World Institute for Nuclear Security

iia INTERNATIONAL IRRADIATION ASSOCIATION

Methodology for assessing the effectiveness of security arrangements at gamma irradiation facilities

May 2024

TABLE OF CONTENTS

INTRODUCTION

Gamma irradiation facilities use radioactive cobalt-60 sources as the source of radiation for the treatment of materials and products. These materials and products are processed on an industrial scale for beneficial applications such as the sterilisation, microbial reduction, disinfestation, and modification of material to improve its performance. Gamma irradiation is used in approximately 50 countries and by many industries for applications that benefit us all every day.

The presence of radioactive sources can make gamma irradiation facilities attractive to adversaries. Security systems are therefore put in place to deter, detect and assess, delay and respond to any attempt by an adversary to cause harm. Gamma irradiation facilities are operated by organisations that apply rigorous protocols and other security arrangements, and the industry is subject to regulation to ensure the safety and security of the radioactive sources and to protect staff and the public.

It is important that operators of these irradiation facilities periodically challenge their security arrangements to ensure that they not only function correctly but that they continue to address the evolving security threat. Consideration also needs to be given to new technology and practices to understand how this may be applied to enhance or replace existing security arrangements.

This document provides a methodology for conducting a security assessment of a gamma irradiator and gives practical guidance on reviewing and measuring the effectiveness of security. It can be used both to conduct a self-assessment of security arrangements in place at a facility or a security review implemented by external experts. This is a high-level document that gives broad direction that can be tailored to the specific circumstances and arrangements at individual irradiators. It is for use by operators of large-scale commercial or semi-commercial irradiators and does not cover the assessment of smaller self-shielding irradiators.

This document has been prepared jointly by WINS and the International Irradiation Association (iia). The information presented is based on accepted international guidance and should be read in conjunction with the WINS/iia Best Practice Guide entitled *Security of Radioactive Sources Used in Industrial Radiation Processing.*

Valuable input based on real-life experiences of security practitioners and managers of gamma irradiation facilities was also received during preparation of this document. In particular, WINS and iia would like to thank the following organisations for their contribution:

- Gammapak Sterilization Ind. & Trd. Inc.
- SQHL (Beijing SanQiangHeLi) Radiation Engineering Technology Co., Ltd
- Sterigenics U.S., LLC
- STERIS Applied Sterilization Technologies, STERIS plc

The preparation of this document was supported by the US Department of Energy/ National Nuclear Security Administration (DOE/NNSA) under Award Number(s) DE-NA0003949. This revision was undertaken based on a pilot security assessment that was undertaken in 2022.

About the International Irradiation Association (iia)

The International Irradiation Association (iia) was established in 2004 and is a non-government organisation that has observer status with the IAEA. It represents the industrial irradiation community that includes gamma, electron beam and x-ray technologies. A core aim of the iia is to promote the safe and beneficial use of irradiation technologies. Members represent a range of organisations with an interest in the scientific and commercial application of the technology. Members of iia include manufacturers, producers and suppliers of cobalt-60 and electron beam/x-ray technology, multinational and national radiation processing facility operators, universities, institutes and organisations providing support services. The membership is geographically diverse and provides a basis for networking and collaboration.

About the World Institute for Nuclear Security (WINS)

In 2008, WINS was established as a non-government organisation tasked with filling a gap by creating a forum to identify and share best practices in nuclear. Since then, WINS has expanded its services and membership base to more than 7,800 Members to better serve the global nuclear security community. WINS has held more than 250 international events and workshops and published numerous International Best Practice Guides on a wide range of issues.

WINS also offers certification from the WINS Academy for each of its ten programmes. Learners who sign up for a WINS Academy programme have the option of taking an exam to become certified either as a Certified Nuclear Security fundamentals Professional (CNSfP) or as a Certified Nuclear Security specialised Professional (CNSsP). Further information on the Radioactive Source Security Management specialisation can be found here.

We Welcome Your Comments

We will periodically update the information in this document to reflect experience gained during the implementation of the proposed methodology, evolutions in gamma irradiation industry practices and new security ideas. We ask that you read it carefully and then let us know how it can be improved.

WINS Contact Information

World Institute for Nuclear Security
Landstrasser Hauptstrasse 1/18
AT-1030 Vienna, Austria

Email: info@wins.org
www.wins.org

iia Contact Information

International Irradiation Association
5 Eco Park Road. Ludlow, Shropshire
SY8 1FD, United Kingdom

Email: info@iiaglobal.com
www.iiaglobal.com

Lars van Dassen
Executive Director
World Institute for Nuclear Security

Mr Paul Wynne
Chairman
International Irradiation Association

Revision 1
May 2024

1. WHY IS IT IMPORTANT TO MEASURE THE EFFECTIVENESS OF SECURITY ARRANGEMENTS AT GAMMA IRRADIATION FACILITIES?

1.1 Understand the threat, identify vulnerabilities and reduce the risk

Gamma irradiation facilities each contain dozens or several hundred cobalt-60 (Co-60) sources and typically contain a total activity of 100kCi to 5MCi. A security incident, such as theft of a Co-60 source, would have serious consequences for an organisation including interruption to normal business operations, potential exposure of a worker or a member of the public to radiation exposure, and negatively affect the reputation of an organisation. The organisation could incur financial losses (e.g., medical costs for employees and members of the public, radiological clean-up costs, loss of the use of facilities, lost business, recovery costs, replacement costs, etc.), and this could constitute a serious crisis for the organisation.

The threat in this context is a person or a group of people who have the motivation, intention and capability to carry out a malicious act. In the case of a gamma irradiation facility, from a radiological security perspective, this would be either theft of radioactive material (Co-60) or sabotage of the facility to cause a radioactive release. This includes theft or sabotage during transport of Co-60 sources as well.

With that in mind, the facility's security arrangements are designed around what needs to be protected, what degree of protection is considered adequate, and what security measures can be implemented to meet the security expectations.

It is essential for the operator of a gamma irradiation facility to periodically review its security arrangements to assess whether these are as efficient and effective as expected. A comprehensive review will identify or anticipate any vulnerability and result in mitigation actions, if required. Regular performance evaluation of the security arrangements, in particular those that concern the key objectives of a security system (deterrence, detection and assessment, delay and response) contributes to operational readiness and reinforces confidence that the security arrangements would effectively reduce the risk.

1.2 Providing security assurances to various stakeholders

Measuring and reporting the effectiveness of security arrangements demonstrates to various stakeholders – including staff, customers, regulators and the public – that security is an integral part of the organisation's culture. The process highlights to staff and regulators that security is treated as a priority and provides additional assurance that the organisation is compliant with all internal and external requirements. Ongoing security assurance is achieved by continually reviewing the effectiveness of an organisation's security arrangements, including consideration of new threats that may emerge and new technologies that may become available.

1.3 Continuous improvement and development of a robust security culture

Conducting a security assessment not only reveals possible shortcomings in an organisation's security arrangements but also helps to identify how these could be improved. It supports the verification that the elements of the security systems function as expected. It also allows the organisation to assess the impact of a change in operations or the implementation of a new security measures and to decide on the most effective way to address a security objective.

Conducting a security assessment, however, only provides a snapshot of the security situation at a given moment and this is why it is important such evaluations are periodically repeated.

Effective security is critical to business success. Evaluating the performance of security arrangements, including the security procedures and their implementation, is a way to engage with staff, raise their awareness on the importance of security, explain the benefit of good security, and finally ensure their engagement in security issues.

2. THE USUAL APPROACHES FOR MEASURING SECURITY EFFECTIVENESS

2.1 Self-assessment and internal assurance processes

The leaders and managers of the operating organisation need to understand the current status of security arrangements in order to fulfil their governance and oversight functions, including their compliance with all external regulations, assessing the effectiveness of the distribution of duties, and make informed judgments and sound investments in security that will mitigate identified security risks to an acceptable level.

Self-assessments provide organisations with a method to determine the current status of their security programmes and, where necessary, identify opportunities for improvement. Organisations usually develop self-assessment guidance utilising questionnaires containing specific control objectives and techniques. Often these controls are feature based (e.g. there is a sensor or there is no sensor) and rely on functional testing (e.g. the sensor triggers an alarm or the sensor does not trigger an alarm). Some larger organisations also conduct internal full scope performance testing of their security arrangements. This may involve third-party organisations and first responders that have been incorporated into the overall security programme.

2.2 Regulatory oversight

Gamma irradiation facilities are regulated by national and local authorities that monitor compliance with licensing and other legal requirements. Regulators are also responsible for communicating the relevant parts of a national threat assessment and set out detailed and comprehensive set of attributes and characteristics of threats against which operators are required to protect. Regulatory activities include authorisation, licensing, inspection and enforcement activities. Regulatory inspections may be announced or unannounced and are likely to involve a highly detailed assessment of the organisation's facilities and security programme. Different regulatory systems are implemented in different ways and may be performance based, prescriptive or a combination of the two.

2.3 Third party audits and peer reviews

Organisations that operate gamma irradiators may invite a third-party organisation to audit and review various elements of their business and operations. This has the advantage of being independent and therefore reducing the risk of bias that may impact the quality of the audit process. While some elements of security at gamma irradiation facilities are generic, specialist knowledge of the irradiation system and processes will be required from any third party that is employed to provide a high-quality audit at such a facility.

