PNNL-30464, Rev. 1

# Security Self-Assessment Toolkit for Nuclear Materials Facilities

## Focus on Insider Threat Mitigation

December 2021

Christine F Noonan
Jessica A Baweja
Madelyn P Dunning
H Lee Day

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

PACIFIC NORTHWEST NATIONAL LABORATORY
*operated by*
BATTELLE
*for the*
UNITED STATES DEPARTMENT OF ENERGY
*under Contract DE-AC05-76RL01830*

**Printed in the United States of America**

**Available to DOE and DOE contractors from the**
**Office of Scientific and Technical Information,**
**P.O. Box 62, Oak Ridge, TN 37831-0062;**
**ph: (865) 576-8401**
**fax: (865) 576-5728**
**email: reports@adonis.osti.gov**

**Available to the public from the National Technical Information Service**
**5301 Shawnee Rd., Alexandria, VA 22312**
**ph: (800) 553-NTIS (6847)**
**email: orders@ntis.gov <https://www.ntis.gov/about>**
**Online ordering: http://www.ntis.gov**

PNNL-30464, Rev. 1

# Security Self-Assessment Toolkit for Nuclear Materials Facilities

Focus on Insider Threat Mitigation

Christine F Noonan
Jessica A Baweja
Madelyn P Dunning
H Lee Day

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

# Summary

Theft or sabotage of weapons-usable nuclear materials is a global concern. To minimize this threat, establishing and maintaining an effective nuclear security regime is required to protect against criminal or other negligent acts. Use of a formalized insider threat mitigation program is one such security measure.

Individuals who have or held authorized access to an organization's critical assets, such as nuclear materials, are considered "insiders." Insider threats, or insider adversaries, are motivated individuals who possess access, authority, and knowledge to conduct a malicious act or facilitate that of an external party. To thwart insider threats (both intentional and unintentional), organizations can formalize an enterprise-wide approach to identify and mitigate the unique risks presented by insiders.

This report provides an approach to evaluate an insider threat mitigation program at facilities with nuclear materials. Formal program evaluations serve many purposes and can be designed using several different methods and techniques. This report presents a self-assessment approach to program evaluation whereby an organization can assess its strengths, identify key gaps, and set priorities for ongoing improvement efforts to mitigate insider threats. Results of the self-assessment can provide critical information to contribute to the continuous improvement of an organization’s insider threat mitigation program within eight specific domain areas.

# Acknowledgments

The authors express appreciation to the U.S. Department of Energy, National Nuclear Security Administration, Office of Global Material Security, for generous support of insider threat mitigation efforts domestically and internationally. Pacific Northwest National Laboratory is operated by Battelle for the U.S. Department of Energy under contract DE-AC05-76RL01830.

# Acronyms and Abbreviations

| | |
|---|---|
| DBT | design-basis threat |
| INSEN | International Nuclear Security Education Network |
| ITM | insider threat mitigation |
| NGT | nominal group technique |
| NMAC | Nuclear Material Accounting and Control |
| SBFD | scenario-based facilitated discussion |
| SMART | specific, measurable, accountable, reasonable, and time-bound |
| SWOT | strengths, weaknesses, opportunities, and threats |
| VA | vulnerability analysis |

# Contents

# Figures



# Tables

# 1.0 Introduction

The global threat to vulnerable nuclear materials has long been a concern. All documented cases of nuclear materials theft were perpetrated by or facilitated with the assistance of insiders who understood weaknesses in security systems (Bunn and Sagan 2016). While improvements have been made to secure nuclear materials and facilities internationally, alarmingly, the Nuclear Threat Initiative's Nuclear Security Index found progress has slowed significantly over the past two years (NTI 2020). The Nuclear Threat Initiative report highlights major weaknesses in key areas such as insider threat prevention and security culture.

To address this concern, countries must strengthen programs on nuclear security, adopt nuclear security regulations, and contribute to best practices on insider threat mitigation (ITM). In our increasingly complex social and technical environment, continuous improvement efforts are critical to stay ahead of evolving threats such as blended cyber-physical attacks and extremism.

Security succeeds when organizational leaders recognize and support operational contributions to enterprise integrity, proactive risk management, and overall business operations. Security program effectiveness can be measured in many ways, including vulnerability assessments, performance evaluations, penetration testing, etc. This report describes the role and benefits of program evaluation and provides a self-assessment toolkit to measure current state of practice and identify opportunities for ITM program improvements at nuclear materials facilities.

## 1.1 The Insider Threat

Insider threat is difficult to define as study of this threat crosses many disciplinary boundaries, from psychology to information security to law. Insider threats affect all industries and organizations. Although insider threat events involving radioactive or nuclear materials occur infrequently, when they do, there is a potential for huge consequences. Insider threats are challenging because most measures put in place by an organization to secure its physical, information, and human assets are oriented toward preventing unauthorized access. These measures, however, will not prevent authorized access by insiders who use their position, knowledge, and authority in ways not intended by the organization.

An insider is generally defined as a person who has, or once had, authorized access to an organization's critical assets (e.g., network, system, data, materials, or facilities). Being an insider does not make a person a threat. Malicious insider threats (sometimes referred to as insider adversaries) are individuals motivated to act in contravention of law or policy. Insider threat events include, but are not limited to, sabotage, theft, espionage, and fraud. Malicious actions may result in harm or degradation of organizational assets and are often carried out through abuse of access rights, overt or covert manipulation of people, and mishandling physical devices. In some organizations, malicious insider actions may also be defined as violent acts toward self or others (e.g., suicide, homicide, workplace violence), hate crimes, and harassment, to include stalking and inappropriate communications (in person, in writing, and online). Insider threats can also be unintentional (e.g., clicking a link in a phishing email) and still negatively affect the confidentiality, integrity, or availability of an organization's assets, or material protections, controls, and inventory levels.

There are two major categories of risk for insider attacks: personal motivations and contributing organizational characteristics. Malicious insiders are motivated by any number of things, including ideology, financial difficulties, stress, and even medical or psychological conditions.

These personal predispositions and external influences can provide an impetus for someone to commit an insider crime, facilitate a third party by sharing critical information, or take other malicious actions. Organizational factors also contribute to risk. Organizational factors that might increase the risk of insider threat include a hostile work environment, lack of or ineffective training, poor enforcement of rules, pressure to perform quickly, or a failure to address concerning behaviors in the workforce.

To thwart insider threats (intentional and unintentional), it is recommended that organizations formalize an enterprise-wide approach to identify and mitigate these compounding risk factors through development of an ITM program.

## 1.2 Insider Threat Mitigation Program

To address the unique threat posed by insiders, organizations with critical assets can and should develop ITM programs. An ITM program is focused on effective detection, deterrence, response, and mitigation of these threats and works to minimize risks to an organization's critical assets. Best practices in development of an ITM program is beyond the scope of this report. However, this report offers information for context.

Nuclear security components enacted to protect against insider threats are preventive and protective in nature (see Figure 1). Preventive measures refer to those actions undertaken by an organization to reduce the number of potential insider threats or minimize opportunity to commit an insider crime throughout the employee life cycle. Preventive actions may include vetting and credibility assessments such as conducting criminal and/or financial background checks and illicit substance screening on a random or periodic basis. Protective measures are tools, technologies, or techniques used to detect, delay, or respond to malicious acts or to mitigate consequences of an insider threat event.

Due to the distributed nature of security and safeguards functions within the nuclear enterprise, many departments are responsible for a distinct piece of preventive and protective measures—e.g., human resources, personnel security, protective force, material safeguards, information and cybersecurity, and counterintelligence. Viewed holistically, this multidisciplinary team of experts all contribute to the prevention, detection, deterrence, and mitigation of real and potential insider threats.

