IEC TR 63486

Edition 1.0 2024-09

TECHNICAL REPORT

colour inside

Nuclear facilities – Instrumentation, control and electrical power systems – Cybersecurity risk management approaches

IEC TR 63486:2024-09(en)

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC TR 63486

Edition 1.0 2024-09

TECHNICAL REPORT

colour inside

Nuclear facilities – Instrumentation, control and electrical power systems – Cybersecurity risk management approaches

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 27.120.20; 27.100

ISBN 978-2-8322-9380-5

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

NUCLEAR FACILITIES – INSTRUMENTATION, CONTROL AND ELECTRICAL POWER SYSTEMS – CYBERSECURITY RISK MANAGEMENT APPROACHES

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC TR 63486 has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear Instrumentation. It is a Technical Report.

The text of this Technical Report is based on the following documents:

Draft	Report on voting
45A/1522/DTR	45A/1541/RVDTR

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this Technical Report is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

a) Technical background, main issues and organisation of the standard

This document focuses on methods for implementing cybersecurity risk management processes for instrumentation and control (I&C) systems and electrical power systems (EPS) at NPPs, resulting in various cyber-risk approaches. The goal of this document applies a common analysis process to each of the cyber-risk approaches to identify and evaluate key insights for cyber-risk management for I&C systems and EPS of NPPs to support potential development of an international standard based upon common elements.

This report considers eleven challenges for applying ISO/IEC 27005:2018 cybersecurity risk management to I&C systems and EPS of NPPs. The report compares how the cyber-risk approaches address these challenges. This report identifies common elements, if any, between these approaches. These common elements will be further analyzed to determine if there is sufficient consensus to recommend developing an IEC risk management standard for I&C Systems and EPS at NPPs.

It is intended that this standard be used by operators of NPPs (utilities), systems evaluators and by licensors.

b) Situation of the current standard in the structure of the IEC SC 45A standard series

IEC TR 63486 is a fourth level IEC SC 45A document. Within the general principles defined by IEC 62645 as the entry level document for IEC SC 45A security standards, this document summarizes an evaluation of cyber-risk approaches that are in use by NPP operators to manage cybersecurity risks.

For more details on the structure of the IEC SC 45A standard series, see item d) of this introduction.

c) Recommendations and limitations regarding the application of the standard

It is important to note that a technical report is entirely informative in nature. It gathers data collected from different origins and it establishes no requirements.

To ensure that the standard will continue to be relevant in future years, the emphasis has been placed on issues of principle, rather than specific technologies.

d) Description of the structure of the IEC SC 45A standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The IEC SC 45A standard series comprises a hierarchy of four levels. The top-level documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046.

IEC 61513 provides general requirements for instrumentation and control (I&C) systems and equipment that are used to perform functions important to safety in nuclear power plants (NPPs). IEC 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply systems of the I&C systems.

IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical power systems for nuclear power plants.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general requirements for specific topics, such as categorization of functions and classification of systems, qualification, separation, defence against common cause failure, control room design, electromagnetic compatibility, human factors engineering, cybersecurity, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 are standards related to specific requirements for specific equipment, technical methods, or activities. Usually these documents, which make reference to second-level documents for general requirements, can be used on their own.

A fourth level extending the IEC SC 45 standard series, corresponds to the Technical Reports which are not normative.

The IEC SC 45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1 , establishing safety requirements related to the design of nuclear power plants (NPPs), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPPs, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPPs, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPPs, the IAEA safety guide SSG-51 dealing with human factors engineering in the design of NPPs and the implementing guide NSS42-G for computer security at nuclear facilities. The safety and security terminology and definitions used by the SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework, IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector.

IEC 61513 and IEC 63046 refer to ISO 9001 as well as to IAEA GSR part 2 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA).

At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC/SC 45A security standards. It builds upon the valid high level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2, IEC 60964 is the entry document for the IEC/SC 45A control rooms standards, IEC 63351 is the entry document for the human factors engineering standards and IEC 62342 is the entry document for the ageing management standards.

NOTE 1 It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards), international or national standards would be applied.

NOTE 2 IEC TR 63400 provides a more comprehensive description of the overall structure of the IEC SC 45A standards series and of its relationship with other standards bodies and standards.

NUCLEAR FACILITIES – INSTRUMENTATION, CONTROL AND ELECTRICAL POWER SYSTEMS – CYBERSECURITY RISK MANAGEMENT APPROACHES

1 Scope

1.1 General

IEC 62645 [1][1] provides a cybersecurity framework for digital I&C programmable systems[2]. IEC 62645 [1] aligns strongly with the information security management system (ISMS) elements detailed within ISO/IEC 27001:2013 [2]. The “I&C digital programmable system security programme” (as defined in 5.2.1 of IEC 62645:2019 [1]) align with the ISMS programme.

The framework for this programme assigns security degrees (SD) to I&C systems and EPS and defines cybersecurity requirements based upon these SDs. The assignment of an SD corresponds heavily to the safety categorization of IEC 61513 [3] and IEC 61226 [4].

IEC 62645 [1] does not provide detailed guidance on risk management. The only guidance outlined in IEC 62645:2019 [1] is in 5.4.3.2.2.4, and it states, that ISO/IEC 27005 [5] “provides a generic framework for information security risk assessment, but the specific implementation methodology is up to the organization, depending on its organizational, industrial, and regulatory context.”

IEC 62645:2019 [1] also references risk in 5.4.3.2.2.5, stating:

> “The specific risk assessment methodologies and tools shall be identified and kept up to date. Risk re-assessments shall be performed periodically throughout the whole life cycle of the I&C systems, when modifications to the system occur and when changes to the threat landscape are identified, such as new threats or new vulnerabilities that can affect the installed I&C programmable digital system. The number of potential threats and vulnerabilities usually increases with progress from stand-alone to interconnected systems.”

In recent years, there have been advances in NPP cybersecurity risk management nationally and internationally. For example, International Atomic Energy Agency (IAEA) publications Nuclear Security Series (NSS) 17-T [6] and NSS 33-T [7], propose a framework for computer security risk management that implements a risk management program at both the facility and individual system levels. These international approaches (i.e., IAEA), national approaches (e.g., Canada’s HTRA [8]) and technical methods[3] (e.g., HAZCADS [9], Cyber Informed Engineering [10], EBIOS [11] [12]) have advanced risk management within NPP cybersecurity programmes that implement international and national standards.

The scope of this document is to capture the national and international cyber-risk approaches employed to manage cybersecurity risks associated with Instrumentation and Control (I&C) and Electrical Power Systems (EPS) at a Nuclear Power Plant (NPP).

[1] Numbers in square brackets refer to the Bibliography.

[2] The terms I&C system and EPS in this document refers to those systems which are digital and thus susceptible to cyber-attacks.

[3] The term “cyber-risk approaches” is used in this document to refer to international approaches, national approaches and technical methods.

This report inherits the scope from IEC 62645 [1], which defines adequate measures for the prevention of, detection of, and reaction to malicious acts by digital means (cyberattacks) on I&C systems and EPS. This scope includes any malicious act that creates an unsafe situation, equipment damage, or plant performance degradation, such as:

- Malicious modifications affecting system integrity;
- Malicious interference with information, data, or resources that could compromise the delivery of or performance of the required I&C system's programmable digital functions;
- Malicious interference with information, data, or resources that could compromise operator displays or lead to loss of management of I&C systems or EPS; and
- Malicious hardware, firmware, or software changes at the programmable logic controller level.

Human errors leading to violation of the security policy and those impacting the performance of cybersecurity controls are key risks to be assessed by risk management processes evaluated for this document.

This document summarizes an evaluation of cyber-risk approaches that are in use by nuclear facility operators to manage cybersecurity risks.

The scope of this document generally follows the exclusions of IEC 62645 [1] which are:

- Non-malevolent actions and events such as accidental failures, human errors (except those stated above, such as impacting the performance of cybersecurity controls), and natural events. In particular, good practices for managing applications and data, including backup and restoration related to accidental failure, are out of scope.

NOTE 1 Although security programs in other normative contexts often cover such aspects (e.g., in the ISO/IEC 27000 series [13] or IEC 62443 series [14]), this document is only focused on evaluating risk management processes that manage risks associated with malicious acts by digital means (cyberattacks) on digital I&C systems (I&C) and Electrical Power Systems (EPS). The main reason for the limitation in scope is that in the nuclear generation domain, other standards and practices already cover accidental failures, unintentional human errors, natural events, etc. The focus of this document is to provide the maximum consistency and the minimum overlap with these other nuclear standards and practices, especially IEC 62645 [1].

- Site physical security, access control (site and specific locations within the site), and site security surveillance systems. While not explicitly addressed in IEC 62645 [1], these systems are generally covered by plant operating procedures and programmes.

NOTE 2 This exclusion does not deny that cybersecurity has clear dependencies on the security of the physical environment (e.g., physical protection, or heating/ventilation/air-conditioning systems). However, this exclusion is based on the scope of IEC subcommittee and the working group that developed this document.

- Confidentiality of information regarding I&C systems and EPS is not within the scope of IEC 62645 [1] (see IEC 62645:2019 [1], 5.4.3.2.3). However, unauthorized disclosure of sensitive information regarding I&C systems or EPS can lead to changes in risks associated with those systems. Loss of confidentiality and its impact on risks were considered within this evaluation.

Standards such as ISO/IEC 27001:2013 [2] and ISO/IEC 27005:2018 [5] are not directly applicable to the cyber protection of NPP I&C systems and EPS. The regulatory and safety requirements needed for the safe operation of systems within an NPP render much of the ISO/IEC 27001:2013 [2] and ISO/IEC 27005:2018 [5] content immaterial or inadequate. However, IEC 62645 [1] builds upon the valid high-level principles and main concepts of ISO/IEC 27001:2013 [2], adapts them, and completes them to fit into the nuclear context. In a similar manner, this document aims to evaluate and summarize key insights within ISO/IEC 27005:2018 [5] risk management elements for possible adaptation for a potential standard under IEC 62645 [1] NPP cybersecurity programmes.

An overview of the hierarchy of IEC SC 45A standards related to cybersecurity is shown in Figure 1.

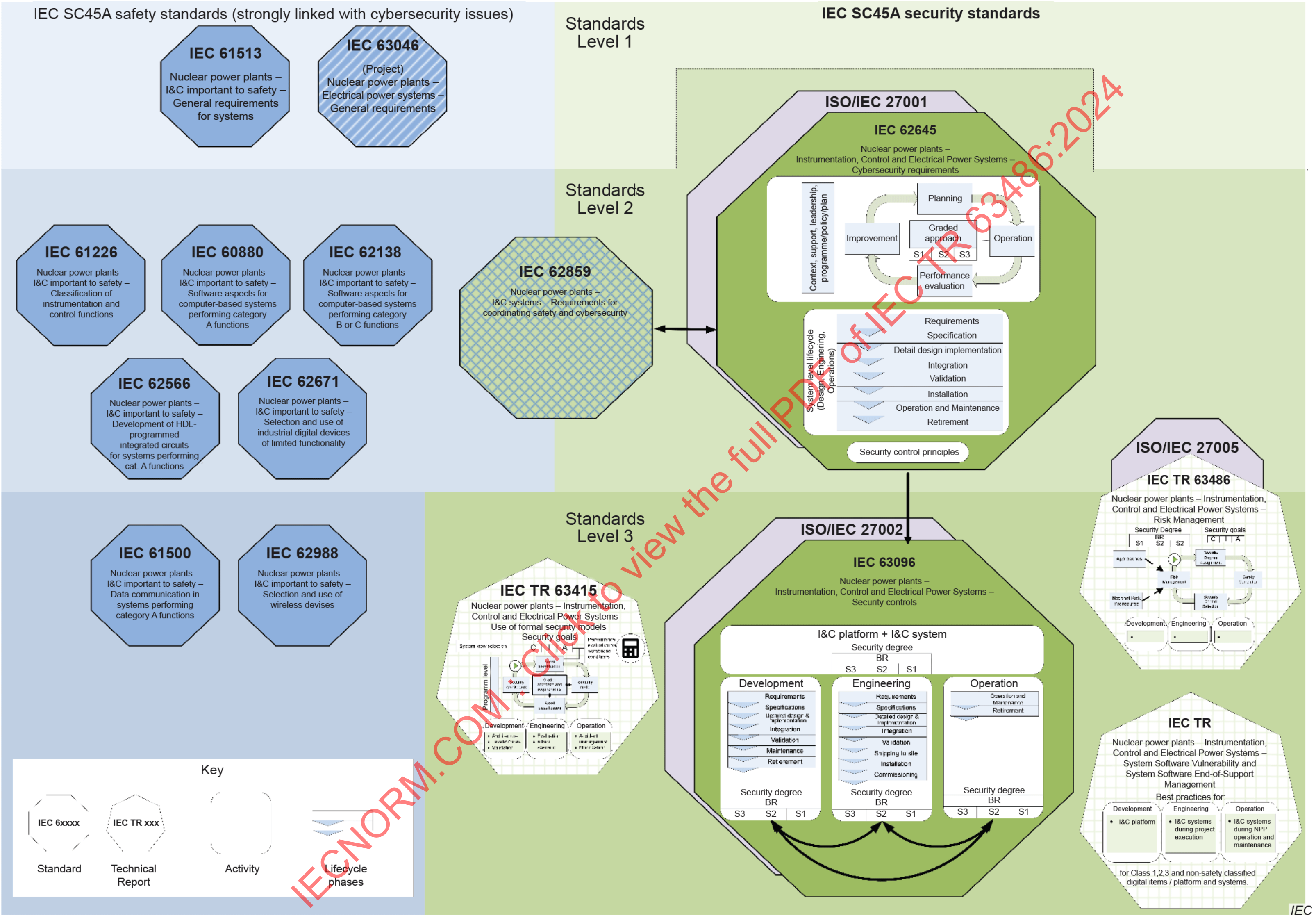

IEC SC45A safety standards (strongly linked with cybersecurity issues)
IEC SC45A security standards
Standards Level 1
Standards Level 2
Standards Level 3
IEC 61513
Nuclear power plants – I&C important to safety – General requirements for systems
IEC 63046
(Project) Nuclear power plants – Electrical power systems – General requirements
IEC 61226
Nuclear power plants – I&C important to safety – Classification of instrumentation and control functions
IEC 60880
Nuclear power plants – I&C important to safety – Software aspects for computer-based systems performing category A functions
IEC 62138
Nuclear power plants – I&C important to safety – Software aspects for computer-based systems performing category B or C functions
IEC 62566
Nuclear power plants – I&C important to safety – Development of HDL-programmed integrated circuits for systems performing cat. A functions
IEC 62671
Nuclear power plants – I&C important to safety – Selection and use of industrial digital devices of limited functionality
IEC 61500
Nuclear power plants – I&C important to safety – Data communication in systems performing category A functions
IEC 62988
Nuclear power plants – I&C important to safety – Selection and use of wireless devises
IEC 62859
Nuclear power plants – I&C systems – Requirements for coordinating safety and cybersecurity
ISO/IEC 27001
IEC 62645
Nuclear power plants – Instrumentation, Control and Electrical Power Systems – Cybersecurity requirements
Context, support, leadership, programme/policy/plan
Planning
Improvement
Graded approach
S1
S2
S3
Operation
Performance evaluation
System level lifecycle (Design, Engineering, Operations)
Requirements
Specification
Detail design implementation
Integration
Validation
Installation
Operation and Maintenance
Retirement
Security control principles
ISO/IEC 27002
IEC 63096
Nuclear power plants – Instrumentation, Control and Electrical Power Systems – Security controls
I&C platform + I&C system
Security degree
BR
S3
S2
S1
Development
Requirements
Specifications
Detailed design & implementation
Integration
Validation
Maintenance
Retirement
Engineering
Requirements
Specifications
Detailed design & implementation
Integration
Validation
Shipping to site
Installation
Commissioning
Operation
Operation and Maintenance
Retirement
ISO/IEC 27005
IEC TR 63486
Nuclear power plants – Instrumentation, Control and Electrical Power Systems – Risk Management
Security Degree
BR
S1
S2
S2
Security goals
C
I
A
Development
Engineering
Operation
IEC TR 63415
Nuclear power plants – Instrumentation, Control and Electrical Power Systems – Use of formal security models
Security goals
C
I
A
Programm level
Development
Engineering
Operation
IEC TR
Nuclear power plants – Instrumentation, Control and Electrical Power Systems – System Software Vulnerability and System Software End-of-Support Management
Best practices for:
Development
Engineering
Operation
I&C platform
I&C systems during project execution
I&C systems during NPP operation and maintenance
for Class 1,2,3 and non-safety classified digital items / platform and systems.
Key
IEC 6xxxx
Standard
IEC TR xxx
Technical Report
Activity
Lifecycle phases
IEC

Figure 1 – Overview of the hierarchy of IEC SC 45A standards related to cyber security

1.2 Framework

This document summarizes key insights of the international and cyber-risk approaches used at NPPs regarding the application of ISO/IEC 27005:2018 [5]. The evaluation is based on 11 challenges to cybersecurity risk management and their applicability to NPP risk management. The challenges are detailed in Clause 7.

The risk management elements within ISO/IEC 27005:2018 [5] considered within the evaluation are listed below:

- Context Establishment (external and internal)
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Decision Point 1 (Assessment satisfactory)
- Risk Treatment
- Risk Decision Point 2 (Treatment satisfactory)
- Risk Acceptance
- Risk Communication and Consultation
- Monitoring and Review

This document also relates the risk management elements of IEC 62645 [1] and IEC 63096 [15].

1.3 Limitations

This document is limited to the scope defined in IEC 62645 [1]. Therefore, this document assumes that I&C systems and EPS do not directly contribute to the potential theft of nuclear material. The risk of theft of nuclear material and its consequence is covered through the design, implementation, and operation of Physical Protection Systems and the design and operation of these are unique for each NPP.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia [16]: available at http://www.electropedia.org/
- ISO Online browsing platform [17]: available at http://www.iso.org/obp
- IAEA Nuclear Safety and Security Glossary [18] available at https://www.iaea.org/publications/15236/iaea-nuclear-safety-and-security-glossary

3.1
attack pathway
path or *route* by which an attacker or malicious program can gain access to a computer-based system

Note 1 to entry: Examples of attack pathways are (1) physical access, (2) wired network connectivity, (3) wireless network connectivity, (4) portable media/mobile device connectivity, and (5) supply chain.

Note 2 to entry: Adapted from “attack vector” definition from IEC 62645:2019, 3.1.

3.2
attack vector
method or means by which an attacker or malicious program *performs tasks on a* computer-based system

Note 1 to entry: The attack vector enables the attacker to perform tasks after accessing an attack pathway.

[SOURCE: IEC 62645:2019, 3.1]

3.3
authorization
function of specifying access rights to resources, which is related to information security and computer security in general and access control in particular

[SOURCE: IEC 62645:2019, 3.2]

3.4
availability
property of being accessible and usable upon demand by an authorized entity

Note 1 to entry: This definition is specific to the context of security of nuclear information and is therefore different from the one used in other IEC/SC45A standards, which is “ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.”

[SOURCE: IAEA Nuclear Safety and Security Glossary, 2022 Interim Edition]

3.5
computer-based item
item that relies on software instructions running on microprocessors or microcontrollers

Note 1 to entry: The term item can be replaced by the terms “system,” “equipment,” or “device.”

Note 2 to entry: A computer-based item is a kind of programmable digital item.

Note 3 to entry: This term is equivalent to a software-based item.

[SOURCE: IEC 62138:2018, 3.8]

3.6
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: IAEA Safety and Security Glossary, 2022 Interim Edition]

3.7
cyberattack
malicious acts by digital means

[SOURCE: IEC 62645:2019, 3.6]

3.8
cybersecurity
set of activities and measures whose objective is to prevent, detect, and react to:

- *Malicious modifications* (integrity) of functions that may compromise the delivery or integrity of the required service by I&C system (including loss of control) or EPS, which could lead to an accident, an unsafe situation, or plant performance degradation;
- *Malicious withholding or prevention* of access to or communication of information, data, or resources (including loss of view) that could compromise the delivery of the required service by I&C systems or EPS (availability), which could lead to an accident, an unsafe situation or plant performance degradation;
- *Unauthorised disclosure of information* (confidentiality) that could be used to perform malicious acts which could lead to an accident, an unsafe situation, or plant performance degradation.

Note 1 to entry: This definition is tailored to reflect the IEC 62645 standard scope and the overall SC 45A document structure. It is recognized the term “cybersecurity” has a broader meaning in other standards and guidance, often including non-malevolent threats, human errors, and protection against natural disasters, those aspects – except human errors that degrade cybersecurity protections – are not included in the concept of cybersecurity used in the SC 45A standard series. See Annex A of IEC 62645:2019 for more detail regarding this document scope exclusions.

Note 2 to entry: Computer security and cybersecurity are considered synonymous in this document.

3.9
design
process and result of developing a concept, detailed plans, supporting calculations, and specifications for a facility and its parts

[SOURCE: IAEA Nuclear Safety and Security glossary, 2022 Interim Edition]

3.10
design basis threat
DBT
attributes and characteristics of potential insider or external adversaries who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated

Note 1 to entry: Cyberattacks and related adversaries are not considered in an equivalent manner in DBTs; this depends on each cyber-risk approach and legal framework. Moreover, the content of a nuclear DBT is treated as highly confidential.

Note 2 to entry: IAEA Nuclear Security Series publications leverage the concept of a physical protection system to protect against malicious acts targeting theft of nuclear material or resulting in radiological sabotage. Conversely, IEC SC 45A standards focus on protection against compromise of I&C systems and EPS of resulting in unacceptable impacts to the safety and security of an NPP.

[SOURCE: IAEA NSS No. 13, 2011 modified: notes 1 and 2 added]

3.11
electrical/electronic/programmable electronic item
E/E/PE item
item based on electrical (E) or electronic (E) and/or programmable electronic (PE) technology

Note 1 to entry: This term and its definition, the word “item,” can be replaced by the words: “system,” “equipment,” or “device.”

Note 2 to entry: The definitions of the terms related to the technology: E/E/PE item, programmable digital item, computer-based item, hardwired item, programmable logic item provide a taxonomy that allows for a consistent and coherent means of classifying these items. Programmable digital items are susceptible to cyber-attacks.

[SOURCE: IEC 62138: 2018, 3.15]

3.12
Hardware Description Language-programmed device
HPD
integrated circuit configured (for NPP I&C systems), with Hardware Description Languages (HDL) and related software tools

Note 1 to entry: HDLs and related tools (e.g., simulator, synthesizer) are used to implement the requirements in a proper assembly of pre-developed micro-electronic resources.

Note 2 to entry: The development of HPDs can use pre-developed Blocks.

Note 3 to entry: HPDs are typically based on blank Field Programmable gate Arrays or similar micro-electronic technologies.

Note 4 to entry: HPD is a kind of programmable logic item.

Note 5 to entry: See the definition of “E/E/PE item” and the associated notes.

[SOURCE: IEC 62566: 2012, 3.7]

3.13
I&C function
function to control, operate or monitor a defined part of the process

[SOURCE: IEC 61513:2011, 3.28]

3.14
I&C system
system, based on E/E/PE items, performs plant instrumentation and control functions as well as service and monitoring functions related to the operation of the system itself

Note 1 to entry: A general term that encompasses all system elements such as internal power supplies, sensors, and other input devices, data highways and other communication paths, interfaces to actuators, and other output devices. The different functions within a system may use dedicated or shared resources.

Note 2 to entry: The elements included in a specific I&C system are defined in the specification of the system’s boundaries.

Note 3 to entry: See also “electrical power system.” The terms “electrical power system” and “I&C system” are terms related to the main functions the systems perform, respectively, “electrical power generation, transmission and distribution” and “measurement, protection, control and HMI related to the NPP process.” They have to be considered in conjunction and are consistent and coherent with the general requirements established by IEC 61513 and IEC 63046 for instrumentation, control, and electrical power systems for nuclear power plants.

Note 4 to entry: See also the definition of the E/E/PE item and the associated notes.

Note 5 to entry: According to their typical functionality, IAEA distinguishes between automation/control systems, HMI systems, interlock systems, and protection systems.

[SOURCE: IEC 62138: 2018, 3.26]

3.15
integrity
property of protecting the accuracy and completeness of assets

[SOURCE: ISO/IEC 27000:2018, 3.36, modified – the phrase “of assets” was added]

3.16
programmable digital item
item that relies on software instructions or programmable logic to accomplish a function

Note 1 to entry: In this term and its definition, the term item can be replaced by the terms: system or equipment, or device.

Note 2 to entry: See also the definition of the E/E/PE item and the associated notes.

Note 3 to entry: The main kinds of programmable digital items are computer-based and programmable logic items.

Note 4 to entry: This term used by IEC SC 45A is equivalent to programmable electronic item (PE item) defined accordingly to IEC 61508.

[SOURCE: IEC 62138:2018, 3.34]

3.17
risk
potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the likelihood of an event and the severity of its consequences

[SOURCE: IAEA Nuclear Security Series No. 17:2011]

3.18
risk assessment
overall process of systematically identifying, estimating, analysing, and evaluating risk

[SOURCE: IAEA Nuclear: Safety and Security Glossary, 2022 Interim Edition, modified – the phrase "for the purpose of informing priorities, developing or comparing courses of action, and informing decision making of assets" was deleted]

3.19
security controls
means of managing security which can be technical, physical, or administrative

[SOURCE: IEC 62645:2019, 3.18]

3.20
security degree
gradation of security protection with associated sets of requirements assigned to a system according to the maximum consequences of a successful cyberattack on this system in terms of plant safety and performance

Note 1 to entry: IEC 62645 defines three security degrees corresponding to S1, S2, and S3. The rationale behind the use of these three degrees for I&C systems is provided in Annex B. This document is limited to I&C systems and EPS and does not make any assumptions about the security degrees for other systems. Non-I&C systems (e.g., office computers) might be assigned to supplemental/different security degrees, leading to a graded approach with more than three security degrees from a global perspective. Moreover, some national practices involved the subdivision of security degrees.

Note 2 to entry: The term "security degree" is preferred to "security level" or avoid possible confusion with the concept of I&C levels commonly found in other standards and industry practices.

[SOURCE: IEC 62645:2019, 3.19]

3.21
security programme
set of interrelated or interacting elements of an organization to establish security policies and objectives, as well as processes and security plans to achieve those objectives

Note 1 to entry: Programme is a concept similar to a "management system" as defined in ISO/IEC 27000:2018.

Note 2 to entry: Computer security programme, cybersecurity programme, and security programme are considered synonymous in this document.

[SOURCE: IEC 62645:2019, 3.20]

3.22
threat
potential cause of an unwanted incident, which may result in harm to a system, organization, or people

Note 1 to entry: In the frame of this document (see IEC 62645), the considered events or occurrences are limited to malicious ones and to human errors that degrade cybersecurity – not include accidental aspects (e.g., natural hazards, human errors not impacting cybersecurity).

[SOURCE IEC 62645:2019, 3.22, modified – the phrase "harm to a system or organization" was amended to "harm to a system, organization, or people"]

3.23
vulnerability
weakness of an asset or a security control that can be exploited by a threat

[SOURCE: IEC 62645:2019, 3.23]

4 Abbreviated terms

CDA	Critical Digital Asset
CFR	Code for Regulation
CR	Component Requirement
CSP	Computer Security Policy
CERT	Computer Emergency Response Team
CIE	Cyber Informed Engineering
CSRM	Computer Security Risk Management
DBSy	Domain Based Security
DBT	Design Basis Threat
DCSA	Defensive Computer Security Architecture
DER	Detection and Reaction
DiD	Defense in Depth
DI&C	Digital Instrumentation and Control
DBT	Design Basis Threat
DOE	United States Department of Energy
EBIOS	Expression of needs and identification of security objectives
EPRI	Electric Power Research Institute
EPS	Electrical Power System
ES	Electrical System
FCSRM	Facility Computer Security Risk Management

FOI	Focus of Interest
FSTEC	Russian Federal Service for Technical and Export Control
FTA	Fault Tree Analysis
HAZCADS	Hazards and Consequences Analysis for Digital Systems
HAZOP	Hazard and Operability
HDL	Hardware Description Language
HMG	His Majesty’s Government (UK)
HPD	HDL Programmed Device
HTRA	Harmonized Threat and Risk Assessment Methodology
I&C	Instrumentation and Control
IACS	Industrial Automated Control Systems
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information technology
I&C	Instrumentation and Control
MFA	Multi-factor authentication
NEI	Nuclear Energy Institute
NM	Nuclear Material
NPP	Nuclear Power Plant
NRC	United States Nuclear Regulatory Commission
NSS	Nuclear Security Series
OT	Operational Technology
PRA	Probabilistic Risk Assessment
RE	Requirement Enhancement
RG	Regulatory Guide
RMF	Risk Management Framework
SCSRM	System Computer Security Risk Management
SD	Security Degree
SIEM	Security Information and Event Management
SL	Security Level
SL-T	Security Level – Target
SOC	Security Operations Centre
SR	System Requirement
SSEP	Safety, Security and Emergency Preparedness
STPA	Systems Theoretic Process Analysis
TR	Technical Report
UCA	Unsafe Control Actions
URC	Unacceptable Radiological Consequences
V&V	Verification & Validation

5 IEC 62645 risk management elements

5.1 General

IEC 62645:2019, 5.4 [1] provides a high-level outline of cyber security management processes, which are adapted from ISO/IEC 27001:2013 [2]. However, IEC 62645 [1] does not attempt to provide detailed guidance on how to perform a risk management process. IEC 62645 [1] scope is limited to establishing "requirements and provides guidance for the development and management of effective computer security programmes for I&C systems and EPS. Inherent to these requirements and guidance is the criterion that the power plant I&C programmable digital system security programme complies with the applicable country's requirements."

