1

ONR GUIDE			
EFFECTIVE CYBER AND INFORMATION RISK MANAGEMENT			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNS-TAST-GD-7.1 Revision 1		
Date Issued:	March 2020	**Review Date:**	March 2023
Approved by:	Paul Shanes	Professional Lead (cyber security)	
Record Reference:	CM9 Folder 4.4.2.23373. (2019/135696)		
Revision commentary:	Fit for purpose review of Revision 0		

TABLE OF CONTENTS

© *Office for Nuclear Regulation, 2020*
If you wish to reuse this information visit www.onr.org.uk/copyright for details.
Published 03/20

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 7). 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 (Reference 1).

1.2 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.

2. PURPOSE AND SCOPE

2.1 This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder's cyber and information risk management processes. 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.

3. RELATIONSHIP TO RELEVANT LEGISLATION

3.1 The term 'dutyholder' mentioned throughout this guide is used to define 'responsible persons' on civil nuclear licensed sites and other nuclear premises subject to security regulation, a 'developer' carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI.

3.2 NISR defines a 'nuclear premises' and requires 'the responsible person' as defined to have an approved security plan in accordance with Regulation 4. It further defines approved carriers and requires them to have an approved Transport Security Statement in accordance with Regulation 16. Persons to whom Regulation 22 applies are required to protect SNI. ONR considers CS&IA to be an important component of a dutyholder's arrangements in demonstrating compliance with relevant legislation.

4. RELATIONSHIP TO IAEA DOCUMENTATION AND GUIDANCE

4.1 The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 4) and the IAEA Nuclear Security Fundamentals (Reference 3). Further guidance is available within IAEA Technical Guidance and Implementing Guides.

4.2 Fundamental Principle L of the CPPNM refers to confidentiality and details that the State should establish requirements for protecting the confidentiality of information, the unauthorised disclosure of which could compromise the physical protection of nuclear

material and nuclear facilities. The importance of issues relating to CS&IA is also recognised in the Nuclear Security Fundamentals, specifically:

- Essential Element 3: Legislative and Regulatory Framework – 3.3 The legislative and regulatory framework, and associated administrative measures, to govern the nuclear security regime:
  - Provide for the establishment of regulations and requirements for protecting the confidentiality of sensitive information and for protecting sensitive information assets.
  - Ensure that prime responsibility for the security of nuclear material, other radioactive material, associated facilities, associated activities, sensitive information and sensitive information assets rests with the authorised persons.
- Essential Element 12: Sustaining a Nuclear Security Regime – 3.12 A nuclear security regime ensures that each competent authority and authorised person and other organisations with nuclear security responsibilities contribute to the sustainability of the regime by:
  - Routinely performing assurance activities to identify and address issues and factors that may affect the capacity to provide adequate nuclear security, including cyber security, at all times.

4.3 A more detailed description of the elements is provided in Recommendations level guidance, specifically Nuclear Security Series (NSS) 13, Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) (Reference 2). Paragraphs 3.53 to 3.55 specifically refer to issues relating to confidentiality.

4.4 The IAEA also publishes Implementing Guide NSS No. 23-G 'Security of Nuclear Information' (Reference 8) and Technical Guidance NSS No. 17 'Computer Security at Nuclear Facilities' (Reference 9).

5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS

5.1 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 TAGs and associated guidance and policy documentation.

5.2 The HMG Security Policy Framework (SPF) (Reference 5) describes the Cabinet Secretary's expectations of how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. The security outcomes and requirements detailed in the SPF have been incorporated within the SyAPs. This ensures that dutyholders are presented with a coherent set of expectations for the protection of nuclear premises, SNI and the employment of appropriate personnel security controls both on and off nuclear premises.

5.3 The Classification Policy (Reference 6) indicates those categories of SNI, which require protection and the level of security classification to be applied.

