Assessment Guide

Guide for Assessing Cybersecurity Programs at Gamma Irradiation Facilities

January 2025

iia

About This Document

Cybersecurity has become an increasing priority for all businesses in recent years. It is reported that between 2021 and 2022, the exploitation of vulnerabilities increased by 55% with 147,342 attempts reported in 2021 and 228,345 reported in 2022 [1]. In their 2023 M-Trends report, Mandiant noted that "attackers are not giving up… we're seeing attackers cause bigger impacts with less skills. They're also more brazen and willing to get much more aggressive and personal to achieve their goals. They will bully and threaten and ignore the traditional rules of engagement" [2]. And finally, in the 2023 DBIR Report, Verizon's team found that of 3,966 incidents of system intrusion, 1,944 resulted in confirmed data disclosure [3].The impact of a cyberattack can result in financial loss, the inability to operate or provide a service, or the loss of assets such as data and facilities. Operators of gamma irradiation facilities additionally need to prevent cyber vulnerabilities from being introduced into a physical security system that protects their cobalt-60 sources.

Operators of gamma irradiation facilities should therefore implement and manage cyber and computer security programs to protect their radioactive sources. At the time of publication, there is a lack of international and national standards on cybersecurity programs specific for users of radioactive sources.

This document focuses on maintaining and sustaining existing cybersecurity programs through assessments that help to identify vulnerabilities and good practices and recommend improvements to arrangements where necessary. It provides practical guidance on assessment activities, approaches, and timetables, supported by checklists and templates. Further reading and other guidance, including that on the implementation of a cybersecurity program, is available and this is highlighted in the document.

This publication is the result of a collaboration with the US Department of Energy National Nuclear Security Administration's Office of Radiological Security and Sandia National Laboratories with the support of the International Irradiation Association (iia). The iia, through its Gamma Working Group and Sandia National Laboratories undertook a program of research to understand the needs of gamma irradiation facilities before publication of this document. The iia thanks those members of the Gamma Working Group that have contributed to this project. The iia also thanks and acknowledges the significant work undertaken by the experts of Sandia National Laboratories that has enabled and resulted in publication of this document. Particular thanks go to Jenna deCastro and Michael T. Rowland of Sandia National Laboratories, the lead authors of this publication, who worked with the support of Martin Comben of iia.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2024-14374O.

[1] Unit 42, "Network Threat Trends Research Report (Vol 2.)," Palo Alto Networks, Santa Clara, CA, USA, 2023.
[2] Mandiant, "M-Trends 2023 | Mandiant Special Report," Mandiant, Reston, VA, USA, 2023.
[3] "Verizon 2023 Data Breach Investigations Report," Verizon, 2023.

About the International Irradiation Association (iia)

The iia is a non-governmental organization (NGO) that represents the interests of the global irradiation industry and scientific community. A core aim of the iia is to promote the safe and beneficial use of gamma, electron-beam, and X-ray technologies. The irradiation community includes operators of gamma irradiation facilities that process products and material for many beneficial applications. Gamma irradiation facilities are industrial scale irradiation or radiation processing facilities that utilize cobalt-60 sealed sources. Membership of iia is diverse and includes corporations, research institutes, universities, and governmental bodies around the world.

To learn more about the iia, please visit https://iiaglobal.com/

Table of Contents

List of Figures

List of Tables

Acronyms and Definitions

Abbreviation	Definition
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
iia	International Irradiation Association
ISO	International Standards Organization
IT	Information Technology
NGO	Non-Governmental Organization
NPP	Nuclear Power Plant
NSS	Nuclear Security Series
ORM	Other Radioactive Material
ORS	Office of Radiological Security
OT	Operational Technology
SME	Subject Matter Expert
CDA	Critical Digital Asset

Introduction

Computer security is becoming an increasingly pressing concern worldwide. Despite its growing importance, many companies lack confidence in their staff's ability to maintain robust computer security. Currently, it is estimated that there is a shortage of over 3 million computer security professionals, and in the near future, significant computer security incidents are likely to result from a lack of skilled personnel or general human error [4].

These concerns underscore the critical need for efficient computer security programs. However, there is no single guide that comprehensively addresses these issues. The general assumption is that nuclear facilities have dedicated staff and established computer security programs and regulations. In contrast, other radioactive material (ORM) facilities, such as gamma irradiation facilities that utilize cobalt-60 sources, often do not have this luxury. Therefore, it is vital to implement and maintain a computer security program that provides necessary protection while using resources effectively.

One central aspect of effective computer security programs is the requirement for periodic assessments to ensure that requirements are being appropriately implemented, managed, and sustained. The International Atomic Energy Agency (IAEA) Nuclear Security Series (NSS) No. 20, Nuclear Security Fundamentals, which emphasizes the importance of "routinely performing assurance activities to identify and address issues and factors that may affect the capacity to provide adequate nuclear security, including cyber security, at all times"[5].

Computer security assessments aim to identify potential vulnerabilities and weaknesses in computer security posture, activities, and measures. They recommend improvements or mitigation strategies, identify best practices, and provide considerations for applying a graded approach and implementing defense-in-depth. Despite their criticality, planning and conducting assessments face challenges, particularly due to a lack of international and national standards and guidance applicable. These challenges specifically apply to the assessment of computer security arrangements at gamma irradiation facilities.

This is especially important as cyberattacks are an increasing concern, yet many facilities lack dedicated computer security personnel. Conducting computer security assessments is a key assurance activity to provide evidence that the ongoing effectiveness of a computer security program is sustained.

A key assumption of this document is that there is already an existing computer security program to assess. If there is no existing program, please refer to the table provided in Appendix B, which is sourced from the Office of Radiological Security document titled "Best Practices for Users of Radioactive Sources" [6].

[4] NIST, "Cybersecurity Workforce Demand," NIST, 2023.
[5] International Atomic Energy Agency, "IAEA NSS No. 20 – Nuclear Security Fundamentals: Objective and Essential Elements of a State's Nuclear Security Regime," IAEA, Vienna, 2013.
[6] ORS, "Cybersecurity Best Practices for Users of Radioactive Sources," ORS, 2022.