The current approach of IEC 62645 [1] is to establish a cyber security programme that uses the risk assessment process from ISO/IEC 27005:2018 [5] and the risk assessment method adapted from ISO/IEC 27001 [2]. However, the ISO/IEC 27001 [2] and ISO/IEC 27005 [5] standards are not directly applicable to the cyber protection of NPP I&C systems and EPS. As a result, there is a need for further guidance to aid risk management approaches for NPP cybersecurity programmes similar to the relationship between ISO/IEC 27001 [2] and ISO/IEC 27005 [5] to further optimize the allocation of limited resources for cybersecurity at NPPs.

Risk is typically described as consequences times likelihood. However, applying this description in the nuclear domain tends to prioritize consequence over likelihood. This inherent pragmatic assumption as the potentially severe consequences associated with nuclear power plants is unacceptable, and risks associated with these consequences cannot be accepted under any circumstances. Therefore, for instrumentation, control, and electrical systems critical to safety, a near-total reliance on consequence determines the level of effort to ensure these risks are mitigated/reduced to the greatest extent possible.

5.2 Assignment of security degrees in the management of risk

IEC 62645:2019, [1] 5.4.3.1.1.2 outlines a risk classification scheme that is based upon:

a) the consequences of a cyberattack;

b) functional assessment; and

c) consequence-based assignment approach that is rigorous and repeatable.

IEC 62645 [1] requires the application of a graded approach where sets of requirements (i.e., Security Degrees) are imposed on I&C systems and EPS based upon an analysis that identifies and evaluates the potential consequences resulting from compromise of these systems. The three security degrees from most demanding (i.e., most significant consequence) to least demanding are (SD1, SD2, and SD3) and baseline requirements (i.e., requirements that result in generic measures applied to all I&C systems and EPS).

The evaluation of consequences and SD assignments are dependent upon the following risk elements and activities:

- External Context (Regulation, Laws, Safety Classification);
- Internal Context (Operational Performance, Organization Objectives);
- Risk Identification (identification of consequences: ISO/IEC 27005:2018, [5] 8.2.6); and
- Risk Analysis (assessment of consequences: ISO/IEC 27005:2018, [5] 8.3.2).

IEC 62645 [1], however, gives no detailed description of how to implement risk management processes in conjunction with the security degrees and safety classification.

5.3 Safety correlation

IEC 62645:2019 [1], 5.4.3.1.2 provides guidance on the link between safety categories, safety classes, and SDs. The assignment of the appropriate SD to a system shall consider the effects of a compromise with its safety class. Consequently, the assignment of SD without critical thought based on the safety categories is not recommended as there is no strict one-to-one mapping between safety classes and security degrees for instrumentation, control, and electrical systems. If there is a potential for a cyberattack to increase the consequence severity of the system not operating as expected an assignment to a higher security degree may be warranted.

Typically, the final determination of the SDs is based on the function category or the maximum consequences of a malicious act or event on any part of the function. Concurrence by the personnel responsible for safety and those responsible for security on the determined SD is necessary to ensure that both perspectives are incorporated. This agreement is a necessity to provide the appropriate protection based on the maximum severity associated with the potential safety and security consequences. The agreement shall account for differences in measures put in place for safety that may not provide protection for security. For example, safety systems implement redundant components and systems to increase reliability and avoid potential safety consequences resulting from the failure of these components and systems, thereby ensuring availability. However, implementing identical redundant digital components that contain the same vulnerabilities will provide cyber security protection. The vulnerabilities can be exploited if the primary or secondary systems are active, and the attack can potentially impact integrity and confidentiality.

6 NPP cyber risk management challenges and analyses

6.1 General

This document identifies challenges considered not adequately covered by IEC 62645 [1]. The following sections of this document, summarize and provide analyses of cyber-risk approaches to risk management that could provide insight into these specific challenges affecting NPP operators when managing cybersecurity risks. Challenges affect effective cyber risk management. Challenges can increase uncertainty of elements necessary to measure or estimate risks, increasing complexity or ambiguity in relationships between related risks, activities, or systems, or involve different organizations or methods in risk management activities. The analyses were structured to align the cyber-risk approaches' elements with ISO/IEC 27005:2018 [5], Clauses 7 through 12.

The challenges evaluated in this document are listed in Table 1. Challenges impact risk management activities and increase uncertainty in risk management outputs, but do not represent specific cybersecurity risks (like those associated with theft or sabotage) that are identified, analyzed, evaluated, treated and managed by a nuclear facility operator,

Table 1 – Risk management challenges

#	Description	Rationale
1	**Aggregate risk of multiple units / locations:** There is a need for additional ways to evaluate levels beyond Security Degree assignment for aggregate risk of multiple units / locations.	The analysis focuses on multiple locations (not co-located), and some clauses of IEC 62645 [1] do not address multiple co-located units.
2	**Complexity of interdependencies and interactions:** Identifying and analyzing risks associated with attacks that target more significant functions through their interdependencies and/or interactions with less significant functions.	The NPP may not directly manage risks associated with interdependencies between systems and functions. For example, an attack on a diesel fuel supply may impact standby generator operation or external offsite power.

#	Description	Rationale
3	**Incident likelihood determination (leading to extremely rare but unacceptable events):** Estimating the likelihood of an extremely rare but unacceptable event is challenging.	Severe accidents at NPPs are extremely rare and can result in unacceptable radiological consequences. Accidents for which the initiating event is a cyberattack are rare and lack statistical data that would allow for likelihood to be considered in risk analysis and evaluation.
4	**Unknown or lacking sufficient detail for pre-developed components:** Pre-developed components that make up digital I&C systems have not been individually identified and evaluated for risks associated with NPP applications. In these cases, the Operator performs the risk assessment and may incur extra effort to treat risk.	Modern supply chains that result in digital I&C system components are complex. Specifically, the NPP operator is not provided a complete bill of materials and software provenance. This gap in information increases uncertainty in risk management activities.
5	**Differences in cyber-risk management:** Many differing risk management processes are used across or within member states.	The differences between member states' regulations or between organizations within a member state with respect to risk management are significant, especially where the level of abstraction is low (e.g., asset).
6	**Lack of abstract analysis methods:** There exists a general lack of guidance on risk management applied to conceptual facilities, systems, and processes where the technology or operational environment is not completely known. The risk impact has a greater dependence on the controlled process (e.g., primary asset; Domain Based Security) that may be unknown. There is a need to provide additional guidance on performing cybersecurity risk management at an abstract level.	Standard processes that provide for abstract analysis, where functions and levels are considered, are not available for this level of risk assessment. IAEA FCSRM [6] and NIST Risk Management Framework (RMF NIST SP800-37 [19]) provide for multiple levels of risk management processes based on the level of abstraction to separate the nature and source of risks to simplify tasks and activities associated with risk management.
7	**Uncertainty in vulnerability / susceptibility analysis:** Significant uncertainty is associated with the use of vulnerability / susceptibility analysis / documents necessary for effective risk management.	An unacceptable degree of uncertainty in the quality of vulnerability analysis of an I&C system increases the difficulty in performing effective risk management.
8	**Adversary characterization uncertainty:** Applying a cyber DBT/Adversary analysis to formal risk management of cybersecurity for NPPs is difficult due to the degree of uncertainty associated with adversary analysis in the DBT.	The application of cyber DBT within risk management and the degree of uncertainty associated with adversary analysis (e.g., DBT) increases the difficulty in performing effective risk management.
9	**Excessive information volume:** Effective and timely analysis of the large volume of information to assess risk is not practical (reasonable).	Modern digital information systems and cybersecurity risk management rely upon a tremendous volume of input data. Rationalizing this amount of information is challenging and could lead to ineffective risk management
10	**Lack of a common and comprehensive risk management process:** There exists a need for a common and comprehensive process that manages all significant risks, both regulatory and organizational objectives.	Significant risks are associated with consequences that will not result in radioactive release or theft of nuclear material (i.e., not required by regulation). The risks that lead to these consequences may not be identified and effectively managed.
11	**Advanced security capabilities incompatibility:** Security controls that provide advanced security capabilities (e.g., Cyber SOC or SIEM, cryptography, virtualization) are unsupported or incompatible with isolated or legacy systems reducing defense in depth and increasing risk.	Contemporary and effective technical measures cannot be implemented on legacy and/or physically isolated systems.

The cyber-risk approaches evaluated to determine whether effective guidance exists to address each of the challenges are listed in Table 2.

Table 2 – Cyber-risk approaches

Approach	Description	Entity
Facility Computer Security Risk Management (FCSRM) [6]	The FCSRM [6] assesses the impacts of compromise on facility functions and strategic risks.	IAEA
System Computer Security Risk Management (SCSRM) [6]	The SCSRM assesses the assets, systems, security controls, attack pathways, and tactical risks.	IAEA
EBIOS [11], [12]	EBIOS provides a formalized approach for assessing and treating risks within the field of information systems security, including support tools for contracting authorities, drafting documents, and raising awareness	Agence nationale de la sécurité des systèmes d'information (ANSSI)[4]
YVLA.12 [20]	YVLA.12 [20] sets out requirements for the management of information security at a nuclear facility, and it specifies in more detail the design requirements outlined in the STUK Regulation on Security in the Use of Nuclear Energy (STUK Y/3/2020) [20]	Finland
IEC 62443 [14]	IEC 62443 [14] provides a series of standards with a focus on Operational Technology (OT). The IEC 62443 considers systems and components in risk informing requirements and implementation of security controls.	IEC
Cyber Informed Engineering (CIE) [10]	CIE [10] provides a framework for understanding and addressing cyber threats to NPP systems and facilities.	US Department of Energy (DOE)
Hazards and Consequences Analysis for Digital Systems (HAZCADS [9])	HAZCADS [9] leverages Systems Theoretic Process Analysis (STPA) [21] to identify Unsafe Control Actions (UCAs) within control systems that may result from faults including those caused by cyberattacks. This analysis allows for risk-informed hazard analysis and selection of security controls.	Electric Power Research Institute (EPRI)
Harmonized Threat Risk Assessment (HTRA) [8]	HTRA [8] provides a scalable framework to address strategic and tactical risks. HTRA provides several tools and tables to simplify the risk management processes.	Canada
Malicious Acts Guidelines for Computer-Based Systems (SEWD) [22]	These guidelines are “classified information – for official use only” and not publicly available. They cover the whole IT-security framework for the nuclear field with some parts for cyber risks.	Germany
Information Security Technology—Implementation Guide to Risk Assessment of Industrial Control Systems GB/T 36466 [23]	The national standard GB/T 36466-2018 [23] “Information security technology—Implementation guide to risk assessment of industrial control systems” provides guidelines for cyber security assessment for industrial control systems.	China
Regulatory Guide (RG) 5.71 [24]	RG 5.71 provides one acceptable approach regarding the protection of digital computers, communications systems, and networks from a cyber attack as defined by Title 10 Code of Federal Regulations (CFR) Part 73.1 [25]	US Nuclear Regulatory Commission (NRC)

[4] EBIOS [11][12] is a risk analysis method recommended by ANSSI but is not the national approach for France which is detailed in [14]. This approach consists of an approved procedure for information systems of vital importance. This procedure requires NPP operators to periodically perform risk analysis (which can be performed using EBIOS) as well as security audits and formal management of the associated risks to information systems of vital importance.

Approach	Description	Entity
Russian Federal Service for Technical and Export Control (FSTEC) [26], [27], [28], [29], [30], [31], [32], [33]	FSTEC [26], [27], [28], [29], [30], [31], [32], [33] provides a series of documents with a focus on the security of the control systems for the critical infrastructure. The FSTEC classifies the systems using risk-oriented approach and assign the set of the security controls to protect the control system.	Russia
His Majesty's Government (HMG) Information Assurance Standard Numbers 1 & 2 and Domain Based Security (DBSy) [34] [35]	Provides a methodology for technical risk assessment and risk treatment for implementation by Central Government Departments and Agencies. It was also recommended for the wider public sector. The technical risk assessment is supported the DBSy modelling technique. The standard has been withdrawn but is still in use by NPPs.	United Kingdom

This document was developed through the execution of four tasks:

a) Identification and description of NPP operator-specific challenges associated with risk management are detailed in Table 1.

b) Identification and analysis of cyber-risk approaches that may offer insights into reducing the challenges; the cyber-risk approaches are detailed in Table 2.

c) Using ISO/IEC 27005:2018 [5] as the base:

   1) Associate the Challenges (Table 1) with specific ISO/IEC 27005:2018 [5] Risk Phases and Clauses (process shown in green in Figure 2).

   2) Associate the cyber-risk approaches with ISO/IEC 27005:2018 [5] Risk Phases and Clauses (process shown in blue in Figure 2).

d) Combine the challenges and cyber-risk approaches, leveraging ISO/IEC 27005:2018 [5] Clause numbers as an index and summarize the combined data.

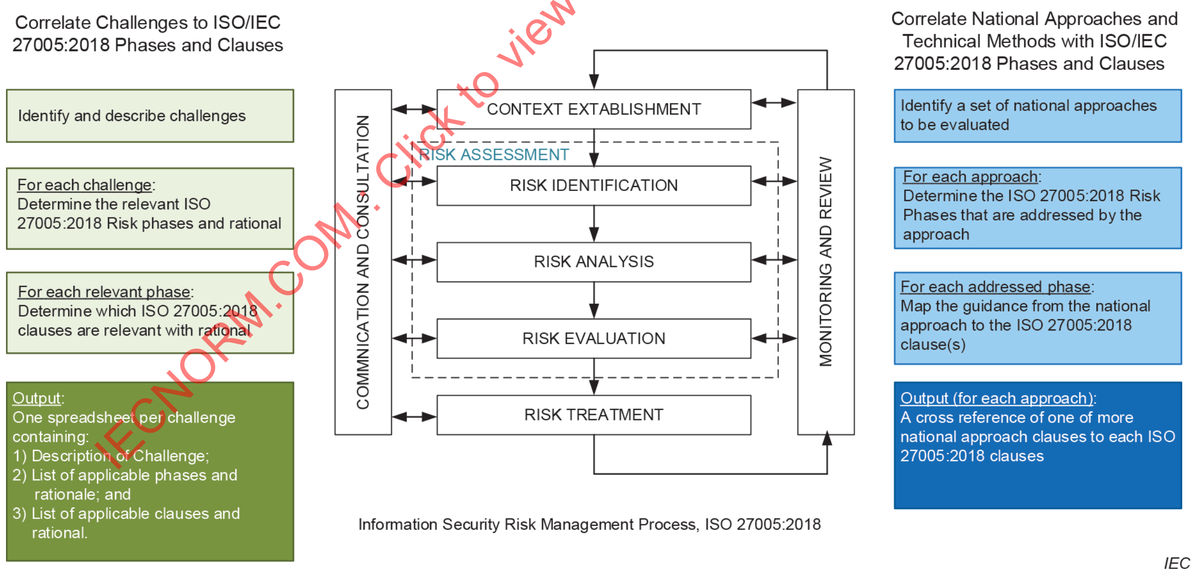

Correlate Challenges to ISO/IEC 27005:2018 Phases and Clauses
Identify and describe challenges
For each challenge: Determine the relevant ISO 27005:2018 Risk phases and rational
For each relevant phase: Determine which ISO 27005:2018 clauses are relevant with rational
Output: One spreadsheet per challenge containing:
1) Description of Challenge;
2) List of applicable phases and rationale; and
3) List of applicable clauses and rational.
COMMNICATION AND CONSULTATION
CONTEXT EXTABLISHMENT
RISK ASSESSMENT
RISK IDENTIFICATION
RISK ANALYSIS
RISK EVALUATION
RISK TREATMENT
MONITORING AND REVIEW
Information Security Risk Management Process, ISO 27005:2018
Correlate National Approaches and Technical Methods with ISO/IEC 27005:2018 Phases and Clauses
Identify a set of national approaches to be evaluated
For each approach: Determine the ISO 27005:2018 Risk Phases that are addressed by the approach
For each addressed phase: Map the guidance from the national approach to the ISO 27005:2018 clause(s)
Output (for each approach): A cross reference of one of more national approach clauses to each ISO 27005:2018 clauses
IEC

Figure 2 – Technical report development approach

6.2 Challenge 1: Aggregate risk of multiple units / locations

There is a need for additional ways to evaluate levels beyond security degree assignment for aggregate risk of multiple units/locations. For example, a system can be installed on several units or multiple locations. Current analyses do not focus on multiple installations of the same unit with identical, similar, or common design, configuration, and functionality.

While the impact of a compromise of a single system would affect a single unit or location, the attack could propagate to other identical systems, or an additional attack could be performed targeting like systems. For example, an adversary could leverage a supply chain attack to compromise a vulnerable system located at all units and locations. The current approach to risk management may not consider these strategic risks.

In many current approaches, risk analysis focuses on multiple locations (not co-located), and some clauses in IEC 62645 [1] do not address multiple co-located units. However, both Canada's HTRA [8] and Finland's YVLA12 [20] provide flexibility when setting the scope and context of the risk management process.

6.3 Challenge 2: Complexity of interdependencies and interactions

Identifying and analyzing risks associated with attacks that target more significant functions through their interdependencies and/or interactions with less significant functions is a challenge.

An example of this challenge is the Colonial Pipeline attack that disrupted gasoline supplies to the US Northeast. This attack affected IT systems that interfaced with I&C systems that controlled delivery of gasoline. The attack led to prolonged disruption of gasoline supplies.

Prolonged and widespread disruption of fuel supplies to an NPP may have cascading effects leading to increased risks to NPP systems and processes that depend on fuel supply (e.g., emergency generators).

A non-malicious event that supports this challenge was the loss of bulk electrical supply in the northeast of North America in 2003 (i.e., Northeast blackout of 2003). The complexity of the bulk electrical supply resulted in a latent design deficiency where a failure mode and effects were not anticipated and accounted for resulting in severe consequences. Similarly, latent design deficiencies can lead to flaws that may be exploited by adversaries by cyber-attack leading to consequences and affecting risk management.

Challenge 2 differs from Challenge 1. The interdependencies are targeted in Challenge 2, whereas Challenge 1 addresses a common vulnerability or weakness in multiple locations.

6.4 Challenge 3: Incident likelihood determination

Estimating the likelihood of an extremely rare but unacceptable event is challenging as likelihood values are associated with large uncertainty. A specific example is performing a risk analysis, including the likelihood, of sabotage at NPPs where the initiating event is a cyber-attack.

The example postulated scenario is assumed to be extremely unlikely as it would involve multiple and persistent access to various systems, complex interactions, and other difficult elements for a potential adversary to achieve radiological sabotage.

6.5 Challenge 4: Unknown or lacking sufficient detail for pre-developed components

Pre-developed and purchased components that make up digital I&C systems have not been individually identified and evaluated for risks associated with NPP applications. In these cases, the Operator performs the risk assessment and may incur extra effort to treat the risk.

This challenge differs from Challenge 2: Complexity of Interdependencies and Interactions. This challenge occurs when the NPP operator does not have sufficient resources or the capability (e.g., as in reverse engineering) to span the information gap that is necessary to perform effective risk management.

Additionally, the NPP operator may be restricted by legal obligations (e.g., EULA) prohibiting them from performing these activities. Or, if there are sufficient resources and the capability is present to gather sufficient information to perform effective risk management, the supplier may have limited information about a proprietary product upon which the supplied item depends.

6.6 Challenge 5: Differences in cyber-risk management

There are many different risk management processes used across Member States. Reasons for this difference can come from:

a) differing regulatory constraints on risk management or risk methodologies across Member States; and

b) accreditation of (risk analysis, risk treatment) defensive architecture, zones, or libraries of common controls for risk modification to sensitive systems and digital assets, and associated V&V processes.

This challenge is particularly impactful to the system or asset-level risk management. At the system/asset level, it is difficult to accredit common controls, DCSA elements, and associated V&V processes. The greater the specificity needed to perform risk management tasks and activities, the greater the potential for modifications to the process to account for national differences.

6.7 Challenge 6: Lack of abstract analysis methods

There exists a general lack of guidance on risk management applied to conceptual facilities, systems, and processes where the technology or “asset” is unknown. There is a need to provide additional direction on performing cybersecurity risk management at an abstract level.

The lack of abstract analysis methods increases the difficulty when comparing cyber versus non-cyber risks. For example, it is challenging to :

a) compare and rationalize these risks (i.e., equate cyber versus non-cyber risks and treat them in an equivalent manner) within the NPP operator’s management system; and

b) establish the context for assessing the comparable risks.

For new power plants, some approaches require two risk assessment phases – Facility Level and Systems Level.

First level – Facility Level: systems technology is unknown (could be analogue), validates the DCSA zone/level model; differing risk decision criteria (established context is different) and

Second level – System Level: SD is informed/established by the DCSA model; the system shall comply with SD requirements.

6.8 Challenge 7: Uncertainty in vulnerability / Susceptibility analysis

There is a challenge with accommodating uncertainty associated with vulnerability/susceptibility analysis/documents necessary for effective risk management.

Vulnerability analysis is based on known vulnerabilities, susceptibilities, weaknesses, or adversary tactics, techniques and procedures. This analysis does not account for unknown or unreported weaknesses or exposures. Example: I&C systems that utilize general purpose operating systems rely on a “Penetrate and Patch” approach for security that is not readily accommodated by nuclear I&C configuration management processes.

At any operational time, any operating system has more than several hundred open vulnerabilities, and many of these are critical (i.e., ease of exploitation with high potential impact(s) from compromise).

I&C project management has long lead times and is frequently delayed. The time between design approval, installation, commissioning, and placing into service is significant. Risk assessments completed at earlier stages of this process may be significantly impacted by new weaknesses or vulnerabilities that become known during this period.

6.9 Challenge 8: Adversary characterization uncertainty

There is a challenge in applying DBT/Adversary analysis to formal risk management of cybersecurity for NPPs.

Challenge 8 is similar to Challenge 5 above but differs in the focus on uncertainty with adversary analysis and not the differences in applying this analysis and regulatory requirements.

Adversary analysis is based upon incomplete intelligence informed largely by expert opinion and relies upon the application of sense-making loops to “fill in” missing details concerning adversary capabilities, resources, motivation, opportunity, and intent.

In many national regulations, the DBT is an instrument that delineates the risk-sharing/transfer arrangement for security between state and operator. However, States have not reported, or have not disclosed, a robust or proven capability to detect, intercept, infiltrate, and disrupt cyber adversaries that exceed the DBT.

The developed adversary analysis does not clearly bind threats associated with identified risks because they are too vague or have too much uncertainty when considering the potential consequences of NPP operations. This lack of certainty may not allow for efficient risk management.

6.10 Challenge 9: Excessive information volume

There exists a challenge for the NPP personnel to analyze large volumes of information and assess risk in an effective and practical (reasonable) time period during both the design phase(s) and operations. Additional analysis is required to leverage the safety analysis when considering specific impacts of cyberattacks (i.e., maloperation) by using the safety analysis on each system. Cybersecurity risk management can benefit from these safety analyses (e.g., non-malicious threats like floods). However, safety analysis may not consider specific failure modes and effects associated with cyberattacks. For example, a safety-related air operated valve and high-pressure instrument air unexpected modes of operation (mal-operation) are not considered within the safety analysis.

The resources required to perform a more in-depth analysis that requires additional time and information place excessive demands above the resources available to NPP operators. Additionally, the sensitivity of disclosing information regarding cybersecurity risks results in limiting the personnel who can provide critical review and analysis. Restricted access to sensitive information coupled with a lack of advancement/availability of risk support tools/technology (i.e., modelling and simulation) to ease the challenge associated with data input/analysis and rationalization results in significant reliance on expert opinion or experience.

6.11 Challenge 10: Lack of a common and comprehensive risk management process

There is a need for a common and comprehensive process that manages all significant risks and regulatory and organizational objectives. Other risks may include the long-term impact on production (See Challenge 2 main transformer example), reputation, political, and reduction of public support for nuclear power (e.g., the cyber attack on Korea Hydro and Nuclear Power Co. Ltd, in 2014). For example, a unit outage impacts the maintenance schedule.

A common repeatable process has the potential to reduce effort and errors while providing a comprehensive approach to risk management.

6.12 Challenge 11: Advanced security capabilities incompatibility

There exists a challenge whereby security controls that provide advanced security capabilities (e.g., cyber-SOC or SIEM, cryptography, virtualization) are unsupported or incompatible with isolated or legacy I&C systems reducing defence in depth and increasing risk.

“Air Ggp”, and/or isolated systems and networks impairs network security and real-time (or continuous) monitoring and response. Air gaps eliminate the potential for holistic, comprehensive Security Information and Event Management (SIEM) systems that provide real-time alerting, perform threat hunting, as well as fail to prevent or detect insider threats. The reliance on isolation assumes that placement within Vital Areas is sufficient risk modification for cyberattacks. However, it does not protect against malicious actions (witting or unwitting) of individuals with authorized physical and portable media / mobile device access, and supply chain attacks. Additionally, legacy I&C systems and protocols do not support contemporary (non-deprecated) cryptographic mechanisms.

Use of fail-secure, deterministic, unidirectional data communication pathways (e.g., data diodes) may provide logical isolation while still allowing for real-time operation and continuous monitoring.

7 Cyber-risk approaches versus challenges by ISO/IEC 27005

7.1 General

Cyber-risk approaches (see Annex A through Annex K) were evaluated to determine whether their guidance addressed one or more of the identified challenges (see Clause 7). The evaluation was structured based on the ISO/IEC 27005:2018 [5] clauses to simplify subsequent analysis and summary.

Each of the subclauses below applies to a specific ISO/IEC 27005:2018 [5] clause and provides:

- A summary of the ISO clause
- Applicable challenges to which the clause applies
- Summary of the cyber-risk approaches based on the evaluations (see Annex A through Annex K)
- The cross-reference table legend is below:
  - “Key” – approach contains key insight(s). Key insights are those elements of a cyber-risk approach that have significant benefit to cyber security risk management, and which could be considered for inclusion in a potential new standard for cyber risk management.
  - “X” – approach contains guidance but is not a key insight.
  - Blank – approach does not address the challenge.

7.2 ISO/IEC 27005:2018, 7.1 General considerations

7.2.1 Summary

ISO/IEC 27005:2018, [5] 7.1 requires that an external and internal context for cybersecurity risk management be established. This context involves:

a) setting the basic criteria necessary for information security risk management (ISO/IEC 27005:2018 [5], 7.2);

b) defining the scope and boundaries (ISO/IEC 27005:2018 [5], 7.3), and

c) establishing an appropriate organization operating the information security risk management (ISO/IEC 27005:2018 [5], 7.4).

7.2.2 Applicable challenges

The external and internal context is particularly important for challenges impacted by events and information from inside and outside the organization. For example, the internal context is vital for Challenge 11 (advanced security capabilities incompatibility), as a facility's technology and modification processes would demand specific approaches to obsolescence and the feasibility of integrating advanced technologies. Similarly, the external context is essential for Challenge 10 (common and comprehensive risk process), as national risk approaches may influence the scope and boundaries of risk management. See Table 3.

Table 3 – ISO/IEC 27005:2018, 7.1: Applicable challenges

Challenge	Description
2	Complexity of Interdependencies and Interactions
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process
11	Advanced Security Incompatibility

7.2.3 Summary of key approaches

Cyber-risk approaches with key insights for Challenge 2 are:

- HAZCADS [9] relies upon scenario-informed fault trees, modified fault trees that allow fault tree analysis (FTA). FTA provides a structured manner to analysis systems and interactions.
- IAEA CSRM [6] identifies interdependencies and interactions that need to be considered.
- US NRC [24] addresses the identification and analysis of risks associated with attacks that target safety, security, and emergency preparedness (SSEP) functions and associated systems through their interdependencies and / or interactions with less significant functions / systems.

Key approaches for Challenge 4 are:

- HAZCADS [9] use of FTA will minimize the impact of pre-developed components if there exists a traditional FTA (e.g., existing operating fleets that leverage probabilistic risk assessment (PRA)).
- IEC 62443 [14] has a layered series of standards that specifically address Component layer requirements (IEC 62443 Part 4 [36], [37]).

Key approaches for Challenge 6 are:

- HAZCADS [9] demands a control structure model abstraction to allow for effective STPA [21] analysis to identify UCAs and inform fault tree analysis.
- IEC 62443 [14] leverages a tiered approach focused on different types of organizations. IEC 62443-2 [38], [39].
- is focused on operating the organization's programmes, IEC 62443-3 [40], [41] focuses on architectural analysis, and IEC 62443-4-2 [37] is focused on component analysis.

Key approach for Challenge 9 is:

- IAEA CSRM [6] provides a tiered analysis approach (facility, system) with compartmentalized activities to reduce the amount of information needed for each activity.
- HAZCADS [9] leverages a type of FTA that can provide a pathway to utilize PRA. PRA is associated with many tools and processes to simplify or support analysis than can reduce excessive information.

Key approaches for Challenge 10 are:

- Germany's cyber-risk approach [22] allows different State authorities to authorize differing risk management processes while being compliant with federal guidelines.
- IAEA CSRM [6] allows for all risks to be considered in a common and comprehensive manner. The facility covers strategic risks with unacceptable (major/severe) consequences to the operator, whereas the system covers tactical risks associated with graded consequences impacting the correct operation of a system.
- IEC 62443 [14] provides lists of risk sources that can provide a basis for a common and comprehensive risk process.
- Russia's FSTEC [29], [30], [31], [32] approach provides common ground for challenge 10 by enforcing the same approach for all critical infrastructure.

7.2.4 Cross-reference table (Table 4)

Table 4 – ISO/IEC 27005:2018, 7.1: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China		X		X	X		X		X	X	X
Germany		X			X		X		X	Key	
HAZCADS		Key		Key		Key			Key		
IAEA CSRM		Key							Key	Key	
IEC 62443		X		Key		Key				Key	
Russia				X		X			X	Key	
US NRC		Key		X	X		X		X	X	X

7.3 ISO/IEC 27005:2018, 7.2 Basic criteria

7.3.1 Summary

Risk management basic criteria involve identifying an approach, evaluation, impact, and acceptance criteria. Examples of basic criteria are the significance of sensitive digital assets and the importance of their confidentiality, integrity, and availability. Different risk approaches and/or acceptance criteria can also apply to different risk classes (e.g., strategic, tactical, nuclear safety, and security).

