104 – Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems

Original version

PREFACE

These guidelines are supported by the Norwegian Oil and Gas Security Forum, the HSE Managers Forum and by the Norwegian Oil and Gas Operations Committee. It has also been approved by the director general.

The responsible manager in Norwegian Oil and Gas is the manager HSE and standardisation, who can be contacted via +47 51 84 65 00 (switchboard).

These guidelines have been prepared with the broad-based participation of interested parties in the Norwegian petroleum industry, and are owned by the Norwegian Oil and Gas Association on behalf of the Norwegian petroleum industry.

Norwegian Oil and Gas Association
Vassbotnen 1, NO-4313 Sandnes
P O Box 8065
NO-4068 Stavanger, Norway
Tel.: +47 51 84 65 00
Fax: +47 51 84 65 01
Website: www.norskoljeoggass.no
E-mail: firmapost@norog.no

CONTENTS

1 INTRODUCTION

1.1 Purpose

The purpose of this guideline is to enhance overall information security in the offshore industry and thereby improve the safety and regularity of the operations on the Norwegian continental shelf (NCS).

This document contains guidance on how to implement the Norwegian Oil and Gas information security baseline requirements (ISBRs) in process control, safety and support (PCSS) ICT systems. The implementation guidance in this document is considered “good practice” for information security, but the organisation should adapt these proposed solutions in accordance with their own information security policy and regulations, and aligned with their national legislation. Implementing the information security controls and measures exactly as described in this guidance is not mandatory. Other methods and techniques may be used as long as the objectives of the ISBRs are achieved.

The Norwegian Oil and Gas ISBRs are additional to the company’s own information security policy and regulations, and subject to national legislation.

For reference purposes, each ISBR has references to the cyber security framework (CSF) from the National Institute of Standards and Technology (Nist), because this framework is mapped to relevant IT security standards such as Cobit 5, ISO 27002, IEC 62443 and others. It is also easy to relate the five functions with their categories to the process-oriented Plan–Do–Check–Act approach to defining proactive and reactive activities (see chapter 3).

This list of ISBRs is not pre-emptive nor exhaustive, and each organisation may have to implement additional controls and security measures to obtain the level of information security necessary for their business. Implementing all these controls in the ISBRs would not guarantee that security incidents cannot occur.

Examples of PCSS ICT systems architecture can be found in Appendix A.

As a supplement to the guideline a self-assessment tool for verifying a company's degree of compliance with the Norwegian Oil and Gas information security baseline requirements (ISBRs) is available. The tool (ISBR/SA) is intended to help companies assess the security level of their PCSS ICT systems, and is not meant to be used for external reporting.

1.2 Definitions and terminology

English	Norwegian	Explanation
Accountability	**Ansvarlighet**	The property which ensures that the actions of an entity can be traced uniquely to that entity.
Asset	**Aktiva**	Anything which has value to the organisation.
Authenticity	**Ekthet, pålitelighet**	The property which ensures that the identity of a subject or resource is the one claimed. Authenticity applies to such entities as users, processes, systems and information.
Availability	**Tilgjengelighet**	The property of being accessible and usable upon demand by an authorised entity.
Baseline controls	**Basistiltak**	The minimum set of safeguards established for a system or organisation.
Confidentiality	**Konfidensialitet**	The property which ensures that information is not made available or disclosed to unauthorised individuals, entities or processes.
Consequence	**Konsekvens**	The outcome of an event.
Control	**Tiltak**	Measure that is modifying risk.
ICT	**IKT**	Information and communication technology
ICT system	**IKT-system**	The combination of computer hardware, firmware and software – ie, computers, operating systems, networks, communication equipment and applications.
Information owner	**Informasjonseier**	An information owner is a function responsible for classifying the information concerned and for ensuring that relevant protection is implemented.
Information security	**Informasjonssikker-het**	All aspects related to defining, achieving and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information or information processing facilities.
Integrity	**Integritet**	The property of safeguarding the accuracy and completeness of assets.
IT security	**IT-sikkerhet**	All aspects related to defining, achieving and maintaining the confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of IT.
Likelihood	**Sannsynlighet**	Likelihood is the chance that something might happen. Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively (using mathematics).

English	Norwegian	Explanation
Malware	**Ødeleggende kode**	Software such as viruses, worms, Trojan horses, logical bombs and other malicious code.
Process control, safety and support ICT system	**IKT-basert produk-sjons-, sikkerhets- og støttesystem**	Any ICT system – permanently or temporarily connected – with a direct impact on oil and gas production and on the ICT systems used to support these systems directly. The specific function of the PCSS ICT system is to control, monitor, safeguard and optimise the production process and the integrity of the facilities. See also Appendix A: Examples of PCSS ICT architectures.
Recovery Time Objective (RTO)		RTO refers to the maximum acceptable length of time that can elapse before the lack of a business function severely impacts the organization. This is the maximum agreed time for the resumption of the critical business functions.
Recovery Point Objective (RPO)		RPO is the point in time to which systems and data must be recovered after a disaster has occurred.
Residual risk	**Restrisiko**	The risk remaining after risk treatment.
Risk	**Risiko**	The combination of the probability of an event and its consequences.
Risk analysis	**Risikoanalyse**	The systematic use of information to identify sources and to estimate risk. Risk analysis provides a basis for risk evaluation, risk treatment and risk acceptance.
Risk assessment	**Risikovurdering**	The overall process of risk identification, risk analysis and risk evaluation.
Risk evaluation	**Risikoevaluering**	The process of comparing the estimated risk with specified risk criteria to determine the significance of the risk.
Risk identification	**Identifisering av risiko**	The process of finding, recognising and describing risk.
Risk management	**Risikostyring**	The coordinated activities required to direct and control an organisation with regard to risk.
Risk treatment	**Risikobehandling**	The process of selecting and implementing measures to modify risk.
Security event	**Sikkerhetshendelse**	An identified occurrence of a system, service, or network state which indicates a possible breach of information security policy or a failure of safeguards, or a previously unknown condition which may be security relevant.