Framework

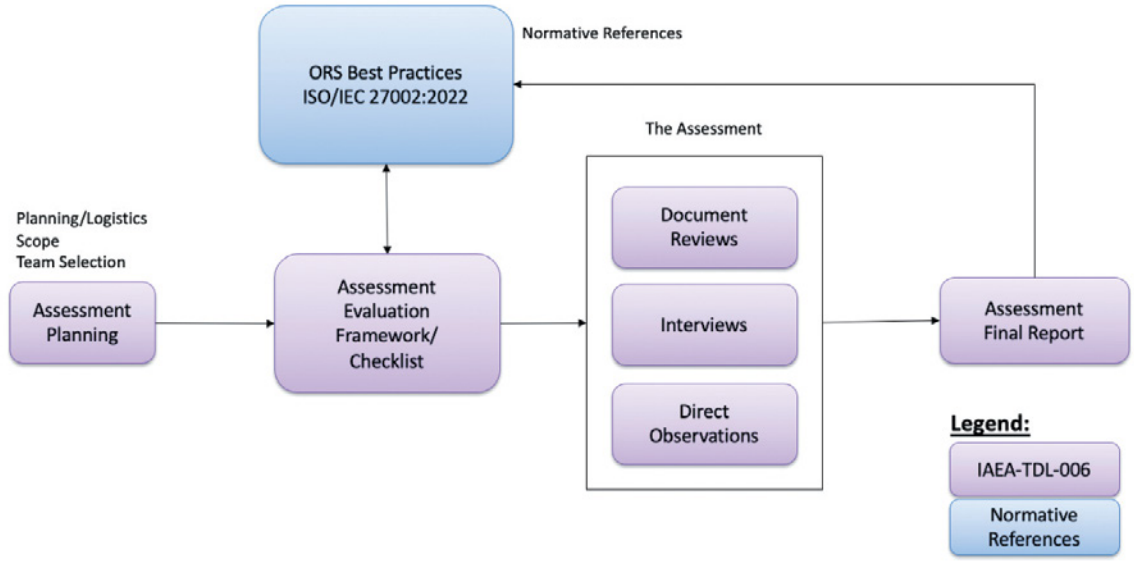
The process begins with a formal request to perform the assessment that can originate from internal stakeholders or from external entities such as regulators. Once this request is received, the planning phase commences. This phase involves defining the scope of the assessment, selecting, and approving an assessment team, and organizing the logistics. These steps are essential for developing an assessment framework that is methodical and repeatable to consistently collect relevant information.

Guidance on interview subjects, questions, areas for direct observations can be found in subsequent sections of this document as well as in IAEA guidance, national standards, regulatory guides, best practices, and lessons learned from previous assessments. These sources can further inform both the assessment process and the creation of a cybersecurity program, though not all may be necessary. Information gathered from this report and the basis documents overviewed in the following sections helps delineate the assessment boundaries, identify interviewees, formulate interview questions, and determine areas for walkdowns/observations.

2.1 Relevant, Important Publications

These documents collectively offer a methodology for conducting assessments in addition to a rough framework for creating a cybersecurity program if one is needed. These documents are suitable for low-resource settings while still being applicable to gamma irradiation facilities. Alone, each document holds individual significance, but when integrated, they provide a practical, scalable, and effective approach for conducting assessments and ensuring the effectiveness and sustainability of cybersecurity programs. The proposed assessment framework and workflow is depicted in Figure 2-1 below and represents the melding of IAEA Conducting Computer Security Assessments at Nuclear Facilities (TDL-006), ISO/IEC Information Security, Cybersecurity and Privacy Protection (ISO/IEC 27002:2022), and ORS Cybersecurity Best Practices for Users of Radioactive Sources (ORS Best Practices). For more information of each of these publications, refer to Appendix A.

Figure 2-1: Assessment Framework and Flow



2.2 Assessment Activities

Depending on the scope of the assessment, assessment activities can include document and records reviews, direct observations, and interviews with relevant personnel.

An example template from IAEA TDL-006 has been modified and provided in Appendix G and can be used to record information observed during these activities.

2.2.1 Documents and Records Review

Reviewing documents and records involves analyzing a range of materials, from national-level guidance to internal documentation of the facility being assessed. Examples of documents that can be requested for analysis include national legislation and regulations, regulatory guides, national strategies (if applicable), international standards, national and international best practices, and internal documents such as the computer security program, plans, policies, procedures, network architecture or design, and technical guidance.

The documents reviewed during this stage form the foundation of the entire assessment. They are critical for identifying the facility's strengths, weaknesses, and opportunities for improving its computer security posture. Reviewing documents is essential for detecting non-compliance, discrepancies, gaps, deviations, and best practices. It can also uncover historical trends and patterns within the organization. By thoroughly examining past documentation, assessors can identify recurring issues, highlight areas needing improvement, and evaluate the effectiveness of previous corrective measures [7].

2.2.2 Direct Observations

Direct observations, also known as walkdowns, are a crucial component of the assessment process. They involve physically evaluating processes, systems, and personnel behavior within an organization to validate and enhance information gathered during document reviews or interviews. This approach provides a unique, real-time perspective, uncovering potential gaps that may otherwise be overlooked.

To conduct effective direct observations, assessors should immerse themselves in the operational environment within the agreed scope of the assessment. This allows them to witness the real-time implementation of procedures, assess the condition of equipment, and evaluate adherence to internal protocols. Direct observations are valuable for identifying discrepancies or deviations that may not be evident through document reviews or interviews alone.

By engaging in direct observations, assessors can gain a comprehensive understanding of the security culture and employee behaviors. They can assess the commitment to security, the level of compliance with established procedures, and the overall awareness of personnel regarding their roles and responsibilities.

Additionally, direct observations help build trust between assessors and the personnel being evaluated. By interacting with employees on-site, assessors can address uncertainties, clarify outstanding concerns, and communicate the purpose and benefits of the evaluation process. This interaction fosters a collaborative atmosphere and enhances the effectiveness of the evaluation. For an example observational template, see Appendix G for a template that has been modified from TDL-006.

[7] IAEA, "TDL-006 – Conducting Computer Security Assessments at Nuclear Facilities," International Atomic Energy Agency, 2016.

2.2.3 Interviews

Interviews are a valuable tool for gathering information during the evaluation process. To maximize their effectiveness, follow these steps:

1. **Preselect Interviewees:** Carefully consider all employees at every level of the organization from irradiator operators to maintenance staff, warehouse personnel, shipping and receiving, quality assurance, physical protection, and IT support staff to executive level staff. Understanding the responsibilities of each position will enable assessors to craft specific questions for each role.
2. **Plan Questions in Advance:** Carefully prepare questions that will elicit detailed and relevant information.
3. **Create an Open Atmosphere:** Foster a conducive and collaborative environment where interviewees feel comfortable sharing information.
4. **Use Active Listening Skills:** Engage in active listening to fully understand the responses and gather nuanced insights.

Conducting interviews provides the assessment team with several key benefits:

- **Gather Additional Information:** Use open dialogue to obtain more detailed information.
- **Verify Understanding and Adherence:** Confirm that personnel understand and follow the facility's written procedures.
- **Assess Knowledge and Training:** Evaluate the knowledge and training levels of personnel within the facility.
- **Validate Observations:** Use interviews to validate or challenge observations made during direct observations.
- **Ensure Policy Compliance:** Verify that policies and procedures are both understood and followed by personnel.

