Your monitoring capability is configured to generate alerts in real-time for analysts to investigate potential incidents.
(d) Your monitoring capability runs 24/7 to catch incidents as soon as possible.

1.3 Outcomes: management of detection capability

1.3.1

(a) You monitor all network/service/user activities.
(b) All monitoring logs are stored securely and regularly reviewed.

1.4 Outcomes: incident management planning

1.4.1

(a) The creation of incident management and response capabilities are driven by senior management as part of their understanding of risk management.
(b) Qualified and competent personnel are brought in to handle and support incident management - inhouse or third party.
(c) Reporting procedures are present and relevant in order to contact applicable authorities, senior management and stakeholders should the need arise.
(d) The communication procedure allows quick response and effective decision - making.

1.5 Outcomes: response capability

1.5.1

(a) Incident response follows documented procedures including evidence collection, use of communication channels, escalation, forensic tool use and chain of custody.
(b) Incident response works closely with detection and analysis to stop incidents earlier in the response lifecycle.
(c) Incident response uses appropriate tools and technologies to effectively respond and mitigate system damage, data loss and downtime.

1.6 Outcomes: testing and exercising

1.6.1

(a) Incident response capabilities should be tested periodically to evaluate its effectiveness.
(b) Incident response exercises should be performed to simulate different situations that may be encountered during an incident.
(c) As a result of testing, procedures should be modified and updated to ensure effectiveness.
(d) Testing should assure that the measures taken for incident response are communicated to relevant personnel with the organisation.

1.7 Outcomes: business continuity

1.7.1

(a) You have business continuity and disaster recovery plans that have been tested for practicality, effectiveness and completeness.
(b) Appropriate use is made of different test methods, e.g. manual failover, table-top exercises or red-teaming.
(c) You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.
(d) Your operational systems are segregated from other business and external systems by appropriate technical and physical means, e.g. separate network and system infrastructure with independent user administration. Internet services are not accessible from operational systems.
(e) You have identified and mitigated any geographical constraints or weaknesses, e.g. systems that your essential service depends upon are duplicated to another location, important network connectivity has alternative physical paths and service providers.

1.8 Outcomes: data recovery

1.8.1

(a) Suitable backups of all important data and information needed to recover critical systems are made, tested, documented and routinely reviewed.
(b) Your comprehensive, automatic and tested technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event.
(c) Key roles are duplicated and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential service.

1.9 Outcomes: RCA and feedback/lessons learnt

1.9.1

(a) You perform root cause analysis (RCA) and apply lessons learnt to all incidents and outages.
(b) Lessons learnt are fed back to senior executives to review for strategic changes as required.

Section 2
Coverage and depth of detection capability (endpoint, network and behaviour)

2.1 Controls

2.1.1 *See Ch 28, 2.1 Controls*

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how the organisation monitors network boundaries.
(b) Provide evidence how you verified all endpoints were monitored effectively.
(c) Provide evidence how you verified the monitored network boundaries aligned to network diagrams.
(d) Provide evidence how the organisation uses host-based monitoring to monitor activities within systems on internal networks.
(e) Provide evidence how you verified that host-based monitoring is used effectively.
(f) Provide evidence how you verified that monitored systems on internal networks aligned to network diagrams.
(g) Provide evidence how you verified monitoring procedures are updated to include alterations to network boundaries.
(h) Provide evidence how you verified that monitoring data provided sufficient detail to detect security incidents.
(i) Provide evidence how the organisation monitors user activity.
(j) Provide evidence how you verified the organisation monitors user/service activity.
(k) Provide evidence how the organisation maintains a baseline (i.e., a minimum level of activity or starting point used for comparisons) of user/service activity.
(l) Provide evidence how the organisation uses this baseline user activity as part of their detection of suspicious/undesirable network policy violations.
(m) Provide evidence how the organisation regularly updates the baseline activity level.
(n) Provide evidence how the organisation maintains a record of suspicious/undesirable network activity for comparisons.
(o) Provide evidence how the organisation has used a risk-based impact assessment of a network compromise to develop the detect and respond procedures.
(p) Provide evidence how you verified that the risk assessment is amended when a new cyber security threat is identified.
(q) Provide evidence how you verified that organisation reviews the detect and respond procedures
    (i) every six months
    (ii) and/or when a new cyber security threat is identified.
(r) Provide evidence how you verified that the detect and respond procedures are aligned to the impact of a network compromise.
(s) Provide evidence how you verified that the detect and respond procedures are aligned to the organisation's threat models.
(t) Provide evidence how you verified the organisation's threat models are amended
    (i) as a result of a security incident
    (ii) and/or when a new cyber security threat is identified.

Section 3
Analysis, investigation and discovery

3.1 Controls

3.1.1 *See Ch 30, 3.1 Controls*

3.2 Required evidence and testing

3.2.1

(a) Provide evidence how the organisation monitoring ties access to individuals and/or services.
(b) Provide evidence how you verified the organisation's monitoring ties access to individuals and/or services.

(c) Provide evidence how the organisation monitoring is able reconstruct:

(i) all logical access requests (including requests to access audit logs and invalid access requests);
(ii) all administrative privilege activities;
(iii) initialising, stopping and pausing monitoring activities;
(iv) and system level object creation/deletion.

(d) Provide evidence how you verified that organisation monitoring is able reconstruct:

(i) all logical access requests (including requests to access audit logs and invalid access requests);
(ii) all administrative privilege activities;
(iii) initialising, stopping and pausing monitoring activities;
(iv) and system level object creation/deletion.

(e) Provide evidence how the organisation monitoring is able to reconstruct usage and/or changes to authentication and authorisation processes, specifically:

(i) privilege elevation;
(ii) administrative privilege modification and/or deletion.