English	Norwegian	Explanation
Security incident	**Sikkerhetsbrudd**	A single unwanted or unexpected information security event or a series of such events which has a significant likelihood of compromising business operations and threatening information security.
System owner	**Systemeier**	The system owner is a function responsible for ensuring that the requirements in this document have been implemented in the PCSS ICT systems. The self-assessment ISBR can be used to identify which controls should be implemented by the system owner.
Threat	**Trussel**	A potential for violating security which exists when a circumstance, capability, action or event could breach security and cause harm.
Vulnerability	**Sårbarhet**	A weakness in an asset or group of assets which can be exploited by one or more threats.
Work permit (WP)	**Arbeidstillatelse (AT)**	A WP is a written document which authorises certain people to carry out specific work at a certain time, and which sets out the main precautions needed to complete the job safely. The WP is an operational safety barrier to protect against undesired incidents. See also Norwegian Oil and Gas recommended guidelines for common model for work permits – 088 (Norwegian only - Anbefalte retningslinjer for Felles modell for arbeidstillatelser (AT))

1.3 Abbreviations

Abbreviation	Description
BCP	Business continuity plan(s)
EPC	Engineering procurement and construction
ICT	Information and communication technology
ISBR	Information security baseline requirement
PCSS	Process control, safety and support
PCSS ICT system	Process control, safety and support ICT system
RPO	Recovery Point Objective
RTO	Recovery Time Objective
WP	Work permit

1.4 References

- Cyber security framework (CSF) from the National Institute of Standards and Technology (Nist) http://www.nist.gov/cyberframework/.
- IEC 62443.
- Cobit 5.
- ISO 27002 - Code of practice for information security controls.
- ISO 27031 - Guidelines for information and communication technology readiness for business continuity.
- Norwegian Oil and Gas' guideline 110 (supplement to guideline 104 (this document)) -
  Recommended guidelines for implementation of information security in process control, safety and support ICT systems during the engineering, procurement and commissioning phases.
- Norwegian Oil and Gas' guideline 123 (supplement to guideline 104 (this document)) -
  Recommended guidelines for classification of process control, safety and support ICT systems based on criticality
- Norwegian Oil and Gas' guideline 104 (this document) and an ISBR self-assessment programme.
- Norwegian Oil and Gas' guideline 088 - Recommended guidelines for common model for work permits (Norwegian only - Anbefalte retningslinjer for Felles modell for arbeidstillatelser (AT)).

2 HIGHLIGHTING OF CHANGES

2.1 Summary

- The main focus of this revision has been to bring the guidelines up to date with a changed threat picture and new modes of operation.

- Three new ISBRs are introduced, and five have been revised.
  The wording of some ISBRs have been slightly changed simply to make it more precise.

- The guidelines are updated in line with the Norwegian Oil and Gas standard template, and the language has been reviewed.

- The main sections of the document, the chapter on ISBRs and the implementation guidance (previous Appendix A), have been merged and restructured into a new chapter 3.

- Guidance on each ISBR
  - is structured in accordance with the functions in the cyber security framework (CSF) from National Institute of Standards and Technology (Nist), leading to sequential changes in the guidance on each ISBR
  - links within each ISBR are replaced with links to the Nist CSF
  - guidance for each ISBR is simplified through the removal of duplicate and/or overlapping statements between the ISBRs, based on the principle that each ISBR should be as “clean” as possible
  - some clarifications and simplifications have been made, partly in response to changes to modes of operation
  - changes to the controls have resulted in some necessary changes to the implementation guidance
  - duplications with Norwegian Oil and Gas guidelines 110 and 123 have been removed.

- A new Appendix C with a figure showing the relationship between the ISBRs has been added.

2.2 Further details of the changes

- Chapter 1.2 Definitions and terminology
  - Moved from former Appendix C.
  - Figure 1 on the relationship between risk activities and Figure 2 on the relationship between risks and work permits have been removed. They were not referenced anywhere in the document and should be covered in any event by other sources.
  - Added some new terms and made clarifying revisions to a few definitions

- Chapter 1.3 Abbreviations – new section.
- Chapter 1.4 References – new section.
- Chapter 2 Highlighting of changes – new section.

Chapter 3

- ISBR-1 revised control.
  - Added a requirement that the policy must be maintained. This is a necessary requirement in the continuously changing environment of information security.
- ISBR-2 No changes to control.
  - Reduced implementation guidance.
  - Removed risk assessment methodology.
  - Added process to control handling of risk.
- ISBR-4 Change to control to improve precision.
  - Replaced “segregated” with “segmented”.
- ISBR-5 Revised control.
  - Emphasised the need for training in information security awareness and acceptable use of the ICT systems.
- ISBR-6 Change to control to improve precision.
- ISBR-7 Revised control.
  - Replaced by a reference to ISO 27031 Guidelines for information and communication technology readiness for business continuity.
- ISBR-8 Change to control to improve precision.
- ISBR-10 Change to control to improve precision.
- ISBR-12 Revised control.
  - Focus on security patches.
- ISBR-13 Precision change to control.
- ISBR-14 Revised control.
  - Emphasised that stringent access control management should be in place.
  - Implementation guidance: elements covering remote access moved to new ISBR 18.
- ISBR-17 New.
- ISBR-18 New.
- ISBR-19 New.

Former Appendix A: merged with ISBR chapter to form new chapter 3.
Former Appendix B: examples of PCSS architectures → new Appendix A.
Former Appendix C: moved to chapter 1.2.
New Appendix B: National Institute of Standards and Technology (Nist) cyber security framework (CSF).
New Appendix C: dependency map – ISBR
Introduced to provide a better overview of relationships between ISBRs.

Changes to figures:

- Figures 1 and 2 in former Appendix C removed.
- No changes to Figures 1, 2 and 3 in examples of PCSS ICT architectures.
- Introduced a figure in chapter 3: bow tie illustrating information security functions.
- Introduced a new Appendix C with figure: dependency map - ISBR.

2.3 Revision history

Revision no 01	Revision date: 2006.06.09
Revision no 02	Revision date: 2006.12.01
Revision no 03	Revision date: 2007.04.01
Revision no 04	Revision date: 2008.02.11
Revision no 05	Revision date: 2009.01.15
Revision no 06	Revision date: 2016.11.09

3 INFORMATION SECURITY BASELINE REQUIREMENTS (ISBRS)

Information security measures shall be implemented in PCSS ICT systems. These measures shall be managed in a life cycle perspective, and include both the project phase when solutions are built and the operational phase after solutions have been handed over to operations.

Each ISBR is defined by a control followed by an objective.

This is supported by an implementation guidance. The implementation guidance is structured in accordance with the five main functions for security measures specified by the Nist CSF.