By following these steps, interviews can become an invaluable source of information, significantly enhancing the overall assessment.

2.3 Scoping the Assessment

Given that gamma irradiation facilities lack the same level of support as nuclear facilities, relying on a single reference to plan, scope, and conduct an assessment is impractical. The best approach is to integrate the revised version of TDL-006, ORS Best Practices, and ISO/IEC 27002:2022. This combined methodology creates a holistic and "right-sized" approach for gamma irradiation facilities.

The proposed assessment framework can be depicted as a checklist, as shown in Figure 2-2 on page 11. This checklist cross-references the security domains detailed in ISO/IEC 27002:2022, TDL-006 assessment activities, and ORS Best Practices functional domains.

Figure 2-2: Assessment Scope Checklist

Functional Domains	Security Domains	Document and Records Review	Interviews	Direct Observation (Vulnerability Assessment)
Operational	Organizational			
	People			
	Physical			
	Technological			
Physical Protection	Organizational			
	People			
	Physical			
	Technological			

2.4 Types of Assessments

2.4.1 Audits

Audits may be conducted by independent third parties to verify compliance or, for example, by customers of a commercial gamma irradiation facilities in order to assess whether their requirements have been met. An example of an audit is when the customer user of a gamma irradiation facility, such as a healthcare product manufacturer, audits to verify that the facility complies with its quality, processing, and other operational requirements. This may be part of a supplier approval process and may include requirements on computer security arrangements.

2.4.2 Regulatory Inspections

This form of assessment is typically conducted by a competent authority and may be either announced and pre-planned or unannounced. Regulatory inspections are commonly used within IAEA NSS No. 13 [8].

2.4.3 Self-Assessments

Self-assessments may be conducted by an internal team from the organization or be a third-party hired by the facility. The underlying goal of conducting a self-assessment is to proactively uncover areas for improvement while also monitoring and reviewing computer security programs. Additionally, self-assessments can be conducted as a preparation activity for either an audit or regulatory inspection.

[8] IAEA, "NSS No. 13 – Nucleaer Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)," IAEA, Vienna, 2011.

Assessment Guidance

This section is intended to provide a structured approach to both assess and enhance a cybersecurity program that draws on ORS's Best Practices guide. It is organized in a manner that addresses facilities ranging from those which have yet to develop a cybersecurity program to those who already have fully operational and well-developed programs.

3.1 Lifetime Phases of a Cybersecurity Program

There are three general phases within the lifetime of a cybersecurity program as defined by the ORS Best Practices: (1) starting, or developing, a cybersecurity program, (2) implementing a cybersecurity program through appropriate controls, and (3) sustaining a cybersecurity program.

3.1.1 Starting (ORS Best Practices – Starting a Cybersecurity Program)

Facilities in this stage are likely to not have any formally defined cybersecurity policies, procedures, dedicated personnel, or focused training programs. At this stage, organizations should work on identifying which regulations, recommendations, and best practices should be used as the basis documents for their cybersecurity program.

Developing a new cybersecurity program should also include defining operational procedures that clearly delineates the roles and responsibilities of all participants in the cybersecurity program; drafting and implementing procedures to execute the policy actions; and identifying critical digital assets (CDA). Clearly defining the criteria for cybersecurity incidents and the corresponding response requirements is crucial. Additionally, it is vital that senior management fully endorses the establishment of a cybersecurity program.

Table 3-1: Suggested Tasks for Starting a Cybersecurity Program

Task	Comments
Review national and international requirements, recommendations, and best practices	Understanding mandatory requirements must first be understood to form the framework of a cybersecurity program Reviewing industry best practices can reveal what other facilities have done successfully and lessons learned. This may simplify implementing a new program
Establish cybersecurity policy, including roles and responsibilities	Roles and responsibilities need to include the relationship between organizations National and international regulations/recommendations can form the foundation for a facility's cybersecurity program
Designate responsible personnel	The facility must designate the team in accordance with the established roles and responsibilities Responsible personnel may be third-party contractors
Identify CDAs	An understanding of these assets, their configuration, architecture, and data flow is essential to select appropriate controls
Conduct risk analysis	The operator is responsible for the identification of risk and prioritizing which security controls to implement
Identify the capabilities needed and any gaps in the cybersecurity program	Facilities should review the above elements to conduct a gap analysis Consultation with SMEs can be useful

For a checklist that can be used to begin developing a cybersecurity program, see Appendix B.

3.1.2 Implementing and Sustaining a Cybersecurity Program

Understanding that cybersecurity is a constantly evolving landscape, no cybersecurity program can remain the same as the day it was implemented. Sustaining a program is a key element within the ORS Best Practices. The table below provides an example list of tasks and associated comments that can aid with the sustainment of a cybersecurity program.

Table 3-2: Suggested Tasks for Implementing and Sustaining a Cybersecurity Program

Task	Comments
Report computer security incidents or suspicious activities	The facility may designate specific reporting requirements for computer events This may detail the specific events that the operator is responsible for reporting
Ensure adequate data monitoring	Facilities are responsible for ensuring adequate data monitoring for compliance audits
Construct an adequate test and evaluation environment (optional)	Facilities should develop a testing environment, if possible, to test new cybersecurity tools and protocols prior to deployment in the operational environment
Collect and preserve information	Facilities should collect and store records and other information commensurate with the security level of the data
Analyse the cyber-threat and update the threat assessment	Facilities should conduct routine threat assessments and update their policies and procedures as appropriate
Conduct attack surface analysis (optional)	Facilities should conduct an attack surface analysis to find vulnerabilities
Develop a mitigation strategy	Facilities should develop a mitigation strategy for cyber incidents. Information regarding mitigation strategies may be sourced from national and international documents
Monitor program changes	Facilities should monitor any implemented mitigations or other changes to the cybersecurity program to ensure effectiveness
Develop lessons learned (optional)	Facilities may consider developing a lessons learned document to support future stakeholder decisions after cyber events
Assess resource allocation	Facilities may conduct an assessment to determine the resources required to maintain and address the cybersecurity program and potential security incidents
Share lessons learned with the wider community	

For a checklist that can be used to maintain a cybersecurity program, see Appendix C and for sustaining a program, see Appendix D.

3.2 Developing Cybersecurity Program Assessments

Assessments of cybersecurity programs in their infancy will primarily focus on document reviews with the possibility of some direct observations to improve initial establishment of policies and processes as well as improve eventual implementation of controls when considering organizational resources to implement and then sustain a program.

Tables 3-3 through 3-5 in the following sections have the same format and are designed to inform an assessment of a cybersecurity program at the different stages within the program's lifecycle.