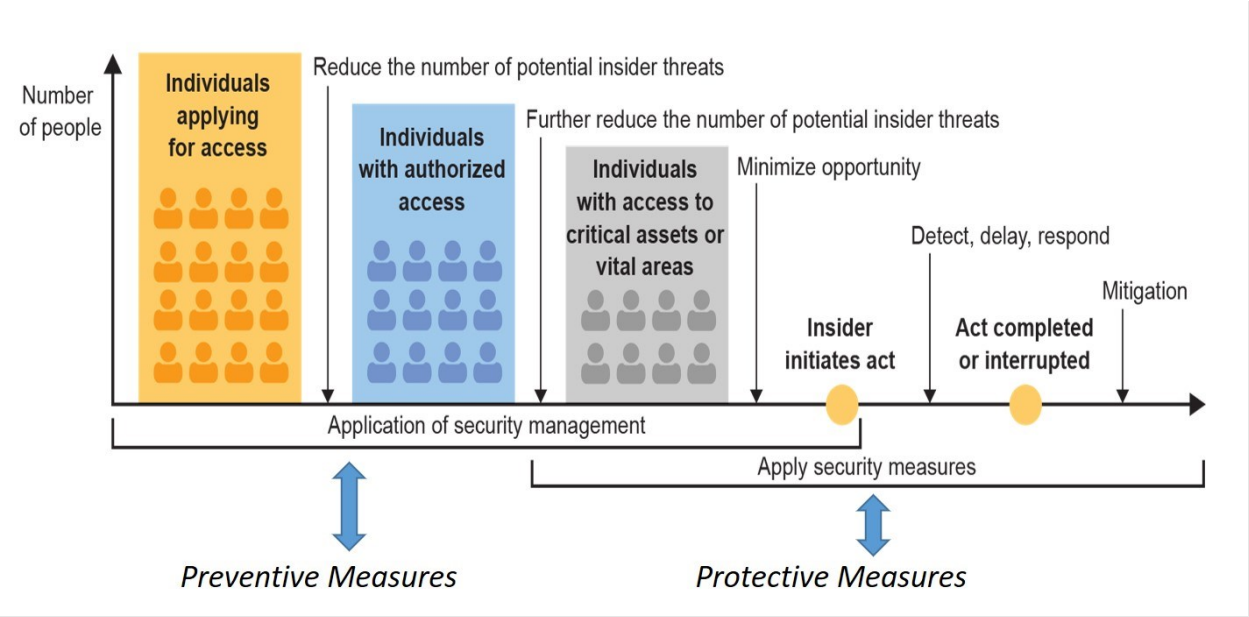


Figure 1. Measures to Minimize Insider Threats (adapted from IAEA 2020)

Unless specified by law or regulation, ITM programs can vary across different organizations. This variation is due to geographic location, the types and volume of nuclear materials and other critical assets, the size of the organization, the threat landscape, and other factors. Programs may operate in a formal or ad hoc fashion. At a minimum, a robust ITM program will be grounded in local, state, and national law and any applicable nuclear security regulations. From that foundation, an organization can develop a governance model, specific policies and procedures, and data and information-sharing agreements across business/departmental units. Programs may also be developed with input from industry guidance or best practices.

## 1.3 Value of Program Evaluation and Self-Assessment

After an ITM program is established, it should be evaluated periodically. Program evaluation can be defined as *the systematic assessment of a program designed to improve a specific condition or issue*. Evaluations serve many purposes, from assessing needs to estimating impacts and calculating cost-benefit ratios. Program evaluations can be designed using several different methods and techniques and can be loosely configured or highly structured. Evaluations can involve measurements, calculations, or observations, and can even be conducted by a third party. For a comprehensive look at program evaluation methods and techniques, see McDavid, Huse, and Hawthorn (2018) and Rossi, Lipsey, and Henry (2018).

Periodic evaluations generate useful information about the effectiveness of policy and program planning, and, through assessment of the results, allow the organization to document potential process enhancements, implement specific actions, and hold themselves accountable to continuous improvement. As a side benefit, evaluations can uncover unintended impacts of programs and policies. Figure 2 summarizes the five components of evaluation and the kinds of questions each component helps elucidate.

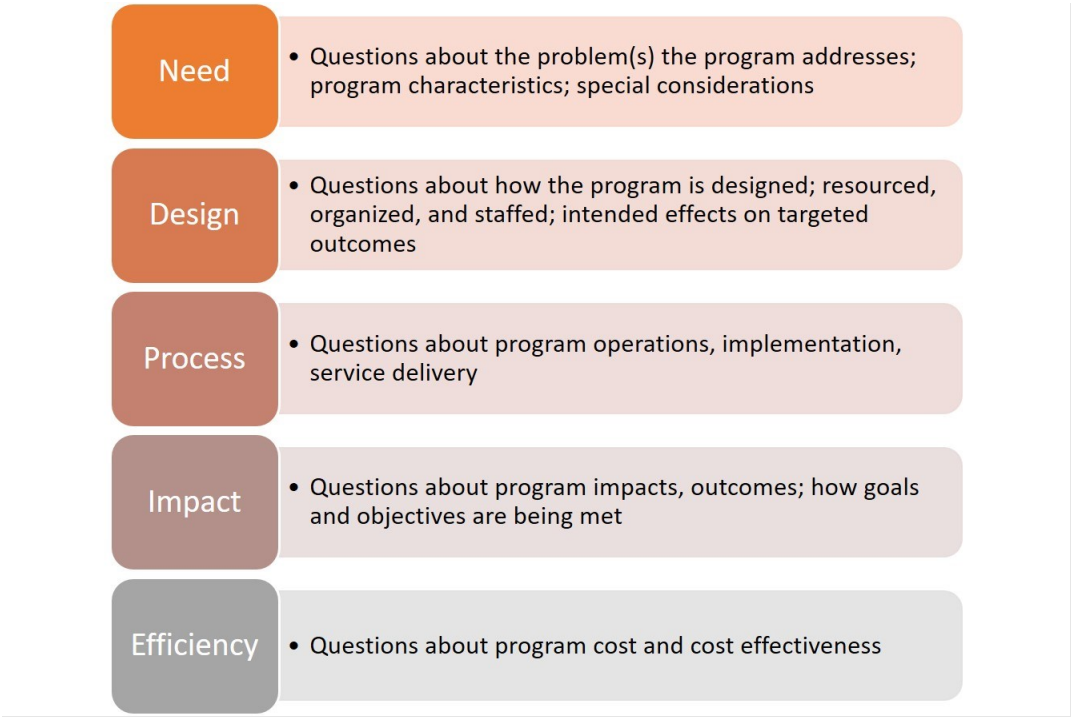


Figure 2. Five Components of Evaluation Questions

Self-assessment is a form of evaluation that provides an opportunity to systematically reflect on an organization's strengths, identify key gaps, and set priorities for ongoing improvement efforts. Self-assessment provides a way to characterize ITM program capacity, maturity, and performance. Results of self-assessment efforts can be used to identify gaps and vulnerabilities and recommend specific process improvements or security enhancements.

## 1.4 Capacity Building

In the late 1980s, the Department of Defense funded research to characterize the processes used by organizations to develop and enhance software products (Humphrey 1988). The "maturity" of an organization refers to the degree of formality and optimization of processes used in various stages of product development. In the 30 years since the approach was popularized, it has been adapted and applied in various organizations and industries as a formal method to articulate how well the behaviors, practices, and processes of an organization can reliably and sustainably produce required outcomes.

The self-assessment process presented herein incorporates a maturity model across eight specific domains germane to mitigating insider threats at nuclear facilities (see Table 1). Results of the self-assessment can be used to benchmark current ITM program capacity. Organizations are likely to be situated at different capacity scales (low, developing, intermediate, or exemplary) with some variation across the eight domains. To move from a lower capacity level to a higher level, organizations can use the self-assessment process to identify and implement a specific set of actions.

Table 1. Self-Assessment Domains for Insider Threat Mitigation

| Domain | Description |
|---|---|
| 1. National, Legal, and Regulatory Framework | Organization/facility complies with existing national legal and regulatory framework for managing and securing the nuclear industry and materials. Laws, regulations, and policies exist to provide basis for ITM program. Nuclear regulator or competent authority provides requirements. ITM program may be supported through a national-level threat assessment or design-basis threat (DBT). |
| 2. Facility Management and Planning | Nuclear materials facilities are secured and managed by incorporating established nuclear security principles, administrative and operational controls, a robust site security plan, and review, approval, and quality assurance measures. |
| 3. Personnel Security | Individuals with access to, authority for, or knowledge of high consequence materials, facilities, information, and programs are vetted to ensure the highest standards of reliability, trustworthiness, and physical and mental suitability. Personnel security programs address the entire employment life cycle. |
| 4. Physical Protection | A facility's physical protection system includes technical, administrative, and operational measures designed to provide the defense-in-depth necessary for insider mitigation. The state, regulator, or competent authorities define the physical protection requirements, and the facility operators implement these requirements in regulatory requirements, security policies and procedures, or both. |
| 5. Nuclear Material Accounting and Control | The Nuclear Material Accounting and Control (NMAC) system tracks and manages a facility's nuclear material inventories to mitigate the risk posed by potential insider adversary theft, sabotage, or misuse. NMAC and surveillance measures exist to delay or slow adversary's ability to access materials and provide alarms if potential malicious activity is detected. |
| 6. Cybersecurity | Computer-based systems at nuclear materials facilities are protected against internal or external cyberattacks that may target NMAC records, safety systems, operational systems, facility systems, and security systems. |
| 7. System Evaluation and Performance Assurance | Security assessments are used in various phases of the facility life cycle, to optimize physical protection during the facility design and to provide assurance of physical protection system effectiveness during operations and decommissioning. Tests, assessments, and inspections are performed and documented to verify systems are performing as expected. |
| 8. Nuclear Security Culture | The facility's culture—the collection of characteristics, attitudes, and behavior of individuals, organizations, and institutions—supports and enhances nuclear security. Guiding principles of security culture are propagated through training and awareness campaigns, organizational leadership, employee assistance programs, etc. |

Self-assessment is a means to improve security performance—the effectiveness and efficiency of an organization's ability to mitigate insider threats. The process helps identify and eliminate program deficiencies and shortcomings; can address outdated policies and procedures; help identify program strengths, weaknesses, opportunities, and threats; and increase staff commitment to the mission.