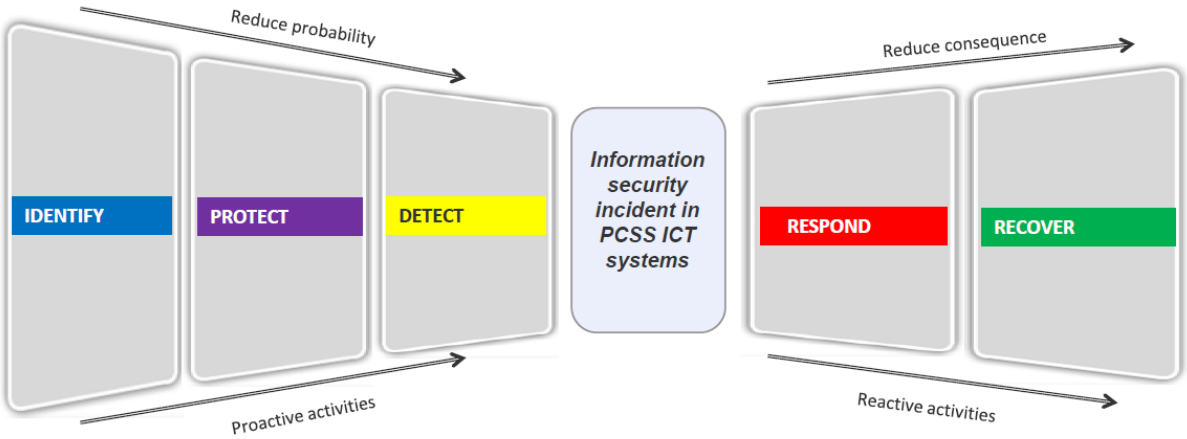

Figure 3.1 illustrating the information security functions.

- **Identify** – develop the organisational understanding required to manage the cyber security risk to systems, assets, data and capabilities. That includes planning and activities required in an early phase, before potential information security incidents can occur. Examples could be asset management and risk assessments.
- **Protect** – develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. That includes measures and activities to protect the actual systems. Examples could be awareness training, access controls and proper network segmentation.
- **Detect** – develop and implement the appropriate activities for identifying the occurrence of a cyber security event. That includes continuous security monitoring and detection processes. Example could be logging and analysis of malicious anomalies and events.
- **Respond** – develop and implement the appropriate activities for responding to a detected cyber security event. Examples could be executing response plans and mitigating actions.
- **Recover** – develop and implement the appropriate activities to maintain resilience plans and to restore any capabilities or services impaired by a cyber security event. An example could be executing a recovery plan.

3.1 ISBR 1 Information security policy

Control: An information security policy for PCSS ICT system environments shall be documented and maintained.

Objective: Ensure that an information security policy is entrenched with the board of directors and senior management.

Implementation guidance
An information security policy is an overall management document which specifies the foundations for information security in the PCSS ICT domain. It describes the management intent and direction for information security.

- **Identify**
  - An information security policy should include the following:
    - the information security objectives for the organisation
    - the organisation's definition of information security
    - principles and strategies
    - the scope of the policy:
      - who – is it for?
      - what – does it cover?
      - where – is it applicable?
    - a framework for risk assessment and implementing security measures and controls
    - describe how information security work is structured in the organisation:
      - roles
      - responsibilities and authorities.
    - information security incidents:
      - definitions
      - requirements for reporting events and handling incidents.
    - references to other security documents.
- **Detect**
  - A process must be defined for reviewing and validating the overall information security policy.
- **Respond**
  - Any changes to the policy need to be validated and approved by management and implemented throughout the organisation.

Links to Nist CSF: ID.GV

3.2 ISBR 2 Information security risk management

Control: An information security risk management process for the PCSS ICT systems and networks shall be in place.

Objective: To ensure that criticality and risks are identified, mitigated or accepted.

Implementation guidance
The risk management process shall cover the risk from identification through assessment, planning and implementation of mitigating action and/or risk acceptance. A process must also be in place to ensure that critical risks are handled quickly when they are identified.

Risk assessments shall identify the likelihood and consequences of security incidents, taking account of the security measures adopted and activities pursued to mitigate potential risks.

A criticality assessment is advisable before conducting a risk assessment. This helps the organisation to prioritise its most critical ICT systems in the PCSS domain. A methodology for and guidance on criticality assessments can be found in Norwegian Oil and Gas guideline 123.

- **Identify**
  - Each risk assessment shall have a defined context.
  - All identified risk shall be documented.
  - Develop a risk mitigation plan
    - identify possible security measures and controls which will reduce unacceptable risks to an acceptable level.
  - Risk acceptance
    - obtain management (risk owner) approval of the residual risk and the implementation plan for the proposed security measures and controls.

- **Protect**
  - Implementation of the risk mitigation plan.
  - Controls must be in place to minimise the number of people with access to information in the risk assessment.

- **Detect**
  - Continual monitoring and review of risk.

- **Respond**
  - Maintain and improve the process for managing information security risk.

Links to Nist CSF: ID.RA and ID.RM

3.3 ISBR 3 System and information owners

Control: PCSS ICT systems shall have designated system and information owners.

Objective: Ensure ownership of PCSS ICT systems in the organisation.

Implementation guidance
The system owner shall have the overall system responsibility and ensure that only authorised applications and services are installed in the PCSS ICT systems**.**

- **Identify**
  The following roles should be identified.
  - System owner
    A system owner is responsible for ensuring that the requirements in this document have been implemented in the PCSS ICT systems. The self-assessment ISBR can be used to identify which controls the system owner should implement.

  - Information owner
    An information owner is responsible for classifying the information and ensuring that relevant protection is implemented.

- **Protect**
  The information and system owners should ensure that all necessary security controls have been implemented and that they are effective and efficient.

Links to Nist CSF: ID.AM and ID.BE

3.4 ISBR 4 Segmented networks

Control: The PCSS ICT infrastructure shall provide segmented networks, and all communication paths shall be controlled.

Objective: To be in control of PCSS ICT systems.

Implementation guidance

- **Identify:**
  - The ICT infrastructure must provide segmented networks, so that PCSS ICT systems with different levels of security, real-time systems which require a guaranteed response time or network throughput, or especially critical systems are installed in logically or physically divided networks. Using the principles in Norwegian Oil and Gas guideline 123 on classification of process control, safety and support ICT systems based on criticality is recommended in order to identify the criticality of the different systems.

- **Protect**
  - PCSS ICT systems shall not be installed in network segments which contain ICT systems running administrative tasks, system development processes or application testing. These shall be physically segmented from each other. Critical PCSS networks shall also be segmented from other PCSS networks.
  - Communication between networks shall always be controlled and logged by firewalls, packet filtering routers or the like. Firewalls should only permit traffic which has been explicitly allowed. All other traffic should be dropped.