- **Task:** assessment task and roughly when it should be completed, either before the assessment, or during the onsite portion.
- **Description:** Includes hints on policies to look for and review during the assessment
- **Related ORS Best Practices:** The best practices listed here are an example of some of the best practices that may be significantly important to a facility. The best practices listed in each table are by no means exhaustive. For a full list of all ORS best practices, see Appendix B through Appendix D. These best practices may also serve as guides for facilities looking to develop a new program and need a few best practices to focus on as a part of the first steps.
- **References to ISO/IEC 27002:2022:** This section is by no means exhaustive; example clauses are provided simply as an aid. However, additional clauses are likely to be applicable.

Table 3-3 provides an example of areas in which an assessor may be interested in reviewing for facilities which have just recently implemented a cybersecurity program. Assessments at this phase should primarily focus on document reviews to improve upon the initial establishment of policies, processes, and procedures surrounding a cybersecurity program. The assessment scope at this level of maturity should be a complete document review to ensure there are no gaps in the initial program framework. Because this assessment is reviewing a new program, there are no existing records to review nor direct observations to be made. However, there may responsible personnel to interview and whether those interviews are conducted should be determined during the scoping phase when planning the assessment.

Table 3-3: Assessment of New Programs

When	Assessment Details		Related, Significant ORS Best Practices associated with Task	Example Reference Sections from ISO/IEC 27002:2022
	Task	Description		
Prior	Policy Review Identify potential gaps in Policies	Policies to look for can include: • Information Security • Privacy • Acceptable Use • Identify critical assets • Managing critical assets • Roles/Responsibilities • Training Policies • National/ International regulations and recommendations	A.1 Identify single person responsible for CS A.2 Policies stress importance of CS A.3. Policies require CS documentation and CS A.4 Policies require use of CS zones A.7 Policies require firewall(s) A.8 Conduct best practices evaluation for CS	For example, policy considerations for a cybersecurity program, see Clause 5.2
	Procedure Review	Identify potential gaps in written procedures Key procedures to look for can include: • Identifying CDAs • Managing CDAs • Using vulnerability scanners • Operation of Network Intrusion Detection System (NIDS).	A.5 Implement network access controls A.9 Procedures detail attack surface evaluation steps A.12 Procedures detail use of vulnerability assessment tools	For example, considerations to establish procedures on access control, both logical and physical, see Clause 5.15
	Records Review	Review records of previous incidents, if any. Records may contain information on IT/OT or PPS component failures, and implemented	A.2 Evaluate overall cybersecurity awareness and acceptance	For example, clauses on how to protect records, see Clause 5.33
During (On-site)	Interview(s)	Interview personnel to determine security culture and extent of organization wide acceptance of cybersecurity practices.	A.1 Interview responsible personnel A.7 Ask questions about cybersecurity policies such as firewalls	For example, considerations on interview topics regarding information security and the organization's approach to meeting those requirements, see Clause 5.31
	Direct Observation(s)	Conduct a walkdown of network architecture and devices.	A.3 Review map of system dependencies A.5 Determine if network access controls are implemented A.11 Observe network terminals, workstations, firewall security zones etc.	For example, considerations regarding information transfer rules, see Clause 5.14

3.3 Cybersecurity Program Assessments for Established Cybersecurity Programs

Organizations with a defined cybersecurity program are more likely to have established and disseminated cybersecurity program policies and procedures. They are also more likely to have dedicated cybersecurity personnel, either an internal team or a third-party contractor, and may conduct regular risk assessments as part of their vulnerability management processes.

At this level of maturity, it is possible that while the program is established and implemented, it has not yet been assessed. For organizations with a relatively mature program, the assessment scope should include the elements discussed in Section 4.1 in addition to doing a record review, interviews, and direct observations. Table 3-4 below provides an example of areas in which an assessor may be interested in reviewing for facilities which have established a new program but have yet to assess it.

Table 3-4: Assessment Guidance Established/Defined Programs

When	Assessment Details		Related, Significant ORS Best Practices associated with Task	Example Reference Sections from ISO/IEC 27002:2022
	Task & Objective	Description		
Prior	Policy Review: Identify potential gaps in written policies	Key policies to look for can include: • Information Security • Privacy • Acceptable Use • Identifying CDAs • Managing CDAs • Roles/Responsibilities • Training Policies • National/ International regulations and recommendations	See Table 3-3 and review the following additional best practices: B.1 Strict user access is enforced B.7 Develop an acceptable use policy for cyber resources B.9 Ensure software is sourced from a reputable vendor B.11 Purchase equipment through a vetted supply chain B.12 Ensure only admins can modify systems B.32 Sanitization of end-of-life hardware	For example, guidelines regarding managing supply chain relationships and developing supply chain policies, see Clause 5.19
	Procedure Review: Identify potential gaps in written procedures	Key procedures to look for can include: • Identifying CDA • Managing CDAs • Using vulnerability scanners • Operation of Network Intrusion Detection System (NIDS).	See Table 3-3 and review the following additional best practices: B.1 Procedure for access controls B.2 Remove unnecessary user accounts B.10 Keep components updated with current firmware versions B.14 Develop procedure for physically hardening equipment B.18 Develop backup and recovery procedure B.24 Create and maintain access control lists for admins B.29 Deploy network intrusion detection	For example, considerations on defining, establishing and communicating cybersecurity incident management processes/ procedures, roles, and responsibilities, see Clause 5.24
	Records Review: Identify if records are properly maintained and stored	Key elements to look for can include: • Are records maintained in a secure manner. • Are incidents and incident response(s) recorded.	See Table 3-3 and review the following additional best practices: A.12 Conduct vulnerability assessments as appropriate A.13 Conduct penetration testing as appropriate	For example, considerations on how to assess and potentially respond to security events, see Clause 5.25
During (On-site)	Interview(s)	Interview relevant personnel	See Table 3-3 and review the following additional best practice: B.19 Does the organization have a security awareness program?	For example, considerations on interview topics regarding security awareness, see Clause 5.27
	Direct Observation(s) • Review vulnerability scans • Review controls	Conduct walkdowns of the facility that are within the scope of the assessment	See Table 3-3 and review the following additional best practices: B.14 Physically hardened equipment B.25 Are critical systems air gapped where possible? B.30 Use of multifactor authentication	For considerations regarding security engineering principles and hardening systems, see Clause 8.27

3.4 Sustained Cybersecurity Program Assessments

A mature and well-integrated cybersecurity program is characterized by its proactive approach to threat intelligence and the implementation of advanced security measures. Such a program is not static; it continuously evolves, adapting to emerging threats and incorporating improvements to stay ahead of potential risks. Sustainment is key, ensuring that these measures are consistently maintained and updated to provide ongoing protection.