(f) Provide evidence how verified the organisation monitoring is able to reconstruct usage and/or changes to authentication and authorisation processes, specifically:

(i) privilege elevation;
(ii) and administrative privilege modification and/or deletion.

(g) Provide evidence how you verified the organisation monitoring recorded for each network event the:

(i) user identification;
(ii) date, time, type, source and target;
(iii) and success and failure.

(h) Provide a description of the time synchronization services used by the organisation. Provide evidence how you verified that the organisation receives time settings from industry recognised sources;

(i) Provide evidence how you verified that:

(i) all systems have correct and consistent time;
(ii) access to time data is restricted and logged;
(iii) and access to time synchronization services is restricted and logged.

(j) Provide evidence how the organisation protects and prevents any modification to the monitoring logs;

(k) Provide evidence how you verified the organisation protects and prevents any modification to the monitoring logs, specifically:

(i) access to monitoring logs are restricted (to individuals with a job related need);
(ii) access to monitoring logs is recorded (as above);
(iii) access privileges restrict access to read only;
(iv) all monitoring logs (including those from external facing components) are backed up to a secure and central storage.
(v) and archived logs are protected with file integrity monitoring;

(l) Provide evidence how you verified the organisation retains monitoring logs in line with industry recognised best practice;

(m) Provide evidence how you verified the organisation monitoring capability is configured to generate real-time alerts;

(n) Provide evidence how you verified the organisation monitoring capability operates continuously;

(o) Provide evidence how the organisation ensures alerts are generated if the monitoring capability becomes unavailable;

(p) Provide evidence how you verified alerts are generated if the organisation monitoring capability becomes unavailable.

Section 4
Management of detection capability

4.1 Controls

4.1.1 The organisation must ensure that the identification, collection and preservation of any evidence of security incidents follows defined policies and procedures.

4.1.2 Mappings:

- ISO 27002: 16.1.7
- IEC 62443-3
    - SR 2.10 – Response to audit processing failures

4.2 Required evidence and testing

4.2.1

(a) Provide evidence how the organisation uses the monitoring data to create a baseline activity from which to identify suspicious/undesirable user, network and/or service activity.

(b) Provide evidence how the organisation selected the types and sources of monitoring data used to identify suspicious/undesirable user, network and/or service activity.

(c) Provide evidence how you verified that the organisation uses the monitoring data to identify suspicious/undesirable user, network and/or service activity.

(d) Provide evidence how the organisation determines what is an appropriate timescale for the periodic review of monitoring data.

(e) Provide evidence how you verified that the periodic review of monitoring data:

(i) is conducted as defined in the documented procedure;

(ii) results in an amended user, network and/or service baseline;

(iii) and includes actions to investigate any irregularities found during the review.

(f) Provide evidence how the organisation makes individuals (including contractors) aware of their responsibilities to quickly report cyber security incidents (including suspected weaknesses in the cyber security mechanisms).

(g) Provide evidence how you verified that individuals (including contractors) are aware of the procedures for reporting cyber security incidents (including suspected weaknesses in the cyber security mechanisms).

■ *Section 5*
Incident management planning

5.1 Controls

5.1.1 *See Ch 30, 4.1 Controls*

5.2 Required evidence and testing

5.2.1

(a) Provide evidence how your organisation incident management methodology:

(i) is a product of senior management's risk management process;

(ii) ensures those responsible for response are competent;

(iii) and a clear chain of communication exists to facilitate effective decision making and contact to relevant parties.

(b) Provide evidence how you verified the organisation’s incident management methodology ensures designated individuals:

(i) are available to immediately respond to cyber security incidents;

(ii) and are periodically trained in the latest cyber security incident investigation techniques.

(c) Provide evidence how the organisation's incident management methodology takes into account the organisation’s:

(i) cyber security threat models;

(ii) and cyber security risk management strategy.

(d) Provide evidence how you verified that the organisation's incident management methodology takes into account the organisation’s:

(i) cyber security threat models;

(ii) and cyber security risk management strategy;

(e) Provide evidence how you verified the organisation’s incident management methodology has procedures for monitoring alerts from system components with security capabilities.;

(f) Provide evidence how the organisation's incident management methodology provides procedures for:

(i) reporting and logging of cyber security incidents;
(ii) responding to/and communicating about a cyber security incident;
(iii) collecting and storing evidence from a cyber security incident;
(iv) and recovery and learning from a cyber security incident.

(g) Provide evidence how the organisation's incident management methodology ensures:

(i) appropriate and competent individuals investigate the cyber security incident;
(ii) only a single designated individual is responsible for managing the response to the cyber security incident;
(iii) and rapid and effective communication is developed and maintained with relevant external bodies.

(h) Provide evidence how the organisation's incident management methodology ensures incident response procedures are;

(i) tested every 12 months;
(ii) updated to include lessons learnt and/or in line with industry developments.

(i) Provide evidence how you verified the organisation's incident management methodology is updated to include lessons learnt and/or in line with industry developments;

(j) Provide evidence how the organisation's incident management methodology ensures the reporting of the cyber security incident follows a formal, documented, organised and methodical approach that has been rehearsed and practised (*see* above).

Section 6
Response capability

6.1 Controls

6.1.1 *See Ch 30, 5.1 Controls*

6.2 Required evidence and testing

6.2.1

(a) Provide evidence how the organisation's incident response capability and procedures are based on industry-accepted practice (e.g., NIST SP800-800-61, etc.).

(b) Provide evidence how you verified the organisation's incident response capability and procedures are based on industry-accepted practice (e.g., NIST SP800-800-61, etc.).

(c) Provide evidence how the organisation's incident response capability incorporates detection and analysis of cyber security incidents.

(d) Provide evidence how you verified the organisation's incident response capability incorporates detection and analysis of cyber security incidents.