- **Detect**
  - Monitor the networks to ensure that only authorised PCSS ICT systems are installed in the production networks and that only authorised and documented services are running in the networks.

Links to Nist CSF: PR.AC, PR.DS and PR.PT

3.5 ISBR 5 User training and awareness

Control: Users of PCSS ICT systems shall be trained in information security awareness and the acceptable use of the ICT systems.

Objective: Ensure that users, administrators and any other individual, including but not limited to third parties, who intend to access ICT equipment supporting and running the PCSS are made aware of the relevant cyber security threats and of the consequences which a breach in cyber security might have on the PCSS ICT systems.

Implementation guidance
The organisation shall ensure that users of PCSS ICT systems are qualified by providing relevant training, which includes how to implement and maintain information security in the systems.

- **Identify**
  - Identify necessary and updated training programmes to address and reflect developments in cyber security threats. Training should include best practice on how to access and use the systems.

- **Protect**
  - Provide training in cyber security threats and how to avoid them for any individual accessing the PCSS offshore and/or on land.
  - Training should be repeated to ensure that personnel are kept up to date with developments in cybercrime.
  - Document that cyber security training for relevant individuals has been completed before access to the PCSS ICT equipment is granted.
  - Build a cyber security culture which focuses on personal involvement with and ownership of cyber security.

Links to Nist CSF: PR.AT

3.6 ISBR 6 Designated use of systems

Control: PCSS ICT systems shall only be used for their designated purposes.

Objective: Ensure that vulnerabilities and associated risks are kept as low as possible.

Implementation guidance
The PCSS ICT system shall be configured for its specific needs. The authorised and tested configuration of the PCSS ICT system shall be documented, and the documentation shall be kept updated.

- **Identify**
  - Only approved software shall be installed.
  - Rules for acceptable use of PCSS ICT systems shall be identified, documented and implemented:
    - PCSS ICT systems shall not be used for general internet access, e-mail and office activities.
    - rules on the use of portable devices (service laptops, smart phones, tablets, USB memory sticks, CDs/DVDs and so forth) shall be developed and complied with.

- **Protect**
  - The ICT equipment configuration should be configured and hardened on the basis of its specific needs – ie, unnecessary services, programmes and other system parameters should be removed or disabled.
  - If mobile equipment is needed to support the PCSS ICT system, approved service laptops and portable devices which need to connect to PCSS ICT systems must be updated with the latest security patches and anti-virus software. Approved USB storage devices and CDs/DVDs must be scanned for malware before being connected to PCSS ICT systems.

Links to Nist CSF: PR.IP and PR.MA

3.7 ISBR 7 Preparedness for disaster recovery

Control: Disaster recovery plans for critical PCSS ICT systems shall be documented, tested and maintained to support the business continuity plans.

Objective: Ability to restore critical PCSS ICT systems through disaster recovery plans to support the business continuity plans (BCP.

Implementation guidance
For guidance on how to implement, maintain and test disaster recovery plans we recommend looking at ISO 27031 Guidelines for information and communication technology readiness for business continuity. It is recommended to align the BCP with the disaster recovery plans through documented expectation to Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Links to Nist CSF: RC.RP, RC.IM and RC.CO

3.8 ISBR 8 Information security in engineering, procurement and commissioning processes

Control: Information security requirements for PCSS ICT systems shall be integrated in engineering, procurement and commissioning processes.

Objective: Ensure that PCSS ICT systems are designed and implemented to support secure operation.

Implementation guidance
As a minimum, the requirements should include the information security baseline described in this guideline document. Vendors, suppliers and contractors must document their degree of compliance.

- **Identify**
  EPC contracts, tenders and other agreements where PCSS ICT systems form part of the scope should include a chapter which describes relevant information security requirements. Contracts should also describe how these requirements will be followed up.

For further detailed guidance, see Norwegian Oil and Gas guideline 110.

Links to Nist CSF: ID.BE and ID.GV

3.9 ISBR 9 Service and support levels

Control: Critical PCSS ICT systems shall have defined and documented service and support levels.

Objective: Ensure system security can be maintained and supported.

Implementation guidance
PCSS ICT systems which have been identified through criticality assessments as critical to operations must have documented solutions for service and support life cycles.

- **Identify**
  - The solution for handling hardware and software problems could be a standby system, a contractual service and/or a support agreement with the developer, the vendor or a service bureau, or a combination of these.
  - The solution should include a description of the required response time for restoring the ICT service, how restoration should be accomplished and all the resources needed to do so.
  - A description of how the support will be delivered should be documented.

Links to Nist CSF: ID.GV and PR.IP

3.10 ISBR 10 Change management and work permit procedures

Control: Change management and work permit procedures shall be followed for all maintenance and changes in the PCSS ICT systems and networks.

Objective: Maintain integrity of the systems.

Implementation guidance
No changes should be made to the PCSS ICT systems infrastructure – ie, any hardware or software – unless a work permit has been issued. Changes should be carried out in accordance with the change management procedures. The latter include, but are not limited to, the following.

- **Identify**
  - Formal approval procedures for all stages of the change process.
  - Implementation plan.
  - Updating of all relevant documentation.
  - Communication and early warnings to all personnel affected and other relevant people.

- **Detect**
  - Pre-checking of product integrity (for software updates and new installations).
  - Pre-evaluation of network and computer capacities (for hardware add-ons, reconfigurations, relocations and replacements).
  - Pre-testing of software in an isolated ICT environment before rollout.
  - Pre-assessment of the possible impact on the security of the installation.

- **Protect**
  - Documentation of a fall-back plan, including roll-back procedures if the change is software-related.

- **Respond**
  - Ensure that the change does not introduce any new information security vulnerability.
  - Verify that the changes are working as intended.

- **Recover**
  - Execute the rollback plan should the change be unsuccessful.

Links to Nist CSF: PR.IP, PR.MA and PR.PT

3.11 ISBR 11 Network topology

Control: An updated network topology diagram, including all system components and interfaces to other systems, shall be available.

Objective: Possess an overview of the way the systems are connected to ensure proper protection.

Implementation guidance

- **Identify**
  - Network topology diagrams for the installed networks need to be produced in order to secure an overview of the way system components in the PCSS ICT systems are connected. The level of detail should make it possible to identify all critical components, such as servers, operator stations, network switches/routers, gateways, telecommunication devices and firewall/security equipment. Relevant information in the topology diagram can include:
    - name/identification of component
    - physical location of the equipment
    - network addresses – eg, IP address
    - description of how components are connected.