At this level of maturity, it is likely that the cybersecurity program is well-established and implemented and has likely undergone at least one assessment. The assessment scope for such facilities should be well defined as assessing facilities that are actively sustaining their cybersecurity program can be an arduous process (See Section 4.1 and 4.3). Table 3-5 below provides an example of areas in which an assessor may be interested in reviewing for facilities which are sustaining their program. For these assessments, focus should revolve around the organization's security culture.

Table 3-5: Assessment Guidance for Sustained Programs

When	Assessment Details		Related, Significant ORS Best Practices associated with Task	Example Reference Sections from ISO/IEC 27002:2022
	Task	Description		
Prior	Policy Review Key policies to look for can include: • Information Security • Privacy • Acceptable Use • Identifying CDAs • Managing CDAs • Roles/ Responsibilities • Training Policies • National/ International regulations and recommendations	Identify potential gaps in written policies	See Table 3-3 and 3-4 and review the following additional best practices: C.1 Implement configuration change management policy C.2 Review and update CS program requirements and update policies accordingly.	For example, considerations regarding change management, see Clause 8.32
	Procedure Review Key procedures to look for can include: • Identifying CDAs • Managing CDAs • Using vulnerability scanners • Operation of Network Intrusion Detection System (NIDS).	Identify potential gaps in written procedures	See Table 3-3 and 3-4 and review the following additional best practices: C.1 Develop change management procedure C.2 Review and update CS program requirements and update policies accordingly. C.4 Update security plans after changes are made to the environment. C.7 Implement procedures for upgrading systems (software or hardware)	For example, considerations regarding procedures on recording events, preventing unauthorized access, and NIDS, see Clause 8.15
	Records Review Key elements to look for can include: • Are records maintained in a secure manner • Review previous assessment reports	Identify if records are properly maintained and stored	See Table 3-3 and 3-4 and review the following additional best practices: C.2 Continually evaluate and address gaps and vulnerabilities Are previous assessments used to inform these assessments? C.13 Are there records of tests conducted against the backup and recovery plan?	For example, considerations regarding how to identify technical vulnerabilities through the use of vulnerability assessments, see Clause 8.8

During (On-site)	Interview(s) • Can personnel answer questions confidently and accurately? • Are personnel trained in their roles and responsibilities? • Is there a general understanding of cyber hygiene? • Does upper management support overall security culture? • Are employees aware of national/ international regulations they must adhere to?	Interview relevant personnel	See Table 3-4 and review the following additional best practices: C.10 Are virus scans frequently run? C.11 Are penetration tests used? C.12 Is network activity monitored? And are logs either kept or reviewed?	For example, considerations regarding compliance with policies, rules, procedures, and other standards, see Clause 5.36
	Direct Observation(s) • Review vulnerability scans • Review controls	Conduct walkdowns of the facility that are within the scope of the assessment	Review all previous Best Practices from Table 3-3 and 3-4, and the above in this table and observe daily operations in real-time to verify conformance.	For example, considerations regarding the protection of record against loss, destruction, unauthorized access or release, or falsification, see Clause 5.33

Building an Assessment Plan

Assessments are "the process of identifying risks to organizational operations…, organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system" [9]. To remain consistent, the term "assessment" will be used throughout this paper however the term can be used to describe different assessment types or activities such as audits, regulatory inspections, and self-assessments. Regardless of the type of assessment being conducted, each assessment should follow the same steps, or stages to create a methodical framework that is easily repeatable each assessment [10, 7].

For organizations that have yet to develop computer security programs or have recently developed them, the scope must be sufficiently focused to ensure insights can be gained on how to improve cybersecurity but also in a manner that will not overwhelm limited resources.

4.1 Planning Key Assessment Activities

An effective assessment must always be thoroughly planned, and the scope and objectives agreed to prior to being formally conducted. The planning phase must be finalized before conducting the assessment. The most critical task during this stage is to properly scope each assessment. Given the complexity and number of computer systems and control elements in a gamma irradiation facility, a single assessment may not cover the entire computer security program. Follow these steps to plan an effective assessment:

1. **Define Assessment Scope and Objectives:**
   - Determine the specific areas and objectives for the assessment.
   - See Section 2.3
2. **Create an Assessment Plan:**
   - Select Appropriate Assessment Type: Choose the type of assessment that fits the scope and objectives.

     See Section 2.4
   - Determine Normative References: Identify relevant standards and best practices, such as ISO/IEC 27002:2022 and ORS Cybersecurity Best Practices for Users of Radioactive Sources.
3. **Create an Assessment Schedule:**
   - Schedule Pre-Assessment Meetings: Arrange meetings with assessment team leads and the host organization.
   - Schedule Document Exchange: Plan secure methods for exchanging requested documents and records.
   - Schedule Preliminary Document Review: Set times for initial review of documents.
4. **Determine Required Expertise:**
   - Identify the necessary expertise for assessment personnel and allocate accordingly.
5. **Allocate and Schedule Personnel:**
   - Plan and schedule the involvement of assessment team members.

[9] NIST, "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171," NIST, 2021.
[10] G. White and M. T. Rowland, "Remote Inspection Information Security Guide," Office of International Nuclear Security, 2022.
[7] IAEA, "TDL-006 – Conducting Computer Security Assessments at Nuclear Facilities," International Atomic Energy Agency, 2016.

6. **Plan for Equipment and Communication Needs:**
    - Develop a plan to meet equipment and communication platform requirements.
7. **Request for Documents and Records:** Request necessary documents and records for review. Ensure secure transmission of information if conducted in advance.
8. **Identify staff for interviews**.
9. **Draft Initial Interview Questions:** Prepare questions and identify the staff/position for each question to gather to substantiate or identify key information.
10. **Determine Target Areas for Direct Observations:** Identify digital assets and functional domains (OT, IT, or both) and security domains (Organizational, People, Physical, Technological) to be assessed.
11. **Identify Permitted Assessment Team Tools (if necessary):** Choose tools like vulnerability scanners, network scanners, and protocol analyzers for direct observation.
12. **Notifications (if applicable):**
    - Notify appropriate personnel about the planned assessment.
    - Schedule interviews
    - Plan and notify staff and managers about any Direct Observations
13. **Conduct Assessment:**
    - On site assessment
    - Initial Assessment Out-Brief to site management
        1. Recommendations – findings where the site is not meeting the normative guidance (ORS Best Practices; ISO 27002)
        2. Suggestions – insights into optimizing cybersecurity program, controls, or activities; site meets the normative guidance.
        3. Good Practices – site implements cybersecurity in an effective and optimized manner. Good practices need to be identified in an assessment to highlight areas of high capability.
14. **Address Identified Weaknesses Immediately:**
    - If weaknesses or vulnerabilities are identified during this stage, take corrective actions immediately without waiting for the assessment to be completed.
15. **Draft Report:**
    - Assessment Team provides draft report to management for review, comment, and acceptance.
16. **Final Report:**
    - Acceptance of Final Report
    - Plan or schedule corrective actions based upon assessment findings (recommendations)
    - Consider implementing suggestions.