Section 7
Testing and exercising

7.1 Controls

7.1.1 In order to ensure that established and implemented incident response plans remain valid and effective, the organisation must regularly test and exercise such plans.

7.1.2 Mappings:

- ISO 27002: 17.1.3

7.2 Required evidence & testing

7.2.1

(a) Provide evidence how the organisation reviews and tests the incident response procedures;
(b) Provide evidence how testing of the incident response procedures incorporates cyber security incident scenarios developed from the organisation's threat models;
(c) Provide evidence how you verified testing of the incident response procedures incorporates cyber security incident scenarios developed from the organisation's threat model;
(d) Provide evidence how you verified the organisation's incident procedures are updated to include lessons learnt from testing and/or in line with industry developments;
(e) Provide evidence how you verified testing of the incident response procedures is undertaken in line with organisation's incident management methodology.

Section 8
Business continuity

8.1 Controls

8.1.1 *See Ch 28, 3.1 Controls*

8.2 Required evidence and testing

8.2.1

(a) Provide evidence how you verified the organisation has embedded cyber security continuity within business continuity and/or disaster recovery;
(b) Provide evidence how the organisation determined its cyber security continuity requirements;
(c) Provide evidence how the organisation ensures continuity for cyber security will be in place during an adverse situation.;
(d) Provide evidence how you verified the cyber security continuity requirements are in line with the organisation's threat models;
(e) Provide evidence how you verified the cyber security continuity requirements are updated:
    (i) after being tested;
    (ii) in line with threat intelligence received;
    (iii) and/or when a new cyber security vulnerability is identified.
(f) Provide evidence how you verified testing of the cyber security continuity requirements is undertaken in line with recognised industry best practice;
(g) Provide evidence how you verified the organisation has formal, documented and approved response and recovery plans and procedures;
(h) Provide evidence how you verified that the response and recovery plans include additional procedures/;
    (i) for maintaining current cyber security controls during an adverse situation;
    (ii) and for deploying compensating cyber security controls when the current cyber security controls cannot be maintained.
(i) Provide evidence how the organisation has identified and mitigated any geographical constraints or weaknesses within the cyber security continuity plans and procedures.

Section 9
Data recovery

9.1 Controls

9.1.1 *See Ch 30, 7.1 Controls*

9.2 Required evidence and testing

9.2.1

(a) Provide evidence how the organisation's business continuity plans makes provision for data and software recovery;
(b) Provide evidence how the organisation's business continuity plans details the recovery procedures;

(c) Provide evidence how you verified the recovery procedures are based on the organisation's:

(i) business requirements;
(ii) cyber security threat models;
(iii) and a risk assessment of the data/software/system availability to the organisation's well-being.

(d) Provide evidence how you verified the appropriateness of organisation's recovery procedures;

(e) Provide evidence how you verified the recovery procedures were tested;

(f) Provide evidence how you verified the recovery time was in line with the organisation's business continuity strategy;

(g) Provide evidence how you verified the organisation's documented records of the data backups and software/system images were current and accurate;

(h) Provide evidence how the organisation manages and controls the data/software/system replication process;

(i) Provide evidence how the organisation ensured that backup location would be immune from a similar adverse condition that initially caused the recovery process to be initiated;

(j) Provide evidence how you verified the selection of the backup location would mitigate against a similar adverse condition from impacting on the availability of the data/software/system being replicated;

(k) Provide evidence how you verified the replicated data/software/system was provided with the same level of logical, physical, environmental and cryptographic protection as that provided to the original data/software/system.

Section 10
RCA and feedback/lessons learnt

10.1 Controls

10.1.1 The organisation must ensure that after any incident/outage a root cause analysis (RCA) is undertaken, and lessons learnt are used to update the detect and respond procedures.

10.1.2 Mappings:

- ISO 27002: 16.1.6

10.2 Required evidence and testing

10.2.1

(a) Provide evidence how the organisation conducts an RCA after any incident/outage.

(b) Provide evidence how you verified results of the RCA are used to update the detect and respond procedures (including the organisation's cyber security threat models).

Contents

Contents

Section 1
Outcomes

1.1 Outcomes

1.1.1

(a) Senior management have visibility of key risk decisions made throughout the organisation (on board vessels and shore based).

(b) You maintain a current understanding of the exposure of the external environment to publicly-known vulnerabilities. You regularly test to fully understand the vulnerabilities of the networks and information systems that support your operations and verify this understanding with third-party testing. Announced vulnerabilities for all software packages, network equipment and operating systems used to support your operations are tracked, prioritised and mitigated (e.g. by patching) promptly.

(c) Identify and record changes in your environment.

Section 2
Risk management

2.1 Controls

2.1.1 Maintain an updated risk register that evaluates risks and the actions taken in result of these evaluations.

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how you verified that a risk assessment:

(i) is undertaken every 12 months and/or after any significant infrastructure or application upgrade;
(ii) is able to identify critical assets, and threats and vulnerabilities to those assets;
(iii) provides a documented risk assessment;
(iv) and results in an updated risk register and a senior management plan to manage those risks.

Section 3
Vulnerability management

3.1 Controls

3.1.1 The organisation must establish a process

(a) for the timely identification of new security vulnerabilities;

(b) to assess the risk posed by such vulnerabilities (and if necessary, update the organisation's cyber security threat models);

(c) and for the development of appropriate controls to mitigate against those risks.

(Maps to ISO 27002: 12.6.)

3.2 Required evidence and testing

3.2.1

(a) Provide evidence how the organisation's vulnerability management process identifies specific vulnerability management roles and responsibilities, e.g.