A peer review may also be an appropriate approach although it is recognised that organisations within the same industry (e.g. contract irradiation service providers) might find this challenging to establish due to the sensitivity of some commercial and security matters. Peer reviews are based on evaluations carried out by experienced professionals with the objective of identifying areas for improvement, sharing experience and highlighting best practices. Because the peer review

team includes fellow professionals with relevant backgrounds, it builds confidence in a shared understanding of the importance of appropriate arrangements for the security of the gamma irradiator and the need to ensure the protection of sensitive information. It also gives reviewers the opportunity to learn by refreshing and expanding their own knowledge prior to undertaking the review, as well as by acquiring new ideas and effective solutions to problems as they gain insight into another organisation's operations. Peer review can be highly cost effective if it is undertaken on a reciprocal basis with other operating organisations.

External audits and peer reviews are not a substitute for regulatory inspections. The scope of audits and peer reviews can go beyond the scope of regulatory requirements if deemed necessary and include any security expectations determined by the organisation itself. Corporate internal audits and peer reviews can provide a basis for benchmarking performance and powerful incentives to achieve improvement. They can also contribute to the convergence of policies and practices.

3. A METHODOLOGY FOR CONDUCTING A SECURITY ASSESSMENT

The proposed methodology follows a usual five-step process (see *Figure 1*) describing the planning phase, the preparation of the review, conducting the assessment at the facility, the reporting of the key findings, and the follow-up activities to implement the recommendations and suggestions received during the review.

The reader is encouraged to adapt this methodology to take into account the specificity of the gamma irradiation facility to be assessed (e.g., size of the facility and maturity of the security programme) and the review process considered (e.g., self-assessment by an operator of the security arrangements at their gamma irradiation facility or assessment to be conducted by an external team to the host facility).

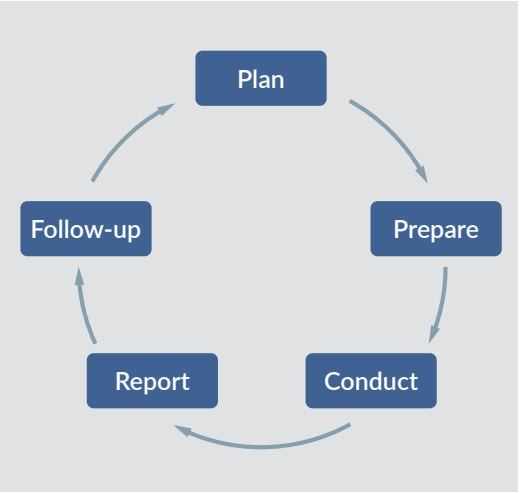


Figure 1. Methodology process

3.1 Plan

The planning phase starts a few months prior to conducting the assessment. The assessment process usually involves one to three experts, depending on the exact scope of the review and the size of the organisation involved.

As a first step, it is recommended to identify an expert who will lead the assessment (the lead expert). If the assessment is to be performed by an external team, the host facility should designate a suitable representative to act as counterpart to the assessment team. The counterpart will serve as a point of contact and will coordinate organisational and practical matters including scheduling interviews, organising a walk-down, supplying appropriate documentation and providing workspace, among others.

The scope and process for conducting the assessment needs to be agreed upon in advance. The exact security topics to be covered by the assessment team also need to be identified beforehand. They may cover some or all security areas identified in *Section 4.1* below.

The assessment should cover security arrangements for all status of the facility in normal operations (standard radiation processing mode, day/night shift) and non-standard operations (such as under maintenance, loading/unloading of sources, etc.). For non-standard operations, the assessment might be limited to a review of relevant procedures and documents.

The assessment should include arrangements for Co-60 transport matters (delivery and repatriation of sources) as it relates to the preparation of a shipment, the reception of the shipment and any movement of sources within the boundaries of the facility.

The functional and limited performance testing of selected security equipment might be conducted during the actual assessment.

The expert(s) on the assessment team should possess adequate security and gamma irradiation knowledge. Furthermore, the team members should have demonstrated experience in conducting such reviews and consolidating their findings in written reports.

An assessment performed by an external team, either from within the corporation or from a third-party organisation, can be an opportunity for the staff of the host facility to develop their own skills for conducting security assessments and implementing security. The host facility may identify one or two of their staff who will shadow the assessment team to learn about the process and develop their competencies in security.

The assessment should be seen as part of a continuous improvement approach and opportunities for complementary actions should be considered during the planning phase.

Engagement with the Regulator

Because of the understandable sensitivities over security assessments conducted by outsiders to the facility, it is important that, for external reviews, the host facility assesses the need to inform and obtain 'buy-in' from its regulator and other relevant authorities and counterparts. Prior to conducting the assessment, sufficient notice should be provided to facilitate communication and clarification of any concerns.

3.2 Prepare

Once the scope and dates for the assessment have been finalised, preparation can begin.

If the assessment is performed by an external team, the expert(s) preparing for the assessment will benefit from already having information about the gamma irradiation facility. An Advance Information Package (AIP) may be prepared by the host to include an introduction to the facility, an organisational chart and other generic information which is not considered classified or very sensitive to the operation of the organisation. The external assessment team may provide the host facility with a template or outline AIP. This advance information will enable the assessment team to develop focus areas and be time efficient during the assessment itself. Further information on possible content of the AIP can be found in *Section 3.3* below.

It is crucial to prepare the locations to be visited (walk-down) and identify people to be interviewed (staff and contractors) beforehand. If not properly prepared, the security assessment might end up being disruptive to the radiation processing operations of the facility. Interviews and walk-downs need to be carefully planned to minimise impact.

Necessary arrangements need to be made to ensure that identified areas will be accessible and that interviewees will be present and will have been informed of the objective and nature of the discussion and of the assessment. Accessing the irradiation cell/pool area requires stopping operations, meaning that any need to visit this area should be scheduled to minimise time and cost.

A structured, cross-section of employees from senior management to operational staff should be selected for interview. The selection of employees must be as diverse and as representative of the workforce as possible to avoid the organisation putting their "best people" forward, resulting in a bias in the assessment.

3.3 Conduct

It is anticipated that implementing the proposed security assessment will last up to two days. A template agenda for an external review is available in Appendix 1. Although timing and duration is of less relevance for self-assessment, it is recommended that such reviews are conducted over a rather short period (i.e., a few days).

The assessment process includes reviews of organisational charts, procedures and other documents as required, observations made during the facility walk-down, interviews of staff and contractors if appropriate, follow-up discussion of observation results if needed, consolidation of key findings, and writing of the report.

The process and conclusions of the assessment are based on the security areas, performance indicators and questions listed in *Section 4* below.

If the assessment is performed by an external team, the assessment review usually starts with an opening meeting between the team and senior managers of the host facility. This is an opportunity to explain the process again and purpose of the assessment, update the scope and agenda if necessary, and agree on certain practical considerations such as safety matters, local rules and behaviour while at the facility. Behaviour includes controlling taking photographs and any other sensitive issues such as the use of portable electronic devices by the assessment team.

Facility description and main characteristics impacting security arrangements

The self-assessment team is expected to have an understanding the facility and its operation, as well as of all information and factors relevant for the security arrangements. An external assessment team will need to develop of this understanding, in particular of the following:

- What is the general layout of the site and building in which the irradiation facility is located? What are the entry points to the site and building (i.e. pathway to radioactive sources)?
- What is the design of the irradiator? Where are the sources located in the irradiation cell during operation and safe storage? What are the entry points to the irradiation cell?
- What are the modes of operation of the facility (24/7 or part time; local or remote operation; maintenance periods; source loading/unloading operations, etc.)?
- How many and what type of personnel are needed to operate the irradiator during the various modes of operation? Are there personnel shift changes?
- What is the general source inventory (details of individual source serial numbers are not generally relevant to the assessment)? How often are sources loaded and unloaded? What is the process? Are sources ever stored outside the irradiation cell?
- Was security by design considered or were security features added at a later stage?
- What are the safety measures for the irradiator? Do they contribute to security?
- Are there any particular locations, operations, times or other areas of concern?

Ideally, most of the answers to these questions are included in the AIP provided to the team prior to their visit to the facility. Pending answers might be addressed during the opening meeting of the assessment.

For external assessments, it might be useful to organise video conferences prior to the visit to support preparatory activities. Obviously, particular attention should be given to the sensitivity of any information that might be discussed during these online engagements, and any such video conference should only be recorded after all parties have granted permission.

3.4 Report

The process should always conclude with a written report including key findings and conclusions on the overall security arrangements and detailed findings for each of the main areas. The key findings of the external assessment are usually presented at the end of the onsite assessment.

Benchmarking the security performance

It is instructive to benchmark security performance against best practices in similar facilities and compare it to a maturity scale appropriate for the gamma irradiation industry. Such benchmarking supports the assessed organisation's ability to evaluate and understand how well the facility is performing in specific areas, as well as overall, and to identify areas that may require particular attention.

Section 4 of this report proposes structuring the review around seven security areas and offers a maturity scale for each area describing five levels of performance. A Level 1 rating describes an excellent performance when a Level 5 rating reports significant gaps to be urgently mitigated.