4.2 Selecting the Assessment Team

Selecting the right team to conduct a cybersecurity assessment is crucial for ensuring a thorough and effective evaluation. Ideally, the team should be composed of individuals with diverse expertise and experience in various aspects of cybersecurity, tailored to the specific needs and scope of the assessment. Here are key considerations for assembling an effective assessment team:

1. **Identify Core Competencies:** The team should include members with core competencies in cybersecurity, including knowledge of network security, information security management, and incident response.

2. **Include Domain Experts:** Depending on the scope of the assessment, it may be necessary to include domain experts who understand the specific OT and IT environments of the facility. These experts can provide valuable insights into the unique security challenges and requirements of the systems being assessed.

3. **Leverage Internal Resources:** Utilize internal personnel who are familiar with the facility's operations, policies, and procedures. These individuals can offer specific knowledge that external assessors might lack. However, ensure that internal team members are not assessing areas where they have direct responsibilities to maintain objectivity.

4. **Incorporate Diverse Perspectives:** A well-rounded team should include members with diverse backgrounds and perspectives. This diversity can help identify potential vulnerabilities and risks that might be overlooked. If possible and appropriate, consider including individuals from different departments, such as IT, operations, compliance, human resources, incident response, and physical security.

5. **Request External SME Support:** For specialized expertise or to enhance the assessment's objectivity, consider requesting external Subject Matter Expert (SME) support. These external experts can offer fresh perspectives and advanced technical skills, complementing the internal team's capabilities.

6. **Ensure Clear Roles and Responsibilities:** Clearly define the roles and responsibilities of each team member. Assign specific tasks such as document review, interview conduction, direct observations, and report writing. Having well-defined roles helps streamline the assessment process and ensures that all critical areas are covered comprehensively.

By carefully selecting a team with the right mix of skills, experience, and perspectives, you can ensure a comprehensive and effective cybersecurity assessment. Leveraging external SME support from other agencies such as ORS can further enhance the team's capabilities, providing additional expertise and objectivity. This strategic approach to team selection will help identify vulnerabilities, recommend improvements, and ultimately strengthen the facility's cybersecurity posture.

4.3 Assessment Schedule

Table 4-1 below is a table that outlines the key tasks, descriptions, timelines, responsible parties, and expected outcomes involved in the assessment process. This table should be used to develop an assessment schedule and can be modified based on the assessment type and scope. This structured approach ensures a comprehensive and organized assessment, from initial planning to the final report.

Table 4-1: Assessment Steps and Timeline

Task Title	Description (What)	Time (When)	Who	Expected Result
Initial Meeting	Determine scope Assessment type (self- assessment) Acquire external assistance Develop schedule	3 months before	Assessment/Cyber Leads Organizational leadership	Assessment Type, Scope, Schedule, External Support Request
Assessment Team Formation		2.5 months before		
Information Collection		2 months before	Site/Organizational Leads	Provide collected information to assessment team
Initial Document Review Meeting	Document Review	1.5 months before	Organizational Leads and Assessment Team	Review of information package, identify gaps, provide clarifications, start initial observations
Develop Detailed Assessment Plan	Identify personnel for interviews	1 month before	Organizational Leads and Assessment Team	
Finalize Onsite Assessment Schedule	Meeting to agree to detailed schedule of assessment (interviews, walkdowns, direct observation, sensitive document review)	2 weeks before	Organizational Leads and Assessment Team	
On site assessment		1-3 days	Assessment Team	
Exit Briefing		End of Assessment	Assessment Team	
Draft Final Report Meeting	Agreement on recommendations, suggestions, and good practices	1 month after	All relevant parties	Rough draft of assessment report
Final Report Meeting	Finalize report and complete assessment	1-2 months after	All relevant parties	Final report deliverable

References

[1] Unit 42, "Network Threat Trends Research Report (Vol 2.)," Palo Alto Networks, Santa Clara, CA, USA, 2023.

[2] Mandiant, "M-Trends 2023 | Mandiant Special Report," Mandiant, Reston, VA, USA, 2023.

[3] "Verizon 2023 Data Breach Investigations Report," Verizon, 2023.

[4] NIST, "Cybersecurity Workforce Demand," NIST, 2023.

[5] International Atomic Energy Agency, "IAEA NSS No. 20 – Nuclear Security Fundamentals: Objective and Essential Elements of a State's Nuclear Security Regime," IAEA, Vienna, 2013.

[6] ORS, "Cybersecurity Best Practices for Users of Radioactive Sources," ORS, 2022.

[7] IAEA, "TDL-006 – Conducting Computer Security Assessments at Nuclear Facilities," International Atomic Energy Agency, 2016.

[8] IAEA, "NSS No. 13 – Nucleaer Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)," IAEA, Vienna, 2011.

[9] NIST, "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171," NIST, 2021.

[10] G. White and M. T. Rowland, "Remote Inspection Information Security Guide," Office of International Nuclear Security, 2022.

Appendix A: Informative References

A.1 ORS Cybersecurity Best Practices for Users of Radioactive Sources

This document serves as a comprehensive guide outlining the essential objectives of a cybersecurity program, aiming to safeguard the confidentiality, integrity, and availability of a facility's operational technology (OT) and information technology (IT) networks used to protect radioactive material. For facilities with existing cybersecurity programs, the ORS Best Practices document offers enhancements to improve cyber hygiene throughout the organization. It includes a series of checklists that facilities can use to evaluate and strengthen their computer security programs. The checklists focus on three critical areas: (1) initiating a computer security program, (2) implementing controls, and (3) sustaining the cybersecurity program. This document is particularly valuable for organizations with limited resources compared to nuclear power plants (NPPs), especially those that store, process, or otherwise use ORM.

A.2 ISO/IEC Information Security, Cybersecurity and Privacy Protection (ISO/IEC 27002:2022)

This document offers international guidelines and best practices for information management security systems, aimed at helping organizations effectively manage their computer security risks. Unlike TDL-006 and ORS Best Practices, ISO/IEC 27002:2022 is designed for a broad range of organizations, not just nuclear facilities. Consequently, it is a comprehensive document that addresses an international audience and a diverse array of organizations.

It is important to note that while the ISO 27000 series is scalable, it primarily targets mature organizations that already have a security management system (ISO 27001) in place to manage both information and computer security risks. In this context, ORS Best Practices are extremely valuable as they provide industry-specific guidance. These best practices support the establishment, implementation, and maintenance of a computer security program tailored to the needs of ORM facilities, utilizing ISO/IEC's control domains in a structured and straightforward manner.

Given the international aspect of assessments for International Irradiation Association (iia) members, the ISO/IEC 27002:2022 standard can be utilized when additional clarification of certain suggestions or recommendations is needed. The use of ISO/IEC 27002:2022 should be to provide greater detail and examples to supplement those found in the ORS Best Practices.

