|  |
| --- |
|  |
| Nuclear Industry Security Regulations  Regulation 22 Dutyholder – Evidencing Expectations  Corporate Question Set |



|  |
| --- |
| April 2023 |
| **Nuclear Industry Security Regulations**  **Regulation 22 Dutyholder – Evidencing Expectations**  **Corporate Question Set** |
|  |
| 2023/25874 |

**FSyP 1 - Leadership and Management for Security**

Dutyholders must implement and maintain organisational security capability underpinned by strong leadership, robust governance, an adequate management and accountability of security arrangements incorporating internal and independent evidence-based assurance processes.

|  | **Risk Profile Levels and Question Set Alignment: FSyP1 – Leadership and Management for Security** | | | |
| --- | --- | --- | --- | --- |
| **Associated SyDP** | **Very Low (7 Questions)** | **Low (8 Questions)** | **Moderate (9 Questions)** | **High (2 Questions)** |
| SyDP 1: Security Governance and Leadership | VL1.1: Where are Board roles and responsibilities clearly defined?  VL1.2: Describe how the Board ensures that security is given appropriate prioritisation when providing strategic direction and leadership. | L1.1: What appropriate membership and competence does the Board have to assess and act effectively on security information?  L1.2: What mechanisms are in place to ensure the Board receive current and high-quality security information on threats and risks?  L1.3: Describe what processes are in place so that staff are routinely consulted on security issues. What security competence or experience does the Board have to ensure that this information effectively informs decision making? | M1.1: Describe how security standards and expectations of behaviour for nuclear security are made clear to all stakeholders and contractors from the Board down and how is compliance monitored.  M1.2: What is the Board's strategy for the effective delivery of security and how is this communicated throughout the organisation? | H1.1: Describe how decisions are taken on security matters by the Board based on information gathered from a breadth of sources such as performance indicators, staff feedback, event investigations, independent and self-assessment and how satisfactory quality is maintained. |
| SyDP 1.2: Organisational Security Capability | VL1.3: Describe your competence management system to effectively identify training requirements for all security related roles. | L1.4: Describe how arrangements for security training are effectively resourced, and how the training content is specified and delivered, monitored and course effectiveness assessed. | M1.3: Describe how the culture of the organisation promotes and conducts the transfer of knowledge, particularly tacit knowledge among security personnel, to avoid the risk relating to single points of failure within the organisation.  M1.4: Describe how security related roles are performance managed to ensure that responsibilities are being fully delivered. |  |
| SyDP 1.3: Security Decision Making | VL1.4: Describe how the decision-making process enables prudent and timely security decisions to be made at the appropriate level, by competent personnel with the necessary authority and the means to ensure that their decisions are implemented. | L1.5: What mechanisms in place to involve internal and external stakeholders in the decision-making process?  L1.6: Describe any decision-making processes that allow for a range of potential solutions to be developed and tested. | M1.5: Describe any development programs (e.g. ongoing mentoring, training and assessment) to help improve security decision-making skills.  M1.6: Describe any processes in place to ensure that security intelligence is used to help inform senior decision-making.  M1.7: Describe how security decisions are made in a transparent and auditable way, ensuring that decision makers are accountable for the decisions they make. |  |
| SyDP 1.4: Organisational Learning for Security | VL1.5: What policy mechanisms are in place for systematically identifying and correcting deficiencies in security and describe how staff are encouraged to report them?  VL1.6: Describe how you ensure that lessons are learnt from security events. | L1.7: What mechanisms are in place to encourage reporting of security deficiencies to enable effective root cause analysis? | M1.8: Describe any data analysis conducted to identify internal and external organisation trends or recurring issues, so that proactive measures can be implemented to mitigate these. Include an overview of any. |  |
| SyDP 1.5: Security Assurance Processes | VL1.7: What CS&IA assurance activities are in place to ensure compliance with relevant security policies? | L1.8: Describe how CS&IA security assurance is a key business delivery item. For example, it could be a standing agenda item in Board/management meetings. | M1.9 Describe the assurance processes that informs the Board on the findings of significant security deficiencies including analysis of the event and emerging trends. | H1.2: Describe any security assurance processes to ensure an appropriate level of independence when reporting issues to senior management. |

**FSyP 2 - Organisational Culture**

Dutyholders must encourage and embed an organisational culture that recognises and promotes the importance of security.