A Level 3 rating should be regarded as meeting the minimum expectations for security. WINS and iia encourage organisations to achieve a Level 2 and – depending on certain specific circumstances such as elevated threat situation or strategic decision to be taken by a leader in this area – to consider reaching Level 1. Level 4 or 5 is well below the minimum industry standard, and the facility does not meet the best practices expected by the gamma irradiation industry.

LEVEL	ASSESSMENT
1 RESILIENT	The facility greatly exceeds expectations in this security area. The facility is considered a leader in this area and best practices from this facility should be shared with other like facilities.
2 PROACTIVE	The facility meets and meaningfully exceeds expectations in this area.
3 COMPLIANT	The facility meets expectations in this area.
4 REACTIVE	The facility does not currently meet expectations in this area and requires corrective actions.
5 VULNERABLE	The facility is far from meeting expectations in this area and requires immediate corrective actions.

The maturity scales and associated performance statements to be employed for the benchmarking of the facility for each security area are provided in *Section 4.2* below.

Drafting the report

The report should include a narrative supporting the maturity assessment. A template report is provided in *Appendix 2.*

The assessed performance of a facility versus the benchmark for the seven security areas can be illustrated and included in the report as below.

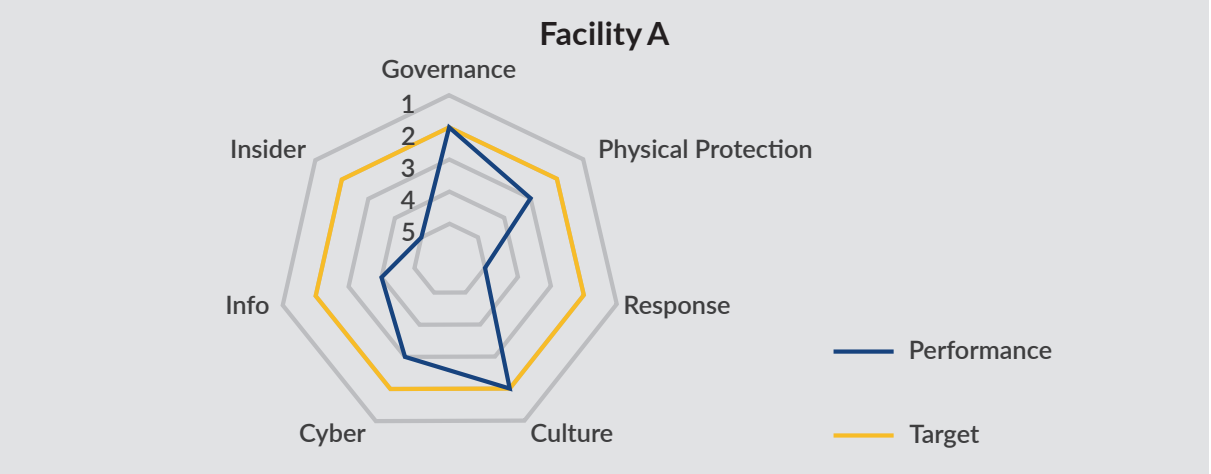


Figure 2: Arbitrary target maturity level of two for each individual security areas (denoted by the orange lines. The actual performance of the facility (blue line) is clearly below target, especially for insider and response areas.

In addition, a maturity scale can also be employed for the overall benchmarking of the facility. An example is provided in *Appendix 3* and is derived from *Appendix B* of the WINS BPG on *Security of Radioactive Sources Used in Industrial Radiation Processing.*

As a complement to the overall maturity grading and per security area, the report will also include a list of recommendations and suggestions to strengthen existing security arrangements.

- **Recommendations** should be issued when the assessment team believes that a security area or an element of a security area does not meet the industry standards or corporate security expectations.
- **Suggestions** should be offered when the assessment team sees an opportunity to enhance the performance of a given security measure.

The report, **especially for external assessments**, should also recognise security arrangements that are to be commended and highlighted as good industry practices. These "strengths" are descriptions of practices, activities or processes employed by an organisation that result in achieving a security performance beyond expectations.

The key findings of the assessment should be presented to the senior management of the gamma irradiation facility. The objective of this meeting is to provide senior management with an overview of the report and its main recommendations, suggestions and strengths. A key purpose is to ensure agreement on the factual basis for – and understanding of – the conclusions for each finding.

In the case of an assessment by an external team, the written report is the exclusive property of the organisation, not the assessment team, and should not be quoted, circulated or used for any other purpose without the approval of the host facility. Responsibility for all follow-up actions falls solely on the facility that was assessed.

Addressing confidentiality matters

For assessment conducted by outside experts, host facilities may express concerns about confidentiality, commercial or proprietary issues, because members of the assessment team may have access to locations, policies, procedures and processes relevant to security or that involve business systems that are proprietary.

Confidentiality issues can be addressed in a variety of ways:

- The exact scope of the review is agreed beforehand and may exclude particular areas or matters;
- Experts selected to conduct the assessment possess specific individual credentials and expertise and usually belong to a limited pool of individuals agreed to and selected by the host organisation;
- Experts may be requested to provide a certified statement from their organisation declaring that they are current employees in good standing. In certain instances, the regulator may request evidence that the experts are trustworthy and hold security clearances, as appropriate;
- The provision of information is provided at the discretion of the host. Experts may have to sign a confidentiality/non-disclosure agreement (NDA) before receiving any information from the host organisation. Finalising NDAs should be initiated as early as possible during the process;
- When producing technical notes or draft sections of the report, experts must take precautions. They should agree not to comment to a third party on specific details of the assessment in particular on its findings;

- Sensitive information generated or received by the assessment team, including electronic data, is destroyed, deleted or returned to the host organisation at the end of the process;
- The assessment report is marked as confidential, kept securely by the host organisation and its further distribution fully controlled by the host organisation.

3.5 Follow-up

The report will contain the security maturity levels, make conclusions on the effectiveness of security arrangements at the gamma irradiator, identify strengths and areas for improvement and indicate where there is a need for follow-up action.

In case of a need for follow-up action, an action plan should be prepared and formalised by the (host) organisation. This plan should include arrangements for making financial and human resources available for security changes that may be necessary at the gamma irradiator.

The objective of the follow-up action plan is to ensure that identified corrective actions are prioritised and addressed on a timely basis. The priority level of corrective actions is likely to be recommended by the expert assessor and, in the case of an external assessment, should be agreed between the assessor and the security specialist at the host company. The priority level will distinguish between the very short term (e.g. actions that address the greatest security risk or can be implemented easily) and the short/medium term (e.g. less urgent with less impact on security effectiveness or requiring a greater financial investment).

For each corrective action, the action plan should include:

- A detailed description of the corrective measure that is required.
- The security risk that is addressed by the corrective action.
- Its implementation priority level.
- Any impact of the corrective measure (e.g. on the irradiator functionality, safety or the radiation processing operation).
- Any related residual security risk after implementation.
- The estimated cost of implementation.

A timetable of corrective actions should then be created to identify each corrective measure, its priority shown in terms of start and target completion date and the person or group responsible for undertaking the action.

Consideration should then be given to the next security assessment to be undertaken within the following 12-24 months.

Where appropriate, it is encouraged that gamma irradiator operators that have performed or hosted a security review share their experience, including identified strengths and opportunities for enhancing the effectiveness of their security arrangement within their industry. This can be done through selected industry associations such as the iia, NGOs and working groups.

When findings challenge the organisation's compliance with its regulatory requirements, it is expected that the organisation takes immediate corrective action and inform relevant competent authorities, as appropriate.

4. REVIEW OF SECURITY AREAS AND PERFORMANCE INDICATORS

4.1 Security areas to be covered by the assessment

Security matters related to the security of radioactive sources used at gamma irradiation facilities have been grouped into the following seven topical areas:

A. Governance arrangements

B. Physical protection

C. Response to security incidents

D. Security culture and awareness

E. Cybersecurity

F. Information security

G. Personnel security

4.2 Review Framework

The section below provides a framework for performing the assessment. It is intended for guidance only and contains examples rather than providing a comprehensive assessment.

It provides an introduction to each of the seven security areas and examples of indicators that demonstrate effective arrangements and capabilities in security.

It is not expected that the assessors systematically covers all these areas and topics during the review. The decision whether to select a topic described below should take into account the outcomes of previous assessments and possible strengths or weaknesses in particular areas that have been identified.

The section below also provides example of questions to help assess security effectiveness and an example format for recording answers received.

It also provides a maturity scale for each security area with its own set of characteristics and associated performance indicators. Each of these individual maturity scales have been designed to help the assessment team identify how the organisation performs in a given security area and better understand what steps can be taken to improve the situation and move to the next level.

A. GOVERNANCE ARRANGEMENTS

Introduction

Governance for security is the systems by which an organisation operates and is controlled and the structure through which it creates effective security. This encompasses the risk management approach taken by the organisation and how it incorporates security into its routine operations and business requirements. Governance includes security policies and procedures that cover organisational responsibilities for security implementation, oversight, compliance and resilience. Budget planning and development of security competencies amongst staff in order to sustain security and material accounting and control (e.g. source inventory and end-of-life management) are also part of governance arrangements.