7.3.2 Applicable challenges

Risk management basic criteria are particularly important for challenges that affect risk criteria. Specifically, the type of approach, evaluation, impact, and acceptance criteria significantly contribute to Challenges 2, 3, 5, 7, and 10. For example, interdependencies (Challenge 2) or vulnerabilities of pre-developed components (Challenge 7) may be difficult to assess at a higher level of complexity or detail with the potential to bring about Challenge 9 (excessive information). National differences in risk tolerance/acceptance (Challenge 5) also need to be considered when applying a common and comprehensive process, especially for organizations operating in multiple national jurisdictions (Challenge 10).

Additionally, the sequence or timing of when specific risk management activities are conducted could impact these challenges. See Table 5.

Table 5 – ISO/IEC 27005:2018, 7.2: Applicable challenges

Challenge	Description
1	Aggregate risk of multiple units/locations
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
9	Excessive Volume of Information
10	Lack of a Common and Comprehensive Risk Management Process

7.3.3 Key approaches

Key approach for Challenge 1 is:

- A key step of UK IS/DBSy [34], [35] is the requirement to create a model of the I&C assessment scope. The model can include a full plant with many Units or can be extended to other plants, although in practice the assessment is done on a plant basis.

Key approaches for Challenge 2 are:

- HAZCADS [9] uses STPA [21] to identify UCAs and link them to hazards and losses (i.e., consequences). This linkage requires deliberate analysis of interactions and interdependencies.
- IAEA CSRM [6] listed interdependencies and interactions that can be used to support risk evaluation criteria and impact criteria identification.
- IEC 62443 [14] tiered approach covers the interactions and interdependencies between different types of organizations, all managed by the operating organization.
- UK IS/DBSy [34], [35] requires the modelling and analysis of requirements for exchanging data between systems and the impact of those interactions in the evaluation of risk.

Key approach for Challenge 3 is:

- CIE [10] focuses on consequences to reduce the impact of uncertainty on incident likelihood. Additionally, CIE accredits cybersecurity culture and planned resilience in protecting against incidents, reducing the likelihood.

Key approaches for Challenge 4 are:

- IEC 62443 Part 4 [36], [37] provides requirements on components that suppliers provide. These requirements identify key attributes of acquired components to support the cybersecurity objectives of the operating organization.
- UK IS/DBSy [34], [35] requires the modelling of assets within the scope of the technical risk assessment to consider the systems that support the evaluated assets, this will include the need to assess components delivered by supply chain.

Key approaches for Challenge 6 are:

- HAZCADS [9] uses abstraction to simplify the STPA [21] efforts. STPA simplifies the cybersecurity analysis by only considering the impact of the cyberattack to cause a system to mal-operate.
- IEC 62443-2 [38], [39] provides abstract analysis to allow an organization to develop and implement its cybersecurity management system (i.e., programme).
- UK IS/DBSy [34], [35] provides a modelling methodology that allows for the creation of a plant abstract model based on I&C systems significance rather than specific technology or system architecture.

Key approach for Challenge 7 is:

- Canada's HTRA [8] provides pre-compiled lists of these vulnerabilities to minimize uncertainty, especially in reducing unknown or missing vulnerability/susceptibility analysis considerations.

Key approach for Challenge 9 is:

- IAEA CSRM [6] leverages existing information and analysis to reduce the information necessary to be considered/re-evaluated to perform cybersecurity risk management. The key activity is the facility characterization which leverages the Facility's safety analysis and other documents.
- The tiered approach of IEC 62443 [14] compartmentalizes the necessary information to perform key risk activities in each tier.

Key approaches for Challenge 10 are:

- France's cyber-risk approach [11], [12] does not exclude considering other systems not directly associated with the consequences of theft of NM or radiological sabotage. The French cyber-risk approach allows NPP operators to apply a common and comprehensive risk management approach to significant and other systems.
- Germany's cyber-risk approach [22] pre-classifies systems and their risks under regulatory requirements by the competent authority.
- IAEA CSRM [6] provides an ordered list of the effects of a system compromise on functions. This approach can provide a basis for setting risk evaluation, impact, and acceptance criteria to support a common and comprehensive risk management process.
- IEC 62443 [14] is an international standard for industrial automated control systems (IACS) or operational technology (OT) systems. It broadly addresses risks associated with critical infrastructure and can inform a common and comprehensive approach.
- Russia's cyber-risk approach [29], [30], [31], [32] provides common ground for challenge 10 by enforcing the same approach for whole all critical infrastructure.US NRC guidance was primarily developed for risks associated with consequences that will result in radioactive release. It could be used as a starting point for developing a cybersecurity framework for addressing risks not required by regulation.
- UK's IS/DBSy [34], [35] provides a very detailed and repeatable stepped process to perform the technical risk assessment, with guidance and templates for use at each step.

7.3.4 Cross-reference table (Table 6)

Table 6 – ISO/IEC 27005:2018, 7.2: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China		X			X		X		X	X	
CIE		X	Key	X		X			X	X	
France		X					X			Key	
Germany		X	X	X	X					Key	
HAZCADS		Key		X		Key				X	
HTRA		X			X		Key		X	X	
IAEA CSRM		Key			X		X		Key	Key	
IEC 62443		Key		Key		Key	X		Key	Key	
Russia	X	X								Key	
US NRC		X			X		X		X	Key	
UK IS/DBSy	Key	X		X		Key		X	X	Key	

7.4 ISO/IEC 27005:2018, 7.3 Scope and boundaries

7.4.1 Summary

Scope and boundaries need to be defined to ensure effective cybersecurity risk management. The assessment scope needs to account for all relevant assets and bounded to ensure risks are considered both within and through them.

Scope and boundaries rely on an organization's policies, risk management approach, functions and structure, sensitive digital assets, DCSA, and stakeholders' expectations.

7.4.2 Applicable challenges

These challenges affect how scope and boundaries are set. For example, boundaries need to consider risks that may arise through interdependencies and interactions (i.e., Challenge 2) between other organizations or systems that may not be directly assessed. The scope of the risk assessment may affect Challenge 5 and Challenge 10. Specifically, differences in national risk management typically reflect different national stakeholders (e.g., national regulators). Additionally, scope and boundaries are associated with Challenges 4, 7, and 9. A wide scope with limited abstraction would lead to uncertainty in vulnerability analysis and/or lack of sufficient detail or excess volume of information. See Table 7.

Table 7 – ISO/IEC 27005:2018, 7.3: Applicable challenges

Challenge	Description
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
6	Lack of Abstract Analysis Method
7	Uncertainty in Vulnerability / Susceptibility Analysis
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process

7.4.3 Key approaches

Key approach for Challenge 1 is:

- A key step of UK IS/DBSy [34], [35] is the requirement to create a DBSy model that defines of the I&C assessment scope. The model can include a full plant with many units or can be extended to other plants.

Key approaches for Challenge 2 are:

- IAEA FCSRM [6] provides a list of interdependencies to be considered within the risk process. This list could be used to set the scope and boundaries of risk assessments and leverage a tiered analysis, and this would reduce the impact of lacking sufficient detail (Challenge 4) and excessive information volume (Challenge 9).
- IEC 62443-3-2 [40] provides a process to investigate the interdependencies and interactions with other systems.
- UK IS/DBSy [34], [35] requires the definition of the specific Focus of Interest (FOI) that defines the scope of the technical risk assessment, as well as to identify any interconnections with other systems outside the FOI.

Key approaches for Challenge 4 are:

- Russia [29], [30], [31], [32] provides guidance to investigate software, firmware and hardware vulnerabilities related to pre-developed components.
- UK IS/DBSy [34], [35] as part of defining the scope allows the modelling of interactions between systems and organisations, including those responsible for system design and development i.e., assessment of the supply chain.

Key approach for Challenge 5 is:

- Germany's cyber-risk approach [22] provides two frameworks (BSI 200-3 [42] and ISO/IEC 27005 [5]). These frameworks are not fully compatible but generally lead to similar outcomes. Application of either framework provides a path to compliance with regulatory requirements. The framework used is dependent upon the utility/operator and vendors or integrators need to be able to comply with either.

Key approaches for Challenge 7 are:

- Canada's HTRA [8] allows for smaller modular assessments that may limit the level of uncertainty in the analysis.
- IEC 62443 [14] specifically addresses component layer requirements (62443-4 [36], [37]) to identify and describe a component's vulnerabilities and addresses vulnerabilities of components provided by the vendor.

Key approaches for Challenge 9 are:

- Canada's HTRA [8] provides pre-compiled lists of these criteria (e.g., asset valuation, safeguard (control measures) listing, threat (sources) listing, impacts, etc.), hierarchical structures, taxonomy, and an extensive glossary to allow for modular assessments that can compartmentalize information, thereby alleviating the challenge of excessive information.
- IAEA CSRM [6] tiered analysis sets the scopes and boundaries to prioritize and compartmentalize information to ease excessive information challenges.
- UK IS/DBSy [34], [35] modelling allows for identification of focus of interest (FOI) from the overall model. Each FOI is then assessed independently, helping to manage the large amount of information.

Key approaches for Challenge 10 are:

- France's cyber-risk approach [11], [12] allows NPP operators to set the scope and boundaries of risk management. It only requires a minimum set of significant systems that shall be considered.
- Canada's HTRA [8] provides a list of risk sources that can provide a basis for a common and comprehensive risk process. These resources can help NPPs address stakeholders' expectations, the socio-cultural environment, and other constraints affecting the organization.
- Russia's approach [29], [30], [31], [32] provides a common and comprehensive approach to set the scope and boundaries of risk management for all critical infrastructure.

7.4.4 Cross-reference table (Table 8)

Table 8 – ISO/IEC 27005:2018, 7.3: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China		X		X	X		X		X	X	
CIE		X	X	X		X			X		
France		X		X			X		X	Key	
Germany					Key					X	
HAZCADS		X		X		X			X	X	
HTRA		X		X	X		Key		Key	Key	
IAEA CSRM		Key		X	X		X		Key	X	
IEC 62443		Key		X		Key					
Russia		X		Key		X	X		X	Key	
UK IS/DBSy	Key	Key		Key	X	Key	X		Key		

7.5 ISO/IEC 27005:2018, 7.4 Organization for information security risk management

7.5.1 Summary

The organization and responsibilities of the cybersecurity risk management process shall be established and maintained. Development of the process, identifying stakeholders, defining the roles and responsibilities of entities, and other key aspects of the process shall be managed.

7.5.2 Applicable challenges

Challenges 2, 4, and 9 are impacted by how the risk management process is organized. A common risk process, organization, and experts shall provide a consistent approach to address these challenges. Challenges 5 and 10 would benefit from a single risk process and responsible organization, thereby reducing variance through centralized control and the conduct of a risk management programme. Challenge 7 may result in the need to address this within decision escalation paths or external parties to supplement analysis. See Table 9.

Table 9 – ISO/IEC 27005:2018, 7.4: Applicable challenges

Challenge	Description
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process

7.5.3 Key approaches

Key approaches for Challenge 9 are:

- Canada’s HTRA [8] outlines how organizational structure may be too large and complex to handle excessive information coherently. HTRA details how to define roles and responsibilities to ensure excessive information is distributed across several roles to a manageable level.
- IAEA CSRM [6] specifies key outputs and outcomes of the risk management process. This method may allow for redundant or unnecessary information to be filtered out.

Key approach for Challenge 10 is:

- France’s cyber-risk approach [11], [12] mandates the involvement of specific multi-disciplinary personnel and roles for security approval allowing for consequences to be identified that are impactful but not regulatory.
- In Russia’s cyber-risk approach [29], [30], [31], [32], the security approval involves the regulator, the owner and operator (usually it is the same), the security officer as well as technical experts. That provides a key insight to dealing with challenge 10 in detecting consequences that are significant but are not regulatory.

7.5.4 Cross-reference table (Table 19)

Table 10 – ISO/IEC 27005:2018, 7.4: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
France		X		X			X		X	Key	
HTRA		X		X	X		X		Key	X	
IAEA CSRM		X		X	X		X		Key	X	
IEC 62443		X		X	X		X		X	X	
Russia		X		X					X	Key	
US NRC		X	X	X		X			X		
UK IS/DBSy		X		X		X			X	X	

7.6 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment

7.6.1 Summary

A general description of information security risk is needed to identify, quantify, or qualitatively describe and prioritize risks. The risk assessment consists of risk identification, analysis, and evaluation and needs to be consistent with established criteria.

7.6.2 Applicable challenges

These challenges require a risk assessment process described with inputs, actions, and implementation guidance. Particularly, Challenge 1 needs to consider strategic risks differently, possibly by application of abstract analysis methods, whereas more detailed analysis may experience Challenges 2, 4, and 7.

A general description of the risk assessment process considers the need to be consistent regardless of the necessary level of detail (i.e., challenge 10). See Table 11.

Table 11 – ISO/IEC 27005:2018, 8.1: Applicable challenges

Challenge	Description
1	Aggregate Risk of Multiple Units / Locations
2	Complexity of Interdependencies and Interactions
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process

7.6.3 Key approaches

Key approach for Challenge 1 is:

- UK IS/DBSy [34][35] methodology consisting of well-defined steps can be applied to different scope of assessment, including an assessment of the overall NPP I&C.

Key approach for Challenge 2 is:

- The Chinese cyber-risk approach [23] recommends that a mock-up of the system be built. This process could be of benefit in identifying a system’s functional interdependencies and interactions with less significant functions.
- IAEA [6] specifically indicates that the operator shall set the scope to include an assessment inclusive of those risks associated with this challenge.

Key approaches for Challenge 4 are:

- US NRC approved the methodology in NEI 10-04, “Identifying Systems and Assets Subject to the Cyber Security Rule,” [43] that could help the Operator when identifying and prioritizing risks to SSEP functions and systems associated with pre-developed components during the risk assessment.

Key approach for Challenge 6 is:

- IAEA CSRM [6] prioritizes analysis of facility functions to address strategic risks in compromising or altering these functions. Functions are an emergent property (abstraction) resulting from the complex interactions and organizations of a set of elements within a system. This analysis technique is widely used for safety analysis.

Key approach for Challenge 7 is:

- IEC 62443 [14] application of common measures, such as DCSA implementing defense in depth reduces the impact of uncertainty in Vulnerability/Susceptibility Analysis on risk management.

Key approach for Challenge 8 is:

- IEC 62443 [14] leverages an attack pathway analysis approach that aims to deny access of the adversary to I&C and EPS by implementing a DCSA. The DCSA may limit the effect of uncertainty on risk management. IEC 62443-3-2 [40] contains a staged risk analysis, first to implement a DCSA and a second more detailed assessment to modify unacceptable residual risks.

Key approach for Challenge 9 is:

- IEC 62443 [14] leverages a tiered approach to manage the facility, system, and supplier risks. Categorizing the information in this way reduces the amount of information required for each activity.

Key approaches for Challenge 10 are:

- IAEA CSRM [6] leverages functions as a common and comprehensive means to assess all risks. Correct performance of functions is necessary for an organization to achieve all objectives.
- UK IS/DBSy [34], [35] applies a consistent risk assessment process that is common and comprehensive for all risks impacting the NPP I&C systems.

7.6.4 Cross-reference table (Table 12)

Table 12 – ISO/IEC 27005:2018, 8.1: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China	X	Key		X		X	X			X	
Germany		X		X			X				
IAEA CSRM		Key		X		Key	X			Key	
IEC 62443		X		X		X	Key	Key	Key	X	
US NRC	X	X		Key		X	X			X	
UK IS/DBSy	Key	X		X	X		X	X	X	Key	

7.7 ISO/IEC 27005:2018, 8.2 Risk identification

7.7.1 Summary

Risk identification involves the identification of assets; threats; existing controls; vulnerabilities; and consequences. The purpose of risk identification as it relates to cybersecurity risk for NPPs is to understand the impacts of compromise, how and why the impact could arise from cyberattacks, and existing mitigations to prevent or protect against these impacts.

7.7.2 Applicable challenges

Subclause 7.7 (i.e. Risk identification) is associated with all challenges.

For example, the identification of assets and vulnerabilities is associated with Challenges 1 (multiple locations), 2 (inter-dependencies), 4 (pre-developed components), 5 (national differences), 7 (uncertainty vulnerabilities), and 9 (excessive information) as the number of assets and their vulnerabilities could be significant.

The identification of threats is associated with Challenge 8 and Challenge 11. Challenge 11 also pertains to existing controls. Advanced technologies can enable techniques such as threat-hunting and behaviour-based detection. Incompatibility with these technologies reduces information regarding threat sources on an organization's networks and systems and may increase uncertainty in threat identification and adequacy of the control measures. See Table 13.

Table 13 – ISO/IEC 27005:2018, 8.2: Applicable challenges

Challenge	Description
1	Aggregate Risk of Multiple Units / Locations
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process
11	Advanced Security Capabilities Incompatibility

7.7.3 Key approaches

Key approaches for challenge 1 are:

- UK IS/DBSy [34], [35] methodology uses a threat-based risk assessment, also allows for modelling of an entire facility, making it easier to identify threats that could impact whole plant.

Key approaches for Challenge 2 are:

- CIE [10] principles are effective in supporting challenges but are very general. However, CIE-related literature leverages HAZAOP analysis to complement risk analysis that considers information and data flow that could harm systems.
- Canada's HTRA [8] provides detailed lists within its annexes to identify risks and identify and describe the potential interdependencies and interactions between items on these lists via grading tables.
- IAEA CSRM [6] considers interactions and interdependencies at the facility level (via functions) and system level (e.g., information flows, engineering/resources) to identify risks in a similar manner but through independent processes.
- IEC 62443-3-2 [40] demands special attention to safety-related systems, wireless, internet-connected devices, mobile devices, and assets that other organizations manage. These are key interdependencies and interactions that increase complexity.

- UK IS/DBSy [34], [35] step 1 includes as part of the asset identification, the modelling of systems and organisations interdependencies.

Key approaches for Challenge 4 are:

- CIE [10] and related literature (see Clause B.13) provides categories of attacks and points of entry within the supply chain. This literature helps analyze key risks within the supply chain and establish the requirements for the level of detail for the pre-developed of components necessary to support effective risk management.
- IEC 62443-4 [36] [37] imposes requirements on suppliers to ensure components can provide the required level of security to meet operator needs.
- UK IS/DBSy [34], [35] step 1 allows for modelling supply chain organisations and systems, therefore providing the opportunity to assess pre-developed components used in the I&C systems.

Key approaches for Challenge 6 are:

- HAZCADS [9] abstraction of the control system structure associates risks with UCAs that are then linked to hazards and losses. This process simplifies the identification of risks. However, in large interconnected systems, a large number of UCAs may be identified.
- IAEA CSRM [6] prioritizes a high degree of abstraction (functions) to identify strategic risks at the facility level.
- UK IS/DBSy [34], [35] step 1 uses an abstract modelling approach that can be used even when the systems are not deployed (i.e., plant under construction).

Key approach for Challenge 7 is:

- Canada's HTRA [8] lists vulnerabilities that aid in identifying risks associated with these vulnerabilities. These lists ensure that vulnerabilities are carefully and systematically considered, reducing the uncertainty associated with deficiencies in identifying vulnerabilities.
- The Chinese cyber-risk approach [23] provides detailed vulnerability risks and provides ways to identify them, reducing the uncertainty in identifying vulnerabilities.
- IAEA CSRM [6] treats functions as targeted by threats. The threat analysis does not consider the vulnerability the adversary would exploit to cause the impact, only that the adversary can do so if they obtain access.

Key approaches for Challenge 8 are:

- Canada's HTRA [8] uses an extensive catalogue of threats, including natural and physical threats. Using this type of catalogue reduces the uncertainty associated with the failure to consider certain types of threats.
- UK IS/DBSy [34], [35] Steps 2 and 4 detail the approach for threat evaluation, uncertainty exists but is reduced by requirements for the use of various government and industry sources to evaluate threat levels as well as the identification of threat actors levels within the NPP.

Key approaches for Challenge 9 are:

- IAEA CSRM [6] identifies risks in modular activities, such as facility characterization and threat characterization in facility-level processes and deeper analysis in system-level processes.
- UK IS/DBSy [34], [35] Step 3 provides the mean for splitting the overall NPP security model into Focus of Interest areas where risks can be identified and assessed, reducing the amount of information into manageable sets.

Key approaches for Challenge 10 are:

- France's cyber-risk approach [44] does not restrict the risk management approach to radiological sabotage or theft of NM. This approach allows other risks to be identified where the impact is graded from minor to critical.
- Germany's cyber-risk approach [22] allows for variance between State regulation and implementation by differing NPP operators.
- HAZCADS [9] risk evaluation is consistent with PRA.
- Canada HTRA [8] identifies all risks to the objectives of an organization. Types of risks, such as safety, security, economic, and cybersecurity, are all identified and managed similarly.
- IAEA CSRM [6] recommends evaluating all significant functions of an organization and provides a 5-level example that accounts for all digital assets associated with a facility.
- US NRC [45] protection of SSEP functions could be a starting point for including other functions and a common and comprehensive approach to risk management.

Key approach for Challenge 11 is:

- The Chinese cyber-risk approach [23] describes the process of choosing and tailoring the security controls, including the advanced security capabilities, for industrial control systems.

7.7.4 Cross-reference table (Table 14)

Table 14 – ISO/IEC 27005:2018, 8.2: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China	X	X		X	X		Key	X	X	X	Key
CIE		Key	X	Key		X			X		
France		X		X			X	X		Key	X
Germany		X			X		X	X	X	Key	
HAZCADS		X		X		Key	X	X	X	Key	
HTRA		Key		X	X		Key	Key	X	Key	X
IAEA CSRM		Key		X	X	Key	Key	X	Key	Key	
IEC 62443		Key		Key	X	X	X	X	X	X	
Russia		X		X				X	X	X	X
USNRC	X	X		X	X		X	X	X	Key	X
UK IS/DBSy	Key	Key		Key		Key	X	Key	Key	X	X

7.8 ISO/IEC 27005:2018, 8.3 Risk analysis

7.8.1 Summary

Risk analysis involves the assessment of incident likelihood, consequences, and level of risk. The purpose of risk analysis as it relates to cybersecurity risk for NPPs is to understand the severity of impacts related to compromise. Conservative decision-making and the lack of statistical data necessary to determine incident likelihood has limited risk analysis associated with the 'worst case' impacts of compromise.

7.8.2 Applicable challenges

Risk analysis is associated with all challenges.

Risk analysis of impacts (i.e., consequence severity) is associated with Challenges 1 (multiple locations), 2 (inter-dependencies), 5 (national differences), 9 (excessive information), 10 (common and comprehensive process), and 11 (technology incompatibility).

Risk analysis of incident likelihood is associated with Challenges 1 (multiple locations), 2 (inter-dependencies), 3 (incident likelihood determination), 4 (pre-developed components), 5 (national differences), 7 (uncertainty vulnerabilities), 8 (uncertainty in threat), and 9 (excessive information).

Level of risk assessments is impacted by all challenges. See Table 15.

Table 15 – ISO/IEC 27005:2018, 8.3: Applicable challenges

Challenge	Description
1	Aggregate Risk of Multiple Units / Locations
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in cyber-risk approaches
6	Lack of abstract analysis methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process
11	Advanced Security Capabilities Incompatibility

7.8.3 Key approaches

Key approach for Challenge 1 is:

- US NRC RG 5.71 [24], “Cyber Security Programs for Nuclear facilities,” [24] and NEI 08-09, “Cyber Security Plan for Nuclear Power Reactors,” [46] discuss the need to perform assessments of those digital assets that, if compromised, could potentially have a high adverse impact or consequence. The security applied to any device that protects multiple Critical Digital Assets (CDAs) is at the same or greater level of the security than that of the protected CDAs. Alternative methods to provide a function may have greater importance to address this challenge.

Key approaches for Challenge 2 are:

- HAZCADS [9] application of STPA identifies UCAs and then associates them with consequences. The risk analysis occurs in the evaluation of scenario-informed fault trees. UCAs that are part of cut sets are assumed to be unmitigated and prioritized for risk treatment. UCAs that are part of prevention sets are assumed to be mitigated (i.e., prevented) and can be accepted.
- UK IS/DBSy [34], [35] ensures that possible risks from interdependencies are evaluated using same criteria as risk present in the I&C system infrastructure.

Key approach for Challenge 3 is:

- The Chinese cyber-risk approach [23] provides a calculation method to estimate the loss (i.e., consequences) and the likelihood of an incident.

Key approach for Challenge 4 is:

- UK IS/DBSy [34], [35] threat evaluation criteria can be used also to assess risks resulting from modelling of the Supply chain and their use of pre-developed components.

Key approach for Challenge 6 is:

- IAEA CSRM [6] two-tiered approach analyzes consequences to the function (facility-level) and the correct operation of the system/assets (system-level). This abstraction aids the analysis in prioritizing strategic risks to functions over tactical risks.

Key approaches for Challenge 7 are:

- HAZCADS [9] uncertainty is addressed via conservative assumptions. The likelihood of a UCA that is not mitigated is set to a likelihood of ‘1’. Whereas the likelihood of a UCA that is mitigated (i.e., prevented) is set to a likelihood of ‘0’.
- IAEA CSRM [6] assumes all systems are vulnerable due to constraints to updating and patching systems at NPPs. Therefore, denial of adversary access to the system is prioritized.

Key approaches for Challenge 8 are:

- Germany’s cyber-risk approach [22] identifies this challenge and defines it as a key element of risk management.
- HAZCADS [9] conservative assumptions for vulnerability/susceptibility reduce reliance on threat assessment and its associated uncertainty.
- Canada’s HTRA [8] lists threat agent capabilities and associates these capabilities to consequences deriving threat impact or gravity. This evaluation of threat agents minimizes the effect of uncertainty in analyzing risks.
- IAEA CSRM [6] leverages the Design Basis Threat and generates functional and technical scenarios to reduce uncertainty in threat assessment as it impacts risk analysis.
- IEC 62443 [14] threat characterization is captured within 62443-3-2 [40] Security Level descriptions. The description creates graded levels to evaluate the protections of OT systems.
- UK IS/DBSy [34], [35] being a threat-based risk assessment uses threat characterisation as input for the risk analysis.

Key approaches for Challenge 9 are:

- IEC 62443-3-2 [40] utilizes two stages: (i) a risk analysis to define and implement DCSA, leveraging a denial of access approach; and (ii) a risk analysis to implement measures that reduce risks not addressed by the DCSA, possibly leveraging a denial of task approach. The complementary approaches reduce the amount of information that needs to be considered for each approach separately.
- UK IS/DBSy [34], [35] being a threat-based risk assessment uses threat characterisation as input for the risk analysis.

Key approaches for Challenge 10 are:

- HAZCADS [9] can be applied to any system where the control structure can be modelled. However, in instances where Fault trees do not pre-exist, the effort to apply to all systems and risks could be challenging. Risk methods that rely on existing analysis tools and information may limit how widely an approach can be leveraged.
- Canada's HTRA [8] provides tables to assist in risk analysis. In these tables, all risks are addressed in an identical matter, such as safety, economic, security, and cybersecurity.
- The UK IS/DBSy [34], [35] risk analysis criteria are well documented and consistently applied throughout the lifecycle of the plant.

7.8.4 Cross-reference table (Table 16)

Table 16 – ISO/IEC 27005:2018, 8.3: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China	X	X	Key	X	X	X	X	X	X	X	X
CIE		X	X	X		X			X		
Germany	X	X	X	X	X	X	X	Key	X	X	X
HAZCADS		Key		X		X	Key	Key	X	Key	
HTRA	X	X	X	X	X	X	X	Key	X	Key	X
IAEA CSRM		X	X	X		Key	Key	Key	X	X	
IEC 62443		X	X	X		X	X	Key	Key	X	
Russia			X							X	
US NRC	Key	X	X	X	X	X	X	X	X	X	X
UK IS/DBSy		Key		Key		X	X	Key	Key	Key	

7.9 ISO/IEC 27005:2018, 8.4 Risk evaluation

7.9.1 Summary

Risk evaluation begins with an ordered set of risks based on severity and is compared against risk criteria (evaluation and acceptance). The risks are then prioritized for risk treatment.

7.9.2 Applicable challenges

Risk evaluation is associated with all challenges.

The ordered set of risks considers many challenges (Challenges 3, 4, 8, and 9). However, the prioritization of those risks depends on cyber-risk approaches (Challenge 5) and may demand modification based on the lack of a common and comprehensive process (Challenge 10). Finally, the risk priority may change with Challenge 1 if several sites have the same risk. Finally, an abstract analysis method may be used to solve some of the other challenges. See Table 17.

Table 17 – ISO/IEC 27005:2018, 8.4: Applicable challenges

Challenge	Description
1	Aggregate Risk of Multiple Units / Locations
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process
11	Advanced Security Capabilities Incompatibility

7.9.3 Key approaches

Key approach for Challenge 1:

- UK IS/DBSy [34], [35] abstract modelling of a full NPP will allow for the identification of threat activities that could have a wider impact i.e., on the overall I&C architecture or plant.

Key approaches for Challenge 2 are:

- US NRC [24] has several controls that aim to cover interdependencies and interactions and simplify risk evaluation.
- UK IS/DBSy [34], [35] ensures that accidental or malicious activities from threats potentially impacting I&C system i.e., risks through their interfaces with other systems are part of the methodology.

Key approaches for Challenge 4 are:

- US NRC [24] guidance recommends licensee/applicant testing (e.g., vulnerability scans), which is performed before the operational use of a CDA.
- UK IS/DBSy [34], [35] modelling of the Supply chain and their interaction with the I&C systems allow the identification of threat activities that could impact pre-developed components.

Key approaches for Challenge 7 are:

- Germany’s cyber-risk approach [22] identifies this challenge and defines it as a key element of risk management.
- IAEA CSRM [6] assumes that the likelihood of postulated scenarios is ‘1’ unless modified by defensive control measures (such as the Defensive Computer Security Architecture (DCSA). DCSA protections are accredited in scenario analysis that prevents or protects against adversary access to the vulnerable or susceptible system.
- US NRC [24] guidance highlights the need for threat and vulnerability management that includes vulnerability scans and assessments to reduce uncertainty.