A.3 IAEA Conducting Computer Security Assessments at Nuclear Facilities (TDL-006)

Originally published by the IAEA in 2016, TDL-006 was designed to provide an assessment framework for nuclear facilities. The initial publication offered a methodology incorporating common assessment techniques such as document reviews, interviews, and direct observations. TDL-006 is currently being updated to align with NSS 42-G, NSS No. 17-T Rev.1, and NSS 33-T, covering all IAEA security domains. It is important to use this document to provide a mature and internationally recognized process for assessments of nuclear facilities which serves as a basis for the guidance of this report.

Appendix B: ORS Best Practices Checklist – Starting a Cybersecurity Program

A cybersecurity program is essential to prevent vulnerabilities from being introduced into a physical security system that protects radioactive sources. As more IP-based security components are integrated, the importance of cybersecurity will only grow. While facility IT staff can assist with the fundamentals of a cybersecurity program, professional cybersecurity expertise may be required for more complex tasks to develop a thorough and effective program. The checklist below is from ORS Best Practices and is intended to provide an example of some specific tasks that can be completed to develop a program depending on the needs of the organization.

Table 4-2: Assessment Steps and Timeline

Domain	Section	Description	✔
Developing a Cybersecurity Program	A.1	Designate a staff member responsible for cybersecurity with sufficient authority to implement the site cybersecurity program	
Developing a Cybersecurity Program	A.2	Evaluate overall cybersecurity hygiene, posture, culture, and awareness level	
Developing a Cybersecurity Program	A.3	Map out all connections and dependencies to other systems	
Developing a Cybersecurity Program	A.4	Determine if physical protection system components are configured into logical security zones with minimum required traffic flows between zones	
Developing a Cybersecurity Program	A.5	Determine if network-level access controls are implemented on the internal network infrastructure that interconnects physical protection system components	
Developing a Cybersecurity Program	A.6	Use a system discovery tool to conduct an inventory of what devices are connected to the protection system and determine if only those authorized devices consistent with the security plan are connected. Vendors may have recommendations for the appropriate tool	
Developing a Cybersecurity Program	A.7	Review all firewall security policies and device configurations to determine if security zones are defined, minimum traffic flows are enforced, attack detection is enabled, logging on permitted and denied traffic flows are enabled, and administrative access capabilities are restricted to the minimum necessary. The references at the end of this guide can provide further information	
Developing a Cybersecurity Program	A.8	Conduct a best practices evaluation for secure router and switch configuration, management, and operation	
Developing a Cybersecurity Program	A.9	Identify potential attack vectors that can lead to potential compromise of the physical protection system, especially from connections permitted through the perimeter or from permitted remote access and management connections	
Developing a Cybersecurity Program	A.10	Review overall attack surface, attack vectors, and firewall rules	
Developing a Cybersecurity Program	A.11	When performing the review keep in mind such items as: • Network terminals vs. workstations • Restricted connectivity using distributed firewall security zones vs. unrestricted internal network connectivity • Hardened centralized server configuration vs. distributed server and software implementation	

Developing a Cybersecurity Program	A.12	Use a vulnerability assessment tool to determine if servers contain potential vulnerabilities and require patching or other security measures to mitigate potential risk. This may require the assistance of cybersecurity experts as these tools have the potential to negatively impact systems.
Developing a Cybersecurity Program	A.13	Conduct penetration testing to validate perimeter security design and implementation. The use of cybersecurity experts is recommended for this activity

Appendix C: ORS Best Practices Checklist – Cybersecurity Controls (Maintaining a Program)

Here are some cybersecurity controls that include technical, physical, and administrative measures, which can be quickly and inexpensively applied to existing security systems either immediately or in the near future. Implementing some of these measures may require assistance from your IT department, cybersecurity professionals, or an external service provider, as they might be too complex for someone without specialized skills. These activities are recommended as essential parts of a comprehensive cybersecurity program. The checklist below is from ORS Best Practices and is intended to provide an example of some specific tasks that can be completed as part of maintaining a program depending on the needs of the organization.

Table 4-3: ORS Best Practices Checklist – Controls

Domain	Section	Description	✔
Controls	B.1	Enforce strict user accounts with limited role-based permissions. Use the "least privilege" model for access to systems	
Controls	B.2	Use strong, complex password management and no longer than 6 months aging policies or use a passphrase. Passphrases are becoming the recommended control instead of passwords. • Minimum of 8 characters, including special characters or use a passphrase	
Controls	B.3	Remove unnecessary accounts, software, and processes	
Controls	B.4	Install Anti-Malware Software and ensure it is kept current	
Controls	B.5	Don't use software that is beyond end-of-life (for instance, Windows XP and 7). New vulnerabilities are often found in this software, but the manufacturer is no longer providing patches	
Controls	B.6	Ensure cybersecurity is included in Site Security Plan with ongoing reviews and is updated following upgrades	
Controls	B.7	Ensure facility has an acceptable use policy for employees using company cyber resources	
Controls	B.8	Establish a baseline to identify all equipment, cabling, and circuits and update documentation to match the physical implementation of the system and implement a configuration management process for reviewing, approving, and documenting equipment and software changes, patches, etc.	
Controls	B.9	Ensure patches and firmware are derived from authorized vendors	
Controls	B.10	Keep network switches, alarm panels, access control devices, computer BIOS, digital cameras, and other components patched to the current firmware version provided by the vendor	
Controls	B.11	Purchase and use enterprise-class hardware instead of consumer-class components meant for home or small office use	
Controls	B.12	Restrict software and firmware upgrades to authorized system administrators/managers	
Controls	B.13	Configure web browsers and dedicated e-mail accounts required by alarm management software to limit access to non-system related sites	
Controls	B.14	Implement physical hardening of host computer locations, workstations, wiring closets, and on-site central monitoring stations to prevent a physical attack on the equipment or the introduction of malware via USB ports, etc.	
Controls	B.15	Perform port scanning of all physical protection system (PPS) components that connect to the network and communication infrastructure to ensure only authorized ports are open	
Controls	B.16	Disable all unnecessary ports and associated services through hardware and software hardening	