Examples of indicators demonstrating effective and resilient governance arrangements:

- The security of the Co-60 sources is part of the overall risk management approach of the organisation.
- A clear, written policy governing the security of the Co-60 sources has been published.
- Security responsibilities are clear and have been effectively assigned.
- Required competencies for fulfilling security roles and responsibilities have been identified and documented.
- Senior management understand and know the types of costs associated with components of security.
- Senior management have an oversight of the security arrangements and can demonstrate that they meet or exceed all these regulatory requirements.
- The organisation takes a whole-life approach to radioactive source management and security. Effective arrangements and funding are in place for handling end-of-life sources.

EXAMPLE QUESTIONS FOR GOVERNANCE ARRANGEMENTS

QUESTION	ANSWER FROM THE FACILITY	SOURCE OF THE INFORMATION*	COMMENTS
Is there a written policy governing the security of radioactive sources?			
How are radioactive source security and industrial security matters coordinated?			
Are security responsibilities clearly assigned? Do job descriptions include security responsibilities?			
Is the entire security function internal or part of it sub-contracted to an external company?			
How is the security competency of the staff demonstrated and assessed?			
How is threat information communicated to the organisation and then to the staff?			
Are you satisfied with the level of security? What are the security objectives? How do you demonstrate you meet them?			
Are you subject to regulatory inspection on radioactive source security? How are report actions recorded and followed up?			
What is the cost of the security arrangements for security? What is the main cost driver?			

* Observation (location of the observation); or Document (reference for the document); or Interview (name and function of the interviewee).

GUIDANCE AND TIPS FOR EXTERNAL REVIEWS

- During the preparation phase and planning for the site interviews, it is important to ensure that a senior executive will attend the opening and closing meetings.
- Receiving the organisational chart prior to the review and clarifying exact roles and responsibilities for security as early as possible in the assessment process will save time during the review itself.

Maturity Scale:

LEVEL	CHARACTERISTICS
1 RESILIENT	Executive management demonstrate their conviction that a threat exists and that security is important by treating security as an integral part of corporate risk, by taking a risk-informed approach toward security, and by taking a whole-life approach toward the management of their radioactive sources.
2 PROACTIVE	Executive management generally believe that a threat exists and that security is important. They are beginning to treat security as an element of corporate risk and are usually successful at taking a risk-informed approach toward security. They also take a whole-life approach toward the management of radioactive sources.
3 COMPLIANT	Executive management generally understand that a threat exists, that security is important, and that it would be a good idea to treat security as an element of corporate risk. They have also begun to create policies and procedures that would support taking a risk-informed approach toward security. Executive management have briefly addressed what to do with disused sources that reach the end of their lives.
4 REACTIVE	Executive management do not believe their facility faces any threats. They assume the radiation safety officer/security director is solely responsible for security. Because they don't believe that security is an issue, they do not treat it as an element of corporate risk. Nor do they take a risk-informed approach toward security. Executive management purchase and use radioactive sources according to regulatory requirements, but they have not addressed what to do with disused sources.
5 VULNERABLE	Executive management do not believe their facility faces any threats. They assume that the radiation safety officer/security director is solely responsible for security. Radioactive sources are generally purchased according to regulatory requirements, but no provision has been made for disused sources.

B. PHYSICAL PROTECTION

Introduction

Physical protection has four functions that form the basis of the security system. The first is to **deter** adversaries from even attempting to steal or sabotage radioactive sources. The second is to **detect** and assess any attempts that adversaries might be making. The third and fourth are to **delay** adversaries that are attempting to steal or sabotage sources until an adequate **response** force (e.g. the police) can arrive and interrupt or neutralise them. Each of these functions is important and works with the others to achieve an effective security system. The physical protection measures should form a series of successive security measures that have to be overcome or circumvented before the security of sources is compromised. Ideally, the facility, the bunker and the irradiator are originally designed to incorporate as many detection and delay opportunities and reducing the need for additional physical protection elements to be added. A security plan should document the design, operation and maintenance of the entire physical protection security system. The security plan should be routinely reviewed, evaluated and updated.

Examples of indicators demonstrating the implementation of an adequate physical protection system that effectively combine the functions of deterrence, detection and assessment, and delay:

- A security plan exists and includes the elements of delay, detection, assessment and response. The plan is periodically reviewed and revised.
- Deterrence measures – such as signage, well-maintained perimeter fencing, cleared vegetation, visible CCTV, lighting of external zones and security presence – have been implemented.
- Detection means have been installed in sensitive areas. Alarms are recorded, and the number of false alarms has been minimised. Alarms are reported onsite and to secure offsite locations.
- Any pathway to the Co-60 sources has several opportunities for detection. Procedures include temporary compensatory measures in case the detection equipment fails.
- Alarm assessment tools and procedures are in place. There is evidence that detections (alarms) are followed by assessment actions.
- Necessary delay measures are in place along any pathway to the Co-60 sources.
- Access control arrangements for staff and contractors are in place and effectively implemented. Access control measures, including search procedures, are more stringent closer to the irradiation cell.
- Various modes of operation (Co-60 loading/unloading and transport operations) have been taken into account in the design and implementation of physical protection measures. Temporary compensatory measures are implemented when necessary.
- There is periodic functional and performance testing. There are maintenance procedures in place and evidence that default or equipment failure is corrected in a timely manner.

EXAMPLE QUESTIONS FOR PHYSICAL PROTECTION ARRANGEMENTS

QUESTION	ANSWER FROM THE FACILITY	SOURCE OF THE INFORMATION*	COMMENTS
Is there a site security plan?			
Are there multiple layers of protection? What are the various security zones (e.g., outer perimeter, building envelope, inner perimeter, source location/cell)?			
What are the detection measures in place? How are they operated? Are alarms reported on site, externally or both? What are the assessment procedures? Are there compensatory measures in case of failure of detection equipment?			
Are alarms recorded? Is there evidence from follow-up action? How many false alarms are generated per month? When was the last recorded false alarm?			
Have you identified scenarios of concern (e.g., to remove one or several sources from the irradiator rack)? Do you have a sense of the time it would take to complete such scenarios?			
What access control arrangements are in place? Do they differ for staff and contractors? Is there contraband detection equipment?			
Have various modes of operation (loading/unloading, transport operations) been taken into account in the design and implementation of the physical protection measures?			
What functional and performance tests are conducted on the physical protection system?			
Have you considered internal threats in the design and evaluation of the physical protection system?			
What is the process for maintaining physical protection equipment? Is there evidence that default or equipment failure is corrected in a timely manner? When was the last failure of detection equipment? How long did it take for this piece of equipment to become operational again? Are compensatory measures taken in case of failure of security equipment?			
Does the security plan reflect the elements discussed above? When was its last revision undertaken? How often is the plan reviewed or revised? What prompts the review of the security plan?			

* Observation (location of the observation); or Document (reference for the document); or Interview (name and function of the interviewee).

GUIDANCE AND TIPS FOR EXTERNAL REVIEWS

- A few functional tests should be conducted for selected detection equipment. In addition, the performance of some sensors, including the adequacy of their technology and proper installation, should be measured.
- Adequately protecting product entry/exit paths to the irradiation area can be challenging. Also, large gamma irradiation facilities may experience a large volume of cargo trucks, which may create some vulnerabilities or specific challenges to accessing control arrangements and effective security. These matters may require specific attention during the assessment. It might also be an opportunity for the experts of external assessment teams to share the practices they may have observed elsewhere and suggest possible improvements in the facility practices.

Maturity Scale:

LEVEL	CHARACTERISTICS
1 RESILIENT	The design of the physical protection system takes into account credible threats and successfully integrates deterrence, detection, delay and response elements and functions. It also follows a defence in depth and graded approach toward security. The physical protection measures are well coordinated with source operation and radiation safety, and the physical protection system is regularly maintained, tested and evaluated. The necessary resources are made available and a continuous improvement programme has been established to ensure the resilience and sustainability of the physical protection system.
2 PROACTIVE	The design of the physical protection system takes into account credible threats and integrates deterrence, detection, delay and response elements and functions. It also follows a defence in depth and graded approach toward security. Security measures are fairly well coordinated with source operation and radiation safety, and the physical protection system is usually well maintained, tested and evaluated. The necessary resources are made available for periodic improvement.
3 COMPLIANT	The physical protection system takes into account identified threats and adheres to the security expectation, such as regulatory requirements. The organisation has implemented expected provisions for deterrence, detection, delay and response and for following a defence in depth and graded approach toward security. Source operation, radiation safety and radiation security departments rarely communicate with each other. The overall effectiveness of the system is tested or evaluated only when required.
4 REACTIVE	The physical protection system adheres to security expectations but nothing more. The organisation has implemented basic provisions for deterrence, detection, delay and response and for following a defence in depth and graded approach toward security. Source operation, radiation safety and radiation security are all separate departments that rarely communicate with each other. The physical protection system is maintained at a minimal level. The overall effectiveness of the system is rarely tested or evaluated.
5 VULNERABLE	The physical protection system generally adheres to the basic security expectations requirements, but sometimes falls short. The organisation has implemented a few elements of deterrence, detection, delay and response, but has not taken a systematic approach for doing so. Source operation, radiation safety and radiation security do not communicate with each other. The maintenance of the physical protection system is minimal.