  (i) the timely identification of new security vulnerabilities;
  (ii) assessing the risk posed by such vulnerabilities (and if necessary, update the organisation's cyber security threat models);
  (iii) and developing appropriate controls to mitigate against those risks.

(b) Provide evidence how you verified the organisation made reference to the asset inventory when identifying new security vulnerabilities;

(c) Provide evidence how the organisation ensured the sources of technical vulnerability information were relevant and useful.

(d) Provide evidence how the organisation used technical vulnerability information to regularly update the cyber security threat models;

(e) Provide evidence how you verified all cyber security mechanisms and controls mapped back to cyber threats and vulnerabilities;

(f) Provide evidence how the organisation's vulnerability management process defined a reaction time to received vulnerability notifications;

(g) Provide evidence how you verified the notification reaction time was established and in use;

(h) Provide evidence how the organisation's vulnerability management process used a risk-based approach to each vulnerability to derive a timeline for remediation.

(i) Provide evidence how the organisation's vulnerability management process maintains a record of all:

  (i) identified vulnerabilities;
  (ii) actions taken to remediate those vulnerabilities;
  (iii) and in cases where remediation is not possible, compensating controls used to reduce the risks associated with the vulnerability.

(j) Provide evidence how verified the organisation's vulnerability management process maintains a record of all:

  (i) identified vulnerabilities;
  (ii) actions taken to remediate those vulnerabilities;
  (iii) and in cases where remediation is not possible, compensating controls used to reduce the risks associated with the vulnerability.

Section 4
Change management

4.1 Controls

4.1.1 Establish change management process.

4.2 Required evidence and testing

4.2.1

(a) Provide evidence how the documented change management methodology:

  (i) identifies when changes are planned or proposed;
  (ii) is undertaken upon changes, upgrades and updates;
  (iii) includes testing before implementation in live environments;
  (iv) raises impacts from implementing tested changes;
  (v) includes obtaining formal approval upon review;
  (vi) verifies that changes meet security requirements;
  (vii) details how changes are communicated to personnel;
  (viii) and includes measures for changes that are not successful.

Contents

Contents

Section 1
Outcomes

1.1 Outcomes

1.1.1

(a) Senior management have visibility of key risk decisions made throughout the organisation (on board vessels and shore based).
(b) Risk management decisions are periodically reviewed to ensure their continued relevance and validity.
(c) Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your ship and operating environment.
(d) You conduct risk assessments when significant events potentially impact the security posture of the ship, such as replacing a system or a change in the cyber security threat landscape.
(e) The effectiveness of your risk management process is reviewed periodically and improvements made as required.
(f) You maintain a current understanding of the exposure of your environment to publicly-known vulnerabilities. You regularly test to fully understand the vulnerabilities of the networks and information systems that support your operations and verify this understanding with third-party testing. Announced vulnerabilities for all software packages, network equipment and operating systems used to support your operations are tracked, prioritised and mitigated (e.g. by patching) promptly.
(g) You regularly test to fully understand the vulnerabilities of the networks and information systems that support your operations and verify this understanding with third-party testing.
(h) Identify and record changes in your environment.
(i) Proposed changes are planned and tested before being implemented.
(j) Possible impacts of implementing proposed changes are identified and evaluated.
(k) Proposed changes obtain formal approval upon review.
(l) Incorporate crisis management as an integral part of incident response and business continuity management.
(m) Identify a methodology of third party management that includes risk management.

Section 2
Risk management

2.1 Controls

2.1.1 Maintain an updated risk register that evaluates risks and the actions taken in result of these evaluations.

2.1.2 Perform risk management reviews.

2.1.3 Integrate vulnerability management into the risk assessment process.

2.1.4 Establish criteria for when risk assessments must be performed.

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how you verified that a risk assessment :

(i) is undertaken every 12 months and/or after any significant infrastructure or application upgrade;
(ii) is able to identify critical assets, and threats and vulnerabilities to those assets;
(iii) provides a documented risk assessment;
(iv) and results in an updated risk register and a senior management plan to manage those risks.

(b) Provide evidence how you verified that risk management reviews are performed in accordance with the risk management strategy.

(c) Provide evidence how the documented penetration-testing methodology :

(i) is based on industry-accepted practice (e.g. NIST SP800-115);
(ii) covers the defined security perimeter;
(iii) includes components that support network functions as well as operating systems (i.e. network-layer testing) as well as external application-layer penetration tests;
(iv) validates any segmentation controls
(v) considers both threat intelligence received and any vulnerabilities identified during the previous 12 months;
(vi) and details how the results of the testing and any remediation required is retained.

(d) Provide evidence how the documented risk assessment methodology:

(i) is based on industry-accepted practice (e.g. OCTAVE, ISO 27005 and NIST SP 800-30);
(ii) covers the defined security perimeter;
(iii) considers both threat intelligence received and any vulnerabilities identified during the previous 12 months;
(iv) and is undertaken every 12 months and/or after any significant infrastructure or application upgrade/

(e) Provide evidence how the review of the risk management process:

(i) demonstrated it's effectiveness;
(ii) indicated the need for improvements and documented how they were acted upon.

■ *Section 3* Vulnerability management

3.1 Controls

3.1.1 *See Ch 32, 3.1 Controls*

3.2 Required evidence and testing

3.2.1 *See Ch 32, 3.2 Required evidence and testing*

■ *Section 4* Vulnerability testing

4.1 Controls

4.1.1 Perform vulnerability testing at regular intervals.

4.1.2 Facilities and/or assets that store, process and/or transmit critical/sensitive data must be regularly reviewed for compliance with the organisation's information security policies, standards and risk assessments.

4.1.3 Mappings:

- ISO 27002: Section 18.2.3
- IEC 62443-3
    - SR 3.3 - Security functionality verification

4.2 Required evidence and testing

4.2.1

(a) Provide evidence how you verified vulnerability testing was performed every 12 months and/or after any significant infrastructure or application upgrade.