The remainder of this report is organized as follows.

- Section 2 describes the development, design, and application of the self-assessment toolkit.
- Section 3 describes the conclusions and recommendations for organizations applying the toolkit.
- Appendix A presents the self-assessment toolkit.
- Appendix B presents the exercise tables.

# 2.0 Self-Assessment Toolkit

Self-assessment is conducted in four phases (see Figure 3). Reflecting this model, the toolkit is divided into four parts.

- Phase 1 helps users identify and collect information, data, and supporting documentation necessary for the assessment process.
- Phase 2 invites users to self-assess how their organization prevents and protects against insider threats, including acts of theft and sabotage.
- Phase 3 encourages users to review the self-assessment.
- Phase 4 helps users articulate key questions about how to address the gaps and goals identified in the self-assessment, including identification of any corrective actions.

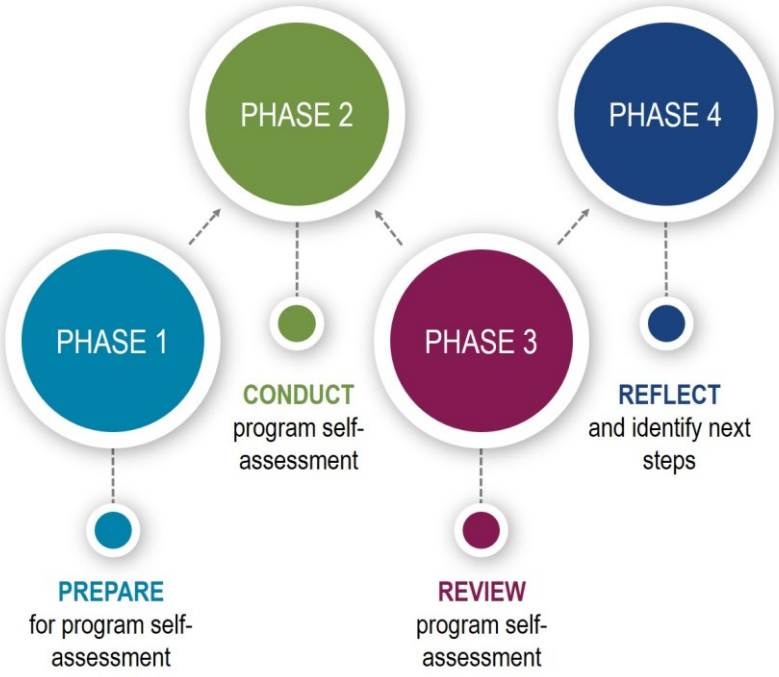


Figure 3. Self-Assessment Process

## 2.1 Toolkit Development

This toolkit has been developed by reviewing literature on the topic of capability and capacity maturity indicators, program evaluation, self-assessment, and international and industry best practices. It represents a compilation of these concepts and ideas from several diagnostic tools developed for other purposes and has been customized for managers and operators at nuclear material facilities. The toolkit is versatile and can be used for quick reflection or as part of a larger, more comprehensive nuclear security program evaluation and audit.

## 2.2 Toolkit Design and Application

The toolkit assesses organizational capacity for mitigation of insider threats. The toolkit is designed to be applied independently, in a facilitated workshop, or in a bilateral engagement. In each phase, the toolkit includes worksheets for the organization to use in completion of the self-assessment, and exercises that they can apply if desired to facilitate the self-assessment experience. Throughout, users are encouraged to modify the worksheets and exercises if needed to fit their organization.

During Phase 1, organizations choose the format that best fits their needs. If the organization is conducting the self-assessment independently, they can choose which worksheets and techniques to use and how to apply them. In a facilitated workshop or a bilateral engagement, instructors can work with the organization to explain the information needed to conduct a self-assessment, to gather the materials necessary to complete it, and to review and interpret the results. The exercises within the toolkit can be used in a workshop in an interactive fashion to facilitate understanding as the organization completes the self-assessment.

As noted, the toolkit is divided into four phases to reflect the self-assessment process. The following sections describe the design of each of phase.

### 2.2.1 Phase 1: Prepare for Self-Assessment

In Phase 1, the organization begins by identifying the team responsible for conducting the self-assessment. Although the self-assessment can be conducted by an individual, users are encouraged to include representatives from the organization's ITM program. If the organization does not have a formal program established, users are encouraged to invite representatives from each department responsible for some aspect of nuclear and radioactive materials security (e.g., policy and regulations, facility operations, physical and personnel security, legal, human resources, and information/computer security).

Before conducting the self-assessment, users must select a format and a timeframe appropriate for their organization. Again, the self-assessment toolkit can be applied in an independent, workshop, or bilateral format; users are provided guidance to help them to consider which format is best for them and their organization based on their knowledge and expertise in nuclear security and ITM. The self-assessment toolkit can be used in one of two ways:

1. Rapid assessment – to identify key gaps and priorities.
2. In-depth analysis – where more time is spent discussing each of the eight self-assessment domains in-depth to reach shared understanding of what each cover; to articulate current state of each domain within the organization; and to clarify opportunities for improvement.

In addition, during the preparation phase, users engage with leadership to help secure the resources necessary to complete the self-assessment process. Users are encouraged to tie the strategy of the ITM program to the organizational goals to help justify the time and resources necessary to conduct the self-assessment.

Finally, the most substantial aspect of preparation is the gathering of information and resources necessary for completing the self-assessment. To support organizations in gathering the information necessary, the toolkit provides a checklist that users can apply to determine whether they have gathered all the relevant documents for self-assessment.

### 2.2.2 Phase 2: Conduct Self-Assessment

During Phase 2, organizations conduct the self-assessment. To do so, they complete a series of worksheets, each focused on one of the ITM program domains (Appendix B). For each domain, a series of closed-ended statements are presented, and the users respond indicating the degree to which they agree with that statement. Closed-ended statements are used as they are conclusive in nature and designed to create data that are easily quantifiable. Closed-ended statements also provide granular feedback on measuring an organization's perceptions regarding the current state of ITM practice.

For each statement, a five-point Likert scale is used to rate the extent to which respondents agree that the item represents their organization's current situation or practice, from 5 (*strongly agree*) to 1 (*strongly disagree*). After each statement is addressed, the points are summed to provide a grand total for the domain. The toolkit provides an example of this process for users.

Finally, an average score is calculated for each ITM program domain to identify areas of strength and opportunities for improvement across the ITM program. The toolkit provides a worksheet to allow for calculation of these domain scores. Users are instructed to apply these scores to understand domains where they might already have a strong ITM program and areas where they need to continue to improve. Because these scores indicate relative strength and weakness within an organization, the toolkit also notes that these are not an appropriate method for comparing results between organizations.

### 2.2.3 Phase 3: Review Results

There are five steps in an iterative assessment process (see Figure 4). Each step in the process contributes to the subsequent step, which in turn generates a continuous feedback loop for organizational learning, growth, and development. Results of the self-assessment process described in Phase 2 ("Assess" in Figure 1) begin with the iterative assessment cycle.


Figure 4. Iterative Self-Assessment Cycle

The self-assessment process provides opportunity to clarify regulatory and legislative drivers, address personnel and physical security measures, and reinforce the value and importance of industry best practices and security culture to threat mitigation.

Using the iterative self-assessment cycle, the toolkit guides users on how to prioritize the findings, how to set goals, and how to measure progress toward those goals. In Phase 4 (Reflect), the toolkit discusses the ways that information can be evaluated and reviewed to ensure continuous improvement.

When prioritizing goals, users are encouraged again to consider organizational priorities and strategies. Not only can this align the ITM program with the organization's goals, articulation of priorities and strategies can also help to secure leadership support of any necessary changes to be implemented.

In addition, the toolkit provides a worksheet for users to complete to understand the key recommendations and actions needed to address any issues identified in the self-assessment approach (Appendix A.3.2). To make progress toward those goals measurable, the toolkit suggests the use of a **s**pecific, **m**easurable, **a**ccountable, **r**easonable, and **t**ime-bound (SMART) action plan (Appendix A.3.4.1). With origins in the field of management and business, the SMART model is widely used across many disciplines and industries to articulate and measure progress toward specific objectives. The SMART action plan formalizes the results of the assessment and provides clear recommendations for program improvement. If helpful to articulate the SMART action plan, structured brainstorming or the nominal group technique (NGT) can be used (Appendix A.3.4.5). Both techniques are forms of brainstorming that encourage idea generation and participation and can be useful when attempting to identify areas for improvement. In addition, a guide is provided for scenario-based facilitated discussions (SBFDs) (Appendix A.3.4.4). SBFDs are an interactive, hands-on engagement activity that allows for open discussion of various facets of an organization's operational

systems and processes. The SBFD is based on a pre-established scenario where a facilitator guides the participants through a hypothetical scenario—soliciting information and input from participants on how they would react or respond to the specific step in the scenario by asking carefully crafted open-ended questions. SBFDs allow participants to identify strengths, weaknesses, gaps, and areas for improvement in their existing systems. SBFDs can be planned for a wide variety of audiences in every pillar of a program's portfolio.