    Further details of components should be kept in the asset inventory.
  - Ensure that procedures are in place to keep network topology diagrams updated after each change.
  - Controls must be in place to minimise the number of people with access to restricted information.

Links to Nist CSF: ID.AM and DE.CM

3.12 ISBR 12 Security patches

Control: PCSS ICT systems shall be updated with security patches.

Objective: Reduce vulnerability in PCSS ICT systems.

Implementation guidance
Unpatched ICT systems are vulnerable to malware and unauthorised access, which may affect the integrity and performance of PCSS ICT systems. Security patches should always be implemented when available and approved, unless this introduces a higher level of business risk.

- **Protect**
  - A plan for how and when vulnerable PCSS ICT systems are updated with security patches should be documented.
  - Advice should be sought from the PCSS ICT system vendor concerning the installation of information security patches on the system, to ensure that functionality is not affected.
  - A system which cannot be updated for any reason should be segmented, or other security measures should be applied to protect the vulnerable system.
  - The risk posed by running a vulnerable system as part of the operational environment should be assessed, documented and communicated. Management (the risk owner) should approve continued production with vulnerable systems as part of the PCSS ICT infrastructure.
  - All information security patching should be carried out in accordance with the requirements for change management.

Links to Nist CSF: PR.MA and PR.PT

3.13 ISBR 13 Malicious software

Control: PCSS ICT systems shall have adequate and updated measures to protect against, detect and recover from malicious software.

Objective: Reduce the risk of malware jeopardising the availability and integrity of PCSS ICT systems.

Implementation guidance
Anti-malware software should be configured to update themselves automatically, when updates are available and approved.

- **Identify**
  - Threat and vulnerability information is received and assessed. Systems vulnerable to malware threats must be identified
  - Executable response plans include how to respond to a malware attack (NB: must include a debriefing on lessons learned). Plans must identify competent people trained to handle computer incident response tasks and tools which need to be available for responding to such events. Plan must include procedures for reporting malware incidents to appropriate parties.
  - Executable recovery plans must include how to recover from a possible malware attack.

- **Protect**
  - Vulnerability scans are performed before handover to production (preferably at the factory acceptance test (FAT) stage).
  - Systems vulnerable to malware threats must have updated malware protection installed.
  - Vulnerable systems where malware protection software cannot be installed should be segmented and protected to reduce exposure to malware. Consideration should be given to using network-based intrusion detection systems or other methods for malware detection at the perimeter.
  - Files, storage facilities and computers should be scanned for malware before they are moved to PCSS ICT systems.
  - USB sticks, service laptops and other mobile equipment must be scanned for malware before being connected to PCSS ICT systems.
  - Storage should regularly be scanned for malware (and not just when files are opened).
  - To ensure that the latest malware protection software is in place, this should be updated automatically or included in the relevant maintenance programme.
  - Consider implementation of host or network-based tools for detecting unknown malware.
  - Evaluate the implementation of whitelisting to prevent unauthorised code running.

- **Detect**
  - Computers and networks are logged, monitored and analysed to detect potential malware.
  - A baseline of expected external data flows for users and systems must be established during network operations.
  - Incident alert thresholds are established to detect abnormal activity in relation to the baseline. Unexpected denials in a firewall log, for example, could indicate that malware is seeking to communicate back to an attacker.

- **Respond**
  - Execute the response plan for handling a malware incident.
  - Perform mitigating activities to prevent any expansion (intentional or unintentional) of the malware.
  - Conduct analysis to ensure an adequate response and to support the correct set of recovery activities.
  - Share information in accordance with response plans.

- **Recover**
  - The recovery plan is executed during or after a malware incident.

Links to Nist CSF: PR.PT, DE.AE, DE.CM, DE.DP, RS.RP and RC.IM

3.14 ISBR 14 Access requests

Control: Stringent access control management should be in place to ensure that only authorised users and systems can access information and functionality in PCSS ICT systems.

Objective: Ensure that all access requests are denied unless explicitly granted.

Implementation guidance
The PCSS ICT systems must be configured to give each user access only to the information and functionality that is necessary to perform their work. The overall principle for system access must be that everything is forbidden unless explicitly permitted. System and network access shall always be granted by users who have a higher level of privileges/rights than the recipient, and as the result of a formal authorisation process.

- **Protect**
  - The PCSS ICT systems should be configured to prevent all user access to information, services, applications and peripherals unless the user is specifically authorised to have such access.
  - System and network access should be granted as the result of a formal authorisation process. Authorisation and access rights should be based on the user's business needs.
  - Wherever possible, users should authenticate as individuals. Strong passwords should be enforced, and supplemented by two-factor authentication where required.
  - Authentications on PCSS ICT systems should not be the same as those in the office network domain.
  - Ensure that authorised users only have access to information and functionality in applications and systems.
  - Formal processes for access management must be in place. That includes approving access for new users and removing access for users who no longer need it. User access rights must be reviewed at regular intervals.

Links to Nist CSF: PR.AC

3.15 ISBR 15 Operational and maintenance procedures

Control: Necessary operational and maintenance procedures shall be documented and kept updated.

Objective: Ensure the optimal performance and stability of the PCSS ICT systems.

Implementation guidance
The PCSS ICT systems should be maintained and operated in a structured manner. Operational routines and maintenance schedules, including back-up and restore procedures, should be documented and specified for all system activities. The documentation should be available to authorised personnel only.

- **Identify**
  - Procedures for operation and maintenance of PCSS ICT systems must be described and implemented. That includes system, operational and end-user documentation. An information security incident response plan must be part of this documentation.
  - The system owner should be responsible for ensuring operational and maintenance procedures are documented and kept updated at all times.

- **Protect**
  - Ensure availability of the documentation.
  - Ensure documentation has the proper confidentiality classification.

- **Recover**
  - Backup and restore procedures should be documented for all PCSS ICT systems.

Links to Nist CSF: PR.IP, PR.MA and PR.DS.

3.16 ISBR 16 Reporting information security events

Control: Procedures for reporting information security events and incidents shall be documented and implemented in the organisation.

Objective: Ensure that an information security event is reported and evaluated as efficiently as possible, and that it is classified and handled as an incident in the most efficient possible manner.

Implementation guidance
Organisational responsibilities for handling and managing information security events and incidents shall be clearly described and documented.