(b) Provide evidence how you verified that the penetration testing was performed by competent individual(s).

■ *Section 5*
Change management

5.1 Controls

5.1.1 Establish change management process.

5.1.2 Demonstrate a methodology to change management process.

5.1.3 Changes are reviewed and obtain formal approval.

5.1.4 The organisation must control all changes to the organisation, business processes, data processing facilities and systems that impact on data security. (Maps to ISO 27002: 12.1.2.)

5.2 Required evidence and testing

5.2.1

(a) Provide evidence how the documented change management methodology:

(i) identifies when changes are planned or proposed;
(ii) is undertaken upon changes, upgrades and updates;
(iii) includes testing before implementation in live environments;
(iv) raises impacts from implementing tested changes;
(v) includes obtaining formal approval upon review;
(vi) verifies that changes meet security requirements;
(vii) details how changes are communicated to personnel;
(viii) and includes measures for changes that are not successful.

■ *Section 6*
Crisis management

6.1 Controls

6.1.1 Establish crisis management process that supports incident response and business continuity.

6.2 Required evidence and testing

6.2.1

(a) Provide evidence how crisis management is included in your:

(i) incident response procedures;
(ii) and business continuity management.

Section 7
Third party management

7.1 Controls

7.1.1 Demonstrate the use of risk management in third party management documentation and procedure.

7.1.2 The organisation must ensure that all of the organisation's data and/or facilities accessed by third party service provides is adequately protected from loss of confidentially, integrity and/or availability. (Maps to ISO 27002:15).

7.2 Required evidence and testing

7.2.1

(a) Provide evidence how the third party management methodology:

(i) encorporates your risk management methodology;
(ii) provides ongoing evaluation of service levels;
(iii) ensures third parties meet security requirements;
(iv) and validates any necessary compliance of third parties through documentation.

Contents

Contents

Section 1
Outcomes

1.1 Outcomes

1.1.1

(a) You perform regular penetration testing on network and application level systems within the environment.
(b) You perform assurance testing on any new critical components, upgrades or significant changes to the environment.
(c) All issues raised are promptly addressed by mitigation and risk treatment plans.
(d) Senior management have visibility of key risk decisions made throughout the organisation (on board vessels and shore based).
(e) Risk management decisions are periodically reviewed to ensure their continued relevance and validity.
(f) Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your ship and operating environment.
(g) You conduct risk assessments when significant events potentially impact the security posture of the ship, such as replacing a system or a change in the cyber security threat landscape.
(h) The effectiveness of your risk management process is reviewed periodically and improvements made as required.
(i) Risk management decision-makers understand their responsibilities for making effective and timely decisions in the context of the risk appetite, as set by senior management. Risk management decision-making is delegated and escalated where necessary, across the organisation, to people who have the skills, knowledge, tools, and authority they need.
(j) Your organisational process ensures that critical security risks to networks and information systems are identified, analysed, prioritised, and managed.
(k) Your risk assessments are based on a clearly articulated set of threat assumptions, informed by an up-to-date understanding of security threats to your essential service.
(l) Your risk assessments are dynamic, and are updated in the light of relevant changes which may include technical changes to networks and information systems, change of use and new threat information.
(m) You maintain a current understanding of the exposure of your environment to publicly-known vulnerabilities. You regularly test to fully understand the vulnerabilities of the networks and information systems that support your operations and verify this understanding with third-party testing. Announced vulnerabilities for all software packages, network equipment and operating systems used to support your operations are tracked, prioritised and mitigated (e.g. by patching) promptly.
(n) You regularly test to fully understand the vulnerabilities of the networks and information systems that support your operations and verify this understanding with third-party testing.
(o) Updates/patches/changes should be tested to provide assurance that they do not introduce new vulnerabilities.
(p) Identify and record changes in your environment.
(q) Proposed changes are planned and tested before being implemented.
(r) Possible impacts of implementing proposed changes are identified and evaluated.

(s) Proposed changes obtain formal approval upon review.
(t) Proposed changes are verified to meet security requirements.
(u) Change details are communicated to all relevant personnel.
(v) Procedures for unsuccessful changes are established and followed.
(w) Incorporate crisis management as an integral part of incident response and business continuity management.
(x) Perform assurance testing of crisis management inline with incident response.
(y) Identify a methodology of third party management that includes risk management.
(z) Ensure visibility of what each third party relationship brings to the organisation.
(aa) Evaluate third party entities through security analysis and scoring.

Section 2
Penetration testing

2.1 Controls

2.1.1 Perform external penetration testing at least annually.

2.1.2 Perform external penetration testing after any significant infrastructure or application upgrade or modification.

2.1.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.

2.1.4 Facilities and/or assets that store, process and/or transmit critical/sensitive data must be regularly reviewed for compliance with the organisation's security policies, procedures and risk assessments. (Maps to ISO 27002: Section 18.2.3.)

2.2 Required evidence and testing

2.2.1

(a) Provide evidence how the documented penetration-testing methodology:
  (i) is based on industry-accepted practice (e.g. NIST SP800-115);
  (ii) covers the defined security perimeter;
  (iii) includes components that support network functions as well as operating systems (i.e. network-layer testing) as well as external application-layer penetration tests;
  (iv) validates any segmentation controls;
  (v) considers both threat intelligence received and any vulnerabilities identified during the previous 12 months;
  (vi) and details how the results of the testing and any remediation required is retained.
(b) Provide evidence how you verified penetration testing was performed every 12 months and/or after any significant infrastructure or application upgrade;
(c) If segmentation is used to isolate facilities and/or devices that store, process and/or transmit critical/sensitive data from other networks, provide evidence how the penetration test verified that the segmentation controls ensured the isolation is operationally effective;
(d) Provide evidence how you verified that the penetration testing was performed by competent individual(s).
(e) Provide evidence how you verified:
  (i) that all exploitable vulnerabilities were remediated;
  (ii) and that a re-test confirmed the remediation was in place and effective.