C. RESPONSE TO SECURITY INCIDENTS

Introduction

Response refers to the action undertaken by onsite security (if present) and/or off-site law enforcement to interrupt and subdue an adversary while the malicious act is in progress. In order to be successful, response time needs to be shorter than the time required to perform a malicious act, and response forces capabilities greater than those of the adversaries. Response to security events need to be implemented in accordance with security procedures and response arrangements need to be periodically practiced in close coordination with law enforcement. External responders need to be familiar with the irradiator site and educated to the radiological risk.

Examples of indicators demonstrating the capacity of the organisation to effectively respond to a security incident:

- There is a written document describing the response arrangements in case of an incident involving the Co-60 sources. Both the operator and the response organisation have approved this document.
- The response arrangements are periodically tested, and the lessons learned are used for continuous improvement.
- First responders are periodically invited to visit the site and understand radiological matters. The security manager and the response force supervisor know each other. Response forces have access to information characterising the site and its risks.
- There are independent redundant communication means between the site and offsite alarm locations and the response force. Remote monitoring capabilities are in place for those with the responsibility to assess alarms.
- Response forces have necessary capabilities to overcome the expected threat.

EXAMPLE QUESTIONS FOR RESPONSE ARRANGEMENTS

QUESTION	ANSWER FROM THE FACILITY	SOURCE OF THE INFORMATION*	COMMENTS
Can you explain what happens between the activation of an alarm and the intervention of the response force? Can you describe the role of the staff and the role of external organisation(s)? Who makes the decision to activate an external response?			
Who is providing the offsite response to the facility in case of an incident? Is there an MoU or similar arrangement between the facility and the response force(s)? When was the last time you met with a representative of the off-site response force?			
How long does it take for the response force to arrive? To deploy? How many individuals comprise the first response? What kind of response equipment do they have? Do they have remote access to your video feeds?			
How often do you test response procedures? What was the main lesson learned from the last exercise? How familiar would the first responder be with the facility and the associated radiological security risk?			
How often do you test response procedures? What was the main lesson learned from the last exercise? How familiar would the first responder be with the facility and the associated radiological security risk? Have you conducted induction training for the response force (e.g., familiarisation of the facility, radiation protection, etc.)? Do you have a set of documents/ information ready to be provided to the responders?			
Have you tested the times for adversaries to complete the scenarios of concern and compared them to the response time?			

* Observation (location of the observation); or Document (reference for the document); or Interview (name and function of the interviewee).

GUIDANCE AND TIPS FOR EXTERNAL REVIEWS

- To save time, it might be more efficient to split responsibilities between team members and conduct a review of the physical protection and response arrangements in parallel.

Maturity Scale:

LEVEL	CHARACTERISTICS
1 RESILIENT	There is strong communication between the operator and the off-site response force, who have been trained in both radiation security and radiation safety so that they know how to respond if an incident occurs. Site/target files exist for all radio-active sources in use and storage, and they are complete and up to date.
2 PROACTIVE	The operator and off-site response force (e.g. the police) have met each other, and the officers have received basic training on radiation security and radiation safety in the event of an incident. Site/target files exist for most of the radioactive sources in use and storage, and they are usually complete and up to date.
3 COMPLIANT	The operator and off-site response force (e.g. the police) have met each other briefly, and officers have received basic training on radiation safety but not on radiation security. Site/target files exist for most radioactive sources and are occasionally updated.
4 REACTIVE	The operator and off-site response force (e.g. the police) have not met each other, and no officers have received any training on either radiation safety or radiation security. Site/target files exist for major radioactive sources, but they are rarely updated.
5 VULNERABLE	The operator and off-site response force (e.g. the police) have not met each other, and no officers have received any training on either radiation safety or radiation security. Furthermore, there are no site/target folders.

D. SECURITY CULTURE AND AWARENESS

Introduction

Security culture is one of the most important aspects of effective security. Security culture begins at the top and filters from there throughout the rest of the organisation. Leadership must lead by example and clearly demonstrate that a credible threat exists and that security of radioactive sources is important and must be treated as a business risk similar to safety. In an organisation with a strong security culture, staff believe that security threats are real, understand that it is their responsibility to contribute to the security of the entire organisation, and adhere to security practices as a normal part of their daily work lives. If they observe an anomaly or hear something suspicious, they report it unhesitatingly to their supervisor. If they make a mistake themselves, they willingly own up to it, seek to understand how it occurred, and work actively to improve their performance. If they have ideas or suggestions to improve security, they share them with their managers and colleagues because they know such contributions are encouraged, respected and rewarded.

It is important that organisations identify positions that require security skills and knowledge. Managers should ensure that individuals filling these positions are demonstrably competent through a combination of education, training and on-the-job experience. Employee engagement in security matters and undertaking professional development opportunities is encouraged.

Examples of indicators demonstrating organisational security awareness and culture:

- Senior management and staff believe that threats to their Co-60 sources exist and that good security can mitigate the threat.
- Senior management promote a robust security culture through clearly defined roles, responsibilities and training.
- Induction programmes for staff include security elements.
- Staff has access to professional development and training in security as appropriate for their positions.
- The organisation has a programme in place that encourages staff to share their security concerns and there is evidence that prompt action is taken when necessary.
- Security non-compliance is taken seriously.

EXAMPLE QUESTIONS FOR SECURITY AWARENESS AND CULTURE ARRANGEMENTS

QUESTION	ANSWER FROM THE FACILITY	SOURCE OF THE INFORMATION*	COMMENTS
Do senior managers believe that the threat to radioactive sources is real? How do you know this?			
Do senior managers and staff believe that effective security can manage the risk? How do you know this?			
How would you describe the organisation security culture?			
Do senior managers believe that an effective security culture is just as important as an effective safety culture?			
Do senior managers demonstrate their personal commitment to security through words and actions?			
Are staff encouraged to share their security con-cerns? Do you have example of such concerns? When was the last time you had a group discussion on security?			
Is there evidence of follow-up action when security concerns are expressed by staff?			
Does the organisation (or staff) participate in national or international forums related to radiological security? If you had a question on radiological security, where would you find the answer?			
Question to each interviewee: If you could improve one thing in the security approach or implementation, what would that be?			

* Observation (location of the observation); or Document (reference for the document); or Interview (name and function of the interviewee).

GUIDANCE AND TIPS FOR EXTERNAL REVIEWS

Experience shows that staff tend to feel that radioactive sources are self-protecting and very difficult or impossible to illicitly remove. This issue needs to be reviewed during the assessment. If interviewed staff display such beliefs, further discussion – including describing selected basic scenarios – could be conducted between the assessor(s) and staff.

Maturity Scale:

LEVEL	CHARACTERISTICS
1 RESILIENT	Security is recognised as an essential element of the business, and maintaining an effective, performance-tested security programme is seen as a core company value. All staff give high priority to security, and there is no sense of security complacency at any level of the organisation. All employees share the belief that security is a critical aspect of their job and that they share responsibility for preventing security incidents. Employee engagement is excellent, with multiple opportunities for feedback and learning from experience.
2 PROACTIVE	The majority of staff in the organisation believe that security is important. Management understand that security vulnerabilities can be caused by a variety of events and that their behaviour needs to constantly reinforce the importance of effective security arrangements. Staff take appropriate action when security weaknesses are identified. The organisation puts significant effort into proactive measures to prevent security weaknesses, including employee engagement and the testing of arrangements.
3 COMPLIANT	Security is recognised as an important business risk and full compliance with regulatory and corporate requirements is expected. Security arrangements are in place and security weaknesses are corrected as soon as they are detected. A majority of staff is prepared to support the security objectives and to take personal responsibility for their own security and those around them. Further employee engagement is developing, and security briefings allow feedback from staff.
4 REACTIVE	Security is seen in terms of regulatory compliance and the adherence to rules and procedures that have been set by the regulator. Security is reluctantly seen as a business risk; senior management view it as an unavoidable financial overhead and believe the risk of an incident is extremely small. Employee engagement is limited to periodic briefings about security rules. Senior managers are reactive to their involvement in security. Staff comply with security rules, but they consider them to be intrusive.
5 VULNERABLE	Security is defined and thought about only in terms of compliance with regulations at a minimum cost. Security is not seen as a key business risk, and the postulated threats are not considered to be real. Security is seen as the sole responsibility of the security staff. Security violations and shortcuts in procedures are not considered serious. Most staff are uninterested in security and see it as an obstacle to getting their work done.

E. CYBERSECURITY

Introduction

Following the global trend in all sectors and activities, security system components are more and more reliant on digital technologies and associated information technology (IT) infrastructures. These components include operations, communications, alarm monitoring and fundamental elements of the intrusion detection, access control and alarm assessment system. If not properly protected, these elements are vulnerable to cyberattacks that could degrade the performance of the physical protection system and lead to vulnerabilities in the security of the radioactive sources themselves. Basic cybersecurity measures include measures such as maintaining software up-to-date, separating the security system network from other irradiator or business ones where possible, and selecting only IT elements of the security system meeting highest industry standards.

Examples of indicators demonstrating the capabilities of the organisation to identify and manage cybersecurity risks:

- Senior managers are aware of the cybersecurity risk.
- Cybersecurity is part of the overall risk management approach.
- Processes and equipment sensitive to cyber threats have been identified and assessed.
- Cybersecurity of IT & OT infrastructure is periodically evaluated and identified weaknesses are addressed in a timely manner.
- Cybersecurity is part of the induction training of each member of the staff.
- Cybersecurity risks for the physical protection system have been identified and compensatory measures prepared in case of a cybersecurity incident.