Controls	B.17	Use Mobile Device Management (MDM) for the administration of mobile devices accessing company networks
Controls	B.18	Ensure facility has a strategy for the development and implementation of plans, processes, and procedures for timely recovery and full restoration of any capabilities or services that are impaired due to a cyber event
Controls	B.19	Ensure facility has an active employee security awareness program to potentially include phishing campaigns
Controls	B.20	Enable built-in firewall attack detection, logging, and alerting features that should already exist in most modern firewalls. Alerts should go to a Security Operations Center, SYSLOG server, a Security Event and Information Manager (SEIM), or at least some means to get the alert to the responsible staff in a timely manner
Controls	B.21	Enforce network traffic flows in existing firewalls
Controls	B.22	Utilize existing firewall DMZ as applicable
Controls	B.23	Enable port security on network switches, disable unused interface ports, and restrict administrative access
Controls	B.24	Create ACLs (access control lists) and restrict administrative access
Controls	B.25	Air gap the system if possible or at least minimize the number of perimeter interconnections to provide network isolation where feasible. Air gapped systems are not invulnerable to cyberattacks as systems should still be updated via USB drives, etc. Another option would be to implement a real time monitoring capability or a data diode
Controls	B.26	Configure a multi-zone network security architecture to isolate security protection components into logical levels and zones as appropriate
Controls	B.27	Utilize thin-client network terminals instead of Windows workstations where possible to reduce the attack surface, patching requirements, and total cost of ownership
Controls	B.28	Incorporate traffic encryption for communication over any external networks or telecommunications circuits
Controls	B.29	Add an intrusion detection system to analyze network traffic. This analysis will identify and alert personnel for attempted cyberattacks via suspicious packets and payloads
Controls	B.30	Use multifactor authentication: • Something a user possesses such as a badge or RSA token • Something a user knows such as a PIN, password, or passphrase • Biological characteristics of a user such as their fingerprint or iris pattern
Controls	B.31	Recommend that prior to deployment any new equipment and components be thoroughly tested for cyber vulnerabilities
Controls	B.32	Ensure excess computers and media are properly sanitized when disposed of

Appendix D: ORS Best Practices Checklist – Sustaining a Cybersecurity Program

The checklist below is from ORS Best Practices and is intended to provide an example of some specific tasks that can be completed as part of sustaining a program depending on the needs of the organization.

Table 4-4: ORS Best Practices Checklist – Sustainability

Domain	Section	Description	✔
Sustainability	C.1	Implement a configuration management plan and update it regularly	
Sustainability	C.2	Revisit program requirements and update policies and procedures for protection system configuration, change control, testing, personnel roles, and documentation as needed; continually evaluate and address gaps	
Sustainability	C.3	Update security plans periodically and after significant changes in your systems or networks	
Sustainability	C.4	Maintain approved equipment lists including hardware, operating systems, application software, firmware, etc., and associated revision levels	
Sustainability	C.5	Update mapping of interdependencies (hardware, software, hosts, and subsystems)	
Sustainability	C.6	Conduct end-to-end testing prior to incorporating new code or technologies	
Sustainability	C.7	Implement comprehensive procedures and checklists for software and firmware upgrades	
Sustainability	C.8	Manage and maintain software licenses	
Sustainability	C.9	Regularly update software and ensure that it continues to be supported by the software vendor. This will minimize software cyber vulnerabilities	
Sustainability	C.10	Run virus scans and update virus definitions on a frequent basis. Automated scans and update may be used but be aware they may impact system performance	
Sustainability	C.11	Perform penetration testing to ensure the effectiveness of hardening and architecture measures. Tests can be tailored to the specific Physical Protection System (PPS) requirements. These tests should be performed by qualified cybersecurity experts	
Sustainability	C.12	Conduct system monitoring of traffic over the network infrastructure and its attached components to detect cyber intrusion attempts; log system activity and report cyber alarm conditions	
Sustainability	C.13	Periodically test the recovery plan, which should include both contingency planning and backups	

Appendix E: Final Report Template/Outline

The following outline is an example that has been modified from IAEA TDL-006 and is intended to provide assessors a way to formally record assessment results. This template is only intended to be an example and should be modified as needed depending on the scope of the assessment.

Executive Summary

The executive summary should briefly, and concisely, describe the context of the assessment and can include information such as the context, objectives, methodology, requirements, major recommendations, and good practices uncovered because of the assessment.

Introduction

- Objectives
- Scope
- Methodology
- Definitions (if applicable)
- Clearly defined roles and responsibilities of the evaluation team and host organization

Evaluation Results

Findings

- Findings are found by applying a requirements filter on the observations. Findings should be listed.
- Requirements documents such as regulations, procedures, standards, good practices, etc. should be defined and identifying them must be mentioned within the finding.
- Observations can be included here, if referenced with the findings, or can be excluded if they're communicated to the facility in another way.

Recommendations, Suggestions, and Good Practice(s)

- Recommendations, based on associated findings, should be defined and mapped to relevant requirements.
- Recommendations may be defined based on who is conducting the assessment.
- Recommendations may be ranked in a graded approach related to their potential risks or facility impacts.

Mitigation Strategy (Optional)
Impact Analysis (Optional)

Conclusion

This section provides a summary of the evaluation results and reiterates the key recommendations, suggestions, and best practices related to requirements and risk analysis for gamma irradiation facilities. If a mitigation strategy is included in the final report, a comprehensive action plan can also be incorporated.

Abbreviations (Optional)
Appendix (Optional)

Appendix F: Observation Template

The following table is an example template that has been modified from IAEA TDL-006 and is intended to provide assessors a way to record information during an assessment. This template is only intended to be an example and should be modified as needed depending on the scope of the assessment. Information entered templates such as this can be used when developing the final report.

Table 4-5: Example Observation Template

Assessor name		**Number**			
Date and time					
Location	Where the observation takes place				
Facility	If applicable				
System	If applicable				
Security level	If applicable				
Observation:	Describe what was observed or identified				
How identified	Document Review	Interview	Observation	Open source	Other:
Intent	Recommendation	Suggestion	Good practice	Other :	
Finding*	Describe the variance				
Basis*	Reference to IAEA guidance, good practice, standard, regulation, known attack vector, etc.				
Root cause*	Reason the problem exists				
Exploitability*	easy	moderate	complex		
Accessibility*	Outsider threat/insider threat (knowing or unknowing)				
Potential impact*	Description of the direct and indirect impact of the finding				
Significance level*	Categorization of the finding based upon its potential impact (Organizations may devise their own significance or impact scale)				
Action*	Implement good practice, implement standard, implement regulation, patch system, etc.				
NOTES:					

*These items may not be immediately evident during the observation phase and can be completed after walkdowns are completed

Field Template Legend

Exploitability	
Easy	Vulnerability generally known; public exploits exist
Moderate	Some details known; proof of concept available
Complex	No details available

Potential types of actions

Modifications to equipment and the installation of additional devices and means to prevent the recurrence of the same or similar events

Improvements of procedures and administrative measures, and additional checks and controls

Rectifying deficiencies revealed in the operation documentation (operation manuals)

Rectifying deficiencies in normative documents

Training personnel to perform jobs properly

Making changes to the working environment

Making changes to the planning and scheduling of work and/or to the individuals assigned to duties

iiaglobal.com