Finally, a template is provided for a **s**trengths, **w**eaknesses, **o**pportunities, and **t**hreats (SWOT) analysis (Appendix A.3.4.3). Common in the business world, SWOT analysis is used to identify and evaluate these areas for projects, plans, and/or organizations. SWOT requires a low amount of effort, can generate, and synthesize large amounts of useful information, and can drive practical plans and recommendations. However, although practical information from SWOT can be used to guide other types of analysis, it often leaves the team with many lists and few direct-action items. It also provides only a "snapshot" in time and is subject to bias, although that bias can be mitigated by including an outsider on the team.

### 2.2.4 Phase 4: Reflect

Phase 4 asks users to reflect on the results of their organization's self-assessment. Unlike the previous phases, Phase 4 does not include worksheets or exercises to guide the users, as it is intentionally somewhat unstructured. Instead, the toolkit provides some suggestions for potential next steps for toolkit users, such as data collection to ensure accountability to the goals created in Phase 3, and planning of the next self-assessment in the iterative cycle.

# 3.0 Conclusions

The self-assessment tools discussed and provided herein could be completed by a third party as part of a larger nuclear security assessment/evaluation. The primary benefit to complete the self-assessment by program staff is that of introspection and reflection. Ultimately, how the self-assessment toolkit and process is used will differ based on a variety of factors, including facility type, material quantities, regulations, and other operational requirements. If conducted regularly, longitudinal information can provide hard data reflecting program improvements, proactive response to regulatory and legislative changes, evolving business demands, etc. Data-driven discussions with management can foster organizational support of ITM and assure adequate allocation of resources, human and financial. Finally, as the threat landscape evolves, organizations must revisit ITM program objectives. Periodically conducting a self-assessment allows an organization to reflect, respond, and mature organizational capacity efforts for ITM.

# 4.0 References

Bunn, M. and Sagan, S.D., Eds. 2016. *Insider Threats*. Cambridge, MA: American Academy of Arts and Sciences.

Humphrey, W.W. 1988. "Characterizing the Software Process: A Maturity Framework." *IEEE Software*, 5(2): 73-79.

IAEA – International Atomic Energy Agency. 2020. *Preventive and Protective Measures against Insider Threats*, IAEA Nuclear Security Series No. 8-G (Rev. 1) Implementing Guide. Retrieved from http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1858_web.pdf

McDavid, J.C., Huse, I., Hawthorn, L.R.L. 2018. *Program Evaluation and Performance Measurement: An Introduction to Practice*, 3rd edition. Thousand Oaks, CA: SAGE Publications, Ltd.

NTI – Nuclear Threat Initiative. July 2020. *NTI Nuclear Security Index: Losing Focus in a Disordered World*, 5th edition. Retrieved from https://media.nti.org/documents/2020_NTI-Index_Report_Final.pdf

Heuer, Jr., R.J. and Pherson, R.H. 2015. *Structured Analytic Techniques for Intelligence Analysis*, 2nd ed. Thousand Oaks, CA: CQ Press.

Rossi, P.H., Lipsey, M.W., and Henry, G.T. 2019. *Evaluation: A Systematic Approach*, 8th edition. Thousand Oaks, CA: SAGE Publications, Ltd.

# 5.0 Recommended Reading

The following are additional recommended readings germane to assessing and evaluating ITM programs.

Bensoussan, B.E., and Fleisher, C.S. 2013. *Analysis Without Paralysis: 12 Tools to Make Better Strategic Decisions*, 2nd edition. Upper Saddle River, NJ: Pearson Education, Inc.

Bunn, M. Roth, N., and Tobey, W.H. 2019. *Revitalizing Nuclear Security in an Era of Uncertainty*. Project on Managing the Atom, Harvard Kennedy School, Belfer Center for Science and International Affairs. Retrieved from https://www.belfercenter.org/publication/revitalizing-nuclear-security-era-uncertainty

Butler, M.O. 2015. *Evaluation: A Cultural Systems Approach*. Walnut Creek, CA: Left Coast Press.

CERT – Carnegie Mellon University. December 2018. *Common Sense Guide to Mitigating Insider Threats*, 6th ed. Software Engineering Institute, CMU/SEI-2018-TR-010. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2019_005_001_540647.pdf

Greitzer, F.L., and Ferryman, T.A. 2013. "Methods and Metrics for Evaluating Analytic Insider Threat Tools." *IEEE Security & Privacy Workshops*, pp. 90-97. Retrieved from https://www.doi.org/10.1109/SPW.2013.34

INSA – Intelligence and National Security Alliance. October 2019. *Categories of Insider Threats*. Retrieved from https://www.insaonline.org/wp-content/uploads/2019/10/INSA_WP_Categories_of_Insider_Threats-1.pdf

INSA – Intelligence and National Security Alliance. October 2019. *Components of Effective Insider Threat Training*. Retrieved from https://www.insaonline.org/wp-content/uploads/2019/10/INSA_WP_Training-Programs.pdf

INSA – Intelligence and National Security Alliance. April 2017. *Assessing the Mind of the Malicious Insider: Using a Behavioral Model and Data Analytics to Improve Continuous Evaluation*. Retrieved from https://www.insaonline.org/wp-content/uploads/2017/04/INSA_WP_Mind_Insider_FIN.pdf

Jaros, S.L. 2018. *A Strategic Plan to Leverage the Social & Behavioral Sciences to Counter the Insider Threat*, PERSEREC-TR-18-16. Seaside, CA: U.S. Department of Defense, Defense Personnel and Security Research Center, Office of People Analytics. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/1063771.pdf

Moore, A.P., Novak, W.E., Collins, M.L., Trzeciak, R.F. and Theis, M.C. 2015. *Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls*. Software Engineering Institute. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=446367

National Insider Threat Task Force (. (2018). *Insider Threat Program Maturity Framework*. Retrieved from https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf

Ohlhausen, P., Poore, M., McGarvey, D., Anderson, L. 2014. *Persuading Senior Management with Effective, Evaluated Security Metrics*. ASIS Foundation. Retrieved from https://capindex.com/wp-content/uploads/ASIS_Report_Complete1.pdf

Thompson, S.M. and M. Choudhary. 2019. *The Ultimate Guide to Building an Insider Threat Program*. ObserveIT. Retrieved from http://www.observeit.com

WINS – World Institute for Nuclear Security. July 2020. *International Best Practice Guides Flye*r. Retrieved from https://wins.org/document/best-practice-guides-flyer/

# Appendix A – Insider Threat Mitigation Program Self-Assessment Toolkit

Self-assessment is an inward-facing evaluation process that enables an organization to review current status, processes, and performance against a specific set of criteria. Results of the self-assessment provide critical information that can contribute to the continuous improvement of an organization's ITM program.

This toolkit is intended to guide an organization through the process of self-assessing an ITM program. The toolkit is divided into four phases to reflect the steps in the self-assessment process: preparing for self-assessment, conducting the self-assessment, reviewing the self-assessment, and reflecting on the results. Each phase begins with a description of the activities that are conducted during that phase. In each phase of the toolkit, there are worksheets that can be used when completing the tasks in that phase. In addition, there are optional exercises that can be used by your organization if desired. Throughout the application of this toolkit, the self-assessment team encourages you and your organization to modify the worksheets and exercises to fit your needs. Think of this toolkit as a guide to facilitate the ITM program self-assessment at your organization, and use the activities, worksheets, and exercises to help you complete the self-assessment process.

## A.1 Phase 1 – Prepare for Self-Assessment

During Phase 1 of the self-assessment process, the organization will identify the self-assessment team, select the format and timeframe available for completing the self-assessment, engage leadership in the self-assessment process, and finally, gather the information and resources necessary to complete the self-assessment. Each of these steps are described in detail below.

### A.1.1 Identify Your Self-Assessment Team

The initiation of a self-assessment can be linked to an organization's annual or strategic planning cycle or may be dictated by a regulatory body or specific legislation. The self-assessment may be led by senior management, an individual from the quality assurance or risk management department, or even a third-party facilitator.

While the self-assessment can be conducted by one ITM program representative, best practice is to work collaboratively with all ITM program representatives. A holistic ITM program will have a diverse membership, each a subject matter expert in his or her own discipline (e.g., legal, human resources, facility management), and each has important knowledge and expertise to contribute during the self-assessment process.

If your organization does not have a formal ITM program established, consider inviting representatives from each department responsible for some aspect of nuclear and radioactive materials security (e.g., policy and regulations, facility operations, physical and personnel security, legal, human resources, and information/computer security). These different groups within your organization will help gather the information needed to complete the self-assessment.

If your organization is conducting self-assessment for the first time, consider the value and importance of senior or executive leadership commitment to and involvement in the assessment process. Managers have significant influence on organizational culture and play a vital role in promoting nuclear security. While these individuals may not serve in a formal capacity on the ITM program, their support of and involvement in program evaluation emphasizes the importance of threat mitigation and can go a long way in assuring adequate resources are available to address findings and implement recommendations.