EXAMPLE QUESTIONS FOR CYBERSECURITY ARRANGEMENTS

QUESTION	ANSWER FROM THE FACILITY	SOURCE OF THE INFORMATION*	COMMENTS
Do senior managers believe that there are cyber threats to the organisation? How do you know this?			
Is cybersecurity part of the overall risk management strategy?			
What is your primary concern regarding cyber threats (e.g., operation disruption, loss of customer data, etc.)?			
What are your organisational arrangements for cyber security? Who has the overall responsibilities for cybersecurity?			
What is your reference for designing and implementing your cybersecurity programme?			
Are you implementing physical security arrange-ments to limit access to sensitive computer hardware, wiring, displays, and network devices?			
What kind of in-house capabilities did you build? What is the role of external contractors?			
Are staff aware of the cybersecurity risk and informed of the necessary mitigation measures?			
What kind of awareness and training opportunities are offered to the staff?			
Is the effectiveness of the cybersecurity measures periodically tested? When was the last penetration test conducted? What were the results? Was any follow-up given?			
Do you know if your physical protection arrangements could be impacted by cyber attacks? Are physical security arrangements reviewed in light of their possible cyber vulnerabilities?			

* Observation (location of the observation); or Document (reference for the document); or Interview (name and function of the interviewee).

GUIDANCE AND TIPS FOR EXTERNAL REVIEWS

Compared to other security issues, cybersecurity is a more recent and more specialised area. Specific attention needs to be given to demonstrate cybersecurity skills within the assessment team. Peer reviews can be a very good opportunity for raising awareness amongst the host facility staff and share lessons learned by the industry.

Maturity Scale:

LEVEL	CHARACTERISTICS
1 RESILIENT	The entire organisation understands that cyber threats exist. Cybersecurity is integrated into the overall risk management strategy and is a recognised process in the management system. The IT & OT infrastructure is understood in detail, and a process for managing changes in the environment is in place. The organisation regularly conducts penetration testing. A process is in place to keep hardware and software in the environment up to date and patched for new vulnerabilities. Operations, security and IT staff regularly hold joint meetings to discuss issues and know exactly what to do should a cyber attack occur. Furthermore, the responsibilities of suppliers, vendors and outsourcers have also been clearly defined, and the process of lever-aging each other's knowledge and expertise is ongoing.
2 PROACTIVE	Management understand that cyber threats exist and the need for cybersecurity has been incorporated into the security policy. The IT & OT infrastructure is understood in detail, and a process for managing changes in the environment is in place. The organisation conducts penetration testing from time to time. Operations, security and IT staff have regular meetings. Should a cyber attack occur, the responsibilities of each department have been clearly defined, and joint training and practice have taken place to ensure that all responsible parties know exactly what actions to take and when to take them. Furthermore, security discussions with vendors and experts have started.
3 COMPLIANT	Senior management believe cyber threats are real. As a result, they have charged people with knowledge of the IT & OT infrastructure to put cybersecurity measures in place. Detailed documentation has been created that provides a comprehensive overview of the IT infrastructure. A rudimentary monitoring process is in place. Operations, security and IT staff have fairly regular contact with each other and generally know who would be responsible for taking which actions should a cyber attack occur. Management know which outside organisations to contact for information about cyber threats and for help should a cyber incident occur, and they have begun to develop regular contacts with them.
4 REACTIVE	A few managers believe the cybersecurity threat is real, but their view is not shared widely by other managers in the company. The IT staff handles firewalling, patch management and monitoring for business IT systems, but similar activities do not fully occur in the process control domain and for the security system. Management have instituted a few procedures to test the effectiveness of cybersecurity measures, but they are not applied systematically. Operations, security and IT staff have only informal, irregular contact with each other. They have a generic understanding of each other's interests, methods and definitions, but no joint, cross-disciplinary training is conducted. Nor do they know who would be responsible for what should a cyber event occur. Management know which outside organisations to contact for information about cyber threats and for help should a cyber incident occur, but they have no formal contact with them.
5 VULNERABLE	Senior management do not believe that cyber threats to the process or the security system are real. The IT staff handles fire-walling, patch management and monitoring for business IT systems, but similar activities do not occur in the process control domain and for the security system. There are no procedures to test the effectiveness of the cybersecurity measures. Operations, security and IT staff have little contact with each other and do not know who would be accountable for what should a cyber attack take place. Management do not know which outside organisations are responsible for notifying them if a cyber threat were developing or who could help them should an attack occur.

F. INFORMATION SECURITY

Introduction

Information that could compromise Co-60 source security is sensitive and needs to be protected. This includes information related to the security plan, access codes, alarm system codes/passwords and intimate details of the physical security element. It also includes the Co-60 source inventory, operational procedures, computer systems, transport timing and routes (for both Co-60 and products for radiation processing), as well as technical data, blueprints, schematics, designs, security procedures and emergency response plans. Information protection involves the development, implementation and maintenance of written policies and procedures that describe how to handle sensitive information and protect it from unauthorised disclosure. Information protection policies and procedures should follow the concept of graded approach. Operators should evaluate an individual's need to know before allowing access to security documents.

Examples of indicators demonstrating the capabilities of the organisation to identify and securely manage sensitive information:

- Sensitive information has been identified and graded in order of the seriousness of the consequences of unauthorised disclosure.
- Information relating to the Co-60 sources, its location, access and movement is treated on a "need to know" basis.
- Clear written policies and procedures are in place regarding the storage, use and dissemination of sensitive information.
- There are physical and IT measures in place to control access to sensitive information.
- Staff who need access to sensitive information are subject to background checks and granted access on a "need to know" basis.
- Staff receive training in information security upon hire and at regular intervals thereafter.

EXAMPLE QUESTIONS FOR INFORMATION SECURITY ARRANGEMENTS

QUESTION	ANSWER FROM THE FACILITY	SOURCE OF THE INFORMATION*	COMMENTS
Is information security part of the overall risk management strategy?			
How does the organisation identify, mark and record information determined to be sensitive?			
Has the organisation developed procedures de-scribing how sensitive information needs to be handled and protected? Do you have a graded ap-proach to categorise and protect information? Do the procedures include actions to be taken in case of unauthorised disclosure?			
Are staff and contractors who need access to sensitive information subject to background checks?			
Have staff received specific training or awareness sessions on the need for information security?			

* Observation (location of the observation); or Document (reference for the document); or Interview (name and function of the interviewee).

GUIDANCE AND TIPS FOR EXTERNAL REVIEWS

Prior to conducting the assessment, the review team is encouraged to identify corporate and national requirements related to the management of sensitive information, including their identification and protection.

Maturity Scale:

LEVEL	CHARACTERISTICS
1 **RESILIENT**	Senior management view information security as an integral part of risk management and sensitive information related to the operation of the facility or the security measures have been identified and categorised based on the consequences in case of disclosure. Comprehensive procedures describe how sensitive information needs to be handled and protected. All staff and contractors who need access to sensitive information are subject to background checks. All employees receive training in information security upon hire and at regular intervals thereafter. All contractors also receive basic and refresher training and must adhere to specific guidelines when handling sensitive information. The organisation periodically conducts exercises on information security.
2 **PROACTIVE**	Senior management take their responsibility for managing information security seriously. Consequently, they have identified sensitive business and security information and put clear written policies and guidance in place for staff and contractors. Policies and physical security measures have been put in place that control access to sensitive information. All staff who need access to sensitive information are subject to background checks. All employees receive training in information security upon hire and at regular intervals thereafter. All subcontractors and suppliers also receive basic and refresher training and must adhere to specific guidelines when handling sensitive information and subcontracting their work to others.

3 **COMPLIANT**	Senior management believe the organisation is responsible for information security. They have identified sensitive business information and the sensitive security information as prescribed by regulations. Staff who need access to sensitive information are subject to background checks. The organisation has developed a written information security policy that is occasionally reviewed and revised. All staff who need access to sensitive information are subject to background checks. All employees receive training in information security when they are recruited.
4 **REACTIVE**	Senior management believe the organisation has some responsibility for information security. They have identified some sensitive business and security information. Employees undergo background checks at the time they are recruited, but the results are not necessarily tied to access to information. Employees receive some basic training in information security when recruited, but no refresher courses take place. Contractors also receive some training in information security policies, but the policies are not enforced in the contract.
5 **VULNERABLE**	Senior management do not believe the organisation has specific responsibility for information security. Consequently, they have not created any specific policies or oversight measures for it. Employees undergo background checks at the time they are recruited, but the results are not tied to access to information. No employees have received training in information security policies and procedures, and neither have any contractors.

G. PERSONNEL SECURITY

Introduction

Insiders are individuals (such as employees, contractors and suppliers) who have authorised access to a facility, transport operation, sensitive information, or computer and communications system who use their trusted position for unauthorised purposes. Insiders are particularly dangerous because they could use their access, authority and knowledge of a facility to bypass dedicated physical protection, safety measures and operating procedures. They can also have more time to select vulnerable targets and carry out a malicious act. The organisation needs to implement a comprehensive set of policies, security measures and procedures to manage internal threats. Operators need to know that their staff can be trusted. Vetting helps to determine the trustworthiness and reliability of potential staff and is a key measure in mitigating the threat posed by insiders. The process can range from a simple confirmation of identity to a comprehensive background check conducted by the national authority. Strong internal controls, a culture of teamwork and high behavioural standards provide the foundation of personnel security and encourage staff to report observations and information that could indicate a potential security concern.