Key approaches for Challenge 8 are:

- IAEA CSRM [6] assumes that the adversary can access systems via any attack pathway. The scenarios evaluate the DCSA and other measures in reducing risks associated with adversary access.
- In the UK IS/DBSy [34], [35] threat characterisation and evaluation are key components of the risk evaluation.

Key approach for Challenge 9 is:

- UK IS/DBSy [34], [35] focus of interest will allow the analysis of threat actors accidental or malicious activities in selected areas of the security model, reducing the volume of information to be assessed.

Key approaches for Challenge 10 are:

- France's cyber-risk approach [44] bases risk analysis on impact grading and considers the risk acceptance criteria for those risks. An adaptable risk acceptance criteria matrix that allows for modification and customizations would simplify challenges in applying a common and comprehensive risk process.
- HAZCADS [9] relies upon PRA elements (i.e., Fussell-Vesely interval, Birnbaum's measure) to evaluate risk. These elements can be commonly applied but require the tools and information on the associated systems and risks, which may not be available.
- IEC 62443 [14] is an international standard for Industrial Automated Control Systems (IACS) or Operational Technology (OT) systems. It broadly addresses critical infrastructure risks and classifies them into categories A, B, and C. These can be generally applied to most NPP consequences (other than radiological sabotage and theft of NM) to produce a common and comprehensive process. Many national standard institutes widely adopt parts of IEC 62443.
- The Russia cyber-risk approach [29], [30], [31], [32] provides common risk acceptance criteria and grading.

7.9.4 Cross-reference table (Table 18)

Table 18 – ISO/IEC 27005:2018, 8.4: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China	X	X	X	X	X	X	X	X	X	X	X
France										Key	
Germany							Key			X	
HAZCADS		X		X		X	X	X	X	Key	
IAEA CSRM			X	X		X	Key	Key	X	X	
IEC 62443			X	X	X	X			X	Key	
Russia										Key	
US NRC	X	Key	X	Key	X	X	Key	X	X	X	X
UK IS/DBSy	Key	Key		Key		X		Key	Key	X	

7.10 ISO/IEC 27005:2018, 9.1 General description of risk treatment

7.10.1 Summary

Risk treatment takes a prioritized list of risks and develops a risk treatment plan to:

a) modify,

b) retain,

c) avoid, or

d) share the risks. NPP cybersecurity has historically focused on the modification of risks through the application of controls with some retention.

7.10.2 Applicable challenges

Risk treatment is associated with Challenges 1-3, 5, and 7-9.

For example, risk treatment is impacted by Challenges 1, 3, 5, and 7. The aggregate risk of multiple units/locations may result in different prioritization or incur costs to modify that other options (like avoidance) may be beneficial. Additionally, Challenge 3 makes risk sharing difficult as consequences may be severe and beyond a third party's ability to cover. Finally, differences in national risk management may demand different risk treatment options based on risk tolerance thresholds. See Table 19.

Table 19 – ISO/IEC 27005:2018, 9.1: Applicable challenges

Challenge	Description
1	Aggregate Risk of Multiple Units / Locations
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Approaches
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
9	Excessive Information Volume

7.10.3 Key approaches

Key approach for Challenge 2 is:

- UK IS/DBSy [34], [35] provides a specific set of controls that can be applied to risks resulting from systems interdependencies.

Key approaches for Challenge 3 are:

- France's cyber-risk approach [44] identifies security risks, that are formally noted by the operator. Furthermore, this approach requires the operator to install all security updates, except when there are justified technical or operational difficulties.
- IAEA CSRM [6] leverages conservative assumptions in assuming that the threat of radiological sabotage and theft of NM is present unless justified by a formal analysis and demonstrated with the necessary rigour.

Key approach for Challenge 4 is:

- The Russian approach [29], [30], [31], [32] which, during the risk analysis, identifies possible security controls to mitigate the risks found within pre-developed components.

Key approach for Challenge 5 is:

- IAEA CSRM [6] provides a hierarchical list of unacceptable consequences that may inform the application of a graded approach in the regulation of IAEA Member States.

Key approaches for Challenge 7 are:

- France's cyber-risk approach [44] demands verification of the security controls. The verification process allows the operator to reduce uncertainty within the vulnerability/susceptibility input documents.
- Germany's cyber-risk approach [22] requires a risk treatment plan as part of the risk management process. All risks shall be avoided, mitigated, or accepted.
- US NRC RG 5.71 [24] and NEI 08-09 [46] guidance on vulnerability analysis and ongoing effectiveness analysis of applied security controls. The guidance prompts licensees to be "aware of evolving cybersecurity threats and vulnerabilities" and be "aware of advancements in cybersecurity protective strategies and security controls."

Key approach for Challenge 8 is:

- The UK IS/DBSy [34], [35] controls level consider their use according to the threat level. More rigorous controls are applied to highest threat level.

Key approach for Challenge 9 is:

- The UK IS/DBSy [34], [35] control sets can be applied independently to the selected focus of interest in the assessment scope, thus allowing for the amount of information to be reduced to manageable levels.

7.10.4 Cross-reference table (Table 20)

Table 20 – ISO/IEC 27005:2018, 9.1: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China	X		X		X		X				
France	X		Key				Key				
Germany			X				Key	X			
HAZCADS											
HTRA	X		X		X		X				
IAEA CSRM			Key		Key		X				
IEC 62443		X					X	X	X		
Russia				Key			X				
US NRC	X		X		X		Key				
UK IS/DBSy	X	Key			X			Key	Key		

7.11 ISO/IEC 27005:2018, 9.2 Risk modification

7.11.1 Summary

Risk modification is the traditional approach to risk treatment for cybersecurity risks at NPPs. It involves the application of security controls to modify (lessen) the level of risk.

7.11.2 Applicable challenges

Risk treatment is associated with all challenges. For example, the aggregate risk of multiple units/locations (Challenge 1) would require modification at all units and leads to the potential for a diverse set of controls. Risk modification needs to consider that security controls can also bring about vulnerabilities that could be used to attack sensitive assets.

Also, Challenges 3, 8, and 9 reflect the difficulty in qualitatively or quantitatively assessing risk. Providing a specific value for the risk and modifying that value based on the implementation of control is difficult. Challenges 5 and 10 may impact the assigned value of the risk before the residual risks can be determined to be acceptable.

Finally, Challenges 11 make continual monitoring and assessment of control effectiveness difficult. See Table 21.

Table 21 – ISO/IEC 27005:2018, 9.2: Applicable challenges

Challenge	Description
1	Aggregate Risk of Multiple Units / Locations
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process
11	Advanced Security Capabilities Incompatibility

7.11.3 Key approaches

Key approach for Challenge 1 is:

- UK DBSy [34], [35] provides controls that can be applied at the plant or plants level, i.e., controls that would help mitigating risks impacting various systems.

Key approach for Challenge 3 is:

- France's cyber-risk approach [44] identifies security risks, that are formally noted by the operator. Furthermore, this approach requires the operator to install all security updates, except when there are justified technical or operational difficulties.

Key approaches for Challenge 4 are:

- IAEA CSRM [6] recommends both DCSA and baseline measures to provide facility-wide protection against uncertainty associated with pre-developed components. Additional recommendations are to perform tests to evaluate the cybersecurity of key pre-developed components to acquire information to support risk management and inform potential additional controls.
- UK IS/DBSy [34], [35] provides controls to mitigate risks related to the Supply Chain and the use of pre-developed components.

Key approaches for Challenge 7 are:

- IAEA CSRM [6] recommended performance testing could also be applied to other assets and components to identify vulnerabilities and provide additional information, thereby reducing uncertainty in Vulnerability/Susceptibility Analysis.
- UK IS/DBSy [34], [35] assurance activities allow for the identification of compensatory controls when the technology used to deliver I&C systems is not compatible with modern technical controls.

Key approaches for Challenge 10 are:

- France's cyber-risk approach [44] is not restricted to regulatory risks. It allows the operator to manage all significant risks.
- Germany's cyber-risk approach [22] requires all unacceptable risks to be modified to an acceptable level.
- HAZCADS [9] introduces three classes of control methods:

  a) Protect;

  b) Detect;

  c) Respond and Recover, which could be applied regardless of the type of risk.
- Canada's HTRA [8] considers all unacceptable residual risks in a similar manner regardless of cause, and these shall be modified.

Key approaches for Challenge 11 are:

- US NRC [24] guidance allows for the use of alternate controls when recommended controls are incompatible with the system.
- UK IS/DBSy [34], [35] provides advanced security controls at DEFEND level that include the use of SOC, network and host monitoring and robust MFA objectives.

7.11.4 Cross-reference table (Table 22)

Table 22 – ISO/IEC 27005:2018, 9.2: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China	X		X		X		X	X	X	X	X
CIE		X	X	X		X			X		
France	X		Key					X		Key	X
Germany			X				X	X	X	Key	
HAZCADS		X		X		X	X	X	X	Key	
HTRA	X		X		X		X	X	X	Key	-
IAEA CSRM				Key		X	Key	X	X	X	
IEC 62443		X		X		X	X	X	X	X	
Russia	X							X		X	X
US NRC	X		X		X		X	X	X	X	Key
UK IS/DBSy	Key			Key	X		Key	X	X		Key

7.12 ISO/IEC 27005:2018, 9.3 Risk retention

7.12.1 Summary

Risk-retention is permitted when the level of risk meets the risk acceptance threshold. NPP cybersecurity generally considers impacts on safety, security, and emergency preparedness functions that have the potential to lead to (or support) scenarios that result in unacceptable radiological consequences or theft of nuclear material.

7.12.2 Applicable challenges

Risk-retention is affected by Challenges 1, 5, 7, and 10. Challenge 1 may result in an aggregate risk that cannot be retained compared to individual units. Also, Challenges 5 and 10 affect the risk acceptance threshold (by raising or lowering it based on national risk tolerance).

Challenge	Description
1	Aggregate Risk of Multiple Units / Locations
5	Differences in Cyber-risk Management
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
10	Lack of a Common and Comprehensive Risk Management Process

7.12.3 Key approaches

Key approach for Challenge 1 is:

- UK IS/DBSy [34], [35] allows to produce an overall plant I&C security case that consolidates the risk assessment from multiple systems thus allowing for an evaluation of risks impacting plant level.

Key approaches for Challenge 5 are:

- Germany’s cyber-risk approach [22] demands a similar level of documentation of retained risks and a formal acceptance process, including the approving authorities. The German cyber-risk approach allows acceptance of differing methods, such as BSI-200 or ISO/IEC 27001 [2].
- US NRC [24] applies a graded approach during the cyber risk assessment for scaling the security controls applied to a given digital asset that may minimize differences in national risk management.

Key approaches for Challenge 7 are:

- Germany’s cyber-risk approach [22] demands a similar level of documentation of retained risks and a formal acceptance process, including the approving authorities.
- IAEA CSRM [6] highlights the challenge of determining the efficacy of administrative controls (e.g., procedures) to reduce exposure of vulnerabilities or correct susceptible elements of systems which in turn increases uncertainty in Vulnerability/Susceptibility Analysis and adversary impact retained risks.
- US NRC [24] guidance identifies assurance activities such as vulnerability analysis as a key element in reducing uncertainty.
- UK IS/DBSy [34], [35] overall security case will consider cumulative risks to legacy systems and reassess compensatory measures to further treat those risks.

Key approach for Challenge 8 is:

- IAEA CSRM [6] details how administrative measures are not to be solely relied upon for an extended time since uncertainty in threat capabilities or access may lead to increases in retained risks that may exceed acceptable levels.

Key approaches for Challenge 10 are:

- France's cyber-risk approach [44] allows for the operator to retain risk if determined to be not significant, and this shall be a formal decision by the operator.
- US NRC [24] considers the protection of SSEP functions as a starting point for developing a common and comprehensive risk management process.

7.12.4 Cross-reference table (Table 23)

Table 23 – ISO/IEC 27005:2018, 9.3: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China	X				X		X	X		X	
France	X						X			Key	
Germany	X				Key		Key	X		X	
HTRA	X				X		X			X	
IAEA CSRM							Key	Key			
Russia										X	
US NRC	X				Key		Key	X		Key	
UK IS/DBSy	Key				X		Key	X		X	

7.13 ISO/IEC 27005:2018, 9.4 Risk avoidance

7.13.1 Summary

Risk avoidance is an option that stops or eliminates an activity to avoid the risk associated with that activity. As with other industries, complete avoidance of cybersecurity risks is unlikely to be achieved. NPPs are associated with URC and nuclear material; however, the dependence on computer-based systems and programmable hardware devices might be reduced to avoid specific risks.

7.13.2 Applicable challenges

Risk avoidance is associated with all challenges except for Challenge 11 (technology incompatibility). Particularly, risk avoidance is affected by Challenges 1, 5, 8, and 9. Risk avoidance may be to avoid reusing common components and technologies in sensitive digital assets to limit Challenge 1. Risk avoidance could also limit the number of countries to license to reduce Challenge 5. However, both potential options would limit the scalability and adversely impact economic considerations.

Challenges 8 and 9 further limits the risks that can be avoided. See Table 24.

Table 24 – ISO/IEC 27005:2018, 9.4: Applicable challenges

Challenge	Description
1	Aggregate Risk of Multiple Units / Locations
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process

7.13.3 Key approaches

Key approach for Challenge 7 is:

- Germany's cyber-risk approach [22] recognizes the uncertainty in vulnerability/susceptibility and prioritizes avoidance of risks affected by this uncertainty.

7.13.4 Cross-reference table (Table 25)

Table 25 – ISO/IEC 27005:2018, 9.4: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
CIE		X	X	X		X			X		
France	X							X			
Germany		X			X		Key	X		X	
HTRA	X				X			X	X		
Russia	X							X			

7.14 ISO/IEC 27005:2018, 9.5 Risk sharing

7.14.1 Summary

Risk sharing involves another party that can most effectively manage a particular risk. In many cases, this is risk transfer to a supplier/vendor where they apply cybersecurity controls or risk sharing with insurance companies to cover the financial impacts of cyberattacks. For NPP cybersecurity, the operator and the State share the most severe consequences of NM theft and URC.

7.14.2 Applicable challenges

Risk sharing is associated with all challenges except for Challenge 1. Particularly, Challenges 1, 3, 5, and 10 result from the severe consequences of URC and NM theft, resulting in differences in risk tolerance and limiting entities that can share risks associated with these consequences. Challenges 6, 7, and 9 are related as they may not be associated with severe consequences but cannot be shared or transferred due to the complexity of the analysis and the potential for error. See Table 26.

Table 26 – ISO/IEC 27005:2018, 9.5: Applicable challenges

Challenge	Description
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process
11	Advanced Security Capabilities Incompatibility

7.14.3 Key approaches

Key approach for Challenge 7 is:

- Germany's cyber-risk approach [22] recognizes the uncertainty in vulnerability/susceptibility and demands formal approval of risk sharing of those risks affected by this uncertainty.

Key approach for Challenge 11 is:

- IEC 62443-4-2 [37] addresses the need for components to have security capabilities. These component requirements allow risk assessments to determine whether a supplied component meets the security level target. Suppliers of components will likely need to maintain and update these capabilities to ensure their continued effectiveness. IEC 62443-4 [36], [37] recognizes that suppliers of these components will need to be managed, and risk is shared between the suppliers and the operator.

7.14.4 Cross-reference table (Table 27)

Table 27 – ISO/IEC 27005:2918, 9.5: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
CIE		X	X	X		X			X		
Germany		X			X		Key	X		X	
IEC 62443		X		X			X	X			Key

7.15 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance

7.15.1 Summary

Risk acceptance involves a decision to accept risks. Risk acceptance is limited for NPP cybersecurity for those risks associated with URC and theft of NM due to national requirements and regulations. However, risk acceptance approaches for those risks not associated with these consequences are diverse.

7.15.2 Applicable challenges

Risk acceptance is associated with all challenges. Risk acceptance is limited by Challenges 1, 3, 5, and 8, which address severe consequences and resulting differences in national security threats and risk tolerance. Challenges 2, 4, 7, and 8 address the uncertainty involved in risk evaluation and hence the level of risk, prioritizing conservative decision making, thus limiting risk acceptance. Challenges 6 and 10 involve potential processes that can be used to accept all risks by reducing uncertainty in the level of risk and minimizing national differences. See Table 28.

Table 28 – ISO/IEC 27005:2018, Clause 10: Applicable challenges

Challenge	Description
1	Aggregate Risk of Multiple units or locations
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or lacking sufficient detail for pre-developed components
5	Differences in Cyber-risk Management
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process
11	Advanced Security Capabilities Incompatibility

7.15.3 Key approaches

Key approach for Challenge 3 is:

- France’s cyber-risk approach [44] requires verification of retained risks. A security audit allows for a reduction in uncertainty associated with likelihood.

Key approach for Challenge 4 is:

- France’s cyber-risk approach [44] requires verification of retained risks. A security audit allows for a reduction in uncertainty associated with pre-developed components.

Key approaches for Challenge 5 are:

- Germany’s cyber-risk approach [22] allows for differing approaches that attain a similar level of risk management effectiveness and acceptance by the national authority.
- The US NRC [24] cyber-risk approach aligns with the risk management approach discussed in ISO/IEC 27005 [5] except for the risk acceptance criteria. US NRC guidance recognizes that regulatory considerations and risk profiles from the different Member States drive risk acceptance criteria.

Key approach for Challenge 7 is:

- France’s cyber-risk approach [44] requires verification of retained risks. A security audit allows for a reduction in uncertainty associated with likelihood.

Key approach for Challenge 10 is:

- France’s cyber-risk approach [44] requires a formal decision by the NPP operator to retain risks.

7.15.4 Cross-reference table (Table 29)

Table 29 – ISO/IEC 27005:2018, Clause 10: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China	X	X	X	X	X	X	X	X		X	X
France	X	X	Key	Key		X	Key	X		Key	
Germany	X	X	X	X	Key	X	X	X		X	X
HTRA	X	X	X	X	X	X	X	X	X	X	
Russia	X	X		X			X	X		X	
US NRC	X	X	X	X	Key	X	X	X		X	X
UK IS/DBSy	X	X	X	X		X	X	X	X	X	

7.16 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation

7.16.1 Summary

Risk communication needs to cover the normal and emergency operations of an NPP. For NPP cybersecurity, there are many stakeholders, both internal (within the operator) and external (regulators, public). Risk communication plans need to be developed to detail how risk will be managed and communicated.

7.16.2 Applicable challenges

Risk communication is associated with all challenges. Each of these challenges affects how risks are communicated and the uncertainty associated with risk management activities. See Table 30.

Table 30 – ISO/IEC 27005:2018, Clause 11: Applicable challenges

Challenge	Description
1	Aggregate Risk of Multiple units or locations
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process
11	Advanced Security Capabilities Incompatibility

7.16.3 Key approaches

Key approaches for Challenge 2 are:

- Germany's cyber-risk approach [22] recognizes the challenges due to complexities resulting from differing cyber-risk approaches. This challenge results from Challenge 5 in differing risk management processes that place increased demands on NPP operators and regulators to perform equivalency evaluation.
- US NRC [24] recognizes that individual stakeholders may have different perspectives and considerations regarding the importance and impact of various situations and events. These differences are factored into risk communication plans and reflect interdependencies among the various stakeholders' efforts and the impact these differences will have on their interactions.

Key approach for Challenge 3 is:

- France's cyber-risk approach [44] requires verification of retained risks. A security audit allows for a reduction in uncertainty associated with likelihood.

Key approach for Challenge 4 is:

- France's cyber-risk approach [44] requires verification of retained risks. A security audit allows for a reduction in uncertainty associated with pre-developed components.
- The Russian cyber-risk approach [29], [30], [31], [32] using the national wide security catalogue of the pre developed components security flaws.

Key approach for Challenge 6 is:

- IAEA CSRM [6] tiered approach that prioritizes abstraction simplifies communication and consultation with senior leadership and management without the need to detail complex cybersecurity elements.

Key approach for Challenge 7 is:

- France's cyber-risk approach [44] requires a formal decision by the NPP operator to retain risks.

Key approaches for Challenge 9 are:

- HAZCADS [9] is simplified if fault trees and PRA reports exist, limiting the new information that shall be created or evaluated. The familiarity of PRA within the organization would also simplify consultation with other departments and risk owners. However, if no PRA experience exists, the effort may be excessive, and this effort may create excessive information.
- IAEA CSRM [6] module approach to both facility and system risk allows for the reduction of the information that needs to be communicated for each required output.
- The Russia cyber-risk approach [29], [30], [31], [32] establishes a nation-wide security incident catalogue.

Key approaches for Challenge 10 are:

- France's cyber-risk approach [44] requires a formal decision by the NPP operator to retain risks.
- Germany's cyber-risk approach [22] allows for differing risk management approaches, which impacts consultation.
- HAZCADS [9] is a way PRA processes could be leveraged to support cybersecurity analysis, thereby increasing the potential for a common and comprehensive approach to managing all types of risks.
- IAEA CSRM [6] focus on functions allows for integration into existing management systems and supports a common and comprehensive risk management approach.
- The Russian cyber-risk approach [29], [30], [31], [32] provides a nation-wide security incident logging facility and defines a common format for security incident descriptions.
- US NRC [24] details two distinct areas for communication and consultation for the cybersecurity team (CST) – internal and external. Potential differences exist in the risk management processes between these areas – and between different external stakeholders. Risk communication plans identify and address these issues and delineate decision makers in the various scenarios.

7.16.4 Cross-reference table (Table 31)

Table 31 – ISO/IEC 27005:2018, Clause 11: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
CIE		X	X	X		X			X		
France	X	X	Key	Key		X	Key	X		Key	
Germany	X	Key	X	X	X	X	X	X	X	Key	X
HAZCADS		X		X		X	X	X	Key	Key	
HTRA	X	X	X	X	X	X	X	X	X	X	X
IAEA CSRM		X	X	X		Key	X	X	Key	Key	
IEC 62443		X	X	X		X			X	X	
Russia	X	X		Key		X		X	Key	Key	
US NRC	X	Key	X	X	X	X	X	X	X	Key	X

7.17 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review

7.17.1 Summary

Monitoring and review need to include risk factors and risk management. Risk factors (value of assets, threats, vulnerabilities, likelihood of occurrence) may change over time, whereas the risk management process may need to be improved based on operational experience.

7.17.2 Applicable challenges

Information security monitoring and review are associated with all challenges. For example, Challenges 1, 3, 4, 7, 8, 9, and 11 are likely to impact how risk factors are reviewed and monitored. Challenges 5, 6, and 10 can be impacted by changes or improvements to risk management, either by the operator or another stakeholder (e.g., a stakeholder). See Table 32.

Table 32 – ISO/IEC 27005:2018, Clause 12: Applicable challenges

Challenge	Description
1	Aggregate Risk of Multiple units or locations
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or lacking sufficient detail for pre-developed components
5	Differences in cyber-risk Management
6	Lack of abstract analysis methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process
11	Advanced Security Capabilities Incompatibility

7.17.3 Key approaches

Key approach for Challenge 1 is:

- The application of UK IS/DBSy [34], [35] in NPPs includes the requirement to review and update the overall plant risk assessment at periodic intervals.

Key approach for Challenge 3 is:

- France's cyber-risk approach [44] requires re-examination of the risk assessment and approval every three years and when an event or an evolution modifies the context of the system unacceptable events occurs.

Key approach for Challenge 4 is:

- France's cyber-risk approach [44] requires re-examination of the risk assessment and approval every three years, and when an event or an evolution modifies the context of the system, e.g. when new significant information on a pre-developed component become known.

Key approach for Challenge 6 is:

- IAEA CSRM's [6] facility-level analysis minimizes the impact of minor events or new incidents allowing for planned and systematic risk assessments at the strategic level.

Key approaches for Challenge 7 are:

- France's cyber-risk approach [44] requires re-examination of the risk assessment and approval when there is an adverse change in uncertainty for vulnerability/susceptibility. For example, disclosure of new vulnerabilities or reports of active exploitation will affect the validity of the vulnerability analysis.
- Germany's cyber-risk approach [22] recognizes the uncertainty in vulnerability/susceptibility and prioritizes reviewing the risks affected by this uncertainty.
- IAEA CSRM [6] recommends a review if changes in vulnerability are identified.

- US NRC RG 5.71 [24] describes a cybersecurity life cycle as a good concept to plan for periodic reviews. This concept allows for a determination that the effectiveness of the implemented controls has not been adversely impacted by changes in the system, network, environment, or emerging threats. Of these four factors, emerging threats are of great concern, and the resulting uncertainty presents a significant challenge to any recurrent vulnerability scan/assessment or other means of determining the continued effectiveness of implemented controls.

Key approaches for Challenge 8 are:

- IAEA CSRM [6] recommends a review if changes in threat are identified.
- The UK IS/DBSy [34], [35] review includes a re-assessment of the threat environment with the objective to consider changes in adversarial threats.

Key approaches for Challenge 9 are:

- Germany's cyber-risk approach [22] recognizes the challenge with monitoring and review, including an analysis of risks associated with an immense amount of information.
- The UK IS/DBSy [34], [35] allows for reviews and updates of the security risks pertaining to specific I&C system(s), for example when a system is changed, upgraded, or replaced.

Key approach for Challenge 10 is:

- France's cyber-risk approach [44] requires a re-examination of the risk approval when new significant risks are identified or every three years.

7.17.4 Cross-reference table (Table 33)

Table 33 – ISO/IEC 27005:2018, Clause 12: Cross-reference table

Approach	1	2	3	4	5	6	7	8	9	10	11
China	X		X	X	X		X	X	X	X	X
CIE		X	X	X		X			X		
France	X		Key	Key			Key	X		Key	X
Germany	X		X	X	X		Key	X	Key	X	X
HTRA	X	X	X	X	X	X	X	X	X	X	X
IAEA CSRM			X	X			Key	Key	X	X	
IEC 62443		X	X	X		X	X	X	X	X	X
Russia	X			X				X		X	
US NRC	X		X	X	X		Key	X	X	X	X
UK IS/DBSy	Key	X		X		X	X	Key	Key		X

7.18 Overall summary of approaches to challenges

Describe how the table was created and how it can be a quick lookup of challenges and practical approaches.

Table 34 summarizes the analysis and the coverage of key insights to any ISO/IEC 27005:2018 [5] clause. Some notable elements are:

- Challenge 1 has little coverage, and only one approach has a key insight. This exclusion may reflect that NPP risk management does not appropriately consider common cause failure resulting from compromising of common or similar design elements.
- Challenges 2-4 and 6-10 have good coverage and many key insights. This coverage may be due to strong relation to existing elements of ISO/IEC 27005:2018 [5] with additional guidance for NPP specificities.
- Challenge 5 has moderate coverage and few insights. This moderate coverage may be due to many of the approaches being evaluated as part of this document being cyber-risk approaches. However, even approaches that are not national such as CIE [10] and HAZCADS [9], do not cover this challenge. The IAEA CSRM [6] is a notable exception.
- Challenge 11 has very little coverage and only two approaches have a key insight including the Chinese cyber-risk approach [23] which describes a process for selecting and tailoring the security controls which includes advanced security capabilities. The lack of widespread coverage across approaches is likely due to many risk approaches prioritizing performance-based or outcome-focused normative guidance. Therefore, a standard or approach that recommends or requires specific technologies and implementations would need to be updated more frequently to keep pace with technology changes and new implementations (e.g., virtualization, cryptography).

Table 34 – Summary of approaches to challenges

Approach	1	2	3	4	5	6	7	8	9	10	11
China	X	Key	Key	X	Key	X	Key	X	X	Key	Key
CIE		Key	Key	Key		X			X	X	
France	X	X	Key	Key		X	Key	X		Key	X
Germany	X	Key	X	Key	Key	X	Key	X	X	Key	X
HAZCADS		Key		Key		Key	Key	Key	Key	Key	
HTRA	X	Key	X	Key	X	X	Key	Key	Key	Key	X
IAEA CSRM		Key	Key	Key	Key	Key	Key	Key	Key	Key	
IEC 62443		Key	X	Key	X	Key	Key	Key	Key	Key	
Russia	X	X	X	Key		X	X	X	Key	Key	X
US NRC	Key	Key	X	Key	Key	X	Key	X	X	Key	Key
UK IS/DBSy	Key	Key		Key		Key	Key	Key	Key	Key	

8 Conclusions

ISO/IEC 27005 [5] provides a generic domain-independent framework for information security risk assessments but does not consider the specific consequences associated with NPPs. Additionally, nuclear power is a heavily regulated industry that demands a certain level of effectiveness in cybersecurity risk management. The specific nuclear risks need to be identified by the threat and risk analysis team and are to be based on the applicable DBT.

Current cyber-risk approaches share many common elements with ISO/IEC 27005:2018 [5] while addressing some or all identified challenges in Clause 7. Additionally, the guidance within these cyber-risk approaches enhances (builds upon) the existing framework of IEC 62645 [1] with respect to risk management. The cyber-risk approaches are complementary and not contradictory, as detailed in the analysis of Annex A through Annex K.