6. ADVICE TO INSPECTORS

6.1 The approach taken to cyber and information risk management can be considered to be one of a suite of risk management activities by dutyholders when assessing risks at a facility. This guidance provides specific information that is applicable to CS&IA risks to assist dutyholders demonstrate that adequate arrangements are implemented. It is important to recognise that these arrangements may need to be different from those used to manage nuclear safety risks, although there is likely to be benefit in selecting measures that enhance both cyber security and nuclear safety resilience.

6.2 Information in all its forms and the systems that operate with it, are a critical element in civil nuclear operations. These operations attract risk and it is essential therefore that dutyholders know what information and associated assets they are responsible for, where they are, and to have mechanisms in place so that they can make informed, practical and business-enabling risk management decisions.

6.3 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 security. Information and associated assets comprise data in various formats (such as digital, hard copy and knowledge) as well as information technology and operational technology (equipment or software). It is a dutyholder's responsibility to determine which information and associated assets are considered relevant. However, hard copy SNI, as well as computer based systems that store, process, transmit, control, secure or access SNI, should always be included. Technology stored or utilised on the premises in connection with activities involving nuclear or other radioactive material relating to either nuclear safety or nuclear security, should also always be considered. Appendix 1 of TAG 7.2 provides a description of SNI and a flow chart to assist in its identification.

6.4 The risk management process comprises a number of stages (see Figure 1) and these have to be tailored to the context in which they operate, accordingly there is no single approach that fits all circumstances. Managers in the organisation should recognise this and utilise those elements of relevant good practice in risk management that suit their specific environment.

6.5 A key aspect in effective cyber and information risk management is proportionality. Risk management is an ongoing process so whilst auditable evidence of risk management is essential, the level of documentary evidence should be proportionate to the complexity and level of risk for the system.

6.6 Effective cyber and information risk management encompasses all relevant aspects of:

- Identifying the scope (which may include business objectives).
- The CS&IA risk governance structure.
- Defining the risk assessment approach.
- Specifying the conduct of risk treatment.
- Managing residual risk.
- CS&IA risk and information management for classified contracts.

Regulatory Expectations

6.7 The regulatory expectation is that the dutyholder will ensure that the security plan clearly details their approach to cyber and information risk management in support of maintaining effective CS&IA arrangements.

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.		

7. SCOPE AND BUSINESS OBJECTIVES

7.1 Dutyholders should have a clear understanding of their own business context in terms of what the major elements of the organisation are and how they interact with partners, customers and supply chain companies. A diagram is often a useful way of clearly communicating this context.

7.2 The description of context should be used to show at a high level where information and associated assets are likely to be located. This view should include partners and all third-parties. The objective is that the business understands how it operates, who with and where information is being transferred, processed or stored. Further guidance is available in TAG 1.2 – Organisational Security Capability.

7.3 Smaller organisations within scope of NISR Regulation 22 (including third-parties) should consider a similar approach with a document or portfolio that summarises the business context of their organisation, business scope and business objectives. This can also be used to cover other topics in this guidance but may be less detailed than that for larger dutyholders holding larger quantities of SNI, particularly of higher classifications.

7.4 Dutyholders should have defined business objectives for cyber and information risk management. Where practicable, statements of risk appetite should be produced for major business functions and each of these will support a risk management objective. Annexes F to J of the SyAPs provide a framework of Cyber Protection System (CPS) outcomes and postures linked to a set of response strategies from which appropriate objectives and risk appetites should be derived.

7.5 Organisations should have a clear understanding of what legal and regulatory requirements are relevant to their business and what their obligations are. It is essential that these obligations are fully reflected within the scope of the business objectives.

Inspectors should consider:

- Is there a clear understanding of how the organisation is structured and how it interacts with partners and suppliers?
- Is there a clear view of where information and associated assets are within the business?
- Have the business objectives for cyber and information risk management been defined?
- Are there risk appetite statements for critical business functions?

- Do the business objectives and risk appetite statements align with the framework provided in the SyAPs annexes?
- Has relevant legislation and regulation been identified?