Examples of indicators demonstrating the capabilities of the organisation to achieve personnel security:

- Senior management believe the insider threat is credible.
- The security plan specifically addresses the insider threat and related mitigation measures.
- The staff are subject to initial and periodic background and trustworthiness checks.
- The separation of duties, two-person rule and other security arrangements are in place.
- The staff are trained to notice suspicious behaviours and would report them to management.
- There is evidence that senior management would take action in case of a report of suspicious behaviour.

EXAMPLE QUESTIONS FOR PERSONNEL SECURITY ARRANGEMENTS

QUESTION	ANSWER FROM THE FACILITY	SOURCE OF THE INFORMATION*	COMMENTS
Do senior managers believe that an insider threat is credible? How do you know this?			
Has the organisation developed a programme to specifically address the insider threat?			
Does staff believe that an insider threat is credible and that adequate mitigation measures have been taken? How do you know this?			
Are you conducting any background checks when recruiting new employees? Are people with security responsibilities subject to additional trustworthiness requirements?			
Would staff report suspicious behaviours from staff, including senior managers and contractors?			
Is there a sanction process for staff not complying with security procedures?			

* Observation (location of the observation); or Document (reference for the document); or Interview (name and function of the interviewee).

GUIDANCE AND TIPS FOR EXTERNAL REVIEWS

Experience shows that, in particular for small organisations with a stable workforce, it is difficult to convince staff that the insider threat is credible. The review team is encouraged to identify relevant case studies in advance and share them with staff that they meet during the assessment process, if appropriate.

Maturity Scale:

LEVEL	CHARACTERISTICS
1 RESILIENT	The organisation takes the insider risk seriously and has developed and implemented specific mitigation measures. A comprehensive trustworthiness programme, including vetting procedures, has been implemented, and the security and human resources departments work hand-in-hand. Security procedures clearly define roles and responsibilities, the separation of duties, and access to sensitive materials and locations. Staff and contractors strongly support measures taken to reduce the internal risks and believe this is important for their work, personal safety, and the reputation of the organisation. Employees quickly notice suspicious behaviour thanks to the organisational culture, and a reporting policy has been implemented and is encouraged.
2 PROACTIVE	The organisation believes that implementing policies, security measures and procedures to manage internal threats is important. Trustworthiness programmes and practices, including employee vetting, have been implemented. The staff considers periodic vetting acceptable. Management recognise the value of strong internal controls and encourage a culture of teamwork and high behavioural standards. Strong and effective action is taken against individuals who violate the behavioural norms of the organisation. Security awareness programmes, including supervisor training, address potential internal threats and the need for vigilance. There is a good level of access control, and the separation of responsibilities is enforced. Staff feel comfortable reporting observations and information that could indicate a potential internal threat.
3 COMPLIANT	The organisation has implemented some policies, security measures and procedures for managing internal threats. The responsibility for managing internal threats is seen as belonging to the Security Department. Trustworthiness programmes that include employee vetting on recruitment are in place but have a limited scope. Contractors are not given the same attention as staff. Insider risks and vulnerabilities have been assessed and access control measures are in place. Insider risk is quoted in se-curity awareness programmes. Staff occasionally report observations or information that could have ramifications for a potential internal threat, and there is modest interest from facility management.
4 REACTIVE	Management have considered policies, security measures and procedures for managing internal threats, but they have not yet implemented them effectively. Management doubt they are really necessary. No security clearance process is being implemented. The organisation reassesses risks and vulnerabilities, including internal threats, only after an incident has occurred. Some security awareness programmes that address potential internal threats have been established for staff but are not mandatory. Staff are not particularly encouraged to report observations or information about fellow employees and therefore are reluctant to do so.
5 VULNERABLE	Senior management seldom considers the risks and vulnerabilities surrounding internal threats. As a result, they have not implemented any policies or procedures to counter potential internal threats and have instituted no requirements to do so. Trustworthiness programmes have not been put in place for staff and contractors. Security awareness programmes and the training of supervisors and managers to address potential internal threats have not been established. Staff do not believe it is their responsibility to report unusual behaviour of fellow employees and contractors to management, and there is no systematic monitoring of unacceptable behaviour. The separation of responsibilities for access to sensitive locations and materials is frequently overlooked or not enforced.

APPENDIX 1 – EXAMPLE AGENDA FOR AN EXTERNAL ASSESSMENT

Review Ref: *#006*	**Review Date:** *1–2 June 2024*	**Reviewed Company/Site:** *Gamma Irradiation Co. / Ruritania site*
Review Purpose	*Security Assessment*	
Objectives:	*To assess, rate and report on the effectiveness of security arrangements*	
Scope:	*Whole site/organisation but with particular focus on security arrangements covering Cobalt-60 sources located onsite. The scope includes: security management; physical protection systems; response to a security incident; security culture.*	
Review Team:	*Name 1*	*Lead Reviewer*
	Name 2	*Reviewer*
Host Key Contact	*Name 3*	*Director of Security*
	Name 4	*Radiation Safety Manager*

REVIEW AGENDA

Day 1			
Time	Activity	Host Participants	Comments
08.30	*Opening meeting*	*Host key contacts*	*Review of local rules, site plan and agenda*
9.30	*Desktop review of Security Plan*	*None (reviewers only)*	*Host key contact to be available to answer questions*
11.00	*Review of physical security arrangements*	*Reviewers and host key contacts*	*Perimeter and irradiator building*
12.30	*Review of detection and onsite alarm arrangements*	*Irradiator Operations Manager*	*Will require access to irradiation cell to test sensors*
15.00	*Review of communication procedures with offsite response forces*	*Host key contact*	*Includes review of agreements in place with third parties*
Etc.	*Etc.*		

Day 2			
Time	Activity	Host Participants	Comments
08.30	*Review of personnel security, staff vetting and training*	*HR Manager*	*A selection of training records should be made available*
10.00	*Interview with staff to assess level of security awareness and engagement*	*5 members of staff*	*Members of staff to be selected by reviewers and from range of duties*
12.00	*Review cybersecurity and security of information*	*IT Manager*	
13.00	*Drafting of the report*	*N/A*	*Time reserved for final clarifications*
17.00	*Closing meeting*	*Reviewers and host key contacts*	*Review findings, agree on follow-up action plan and priorities*

APPENDIX 2 – EXAMPLE REPORT

Security Assessment Report - CONFIDENTIAL

Review Ref: *#006*	**Review Date:** *1–2 June 2024*	**Reviewed Company/Site:** *Gamma Irradiation Co. / Ruritania site*
Review Purpose	*Assessment of selected security arrangements*	
Objectives:	*To assess, rate and report on the effectiveness of selected security arrangements*	
Scope:	*Whole site/organisation but with particular focus on security arrangements covering Cobalt-60 sources located onsite. The scope included: security management; physical security; response to security incident; security culture.*	
Review Team:	*Name 1*	*Lead Reviewer*
	Name 2	*Reviewer*
Key Contact	*Name 3*	*Director of Security*
	Name 4	*Radiation Safety Manager*

1. ASSESSMENT RATING

The effectiveness of the seven areas of security was benchmarked against similar facilities and industry best practice and compared with the following maturity scale:

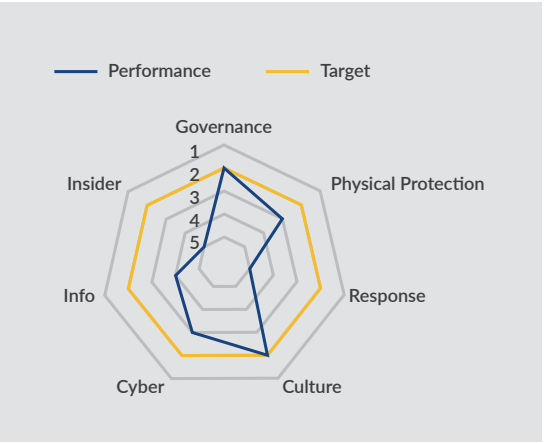
LEVEL	ASSESSMENT
1 RESILIENT	The facility greatly exceeds expectations in this security area. The facility is considered a leader in this area and best practices from this facility should be shared with other similar facilities.
2 PROACTIVE	The facility meets and meaningfully exceeds expectations in this area.
3 COMPLIANT	The facility meets expectations in this area.
4 REACTIVE	The facility does not currently meet expectations in this area and requires corrective actions.
5 VULNERABLE	The facility is far from meeting expectations in this area and requires immediate corrective actions.

2. EXECUTIVE SUMMARY

The result of this assessment is summarised in this image.

This illustrates that security governance and culture, and physical and cybersecurity meet or exceed expectations. Areas where the facility fails to have effective security and where corrective action is necessary are in incident response and the control of the insider threat and information security.

The seven individual areas of security, along with observations and recommended actions are detailed in the following section of the report.



3. ASSESSMENT OF INDIVIDUAL SECURITY AREAS

The priority of recommended corrective actions is rated 0–3.