A future IEC risk management standard for NPP operators may consider the identified key insights from the cyber-risk approaches evaluated for this document. A summary of the key insights for consideration in a potential new standard is as follows:

- Challenge 2 is related to complexity of interdependencies and interactions. China [23], CIE [10], Germany [22], HAZCADS [9], IAEA [6], US NRC [24] provide key insights. The IAEA provide identifies significant categories of common interdependencies and interactions with the potential to inform incident scenarios, likelihood, impacts, threats, and vulnerabilities. Additionally, other methods such as HAZCADS [9] provide a framework to investigate or consider unique interdependencies and interactions within I&C systems and EPS. Therefore, a taxonomy of interdependencies and interactions, listings of specific dependencies, and scenarios that detail how adversaries (e.g., direct and indirect threats from HTRA [8]) could leverage them would address this challenge.
- Challenge 3 is related to uncertainty in incident- scenario likelihood determination. Traditional physical protection approaches are highly dependent upon scenarios based upon the national threat assessment or DBT [47]. Conversely, cybersecurity DBT and scenarios are not as well known or established. Many cyber-risk approaches such as IAEA [6], CIE [10], and France [44] provide key insights. EBIOS [11], [12] identifies security risks that could inform the development of scenario sets that are consistently applied by NPP operators, similar to a DBT. The IAEA [6] recommends two sets of scenarios, functional and technical ones, that align with the two-tiered analysis. CIE [10] incorporates principles of security culture to limit human error as the initiating event of a scenario, and planned resilience. Planned resilience demands a set of incident scenarios for which the system or facility can be protected against. Therefore, a standard set (or catalogue) of scenarios may be a single set for all significant risks and tiers or separate sets of scenarios to address each class of risks or tiers.
- Challenge 4 is related to unknown or lacking sufficient detail for pre-developed components. There are many key insights from the cyber-risk approaches including Russia FSTEC [31] that provides the set of requirements and methodologies to estimate and address vulnerabilities in hardware and software.
- Challenge 6 is related to the lack of abstraction methods to support cybersecurity risk management. Historically, NPP cybersecurity risk management is based upon implemented and in service systems with a heavy reliance on actual implementation (e.g., asset-centric). However, many cyber-risk approaches such as the IAEA [6], IEC 62443 [14], and HAZCADS [9], IEC TR 63415 [33] recommend use of abstraction to allow for multiple tiers (iterations) of risk assessments to address strategic and tactical risks separately. Abstraction can enable a high degree of compartmentalization or modular activities would decrease the amount of information needed to perform an effective analysis (i.e., Challenge 9).
- Challenges 7 and 8 are addressed via risk modification values that can be accredited independently within each of the tiers of risk assessment. A standard method to accredit the risk modification value of common controls. A template of DCSA and other key common controls would minimize some challenges in evaluating their benefits. Coupled with abstract methods or tiered approaches, the iterative risk assessments can apply differing analysis techniques. For example, IEC 62443 [14] and IAEA [6] both recommend an initial denial of access analysis to identify controls such as the DCSA that deny adversary access to an attack pathway. The subsequent analysis applies a denial of task approach to eliminate vulnerabilities, detect their exploitation, and mitigate the consequences of compromise of the I&C system. Therefore, common controls (such as DCSA) resulting from the application of diverse approaches reduce the impact to risk from the uncertainty in vulnerability analysis and the uncertainty in adversary characterization.
- Challenge 9 is addressed through the use of existing mature processes from other domains improves information acquisition and analysis to simplify the rationalization of large volumes of information, addressing Challenge 9. HAZCADS [9] leverages existing PRA approaches that are common to manage NPP safety risks. By leveraging existing approaches, PRA tools and technologies simplify the structure, analysis, and presentation of large amounts of information (e.g., computer models, system notebooks).

- Challenge 10 is related to a common and comprehensive risk management framework to address all types of risks (cybersecurity, regulatory, non-malicious). Cyber-risk approaches such as IEC 62443-1-1 [14], ISO/IEC 27005 [5], and HTRA [8], provide for taxonomy that can be used to relate or describe risks in a similar manner. For example, HTRA [8] provides new criteria (e.g., threat impact or gravity) that is a composite score of attributes associated with all risks. These composite scores allow for a common and comprehensive risk evaluation process addressing all risks using a single composite score. Alternatively, alternate taxonomies for non-regulatory risks could still leverage the same risk management processes with differing risk acceptance criteria. Finally, additional security degrees could be established for different classes of risks (i.e., not I&C systems or EPS).
- Challenges associated with uncertainty is addressed by HTRA [8] and IEC 62443 [14] that provide extensive lists for consequences, threats, vulnerabilities, and tables to provide a systematic means to evaluate the risk and reduce uncertainty's impact. These lists are key to assist risk assessors in comprehensively identifying potential risk sources and attributes.
- NPP cybersecurity risk management demands large amounts of information to perform effective and comprehensive risk assessment. Cybersecurity was not considered within the initial design and construction of the existing NPP fleet. The analyses in this document revealed very few key insights regarding advanced cybersecurity technologies to support risk management. Additionally, cybersecurity technologies and tools to address risk management challenges are not mature or “user-friendly” to be easily adopted, but their design and use within NPPs is needed. For example, SIEM or Cyber Security Operations Centres increase the excessive information (Challenge 9) that may be considered in system risk assessments and require a significant effort to tune and analyze to capture, synthesize, and present this information in a form that lends to rigorous, consistent, and repeatable analysis. Nevertheless, the capture of this information and the improvement of the supporting technology and tools is key for continuous improvement of cyber risk management at NPPs.
- All editions of ISO/IEC 27005 [5] distinguish between two types of assets: primary assets and supporting assets. The primary assets are processes or information of value to an organization and supporting assets are the IT components upon which the primary assets are based (e.g., hardware, software, network, personnel, site, or organizational structure), In the NPP context, examples of top-level processes are reactor core cooling or avoiding the release of radioactivity. Both primary and supporting assets can be structured, for example cooling pumps of the core cooling process and I&C systems and subsystems which control the cooling process and the cooling pumps. The EBIOS [11], [12] method implements this approach within two modules which cover analysis of the risks at the primary asset level (called “essential assets” in EBIOS [11], [12]) and the secondary asset level. Some of the cyber-risk approaches were primarily developed for risks required by regulation, such as those associated with radioactive release. Nonetheless, such cyber-risk approaches could be used as a starting point for developing a cybersecurity framework for addressing risks not required by regulation.
- Performing security audits, as mandated by France’s cyber-risk approach [44] for the approval of information systems of vital importance, allows to better estimate the cybersecurity of those systems. This includes pre-developed components, and thus addresses challenge 4. Furthermore, security audits can help evaluate the effectiveness of security controls that may be proposed during the risk management process, addressing challenge 7.

The cyber-risk approaches have significant alignment with ISO/IEC 27005 [5] elements with many identified key insights that could establish the basis for a new IEC cybersecurity risk management standard for NPPs. However, while each cyber-risk approach is consistent with ISO/IEC, these approaches may not be aligned with each other, and additional work is required to identify and resolve differences between cyber-risk approaches.

Annex A
(informative)

Chinese approach

A.1 Summary of general approach

Currently there is no unified and standard cyber security assessment approach in nuclear sector in China. Based on the previous project experience, a national standard of cyber security assessment for industrial control systems is chosen as the China approach. The national standard is GB/T 36466-2018 [23] “Information security technology-Implementation guide to risk assessment of industrial control systems”. The China approach can provide insights for most of the challenges identified in Table A.1. See also Table A.2 through Table A.12.

Table A.1 – Chinese approach: Challenges addressed

Challenge	Description
1	Aggregate Risk of Multiple Units / Locations
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber- risk management
6	Lack of Abstract Analysis Methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
9	Excessive Information volume
10	Lack of a Common and Comprehensive Risk Management Process
11	Advanced Security Capabilities Incompatibility

A.2 ISO/IEC 27005:2018, 7.1 Context establishment

ISO/IEC 27005:2018, [5] 7.1 deals with context establishment, both internal and external.

The China approach addresses this topic through the following:

- Clause 5 “Implementation Methods,” provides the implementation methods of risk assessment for ICS as checking documents, on-site interviews, on-site review, on-site tests, and simulation tests. All these methods can help discover vulnerabilities. Especially due to the high availability requirements for ICS, it’s not feasible to do a penetration test in the real environment, so it proposes to do the penetration test in a mock-up environment. This method can be used for discovering vulnerabilities of a whole ICS or the components of an ICS.

Table A.2 – Chinese approach: Insights for ISO/IEC subclause 7.1

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.1		X		X	X		X		X	X	X

A.3 ISO/IEC 27005:2018, 7.2 Basic criteria

ISO/IEC 27005:2018, [5] 7.2 covers the basic criteria for the security risk management process.

The China approach addresses this topic through the following:

- 4.3.2 “Risk Assessment Process”: The cited section illustrates the risk evaluation process and specifies it as three steps: preparation of risk assessment, assessment of risk element, and comprehensive analysis.
- 6.1.3 “Scope Definition” provides the process of defining the scope of risk assessment of ICS, including input elements, methods, and output elements. The input elements contain the assets related to the evaluation target of the organization.

Table A.3 – Chinese approach: Insights for ISO/IEC sublause 7.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.2		X			X		X		X	X	

A.4 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment

ISO/IEC 27005:2018, [5] 8.1 provides a general description of the information security risk assessment.

The China approach addresses this topic through the following:

- 6.1 “Preparation” describes the risk assessment's general steps, including Assessment objective identification, Assessment scope determination, Assessment team setup, System investigation, Assessment plan formulation, and Mock-up system building (if necessary).

The key insight for Challenge 2 “Complexity of interdependencies and Interactions,” is provided by the China approach. The 6.1 mock-up system building could be a benefit in identifying the system’s interdependencies and/or interactions with less significant functions.

Table A.4 – Chinese approach: Insights for ISO/IEC subclause 8.1

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.1	X	Key		X		X	X			X	

A.5 ISO/IEC 27005:2018, 8.2 Risk identification

ISO/IEC 27005:2018, [5] 8.2 covers: Identification of assets, threats, existing controls, vulnerabilities, and consequences.

The China approach identifies the four basic elements of risk:

a) Identification of assets,

b) Identification of threats,

c) Identification of vulnerabilities, and

d) Identification of protection capabilities.

The protection capabilities are the capabilities of the organization to provide cyber security protection measures and controls.

The China approach addresses these areas through the following:

- 6.2.2 “Asset Classification” and 6.2.3 “Asset Investigation”. A way of asset classification is suggested. Assets are classified into hardware, software, and personnel assets based on their manifestation pattern.
  - The hardware assets are divided into seven categories: field control layer, network, security, computer, storage, transmission lines, and supporting equipment.
  - The software assets are divided into seven categories: operating system software, application software, source program, proprietary protocols of industrial control systems, the general protocol of networking, data, and system logs.
  - The personnel assets are cybersecurity staff, ICS design and integration staff, critical equipment vendors, operating staff, and maintenance staff.
- 6.3.2 “Threat Classification” and 6.3.3 “Threat Investigation”. The threat sources, like the threat agents, are classified into environmental factors, internal non-malicious false operations, internal malicious compromise, external cyber attacks, and supply chains.
- 6.4.2 “Physical Environmental Vulnerability Identification”, 6.4.3 “Network Vulnerability Identification”, and 6.4.4 “Platform Vulnerability Identification”. Vulnerabilities are grouped into three classes, physical environment, network, and platform. Several vulnerability lists are provided. These lists include the physical environment vulnerability list, the network architecture and boundary vulnerability list, the network equipment vulnerability list, the communication, and wireless connection vulnerability list, the platform hardware vulnerability list, the platform software vulnerability list, and the platform configuration vulnerability list.
- 6.5 “Protection Capability Assessment”. The protection capabilities include the capabilities related to network security management, ICS security management, Cryptography management, education and training, incident response, and technical protection capability. Another Chinese national standard GB/T 32919-2016 [48], “Information security technology – Application guide to industrial control system security control,” is referred by this section.

The key insight for Challenge 7, “Uncertainty in vulnerability/susceptibility analysis,” is provided by the China approach. First, the China approach regards vulnerabilities that can be identified but cannot be easily fixed. Thus, it is suggested the results of the vulnerability assessment be classified. Second, the China approach provides detailed vulnerability lists and ways to identify them.

The key insight for Challenge 11, “Advanced security capabilities incompatibility,” is provided in the China approach. The China approach of GB/T 36466-2018 [23] refers to another Chinese national standard GB/T 32919-2016 [48], “Information security technology – Application guide to industrial control system security control,” which describes the process of choosing and tailoring the security controls, including the advanced security capabilities, for industrial control systems.

Table A.5 – Chinese approach: Insights for ISO/IEC subclause 8.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.2	X	X		X	X		Key	X	X	X	Key

A.6 ISO/IEC 27005:2018, 8.3 Risk analysis

ISO/IEC 27005:2018, [5] 8.3 covers risk analysis. The China approach addresses it through the following :

- 6.2.4 “Asset Analysis” describes the asset valuation method according to the associated applications, referring to GB/T 20984 “Information security technology – Risk assessment method for information security” [49].
- 6.3.4 “Threat Analysis” describes the threat's valuation method, according to the threat probability and impact, referring to GB/T 31509 “Information security technology – Guide of implementation for information security risk assessment” [50].
- 6.4.4 “Vulnerability Analysis,” describes the valuation method for the vulnerabilities, according to the vulnerability impact, vulnerability exploitation difficulty, and vulnerability prevalence, referring to the Common Vulnerability Scoring System.
- 6.5.8 “Protection Capability Analysis,” describes the valuation method for the protection capability, referring to GB/T 32919-2016 “Information security technology – Application guide to industrial control system security control” [48].
- 6.6.1 “Risk Analysis principle”. The basic risk estimation method is R = F(Loss, Likelihood) = F(f(A, P), g(T, V, P)), where the A, T, V, P are the results from the above four valuation process of the assets, the threats, the vulnerabilities, and the protection capabilities.

The key insight for Challenge 3, “Incident Likelihood Determination,” is provided by the China approach. 6.6.1 provides a calculation method to estimate the loss, i.e., consequences and the likelihood of an incident.

Table A.6 – Chinese approach: Insights for ISO/IEC subclause 8.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.3	X	X	Key	X	X	X	X	X	X	X	X

A.7 ISO/IEC 27005:2018, 8.4 Risk evaluation

ISO/IEC 27005:2018, [5] 8.4 deals with risk evaluation. The China approach addresses it through the following:

- 6.6.2 “Risk determination”. It provides a five-level grading method for the risk analysis results. For each level, a description of the risk criteria is given to help determine whether this risk level is acceptable.

Table A.7 – Chinese approach: Insights for ISO/IEC subclause 8.4

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.4	X	X	X	X	X	X	X	X	X	X	X

A.8 ISO/IEC 27005:2018, 9.1 General description of risk treatment

ISO/IEC 27005:2018, [5] 9.1 deals with a general description of risk treatment. The China approach addresses it through the following:

- 6.7 “residual risk control”.

Table A.8 – Chinese approach: Insights for ISO/IEC subclause 9.1

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.1	X		X		X		X				

A.9 ISO/IEC 27005:2018, 9.2 Risk modification

ISO/IEC 27005:2018 [5], 9.2 deals with risk modification. The China approach addresses it through the following:

- 6.7 “residual risk control”.

Table A.9 – Chinese approach: Insights for ISO/IEC subclause 9.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.2	X		X		X		X	X	X	X	X

A.10 ISO/IEC 27005:2018, 9.3 Risk retention

ISO/IEC 27005:2018, [5] 9.3 deals with risk retention. The China approach addresses it through the following:

- 6.7 “residual risk control”.

Table A.10 – Chinese approach: Insights for ISO/IEC subclause 9.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.3	X				X		X	X		X	

A.11 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance

ISO/IEC 27005:2018 [5], Clause 10 deals with risk acceptance. The China approach addresses it through the following:

- 6.6.2 “Risk determination”.

Table A.11 – Chinese approach: Insights for ISO/IEC Clause 10

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
10	X	X	X	X	X	X	X	X		X	X

A.12 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review

ISO/IEC 27005:2018, [5] Clause 12 deals with monitoring and review.

The China approach addresses it through the following:

- 6.7 “residual risk control”.

Table A.12 – Chinese approach: Insights for ISO/IEC Clause 12

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
12	X		X	X	X		X	X	X	X	X

Annex B
(informative)

Cyber informed engineering

B.1 Summary of general approach

Cyber informed engineering (CIE) [10] is a body of knowledge and a methodology to characterize the risks presented by the introduction of digital computer systems in a traditionally analog environment and offer a strategy to apply engineering risk processes to mitigate these risks. It includes methods to ensure that cyber risks are considered throughout the design life cycle, as well as techniques which allow the elimination of cyber risk via traditional engineering methods (see Reference documents, INL 2015) CIE consists of a framework of twelve principles to ensure that cybersecurity demands inform design. These twelve elements are grouped into two types:

a) Design and Operational Principles
   1) Consequence-Focused Design
   2) Engineered Controls
   3) Secure Information Architecture
   4) Design Simplification
   5) Resilient Layered Defenses
   6) Active Defense
b) Organizational Principles
   1) Interdependency evaluation
   2) Digital Asset Awareness
   3) Cyber-secure supply chain controls
   4) Planned resilience with no assumed security
   5) Engineering Information Control
   6) Cybersecurity Culture

The guidance provided by the CIE addressing the following challenges is seen as key insights to the overall risk management process. See also Table B.1 through Table B.11.

Table B.1 – Cyber informed engineering: Key challenges addressed

Challenge	Description
2	Complexity of Interdependencies and Interactions
3	Incident Likelihood Determination
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
6	Lack of Abstract Analysis Methods
9	Excessive Information Volume

Challenges indirectly addressed by the CIE are:

Table B.2 – Cyber informed engineering: Challenges indirectly addressed

Challenge	Description
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
10	Lack of a Common and Comprehensive Risk Management Process
11	Advanced Security Capabilities Incompatibility

These indirectly addressed challenges require analysis and interpretation to derive insights and are therefore not seen as key for establishing a consensus risk management process for NPP cybersecurity.

B.2 ISO/IEC 27005:2018, 7.1 General considerations

CIE [10] principles are applied to the system lifecycle to ensure cybersecurity principles are applied. However, CIE does not address the overall risk management approach and therefore does not cover ISO/IEC 27005:2018, [5] Clause 7.

B.3 ISO/IEC 27005:2018, 7.2 Basic criteria

ISO/IEC 27005:2018, [5] 7.2 considers the following aspects of basic criteria:

- 7.2.1 Risk Management Approach
- 7.2.2 Risk Evaluation Criteria
- 7.2.3 Impact Criteria
- 7.2.4 Risk Acceptance Criteria

CIE [10] has three principles that provide input to the basic criteria:

a) Consequence Focused Design that focuses on functions that could result in unacceptable consequences and examine how to avoid such consequences through secure design, implementation, and operations,

b) Cybersecurity culture to consider cyber-related concerns, and

c) Planned resilience with no assumed security where conservative assumptions are to expect that the system will be compromised at some point in the system lifecycle.

CIE [10] has a branch named “Consequence-driven, Cyber-Informed Engineering” that has four steps:

d) Consequence prioritization;

e) Systems-of-Systems analysis (focused on access);

f) Consequence-based Targeting (e.g., kill chain analysis), and

g) Mitigations and Protections engineering risk analysis (e.g., Kill Chain Mitigations) that provides a key insight to investigate Challenge 3 (Incident Likelihood Determination) (see Reference documents, IntechOpen Journals 2022).

Table B.3 – Cyber informed engineering: Insights for ISO/IEC subclause 7.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.2		X	Key	X		X			X	X	

B.4 ISO/IEC 27005:2018, 7.3 Scope and boundaries

CIE [10] has three principles that directly support Scope and Boundaries:

a) Interdependency evaluation,

b) Consequence-Focused Design,

c) Digital Asset Awareness. The principles and aids (Annex D) are general but provide a good scoping checklist to set the scope and boundaries of a risk assessment for a particular system.

Table B.4 – Cyber-informed engineering: Insights for ISO/IEC subclause 7.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.3		X	X	X		X			X		

B.5 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment

CIE [10] is an approach that supplements risk assessment based on the system lifecycle. CIE does not define a risk assessment sequence or method. However, a case study on CIE [B-3] suggests using the formula:

Cyber Risk = f(threat, vulnerability, consequence)

While this approach does not address the challenges that identify uncertainty in threat and vulnerability, it is an alternative approach to risk evaluation.

B.6 ISO/IEC 27005:2018, 8.2 Risk identification

ISO/IEC 27005:2018, [5] 8.2 considers the following aspects of risk identification:

- 8.2.1 Introduction to risk identification
- 8.2.2 Identification of assets
- 8.2.3 Identification of threats
- 8.2.4 Identification of existing controls
- 8.2.5 Identification of vulnerabilities
- 8.2.6 Identification of consequences

CIE [10] principles effectively support challenges but are too general to provide key insights for risk management. CIE principles:

a) digital asset awareness,

b) Resilient Layered Defenses, and

c) Active Defense state what needs to be achieved and cover much of the risk identification clauses but do not detail how to perform or implement these principles. Annex D contains checklists and questions that can structure the application of CIE principles.

The case study [B-3] provides hazard and operability (HAZOP) analysis as an effective complement to Risk Analysis. The focus of HAZOP was to identify the consequences of cyber incidents on the new I&C components. Cyber incidents considered included deliberate and inadvertent actions that could disrupt data or information flow within a control system leading to degradation, mal-operation, or failure of a digital device and/or system functions. Also considered were incidents that could result in an ‘unknown’ state—a potentially dangerous state for a light water reactor.

Specifically, supply chain analysis is supported by the supply chain attack surface (SCAS) referenced within CIE (see Reference documents, IntechOpen Journals 2022). The SCAS provides categories of attacks, their point of entry within the supply chain, and the interactions and interdependencies within the supply chain. These categories are especially helpful for identifying risks within the supply chain for systems, services, and components.

Table B.5 – Cyber informed engineering: Insights for ISO/IEC subclause 8.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.2		Key	X	Key		X			X		

B.7 ISO/IEC 27005:2018, 8.3 Risk analysis

ISO/IEC 27005:2018, [5] 8.3 considers the following aspects of risk analysis:

- 8.3.1 Risk analysis methodologies
- 8.3.2 Assessment of consequences
- 8.3.3 Assessment of incident likelihood
- 8.3.4 Level of risk determination

The CIE [10] principle of consequence-focused design is key in prioritizing avoidance of consequences. However, CIE does not detail what " avoidance " means and is likely to infer risk avoidance and risk modification options.

Table B.6 – Cyber-informed engineering: Insights for ISO/IEC subclause 8.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.3		X	X	X		X			X		

B.8 ISO/IEC 27005:2018, 9.2 Risk modification

The CIE [10] principles aim to design, implement and operate engineered systems to avoid consequences. Risk modification could be associated with all design, operational, and organizational principles. Cyber-secure supply chain controls apply to modification if an organization is required to impose internal controls (e.g., Site Acceptance Test) and sharing if a supplier is required to impose controls or demonstrate effective risk management.

Table B.7 – Cyber informed engineering: Insights for ISO/IEC subclause 9.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.2		X	X	X		X			X		

B.9 ISO/IEC 27005:2018, 9.4 Risk avoidance

The CIE [10] principle of consequence-focused design states that avoidance of the consequence is prioritized. However, CIE does not detail whether avoidance is in terms of risk avoidance, where the activity is not undertaken or permitted. Therefore, the risk(s) associated with the activity is entirely avoided.

Table B.8 – Cyber informed engineering: Insights for ISO/IEC subclause 9.4

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.4		X	X	X		X			X		

B.10 ISO/IEC 27005:2018, 9.5 Risk sharing

The CIE [10] principle of cyber-secure supply chain controls generally addresses risk sharing by stating that procurement language and contract requirements are imposed on the vendor to ensure products meet design specifications and organizations demonstrate appropriate cybersecurity.

The supply chain attack surface (see Reference documents, IntechOpen Journals 2022) would assist with risk-sharing plans and arrangements.

Table B.9 – Cyber informed engineering: Insights for ISO/IEC subclause 9.5

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.5		X	X	X		X			X		

B.11 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation

The CIE principle of cybersecurity culture generally discusses the need for all employees (and users) of digital systems need to participate in cybersecurity. However, this principle does not contain guidance on how cybersecurity culture informs and communicates risk.

Table B.10 – Cyber informed engineering: Insights for ISO/IEC Clause 11

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
11		X	X	X		X			X		

B.12 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review

If implemented, the CIE [10] principle of active defense would provide key data and information necessary for risk monitoring and review. "Active defense is more than detection; it provides the ability to quickly collapse and remove the attacker's presence within the system. Only by having a full, accurate, and complete understanding of all system interactions are the defenders capable of such a task. Section 3.1.2.11 of INL/EXT-16-40099 Rev 0: Cyber-Informed Engineering (see Reference documents, INL 2017) identifies the key to active defense as being the highly skilled personnel resources that can evolve their capabilities to include creative and flexible behaviors. CIE principles indicate what needs to be achieved rather than how it may be implemented, limiting its insights to general outcomes and outputs.

IntechOpen Journals (see Reference documents, IntechOpen Journals 2022) provides a notional usage of CIE [10] principals throughout the systems engineering lifecycle. While not focused on risk management, this notional usage would be helpful to understand what activities are needed to appropriately identify risks and manage them during the system's lifecycle.

Table B.11 – Cyber informed engineering: Insights for ISO/IEC Clause 12

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
12		X	X	X		X			X		

B.13 Reference documents

R. Anderson, J. Price, "INL/CON-15-34244 PrePrint, Cyber-Informed Engineering: The Need for a New Risk Informed and Design Methodology", International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange, INL, Idaho Falls, 2015

IntechOpen Journals, Cyber-Informed Engineering for Nuclear Reactor Digital Instrumentation and Control, http://dx.doi.org/10.5772/intechopen.101807, 2022

R. Anderson, J. Benjamin, V. Wright, L. Quinones and J. Paz, "INL/EXT-16-40099 Rev 0: Cyber-Informed Engineering," INL, Idaho Falls, 2017

S. L. Eggers, K. L. Le Blanc, R. W. Youngblood III, T. R. McJunkin, K. L. Frick, D. S. Wendt, R. S Anderson, "INL/CON-21-61671-Revision 1 Cyber-Informed Engineering Case Study of an Integrated Hydrogen Generation Plant," INL, Idaho Falls, 2021

Annex C
(informative)

French approach

C.1 Summary of general approach

The French approach consists in an approval procedure for information systems of vital importance. This approval requires to periodically perform risk analysis as well as security audits and requires the operator to formally manage the risks weighing on the systems of vital importance.

The French cyber-risk approach does not specify the risk analysis method that shall be used during the security approval, even though the EBIOS RM method is recommended. As such, the key insights of EBIOS methods regarding the challenges are not directly taken into account in the French approach.

EBIOS is described below. See also Table C.1 through Table C.14.

C.2 EBIOS

C.2.1 General

The EBIOS risk analysis is a comprehensive cybersecurity risk management tool compliant with the ISO/IEC 27001 [2], 27005 [5] and 31000 [51] standards.

'EBIOS' is a French acronym standing for expression of needs and identification of security objectives (*Expression des Besoins et Identification des Objectifs de Sécurité*). It has been designed by the French Information Security Central Office (DCSSI – *Direction Centrale de la Sécurité des Systèmes d'Information*, now called ANSSI – *Agence Nationale de la Sécurité des Systèmes d'Information*). EBIOS provides a formalized approach for assessing and treating risks within the field of information systems security, including support tools for contracting authorities, drafting documents, and raising awareness.

Using EBIOS is recommended by the authorities when implementing the French cyber-risk approach. Two versions of the EBIOS tool are used by the operators: EBIOS 2010 [12] and, more recently, from 2018, EBIOS Risk Manager [11].

C.2.2 EBIOS 2010

EBIOS 2010 [12] is the third revision of EBIOS method. It follows a process around 5 modules, see Figure C.1.

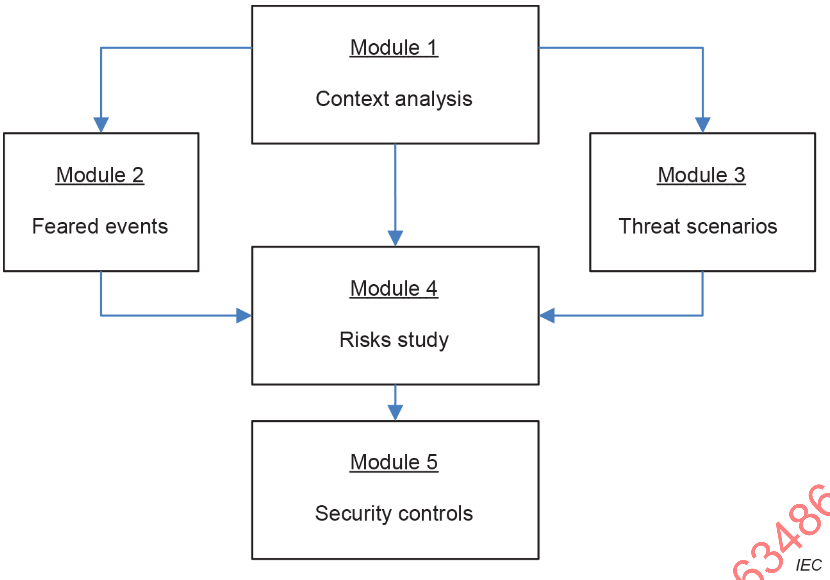


Figure C.1 – EBIOS 2010 process overview

Module 1: context analysis

The first module outlines the study's technical, business, and regulatory context. An information system is specifically based on essential elements, functions, and information that constitute the added value of the information system for the organization.

Output: Target of the study (Context + elements + entities)

Module 2: feared events

The second module contributes to the risk assessment. The module results in identifying the security needs of essential elements (in terms of availability, integrity, and confidentiality), a list of impacts (on missions, personnel security, finance, image, environment, etc.) when these security needs are not observed, and the sources of threats (human, environmental, internal, external, etc.) that can be at the origin. This identification helps define high-risk events.

Output: Sensitivities

Module 3: threat scenarios

The third module allows for identifying and evaluating the scenarios that can cause feared events to express risks. Such evaluation/estimation is performed by considering threats that sources threats can generate and exploitable vulnerabilities.

Output: Threat formalization (including scenarios)

Module 4: risks study

The fourth module highlights the risk to the entity by confronting feared events and threat scenarios. This module also describes how to estimate and evaluate this risk and how to identify associated security objectives.