### A.1.2 Select the Format and Determine Timeframe

After identifying your self-assessment team, determine the self-assessment format that best fits the organization. This toolkit is designed to be used in three different formats: independently, in a facilitated workshop, or through a bilateral engagement.

Because ITM self-assessment requires in-depth knowledge of nuclear security and ITM concepts as well as practices and procedures at your specific organization, the organization and self-assessment team should consider the knowledge and expertise of the organization when determining the best format. Table 2 provides some potential considerations.

Table 2. Self-Assessment Process Matrix

| Format | Description | Best for… | Select this option if… |
|---|---|---|---|
| Independent | The organization completes the self-assessment independently. | Organizations with a well-developed nuclear security regime, with available experts in nuclear security laws, regulations, practices, and procedures to complete a self-assessment and determine next steps. | You feel ready to complete a self-assessment on your own. |
| Facilitated Workshop | The organization attends a workshop before completing the self-assessment. This might be a single workshop to initiate the self-assessment process, or multiple workshops before and after the self-assessment is completed. | Organizations with a strong nuclear regime, but who require additional expert input before completing the self-assessment process. | You are almost ready to complete a self-assessment, but you have a few questions. |
| Bilateral Engagement | The organization works with a US-based team throughout the self-assessment process, with multiple meetings and engagements to facilitate the self-assessment. | Organizations who are still developing nuclear security practices or who need additional expertise as they identify areas for growth and improvement. | You want to complete a self-assessment but will need help throughout the process. |

In addition to deciding on a format, the organization and self-assessment team should consider the time and resources available to complete the self-assessment. The organization can use this toolkit to conduct a rapid assessment to identify key gaps and priorities. The organization can also choose to conduct an in-depth analysis, where more time is spent discussing each of the self-assessment domains in-depth to reach shared understanding of each domain, to articulate current state of each domain within the organization, and to clarify opportunities for improvement.

Regardless of how you use this toolkit, the self-assessment team encourages you to focus on the discussion and reflection prompted by the various self-assessment activities. However, determining how you would like to use this toolkit will help you as you engage with leadership to obtain the resources necessary to complete the self-assessment.

### A.1.3 Engage Leadership

Self-assessment requires time, effort, and resources. Many organizations struggle to connect ITM program strategy to organizational goals, which leads to failure in allocating appropriate resources needed to support the strategy. In addition, executive leadership and management are critical throughout the self-assessment process. Without their support and approval, it will be difficult to address the gaps, vulnerabilities, and opportunities to strengthen the ITM program in one or more of the eight domains.

Based on the way users decide to use this toolkit, engage with leadership to secure the resources necessary to complete the self-assessment and to gain their support for

implementing necessary changes. Be sure to link the goals of the ITM program to those of the organization as a means of demonstrating the value of a robust ITM program.

### A.1.4 Gather Information and Resources

Although tacit knowledge, or knowledge based on experience, is extremely valuable in the self-assessment process, using data, documents, and other supporting materials to conduct program evaluation with defensible judgments is imperative. Thus, the organization and the self-assessment team need to gather information to complete the self-assessment. Using the Self-Assessment Readiness Checklist, gather the materials listed for each domain to prepare to conduct the self-assessment.

### A.1.5 Materials

The materials listed in the following checklist will be useful to prepare for and conduct the self-assessment.

Table 3. Self-Assessment Readiness Checklist

| Collected | N/A | ITEM DESCRIPTION | COMMENTS |
|---|---|---|---|
| DOMAIN 1 – National Legal and Regulatory Framework | | | |
| ☐ | ☐ | Local, regional, or national guidance or directives on mitigating insider threats | |
| ☐ | ☐ | National threat assessment or DBT | |
| ☐ | ☐ | Trustworthiness and reliability regulation and/or requirements | |
| ☐ | ☐ | Legislation regarding criminal offenses and illicit trafficking in nuclear and other radioactive materials | |
| DOMAIN 2 – Facility Management and Planning | | | |
| ☐ | ☐ | ITM policy and program documentation | |
| ☐ | ☐ | Security plan | |
| ☐ | ☐ | Response plan | |
| ☐ | ☐ | Emergency plan | |
| ☐ | ☐ | Operators/material handlers personnel requirements | |
| ☐ | ☐ | Operations schedules | |
| ☐ | ☐ | Operating standards, special procedures, or directives | |
| ☐ | ☐ | Security procedures or directives | |

| Collected | N/A | ITEM DESCRIPTION | COMMENTS |
|---|---|---|---|
| DOMAIN 3 – Personnel Security for Trustworthiness and Reliability | | | |
| ☐ | ☐ | Trustworthiness and reliability program criteria and guidance documents | |
| ☐ | ☐ | List of positions with unescorted access and authority to vital areas and nuclear or other radioactive materials | |
| ☐ | ☐ | List of pre-screening measures | |
| ☐ | ☐ | Continuous evaluation policies and procedures | |
| ☐ | ☐ | Insider threat determination procedure | |
| ☐ | ☐ | Disciplinary policy | |
| ☐ | ☐ | Access revocation policy and procedure | |
| DOMAIN 4 – Physical Protection System | | | |
| ☐ | ☐ | Physical protection system requirements | |
| ☐ | ☐ | Training documentation for overpacks, material containers, delay systems, lock and key control, and shipment vehicles | |
| ☐ | ☐ | Response force training, qualifications, policies, and procedures | |
| ☐ | ☐ | Alarm procedures | |
| ☐ | ☐ | Role-based access control policies | |
| ☐ | ☐ | Search and seizure procedures | |
| ☐ | ☐ | Vehicle and personnel search policy/procedure | |
| ☐ | ☐ | Security incident/Site emergency and site facility plans | |
| DOMAIN 5 – Nuclear Material Accounting and Control | | | |
| ☐ | ☐ | Material inventory monitoring schedule | |
| ☐ | ☐ | Materials segregation procedure | |
| ☐ | ☐ | List of tools, techniques, and procedures implemented to detect unauthorized removal of nuclear material | |
| DOMAIN 6 – Cybersecurity | | | |
| ☐ | ☐ | Facility cybersecurity policy | |

| Collected | N/A | ITEM DESCRIPTION | COMMENTS |
|---|---|---|---|
| ☐ | ☐ | Facility cyber incident response plan | |
| ☐ | ☐ | Network system design | |
| ☐ | ☐ | Vendor trustworthiness and reliability conformance | |
| DOMAIN 7 – System Evaluation and Performance Assurance | | | |
| ☐ | ☐ | Performance assurance program plan | |
| ☐ | ☐ | Threat assessment or DBT | |
| ☐ | ☐ | Security performance metrics | |
| DOMAIN 8 – Nuclear Security Culture | | | |
| ☐ | ☐ | Personnel risk indicators, behavioral observation program guidance, checklists | |
| ☐ | ☐ | Training curriculum and compliance rates | |
| ☐ | ☐ | Recent findings and corrective action plans focused on insiders and insider threat | |
| ☐ | ☐ | Employee assistance program documentation | |
| ☐ | ☐ | Organization security policy and communications plan | |

### A.1.5.1 Rapid Self-Assessment Exercise

This exercise will help to quickly assess how well prepared the organization is to counter the insider threat. It may also help identify existing shortfalls so that they can be addressed.

Mark answers in the following table and then total the points to find your score.

Table 4. Assess Your Organization's Preparedness to Counter Insider Threat

| Characteristic | Strongly Agree 5 points | Agree 4 points | Neutral 3 points | Disagree 2 points | Strongly Disagree 1 point |
|---|---|---|---|---|---|
| The effective implementation of policies, security measures and procedures to manage internal threats is a core organizational value. | | | | | |
| Trustworthiness programs and practices have been implemented. | | | | | |
| The staff believes periodic screening (drugs, alcohol, etc.) is acceptable. | | | | | |

| Characteristic | Strongly Agree 5 points | Agree 4 points | Neutral 3 points | Disagree 2 points | Strongly Disagree 1 point |
|---|---|---|---|---|---|
| Cybersecurity forms an integral part of the security program. | | | | | |
| The security program considers cyber-security's impact on physical security. | | | | | |
| A comprehensive vulnerability analysis (VA) has been conducted that clearly defines roles and responsibilities, the separation of duties, and access to sensitive materials and locations. | | | | | |
| Staff and contractors strongly support the management of internal risks and believe it is important for their work, personal safety, and the reputation of the organization. | | | | | |
| Employees quickly notice and report suspicious behavior. | | | | | |
| Management recognizes the value of strong internal controls, encourage a culture of teamwork, and has an established code of conduct including behavioral standards. | | | | | |
| Strong and effective action is taken against individuals who violate the behavioral values of the organization. | | | | | |
| Reassessment of risks and vulnerabilities, including internal threats, is conducted periodically and used as an important input for enhancing the organization's security. | | | | | |
| Security awareness programs, address potential internal threats and the need for constant vigilance. | | | | | |
| There is a good level of access control, and the separation of duties/responsibilities is enforced. | | | | | |
| Staff feel comfortable reporting observations or information that could indicate a potential internal threat. | | | | | |
| **TOTAL** | | | | | |

## Scoring

**Exemplary, 56-70 points:** Your organization is well positioned to mitigate insider threat.

**Intermediate, 37-55 points:** Your organization has an effective security program but may need to make specific improvements to effectively mitigate insider threat. Look at the characteristics that scored the lowest points to identify where to begin improving your program.

