|  |
| --- |
|  |
| ONR Technical Assessment Guide  Effective cyber and information risk management |



ONR Technical Assessment Guide

Effective cyber and information risk management

**Authored by**: Inspector, Cyber Security and Information Assurance

**Approved by**: Superintending Inspector and Head of Profession for Cyber Security and Information Assurance (CS&IA)

**Issue**: 2.1

**Published**: September 2024

**Next scheduled review**: March 2026

**Document reference**: CNS-TAST-GD-7.1

**Record reference**: 2019/135696

Revision commentary

|  |  |
| --- | --- |
| Issue | Description of update(s) |
| 2 | Revisions to RGP from HMG, ONR and the National Technical Authority and alignment ONR Style Guide. |
| 2.1 | Minor update to correct text in text box in section 5.1. |

Contents

[1. Introduction 4](#_Toc177468640)

[2. Purpose and scope 4](#_Toc177468641)

[3. Relationship to licence and other relevant legislation 5](#_Toc177468642)

[4. Relationship to Security Assessment Principles and IAEA Security Standards and Guides 6](#_Toc177468643)

[5. Advice to Inspectors 8](#_Toc177468644)

[References 26](#_Toc177468645)

[Glossary 28](#_Toc177468646)

# Introduction

1. The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) [1]. This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 [2].
2. The term ‘security plan’ is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.

# Purpose and scope

1. This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder’s arrangements for effective CS&IA risk management. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder’s arrangements. It does not prescribe the detail, targets, or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder’s responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.

# Relationship to licence and other relevant legislation

1. The term ‘dutyholder’ mentioned throughout this guide is used to define ‘responsible persons’ on civil nuclear licensed sites and other nuclear premises subject to nuclear regulation. The term is also used to define a 'developer' carrying out work on a nuclear construction site and approved carriers, as defined in the NISR as well as those holding SNI.
2. NISR defines a ‘nuclear premises’ and requires ‘the responsible person’ as defined to have an approved security plan in accordance with Regulation 4 [2]. This regulation includes a requirement to ensure the security of equipment and software used in connection with activities involving Nuclear Material (NM) or Other Radioactive Material (ORM). NISR further defines approved carriers and requires them to have an approved Transport Security Statement in accordance with Regulation 16 [2]. Persons to whom Regulation 22 applies are required to minimise the risk to their holdings of SNI. ONR considers CS&IA to be an important component of a dutyholder’s arrangements in demonstrating compliance with relevant legislation.
3. The HMG publication Government Functional Standard on Security   
   (hereafter termed ‘GovS 007’) [3] describes expectations for security risk management, planning and response activities for cyber, physical, personnel, technical and incident management. It applies, whether these activities are carried out by, or impact, the operation of government departments, their arm’s length bodies or their contracted third parties.   
   The security principles, governance, life cycle and practices detailed within GovS 007 have been incorporated within SyAPs. This ensures that all NISR dutyholders are presented with a coherent and consistent set of regulatory expectations for protective security whether they are related to government or not.
4. The Government Security Classifications document, together with ONRs NISR Classification Policy [4] describe types of information that contain SNI, the level of security classification that should be applied, and the protective measures that should be implemented throughout its control and carriage.

# Relationship to Security Assessment Principles and IAEA Security Standards and Guides

1. The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder’s security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder’s submission demonstrating they have effective processes in place to achieve Security Delivery Principle 7.1 – Effective Cyber and Information Risk Management, in support of FSyP 7 – CS&IA. The TAG is consistent with other Civil Nuclear Security (CNS) TAGs and associated guidance and policy documentation.
2. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) [5] and the IAEA Nuclear Security Fundamentals, Nuclear Security Series (NSS) No. 20 [6].
3. Fundamental Principle L of the CPPNM refers to confidentiality.   
   The requirements for protecting the confidentiality of information, the unauthorised disclosure of which could compromise the physical protection of nuclear material and nuclear facilities. Additionally, Fundamental Principle E of the CPPNM refers to the responsibility of dutyholders to implement a Physical Protection System (PPS). The efficacy of any PPS in the modern digital age is underpinned by the availability and integrity of the computerised systems charged with the delivery of the four objectives.
4. Essential Element 3 of NSS No. 20 covers the legal and regulatory framework and paragraph 3.3 (g) states that it should provide for the establishment of regulations and requirements for protecting the confidentiality of sensitive information and for protecting sensitive information assets [6].
5. The IAEA also publishes Implementing Guides and Technical Guidance where further relevant information can be found relating to protection of information technology, operational technology and SNI.

* NSS No. 23-G - Security of Nuclear Information [7].
* NSS No. 17-T - Computer Security at Nuclear Facilities [8].
* NSS No. 42-G - Implementing Guide Computer Security for Nuclear Security [9].
* NSS No. 33-T - Computer Security of Instrumentation and Control Systems at Nuclear Facilities [10].
* NSS No. 10-G - National Nuclear Security Threat Assessment, Design Basis Threats, and Representative Threat Statements [11].