8. CS&IA RISK GOVERNANCE STRUCTURE

8.1 Dutyholders should establish and operate an appropriate cyber and information risk governance structure. This should be adequately resourced with suitably trained personnel who are empowered to deliver effective risk management at the appropriate level in the organisation, TAG 1.1 - Governance and Leadership and TAG 1.3 – Security Decision Making, provide further detail.

8.2 The risk governance structure should identify appropriate levels in the business where risk management decisions should be made. For example the SIRO is the Board level representative for information security but while that role is accountable for risk management, the incumbent is not expected to make all risk management decisions. Accordingly, levels of risk management responsibility should be mapped to corresponding management roles and this may be down to lower levels in the organisation. As far as possible the risk governance structure should be part of the business governance structure so that risk management is part of normal management functions.

8.3 It is important that the risk governance structure is understood by all of those operating it and that paths for escalation of decisions to the next level are clear, understood and followed by all.

8.4 Where roles for the management of information risk have been identified, these should have terms of reference that identify the scope, responsibilities, authority, reporting chain, qualifications and training requirements for that role.

8.5 The risk governance structure should be underpinned by a comprehensive CS&IA Policy. This policy should accord with the scope identified in paragraph 6.6 and should meet the cyber and information risk objectives defined in paragraph 7.4.

8.6 The CS&IA Policy should be supported by processes and procedures that ensure it is implemented effectively throughout the organisation. The policy may be aligned to relevant security and management certification standards such as ISO27001, which normally provide extensive guidance on implementation.

8.7 The CS&IA Policy should be available to all personnel and should be maintained. Updates and changes should be clearly communicated to all personnel.

8.8 The effectiveness of the CS&IA Policy should be monitored and reported on.

Inspectors should consider:

- Is it clear throughout the organisation who has responsibilities for risk management?
- Have the key roles identified at paragraph 8.2 been filled and are the details current?
- Is there evidence that post holders are suitably qualified and experienced for the role?
- Is there a CS&IA Policy and is it appropriate to the organisation?
    - Is it current and has it been endorsed by the Board?

- Is it resourced adequately?
- Is it easily available to all personnel (to include partners and suppliers as necessary)?
- Is there a mechanism for communicating updates?
- Is there a monitoring, review and reporting process to identify either areas of weakness or non-compliance?

9. CS&IA RISK MANAGEMENT APPROACH

9.1 Dutyholders should ensure that they have a mechanism and the competent personnel to give them a mature understanding of the CS&IA risks throughout their organisation. This mechanism should include a current and comprehensive register of the location and 'value' of all information and associated assets (which includes individual documents and other assets that are SECRET or above) and adequate mechanisms to identify and analyse all cyber threats, vulnerabilities and potential impacts. Annexes F to J of SyAPs give further information on categorisation, security outcomes, postures and response strategies for a CPS.

9.2 Dutyholders should have a defined approach to proportionate risk management which supports business objectives and which reduces the risk to information and associated assets. One way of achieving this is a CS&IA Risk Management Strategy that defines the organisation's approach to managing cyber and information risks. Part of this strategy document should outline what the proposed processes for risk assessment, risk treatment and residual risk management are.

9.3 The scope of this strategy should be aligned to that defined in paragraph 6.6 above and it is important that the strategy considers risks to information and associated assets held by partners and supply chain companies.

9.4 Cyber and information risk management should be aligned with the wider business risk management as far as practicable. Managers should see CS&IA as part of their role, not something separate to it conducted by someone else.

9.5 The cyber and information risk management process should include mechanisms for feedback and performance management to support continuous improvement.

Figure 1 – Overview of a CS&IA Risk Management Process[1]

9.6 The risk management approach should be aligned to the lifecycle for programmes, projects and systems. The intention is that cyber and information risks are included at the earliest point when a new business capability is being considered. When undertaking risk management, it is important that appropriate coordination between safety and security is a fundamental consideration (further guidance is available in IEC 62859 Reference 11). This will support the "building in" of security requirements at the development stages to enable security by design. Such an approach will facilitate legal and regulatory compliance and also reduce costs, since security functions are much cheaper when built in at the outset as inherent parts of the design.