**Developing, 18-36 points:** Your organization may need to focus more attention on security practices and culture. Start by making sure every level of your organization supports the need

for an ITM program. Then vcoordinate with leadership to discuss how to prioritize and develop an action plan.

**Low, 0-17 points:** If your score falls in this range, your organization may be in the early stages of developing and establishing a security program. Consult best practices and industry guidance for ideas. Seek out training or assistance from regional or international organizations.

## A.2 Phase 2 – Conduct the Self-Assessment

In Phase 2, the organization will conduct the self-assessment. To do so, complete the series of domain worksheets, and then use this qualitative assessment to compare the capacities of the organization's ITM program across the self-assessment domains. This will help you to understand the strengths of your ITM program and identify areas for improvement.

### A.2.1 Complete Domain Worksheets

To assess your ITM program's capability to address insider threat, you and your self-assessment team will complete a series of worksheets, each of which focus on one aspect of ITM (see **Domain Worksheets** in this section). For each of the ITM program domains, you will read a series of closed-ended statements. For each statement, use a five-point Likert scale to rate the extent to which you agree that the item represents your organization's current situation or practice, from 5 (*strongly agree*) to 1 (*strongly disagree*). Use the materials identified before the self-assessment to respond to each statement (the **Self-Assessment Readiness Checklist** from Phase 1). After each statement is addressed, the points are summed to provide a grand total for the domain. See Table 5 for an example.

Table 5. Example Self-Assessment Domain Worksheet

| | **Strongly Agree** | **Agree** | **Neutral** | **Disagree** | **Strongly Disagree** |
|---|---|---|---|---|---|
| | **5 points** | **4 points** | **3 points** | **2 points** | **1 point** |
| **1.1** The country has established national-level legislation and requirements for the protection of nuclear and other radioactive materials, facilities, and/or activities. | 5 | | | | |
| **1.2** The country has a designated nuclear regulator and/or competent authority responsible for oversight and implementation of nuclear security requirements. | | | | 2 | |
| **1.3** The country encourages cooperation between nuclear regulator/competent authority and other agencies (law enforcement, border security, commerce, etc.) for safety and security of nuclear and other radioactive materials. | | 4 | | | |

| | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| | **5 points** | **4 points** | **3 points** | **2 points** | **1 point** |
| **1.4** Nuclear regulator/competent authority develops regulations and requirements to establish trustworthiness and reliability for all persons with access to sensitive data, information, materials, or facilities. | | 4 | | | |
| **1.5** The country or regulator has developed and periodically revises a national threat assessment or design-basis threat (DBT). | | | 3 | | |
| **1.6** The country has established domestic laws for prosecution of criminal or intentional acts involving or directed at nuclear and other radioactive materials, facilities, and/or activities. | 5 | | | | |
| **1.7** The country has established laws, policies, and guidance to combat illicit trafficking in nuclear and other radioactive materials. | 5 | | | | |
| **1.8** The country cooperates with and seeks assistance from nuclear security-oriented organizations (e.g., International Atomic Energy Agency) on nuclear security matters. | | | | 2 | |
| **1.9** The country uses a risk-informed, graded approach to nuclear security. | | | 3 | | |
| **1.10** The country is a subscriber to INFCIRC/908. | | | | 2 | |
| **Total** | 15 | 8 | 6 | 6 | |
| **Domain 1 Total** | | | | | 35 |

Each domain worksheet also provides space for users to document the assessment process. Users can provide general comments, include details to verify, list source documents or materials consulted, people to contact, expected or anticipated changes, etc. These notes can be leveraged during Phase 3, “Review Program Self-Assessment.”

In the process of conducting a self-assessment, questions will arise about the current state of the ITM program. In addition, opportunities to improve or advance the current state of practice will arise. For example, a self-assessment team may identify differences in perspective and diverse assumptions among ITM program team members. These conversations will stimulate organizational learning and contribute to new ideas.

The self-assessment team recommends documenting questions throughout the self-assessment process as a part of formal recordkeeping. Doing so enables your organization to return to the issues under question following the self-assessment. Addressing some of the

questions may require additional resources (human or financial) or investment (tools and equipment) and can be pursued as a follow-on activity.

### A.2.2 Compare Program Domain Capacities

After eight domains are assessed using the Self-Assessment Domain Worksheets, you can use the **Compare Program Capacity Across Domains** worksheet to document each domain score. The score is divided by the number of statements in that domain to obtain an average value. Higher average values represent areas of higher capacity. This qualitative measure is best used internally by your organization to identify areas for improvement or further investigation. It is not necessarily appropriate to conduct comparative analysis or assessment against other organizations' capacity levels.

### A.2.3 Materials

Appendix B provides exercise tables to help assess the organizations national, legal, and regulatory frameworks.

#### A.2.3.1 Compare Program Capacity Across Domains

Use the following table to compare results across domains. Write the total score for each domain in the second column and divide by the number of statements to obtain average values that are comparable across domains. Higher average values represent areas of higher capacity (5 being highest capacity).

Table 6. Compare Capacity Across Domains

| Domain | Domain Total | | Number of Statements | Average |
|---|---|---|---|---|
| 1. National, Legal, and Regulatory Framework | | ÷ | 10 | |
| 2. Facility Management and Planning | | ÷ | 10 | |
| 3. Personnel Security | | ÷ | 10 | |
| 4. Physical Protection | | ÷ | 10 | |
| 5. Nuclear Material Accounting and Control | | ÷ | 10 | |
| 6. Cybersecurity | | ÷ | 11 | |
| 7. System Evaluation and Performance Assurance | | ÷ | 10 | |
| 8. Nuclear Security Culture | | ÷ | 11 | |
| **Total** | Sum the above | ÷ | Sum the above (82) | |

## A.3 Phase 3 – Review Self-Assessment

In Phase 3, you and your self-assessment team will review the results from Phase 2 to identify areas of strength and areas for additional growth. This section of the toolkit guides you as you prioritize the results, set goals for implementation, and monitor progress toward those goals. In addition, a variety of exercises are provided for use within your organization as you reflect and plan next steps in the self-assessment cycle.

There are a variety of exercises included in this section of the toolkit that emphasize idea generation and problem solving from all aspects of your organization. Although these exercises are included during the review phase, they can be used at any point in the self-assessment process where they might be helpful. The self-assessment team encourages users to review the exercises and consider their use at any point during the self-assessment process where engagement with others might be helpful for brainstorming, identifying areas of weakness or strength, or gathering opinions on next steps or current practice.

### A.3.1 Prioritize

First, when reviewing the results of the self-assessment, you should consider your organization's priorities. Strategic priorities are often identified and described in annual plans at the program, departmental, or organizational level. If one or more of the eight self-assessment domains is clearly linked to an existing strategy element, then this is an indicator that any findings within that domain may take priority with executive leadership. Refer to notes taken during the self-assessment process or organizational strategy documents for reference.

### A.3.2 Set Goals

After identifying the higher-priority domains, collect the self-assessment worksheets, resulting analysis across all domains, and all notes taken during the assessment. These materials can be used to identify, develop, and articulate key recommendations (see Table 7). For each issue and recommendation, develop a separate table.

This formal process will clarify the self-assessment findings, set goals, and initiate improvements. The self-assessment team encourages you to review the exercises included in Phase 3 of this toolkit to guide you as you have conversations to identify the key recommendations from your self-assessment. Because of the diverse makeup of ITM teams, people may have differing opinions about key priorities or about the correct response. Using the exercises provided can help to structure those discussions to reach consensus on the next steps to improve your ITM program.

Table 7. Key Recommendations and Management Response

| | | |
|---|---|---|
| ***Self-Assessment Domain X. Recommendation 1.***<br><br>Add example text | | |
| ***Management Response***<br><br>Add example text | | |
| **Key management actions** | **Time frame** | **Responsible unit** |
| Identify action. Define action.<br>Can have more than one action to support the recommendation. | Estimated start date of action. | Who is responsible for completing the activity? This can be an individual, department, etc. Be as specific as possible. |
| 1.2 If applicable, identify second action. Define. | Define. | Define. |

### A.3.3 Measure Progress

After identifying the key priorities and recommended actions, the user should develop concrete goals against which to measure progress. One method of doing so is the creation of a **s**pecific, **m**easurable, **a**ccountable, **r**easonable, and **t**ime-bound (SMART) action plan. The SMART model can be used to clearly articulate how the ITM program will address specific issues identified during the self-assessment.