1. The structure adopted within this TAG acknowledges approaches used within Relevant Good Practice (RGP) examples NIST Risk Management Framework [12] and ISO/IEC 27005 [13] and guidance issued by the National Cyber Security Centre (NCSC) as the UK’s National Technical Authority for Cyber Security [14].

# Advice to Inspectors

1. SNI is information relating to activities carried out on or in relation to civil nuclear premises which needs to be protected in the interests of national security. Information and associated assets comprise of data in various formats (such as digital, hard copy and knowledge) as well as information and operational technology. It is a dutyholder’s responsibility to determine which information and associated assets are considered relevant. However, without consideration of hard copy SNI, computer-based systems that store, process, transmit, control, secure or access SNI should always be included. As well as ONRs NISR Classification Policy [4], Appendix 1 of ONRs TAG on Information Security [15] provides a description of SNI and a flow chart to assist in its identification.
2. Operational Technology (OT) stored or utilised on the premises in connection with activities involving NM or ORM relating to either nuclear safety or nuclear security, should always be considered. Paragraph 4.10 of NSS No. 13 states:

“Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g., cyber-attack, manipulation, or falsification) consistent with the threat assessment or design basis threat.” [16]

1. As a reminder to inspectors, this TAG is a guidance document to ensure consistency in ONR’s regulatory judgements regarding the adequacy of the dutyholders’ arrangements. The inspector should consider if the outcome is achieved irrespective of any methodology or technology presented in this TAG.
2. Information and associated assets, for example, IT and OT, should be resistant to increasingly complex cyber threats and should also be resilient, in terms of being able to recover operational status quickly in the event that these threats are able to impact a system.
3. Designing and embedding a CS&IA risk management methodology or framework facilitates the adoption of a risk informed approach to how the organisation is run. It is the process of understanding what assets the organisation has (and how important they are), how exposed they are to threats and vulnerabilities (the degree of risk), determining organisational tolerance for this risk and then taking steps to mitigate to an approved appetite; This being overlayed by ongoing monitoring and assessment to ensure that desired outcomes are met and to appropriately respond to change e.g., altered threat or tolerance.
4. The approach taken to manage CS&IA risk may exist as one of a suite of activities undertaken by dutyholders when assessing differing categories of risks at a facility. Consideration should be given to how the dutyholder integrates risk management practices and understands/articulates **blended** or **interconnected/holistic** risk between specialisms or disciplines.   
   For example, the impact that CS&IA risks may have on other risks such as nuclear safety should be evident and form part of the overall structured approach to risk management.
5. This TAG provides guidance and advice to help inform the Inspector in exercising their regulatory judgement during assessment activities relating to a dutyholder’s CS&IA risk management processes. It provides a point of reference which draws upon and aligns with RGP (for example, NIST Risk Management Framework [12] and ISO 27005 [13]).
6. Effective cyber and information risk management encompasses all relevant aspects of:

* Preparing the organisation and establishing context for risk management.
* Asset identification and classification.
* Risk assessment, identification, analysis, and treatment.
* Achieving the cyber security posture – Managing risk to approved tolerance.
* Resilience and assurance of controls.
* Ongoing assessment, monitoring and communicating.
* Adaptation of posture in response to changes in the threat environment and or organisational appetite.

## Regulatory expectations

1. The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies arrangements for effective CS&IA risk management.

|  |  |  |
| --- | --- | --- |
| FSyP 7 – Cyber Security and Information Assurance | Effective Cyber and Information Risk Management | SyDP 7.1 |
| Dutyholders should maintain arrangements to ensure that CS&IA risk is managed effectively | | |

1. CS&IA risk management should not be implemented as an isolated or   
   stand-alone activity performed only periodically and only by those in specialist risk or technology related roles. It should be a continual process integrated into all business processes given the pervasive nature of information and technology, and that ownership of these assets is likely to be distributed across all parts of the organisation.
2. Dutyholders should have a mature understanding of CS&IA risks throughout their organisation and the lifecycle of their activities. This is a fundamental aspect of ensuring effective cyber security and one which acts as a prerequisite to the subsequent application of applicable controls. It should be recognised that CS&IA risk management extends beyond information and information/operational technology to include, for example, people and processes.