9.7 Dutyholders should consider early notification of new information or operational technology systems to ONR to facilitate early regulatory engagement. Inspectors should consider such engagement as part of an enabling approach to regulation.

9.8 The risk management approach should also cater for the fact that risks change over time and should therefore have a mechanism for both reviewing risks at regular intervals in the lifecycle, and for including consideration of cyber and information risks as part of the change management process. Where risks change, a reporting mechanism to risk managers and owners should be identified.

9.9 Cyber and information risk management extends beyond the delivery of a new system and should extend to the lifecycle of the information and the associated assets holding it. Accordingly, mechanisms are required to monitor and review compliance with security requirements for as long as the system is in operation and the information is extant.

[1] Based upon an original diagram from www.education.vic.gov.au

9.10 The risk management approach should include secure disposal of assets as well as any retention of information and associated assets under regulation for legal reasons (such as contract or finance information).

9.11 Dutyholders should have a clear plan for communicating risk, internally, and externally to partners and suppliers.

9.12 Where dutyholders have classified contracts, they should consider whether a right for them to conduct a CS&IA assessment of the contractor is included in contracts to ensure that there is adequate legal basis to conduct assessments. Such contractual arrangements should also be in place to support the redress of any deficiencies arising during the course of the contract. Decisions by third-parties to manage residual risk should be reported back, and be incorporated into, the dutyholder's own cyber and information risk register.

9.13 The plan should include any requirements for reporting to external bodies such as ONR.

Inspectors should consider:

- Is there a defined approach for how risk management will be carried out in the organisations?
    - Does it include partners and suppliers?
    - Where appropriate, is this supported adequately by conditions in contracts?
- Is risk management considered in the planning for new systems?
- Does the risk management approach cover the whole lifecycle for the information and associated assets?
    - Does it cater for regular risk reviews?
    - Does it include change control?
- Does system planning include notifying ONR of any new system or high risk system within a suitable time frame?
- Is there a risk management communications plan and is it appropriate?

10. CS&IA RISK ASSESSMENT APPROACH

10.1 Dutyholders should establish mechanisms and utilise trained specialists when necessary to analyse cyber threats, vulnerabilities, and potential impacts which are associated with nuclear security and safety operations and related information.

10.2 The organisation should have a defined risk assessment approach and methodology that is used consistently. Guidance on some of the different methodologies can be found in NSS 17 (Reference 9) and the National Cyber Security Centre (NCSC) guidance document 'A critical appraisal of risk methods and frameworks' (Reference 10).and dutyholders should select an approach that is appropriate for their organisation. Examples include:

- ISO27005:2011
- IEC (ISA) 62443-3-2 Security risk assessment and system design
- US National Institute of Standards and Technology SP 800-30
- Octave Allegro

- Information Systems Audit and Control Association: Control Objectives for IT 5
- Information Security Forum – Information Risk Analysis methodology
- Open Group FAIR Risk Analysis Standard

10.3 Security risk assessment methodologies vary but generally include, as a minimum, consideration of threats, vulnerabilities and impacts. The risk assessment should be informed by a current threat assessment. In-house threat assessments are generally considered to be of the greatest value since they are tailored to the specifics of the business. However these can be informed by threat intelligence from sources such as: the UK Design Basis Threat, NCSC (which includes CERT UK and the Cyber Information Sharing Partnership) and the Centre for the Protection of the National Infrastructure.

10.4 Dutyholders should be aware of the risks associated with the use of modern 'shared' IT/OT solutions, notably cloud based services. Care should be taken to understand what access cloud based service providers have to dutyholder corporate infrastructure where SNI may be stored. An example of such a service is the use by construction companies of Building Information Modelling management tools from cloud based outsourced providers. The potential vulnerability is that the associated building models may contain sensitive information such as building layouts and security-related features such as cable runs, utilities, plant location and security systems. These models often have to be shared with a number of contractors and data access should be risk managed carefully.