As the SMART model does not clearly identify the specific gap or vulnerability identified in the self-assessment or the specific recommendation to increase program capacity, this technique can be used in conjunction with the key recommendations and management responses shown in Table 2. The worksheets for this section also provide an example of a SMART action plan for review.

### A.3.4 Materials

#### A.3.4.1 Example SMART Action Plan

As seen in the following example, this technique provides a formulaic approach for clearly articulating goals and measuring progress.

*The Insider Threat Mitigation Program Manager (accountable) will host an informational staff meeting on January 15, 2021 (time-bound) with the Physical Security team and at least 90% of the third-shift supervisors (measurable) to announce and implement changes in vendor badging, access controls, and adverse-event reporting procedures (specific, reasonable).*

- Specific
  - Action/activity is clearly connected to the goal
    - Write concise statements
    - State what action owner needs to do—not all the details of how
    - Avoid grouping multiple tasks in the same action
    - Begin with an action verb
  - Use—revise, implement, install, develop
  - Avoid these terms: continue, improve, enhance
- Measurable
  - Action/activity has a verifiable start and end point
  - Actions can be verified
  - Effectiveness can be documented and validated
  - Avoid these terms: all, ongoing, continue, and improve. These are difficult to measure and complete

- Accountable
  - Action/activity has a responsible and identified owner
  - Proposed actions should be discussed with management and those responsible for implementing
  - Necessary qualifications and/or training needed to perform actions are identified and understood
- Reasonable
  - Actions/activities should be practical and clearly articulated
  - Avoid “quick fixes”
  - Make sure each action is directly related to issue resolution
- Time-bound, or timely
  - Target dates are neither too optimistic nor too far in the future. Consider:
    - Funding and resource availability
    - Dependencies
    - Other priorities or commitments
  - Documentation/verification requirements

#### A.3.4.2 Exercises and Tools

Depending on the needs of your organization, additional exercises can be used to facilitate collaboration. Three exercises, and a tool are described in this section.

#### A.3.4.3 SWOT Analysis

After completing the self-assessment, interpret the results using a strengths, weaknesses, opportunities, and threats (SWOT) analysis. SWOT can be an effective team-building activity, especially if participants from different departments collaborate on it; consider how ITM programs include representatives from several parts of the organization, such as physical security, human resources, etc.

Table 8. SWOT Analysis

| PURPOSE | |
|---|---|
| Enter the purpose of the analysis here | |

| S | INTERNAL **STRENGTHS** |
|---|---|
| 1 | What do we do well? |
| 2 | What are we most efficient at? |
| 3 | What can we do for less money? |
| 4 | What can we do in less time? |
| 5 | |

| W | INTERNAL **WEAKNESSSES** |
|---|---|
| 1 | Where do we lack efficiency? |
| 2 | Where are we wasting money? |
| 3 | Where are we wasting time and resources? |
| 4 | Does our security culture need improvement? |
| 5 | |

| O | EXTERNAL **OPPORTUNITIES** |
|---|---|
| 1 | What is missing in our industry? |
| 2 | What could we improve or do better? |
| 3 | What new trends are occurring? |
| 4 | What new technology could we use? |
| 5 | |

| T | EXTERNAL **THREATS** |
|---|---|
| 1 | What changes are occurring in our environment? |
| 2 | What technologies could replace what we currently use? |
| 3 | Could current social or environmental events introduce new threats? |
| 4 | Are any government policies or regulations changing? |
| 5 | |

| ACTION ITEMS & GOALS | |
|---|---|
| 1 | Which opportunities should we pursue? How can we use our strengths to help us succeed? |
| 2 | Which weaknesses can be addressed to help maximize security practices? |
| 3 | What strategies can we put into place to be prepared for threats? |
| 4 | |
| 5 | |

### A.3.4.4 Scenario-Based Facilitated Discussions

**Definition**: Scenario-based facilitated discussion (SBFD) is an interactive, hands-on engagement activity that allows for open discussion of various facets of a country's (or region's) operational systems and processes. The event is based around a pre-established scenario where a facilitator guides the participants through a scenario—soliciting information and input from participants on how they would react or respond to the specific step in the scenario by asking carefully crafted open-ended questions. SBFD allows participants to identify strengths, weaknesses, gaps, and areas for improvement in their existing systems. SBFDs can be planned for a wide variety of audiences in every pillar of the program's portfolio.

The SBFD event is a highly customized engagement with the goal of spurring discussion, debate, and collaboration among participants. Scenarios can be simple or complex and are designed to cover points that the facilitator wants participants to talk or work through to move their policy or work-flow processes forward. SBFD events are designed to be unique for each set of event objectives and audience. SBFD events help participants generate ideas for sustaining strengths, improving processes, and identifying areas where progress is needed.

- **What is it? What is it not?**
  - SBFD is focused on engaging and involving participants by discovering, with the facilitator, the systems, processes, strengths, gaps, and functions within their own programs–immediate buy-in.
  - It is **not** a standard classroom-based PowerPoint training presentation, formal tabletop exercise, or a quiz.
- **Why conduct an SBFD?**
  - SBFD events are useful for situations in which the organization needs or would like to identify and explore strengths, weaknesses, gaps, and opportunities in its systems and processes with respect to a specific topic area. They work best when there is a clearly identified target audience that is expected to participate actively in the discussion and share both positive and negative aspects regarding their operational systems.
  - The audience includes organizational members of all levels. Development of a realistic and scenario germane to the organization will actively engage participants, making the session more valuable and conducive to lively discussions.
  - While SBFDs are useful for a diverse range of target audiences and topics, there are scenarios where they may not be as useful. For example, if the goal of an engagement is to test the quality of an aspect of the organization's security system or a specific policy, then a tabletop exercise may be more appropriate. If the target audience has low levels of expertise in the subject area, then a more traditional awareness building workshop may be more appropriate.

**Strengths of Scenario-Based Discussions**

- Allows participants to have candid, collaborative, and granular discussions in a judgment-free environment.
- An innovative and interactive alternative to PowerPoint-centered engagement activities that can yield creative insights into a facet of an organization's operational systems (people, procedures, and equipment).

**Limitations of the Discussions**

- Getting the right people in the room, ensuring people are open to discussing these topics candidly.

**Developing a Scenario-Based Discussion: Key Items to Consider**

- The development process for a successful scenario-based discussion is time intensive. It involves in-depth planning for the organization-specific scenario and working with stakeholders to identify the correct audience. Because the SBFDs are targeted and focused, materials and participant guidelines will need to be produced for each event.
- The typical materials for an SBFD are the scenario slide deck, scenario background information, questions, and participant handout materials.

**Executing an SBFD: Key Guidelines**

- Scenario trajectory and discussions are scripted during the development process to make sure they drive toward desired outcomes and objectives; it is critical that scenario facilitators are intimately involved in the scenario design process.
- Importance of the audience and facilitators: The background and experience of the facilitators is a "make it or break it" part of an SBFD. Relevant stakeholders should work to advocate for the correct audience of participants. Their job is to guide everyone through the scenario and help capture relevant information. When the audience background unexpectedly changes, it is more difficult to modify SBFD content quickly in response to a change in the target audience.
- Questions should be written with the goal of the discussion in mind. While it is natural to write questions that will yield interesting information about an organization's operational systems, it is more crucial to write questions that generate meaningful discussion among the participants (not just questions that will yield useful facts).

#### A.3.4.5 Nominal Group Technique

The nominal group technique is a facilitated form of structured brainstorming that encourages equal participation. It prevents a discussion from being dominated by one person and mitigates the concern that some participants may not speak up. Nominal group technique begins with an open-ended question, allows participants to privately write down their initial ideas for a predetermined time limit, and then the facilitator calls on individuals to share what they have written down. Once participants have all run out of ideas, the discussion begins to make sure everyone understands each presented idea—not to argue for or against any ideas. Voting on ideas by secret ballot is optional. The facilitator and participants should pay special attention to both ideas that many participants had and unique but interesting/useful ideas. For more complex questions and/or larger brainstorming groups, questions can be divided into parts and

each group can run its own nominal group technique session, converging at the end. Imposing a strict time limit can keep the session focused.

#### A.3.4.6 Anonymous Engagement Tools

In potentially contentious environments where individuals may not be comfortable voicing an opinion, such as when introducing the self-assessment process in a multilateral setting, consider the use of anonymous online engagement tools. Many tools are commercially available, such as Mentimeter®, Slido®, Stormz®, and Axis®. Some tools are free, and others require a subscription or license. Participants must have a mobile phone, tablet, or laptop with an internet connection and can access the tools anonymously.

The use of online engagement tools can help promote interactive presentations, real-time feedback, and facilitate use of quizzes to check learning progress. Data can be exported, archived, and analyzed for trends over time.

Self-assessment facilitators can have meaningful impact on the event through real-time digital engagement and interaction. In meetings, decisions get made and everyone feels heard and able to provide real-time feedback. The use of online engagement tools can help foster a dynamic and engaging experience in a variety of settings including workshops, conference calls, meetings, and training sessions.