## Prepare the organisation

1. Dutyholder senior leadership should have defined and approved a strategic approach to the management of CS&IA risk giving consideration to annexes F to J of the SyAPs [1]. The strategy should identify cyber security and information risk obligations upon the organisation, for example, legal and regulatory requirements (which will likely extend beyond those within the remit of ONR), as well as the wider objectives of the organisation.
2. The scope of the strategy should be clearly defined, i.e., to which parts of the organisation its applies and senior leadership should have formally decided organisational risk tolerance or appetite for disruption from CS&IA risk. Consideration should be given to parties outside of the organisation but with whom interaction occurs, for example, suppliers, partners, customers and other third parties.
3. Dutyholders should have taken action to plan and prepare all levels of the organisation to identify and manage their CS&IA risks through employment of a structured risk management methodology or framework. This framework may be aligned to wider enterprise risk management approaches used   
   pan-organisation where these exist, or be bespoke, standalone and specific to CS&IA.
4. The dutyholder should consider how CS&IA risk aligns with wider risk management performed across the organisation. Given the pervasive nature and use of technology, operational technology, and information the dutyholder should consider whether CS&IA risk should be classified as a ‘principal’ or boardroom level organisational risk.
5. The CS&IA risk management methodology should have been designed with clear purpose, giving due consideration to RGP, and be adapted to suit the specific operational requirements of the dutyholder. It should be documented and be used to inform and define the creation of CS&IA risk policy, processes, procedures, standards, and arrangements based on business objectives and proportionate risk management.
6. The roles and responsibilities which must exist to operationalise the CS&IA risk framework should be identified, documented, and approved.   
   Adequate resources should be provided with those in roles aware of their obligations and suitably qualified and experienced personnel (SQEP) to be able to discharge them.
7. When defining roles and responsibilities consideration should be given to where responsibility will reside for leadership and governance of the CS&IA risk framework as well as organisational ownership of assets and any risks identified. Those in roles of responsibility, and those owning CS&IA risks, should be of appropriate status and hold adequate authority to discharge their responsibilities.
8. The design and output from the CS&IA risk framework should be used to inform and instruct dutyholders’ security programmes with any action taken within that programme reflecting prevalent risks and appropriate prioritisation of them.
9. Mechanisms to govern and manage the implementation and operation of the CS&IA risk framework should be designed and documented by the dutyholder.
10. Inspectors should consider:

* Has a CS&IA risk framework been designed, documented, and implemented? Does it align with and form part of the approved security plan?
* Has ownership of the CS&IA risk framework been correctly positioned in the business? Cyber security and information risk should be anchored as a holistic business risk and not positioned exclusively as a technology risk. Are risk/asset owners business leaders or are these roles confined to those working in technology functions?
* Is there clear understanding across the organisation on how CS&IA risks should be identified and managed (which includes oversight, escalation, tolerance, and governance)? Are there ‘lines of defence’ established in the organisational design?
* Is there a clear understanding of how the dutyholder is structured and how it interacts with partners, customers, suppliers and other third parties to identify and manage CS&IA risk?
* Is there clarity over roles and responsibilities for CS&IA risk? Do those with responsibilities understand them and can they evidence that they are discharged? Is there adequate SQEP resource in place?
* Does executive leadership participate in and lead CS&IA risk management and is tolerance understood and reflected in operational practices?
* Is there evidence that governance and leadership activities are understood and take place e.g., regular oversight meetings with appropriately senior personnel?
* Can the dutyholder demonstrate that output from the CS&IA risk framework is used to prioritise business and security investment and resource allocation? Is there evidence of use of artefacts such as risk balance cases or similar?
* Do those with accountabilities in the risk framework have competing or conflicting objectives e.g., cost control? Where these may exist are they recognised, understood, mitigated and managed?

## Asset identification and categorisation

1. Asset categorisation should be performed to inform the dutyholder’s CS&IA risk management framework by determining the adverse impact with respect to the loss of confidentiality, integrity and availability of systems and the information processed by them.
2. Categorisation should provide clarity of how assets are defined. This may involve various categories such as information types, information technology, operational technology, infrastructure, systems, business processes and or individual technology components. The dutyholder may also choose to include characteristics or language to assist in understanding across the organisation, especially outside the technology function.
3. The approach to categorisation should consider guidance within the SyAPs and annexes F and G and ensure that the asset classification schema can record a compliant rating.
4. There should exist a formal and documented process by which assets are to be identified, recorded, categorised, and classified. This should include details of the information asset owner, where the asset resides, arrangements with third parties etc. The process should be repeated to a suitable schedule to ensure the information remains up to date.   
   The classification scheme adopted should consider guidance within SyAPs (and Annexes F and G) [1], and associated TAGs, in particular, guidance within [15] and [17].
5. The classification decision for information assets should be approved by an appropriate individual or decision-making body and there should exist a maintained inventory of organisational information assets (which includes appropriate meta data).
6. The output of the categorisation and classification mechanism should be a clear means/schema by which the dutyholder understands information and information/operational technology, asset ownership and an ability to determine the order of importance of these assets to the safe and secure functioning of the facility.
7. Inspectors should consider:

* Has the dutyholder established a clear means by which information assets have been identified and categorised and is this understood across the organisation?
* Is there clarity over what information assets the dutyholder owns (or has responsibility for), how important they are, and where they are located (stored)/processed/accessed (including when this may be via third parties)? Is the information up to date and resilient?   
  Has consideration been given to characteristics such as resilience, redundancy, back-up requirements etc?
* Is SNI identified and is it understood where and how it is processed?
* Is it clear who owns information assets across the organisation and are owners appropriate, skilled, and empowered to discharge their responsibilities?
* Is there oversight and leadership of any process in place to determine categorisation and classification and ensure that decisions taken are valid?
* Is it clear what assets are involved in the management of NM or ORM?   
  This should include information, information systems, software, operational technology etc.