|  | **Risk Profile Levels and Question Set Alignment: FSyP 2 - Security Organisational Culture** | | | |
| --- | --- | --- | --- | --- |
| **Associated SyDP** | **Very Low (3 Questions)** | **Low (3 Questions)** | **Moderate (3 Questions)** | **High (2 Questions)** |
| SyDP 2.1: Maintenance of a Robust Security Culture | VL2.1: Describe how CS&IA policies, procedures and guidance are made available to staff and how changes are communicated.  VL2.2: Describe your CS&IA awareness and training programme for new and existing employees and how this takes account of the threat to the civil nuclear industry.  VL2.3: How do leaders and managers check to ensure that the security culture of supply chain partners meets expected standards and expectations? | L2.1: Describe how the security policy is contained within the overall management system and any arrangements to demonstrate that the management system is reviewed and updated periodically.  L2.2: Describe any arrangements in place for sharing the rationale for security decisions with staff where it could impact on the security culture of the organisation.  L2.3: Describe any arrangements in place assess/review security culture. | M2.1: How are threat briefings developed, used, communicated, recorded, reviewed and made available to all relevant staff and contractors?  M2.2: How are lessons learned from internal and external security events and good practice, incorporated into the organisation's security culture?  M2.3: How are cultural initiatives identified and improvements made across the organisation? | H2.1: Describe any arrangements in place to maintain continual assurance of a robust security culture, including any arrangements for addressing any findings.  H2.2: How are internal assurance processes used to validate and effective security culture? |

**FSyP 3 – Management of Human Performance**

Dutyholders must implement and maintain effective arrangements to ensure the human contribution to delivery of security is understood and appropriately designed (to include tasks, competence staffing, workspace, equipment and administrative control), implemented and resourced.

|  | **Risk Profile Levels and Question Set Alignment: FSyP 3 – Management of Human Performance** | | | |
| --- | --- | --- | --- | --- |
| **Associated SyDP** | **Very Low (4 Questions)** | **Low (2 Question)** | **Moderate**  **(0 Questions)** | **High**  **(0 Questions)** |
| SyDP 3.1: Identification and Analysis of Security Tasks and Roles | VL3.1: Describe the organisations approach to identify the tasks and roles relevant to security. |  |  |  |
| SyDP 3.2: Sufficiency and competence of Personnel Delivering Security | VL3.2: Describe the approach to identifying the training needs and subsequent competence management of security related staff.  VL3.3: Describe any initial training programme for all personnel whose duties may impact upon security. | L3.1: How does the organisation ensure it has the sufficient numbers of staff, with the necessary mix of skills, to deliver effective security related to Sensitive Nuclear Information (SNI)? |  |  |
| SyDP 3.3: Suitable and Sufficient Workspaces, Equipment and User Interfaces |  | L3.2: Describe how the organisation ensures that the working environment meets the requirements of staff needs and roles to effectively deliver security outcomes. |  |  |
| SyDP 3.4: Suitable and Sufficient procedures and Administrative controls | VL3.4: Describe how the organisation supports the reliable delivery of security functions regarding the protection of SNI. What procedures and controls are in place to minimise the likelihood of human error. |  |  |  |

**FSyP 7 - Cyber Security and Information Assurance**

Dutyholders must implement and maintain effective cyber security and information assurance arrangements that integrate technical and procedural controls to protect the confidentiality, integrity and availability of SNI and technology.