- **Identify**
  - All users of the PCSS ICT systems must be familiar with their reporting responsibility, and have a clear line of command for reporting information security events.
  - The following types of information security events should be identified, with attention concentrated on the loss of information integrity, confidentiality or availability:
    - inefficient security measures
    - human error
    - noncompliance with policy or procedures
    - uncontrolled system changes
    - functional error(s) in software or hardware
    - access breach.
  - All reports should be collected and handled in an uniform way, which makes it possible to follow up, report and learn from information security events in accordance with internal and external requirements.
  - A clear escalation path should be defined from the moment when an information security event is reported to the time it has been evaluated and classified as an information security incident and dealt with by the appropriate incident process.
  - A clear communication responsibility and path should be defined for internal and external stakeholders, including the appropriate government authorities.

- **Detect**
  - Report detected events.

Links to Nist CSF: DE.AE, DE.CM and DE.DP

3.17 ISBR 17 Hardware and software inventory

Control: All PCSS ICT hardware and software shall be clearly identified and registered in an inventory.

Objective: Identify PCSS ICT hardware and software in order to achieve and maintain appropriate protection of the integrity of the system and its assets.

Implementation guidance
An asset inventory helps to ensure that effective protection and recovery controls are available. The rationale is that if you do not know what you have, you cannot protect or recover it.

- **Identify**
  - The asset inventory must include all the information required to protect against and recover from information security incidents. Relevant information should include:
    - name of equipment, name and version of software/firmware, licence information, patch level, configuration files and backup/recovery information
    - contact information on the equipment/software manufacturer/vendor/reseller
    - physical address and/or description of the physical location of the equipment
    - network addresses – eg, IP address
    - the hardware configuration – eg, the number, size and type of discs, the amount of memory and the number of network interfaces
    - list of open ports and services being provided
    - list of protocols being transmitted
    - system-owner contact information, pointers to service and support contracts
    - link to relevant operational documentation and maintenance procedures
    - criticality classification (see Norwegian Oil and Gas guideline 123).
  - Network equipment and firewalls should be part of the asset inventory.
  - Controls must be in place to minimise the number of people with access to restricted information in the asset inventory.
  - Information must be complete and kept up to date.

Links to Nist CSF: ID.AM, ID.RA and ID.RM

3.18 ISBR 18 Remote access

Control: Remote access to PCSS ICT systems shall be limited to authorised users, processes or devices, and to authorised activities.

Objective: Ensure that remote access is managed.

Implementation guidance
Remote access shall only be granted by authorised users following a formal authorisation process.

- **Identify**
  - Establish a policy for acceptable use of remote access.
  - Establish documented work processes for remote access.
    - Work processes should describe how to approve access for new users and to terminate access for users who no longer require access (movers and leavers).
    - Work processes should describe how to permit time-limited access based on work orders.
  - Implement a secure remote access solution which supports the policy and work processes.
    - Use an industry-accepted secure architecture when implementing the solution. Only approved secure computers configured for this use should be used. Other computers can connect to a remote access solution which is based on dedicated secured terminal servers configured to act as a secure runtime environment for connecting to the PCSS ICT systems. In such cases, the software which accesses the PCSS ICT systems will run on the secured terminal servers, and not on the client computer accessing the terminal server.
    - The remote access solution should support secure file transfers to avoid the need for temporary USB storage when transferring files to PCSS ICT systems. Files should be scanned for known and unknown malware.
    - The remote access solution should support time-limited on-demand access based on work permits.
  - Consider if it is possible to transfer information to office network environments and allow users to access it there, as an alternative to giving them remote access to PCSS ICT systems.

- **Protect**
  - Ensure that PCSS ICT systems utilise the secure remote access solution – no backdoors may exist. That includes access to ICT infrastructure equipment such as servers, networking equipment and firewalls.
  - For traceability, users should authenticate as individuals and strong authentication (two-factor) shall be enforced. That includes users with privileged access (admin privileges).

- Remote access should be limited to the systems needed to perform the work. Read-only functionality shall be used when this meets business requirements and is supported by the solution.
- Equipment-specific configuration ports (such as out-of-band ports) shall utilise the remote access solution unless they are disabled.

- **Detect**
  - All remote access activity must be logged and auditable.
  - Processes and the remote access solution should be reviewed regularly to ensure security.

Links to Nist CSF: PR.AC and PR.PT

3.19 ISBR 19 Access management

Control: A process for managing access to PCSS ICT systems shall be documented and complied with.

Objective: Ensure that the access control process to the PCSS ICT systems and protected information are described and based on business and security requirements.

Implementation guidance
Access control is the method used to control which people and what resources can access premises and systems, when that can happen, and what type of access is permitted.

Three key aspects are associated with access control: account management and administration, identification and authentication, and user control and authorisation. All three must work together to establish a sound and secure access control strategy.

- **Protect**
  - Account management and administration process.
    - A formal account registration and deregistration process shall be in place (for both authentication and authorisation).
      - A formal user registration and deregistration procedure must be in place as part of the account management and administration process for granting and revoking access to all PCSS ICT systems.
      - Users shall only be given access to the functionality and information they need (and nothing more), based on business requirements (ISBR 14).
      - Normal operation shall not depend on administrator accounts, and no control functions should ever require administrator rights.
    - Access rights shall be reviewed at regular intervals, using a formal process.
      - Unused system default accounts shall be removed or disabled.
      - Access will be removed for users who no longer need it.
      - Supplier “super user” or guest accounts shall be removed or disabled.
  - Control and authorisation of privileged and admin accounts.
    - The allocation and use of privileged accounts (admin users) shall be restricted and controlled.
      - Only authorised users shall be able to create, maintain and delete accounts, including those for administrators, super users and service.
      - Admin accounts shall be used only for configuring systems and not for operational tasks.

- Personnel with administrative rights and access to firewalls, servers, switches and other manageable network devices in a plant shall be kept to a minimum.
- Domain admin accounts should be avoided, and an admin account shall only have the access needed for the intended work.

- Identification and authentication.
  - Deploying a relevant technology for central management of user rights and privileges on workstation and servers is recommended.
  - All PCSS users shall be uniquely identified when they access the system.
  - In the event that a shared login/password is used to access the system, a process should be in place to document and follow up the use of this account through an organisational process, such as a logbook.

Links for Nist CSF: PR.AC

APPENDIX A: EXAMPLES OF PCSS ICT ARCHITECTURES

Many possible ways exist to configure systems and networks in the production environment, and to link the production network to the office network, transfer statistical production data to production planning systems, and enable remote support of the production systems. Three conceptual examples of architectures are provided below.