## Risk assessment and analysis

1. As part of the CS&IA risk framework the dutyholder should have determined a structured and documented process by which risks will be assessed and analysed.
2. The risk assessment and analysis process should also be part of dutyholders’ change management activities and system development lifecycle to ensure that programmes, projects, procurement, and other change activity adequately consider CS&IA risk. This should be as early as possible in the change management and system development lifecycle to ensure that security requirements are understood and implemented by design. Consideration should be given to all stages of the lifecycle, particularly end of life where specific CS&IA risks may exist, for example, secure destruction.
3. The process should be designed to identify threats to the assets within scope of the CS&IA risk framework (threat intelligence led). This should be achieved via established mechanisms of cyber threat analysis/profiling performed by SQEP specialists with knowledge of the facility and with inputs from specialist government and industry bodies with awareness of nuclear operations. Consideration should also be given to guidance within SyAPs and annexes F, G and H.
4. The process should be designed to identify vulnerabilities present or inherent within identified assets, the organisation, and the environment (internal and external). This should be via established mechanisms of cyber vulnerability analysis/profiling performed by SQEP specialists with knowledge of the facility and with inputs from specialist government and industry bodies with awareness of nuclear operations. Consideration should be given to guidance within SyAPs and Annexes H and I.
5. The process should include evaluation criteria capable of determining types and level of impact (harm/consequence) which may occur should threats exploit vulnerabilities causing a loss of confidentially, integrity and or availability. This may involve the use of scenarios. The dutyholder should ensure appropriate coordination between safety and security functions (further guidance is available in [8] and the British Standard (BS) for coordinating safety and cybersecurity within nuclear power plants   
   (BS 62859:2020) [18].
6. The process should include evaluation criteria capable of determining a means of measurement of likelihood that the impact (harm/consequence) will occur. This may involve the use of scenarios.
7. The dutyholder may support implementation of the process through dedicated specialist tooling and or utilise techniques/methodologies aligned with or replicating RGP models (for example, NIST Risk Management Framework [12]).
8. The dutyholder should design the process to consider the inherent risk to the asset (i.e., without consideration of any existent treatment, control baselines or mitigations) and the residual risk to the asset (where consideration is given to existing treatment, control baselines or mitigations). It should be clearly defined within the process how both inherent and residual risk will be captured, measured, and reported.
9. It should be clear who has responsibility for completing risk assessment and analysis across the organisation, how individual or collective assets will be assessed (scope of each assessment) and thresholds defined indicating when they are required.
10. When completing the process, the information sources used should be clearly identified, validated and reliable. These will typically include use of quantitative, qualitative and or semi-qualitative data.
11. The means by which risk assessment and analysis are to be recorded, documented, and approved, and the frequency/conditions for reassessment should be determined as part of the overarching risk assessment process.
12. The risk process should include a means by which outcomes are summarised, categorised and described. This may involve means of identification and prioritisation, for example, title and score.
13. The output of the process should be a register (log) of profiled risks which are descriptively titled and have a means of rating or prioritisation. It should be clear how profiled risks align to assets in scope of them and should include all relevant necessary data, for example, equipment, activities at risk, mitigation, tolerance, current level of risk etc.
14. The dutyholder should review the output from the process and seek to understand themes, possible risk profile aggregation/concentration and or tiers (for example, organisation, mission/business/safety process, or information system level (further guidance is available on the [NIST website](https://www.nist.gov/)) of risk which may exist within and across the organisation. Where these exist the dutyholder should ensure the risk is registered as such and ensure impact and likelihood assessments are commensurate.
15. The dutyholder should consider how they link risk appetite to cyber security and how this is articulated at senior leadership and wider organisational levels. Further guidance is available on the [NIST website](https://www.nist.gov/).
16. Inspectors should consider:

* Is the risk assessment and analysis methodology repeatable, well defined, documented, and understood? Is it appropriate/proportionate to the size of the organisation and is it operated by SQEP personnel?
* Are the risk assessment and analysis process and outputs approved, auditable and is there oversight and assurance activity undertaken by the dutyholder?
* Is the risk assessment and analysis process threat intelligence led? Does the dutyholder have established mechanisms to gather cyber threat analysis etc. from specialist government and industry bodies with awareness of nuclear operations?
* Does the risk assessment and analysis process consider risks from partners, suppliers, customers, and other third parties?
* Are thresholds clearly set and is it communicated for when a risk assessment is needed? Are risk assessments completed by the correct personnel i.e., those who own the underlying asset?
* Does risk assessment and analysis activity take place in change activity such as projects and programmes and system development? Is this activity performed at the correct points to allow early identification of security requirements?
* Is the output from risk assessment and analysis compiled into a risk register or log and is this of suitable quality to understand currency of risks and order of significance? Is this output effectively used in other stages of the cyber security and information risk management framework?
* Does the dutyholder’s risk assessment and analysis process allow for the identification and communication of both strategic risk (those at an organisation or thematic level) and tactical risks (those at system or component level)?
* Is there evidence to show that risk assessment and analysis is repeated to an appropriate cycle or when the environment/tolerances change?
* Have safety requirements been considered as part of the risk assessment process?
* Are processes in place to ensure upward communication if there have been material changes in the threat environment? Is there evidence that this happens?

## Risk treatment – Select

1. As part of the CS&IA risk framework the dutyholder should have determined a structured and documented process by which they will select treatment of identified risks.
2. The output (identified risks) from the risk assessment and analysis process should be progressed for risk treatment decisioning.
3. Selection of appropriate treatment should be prioritised and based upon achieving the determined tolerance/appetite for CS&IA risk.   
   Consideration for both security and safety risk tolerance/appetite should be given. Guidance within the SyAPs and Annex H should be considered by the dutyholder during this activity.
4. An appropriate defence-in-depth approach to risk treatment should be implemented. Security control selection should take account of existing measures, including those employed for physical and personnel security.
5. Risk treatment options will typically fall into either risk modification (reduction), risk retention (acceptance), risk avoidance and or risk sharing (transfer) or combinations thereof. It should be clear which option(s) has been selected and the rationale for this decision described. Decisions should be approved by asset/risk owners and presented to appropriate governance fora.
6. Once the risk treatment has been selected the decision should be recorded and an action plan should be created, documented, and approved.   
   The action plan should as a minimum contain details of any existing controls and additional controls to be applied (for example, baselines/configurations), what level of risk reduction will be achieved by the treatment selection and over what timeframe, the owner of the treatment plan and required resources. The speed and degree of risk reduction achieved through the treatment plan should be commensurate to the gap between the current risk and agreed tolerance.
7. Where risk treatment is to accept the risk, this should be documented   
   (to include details of any compensating controls), approved at a level proportionate to the level of risk and a date set for review.
8. Consideration should be given to the potential for common controls which may be applicable to asset groups, for example, baselines. This may offer the dutyholder an efficient and simplified way of dealing with risks which traverse multiple assets and or environments.
9. Where organisational or thematic risks exist at a strategic tier consideration should be given to risk treatment selection and the appropriate vehicle for implementation.
10. Inspectors should consider:

* Is there evidence of auditing and oversight of the risk treatment process and its effectiveness?
* Are treatment selection decisions documented, appropriate and challenged/approved by SQEP resource through suitable governance mechanisms?
* Are risks selected for treatment correctly prioritised with supporting justification? Are target dates for risk reduction proportionate and reasonable?
* Is there evidence of risk treatment plans being in place and underway for both tactical and strategic cyber security and information risks?   
  Are risks being reduced to clearly defined appetite/tolerance?
* Have baseline controls and or configurations been established for asset categories, types, and environments, for example, cloud? Is there evidence that these are enforced and monitored for exceptions/changes?
* Have adequate SQEP resources been made available to implement the risk treatment action plan?
* Have any accepted risks been correctly documented and approved at an appropriate level? Is approval appropriate? Is there evidence that these risks have been reviewed again at an agreed date?
* Is there evidence to show that policy, standards, and procedures are amended through use of output from the risk framework, for example, when tolerance changes or new threats emerge?
* Do behavioural controls feature as part of treatments considered?   
  Are cultural norms appropriate and or challenged?

## Risk treatment – Implement

1. As part of the CS&IA risk framework the dutyholder should have determined a structured and documented process by which they will implement the selected treatment of identified risks.
2. There should exist a means by which confirmation that the selected risk treatments have been implemented as expected and on time. This should be reviewed by the risk owner and appropriate governance fora.
3. There should exist an independent means of overseeing the implementation of risk treatment to ensure that it is as described and validate that the anticipated risk reduction has been achieved and residual risk does not exceed defined organisational tolerance/appetite.
4. Once risk treatments have been implemented and validated there should exist a means to update risk treatment action plans.
5. Where risk treatment has not been implemented or it does not achieve the expected level of risk reduction there should exist a means to appropriately approve this exception, for example, a waiver or dispensation process.   
   This mechanism should provide details of the exception (including a means to measure the degree of risk introduced by the exception), activity needed to remediate and permitted time within which to do so. The level of required approval should be commensurate to the degree of risk experienced through the exception.
6. Inspectors should consider:

* Is there evidence that risk treatment plans are being implemented and that the target residual risk has been achieved? Are risk owners involved in review and approval?
* Is there adequately SQEP resource in place to review and validate implementation of risk treatment? Is it proportionate to the level of cyber security and information risk within the organisation?
* Is there evidence of exceptions being reported and managed through a structured approval process? How many exceptions are there and what are their materiality? Are they in date?
* Are risks being reassessed as a result of changes in threat level or changes to the organisational environment?