|  | **Risk Profile Levels and Question Set Alignment: FSyP 7 - Cyber Security and Information Assurance** | | | |
| --- | --- | --- | --- | --- |
| **Associated SyDP** | **Very Low (21 Questions)** | **Low (8 Questions)** | **Moderate (5 Questions)** | **High (1 Questions)** |
| SyDP 7.1: Effective Cyber and Information Risk Management | VL7.1: Describe your approach to managing CS&IA risk in relation to holding of SNI. Provide references and/or an overview of any relevant overarching strategy, resourced plans and appropriate policies. | L7.1: Describe how senior management focus the organisation on prioritising resources towards the greatest risks. |  |  |
| **Scope and Business Objectives** | | | |
| VL7.2: Where are the business objectives for cyber and information risk management defined and where has relevant legislation and regulation been identified?  VL7.3: How is a clear view maintained of where digital and information assets are within the business, including their value? |  | M7.1: Do risk appetite statements for critical business functions exist and how do you ensure that they are appropriate? |  |
| **CS&IA Risk Governance Structure** | | | |
| VL7.4: Who holds responsibility for CS&IA risk management? Clearly identify any key roles and responsibilities for delivery and accountability, including in relation to management of classified contracts. | L7.2: Describe the governance arrangement for any CS&IA policies. Include reference to how policies are endorsed, resourced, made available and monitored for compliance. |  |  |
| **CS&IA Risk Management Approach** | | | |
| VL7.5: Describe your organisational CS&IA risk assessment methodology and associated approach to risk treatment and management of residual risk.  VL7.6: Describe the approach to the communication of risk across the business and how this extends to the supply chain and other external stakeholders, including CAs and/or ONR (where appropriate). | L7.3: Describe how your risk management approach covers the whole lifecycle for the information assets (including suppliers). Include details of how the approach caters for regular risk review, handles change control and how the CA is notified of any relevant or planned changes to the handling of SNI and any associated risks. | M7.2: Describe your process for conducting threat assessments and the relevant sources used to ensure they cover the correct scope.  M7.3: Describe how you gain assurance that security controls are maintained and remain effective. Include any arrangements to ensure that a level of independence is maintained as appropriate. |  |
| **CS&IA Residual Risk Management** | | | |
| VL7.7: Describe how risk managers at all levels understand their role in the governance structure, are empowered appropriately and own, report and/or escalate risk through the life of information assets. |  |  |  |
| SyDP 7.2: Information Security | **CS&IA Policy and Standards** | | | |
| VL7.8: Describe the structure of your organisation's CS&IA policies, procedures and guidance. Provide references for key documents as required.  VL7.9: Describe your processes to identify SNI and associated assets. This should include any arrangements for the maintenance of an information asset register that identifies SNI and relevant equipment and software. |  |  |  |
| **Data Classification and Sensitivities** | | | |
| VL7.10: What arrangements does your organisation have in place to classify and control access to SNI? |  |  | H7.1: Describe the arrangements in place to comply with the Government Security Classification policy, and supporting guidance, at higher sensitivity levels, as appropriate. |
| **Identification of Classified Subcontracts** | | | |
| VL7.11: Describe briefly any classified subcontracts involving SNI that your organisation currently has.  VL7.12: Describe your mechanisms for identifying classified contracts.  VL7.13: Describe your mechanisms for assuring classified contracts to ensure that suitable security controls are implemented and maintained.  VL7.14: Describe the process for identifying SNI and associated assets that will be held and/or generated in third-party contracts. What is the assurance process to ensure they are protected throughout the lifecycle? |  |  |  |
| **CS& IA Assessments and Assurance of Third-Parties** | | | |
| VL7.15: Describe the arrangements used to assess CS&IA maturity for third party companies that may impact upon the security of SNI, such as those providing disposal, storage, managed IT services. | L7.4: How are CS&IA arrangements for third party companies reviewed and assured on a continuing basis?  L7.5: Describe how any third-party supply chain issues are identified and the results of any assessments are reflected into central risk management processes, such as a risk register. |  |  |
| **End of Contract** | | | |
| VL7.16: Describe your processes to manage the closure of contracts with third party companies involving SNI and associated assets. | L7.6: Describe any processes that require evidence of asset transfer and destruction and how this is reflected in asset and risk management registers. |  |  |
| SyDP 7.3: Protection of Nuclear Technology and Operations | **System Classification and Critical Dependencies** | | | |
| VL7.17: Describe your process to identify and categorise sensitive digital assets and systems holding SNI (including dependencies on other assets) that need to be appropriately protected in line with the Government Security Classification scheme and the NISR Classification Policy |  | M7.4: Describe how you ensure that an appropriate and effective categorisation methodology is in place and whether it covers partners, service providers and suppliers. |  |
| SyDP 7.4: Physical Protection of Information | **Physical Security Risk Assessment** | | | |
| VL7.18: Describe the process the organisation uses to identify appropriate physical security measures in order to mitigate specific security risks. | L7.7: Describe how physical security measures are part of a layered approach in order to apply the defence in depth principle. |  |  |
| SyDP 7.5: Preparation and Response to Cyber Security Incidents | VL7.19: Describe your strategy for identifying and managing all types of security incidents. Include brief details of how incidents are logged, reported to (internal and external stakeholders) and any lessons learned processes.  VL7.20: Describe your process for reporting security incidents and matters of interest in compliance with the Nuclear Industry Security Regulations 2003.  VL7.21: Describe your processes to test and exercise your security incident management arrangements, relating to SNI. | L7.8: Confirm that an incident management policy and plan exist and briefly describe how incident response plans are resourced. | M7.5: How do you ensure that the incident response plan is aligned with business continuity and disaster recovery plans. |  |

**FSyP 8 - Workforce Trustworthiness**

Dutyholders must implement and maintain a regime of workforce trustworthiness to reduce the risks posed by insider activity.