Output: Security objectives

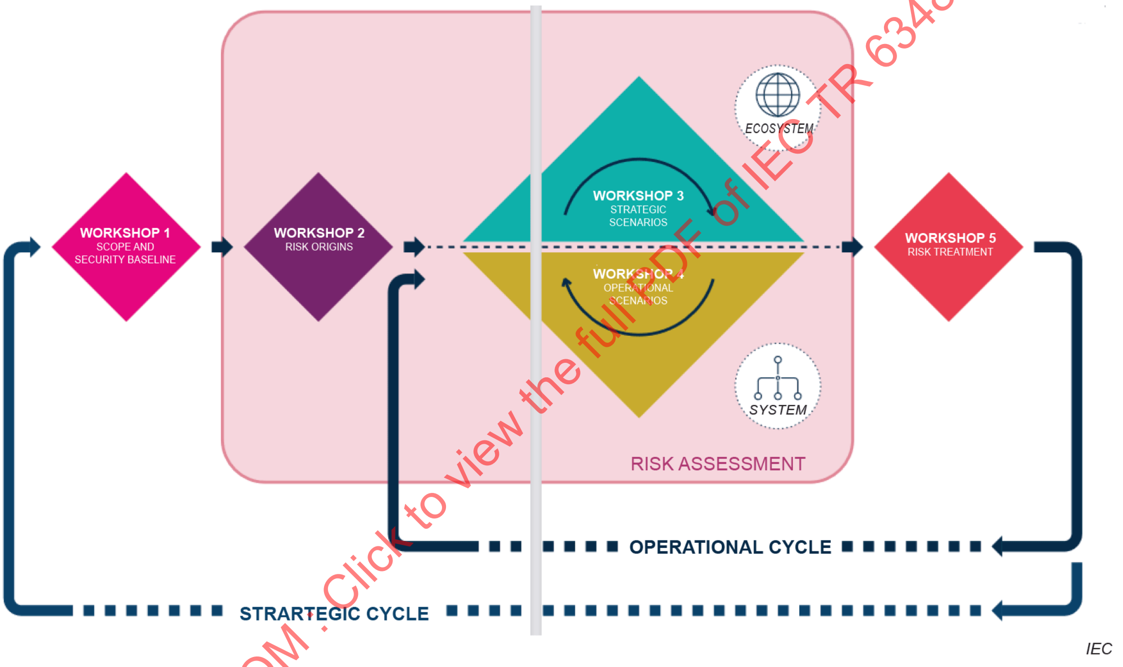
Module 5: security controls

The last module identifies security controls, how to implement these controls, and deal with residual risks. For systems under the nuclear cybersecurity order, the process of specific risk analysis leads, if appropriate, to implementing complementary security measures on top of the homogenous requirements provided by the security degree approach.

Output: Functional and assurance requirements

C.2.3 EBIOS RM

EBIOS Risk Manager [11] is the fourth and latest revision of the EBIOS method. It adopts an approach to managing the digital risk starting from the highest level (major missions of the studied object) to progressively reach the business and technical functions by studying possible risk scenarios. It is organized around five workshops, see Figure C.2.



https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf

Figure C.2 – EBIOS risk manager overview [11]

Workshop 1: scope and security baseline

The first workshop aims to identify the studied object, the workshop participants, and the timeframe. The mission, business assets, and supporting assets related to the studied object are listed during this workshop. The feared events associated with the business assets are identified, and the severity of their impacts is assessed. The security baseline is also defined.

Workshop 2: risk origins

In the second workshop, the risk origins (RO) and their high-level targets, called target objectives (TO), are identified and characterized. The RO/TO pairs deemed the most relevant are selected at the end of the workshop. The results are formalized in a mapping of the risk origins.

Workshop 3: strategic scenarios

In workshop 3, a mapping of the digital threat of the ecosystem for the studied object is established to construct high-level scenarios called strategic scenarios. They represent the attack paths a risk origin is likely to take to reach its target. The scenarios reflect the scale of the ecosystem and the business asset of the studied object and are assessed for severity. At the end of this workshop, the security measures on the ecosystem can already be defined.

Workshop 4: operational scenarios

The purpose of workshop 4 is to construct technical scenarios that include the methods of attack that are likely to be used by the risk origins to carry out the strategic scenarios. This workshop adopts an approach similar to the prior workshops but focuses on critical supporting assets. The level of likelihood of the operational scenarios obtained is then assessed.

Workshop 5: risk treatment

The last workshop consists of creating a summary of all the risks studied to define a risk treatment strategy. The latter is then broken down into security measures written into a continuous improvement plan. During this workshop, the summary of the residual risks is established, and the framework for monitoring risks is defined.

C.2.4 Mapping between modules/workshops from EBIOS methods and challenges

The modules or workshops that constitute key insights for the challenges are noted in bold in the following table.

Table C.1 – French approach: Challenges addressed

Challenge	EBIOS 2010 [12]	EBIOS RM [11]
1	Module 1	Workshop 1
2	Module 2	Workshop 2
3	**Module 2, Module 4**	Workshop 4
4	Module 3, Module 5	Workshop 3, Workshop 5
5	Not addressed	Not addressed
6	Module 1	Workshop 1
7	Not addressed	Not addressed
8	Module 2	Workshop 2
9	Not addressed	**Workshop 2**
10	**Module 2**	**Workshop 1**
11	Module 5	Workshop 5

Modules 2 and 4 from EBIOS 2010 method provide key insights for Challenges 3 and 10:

- Module 2 results in identifying all relevant risk sources (Challenge 3) and determining the final states (challenge 10).
- Module 4 supports the identification of the likelihood of each risk (Challenge 3).

Workshops 1 and 2 from EBIOS RM method provide key insights for Challenges 9 and 10:

- Workshop 1 identifies missions, business/essential assets, supporting assets, high-risk events associated with the business assets, and the severity of the associated impact. All events, even those with a less severe impact, are thus identified (Challenge 10).
- Workshop 2 results in selecting the most relevant pair risk origins/target objectives, reducing the number of situations to be considered (challenge 9).

None of the two EBIOS methods address Challenges 5 and 7, and EBIOS 2010 does not address Challenge 9.

C.3 ISO/IEC 27005:2018, 7.2 Basic criteria

ISO/IEC 27005:2018 [5] , 7.2 maps to the following French cyber-risk approach clauses:

- 7.2.1 (Risk management approach), 7.2.2 (Risk evaluation criteria), 7.2.3 (impact criteria), 7.2.4 (Risk acceptance criteria)
  – “Arrêté du 10 mars 2017” [44], appendix I, rule 2 (rule regarding the security approval)
  – “L’homologation de sécurité en neuf étapes simples” (“The security approval in nine simple steps”), step 1 (“what information systems do I need to get approved and why?”): “Detail the regulatory framework”

The French cyber-risk approach does not deal with challenges 5 and 9.

However, the French cyber-risk approach provides insights for Challenge 10 by not restricting the security approval only to systems whose attack may result in radioactive release or theft of nuclear material.

Table C.2 – French approach: Insights for ISO/IEC subclause 7.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.2		X					X			Key	

C.4 ISO/IEC 27005:2018, 7.3 Scope and boundaries

ISO/IEC 27005:2018, [5] 7.3 maps to the following French cyber-risk approach clauses:

- “Arrêté du 10 mars 2017” [44], appendix I, rule 2 (rule regarding the security approval)
- “L’homologation de sécurité en neuf étapes simples” (“The security approval in nine simple steps”), step 1 (“what information systems do I need to get approved and why?”): “2. Delimit the perimeter of the system”

The French cyber-risk approach does not deal with challenge 5.

However, the French cyber-risk approach provides insights for Challenge 10 by not restricting the security approval only to systems whose attack may result in radioactive release or theft of nuclear material.

Table C.3 – French approach: Insights for ISO/IEC subclause 7.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.3		X		X			X		X	Key	

C.5 ISO/IEC 27005:2018, 7.4 Organization for information security risk management

ISO/IEC 27005:2018 [5], 7.4 maps to the following French cyber-risk approach clauses:

- “Arrêté du 10 mars 2017” [44], appendix I, rule 2 (rule regarding the security approval)
- “L’homologation de sécurité en neuf étapes simples” (“The security approval in nine simple steps”), step 3 (“Who contributes to the approval?”)

The security approval involves the operator, the system owner, the security officer, and technical experts. As such, the French approach provides a key insight to dealing with challenge 10 in detecting consequences that are significant but are not regulatory.

Table C.4 – French approach: Insights for ISO/IEC subclause 7.4

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.4		X		X			X		X	Key	

C.6 ISO/IEC 27005:2018, 8.2 Risk identification

ISO/IEC 27005 [5]:2018, 8.2 maps to the following French cyber-risk approach clauses:

- 8.2.1 General
  - “Arrêté du 10 mars 2017” [44], introductory text
- 8.2.2 (Identification of assets), 8.2.3 (Identification of Threats), 8.2.4 (Identification of Existing Controls), 8.2.5 (Identification of Vulnerabilities)
  - “Arrêté du 10 mars 2017” [44], chapter II (declaration of information systems of vital importance)
- 8.2.6 (Identification of consequences)
  - “Arrêté du 10 mars 2017” [44], chapter II (declaration of information systems of vital importance)
  - “Arrêté du 10 mars 2017” [44], appendix I, rule 2 (“The approval of a system is a formal decision taken by the operator attesting that the security risks on a system have been identified and that the adequate protective means have been undertaken. It also attests that the possible residual risks have been identified and accepted by the operator.”)

The French cyber-risk approach regarding risk identification does not directly address challenges 5 and 9.

The French cyber-risk approach provides insights for Challenge 10 by not restricting the risk management approach only to consequences resulting in a radioactive release or theft of nuclear material. The security audit undertaken during the system approval may identify security risks whose impact may range from minor to critical.

Table C.5 – French approach: Insights for ISO/IEC subclause 8.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.2		X		X			X	X		Key	X

C.7 ISO/IEC 27005:2018, 8.3 Risk analysis

ISO/IEC 27005:2018 [5], 8.3 maps to the following French cyber-risk approach clauses:

- 8.3.1 (Risk analysis methodologies), 8.3.2 (Assessment of consequences), 8.3.3 (Assessment of incident likelihood), 8.3.4 (Level of risk determination)
  - "Arrêté du 10 mars 2017" [44], chapter II (declaration of information systems of vital importance)
  - "L'homologation de sécurité en neuf étapes simples" ("The security approval in nine simple steps"), step 5

The French cyber-risk approach does not specify the risk analysis method that shall be used during the security approval, even though the EBIOS method is recommended. As such, the French cyber-risk approach does not address the challenges of ISO/IEC subclause 8.3.

Table C.6 – French approach: Insights for ISO/IEC subclause 8.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.3											

C.8 ISO/IEC 27005:2018, 8.4 Risk evaluation

ISO/IEC 27005:2018 [5], 8.4 (Risk evaluation) maps to the following French cyber-risk approach clauses:

- "Arrêté du 10 mars 2017" [44], chapter II (declaration of information systems of vital importance)
- "L'homologation de sécurité en neuf étapes simples" ("The security approval in nine simple steps"), step 5 ("Which risks concern the system?")

The French cyber-risk approach does not specify the risk analysis method that shall be used during the security approval, even though the EBIOS method is recommended. As such, the French cyber-risk approach does not address the challenges of ISO/IEC subclause 8.4.

However, the French cyber-risk approach provides insights for Challenge 10 by not restricting the risk management approach only to consequences resulting in radioactive release or theft of nuclear material. The security audit undertaken during the system approval may identify security risks whose impact may range from minor to critical. From those risks and their acceptance criteria, the operator can manage the risk by either avoiding the risk, implementing security controls to mitigate it, or accepting the residual risks.

Table C.7 – French approach: Insights for ISO/IEC subclause 8.4

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.4										Key	

C.9 ISO/IEC 27005:2018, 9.1 General description of risk treatment

ISO/IEC 27005:2018 [5], 9.1 (General description of risk treatment) maps to the following French cyber-risk approach clauses:

- “Arrêté du 10 mars 2017” [44], appendix I, rule 2 (rule regarding the security approval)
- “Arrêté du 10 mars 2017” [44], appendix I, rule 4 (rule regarding the maintenance in security condition)
- “L’homologation de sécurité en neuf étapes simples” (“The security approval in nine simple steps”), step 7 (“Which supplementary security controls are required to address the risks?”)

The French cyber-risk approach regarding risk identification does not directly address challenge 5.

The French cyber-risk approach provides insights for Challenge 3. During the risk analysis, the French approach identifies security risks. During the security approval process, the operator notes those security risks. Furthermore, the French approach requires that the operator install all security controls mitigating risks on a system, except when there are justified technical or operational difficulties.

The French cyber-risk approach also provides insights for Challenge 7. Indeed, the risk analysis is followed by a security audit to verify that the security controls are implemented to mitigate the risks effectively and identify other risks. This security audit reduces the uncertainty associated with the input documents.

Table C.8 – French approach: Insights for ISO/IEC subclause 9.1

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.1	X		Key				Key				

C.10 ISO/IEC 27005:2018, 9.2 Risk modification

ISO/IEC 27005:2018 [5], 9.2 (Risk modification) maps to the following French cyber-risk approach clauses:

- “Arrêté du 10 mars 2017” [44], appendix I, rule 2 (rule regarding the security approval)
- “Arrêté du 10 mars 2017” [44], appendix I, rule 4 (rule regarding the maintenance in security condition)
- “L’homologation de sécurité en neuf étapes simples” (“The security approval in nine simple steps”), step 7 (“Which supplementary security controls are required to address the risks?”)

The French cyber-risk approach regarding risk modification does not directly address challenges 5 and 9.

The French cyber-risk approach provides insights for Challenges 3 and 10.

During the risk analysis, the French approach identifies security risks. During the security approval process, the operator notes those security risks. Furthermore, the French approach requires that the operator install all security controls mitigating risks on a system, except when there are justified technical or operational difficulties.

The operator can also manage all significant risks, not restricted to the radioactive release. Indeed, the risk management approach is not focused only on consequences resulting in radioactive release or theft of nuclear material. Furthermore, the security audit undertaken during the system approval may identify security risks whose impact may range from minor to critical. When the risk is judged significant enough, the operator can implement security controls to modify it.

Table C.9 – French approach: Insights for ISO/IEC subclause 9.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.2	X		Key					X		Key	X

C.11 ISO/IEC 27005:2018, 9.3 Risk retention

ISO/IEC 27005:2018, [5] 9.3 (Risk retention) maps to the following French cyber-risk approach clauses:

- "Arrêté du 10 mars 2017" [44], appendix I, rule 2 (rule regarding the security approval)
- "Arrêté du 10 mars 2017" [44], appendix I, rule 4 (rule regarding the maintenance in security condition)
- "L'homologation de sécurité en neuf étapes simples" ("The security approval in nine simple steps"), step 7 ("Which supplementary security controls are required to address the risks?")

The French cyber-risk approach regarding risk modification does not directly address Challenge 5.

The French cyber-risk approach provides insights for Challenges 7 and 10.

The risk analysis is followed by a security audit that verifies the risk level of the retained risks. This security audit reduces the uncertainty associated with the input documents.

Furthermore, the operator can manage all significant risks, not restricted to the radioactive release: indeed, the risk management approach only to consequences resulting in radioactive release or theft of nuclear material. Furthermore, the security audit undertaken during the system approval may identify security risks whose impact may range from minor to critical. When the risk is judged insignificant enough, the operator can take the formal decision to retain this risk.

Table C.10 – French approach: Insights for ISO/IEC subclause 9.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.3	X						X			Key	

C.12 ISO/IEC 27005:2018, 9.4 Risk avoidance

ISO/IEC 27005:2018 [5], 9.4 (Risk avoidance) maps to the following French cyber-risk approach clauses:

- “Arrêté du 10 mars 2017” [44], appendix I, rule 2 (rule regarding the security approval)
- “Arrêté du 10 mars 2017” [44], appendix I, rule 4 (rule regarding the maintenance in security condition)
- “L’homologation de sécurité en neuf étapes simples” (“The security approval in nine simple steps”), step 7 (“Which supplementary security controls are required to address the risks?”)

The French cyber-risk approach regarding risk modification does not directly address challenge 5 and 9.

The French national indirectly addresses challenges 1 and 8.

Table C.11 – French approach: Insights for ISO/IEC subclause 9.4

ISO /IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.4	X							X			

C.13 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance

ISO/IEC 27005:2018 [5], Clause 10 (Risk acceptance) maps to the following French cyber-risk approach clauses:

- “Arrêté du 10 mars 2017” [44], appendix I, rule 2 (rule regarding the security approval)
- “Arrêté du 10 mars 2017” [44], appendix I, rule 4 (rule regarding the maintenance in security condition)
- “L’homologation de sécurité en neuf étapes simples” (“The security approval in nine simple steps”), step 7 (“Which supplementary security controls are required to address the risks?”)

The French cyber-risk approach regarding risk modification does not directly address challenge 5.

The French cyber-risk approach provides key insights regarding challenges 3, 4, 7, and 10.

During the risk analysis, the French approach identifies security risks. During the security approval process, the operator takes note of all the security risks, including those with an extremely rare occurrence. Furthermore, the French approach requires that the operator install all security controls mitigating risks on a system, except when there are justified technical or operational difficulties.

The risk analysis is followed by a security audit that allows to verify the risk level of the retained risks. This security audit allows to reduce the uncertainty associated with the input documents and with the pre-developed components with no identified or evaluated risks.

The operator is also able to manage all significant risks, not restricted to the radioactive release: indeed, the risk management approach only to consequences resulting in radioactive release or theft of nuclear material. Furthermore, the security audit undertaken during the system approval may identify security risks which impact may range from minor to critical. When the risk is judged insignificant enough, the operator is able to take the formal decision to retain this risk.

Table C.12 – French approach: Insights for ISO/IEC Clause 10

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
10	X	X	Key	Key		X	Key	X		Key	

C.14 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation

ISO/IEC 27005:2018, [5] Clause 11 (Information security risk communication and consultation) maps to the following French cyber-risk approach clauses:

- “Arrêté du 10 mars 2017” [44], appendix I, rule 2 (rule regarding the security approval)
- “L’homologation de sécurité en neuf étapes simples” (“The security approval in nine simple steps”), step 8 (“How to decide on the approval?”)

The French cyber-risk approach regarding risk modification does not directly address challenges 5 and 9.

The French cyber-risk approach provides key insights regarding challenges 3, 4, 7, and 10.

During the risk analysis, the French approach identifies security risks. During the security approval process, the operator takes note of all the security risks, including those with an extremely rare occurrence. Furthermore, the French approach requires that the operator install all security controls mitigating risks on a system, except when there are justified technical or operational difficulties.

The risk analysis is followed by a security audit that allows to verify the risk level of the retained risks. This security audit allows to reduce the uncertainty associated with the input documents and with the pre-developed components with no identified or evaluated risks.

The operator is also able to manage all significant risks, not restricted to the radioactive release: indeed, the risk management approach only to consequences resulting in radioactive release or theft of nuclear material. Furthermore, the security audit undertaken during the system approval may identify security risks which impact may range from minor to critical. When the risk is judged insignificant enough, the operator is able to take the formal decision to retain this risk.

The security risks identified, the results of the security audit, the assumed security risks are all part of the approval file, which is share between the stakeholders.

Table C.13 – French approach: Insights for ISO/IEC Clause 11

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
11	X	X	Key	Key		X	Key	X		Key	

C.15 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review

ISO/IEC 27005:2018 [5], Clause 12 (Information security risk monitoring and review) maps to the following French cyber-risk approach clauses:

- “Arrêté du 10 mars 2017” [44], appendix I, rule 2 (rule regarding the security approval)
- “L’homologation de sécurité en neuf étapes simples” (“The security approval in nine simple steps”), step 8 (“How to decide on the approval?”)

The French cyber-risk approach regarding risk modification does not directly address challenges 5 and 9.

The French cyber-risk approach provides key insights regarding challenges 3, 4, 7, and 10. The approval is reviewed at least every three years as well as when an event or an evolution modifies the context of the system. The same process as the initial approval is thus regularly conducted: a new risk analysis, taking into account the potential new risks identified, and another security audit is conducted.

This reexamination allows to update the unacceptable events (challenge 3), to take into account the potential new information regarding pre-developed components (challenge 4), to reduce the uncertainty associated with input documents (challenge 7), or to take into account new significant risks (challenge 10).

Table C.14 – French approach: Insights for ISO/IEC Clause 12

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
12	X		Key	Key	X		Key	X	X	Key	X

Annex D
(informative)

German approach

D.1 Summary of general approach

The German approach addresses, deals within the nuclear sector not with all the challenges identified in Table 1 below. The basis of the German approach within nuclear is the so called SEWD-RL IT guideline [22]. This document is classified as restricted and some additional document as confidential.

There are in Germany many other sector overlapping rules and guidelines which cover the missing challenges. These additional guidelines are the Energy Industry Act with the corresponding papers for the critical infrastructure. See also Table D.1 through Table D.15.

D.2 ISO/IEC 27005:2018, 7.1 General considerations

7.1 deals with general considerations.

For the German perspective the key element is Challenge 10 “Lack of a common and comprehensive risk management process” due to the fact, that different authorities and the authorized technical support organizations are coping with different risk assessment objectives in a comprehensive manner.

Table D.1 – German approach: Insights for ISO/IEC subclause 7.1

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.1		X			X		X		X	Key	

D.3 ISO/IEC 27005:2018, 7.2 Basic criteria

7.2 covers the basic criteria for the security risk management process.

Challenge 10 deals with the topic of “Lack of a common and comprehensive risk management process.” Specifically, this challenge deals with risks associated with consequences that will not result in radioactive release or theft of nuclear material (i.e., required by other regulations). The risks that lead to these consequences will be identified according to domain independent standards and guidelines, like those that especially address cybersecurity for IT and digital I&C as well as overall plant security and therefore, not effectively managed. The SEWD-RL IT covers these risks only implicit, as the main focus is on systems and their risks which are under authority supervision. Also, there is an appendix with a given classification, where the resulting classification is not intuitive or simple for all.

Table D.2 – German approach: Insights for ISO/IEC subclause 7.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.2		X	X	X	X					Key	

D.4 ISO/IEC 27005:2018, 7.3 Scope and boundaries

7.3 covers topics to scope and boundaries for the security risk management process.

Challenge 5 deals with differences in national risk management and there are two frameworks in that area in Germany. One is ISO/IEC 27005 [5] and the other BSI 200-3 [42] (former version BSI 100-3) which are not fully compatible.

Table D.3 – German approach: Insights for ISO/IEC subclause 7.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.3					Key					X	

D.5 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment

8.1 provides a general description of the information security risk assessment. In the German approach:

Challenge 4 with “Unknown or lacking sufficient detail for pre-developed components.” is the key element, as there is specific topic in the guideline, but this topic is unspecific in requirements and measures.

Table D.4 – German approach: Insights for ISO/IEC sublause 8.1

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.1		X		X			X				

D.6 ISO/IEC 27005:2018, 8.2 Risk identification

8.2 covers:

a) Asset Identification,

b) Threat Identification,

c) Identification of existing controls,

d) Identification of vulnerabilities, and

e) Identification of consequences.

The German approach addresses these areas through the SEWD-RL IT which request of all five mentioned points.

But the risk management process underlay some restrains by local nuclear authorities and can vary between plants.

Table D.5 – German approach: Insights for ISO/IEC subclause 8.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.2		X			X		X	X	X	Key	

D.7 ISO/IEC 27005:2018, 8.3 Risk analysis

8.3 covers risk analysis. The German approach can be done with ISO/IEC 27005 [5] as well as BSI 200-3 [42]. But in both cases the uncertainty in the adversary characterisation is the challenge and so defined as key element.

Table D.6 – German approach: Insights for ISO/IEC sublause 8.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.3	X	X	X	X	X	X	X	Key	X	X	X

D.8 ISO/IEC 27005:2018, 8.4 Risk evaluation

8.4 deals with risk evaluation. The German approach is based on classified nuclear documents and in addition on domain independent guidelines and standards. Therefore challenge 10 is concerned. The key element is Challenge 7, “Uncertainty in vulnerability/susceptibility analysis.”

Table D.7 – German approach: Insights for ISO/IEC subclause 8.4

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.4							Key			X	

D.9 ISO/IEC 27005:2018, 9.1 General description of risk treatment

9.1 deals with a general description of risk treatment. The German approach addresses it through ISO/IEC 27005:2018, [5] 9.1, which states that: "Output: Risk treatment plan and residual risks subject to the acceptance decision of the organization's managers." And no risk can be untreated. It shall be avoided, mitigated, or accepted.

Table D.8 – German approach: Insights for ISO/IEC subclause 9.1

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.1			X				Key	X			

D.10 ISO/IEC 27005:2018, 9.2 Risk modification

9.2 deals with risk modification. The German approach addresses it through the requirement in the guidelines, that risks shall be modified to an acceptable level.

Table D.9 – German approach: Insights for ISO/IEC subclause 9.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.2			X				X	X	X	Key	

D.11 ISO/IEC 27005:2018, 9.3 Risk retention

9.3 deals with risk retention. The German approach addresses it through the requirement, that risk retention shall be clearly documented and formal accepted by the company board and the risk owner.

Table D.10 – German approach: Insights for ISO/IEC sublause 9.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.3	X				Key		Key	X		X	

D.12 ISO/IEC 27005:2018, 9.4 Risk avoidance

9.4 deals with risk avoidance. The German approach also addresses the avoidance of risk. This is a key element for Challenge 7.

Table D.11 – German approach: Insights for ISO/IEC sublause 9.4

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.4		X			X		Key	X		X	

D.13 ISO/IEC 27005:2018, 9.5 Risk sharing

9.5 deals with risk sharing. The German approach allows the sharing of risk, but it shall be clearly documented and formal accepted by the risk owner and the company board. This is a key element for Challenge 7.

Table D.12 – German approach: Insights for ISO/IEC sublause 9.5

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.5		X			X		Key	X		X	

D.14 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance

Clause 10 deals with risk acceptance. The German approach addresses like Clause 10 of ISO/IEC 27005:2018 [5]. The key element is again Challenge 5 with the different objectives and tasks of different authorities, see Clause D.2.

Table D.13 – German approach: Insights for ISO/IEC Clause 10

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
10	X	X	X	X	Key	X	X	X		X	X

D.15 ISO/IEC 27005 :2018,Clause 11 Information security risk communication and consultation

Clause 11 deals with risk communication and consultation. The German approach addresses like Clause 11 of ISO/IEC 27005:2018 [5]. Key elements are Challenge 2 due to the complexity and Challenge 10 a common and comprehensive risk management, see Clause D.2.

Table D.14 – German approach: Insights for ISO/IEC Clause 11

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
11	X	Key	X	X	X	X	X	X	X	Key	X

D.16 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review

Clause 12 deals with monitoring and review. The German approach is especially directed to the two key aspects: Challenge 7 with an uncertainty of analysis and Challenge 9 by the immense amount of information, risks and systems.

Table D.15 – German approach: Insights for ISO/IEC Clause 12

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
12	X		X	X	X		Key	X	Key	X	X

Annex E
(informative)

Harmonized threat and risk assessment (Canada)

E.1 ISO/IEC 27005:2018, 7.2 Basic criteria

The key to HTRA (see Reference documents, CSE 2007) is the ability to tier the analysis (e.g., System, Department, Organization), scoping, and providing multiple generic lists for vulnerabilities, threats, consequences, etc.

Challenge 2 – is not directly covered by the HTRA.

7.2 covers a wide range of risk criteria. HTRA assists this through providing pre-compiled lists of these criteria. A key part of HTRA are the hierarchical structures, taxonomy, extensive glossary and criteria that provides for a consistent approach even though specific consequences associated with NPPs are not detailed other than Nuclear Accidents.

Challenge 7 deals with uncertainty regarding vulnerabilities. A key insight in HTRA is the use of lists of vulnerabilities which can be used where the actual vulnerabilities are not known with certainty. See also Table E.1 through Table E.14.

Table E.1 – Harmonized threat and risk assessment: Insights for ISO/IEC subclause 7.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.2		X			X		Key		X	X	

E.2 ISO/IEC 27005:2018, 7.3 Scope and boundaries

ISO/IEC 7.3 maps to HTRA:

- Management Summary, Section 2.4 ("Scope of the TRA Project") recommends that TRAs be “*as short as possible consistent with the need for informed decision making*”. It is recommended that modular assessments are performed rather than a single large project, and that projects can be rescoped “*to meet changing circumstances such as the discovery of previously unknown threats and vulnerabilities*”
- Annex A – Section 4 ("Scope of assessment") warns that “*[u]nless realistic bounds are set at the start, subsequent data collection and analysis could become open-ended and the project might collapse under the sheer weight of the effort*”.
- Management Summary, Section 4 (“Threat Assessment”) notes “Upon completion of the Asset Identification and Valuation Phase, the TRA team shall identify “*any threats that could reasonably be expected to cause injury to employees, assets or service delivery*” and that “[*a*]*ll threats – man-made (deliberate or accidental) and natural hazards – are considered at a level of detail commensurate with the scope of the assessment*”. This approach is used throughout the document.

The use of smaller modular assessments is a key insight for addressing the following challenges

- 7 – Uncertainty in Vulnerability / Susceptibility Analysis
- 9 – Excessive Information Volume

The identification of “any threat that could reasonably expected to cause injury” is a key insight to challenge 10 “lack of a common and comprehensive risk management process” in that risks arising from any threat will be assessed and recommendation made (note that HTRA does not cover the risk management).

Table E.2 – Harmonized Threat and Risk Assessment: Insights for ISO/IEC Clause 7.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.3		X		X	X		Key		Key	Key	

E.3 ISO/IEC 27005:2018, 7.4 Organization for information security risk management

ISO/IEC 7.4 maps to the following HTRA clauses:

- Management Summary, Section 2.5 ("Team Composition")
- Management Summary, Section 2.6 ("Other Resources")
- Annex A, Section 5 ("TRA Team Composition")
- Appendix A-2, Section 2.3 ("Subject-Matter Experts")
- Appendix A-4 ("Use of TRA Consultants")
- Annex A, Section 6 ("TRA Work Plan")

HTRA [8] (clause 2.5) provides minimum list of staff to be included as stakeholders (program or business managers, project managers, facility manager, chief information officers, departmental security authorities). HTRA (clause 2.6) provides examples of other resources such as privacy coordinators, occupational health and safety staff, financial and material managers, internal auditors, and legal council and also provides (Appendix A-5) provides a more detailed list. HTRA states that the plan defines the terms of reference for each TRA team member (Appendix A-6).