## Assess and review

1. The CS&IA risk framework designed by the dutyholder should have a defined and documented process for performing continuous assessment and review of risk. It should contain validation processes to ensure cyber mitigations are, and remain, effective and achieve the required security outcome through the conduct of regular reviews including cyber risk and vulnerability assessments. Consideration should be given to the guidance within [17].
2. There should exist capability to scan and test the environment to ensure that risk treatments are in place, operating as intended and producing the required outcome. This may be achieved through varying means dependent on the risk treatment, for example, compliance scans to ensure that baseline controls remain in effect for technology and operational technology assets.
3. Compliance monitoring should be performed by design and across all lines of defence, for example, operations, risk, and internal regulation/audit.
4. Adequate SQEP resource should be in place to perform continuous oversight and this activity should take place against a defined assessment plan/schedule which is proportionate and prioritised to levels of cyber security and information risk.
5. Actions identified within assessment reports should be rated, reviewed, approved, and actioned with confirmation of closure being reported to appropriate governance fora.
6. The risk register should be updated to reflect output from ongoing assessment reports with risk assessment and analysis repeated if necessary to ensure that the risk is correctly understood and documented.
7. CS&IA risk management should be embedded across all organisational functions and managed as an ongoing iterative activity It should not be seen or actioned as a standalone task performed periodically.
8. Inspectors should consider:

* Can the dutyholder produce a schedule or plan of assessment of risk action management action plans? Is there evidence that these are carried out and that any issues identified are actioned?
* Is there evidence of oversight of cyber security and information risk performed by other lines of defence such as internal regulatory function or audit?
* Does there exist a governance body where reports are reviewed, and actions approved? Are attendees of this forum appropriate in terms of role and seniority?
* Is there evidence that cyber security and information risk as a process is embedded across the business and that asset and risk owners are appropriate (with the risk not being anchored in technology)?

## Authorise, communicate and consult

1. The CS&IA risk framework designed by the dutyholder should have a defined and documented governance process. This should, where possible align with wider business/risk governance arrangements across the organisation.
2. The governance process should show how the Board (as the ultimate accountable body) oversees the management of CS&IA risk and how it delegates authority to sub-committees and individuals. The parameters, roles and responsibilities of these positions and fora should be documented and approved by the Board, for example, through terms of reference and or job/role descriptions.
3. The approach to CS&IA assurance/governance should be communicated across the organisation.
4. The suite of policies relating to CS&IA risk management (informed by output from the risk framework) should be reviewed and approved by the Board and updated to an agreed schedule or when environmental changes/new information require.
5. The Board should review, approve and communicate organisational tolerance/appetite for CS&IA risk. This should be documented and recorded with review occurring to an agreed schedule or when environment changes/new information require.
6. Baseline configurations and controls (i.e., policy, procedures, standards, etc.) for assets in scope of the CS&IA risk framework should be documented, reviewed, and agreed through a formal auditable process overseen by an appropriate governance body. These should be reviewed to an agreed schedule or when environmental changes/new information require.
7. There should exist a means by which change activity (i.e., plant modifications, projects, programmes, etc.) is reviewed and approved to ensure any CS&IA risks have either been managed to agreed tolerance/appetite or have been recorded and scheduled for future treatment.
8. Any change activity which results in the amendment of assets (new or removed), or personnel should be reflected within the CS&IA risk framework.
9. The Board should regularly communicate its strategy for the management of CS&IA risk to all employees.
10. There should be mechanisms in place to ensure that CS&IA risk is regularly communicated to all employees and that there is clarity on how employees can contribute to risk reduction. This should include consideration of how risk will be communicated in emergency situations.
11. Employees (and other relevant personnel, i.e., contractors, third party personnel, etc.) should be supported with structured and regular education and awareness training on CS&IA risk, for example, at onboarding and annually. They should be aware of how they can report risks and be encouraged to do so in line with other reporting frameworks which may exist in the organisation.
12. Those in specific roles within the CS&IA risk framework should be aware of this responsibility and provided with appropriate information/outputs and support through structured education and awareness training.
13. There should be regular communications on CS&IA risk management to stakeholders. These should be targeted to audience types, for example, all staff, asset owners, procurement teams, network/system administrators, approvers of system access etc. External stakeholders, including ONR, should also be considered as part of the communications plan.
14. The CS&IA risk framework designed by the dutyholder should include a structured and specifically designed management information reporting model. The model should be approved by the Board and aid their governance activities.
15. The management information reporting model should show how performance of the risk framework is to be measured and reported and to whom. It should detail how the reporting ecosystem will work and include detail such as what reports will be created, their purpose, frequency of generation, who has responsibility for report creation, metrics/key performance, or risk indicators etc. Consideration should be given to reporting requirements to and from external stakeholders and partners   
    (i.e., service providers, supply chain entities, regulatory bodies, etc).
16. The Board should define what information it wishes to receive and to what frequency. This should include details of key performance indicators (KPIs) or key risk indicators (KRIs) which allow understanding of performance against agreed risk tolerance/appetite.
17. The management information reporting model should align with and support the defined governance model within the CS&IA risk framework.
18. When CS&IA risks are recorded, they should be articulated in a way which allows understanding by all those involved in their management up to and including Board. Complex and specialist language should be used cautiously. It should be clear what the risk is and actions to manage it should be clear and measurable.
19. As the CS&IA risk framework is operated there should be means by which the dutyholder regularly consults with employees and other stakeholders (i.e., service providers, etc.) to assess its effectiveness.
20. Consideration should be given to overall CS&IA culture prevalent within the organisation and how this will be measured. Thought should be given to potential for risk bias/pre-disposition and other human factors which may inhibit the organisation’s ability to determine a mature and transparent view of CS&IA risk posture.
21. Inspectors should consider:

* Is there an effective means by which CS&IA risk is governed across the organisation? Is there transparency of the risks that exist and is valid information on risk status being provided into the Board?
* Is there evidence that senior leadership are aware CS&IA risk and directing appropriate and timely response?
* Do risk managers/owners at all levels understand their role in the governance structure, are the empowered appropriately and are there structured escalation paths?
* Is the suite of MI reporting comprehensive and does it articulate risk clearly and to the right people? Are there clear KPIs at all levels of reporting which allow understanding of risks faced by the organisation?
* Do risk owners understand the risks they own and levels of residual risk? Have they approved these and do they receive regular reporting to enable ongoing monitoring of risk posture?
* Are governance meetings and management information reporting held and to an appropriate frequency? Is there evidence meetings are held, and decisions recorded? Do the governance sessions adequately measure progress of risk management and hold people to account?
* Have risks been recorded and reported in a clear way reflecting tiering e.g., strategic and or thematic risks ranging through to operational tactical risks?
* Does the prevalent organisational culture at all levels (i.e., leadership and operations) allow for CS&IA risks to be openly communicated and recorded in a transparent and appropriate way, and without influence which may unduly suppress understanding of the degree of CS&IA risk the organisation is exposed to?

## Monitor

1. The dutyholder should perform regular monitoring to ensure that the CS&IA risk framework is embedded and operating as intended i.e., that CS&IA posture is as expected. Alterations in approach should be taken where performance is found to be suboptimal.
2. There should exist a clear and documented process which defines response procedures when identified risks and or key performance or risk indicators exceed agreed tolerance/appetite. It should be clear at what point activity is triggered and who has responsibility for enacting this.
3. There should be arrangements in place to continuously monitor the internal and external environments for changes to threats and or vulnerabilities and their potential effect on impact and likelihood. Where these occur risk assessment and analysis should be updated/invoked to ensure that captured risks are accurate and up to date.
4. Changes to business activities and or objectives should be continuously monitored, and consideration given to whether these require amendment to the CS&IA risk strategy.
5. The dutyholder should continuously monitor changes to legal and regulatory requirements as well as updates to RGP and ensure that their CS&IA risk framework remains fits for purpose.
6. Where CS&IA risks crystalise there should be post incident and root cause analysis to determine whether the risk strategy remains appropriate and whether changes to the risk framework are necessary. In such instances dutyholders are encouraged to share learning with other relevant organisations, including where appropriate, regulatory bodies, for example, ONR.
7. Inspectors should consider:

* Is there evidence that the dutyholder regularly reviews the risk framework and makes alterations in response to changes in legal, regulatory, and RGP?
* Are there resources in place with adequate SQEP to assess changes to the internal and external environments (threats and vulnerabilities)?
* Is there evidence that when tolerances are exceeded response action is successfully invoked?
* Is post incident and root cause analysis performed and is this reflected in changes to the risk framework?