Example 1 - basic context for PCSS ICT systems

Many automation systems are connected to a company office network for reporting, optimisation and maintenance. As shown in Figure 1, the plant system is located on a dedicated network to reduce interference between plant and office and to avoid uncertified traffic between the networks. The plant system resides in the PCSS domain and consists of automation devices (PLCs), the user interface (HMI), and a selection of servers maintaining data storage, processing and reporting functions. Vendor support can be achieved through a secure remote access solution.

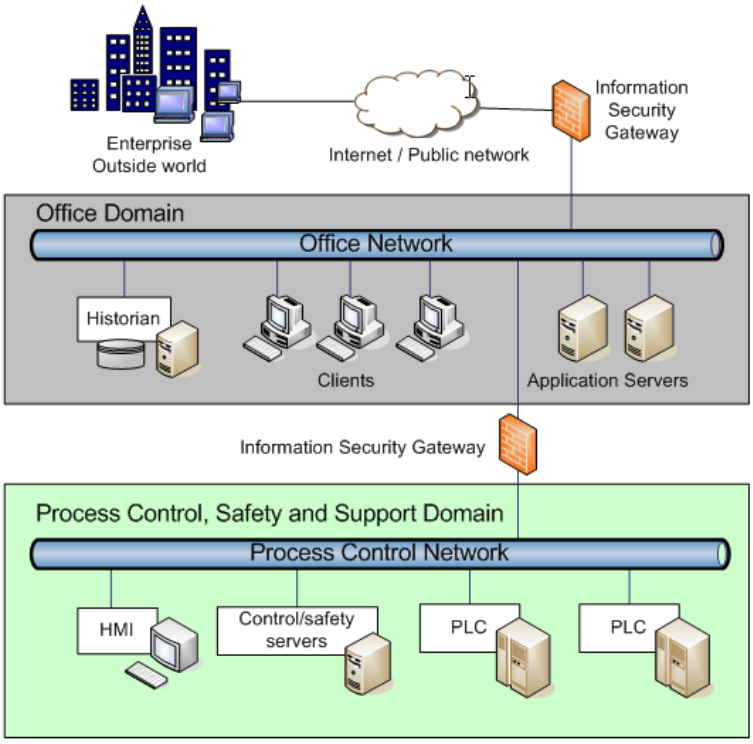

Figure 1: Basic context for PCSS ICT systems.

Example 2 - detailed context for PCSS ICT systems

The configuration in Figure 2 provides a more in-depth look, and details both vendor support and the process control systems. To make the vendor's data communication path even more secure, a private network can be utilised to connect the vendor to the company network.

The process control network is populated with a dedicated control bus hosting the pure process control and safety systems, as well as the other process-related systems not directly required for process control and safety. These systems are not connected to the control bus, but utilise the process control network.

Field devices related to the control functions can be interfaced to the process control system using a field-bus-based system as well as direct connection to the controller.

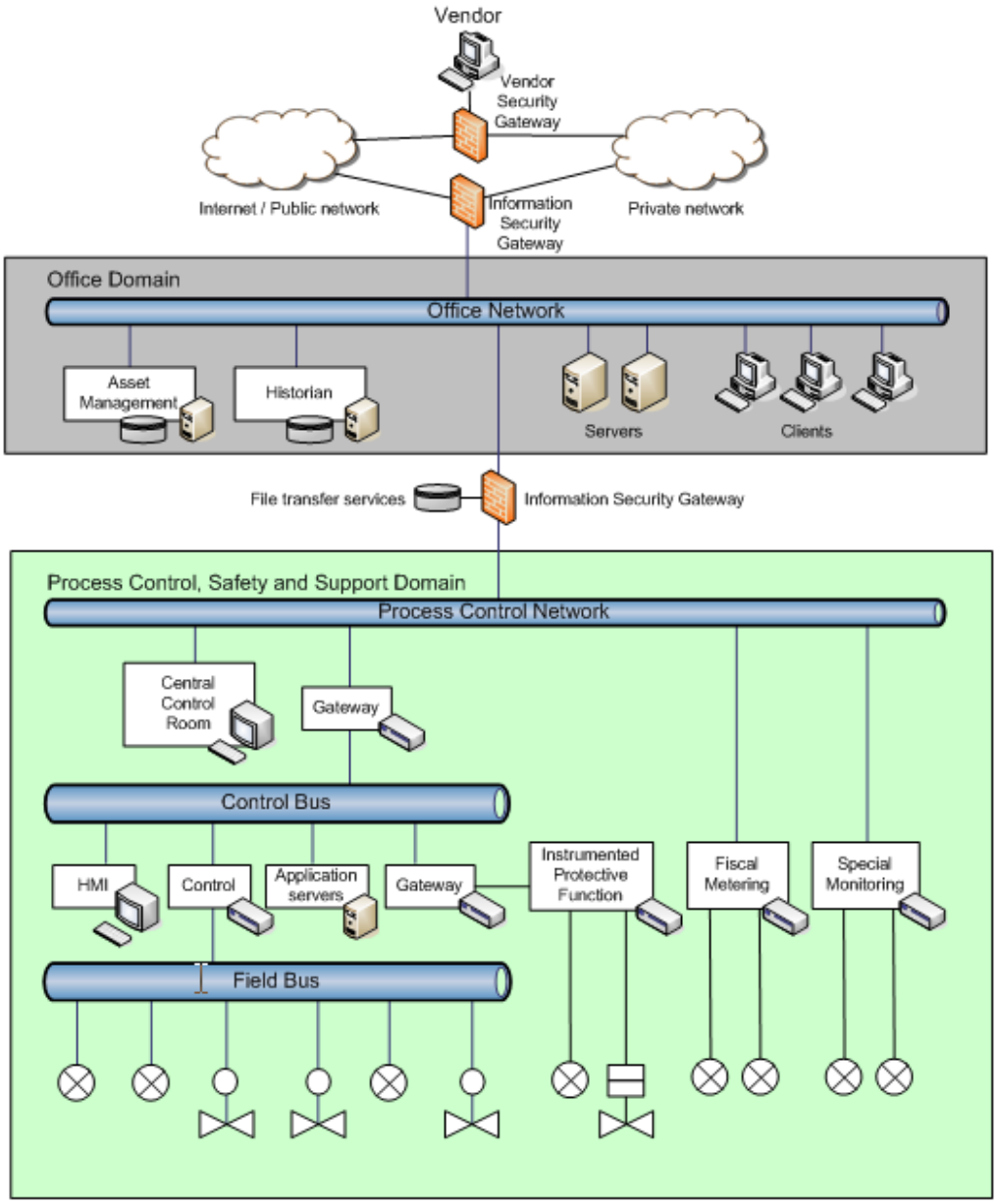

Figure 2: Detailed context for PCSS ICT systems.