|  | **Risk Profile Levels and Question Set Alignment: FSyP 8 – Workforce Trustworthiness** | | | |
| --- | --- | --- | --- | --- |
| **Associated SyDP** | **Very Low (10 Questions)** | **Low (3 Questions)** | **Moderate (6 Questions)** | **High (7 Questions)** |
| SyDP 8.1: Cooperation of Departments with Responsibility for Delivering Screening, Vetting and Ongoing Personnel Security | VL8.1: Describe any processes to demonstrate that your organisation has appropriate internal arrangements in place to ensure that departments work together to implement and maintain effective personnel security arrangements.  VL8.2: Describe how your organisation meets effective National Security Vetting and ongoing personnel security arrangements for the workforce. This should include how the appropriate combination of recruitment checks and vetting is delivered so that the honesty and integrity of potential employees is satisfactorily assessed.  VL8.3: Describe how your organisation implements and maintains on-going personnel security management to remain assured about your employees and contractors; and to mitigate the risks from well-placed insiders. | L8.1: Describe any regular meetings and identification of relevant stakeholders (such as HR, OH and Security) involved in discussing personnel security concerns or policy developments. | M8.1: Describe any collaborative approaches between departments (e.g. HR, OH and Security) to developing and amending relevant policies within the organisation.  M8.2: Describe how HR staff and other relevant stakeholders receive appropriate personnel security training (e.g. CPNI) to raise awareness of personnel security considerations including issues that may indicate a personnel security concern. For example, Right to work training.  M8.3: Describe how the organisation receives management information about usage (trends) of employee assistance programmes and / or reporting hotlines and how this information is used to inform leadership decision making. |  |
| SyDP 8.2: Pre-employment Screening and National Security Vetting | VL8.4: Describe how the organisation has implemented/supported the BPSS process so that it is compliant with at least minimum standards as published in Cabinet Office guidance. If applicable, include an overview of processes that involve overseas criminal record checks and escalation of vetting concerns to the NSV sponsor (usually the Contracting Authority). If this process is conducted externally, explain what due diligence is conducted and how oversight is maintained.  VL8.5: Describe any processes used to determine the level of NSV clearance (where required).  VL8.6: Describe what arrangements exist, as part of the contractor record requirement, to disclose relevant information to the NSV sponsors from personal files, staff reports, sick leave returns and security records that may be of a security interest. |  |  |  |
| SyDP 8.3: Ongoing Personnel Security | VL8.7: Describe how supply chain organisations (required to handle SNI) are initially assessed from a personnel security perspective and how this is assured on an ongoing basis. Include a description of how potential security concerns in the supply chain are identified and discussed between the supply chain and the organisation.  VL8.8: Describe any arrangements that are in place to ensure appropriate actions (e.g. exit interviews, asset and pass recovery) are taken on termination of employment.  VL8.9: Describe any arrangements that are in place to ensure appropriate actions (e.g. access rights and permissions) are taken for staff moving within the organisation.  VL8.10: Describe how employees are supported in dealing with personal challenges that may have an impact upon security in the organisation. | L8.2: Describe how the security department work collaboratively with appropriate departments (e.g. HR, Training) to develop the content of induction programmes, the annual learning and development strategy, and the content of staff surveys.  L8.3: Describe any HR processes that take account of the potential security consequences of HR interventions including exit interviews and where concerns arise, how they discussed with the security department and for NSV holder communicated to the NSV sponsor. | M8.4: Where a clearance has been issued with a caveat or condition of employment, how are you notified and how is that caveat actively managed (such as relevant parties notified, required actions (e.g. requiring a basic disclosure)? How are any outcomes communicated to NSV sponsor?  M8.5: Describe any occupational health processes that take security factors into consideration when considering workforce ailments. Explain how it balances medical confidentiality against disclosure and how any thresholds that the OH representative advise are considered. For NSV holders, describe how applicable information would be shared with the NSV sponsor.  M8.6: Where applicable, describe how the themes of workforce calls to Employee Assistance programmes and Benevolent Funds is shared with HR, OH and security, to support ongoing personnel security programmes and strategy. | H8.1: Describe how NSV holders are made aware/reminded of when they are required to complete Change of Personal Circumstances (CPC) questionnaires.  H8.2: What processes are in place to ensure that requests for a renewal of a NSV clearance are generated in adequate time before the current clearance expires and what reports are run to support the prompt to renew?  H8.3: Describe how NSV holders are made aware of the need to seek travel advice when travelling overseas on either business or pleasure. Who would provide the appropriate briefing, and where required debriefing. How is this information shared with the NSV sponsor?  H8.4: Are all leavers that hold an NSV reported to the NSV sponsor, so that required action can be taken?  H8.5: If applicable, describe any processes to meet the NSV Sponsors requirement to ensure that DV holders complete an Annual Security Appraisal Form (ASAF).  H8.6: Describe any triage process in place for ASAF’s between the NSV sponsor and the organisation so immediate mitigations can be put into place rather than waiting on the completion of the ONR assessment.  H8.7: If applicable, describe how security concerns for NSV holders are managed internally and reported to the NSV sponsor. |