## CS&IA management for classified contracts

1. Where dutyholders have classified contracts, they should ensure there are contractual arrangements that enable both pre and in-contract assurance activities and assessment of CS&IA arrangements to ensure the risk to SNI is minimised.
2. Contractual arrangements should also be in place to support the redress of any deficiencies arising during the contract.
3. Decisions by third parties to manage residual risk should be reported back, and be incorporated into, the dutyholder’s own CS&IA risk framework.
4. Dutyholders should be able to determine and satisfy themselves that delivery partners, service providers and third parties are applying adequate security controls to mitigate risks to the information and associated assets that they are responsible for.
5. Dutyholders should also ensure that contractors are made aware of the legal obligations arising from the processing, storage and handling of SNI, and as a minimum be guided on the expectations of the NISR Classification Policy [4] and relevant regulatory expectation within SyAPs.
6. Dutyholders should make provision to manage the risks for access by subcontractors to information and associated assets. The risks from sub-contractors should be accommodated in the organisation’s risk management process and the residual risk reporting mechanism should include summaries from sub-contractors. Further guidance on risk management of information held by sub-contractors can be found in [15] and IAEAs publication on the computer security approaches to reduce cyber risks in the nuclear supply chain [19].

# References

|  |  |
| --- | --- |
| [1] | ONR, “Security Assessment Principles (SyAPs) for the Civil Nuclear Industry (Version 1),” 2022. [Online]. Available: https://www.onr.org.uk/media/g05fszjn/security-assessment-principles.pdf. |
| [2] | HM Government, “The Nuclear Industries Security Regulations 2003 (NISR),” 2003. [Online]. Available: https://www.legislation.gov.uk/uksi/2003/403/contents/made. |
| [3] | HM Government, “Government Functional Standard GovS 007: Security,” 13 September 2021. [Online]. Available: https://www.gov.uk/government/publications/government-functional-standard-govs-007-security. |
| [4] | ONR, “ONR-CNSS-POL-001 - NISR 2013 Classification Policy for the Civl Nuclear Industry,” November 2021. [Online]. Available: https://www.onr.org.uk/documents/classification-policy.pdf. |
| [5] | IAEA, “Convention on the Physical Protection of Nuclear Material (CPPNM),” May 1980. [Online]. Available: https://www.iaea.org/sites/default/files/infcirc274r1.pdf. |
| [6] | IAEA, “Nuclear Security Series No. 20 - Objective and Essential Elements of a State’s Nuclear Security Regime,” 2013. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590\_web.pdf. |
| [7] | IAEA, “Nuclear Security Series No. 23-G IAEA Implementing Guide: Security of Nuclear Information,” 2015. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1677web-32045715.pdf. |
| [8] | IAEA, “Nuclear Security Series 17-T - Computer Security at Nuclear Facilities,” 2021. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1921\_web.pdf. |
| [9] | IAEA, “Nuclear Security Series No. 42-G - Implementing Guide Computer Security for Nuclear Security,” 2021. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918\_web.pdf. |
| [10] | IAEA, “Nuclear Security Series No. 33-T - Computer Security of Instrumentation and Control Systems at Nuclear Facilities,” 2018. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/P1787\_web.pdf. |
| [11] | IAEA, “Nuclear Security Series 10-G - National Nuclear Security Threat Assessment, Design Basis Threats, and Representative Threat Statements,” 2021. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/P1926\_web.pdf. |
| [12] | NIST, “Risk Management Framework,” 7 February 2023. [Online]. Available: https://csrc.nist.gov/projects/risk-management/about-rmf. |
| [13] | ISO, “ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks,” 2022. |
| [14] | NCSC, “Risk management guidance,” 16 November 2018. [Online]. Available: https://www.ncsc.gov.uk/collection/risk-management-collection. |
| [15] | ONR, “CNS-TAST-GD-7.2 - Information Security”. |
| [16] | IAEA, “Nuclear Security Series No. 13 - Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5),” 2011. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481\_web.pdf. |
| [17] | ONR, “CNS-TAST-GD-7.3 - Protection of Nuclear Technology and Operations”. |
| [18] | BSI, “BS IEC 62859:2020 - Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Coordinating Safety and Cybersecurity,” 2020. |
| [19] | IAEA, “Non-serial publication (ref.: IAEA-TDL-011) - Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain,” 2022. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/TDL-011web.pdf. |

# Glossary

|  |  |
| --- | --- |
| CPPNM  CPS  CS&IA  FSyP  HMG  IAEA  ISO  NCSC  NISR  NIST  NM  NSS  NTA  ONR  ORM  PSS  RGP  SIRO  SNI  SPF  SyAP  SQEP  TAG | Convention on the Physical Protection of Nuclear Material  Cyber Protection System  Cyber Security and Information Assurance  Fundamental Security Principle  His Majesty’s Government  International Atomic Energy Agency  International Standards Organisation  National Cyber Security Centre  Nuclear Industries Security Regulations  National Institute of Standards and Technology  Nuclear Material  Nuclear Security Series  National Technical Authority  Office for Nuclear Regulation  Other Radioactive Material  Physical Protection System  Relevant Good Practice  Senior Information Risk Officer  Sensitive Nuclear Information  Security Policy Framework  Security Assessment Principle  Suitably Qualified and Experience Personnel  Technical Assessment Guide |