Example 3 - enhanced context for PCSS ICT systems

A system configuration of the kind which might be found on an offshore installation is depicted in Figure 3. The production network will typically have a substructure in the PCSS domain consisting of a control bus and a safety bus, and might also have other buses not included in this example.

The safety bus will only support the safety systems, but the control network might support several types of control functions as well as analysers and other special instruments communicating with the control system through the use of networks.

A common user interface is implemented at the process control network level to support safety, process control and other systems operated from the central control room. The process control network is also extended into the company's integrated operational environment.

The system support domain hosts systems for data delivery to the office domain as well as service functions implemented to maintain support of the systems in PCSS domain. All data flows between each domain are controlled and secured using information security gateways.

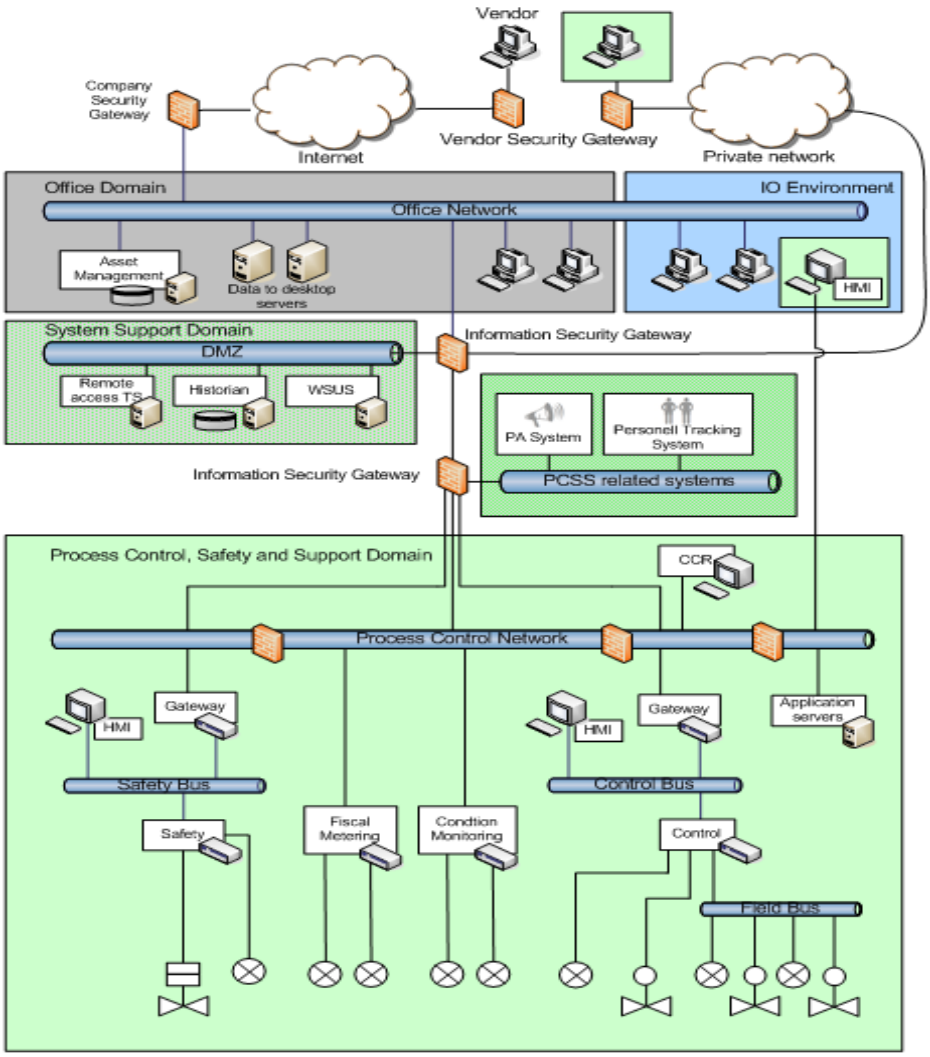

Figure 3: Enhanced context for PCSS ICT systems.

APPENDIX B: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) CYBER SECURITY FRAMEWORK (CSF)

Function	Category
IDENTIFY (ID)	**Asset management (ID.AM):** The data, personnel, devices, systems and facilities which enable the organisation to achieve business purposes are identified and managed consistently with their relative importance to business objectives and the organisation's risk strategy.
	Business environment (ID.BE): The organisation's mission, objectives, stakeholders and activities are understood and prioritised; this information is used to inform cyber security roles, responsibilities and risk management decisions.
	Governance (ID.GV): The policies, procedures and processes for managing and monitoring the organisation's regulatory, legal, risk, environmental and operational requirements are understood, and inform the management of cyber security risk.
	Risk assessment (ID.RA): The organisation understands the cyber security risk to organisational operations (including mission, functions, image or reputation), organisational assets and individuals.
	Risk management strategy (ID.RM): The organisation's priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions.
PROTECT (PR)	**Access control (PR.AC):** Access to assets and associated facilities is limited to authorised users, processes or devices, and to authorised activities and transactions.
	Awareness and training (PR.AT): The organisation's personnel and partners are provided with cyber security awareness education and are adequately trained to perform their information security-related duties and responsibilities consistently with related policies, procedures and agreements.
	Data security (PR.DS): Information and records (data) are managed consistently with the organisation's risk strategy to protect the confidentiality, integrity and availability of information.
	Information protection processes and procedures (PR.IP): Security policies (which address purpose, scope, roles, responsibilities, management commitment and coordination among organisational entities), processes and procedures are maintained and used to manage protection of information systems and assets.
	Maintenance (PR.MA): Maintenance and repair of industrial control and information system components are performed consistently with policies and procedures.
	Protective technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistently with related policies, procedures and agreements.
DETECT (DE)	**Anomalies and events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.
	Security continuous monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cyber security events and verify the effectiveness of protective measures.
	Detection processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
RESPOND (RS)	**Response planning (RS.RP):** Response processes and procedures are executed and maintained to ensure a timely response to detected cyber security events.

	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects and eradicate the incident.
	Improvements (RS.IM): Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RECOVER (RC)	**Recovery planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cyber security events.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centres, internet service providers, owners of attacking systems, victims, other CSIRTs and vendors.

APPENDIX C DEPENDENCY MAP – ISBR