Section 3
Risk management

3.1 Controls

3.1.1 Maintain an updated risk register that evaluates risks and the actions taken in result of these evaluations.

3.1.2 Perform risk management reviews.

3.1.3 Integrate vulnerability management into the risk assessment process.

3.1.4 Establish criteria for when risk assessments must be performed.

3.1.5 Establish that roles and responsibilities are understood for those involved in the risk process.

3.1.6 Establish a hierarchy for personnel and processes involved in risk management.

3.2 Required evidence and testing

3.2.1

(a) Provide evidence how you verified that a risk assessment:

  (i) is undertaken every 12 months and/or after any significant infrastructure or application upgrade;
  (ii) is able to identify critical assets, and threats and vulnerabilities to those assets;
  (iii) provides a documented risk assessment;
  (iv) and results in an updated risk register and a senior management plan to manage those risks.

(b) Provide evidence how you verified that risk management reviews are performed in accordance with the risk management strategy.

(c) Provide evidence how the documented penetration-testing methodology:

  (i) is based on industry-accepted practice (e.g. NIST SP800-115);
  (ii) covers the defined security perimeter;
  (iii) includes components that support network functions as well as operating systems (i.e., network-layer testing) as well as external application-layer penetration tests;
  (iv) validates any segmentation controls;
  (v) considers both threat intelligence received and any vulnerabilities identified during the previous 12 months;
  (vi) and details how the results of the testing and any remediation required is retained.

(d) Provide evidence how the documented risk assessment methodology:

  (i) is based on industry-accepted practice (e.g. OCTAVE, ISO 27005 and NIST SP 800-30);
  (ii) covers the defined security perimeter;
  (iii) considers both threat intelligence received and any vulnerabilities identified during the previous 12 months;
  (iv) and is undertaken every 12 months and/or after any significant infrastructure or application upgrade.

(e) Provide evidence how the review of the risk management process:

  (i) demonstrated its effectiveness;
  (ii) indicated the need for improvements and documented how they were acted upon.

(f) Provide evidence how the risk management policy and procedures:

  (i) ensure that risk management decision-making is delegated to those individuals who have appropriate skills, knowledge, tools and authority;
  (ii) and highlight the responsibility those delegated individuals have for making (in the context of the organisation's risk appetite), effective and timely decisions.

(g) Provide evidence how you verified that delegated decision-makers have appropriate skills, knowledge, tools and authority to make effective and timely decisions.

(h) Provide evidence how you verified that delated decision-makers:

  (i) are aware of their risk management roles and responsibilities;
  (ii) and that they have formally acknowledged them.

(i) Provide evidence how risks are communicated between individuals;

(j) Provide evidence how the documented risk assessment methodology.

Section 4
Vulnerability management

4.1 Controls

4.1.1 *See Ch 32, 3.1 Controls*

4.2 Required evidence and testing

4.2.1 *See Ch 32, 3.2 Required evidence and testing*

Section 5
Vulnerability testing

5.1 Controls

5.1.1 Perform vulnerability testing at regular intervals.

5.1.2 Validate that updates to systems do not introduce new vulnerabilities.

5.1.3 Facilities and/or assets that store, process and/or transmit critical/sensitive data must be regularly reviewed for compliance with the organisation's security policies, procedures and risk assessments. (Maps to ISO 27002: Section 18.2.3.)

5.2 Required evidence and testing

5.2.1

(a) Provide evidence how you verified vulnerability testing was performed every 12 months and/or after any significant infrastructure or application upgrade.

(b) Provide evidence how you verified that the penetration testing was performed by competent individual(s).

(c) Provide evidence how you verified

  (i) that all exploitable vulnerabilities were remediated

  (ii) and that a re-test confirmed the updates/patches/changes/remediation was in place and effective.

Section 6
Change management

6.1 Controls

6.1.1 Establish a change management process.

6.1.2 Demonstrate a methodology for the change management process.

6.1.3 Changes are reviewed and obtain formal approval.

6.1.4 Demonstrate assessment of changes to verify they meet rigour of security requirements.

6.1.5 Demonstrate how changes are communicated to personnel.

6.1.6 Demonstrate process for unsuccessful changes and rollback.

6.1.7 The organisation must control all changes to the organisation, business processes, data processing facilities and systems that impact on data security. (Maps to ISO 27002: 12.1.2.)

6.2 Required evidence and testing

6.2.1

(a) Provide evidence how the documented change management methodology

(i) identifies when changes are planned or proposed
(ii) is undertaken upon changes, upgrades and updates
(iii) includes testing before implementation in live environments
(iv) raises impacts from implementing tested changes
(v) includes obtaining formal approval upon review
(vi) verifies that changes meet security requirements
(vii) details how changes are communicated to personnel
(viii) and includes measures for changes that are not successful

Section 7
Crisis management

7.1 Controls

7.1.1 Establish crisis management process that supports incident response and business continuity.

7.1.2 Perform Crisis testing as a part of incident response.

7.2 Required evidence and testing

7.2.1

(a) Provide evidence how crisis management is included in your
  (i) incident response procedures
  (ii) and business continuity management.
(b) Provide evidence how you verified that crisis management is tested as part of your incident response procedures.

Section 8
Third party management

8.1 Controls

8.1.1 Demonstrate the use of risk management in third party management documentation and procedure.

8.1.2 Assess ongoing behaviour, performance and risk from third parties.

8.1.3 Analyse the security of third parties to gauge the risk they pose.

8.1.4 The organisation must ensure that all of the organisation's data and/or facilities accessed by third party service provides is adequately protected from loss of confidentially, integrity and/or availability. (Maps to ISO 27002:15.)