Inspectors should consider:

- Is the risk assessment methodology appropriate for the size and scope of the organisation?
  - Is it operated by suitably qualified and experienced personnel?
  - Is it auditable?
- Does the risk assessment consider risks from partners and supply chain companies?
- Is there a threat assessment informed from relevant sources and does it cover the correct scope?

11. CS&IA RISK TREATMENT APPROACH

11.1 There are many ways to conduct risk treatment for cyber and information risks and dutyholders should select a formal, auditable and repeatable risk treatment process to decide upon the security controls necessary to manage and/or mitigate CS&IA risks to information and associated assets of all types.

11.2 The selection of security controls should be based upon a risk assessment and those controls chosen should be suitable and adequate to mitigate the identified risks within agreed appetites. Annex H of SyAPs details guidance on security postures and security functions that dutyholders may wish to incorporate into their risk treatment approach.

11.3 An appropriate defence in depth approach to risk mitigation should be implemented. Security control selection should take account of existing or proposed physical and personnel security measures.

11.4 Once controls have been selected it is essential that there is assurance that they are in place and effective. There are a number of assurance schemes available from NCSC, commercial providers and other organisations for technical assurance with differing degrees of rigour. In addition, assurance through system testing should also be considered. An auditable mechanism should be in place to provide traceability of how assurance requirements have been specified, implemented and managed.

11.5 The approach should include assurance of technical and non-technical controls. Any testing required as part of the assurance process should be carried out by suitably qualified and experienced personnel.

11.6 The assurance process should be implemented both before system operations commence and at pre-determined intervals throughout the lifetime of the information and associated assets in scope. Additionally, there should be oversight from risk managers (ultimately to Board level), to ensure that CS&IA risk mitigations are effective.

Inspectors should consider:

- Have security controls been selected to mitigate risks identified from a risk assessment?
- Is there evidence of a clear mapping of security controls to identified risks?
- Is there evidence of assurance functions tailored to the level of risk and the risk appetite of the business?
- Is there evidence that the assurance process is planned and resourced for the lifetime of the information and associated assets?
- Are risk managers involved in assessing effectiveness?

12. CS&IA RESIDUAL RISK MANAGEMENT

12.1 Residual risk management is implemented following the previous stages of risk assessment and risk treatment. Risk can rarely be mitigated completely and to attempt to do so may prevent the organisation from taking risk reduction opportunities in other areas of the business. The risk appetite statements for critical business functions (see paragraph 7.4 above) should specify how much risk can be considered in a particular area and provide guidance to managers on how the element of risk remaining, the residual risk, can be managed.

12.2 Dutyholders should have a process in place to ensure that risk management judgements made by the SIRO (or by other responsible personnel with formal delegated authority) are objective, informed, auditable, communicated clearly and are based on a meaningful understanding of risk for the organisation.

12.3 The organisation should have defined an approach to managing cyber & information risk (see paragraph 9.2) and this should be known to all those identified in the CS&IA Risk Governance structure. Accordingly, risk managers should understand their responsibilities and be aware of where they fit in to the process as a whole.

12.4 Organisations should have a mechanism for assessing and evidencing residual risk for information and associated assets so that it can be reviewed and managed. One such approach might be to summarise the identified risks, the controls in place to mitigate them and the residual risk to be considered. Whichever mechanism is chosen, the aim is to provide managers with evidence and adequate information to make a properly

informed decision. There should also be evidence of the mapping of residual risk to risk appetite and evidence of how the acceptable level of residual risk was arrived at.

12.5 The process needs to function effectively for all levels in the business so that managers, empowered to different degrees, can make decisions appropriate to their responsibilities. A mechanism is required to record who made what risk management decisions, when, and the context around the decision at the time. Apart from being good practice there are likely to be legal and regulatory reasons for keeping such records and ensuring that the decision making is traceable and auditable.