The roles and responsibilities are based on Canada and the Canadian government, so they are not directly applicable outside of Canada, although the selected roles could inform the selection of similar individuals in other countries.

This provides an insight for challenge 9 where the organizational structure may be large and complex to deal with large amounts of information. HTRA requires definition of the roles and responsibilities within the TRA work plan which could be helpful for a large complex organization.

Table E.3 – Harmonized threat and risk assessment: Insights for ISO/IEC subclause 7.4

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.4		X		X	X		X		Key	X	

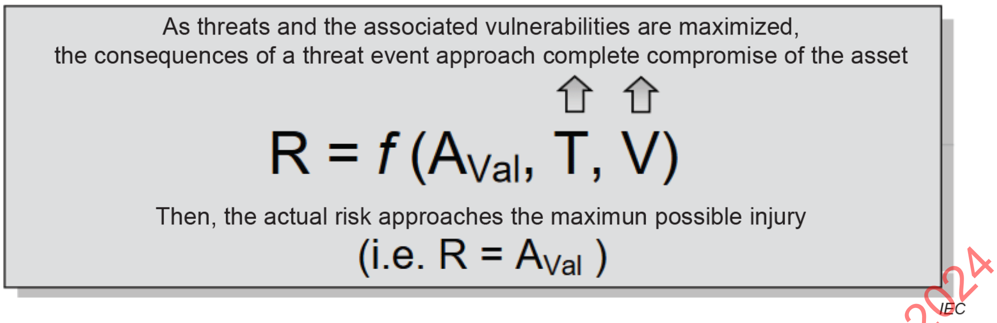
E.4 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment

HTRA is an approach that provides for assessment of risk arising from deliberate threats, accidental threats and natural hazards. HTRA uses the following formula for risk:

Risk = f (Asset Value, Threat, Vulnerability)

HTRA notes that as threat and vulnerability the risk approaches the maximum possible injury, see Figure E.1.

Risk = Asset Value



As threats and the associated vulnerabilities are maximized, the consequences of a threat event approach complete compromise of the asset

$$R = f\,(A_{Val}, T, V)$$

Then, the actual risk approaches the maximun possible injury

$$(\text{i.e. } R = A_{Val})$$

Figure E.1 – HTRA risk formula (Figure B-4 of [8])

E.5 ISO /IEC 27005:2018, 8.2 Risk identification

HTRA provides worksheets for performing the ISO/IEC 27005 [5] activities for risk identification (8.2.2 Identification of Assets, 8.2.3 Identification of threats, 8.2.4 Identification of Existing Controls, 8.2.5 Identification of Vulnerabilities, and 8.2.6 Identification of Consequences)

HTRA Annex C, §1.1 provides insights for risk identification, namely:

- Threat Identification – to list all threats that might affect assets within the scope of the assessment at an appropriate level of detail.
- Likelihood Assessment – to assess the probability of each threat actually occurring;
- Gravity Assessment – to determine the prospective impact of each threat.
- Threat Assessment – to assign threat levels ranging from Very Low to Very High for each threat based upon common metrics for likelihood and gravity.
- Prioritized Threat Listing – to produce a comprehensive list of threats which may be ranked from the most serious to the least.

This approach defines threat based upon likelihood and gravity, and table D-2 provides a relationship between threat capability and gravity.

Table E.4 – HTRA: Relationship between threat capability and gravity [8]

Deliberate Threat Agent Capabilities	Magnitude of Accidents of Natural Hazards	Threat Impact or Gravity
Extensive Knowledge/Skill Extensive Resources	Highly Destructive Extremely Grave Error Widespread Misuse	High
Limited Knowledge/Skill Extensive Resources Or Extensive Knowledge/Skill Limited Resources Or Moderate Knowledge/Skill Moderate Resources	Moderately Destructive Serious Error Significant Misuse	Medium
Limited Knowledge/Skill Limited Resources	Modestly Destructive Minor Error Limited Misuse	Low

This approach is applicable to any challenges which involve risk assessment and provides a key insight for challenge 10 (Lack of a common and comprehensive risk management process).

Figure C-3 provides insight into how indirect and direct threats contribute to risk. This is a key insight for challenge 2 (Complexity of interdependencies and interactions).

Annex C §4, (Threat Assessment) makes use of an extensive catalogue of threats which includes natural and physical threats and as a threat catalogue, as recommended in ISO/IEC 27005 [5]. This catalog is a key insight for addressing Challenge 8 (Adversary Challenge Uncertainty), and Challenge 10 (Lack of common and comprehensive risk management process).

Table D-1 provides insight into the impact of safeguards on the risk variables, asset value, threat (and its sub components gravity and likelihood) and vulnerability. This table also shows how safeguards affect the probability of the threat event occurring, the probability of compromise and the severity of outcome. Table D-2 provides insight on how vulnerabilities and safeguard effectiveness affect the probability of compromise. These insights are applicable to all challenges and are key insights to challenge 10.

Appendix D-2 provides a list of vulnerabilities which could be an approach used to address challenge 7 (“Uncertainty in vulnerability”) whereby a list of vulnerabilities could be used where there is uncertainty regarding the actual vulnerability.

Table E.5 – Harmonized threat and risk assessment: Insights for ISO/IEC subclause 8.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.2		Key		X	X		Key	Key	X	Key	X

E.6 ISO/IEC 27005:2018, 8.3 Risk analysis

HTRA [8] describes risk analysis in the same section as risk identification.

Table D-4 provides a method for calculating a rating for each vulnerability that exposes an asset (from Very Low to Very High). This calculation is based upon the impact of a vulnerability on the probability of compromise and the severity of the outcome that were determined during risk assessment. This is the fundamental means by which HTRA establishes common metrics which allow for comparative analysis and is a key insight for challenge 10 (Lack of common and comprehensive risk management process). Annex E provides the method for calculating residual risk and developing a prioritized list of risks.

A key insight of table D-2 is that measures can work on the adversary (e.g., to reduce likelihood) or on consequence (to reduce gravity). This is a key insight where the threat is uncertain, such as challenge 8.

Table E.6 – Harmonized threat and risk assessment: Insights for ISO/IEC subclause 8.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.3	X	X	X	X	X	X	X	Key	X	Key	X

E.7 ISO/IEC 27005:2018, 8.4 Risk evaluation

HTRA [8] method provides a prioritized list of risks which is presented to the risk authority (risk management is external to this process). The list includes recommendations for risk treatment:

- Acceptance, where risk is acceptable
- Additional safeguards to reduce risk to an acceptable level, and
- Removal of safeguards, in rare cases where safeguards are excessive.

The method is applicable to all challenges, but does not offer key insight into any specific challenges.

Table E.7 – Harmonized threat and risk assessment: Insights for ISO/IEC subclause 8.4

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.4	X		X	X	X	X		X	X	X	X

E.8 ISO/IEC 27005:2018, 9.1 General description of risk treatment

Annex F §2.4.2 of the HTRA [8] provides a general description of risk treatment options ("*responsible managers may be presented with the following options:" (1) Retain Existing Safeguards, (2) Implement Proposed Safeguards, or (3) Remove Excessive Safeguards*").

HTRA does not provide any key insights for the above challenges.

Table E.8 – Harmonized threat and risk assessment: Insights for ISO/IEC subclause 9.1

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.1	X		X		X		X				

E.9 ISO/IEC 27005:2018, 9.2 Risk modification

HTRA [8] Annex F, §3, “Selection of potential safeguards” outlines a two-stage process in which security measures are identified to address all unacceptable residual risk followed by an assessment of the effectiveness of the safeguard selected. HTRA recommends that one (and preferably several options) are identified for each unacceptable risk. A table of safeguards is provided in F-2 and a checklist of selection criteria (with instructions) is provided in section 3.

The HTRA [8] guidance is applicable to all challenges, gut is a key insight to challenge 10 (“Lack of common and comprehensive risk management processes”) since it considers all unacceptable residual risk, regardless of cause.

Table E.9 – Harmonized threat and risk assessment: Insights for ISO/IEC subclause 9.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.2	X		X		X		X	X	X	Key	X

E.10 ISO/IEC 27005:2018, 9.3 Risk retention

HTRA [8] Annex F, §2.4.2 discusses risk retention and states that when risk is retained, existing safeguards can be retained, new safeguards required to achieve acceptable level of risk be implemented or in rare cases excessive safeguards can be removed. There is no key insight to any of the above challenges.

Table E.10 – Harmonized threat and risk assessment: Insights for ISO/IEC subclause 9.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.3	X				X		X			X	

E.11 ISO/IEC 27005:2018, 9.4 Risk avoidance

HTRA [8] Annex F §2.4.3 recommends that, if risk is excessive, options are to propose additional safeguards (i.e., risk modification), to revise the original requirements (which could include accepting an elevated residual risk), or cancelling the project (to avoid risk altogether). This is consistent with the advice of ISO/IEC 27005 [5] and there is no key insight to any of the above challenges.

Table E.11 – Harmonized threat and risk assessment: Insights for ISO/IEC subclause 9.4

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.4	X				X			X	X		

E.12 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance

HTRA [8] Annex F provides process for determining if assessed risk is acceptable and recommending corrective actions, if not. This depends upon the target risk level identified during TRA work planning, however the guidance on TRA work planning provided in Annex A, §6 states “a typical work plan should include … the target risk level that is deemed acceptable”.

HTRA [8] Provides no specific insights for the above challenges.

Table E.12 – Harmonized threat and risk assessment: Insights for ISO/IEC Clause 10

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
10	X	X	X	X	X	X	X	X		X	

E.13 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation

HTRA [8] provides the following insights:

- Annex A 2.3 provides general requirement for management to promote information sharing, and Annex A, §4.3 notes that the report length is "as long as necessary to convey the findings and recommendations to the risk acceptance authority".
- Annex A §5.5 identifies (internal and external) sources of specialized information
- Annex F-7 provides a HTRA sample report.

The HTRA [8] guidance does not go significantly beyond what is currently in ISO/IEC 27005 [5] and consequently provides no insight to addressing any of the challenges.

Table E.13 – Harmonized threat and risk assessment: Insights for ISO/IEC Clause 11

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
11	X	X	X	X	X	X	X	X	X	X	

E.14 ISO/IEC 27005:2018, 12 Security risk monitoring and review

For these approaches ISO/IEC 27005:2018, [5] Clause 12, HTRA [8] addresses 12.1 only which it maps to HTRA Section 7.2 (TRA Projects and Risk Management)

Most challenges identified the need for continuous management due to the dynamic nature of cyber risk variables (asset value, threat, or vulnerability). HTRA (Section 7.2, Page MS-8) recognizes that:

- A fundamental requirement is that continuous risk management is essential.
- Shows that managers monitor implementation of the TRA recommendations.
- Review and update the TRA when the risk variables evolve significantly.
- Formal TRA method simplifies the process since only the affected portions need to be updated and an entire reassessment is not needed.
- Shows how the TRA report (a static record) fits into a simplified management system.

The HTRA [8] guidance does not go significantly beyond what is currently in ISO/IEC 27005 [5] and consequently provides no insight to addressing any of the challenges.

Table E.14 – Harmonized threat and risk assessment: Insights for ISO/IEC Clause 12

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
12.	X		X	X	X		X	X	X	X	X

E.15 Reference document

Government of Canada, Communications Security Establishment/Royal Canadian Mounted Police, "Harmonized Threat and Risk Assessment Methodology," CSE, Ottawa, 2007 (see Reference documents, CSE 2007).

Annex F
(informative)

HAZCADS approach

NOTE This analysis was performed prior to the revision of HAZCADS [9] in 2021 (see Reference documents, EPRI 2021).

F.1 Summary of general approach

HAZCADS [9] combines the application of STPA (Systems Theoretic Process Analysis) [21] and FTA (Fault Tree Analysis) by integrating UCAs (Unsafe Control Actions) into a traditional fault tree, resulting in a Systems-Theoretic Fault Tree (SIFT). The application of STPA allows for identification of UCAs that could be initiated by a cyberattack. UCAs are associated with hazards and losses. Combination of STPA with FTA allows for existing reliability information to be considered, thereby enhancing risk assessment.

Risks can be qualitatively or quantitatively assessed with HAZCADS. The key element is how to incorporate UCAs into SIFT, which is central to evaluation of risk. The EPRI report (See Reference documents, EPRI 2018) consists of a methodology and two case examples to which HAZCADS was applied. See also Table F.1 through Table F.10.

Table F.1 – HAZCADS approach: Key challenges addressed

Challenge	Description
2	Complexity of Interdependencies and Interactions
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
6	Lack of Abstract Analysis Methods
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process

The guidance provided by the HAZCADS addressing the above challenges is seen as key insights to the overall risk management process.

Challenges indirectly addressed by HAZCADS are given below:

Table F.2 – HAZCADS approach: Challenges indirectly addressed

Challenge	Description
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty

These indirectly addressed challenges demands analysis and interpretation to derive insights and is therefore not seen as key for the establishment of a consensus risk management process for NPP cybersecurity.

F.2 ISO/IEC 27005:2018, 7.1 General considerations

HAZCADS [9] process is outlined in Figure F.1. The key insights are its combinatory approach to both STPA [21] and FTA. STPA provides for a model (abstraction) of the control structure (STPA step 2) to address Challenges 2 and 6, whereas FTA provides a structured manner to interpret system/components interactions and faults to address Challenges 4 and 9. The use of FTA in this manner is consistent with PRA approaches and may further alleviate Challenge 9 as PRA tools can be leveraged to assist with structuring, presentation, and analysis of tremendous amounts of information.

Specifically, use of FTA only mitigates Challenges 4, 9, and 10 when a traditional fault tree already exists. Otherwise, the information may not be available or exist to create a traditional fault tree, thereby requiring an extensive effort that may limit the use of HAZCADS.

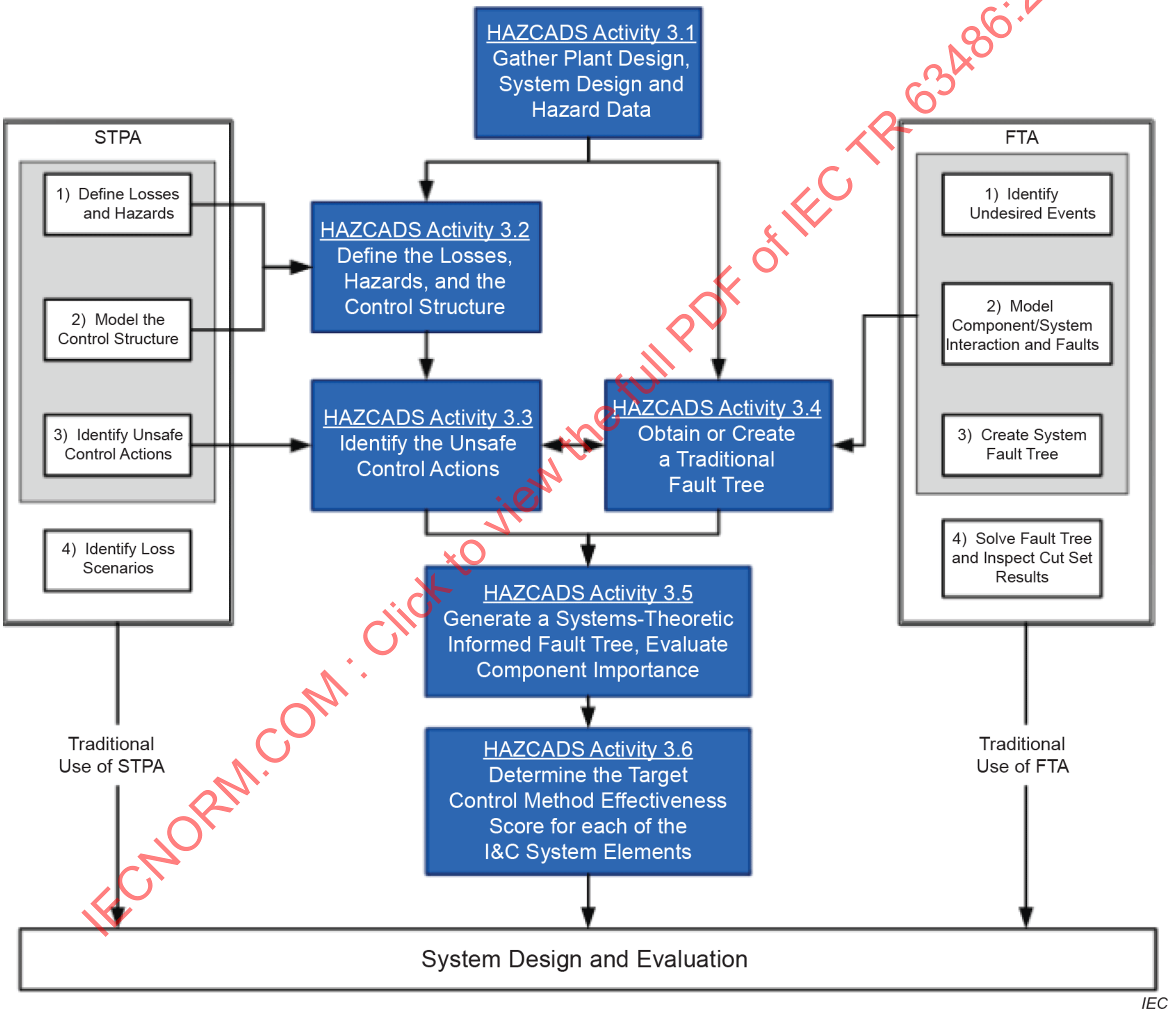

HAZCADS Activity 3.1
Gather Plant Design, System Design and Hazard Data
STPA
1) Define Losses and Hazards
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
HAZCADS Activity 3.2
Define the Losses, Hazards, and the Control Structure
HAZCADS Activity 3.3
Identify the Unsafe Control Actions
HAZCADS Activity 3.4
Obtain or Create a Traditional Fault Tree
FTA
1) Identify Undesired Events
2) Model Component/System Interaction and Faults
3) Create System Fault Tree
4) Solve Fault Tree and Inspect Cut Set Results
HAZCADS Activity 3.5
Generate a Systems-Theoretic Informed Fault Tree, Evaluate Component Importance
HAZCADS Activity 3.6
Determine the Target Control Method Effectiveness Score for each of the I&C System Elements
Traditional Use of STPA
Traditional Use of FTA
System Design and Evaluation
IEC

Figure F.1 – Overview of HAZCADS method (See Reference documents, EPRI 2018)

Table F.3 – HAZCADS approach: Insights for ISO/IEC subclause 7.1

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.1		Key		Key		Key				Key	

F.3 ISO/IEC 27005:2018, 7.2 Basic criteria

ISO/IEC 27005:2018 [5], 7.2 considers the following aspects of basic criteria:

- 7.2.1 Risk Management Approach
- 7.2.2 Risk Evaluation Criteria
- 7.2.3 Impact Criteria
- 7.2.4 Risk Acceptance Criteria

HAZCADS [9] is a system-level analysis approach that uses both FTA and STPA [21] to assess risk. The impact criteria are either in linking UCAs to hazards and losses (STPA approach) or in identifying a top event (i.e., unacceptable consequence) and determining a single or set of failures that lead to a failure of systems to perform their intended functions (FTA approach). The key insight for addressing cybersecurity (and challenges 2 and 6) is the identification of UCAs and their linking to Hazards and losses. Traditional fault trees are unlikely to consider failure modes and effects resulting from compromise (i.e., cyberattack) of a system or components.

HAZCADS [9] section 2.2.1 evaluated specific criteria for the application of the STPA method. STPA was evaluated to be highly effective for identifying new failure modes and new interactions and system effects, and moderately effective for interrelationships between digital and analogue system elements. However, STPA method has low value for risk prioritization.

HAZCADS [9] section 2.2.2 evaluated FTA method against the same criteria as the STPA method. FTA has high value for risk prioritization and can be easily used within existing hazard analysis.

Table F.4 – HAZCADS approach: Insights for ISO/IEC sublause 7.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.2		Key		X		Key				X	

F.4 ISO/IEC 27005:2018,7.3 Scope and boundaries

HAZCADS [9] is a system analysis approach that depends upon STPA [21] and FTA. Existing traditional fault trees are necessary to leverage this approach effectively, without incurring a significant effort to create. Section 3.1 provides a list of appropriate PRA and fault tree information that would be beneficial. These are:

- System fault trees from the plant's Probabilistic Risk Assessment (PRA) model, including spatial initiators such as fires and floods;
- System notebooks, written for the PRA;
- System operator training manuals;
- System Piping and Instrumentation Diagrams; and
- Plant operation procedures, manuals, processes and policies.

Digital Instrumentation and Control (DI&C) System documentation is a key HAZCADS inputs. The recommended list of information and appropriate documentation is:

- Design criteria, such as independence, separation, environmental (heat, electromagnetic and radio frequency interference, , etc.), human factors engineering, etc.
- DI&C architecture;
- DI&C network topology;
- Description of network segregation;
- Description of digital controller logic, along with process variable sensors providing information to digital controllers;
- Network component configurations;
- Network equipment (routers, switches, etc.);
- Facility power sources (both primary and backup);
- Computer and control system policies and procedures;
- Procedures and systems to govern computer user access;
- Operation plans or disaster recovery plans; and
- DI&C component (e.g., controllers) manuals and other technical details.

The above lists are for a single system or small set of system that perform/provide a key function. The STPA [21] analysis relies upon the DI&C documentation and relies upon the competence of the expert performing the analysis.

Table F.5 – HAZCADS approach: Insights for ISO/IEC subclause 7.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.3		X		X		X			X	X	

F.5 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment

HAZCADS [9] is an approach that supplements over risk assessment. HAZCADS does not define a risk assessment sequence or method.

F.6 ISO/IEC 27005:2018, 8.2 Risk identification

ISO/IEC 27005:2018, [5] 8.2 considers the following aspects of risk identification:

- 8.2.1 Introduction to risk identification
- 8.2.2 Identification of assets
- 8.2.3 Identification of Threats
- 8.2.4 Identification of Existing Controls
- 8.2.5 Identification of Vulnerabilities
- 8.2.6 Identification of Consequences

HAZCADS [9] leverages STPA to (1) define losses and hazards, (2) model the control structure, (3) identify UCAs, and (4) identify loss scenarios (HAZCADS Figure 3-2). Specifically, the losses that may be considered are:

(1) Severe human injury or loss of life

(2) Environmental contamination

(3) Equipment damage

(4) Significant loss of revenue

(5) Reputational damage

These consequences (while not complete) demonstrate that HAZCADS can be leveraged to apply a common and comprehensive risk management process for both severe and moderate consequences. Additionally, STPA abstracts the threats by using UCAs as the initiating event that results in the appearance of a hazard. HAZCADS considers four types of UCAs which are:

(1) Control Action Not Provided

(2) Control Action Provided

(3) Control Action Provided Too Early, Provided Too Late, or Provided in the Wrong Order

(4) Control Action Stopped Too Soon or Provided Too Long

The above UCA types are key insights for Challenge 6, but also assists with Challenges 7 and 8 (uncertainty in vulnerability and threat).

Table F.6 – HAZCADs approach: Insights for ISO/IEC subclause 8.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.2		X		X		Key	X	X	X	Key	

F.7 ISO/IEC 27005:2018, 8.3 Risk analysis

ISO/IEC 27005:2018 [5], 8.3 considers the following aspects of risk analysis:

- 8.3.1 Risk Analysis Methodologies
- 8.3.2 Assessment of consequences
- 8.3.3 Assessment of incident likelihood
- 8.3.4 Level of Risk Determination

HAZCADS [9] Section 3.5 and 3.6 outline an approach to solve the SIFT for prevention sets. Prevention sets represent the complete success paths based on prevention analysis. Prevention sets can be credited in prevention of the top event (or unacceptable consequence). HAZCADS provides key simplifying assumptions based on these prevention sets. UCAs are set to True if not contained within a selected prevention set (i.e., the UCA is not prevented by controls) or else set to false (i.e., contained in prevention set; UCA is prevented by controls). These assumptions within the SIFT are key insights for Challenges 2, 7, and 8. Challenge 2 is addressed by the STPA analysis to capture interdependencies and interactions, whereas the conservative assignment of true and false values accounts for Challenges 7 and 8 (uncertainties).

Table F.7 – HAZCADS approach: Insights for ISO/IEC subclause 8.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.3		Key		X		X	Key	Key	X	Key	

F.8 ISO/IEC 27005:2018, 8.4 Risk evaluation

HAZCADS [9] leverages Fussell-Vesely Interval and Birnbaum's measure to evaluate risk importance. Both Fussell-Vesely Interval and Birnbaum's measure are widely used in PRA. Fussell-Vesely measures the overall percent contribution of cut sets (failures) associated with an unacceptable consequence. Birnbaum measures the rate of change in total risk because of changes to the probability of an individual basic event. Based on these values, Figure 3-6 and Table 3-3 provide a Basic Control Method Effectiveness Score. This provides a key insight to how to leverage a common and comprehensive risk approach for the selection of controls.

Table F.8 – HAZCADS approach: Insights for ISO/IEC subclause 8.4

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.4		X		X		X	X	X	X	Key	

F.9 ISO/IEC 27005:2018, 9.1 General description of risk treatment

HAZCADS [9] does not discuss General Risk Treatment other than application of controls evaluated as per Clause F.8.

F.10 ISO/IEC 27005:2018, 9.2 Risk modification

In addition to 15.8 above, HAZCADS provides a Control Method Classes and CME Score Differentiation (Section 3.6.3 of EPRI, 2018, in Reference documents) that introduces three classes of control methods:

(1) Protect – control reduces or eliminates component failure or less significant

(2) Detect – detect degradation or failure of component

(3) Respond and Recover – prevent the occurrence of the failure or minimize the consequences of failure

While these are limited to safety considerations, the protect, detect, and respond and recover classes may provide key information for cybersecurity analysis if implemented. A standard set of control classes for risk modification could be a key insight for a common and comprehensive risk management process.

Table F.9 – HAZCADS approach: Insights for ISO/IEC subclause 9.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.2		X		X		X	X	X	X	Key	

F.11 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation

HAZCADS [9] integration of FTA and its conservative assumptions with respect to probability of UCAs are key insights that may progress use of PRA for cybersecurity analysis. Organizations that already rely upon PRA and have the associated documentation (e.g., PRA models) could leverage HAZCADS for a common and comprehensive risk approach that considers cyber while using their existing tools and technologies for analysis of the large amounts of information associated with PRA and cybersecurity analysis.

However, a significant effort will be needed to perform the STPA analysis and generate the SIFT.

Table F.10 – HAZCADS approach: Insights for ISO/IEC Clause 11

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
11		X		X		X	X	X	Key	Key	

F.12 Reference documents

Energy Power Research Institute, "EPRI TR 3002012755 HAZCADS – Hazards and Consequences Analysis for Digital Systems,," EPRI, Palo Alto, 2018

Energy Power Research Institute, “EPRI, Technical Report 3002016698 HAZCADS: Hazards and Consequences Analysis for Digital Systems – Revision 1,”, 2021

Annex G
(informative)

IAEA computer security risk management

G.1 Summary of general approach

The IAEA Nuclear Security Series (NSS) publications No. 17-T [6] and 33-T [7] both discuss risk management. IAEA NSS No. 17-T [6] has extensive guidance on facility and system risk management. In particular, the focus is on protection of facility functions, use of security levels to apply a graded approach, security zones for establishment of secure boundaries, and arrangement of these zones into a defensive cybersecurity architecture (DCSA) to implement defense in depth (DiD).

Specific challenges that are explicitly addressed by IAEA publications are given below. See also Table G.1 through Table G.15.

Table G.1 – IAEA approach: Key challenges addressed

Challenge	Description
2	Complexity of Interdependencies and Interactions
6	Lack of Abstract Analysis Methods
9	Excessive Information Volume
10	Lack of a Common and Comprehensive Risk Management Process

The guidance provided by the IAEA publications addressing the above challenges is seen as key insights to the overall risk management process.

Challenges indirectly addressed by the IAEA publications are given below.

Table G.2 – IAEA approach: Challenges indirectly addressed

Challenge	Description
4	Unknown or Lacking Sufficient Detail for Pre-developed Components
5	Differences in Cyber-risk Management
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty

These indirectly addressed challenges demands analysis and interpretation to derive insights and is therefore not seen as key for the establishment of a consensus risk management process for NPP cybersecurity.

G.2 ISO/IEC 27005:2018, 7.1 General considerations

The IAEA publication NSS 17-T [6] key insights pertain to challenge 2, 9 and 10.

NSS 17-T [6] para 4.26 identifies four types of interdependencies:

a) Information dependency,

b) Engineering and physical resource dependency,

c) Policy and procedural dependency, and

d) Proximity.

These four types need to be considered within the context of risk management to address Challenge 2.

NSS 17-T [6] para 3.20 describes a two-tier risk management approach that addresses Challenges 9 and 10. The two-tiers separate strategic risks (facility) and tactical risks (system) that reduce the amount of information that is necessary to identify, assess and treat risks. The facility has the overall scope of the NPP and relies upon abstraction (e.g., functions) that limit the depth of technical information needed to perform a strategic risk assessment. This assessment can be iterated (para 2.19) to balance efficiency and simplicity.

The IAEA publication NSS 17-T [6] has some insights pertain to challenge 7.

Para 4.16 provides elements to characterize all facility functions may be assessed in this manner and may include all consequences listed in ISO/IEC 27005:2018 [5] (IAEA para 4.16) to address Challenge 10.

The IAEA publications rely upon the DCSA (paras 4.67 to 4.83) to implement DiD and address uncertainty associated with Challenges 7.

The IAEA publications do not address Challenge 11.