8.2 Required evidence and testing

8.2.1

(a) Provide evidence how the third party management methodology
  (i) Incorporates your risk management methodology;
  (ii) provides ongoing evaluation of service levels;
  (iii) ensures third parties meet security requirements;
  (iv) and validates any necessary compliance of third parties through documentation.

Contents

Contents

Section 1
Outcomes

1.1 Outcomes

1.1.1

(a) You perform regular penetration testing on network and application level systems within the environment.
(b) You perform assurance testing on any new critical components, upgrades or significant changes to the environment.
(c) All issues raised are promptly addressed mitigation and risk treatment plans.
(d) Senior management have visibility of key risk decisions made throughout the organisation (on board vessels and shore based).
(e) Risk management decisions are periodically reviewed to ensure their continued relevance and validity.
(f) Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your ship and operating environment.
(g) You conduct risk assessments when significant events potentially impact the security posture of the ship, such as replacing a system or a change in the cyber security threat landscape.
(h) The effectiveness of your risk management process is reviewed periodically and improvements made as required.
(i) Risk management decision-makers understand their responsibilities for making effective and timely decisions in the context of the risk appetite, as set by senior management. Risk management decision-making is delegated and escalated where necessary, across the organisation, to people who have the skills, knowledge, tools, and authority they need.
(j) Your organisational process ensures that critical security risks to networks and information systems are identified, analysed, prioritised, and managed.
(k) Your risk assessments are dynamic, and are updated in the light of relevant changes which may include technical changes to networks and information systems, change of use and new threat information.
(l) The output from your risk management process is a clear set of security requirements that will address the risks in line with your organisational approach to security.
(m) Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals.
(n) You maintain a current understanding of the exposure of all systems in your environment to publicly-known vulnerabilities. You regularly test to fully understand the vulnerabilities of the networks and information systems that support your operations and verify this understanding with third-party testing. Announced vulnerabilities for all software packages, network equipment and operating systems used to support your operations are tracked, prioritised and mitigated (e.g. by patching) promptly. You maximise the use of supported software, firmware and hardware in your networks and information systems supporting your essential service.
(o) You regularly test to fully understand the vulnerabilities of the networks and information systems that support your operations and verify this understanding with third-party testing. Updates/patches/changes should be tested to provide assurance that they do not introduce new vulnerabilities.

(p) Identify and record changes in your environment.
(q) Proposed changes are planned and tested before being implemented.
(r) Possible impacts of implementing proposed changes are identified and evaluated.
(s) Proposed changes obtain formal approval upon review.
(t) Proposed changes are verified to meet security requirements.
(u) Change details are communicated to all relevant personnel.
(v) Procedures for unsuccessful changes are established and followed.
(w) Emergency change control process is designated in response to responding to incidents.
(x) Encorporate crisis management as an integral part of incident response and business continuity management.
(y) Perform assurance testing of crisis management inline with incident response.
(z) Understand the impact of a crisis on personnel and communication within the organisation.
(aa) Set out requiremnts for managing crisis through tools, communication, and procedures.
(ab) Identify a methodology of third party management that includes risk management.
(ac) Ensure visibility of what each third party relationship brings to the organisation.
(ad) Evaluate third party entities through security analysis and scoring.
(ae) Identify any standards that third parties must comply with.

Section 2
Penetration testing

2.1 Controls

2.1.1 *See Ch 34, 2.1 Controls*

2.2 Required evidence and testing

2.2.1 *See Ch 34, 2.2 Required evidence and testing*

Section 3
Risk management

3.1 Controls

3.1.1 Maintain an updated risk register that evaluates risks and the actions taken in result of these evaluations.

3.1.2 Perform risk management reviews.

3.1.3 Integrate vulnerability management into the risk assessment process.

3.1.4 Establish criteria for when risk assessments must be performed.

3.1.5 Establish that roles and responsibilities are understood for those involved in the risk process.

3.1.6 Establish a hierarchy for personnel and processes involved in risk management.

3.1.7 Establish a formal and standardised format for translating risks into treatment.

3.1.8 Establish a process for how assessment results are communicated to decision-makers.

3.2 Required evidence and testing

3.2.1

(a) Provide evidence how you verified that a risk assessment
    (i) is undertaken every 12 months and/or after any significant infrastructure or application upgrade;
    (ii) is able to identify critical assets, and threats and vulnerabilities to those assets;
    (iii) provides a documented risk assessment

(iv) and results in an updated risk register and a senior management plan to manage those risks.

(b) Provide evidence how you verified that risk management reviews are performed in accordance with the risk management strategy.

(c) Provide evidence how the documented penetration-testing methodology

(i) is based on industry-accepted practice (e.g. NIST SP800-115);
(ii) covers the defined security perimeter;
(iii) includes components that support network functions as well as operating systems (i.e., network-layer testing) as well as external application-layer penetration tests;
(iv) validates any segmentation controls;
(v) considers both threat intelligence received and any vulnerabilities identified during the previous 12 months;
(vi) and details how the results of the testing and any remediation required is retained.

(d) Provide evidence how the documented risk assessment methodology

(i) is based on industry-accepted practice (e.g. OCTAVE, ISO 27005 and NIST SP 800-30);
(ii) covers the defined security perimeter;
(iii) considers both threat intelligence received and any vulnerabilities identified during the previous 12 months;
(iv) and is undertaken every 12 months and/or after any significant infrastructure or application upgrade.

(e) Provide evidence how the review of the risk management process

(i) demonstrated it's effectiveness;
(ii) indicated the need for improvements and documented how they were acted upon.