12.6 Ultimately, the Board retains overall accountability for cyber and information risk management so the process should support the oversight for all such risks in the organisation.

12.7 Risk management does not end when a system enters operation because risks change dynamically over time and therefore the management of residual risk should be ongoing for the lifetime of the information and associated assets. The risk management process should take this into account through incorporating planned reviews at appropriate intervals as justified by the risk owner. There should be adequate audit and compliance mechanisms to pick up on the review of security control assurance and feed this into the review of residual risks.

12.8 Dutyholders should establish a mechanism for reporting risk within the organisation both as part of the escalation process and in order to provide senior management oversight. Reporting of residual risk may include external as well as internal bodies and a mechanism should be established to provide the reports in the appropriate formats and at the appropriate level of detail.

12.9 Dutyholders should consider including an annual review of security and any return to ONR to demonstrate assurance as part of their CS&IA Risk Management Policy.

Inspectors should consider:

- Is there a defined process supported by evidence for explaining risks and presenting them to managers?
- Do risk managers at all levels understand their role in the governance structure, are they empowered appropriately and are there clear escalation paths?
- Is there a defined structure for capturing and presenting residual risk to managers?
- Is it clear who owns residual risk for each system?
- Does this structure provide an auditable path to explain the context of decision making as well as identify who made what decision and when?
- Is there a mechanism for identifying CS&IA risks from different operational areas to senior managers and ultimately to the Board?
- Does the risk management process operate over the lifetime of the information and associated assets?

13. CS&IA RISK MANAGEMENT FOR CLASSIFIED CONTRACTS

13.1 Dutyholders should be able to determine and satisfy themselves that delivery partners, service providers and third party suppliers, apply proper security controls to mitigate risks to the information and associated assets that they are responsible for.

13.2 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 TAG 7.2 –Information Security.

14. REFERENCES

1. **Nuclear Industries Security Regulations 2003**. Statutory Instrument 2003 No. 403

2. **IAEA Nuclear Security Series No. 13.** Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (**INFCIRC/225/Revision 5**). January 2011. www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf.

3. **IAEA Nuclear Security Series No. 20**. Objective and Essential Elements of a State's Nuclear Security Regime. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf

4. **Convention on the Physical Protection of Nuclear Material (CPPNM)** https://ola.iaea.org/ola/treaties/documents/FullText.pdf

5. **HMG Security Policy Framework**. Cabinet Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

6. **Classification Policy for the Civil Nuclear Industry**. ONR. http://www.onr.org.uk/documents/classification-policy.pdf

7. **Security Assessment Principles for the Civil Nuclear Industry** – ONR. http://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf

8. **IAEA Nuclear Security Series No. 23-G**. Security of Nuclear Information http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1677web-32045715.pdf

9. **IAEA Nuclear Security Series No. 17**. Computer Security at Nuclear Facilities http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf

10. **NCSC - A Critical Appraisal of Risk Methods and Frameworks** https://www.ncsc.gov.uk/guidance/critical-appraisal-risk-methods-and-frameworks

11. **BS IEC 62859:2016 - Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Coordinating Safety and Cybersecurity**

Note: ONR staff should access the above internal ONR references via the How2 Business Management System.

15. GLOSSARY AND ABBREVIATIONS

CPS	Cyber Protection System
CPPNM	Convention on the Physical Protection of Nuclear Material
CS&IA	Cyber Security and Information Assurance
FSyP	Fundamental Security Principle
HMG	Her Majesty's Government
IAEA	International Atomic Energy Agency
NCSC	National Cyber Security Centre
NISR	Nuclear Industries Security Regulations
NSS	Nuclear Security Series
ONR	Office for Nuclear Regulation
SIRO	Senior Information Risk Officer
SNI	Sensitive Nuclear Information
SPF	Security Policy Framework
SyAP	Security Assessment Principle
TAG	Technical Assessment Guide