Table G.3 –IAEA approach: Insights for ISO/IEC subclause 7.1

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.1		Key		X	X		X	X	Key	Key	

G.3 ISO/IEC 27005:2018, 7.2 Basic criteria

The IAEA publication NSS 17-T [6] key insights pertain to challenge 2, 9 and 10.

NSS 17-T [6] para 4.26 describes the four types of interdependencies and the impacts of their maloperation. These impacts can support both the risk evaluation criteria and the impact criteria, especially the level of classification of an SDA which has interdependencies with more sensitive functions through one or more of the specified interdependencies. This is key for addressing Challenge 2.

NSS 17-T [6] para 4.22 provides an ordered list of the effects of compromise on a facility function. This is key for setting the risk evaluation, impact, and acceptance criteria for risk management. The ordered list provides a common and comprehensive manner by which to assess risks from compromise of a facility function, thereby supporting a common and comprehensive risk management process (Challenge 10).

Para 4.16 provides a common manner by which to characterize facility function that reduces Challenge 9 as information is identified and listed in a common manner. While the IAEA publications prioritize those functions if compromised could lead to or support URC or theft of NM, the publications address all facility functions to illustrate the contributions of other functions to DiD against risks associated with compromise of computer-based systems. This extends the security levels (degrees) from 3 in IEC 62645 [1] to 5 in IAEA NSS 17-T [6].

The IAEA publications indirectly address Challenge 5 and 7.

Additionally, the IAEA NSS publications are international consensus publications and are key informative references to many national standards (CSA N290.7 [52], US NRC, IEC 62645 [1]), which may reduce national differences in risk management approaches (Challenge 5). The DiD strategy and DCSA concept indirectly address Challenge 7.

Table G.4 – IAEA approach: Insights for ISO/IEC subclause 7.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.2		Key		X	X		X	X	Key	Key	

G.4 ISO/IEC 27005:2018, 7.3 Scope and boundaries

The IAEA publication NSS 17-T [6] key insights pertain to Challenges 2 and 9.

The two-tiered approach of the IAEA assists with Challenges 2 and 9. The entire scope and boundaries of each tier are provided in paras 4.9 and 4.13 (facility) and 5.9 and 5.14 to 5.16 (system). This division helps to compartmentalize information and reduce the volume needed to perform an effective risk assessment, thereby minimizing Challenge 9.

The abstraction within the Facility CSRM simplifies the interdependencies and interactions analysis. This abstraction provides a common manner to document interdependencies and interactions to consider those that are permanent or temporary (paragraph 4.35). Additionally, significant attacks (associated with severe consequences) will likely demand the compromise of multiple facility functions or involve blended elements (para 4.36). The guidance provided particularly includes this to be in scope and may require iterative assessments for each facility function (para 4.37) to address Challenge 2.

The IAEA publication indirectly addresses Challenges 4, 7, and 10.

Paras A.39 to A.41 detail the external scope and interfaces for risk management but do not provide insights that are not already found within ISO/IEC 27005:2018 [5] to address Challenges 4,7 and 10.

Table G.5 – IAEA approach: Insights for ISO/IEC subclause 7.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.3		Key		X	X		X		Key	X	

G.5 ISO/IEC 27005:2018, 7.4 Organization for information security risk management

The IAEA publication NSS 17-T [6] key insights pertain to Challenge 9.

The IAEA publication details the records to be kept in paras 4.16, 4.33 to 4.38 (facility functions), 4.54 to 4.60 (CSP), 4.66, and 4.126 to 4.130. By specifying the outputs of FCSRM, superfluous information not necessary for risk management can be filtered out, thereby reducing Challenge 9. The outputs of the FCSRM are the Cybersecurity Programme and the DCSA specification.

The IAEA publication NSS 17-T [6] addressed stakeholders and their roles and responsibilities in paras A.39 and A.41 but did not provide additional information beyond what is found in ISO/IEC 27005:2018 [5].

Table G.6 – IAEA approach: Insights for ISO/IEC subclause 7.4

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.4		X		X	X		X		Key	X	

G.6 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment

The IAEA publication NSS 17-T [6] key insights pertain to Challenges 2, 6, and 10. The key insights are found in paras 3.12 to 3.20 of IAEA NSS 17-T [6]. Para 3.12(a) provides for the assessment and management of aggregated computer security risks to facility functions for the entire facility. The focus on “facility functions” provides an abstract analysis method that enhances the identification and assessment of risks (i.e., Challenge 6). Additionally, the assessment of functions provides for a common and comprehensive risk management process (i.e., Challenge 10) and simplifies the analysis of independencies and interactions (i.e., challenge 2).

Table G.7 – IAEA approach: Insights for ISO/IEC subclause 8.1

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.1		Key		X		Key	X			Key	

G.7 ISO/IEC 27005:2018, 8.2 Risk identification

ISO/IEC 27005:2018 [5], 8.2 considers the following aspects of risk identification:

- 8.2.1 Introduction to risk identification
- 8.2.2 Identification of assets
- 8.2.3 Identification of threats
- 8.2.4 Identification of existing controls
- 8.2.5 Identification of vulnerabilities
- 8.2.6 Identification of consequences

The IAEA guidance provides key insights into Challenges 2, 6, 7, 9, and 10. Identifying facility functions (IAEA NSS 17-T [6] paras 4.14 to 4.17) provides key insights into identifying functions that have value (i.e., significance) to the NPP. IAEA guidance treats "facility functions" as assets that have value to the organization. This guidance simplifies the strategic analysis. This abstraction provides a key insight to reduce the necessary information (i.e., Challenge 9) and provides a consistent manner in which functions and the consequences of their compromise are assessed (i.e., Challenge 10).

The IAEA guidance considers uncertainty in vulnerabilities (i.e., Challenge 7) by prioritizing DCSA. The DCSA acts to deny access to the adversary to one or more of the attack pathways. One or more attack pathways shall be accessed for the adversary to compromise a system function and achieve its goals. The DCSA layers and their associated measures may prevent or delay the advancement of attacks (para 4.80).

Table G.8 – IAEA approach: Insights for ISO/IEC subclause 8.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.2		Key		X	X	Key	Key	X	Key	Key	

G.8 ISO/IEC 27005:2018, 8.3 Risk analysis

ISO/IEC 27005:2018 [5], 8.3 considers the following aspects of risk analysis:

- 8.3.1 Risk analysis methodologies
- 8.3.2 Assessment of consequences
- 8.3.3 Assessment of incident likelihood
- 8.3.4 Level of risk determination

The IAEA publication NSS 17-T [6] key insights pertain to challenges 7 and 8. The two-tiered approach simplifies the assessment of consequences and provides for two types of scenarios. The top tier leverages the Design Basis Threat (DBT) or national threat statement to develop functional scenarios. Functional scenarios include sabotage resulting in unacceptable radiological consequences or unauthorized removal of nuclear material (para 4.120(a)). Technical Scenarios are those based on the specific implementation of measures and digital assets (para 4.120(b)). The Functional scenarios are used to evaluate the DCSA specification and analyze critical dependencies between functions and systems. Functional scenarios prioritize access to the adversary, whereas technical scenarios consider both access and tasks of the adversary. Further guidance is provided in paras 4.122 and 4.123 to bind and provide guidance on the scenarios.

A key insight for Challenge 6 is developing a hierarchical list of potential nuclear security events resulting from the compromise of facility functions (para 4.6 and footnote 21). An ordered list of functions provides a key insight for completing a level of risk determination.

Table G.9 – IAEA approach: Insights for ISO/IEC subclause 8.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.3		X	X	X		Key	Key	Key	X	X	

G.9 ISO/IEC 27005:2018, 8.4 Risk evaluation

The IAEA publication NSS 17-T [6] key insights pertain to Challenges 7 and 8. IAEA NSS 17-T [6] para 4.95 states,

> “The operator should justify all assumptions about the likelihood of attacks or their success (e.g., vulnerability, exposure, opportunity) used in the evaluation. The likelihood should be assumed to be 1 for postulated scenarios that can result in unacceptable radiological consequences or unauthorized removal of nuclear material (i.e., compromise of SDAs).”

The assumption that the likelihood of attacks and success is assumed to be “1” ensures conservative decision-making and demands risk modification or, in some cases, risk avoidance.

The aforementioned paragraphs 4.120 and 4.122 also ensure a rigorous and repeatable process is used to prioritize risks associated with incident scenarios.

Table G.10 – IAEA approach: Insights for ISO/IEC subclause 8.4

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.4			X	X		X	Key	Key	X	X	

G.10 ISO/IEC 27005:2018, 9.1 General description of risk treatment

The IAEA publications provide two types of unacceptable events:

a) sabotage resulting in unacceptable radiological consequences (URC), and

b) theft of nuclear material.

IAEA NSS 33-T [7] para 3.12 provides a hierarchical list of potential consequences of sabotage which are:

- Radiological consequence below the URC threshold: Targets posing these low consequences need a correspondingly low level of protection.
- URC can be graded into three categories ranked from the lowest to the highest consequences:
  - Consequence Level C: Sabotage that could result in doses to persons on-site that warrant urgent protective action to minimize on-site health effects.
  - Consequence Level B: Sabotage that could result in doses or contamination off-site that warrants urgent protective action to minimize off-site health effects (may also be considered high radiological consequences).
  - Consequence Level A: Sabotage that could result in severe deterministic health effects off-site (likely also high radiological consequences).

The consequences associated with the theft of nuclear material are based on the category of the material (IAEA NSS 13 Table I). The categorization of material is based on the quantity of material (in kg) and the enrichment. The hierarchical lists for both sabotage and material provide key international norms on which to consider risk treatment options.

Table G.11 – IAEA approach: Insights for ISO/IEC subclause 9.1

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.1			Key		Key		X				

G.11 ISO/IEC 27005:2018, 9.2 Risk modification

IAEA NSS 17-T [6] recommends specifying baseline measures that apply to the entire facility within the CSP (para 4.57) and DCSA (para 4.68). The CSP baseline measures consist of requirements that will be implemented in policies and translated into procedures. For example, these policies and procedures could address and modify the risk of future procurements of systems and services, thereby mitigating the potential impact of Challenge 4 (unknown or lacking sufficient detail for pre-developed components). Additional baseline measures would implement functional and performance testing (para 4.93) to address Challenges 4 and 7.

Additionally, the independence of the two tiers (Facility and System) ensures that the teams responsible for setting the requirements for the facility, those implementing the requirements, and those validating the requirements are not the same (para 3.16). This independence minimizes the potential that a single error or weakness invalidates the cybersecurity of the NPP.

Table G.12 – IAEA approach: Insights for ISO/IEC subclause 9.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.2				Key		X	Key	X	X	X	

G.12 ISO/IEC 27005:2018, 9.3 Risk retention

IAEA NSS 33-T [7] para 3.49 and IAEA NSS 17-T [6] para 6.26 indicate that risk retention is allowed for risks at or below an acceptable level. However, where administrative measures are used it recommends that they not be solely relied upon for an extended period to reduce risk to an acceptable level. This guidance implies that the adversary may, over time, acquire new capabilities or access (i.e., Challenge 8) or that the administrative measures may be implemented incorrectly (e.g., weakness or vulnerability to adversary capabilities) or are not adhered to by NPP staff. The efficacy of administrative measures is challenging to determine and thus contributes greatly to Challenge 7 (Uncertainty in Vulnerability / Susceptibility Analysis).

Table G.13 – IAEA approach: Insights for ISO/IEC subclause 9.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.3							Key	Key			

G.13 ISO/IEC 27005:2018, 9.4 Risk avoidance

The IAEA guidance does not discuss risk avoidance, and the publications address facilities where the associated consequences of sabotage and theft of nuclear material cannot be reasonably avoided.

G.14 ISO/IEC 27005:2018, 9.5 Risk sharing

The IAEA guidance does not discuss risk sharing via contracts, and the IAEA guidance is limited to specific policies and procedures for suppliers, service providers, and other contractors.

G.15 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance

IAEA guidance does not discuss a list of accepted risks with justification for those not meeting the organization’s normal risk acceptance criteria, except when safety conflicts with security (see Clause G.12).

G.16 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation

IAEA NSS 17-T [6] provides a list of key elements for the FCSRM outputs (para 4.59) and SCSRM outputs (para 5.56) that provides for a common and comprehensive risk management process at each of the two tiers. The FCSRM focuses on strategic risks to the NPP based upon the compromise of functions and the specification of requirements for the CSP and DCSA. The SCSRM focuses on tactical risks to the NPP based upon systems (i.e., systems), implementation of the DCSA, Security Zones, and measures. There is one FCSRM for many SCRSM reports, simplifying the acceptance or risks at the facility (strategic) or system (tactical) level. A common method of reporting risks, especially for systems and reconciling with the FCSRM, eases the Information security risk communication and consultation.

Table G.14 – IAEA approach: Insights for ISO/IEC Clause 11

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
11		X	X	X		Key	X	X	Key	Key	

G.17 ISO/IEC 27005:2018, Clause 12 Security risk monitoring and review

ISO/IEC 27005:2018, [5] Clause 12 considers the following aspects of risk identification:

- 12.1 Monitoring and review of risk factors
- 12.2 Risk Management monitoring, review, and improvement

IAEA NSS 17-T [6] provides examples of situations where the FCSRM and SCSRM outputs require review. These include instances where new or changed threats or vulnerabilities are identified (para 4.87(e)). Additionally, risk trends based on successive iterations of FCSRM and SCSRM need to be accounted for within security risk monitoring and review (para 4.89). Periodic review and update of scenarios are also recommended based on updates to the DBT, new credible attack routes, new critical vulnerabilities, and changes to the threat/adversary characterization (para 4.124). The lists provided by IAEA guidance are particularly beneficial in addressing Challenges 7 and 8 systematically and rigorously.

Table G.15 – IAEA approach: Insights for ISO/IEC Clause 12

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
12			X	X			Key	Key	X	X	

Annex H
(informative)

IEC 62443

H.1 Summary of general approach

IEC 62443 aims to secure Industrial Automated Control Systems (IACS). Key to IACS security is to reduce risks to assets. Within IEC, Assets are the focus of a security program. Assets can be physical, logical (informational), or human. “Process automation assets are a special form of logical assets. These processes are highly dependent upon the repetitive or continuous execution of precisely defined events” [14].

Risk management involves

a) assess initial risk;

b) implement risk mitigation countermeasures; and

c) assess residual risk.

Risk treatment is referred to as “risk response,” which includes:

d) Design the risk out ~ Risk avoidance (ISO/IEC 27005 [5])

e) Reduce the Risk ~ Risk Modification

f) Accept the Risk ~ Risk Acceptance/Retention

g) Transfer or Share the Risk ~ Risk Sharing

h) Eliminate or redesign redundant or ineffective controls ~ Risk Review and Risk Modification

Specific challenges that are explicitly addressed by IEC 62443 are given below. See also Table H.1 through Table H.15.

Table H.1 – IEC 62443: Key challenges addressed

Challenge	Description
2	Complexity of Interdependencies and Interactions
4	Unknown or lacking sufficient detail for pre-developed components
6	Lack of abstract analysis methods
7	Uncertainty in Vulnerability / Susceptibility Analysis
8	Adversary Characterization Uncertainty
9	Excessive Information Volume
10	Lack of a common and comprehensive risk management process

The guidance provided by the IAEA publications addressing the above challenges is seen as key insights into the overall risk management process.

Challenges indirectly addressed by the IAEA publications are given below.

Table H.2 – IEC 62443: Challenges indirectly addressed

Challenge	Description
1	Aggregate Risk of Multiple units/locations
3	Incident Likelihood Determination
5	Differences in cyber-risk approaches
11	Advanced security capabilities incompatibility

These indirectly addressed challenges demand analysis and interpretation to derive insights and are therefore not seen as key for establishing a consensus risk management process for NPP cybersecurity.

H.2 ISO/IEC 27005:2018, 7.1 General considerations

IEC 62443-2-1 [38] addresses cyber security risks for the entire organization by specifying requirements for establishing, implementing, maintaining, and continually improving an IACS security program (SP). These requirements provide security capabilities that aim to reduce IACS security risks to a tolerable level, and these requirements shall be implementation independent (i.e., abstract). The specification of implementation independent requirements that provide the organization capability to reduce risk to an acceptable level are key insights for Challenges 6 and 10.

The structure of the IEC 62443 series of standards is given in Figure H.1.

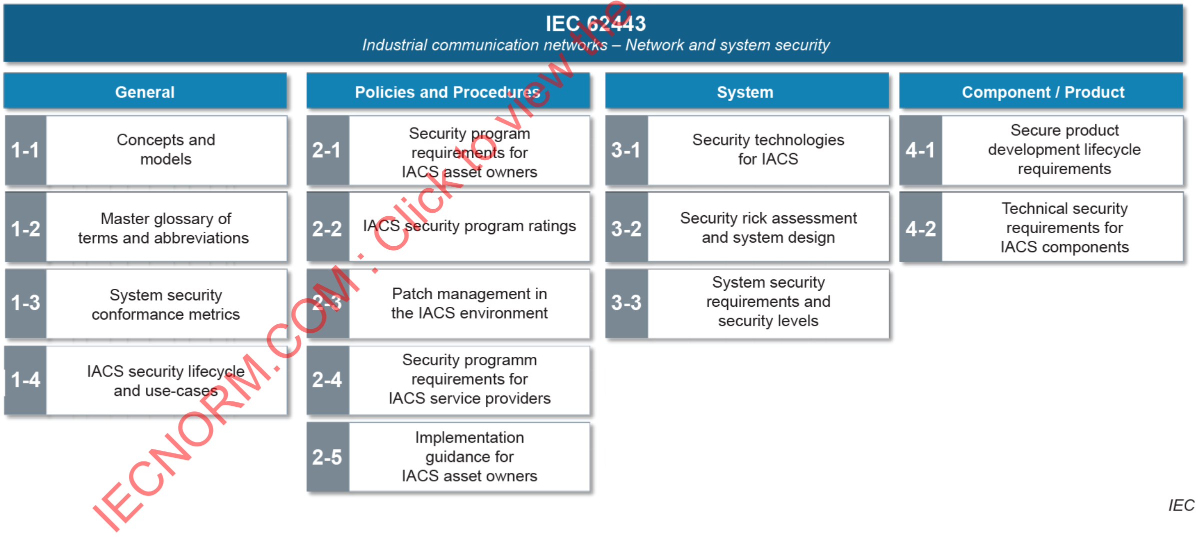

IEC 62443
Industrial communication networks – Network and system security
General
Policies and Procedures
System
Component / Product
1-1 Concepts and models
1-2 Master glossary of terms and abbreviations
1-3 System security conformance metrics
1-4 IACS security lifecycle and use-cases
2-1 Security program requirements for IACS asset owners
2-2 IACS security program ratings
2-3 Patch management in the IACS environment
2-4 Security programm requirements for IACS service providers
2-5 Implementation guidance for IACS asset owners
3-1 Security technologies for IACS
3-2 Security rick assessment and system design
3-3 System security requirements and security levels
4-1 Secure product development lifecycle requirements
4-2 Technical security requirements for IACS components
IEC

Figure H.1 – Parts of the IEC 62443 series [39]

This structure provides for Global fundamentals and definitions (Part 1), Organizational Management (e.g., ISMS, IACS SP; Part 2), System Level (Part 3), and Components (Part 4). This structure intrinsically assists with many of the Challenges identified in this document.

Table H.3 – IEC 62443: Insights for ISO/IEC subclause 7.1

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.1		X		Key		Key				Key	

H.3 ISO/IEC 27005:2018, 7.2 Basic criteria

The key insights are the tiered analysis for risks:

a) organizational level with independent implementation requirements to provide organizational security capabilities,

b) system level with a focus on zone and conduit requirements, and

c) component level focused on suppliers and secure development to reduce the likelihood of vulnerabilities and assurance of the security of the components.

This tiered approach allows for abstract analysis (organizational; IEC 62443-2 [38] [39]), architectural analysis (system IEC 62443-3 [40] [41]), and component analysis (IEC 62443-4 [36] [37]). The tiered approach minimizes the information that needs to be considered within each assessment, simplifying and structuring the evaluation of interdependencies and interactions. IEC 62443 contains the concepts of security levels (requirements) that provide organizational security capabilities and security zones (and conduits) that constitute a defensive architecture. These concepts seem in line with a common approach when compared to IAEA guidance.

Table H.4 – IEC 62443: Insights for ISO/IEC subclause 7.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.2		Key		Key		Key	X		Key	Key	

H.4 ISO/IEC 27005:2018, 7.3 Scope and boundaries

The IEC 62443 tiers of the organization, system, and components provide natural scope and boundaries for risk management. Specifically, the organization focuses on requirements to provide security capabilities aligned with NIST Cybersecurity functions or ISO/IEC 27001 [2] domains. The capabilities are challenging to quantify as they broadly apply to the entire organization’s automation solution (for a facility). However, once the scope and boundaries of a particular IACS are known, the risk can be further addressed via security zones and architecture and the imposition of the organizational cybersecurity programme requirements to the IACS. The specification of implementation-independent requirements is a key insight to simplify the analysis via abstraction.

Table H.5 – IEC 62443: Insights for ISO/IEC subclause 7.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.3		Key		X		Key					

H.5 ISO/IEC 27005:2018,7.4 Organization for information security risk management

IEC 62443 has similar text to IEC 62645 [1], IAEA Guidance, and other cyber-risk approaches. There are no key insights that go beyond those found in similar guidelines.

Table H.6 – IEC 62443: Insights for ISO/IEC subclause 7.4

ISOIEC Clause	1	2	3	4	5	6	7	8	9	10	11
7.4		X		X	X		X		X	X	

H.6 ISO/IEC 27005:2018, 8.1 General description of information security risk assessment

IEC 62443-3-2 [40] has several insights to address uncertainty. System risks are iterative with the risk treatment decisions varied. The initial risk assessment involves grouping of assets intention of grouping assets into zones and conduits to identify those assets which share common security requirements and to permit the identification of common security measures required to mitigate risk. This reduces the amount of information needed to analyze risks related to a specific asset (e.g., address risk in the aggregate).

Additionally, applying common measures to a group of assets is likely more efficient and better managed to provide for a greater degree of protection. Also, a prudent design would incorporate defense in depth to ensure that multiple, overlapping, layers of protection were provided to groups of assets associated with the most severe consequences.

The two-tiered risk analysis and implementation of controls allows for crediting common controls in the first tier, such as DCSA, to account for protections against adversary access to attack pathways. Therefore, a denial of access risk analysis is less affected by uncertainty in vulnerability analysis of a component.

The second tier of analysis prioritizes a denial of task, which imposes controls to mitigate, eliminate, or defend against adversary attempts to exploit a vulnerability, mal-operate a system, or compromise a component via an attack vector. Therefore, the denial of task analysis is more affected by the uncertainty in vulnerability analysis of a component.

Table H.7 – IEC 62443: Insights for ISO/IEC subclause 8.1

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.1		X		X		X	Key	Key	Key	X	

H.7 ISO/IEC 27005:2018, 8.2 Risk identification

ISO/IEC 27005:2018 [5], 8.2 considers the following aspects of risk identification:

- 8.2.1 Introduction to risk identification
- 8.2.2 Identification of assets
- 8.2.3 Identification of Threats
- 8.2.4 Identification of Existing Controls
- 8.2.5 Identification of Vulnerabilities
- 8.2.6 Identification of Consequences

IEC 62443-3-2:2020, [40] 4.4.2 mentions that special attention be paid to safety-related systems, wireless systems, systems connected to the internet, mobile devices, and assets connected to IACS managed by other entities. Safety-related systems protect against severe consequences, and the other elements have interfaces, interactions, or interdependencies with elements beyond the system evaluation. Nonetheless, the risks of these elements need to be considered, especially for architectural design.

Another key insight is a supplier reference architecture, which may account for uncertainty in component cybersecurity. The supplier reference architecture may precede the Purdue reference model defined in IEC 62264-2-1 [53].

Finally, IEC TS 62443-1-1 [14] provides a way to evaluate controls between traditional cyber/digital control measures and analogue (or non-cyber independent protection layers). The non-cyber-independent layers may be paired with safety-related systems to prevent, protect or mitigate severe consequences.

Table H.8 – IEC 62443: Insights for ISO/IEC subclause 8.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.2		Key		Key	X	X	X	X	X	X	

H.8 ISO/IEC 27005:2018, 8.3 Risk analysis

ISO/IEC 27005:2018, [5] 8.3 considers the following aspects of risk analysis:

- 8.3.1 Risk Analysis Methodologies
- 8.3.2 Assessment of consequences
- 8.3.3 Assessment of incident likelihood
- 8.3.4 Level of Risk Determination

Assessment of incident likelihood depends on an understanding of the threat. IEC 62443-3-2 [40] Annex A contains threat statements and links them to security levels (SLs). These are:

- SL 1: Protection against casual or coincidental violation
- SL 2: Protection against intentional violation using simple means with low resources, generic skills, and low motivation
- SL 3: Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation
- SL 4: Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, and high motivation

The SLs are graded based on the means, resources, skills, and motivation of the adversary (threat). This linking of protection requirements to threat statements simplifies the assessment of the incident likelihood and addresses the challenge of uncertainty in threat.

The risk analysis is performed at the organization, system, and component levels. The organization focuses on requirements that lead to security capabilities captured within the cybersecurity programme. The system level (IEC 62443-3-2 [40] performs two risk assessments, an initial one focused on architecture and a second detailed analysis that provides supplemental guidance and rationale for the IACS system requirements. The previous grouping of assets into zones aims to optimize the risk analysis, especially if the grouped assets share similar threats or are affected by the same threat events.

Specially, IEC 62443-3-2 [40] clause 4.6 (ZCR5) indicates that any detailed risk assessment methodology may be considered. ISO 31000 [51], NIST SP800-39 [54], and ISO/IEC 27005 [5] are all considered suitable for the detailed risk assessment methodology.

Table H.9 – IEC 62443: Insights for ISO/IEC subclause 8.3

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.3		X	X	X		X	X	Key	Key	X	

H.9 ISO/IEC 27005:2018, 8.4 Risk evaluation

Risk evaluation is performed at all levels (organization, system, component). IEC 62443-3-2 [40] Annex B provides some key tables that assist in prioritizing risks through a combination of event likelihood and consequences. Examples of consequence types are operational, financial (including reputation), health, safety, and environment. Several example consequences for each type are provided and equated. The consequences are then assigned a category of A, B, and C. This assignment allows for a common risk evaluation approach to consider diverse and differing consequences. Lookup tables and examples are extremely useful and apply to NPPs, especially for consequences that do not meet the threshold of unacceptable radiological sabotage.

Table H.10 – IEC 62443: Insights for ISO/IEC subclause 8.4

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
8.4			X	X	X	X			X	Key	

H.10 ISO/IEC 27005:2018, 9.1 General description of risk treatment

Risk treatment within IEC 62443 is performed at several tiers (organizational, system, and component). The security capabilities provided by the organizational cybersecurity programme do not allow for IACS risks to be directly treated but provide a holistic approach to cybersecurity protection (similar to nuclear security fundamentals). The system risk assessment is completed in two stages. The first stage treats risk by grouping assets, impositions of zones and easements for conduits, and the arrangement within an architecture. After this assessment, a detailed assessment is performed, and the focus is on measures at the zone boundaries, within the conduits and within the zones. In some cases, this detailed risk assessment may result in an asset or group of assets being evaluated with an unacceptable risk (IEC 62443-3-2:2020, [40] 4.6.13) and additional controls are imposed, or the zone is moved "deeper" within the architecture to take advantage of the protection of an additional zone.

The detailed risk assessment calculates the unmitigated risk (IEC 62443-3-2:2020, [40] 4.6.6) and assigns a target SL. The risk is once again evaluated and compared to acceptable risk. If this is still unacceptable, the zone/conduit is moved up to another SL (higher protection requirements).

Table H.11 – IEC 62443: Insights for ISO/IEC subclause 9.1

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.1		X					X	X	X		

H.11 ISO/IEC 27005:2018, 9.2 Risk modification

IEC 62443 relies mostly on the imposition of controls, especially at the IACS (System) level to reduce risk to a tolerable level.

Table H.12 – IEC 62443: Insights for ISO/IEC subclause 9.2

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.2		X		X		X	X	X	X	X	

H.12 ISO/IEC 27005:2018, 9.3 Risk retention

IEC 62443 only allows for risk retention when the risk is at or below tolerable levels.

H.13 ISO/IEC 27005:2018, 9.4 Risk avoidance

The IEC 62443 does not discuss risk avoidance as this discusses how to manage risks associated with the operation or an automation solution by an organization.

H.14 ISO/IEC 27005:2018, 9.5 Risk sharing

IEC 62443-4-2 [37] addresses the need for components to have capabilities to support cybersecurity. The standard provides a list and rationale for component requirements (CRs) that are derived from system requirements (SRs) in IEC 62443-3-3 [41]. CRs may also include a set of requirement enhancements (REs) which are additional subsets of component requirements to provide a capability similar to information and communication technology controls (e.g., NIST SP800-53 [55]). The combination of CRs and REs allows for the risk assessment to determine whether a supplied component can meet the requirements of a specific security level target (SL-T).

The imposition of CRs and REs in line with SRs would reduce the incompatibility challenge associated with advanced security technologies and IACS.

Table H.13 – IEC 62443: Insights for ISO/IEC subclause 9.5

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
9.5		X		X			X	X			Key

H.15 ISO/IEC 27005:2018, Clause 10 Information security risk acceptance

IEC guidance does not discuss a list of accepted risks with justification for those not meeting the organization's normal risk acceptance criteria.

H.16 ISO/IEC 27005:2018, Clause 11 Information security risk communication and consultation

IEC 62443 identifies that the asset owner management approves risk assessment results. IEC 62443 requires that those accountable for the safety, integrity, and reliability of the process controlled by the system under consideration review and approve the risk assessment results. IEC 62443 indicates that no other personnel have the authority to make decisions that accept risk.

Table H.14 – IEC 62443: Insights for ISO/IEC Clause 11

ISO/IEC Clause	1	2	3	4	5	6	7	8	9	10	11
11		X	X	X		X			X	X	