(f) Provide evidence how the risk management policy and procedures

(i) ensures that risk management decision-making is delegated to those individuals who have appropriate skills, knowledge, tools and authority;
(ii) and highlights the responsibility those delegated individuals have for making (in the context of the organisation's risk appetite), effective and timely decisions.

(g) Provide evidence how you verified that delegated decision-makers have appropriate skills, knowledge, tools and authority to make effective and timely decisions.

(h) Provide evidence how you verified that delated decision-makers

(i) are aware of their risk management roles and responsibilities;
(ii) and that they have formally acknowledged them/

(i) Provide evidence how risks are communicated between individuals.

(j) Provide evidence how the documented risk management process

(i) produces meaningful and actionable output;
(ii) helps you address risk that is relevant to your organisation;
(iii) and helps you manage risk in a top/down methodology.

(k) Provide evidence how you verified that risk assessments result in an updated risk register and a senior management plan to manage those risks.

Section 4
Vulnerability management

4.1 Controls

4.1.1 *See Ch 32, 3.1 Controls*

4.2 Required evidence and testing

4.2.1

(a) Describe how the organisation's vulnerability management process identifies specific vulnerability management roles and responsibilities, e.g.

(i) the timely identification of new security vulnerabilities;

(ii) assessing the risk posed by such vulnerabilities (and if necessary, update the organisation's cyber security threat models);
(iii) and developing appropriate controls to mitigate against those risks.

(b) Describe how you verified the organisation made reference to the asset inventory when identifying new security vulnerabilities.

(c) Describe how the organisation ensured the sources of technical vulnerability information were relevant and useful.

(d) Describe how the organisation used technical vulnerability information to regularly update the cyber security threat models.

(e) Describe how you verified all cyber security mechanisms and controls mapped back to cyber threats and vulnerabilities.

(f) Describe how the organisation's vulnerability management process defined a reaction time to received vulnerability notifications.

(g) Describe how you verified the notification reaction time was established and in use.

(h) Describe how the organisation's vulnerability management process used a risk-based approach to each vulnerability to derive a timeline for remediation.

(i) Describe how the organisation's vulnerability management process maintains a record of all

(i) identified vulnerabilities;
(ii) actions taken to remediate those vulnerabilities;
(iii) and in cases where remediation is not possible, compensating controls used to reduce the risks associated with the vulnerability.

(j) Describe how verified the organisation's vulnerability management process maintains a record of all

(i) identified vulnerabilities;
(ii) actions taken to remediate those vulnerabilities;
(iii) and in cases where remediation is not possible, compensating controls used to reduce the risks associated with the vulnerability.

(k) Describe how the organisation ensures the continual effectiveness of its vulnerability management process.

(l) Describe how you verified the organisation ensures the continual effectiveness of its vulnerability management process.

(m) Describe how the organisation's vulnerability management process communicates information on identified security vulnerabilities to the incident response team.

(n) Describe how you verified the organisation's vulnerability management process communicates security vulnerability information to the incident response team.

Section 5
Vulnerability testing

5.1 Controls

5.1.1 *See Ch 34, 5.1 Controls*

5.2 Required evidence and testing

5.2.1 *See Ch 34, 5.2 Required evidence and testing*

Section 6
Change management

6.1 Controls

6.1.1 Establish a change management process.

6.1.2 Demonstrate a methodology for the change management process.

6.1.3 Changes are reviewed and obtain formal approval.

6.1.4 Demonstrate assessment of changes to verify they meet rigour of security requirements.

6.1.5 Demonstrate how changes are communicated to personnel.

6.1.6 Demonstrate a process for unsuccessful changes and rollback.

6.1.7 Demonstrate a process for changes as a result of incident response.

6.1.8 The organisation must control all changes to the organisation, business processes, data processing facilities and systems that impact on data security. (Maps to ISO 27002: 12.1.2.)

6.2 Required evidence and testing

6.2.1

(a) Provide evidence how the documented change management methodology

(i) identifies when changes are planned or proposed;
(ii) is undertaken upon changes, upgrades and updates;
(iii) includes testing before implementation in live environments;
(iv) raises impacts from implementing tested changes;
(v) includes obtaining formal approval upon review;
(vi) verifies that changes meet security requirements;
(vii) details how changes are communicated to personnel;
(viii) and includes measures for changes that are not successful.

(b) Provide evidence how emergency change management differs from the traditional change management methodology and verify its effectiveness as part of your incident response plan and procedure.

Section 7
Crisis management

7.1 Controls

7.1.1 Establish crisis management process that supports incident response and business continuity.

7.1.2 Perform crisis testing as a part of incident response.

7.1.3 Demonstrate assessment of processes and changes to help mitigate errors during time of crisis.

7.1.4 Include technology tools, communication methods, and management processes when establishing requirements for cisis management.

7.2 Required evidence and testing

7.2.1 *See Ch 34, 7.2 Required evidence and testing*

Section 8
Third party management

8.1 Controls

8.1.1 Demonstrate the use of risk management in third party management documentation and procedure.

8.1.2 Assess ongoing behaviour, performance and risk from third parties.

8.1.3 Analyse the security of third parties to gauge the risk they pose.

8.1.4 Continue assessment and verification of any standards that third parties are certified in.

8.1.5 The organisation must ensure that all of the organisation's data and/or facilities accessed by third party service provides is adequately protected from loss of confidentially, integrity and/or availability. (Maps to ISO 27002:15.)

8.2 Required evidence and testing

8.2.1 *See Ch 34, 8.2 Required evidence and testing*

Published by Lloyd’s Register Group Limited
Registered office (Reg. no. 08126909)
71 Fenchurch Street, London, EC3M 4BS
United Kingdom