PRIORITY	DESCRIPTION
0	No action required.
1	Security in not effective. There is a significant security vulnerability and very short-term action is recommended.
2	Security effectiveness is reduced. Short-term action is recommended to improve security effectiveness.
3	Security effectiveness is not significantly impaired but there is scope for improvement. Mid-term action is recommended.

(i) Physical protection

No.	ITEM	PRIORITY	OBSERVATIONS	RECOMMENDATIONS
1	*Deterrent features*	0	*Security fencing and highly visible signage and CCTV in place*	*None*
2	*Pool cover*	0	*Solid cover with security fittings is installed*	*None*
3	*Temporary operations*	3	*Security plan does not cover temporary storage of sources prior to installation*	*Update security plan prior to next source delivery*
4	*Source installation tools*	2	*Source installation tools are stored in an unsecure area*	*Store source installation tools in a locked area with controlled access*
3 COMPLIANT		The facility meets expectations in this area.		

(ii) Security Culture

No.	ITEM	PRIORITY	OBSERVATIONS	RECOMMENDATIONS
1	*Personnel interviews*	0	*There was a strong understanding of security and what action to take if a vulnerability is identified*	*None*
2	*Insider threat*	0	*There is a comprehensive formal process for vetting staff*	*None*
3	*Training*	3	*All staff are offered security training, but this is not recorded by HR*	*Formalise security training and record in personnel training records*
2 PROACTIVE	The facility meets and meaningfully exceeds expectations in this area.			

SIGNATURE

Signature of Lead Reviewer	Name	Date

APPENDIX 3 – MATURITY SCALE FOR THE OVERALL SECURITY PERFORMANCE OF THE FACILITY

The following chart, derived from *Appendix B of WINS' Security of Radioactive Sources in Industrial Radiation Processing* BPG, presents the five levels of organisational maturity for ensuring the security of radioactive sources at a gamma irradiation facility.

LEVEL	CHARACTERISTICS
1 **RESILIENT**	Executive management demonstrate their conviction that a threat exists and that security is important by treating security as an integral part of corporate risk, by taking a risk-informed approach toward security, and by taking a whole-life approach toward the management of their radioactive sources. Executive management have put a programme in place to encourage a positive security culture. This includes a human reliability programme that helps to ensure the trustworthiness and reliability of all staff and a programme for sharing concerns. It also includes conducting training in security matters at least annually. The design of the physical protection system successfully balances deterrence, detection, delay and response elements and functions. It also follows a defence in depth and graded approach toward security. Security measures are well coordinated with source operation and radiation safety, and the physical protection system is regularly maintained, tested and evaluated. Staff believe that a potential threat exists to the organisation's radioactive sources, that security is important, and that they have personal responsibility for security. They have been trained in how to keep sensitive information secure, how to recognise red flag behaviours, and how to respond should an incident occur. They are also willing to share any security concerns because they know that management welcomes them and will take appropriate action while insuring confidentiality. There is strong communication between the operator and the offsite response force, who have been trained in both radiation security and radiation safety so that they know how to respond if an incident occurs. Site/target files exist for all radioactive sources in use and storage, and they are complete and up to date.

LEVEL	CHARACTERISTICS
2 **PROACTIVE**	Executive management generally believe that a threat exists and that security is important. They are beginning to treat security as an element of corporate risk and are usually successful at taking a risk-informed approach toward security. They also take a whole-life approach toward the management of radioactive sources. Executive management have put a programme in place to encourage a positive security culture. This includes a human reliability programme that helps to ensure the trustworthiness and reliability of all staff and a programme for sharing concerns. It also includes conducting refresher training in security every two to three years. The design of the physical protection system balances deterrence, detection, delay and response elements and functions. It also follows a defence in depth and graded approach toward security. Security measures are fairly well coordinated with source operation and radiation safety, and the physical protection system is usually well maintained, tested and evaluated. Most staff believe that a potential threat exists to the organisation's radioactive sources, that security is important, and that they have personal responsibility for security. They have been trained in how to keep sensitive information secure, understand what red flag behaviours are, and can recognise some of them. Staff are willing to share major security concerns on an anonymous hotline, and they have a good idea about what to do if an incident occurs. The operator and offsite response force (police) have met each other, and the officers have received basic training on radiation security and radiation safety in the event of an incident. Site/target files exist for most of the radioactive sources in use and storage, and they are usually complete and up to date.

LEVEL	CHARACTERISTICS
3 **COMPLIANT**	Executive management generally understand that a threat exists, that security is important, and that it would be a good idea to treat security as an element of corporate risk. They have also begun to create policies and procedures that would support taking a risk-informed approach toward security. Executive management have briefly addressed what to do with disused sources that reach the end of their lives. Executive management generally understand the importance of a positive security culture and have put some measures in place to improve it, such as better vetting of new staff and addressing security in the overall training that new hires receive. Current staff occasionally receive refresher training in security, but not on a fixed schedule. The physical protection system adheres to the basic regulatory requirements, but nothing more. The organisation has implemented simple provisions for deterrence, detection, delay and response and for following a defence in depth and graded approach toward security. Source operation, radiation safety and radiation security are all separate departments that rarely communicate with each other. The physical protection system is maintained at a minimal level. The overall effectiveness of the system is rarely tested or evaluated. In general, staff believe that a potential threat exists to the organisation's radioactive sources and that security is important, but they do not understand their personal responsibilities for security. They have been trained in how to keep sensitive information secure but have not been trained about red flag behaviours. There is a 24-hour hotline available to someone who wants to share security concerns, but it is rarely used. Staff have a basic idea about what to do if an incident occurs. The operator and offsite response force (police) have met each other briefly, and officers have received basic training on radiation safety, but not on radiation security. Site/target files exist for most radioactive sources and are occasionally updated.

LEVEL	CHARACTERISTICS
4 **REACTIVE**	Executive management do not believe their facility faces any real security threats. They assume the radiation safety officer/security director is solely responsible for security. Because they do not believe that security is an issue, they do not treat it as an element of corporate risk, nor do they take a risk-informed approach toward security. Executive management purchase and use radioactive sources according to regulatory requirements, but they have not addressed what to do with disused sources. Executive management vaguely understand what security culture means but have put no measures in place to test, measure or improve it. Staff receive a handout on security issues when they are hired, but that is the extent of their training. The physical protection system adheres to the basic regulatory requirements but nothing more. The organisation has implemented basic provisions for deterrence, detection, delay and response and for following a defence in depth and graded approach toward security. Source operation, radiation safety and radiation security are all separate departments that rarely communicate with each other. The physical protection system is maintained at a minimal level. The overall effectiveness of the system is never tested or evaluated. Staff do not believe that a potential threat exists to the organisation's radioactive sources, nor do they understand that they have security responsibilities. They have received a brief introduction on how to protect sensitive information but do not understand or recognise red flag behaviours. There is a 24-hour hotline, but staff do not use it. Staff have only a vague idea about what to do if an incident occurs or who would be in charge. The operator and offsite response force (police) have not met each other, and no officers have received any training on either radiation safety or radiation security. Site/target files exist for major radioactive sources, but they are rarely updated.

LEVEL	CHARACTERISTICS
5 **VULNERABLE**	Executive management do not believe their facility faces any security threats. They assume that the radiation safety officer/security director is solely responsible for security. Radioactive sources are generally purchased according to regulatory requirements, but no provision has been made for disused sources. Executive management do not consider security culture to be a risk. The only emphasis in staff training is on safety issues. The physical protection system generally adheres to the basic regulatory requirements but sometimes falls short. The organisation has implemented a few elements of deterrence, detection, delay and response, but has not taken a systematic approach for doing so. Source operation, radiation safety and radiation security do not communicate with each other. The maintenance of the physical protection system is minimal. Staff do not believe that a potential threat exists to the organisation's radioactive sources. Nor do they understand that they have security responsibilities. Furthermore, they have not received any training on how to protect sensitive information, there is no provision for sharing concerns, and they have no idea what to do if an incident occurs or who would be in charge. The operator and offsite response force (police) have not met each other, and no officers have received any training on either radiation safety or radiation security. Furthermore, there are no site/target folders.

5. SUGGESTIONS FOR FURTHER READING

IAEA Nuclear Security Recommendations. https://www.iaea.org/resources/security-series/search

No. 14. (2011). *Nuclear Security Recommendations for Radioactive Material and Associated Facilities.*

No. 11-G (Rev. 1). (2019). *Security of Radioactive Sources.*

No. 9-G (Rev. 1). (2020). *Security in the Transport of Radioactive Material.*

IAEA. (2014). Services Series No. 29. *International Physical Protection Advisory Service* (IPPAS) *Guidelines*. https://www.iaea.org/publications/10772/international-physical-protection-advisory-service-ippas-guidelines

WINS International Best Practice Guide Series. *Security of Radioactive Sources Used in Industrial Radiation Processing*. https://www.wins.org/knowledge-centre

WINS(24)10 ISBN: 978-3-903418-28-8

Landstrasser Hauptstrasse 1/18, 1030 Vienna (Austria)

+43 1 710 6519 | info@wins.org | www.wins.org

International NGO under Austrian Law BGBI. I Nr 54/2021 | GZ: StF: BGBI. II Nr 593/2021