## A.4 Phase 4 - Reflect

After goals are articulated, recommended actions undertaken, and a specified time period has elapsed, the organization will need to formally evaluate and review progress. This could be conducted by the ITM program independently or together with executive leadership. Each recommendation is reviewed individually in a stepwise fashion.

The accountable individual or department will review each recommendation and associated action. Data can be provided as evidence to support progress toward the goal. Data analysis will show impact and enable discussion regarding each recommendation, e.g., did the suggested action decrease the concern, improve response time, or minimize a vulnerability. If specific actions required acquisitions/procurements, changes in policy or procedure, or specific interventions, they should be described.

In some cases, recommended actions may require multiple phases for improvements to be seen. This frequently occurs when something external to the organization (e.g., a legislative change) is implemented in phases over time or if the organization relies on a third party (e.g., security patching of a critical system). Both lagging and leading indicators of improvements are valuable to disclose in the formal review. During the next self-assessment cycle, completed actions are likely to have a net-positive impact on domain scores.

### A.4.1 Next Steps

As described, reviewing the self-assessment results is just the first step in articulating and developing an action plan for an organization’s continuous development and improvement. The self-assessment process is iterative. It helps an organization evaluate current state of practice and alignment with best practices and identify specific actions that are necessary to improve the ITM program.

## A.5 Resources

Bunn, M., and Sagan, S. D. 2014. *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes*. Cambridge, MA: American Academy of Arts and Sciences. Retrieved from www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderThreats.pdf

CISA – Cybersecurity and Infrastructure Security Agency. 2020. "Assessments: Cyber Resilience Review." Retrieved from https://us-cert.cisa.gov/resources/assessments

IAEA – International Atomic Energy Agency. 2020. *Preventive and Protective Measures against Insider Threats*. Nuclear Security Series No. 8-G (Rev. 1), Implementing Guide. Retrieved from http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1858_web.pdf

IAEA – International Atomic Energy Agency. 2019. *Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility during Use, Storage and Movement*. Nuclear Security Series, No. 32-T, Technical Guidance. Retrieved from https://www.iaea.org/publications/11165/establishing-a-system-for-control-of-nuclear-material-for-nuclear-security-purposes-at-a-facility-during-use-storage-and-movement

IAEA – International Atomic Energy Agency. 2019. *Preventive Measures for Nuclear and Other Radioactive Material our of Regulatory Control*. Nuclear Security Series No. 36-G, Implementing Guide. Retrieved from http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1855_web.pdf

IAEA – International Atomic Energy Agency. 2019. *Security of Radioactive Material in Use and Storage and of Associated Facilities*. Nuclear Security Series No. 11-G (Rev. 1), Implementing Guide. Retrieved from http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1840_web.pdf

IAEA – International Atomic Energy Agency. 2018. *Physical Protection of Nuclear Material and Nuclear Facilities*. Nuclear Security Series No. 27-G, Implementing Guide. Retrieved from http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1760_web.pdf

IAEA – International Atomic Energy Agency. 2018. *Computer Security of Instrumentation and Control Systems at Nuclear Facilities*. Nuclear Security Series, No. 33-T, Technical Guidance. Retrieved from http://www-pub.iaea.org/MTCD/Publications/PDF/P1787_web.pdf

IAEA – International Atomic Energy Agency. 2017. *DRAFT Computer Security Techniques for Nuclear Facilities*. Retrieved from https://www-ns.iaea.org/downloads/security/security-series-drafts/tech-guidance/nst047.pdf

IAEA – International Atomic Energy Agency. 2017. *Self-Assessment of Nuclear Security Culture in Facilities and Activities*. Nuclear Security Series No. 28-T, Technical Guidance. Retrieved from http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1761_web.pdf

IAEA – International Atomic Energy Agency. 2016. *DRAFT Computer Security for Nuclear Security*, Draft Implementing Guide. Retrieved from https://www-ns.iaea.org/downloads/security/security-series-drafts/implem-guides/nst045.pdf

IAEA – International Atomic Energy Agency. 2016. "Amendment to the Convention on the Physical Protection of Nuclear Material." INFCIRC/274/Rev.1/Mod.1. Retrieved from https://www.iaea.org/sites/default/files/infcirc274r1m1.pdf

IAEA – International Atomic Energy Agency. 2015. *Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities*. Nuclear Security Series, No. 25-G, Implementing Guide. Retrieved from https://www.iaea.org/publications/10763/use-of-nuclear-material-accounting-and-control-for-nuclear-security-purposes-at-facilities

IAEA – International Atomic Energy Agency. April 2014. *SARIS Guidelines*, 2014 Edition. Retrieved from https://www.iaea.org/publications/10697/saris-guidelines

IAEA – International Atomic Energy Agency. 2013. *Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme*. Nuclear Security Series No. 19, Implementing Guide. Retrieved from http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1591_web.pdf

IAEA – International Atomic Energy Agency. 2013. *Objective and Essential Elements of a State's Nuclear Security Regime*. Nuclear Security Series No. 20, Nuclear Security Fundamentals. Retrieved from http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf

IAEA – International Atomic Energy Agency. 2011. *Computer Security at Nuclear Facilities*. Nuclear Security Series, No. 17, Technical Guidance Reference Manual. Retrieved from https://www.iaea.org/publications/8691/computer-security-at-nuclear-facilities

IAEA – International Atomic Energy Agency. 2011. *Nuclear Security Recommendations on Nuclear and Other Radioactive Material Out of Regulatory Control*. Nuclear Security Series, No. 15, Recommendations. Retrieved from https://www.iaea.org/publications/8622/nuclear-security-recommendations-on-nuclear-and-other-radioactive-material-out-of-regulatory-control

IAEA – International Atomic Energy Agency. 2011. *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*. Nuclear Security Series, No. 13 (Rev. 5), Recommendations. Retrieved from https://www.iaea.org/publications/8629/nuclear-security-recommendations-on-physical-protection-of-nuclear-material-and-nuclear-facilities-infcirc/225/revision-5

IAEA – International Atomic Energy Agency. 2009. *Development Use and Maintenance of the Design Basis Threat*. Nuclear Security Series No. 10, Implementing Guide. Retrieved from https://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf

IAEA – International Atomic Energy Agency. 2008. *Nuclear Security Culture*. Nuclear Security Series No. 7, Implementing Guide. Retrieved from http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1347_web.pdf

IAEA – International Atomic Energy Agency. 2007. *Combating Illicit Trafficking in Nuclear and Other Radioactive Material*. Nuclear Security Series No. 6, Technical Guidance Reference Manual. Retrieved from http://www-pub.iaea.org/MTCD/Publications/PDF/pub1309_web.pdf

INSEN – International Nuclear Security Education Network. 2018. *Nuclear Security Culture: The State of Play*. INSEN Textbook. Vienna, Austria: International Atomic Energy Agency. Retrieved from http://spia.uga.edu/wp-content/uploads/2018/05/INSEN-TEXTBOOK-Pages-1-8-NS24-Nuclear-Security-Culture-Textbook.pdf

Mylrea, M., Gourisetti, S.N. G., Larimer, C., and Noonan, C. (2018). "Insider Threat Cybersecurity Framework Webtool & Methodology: Defending Against Complex Cyber-Physical

Threats." In *IEEE Security and Privacy Workshops,* pp. 207-216. Retrieved from https://www.doi.org/10.1109/SPW.2018.00036

NRC – U.S. Nuclear Regulatory Commission. 2018. *Insider Threat Program for Licensees*. Retrieved from https://www.nrc.gov/security/insider-threat-program-for-licensees.html

NIST – National Institute of Standards and Technology. Updated September 2020. *Cybersecurity Framework*. Accessed September 22, 2020 from https://www.nist.gov/cyberframework

WINS – World Institute for Nuclear Security. 2020. *Countering Violent Extremism and Insider Threats in the Nuclear Sector*. Best Practice Guide 3.8, Version 2.0. Retrieved from https://wins.org/document/3-8-countering-violent-extremism-and-insider-threats-in-the-nuclear-sector-mitigation-strategies/

WINS – World Institute for Nuclear Security. 2020. *Nuclear Transport Security*. Best Practice Guide 4.10, Version 2.0. Retrieved from https://wins.org/document/4-10-nuclear-transport-security-2/

WINS – World Institute for Nuclear Security. 2020. *Security of Radioactive Sources Used in Industrial Radiation Processing*. Best Practice Guide 5.8, Version 1.0. Retrieved from https://wins.org/document/bpg-5-8-security-of-radioactive-sources-used-in-industrial-radiation-processing/

WINS – World Institute for Nuclear Security. 2019. *Assessing and Communicating Nuclear Security Threats*. Best Practice Guide 2.6, Version 1.1. Retrieved from https://wins.org/document/2-6-assessing-and-communicating-nuclear-security-threats/

WINS – World Institute for Nuclear Security. 2019. *Effectively Integrating Physical and Cyber Security*. Best Practice Guide 4.11, Version 1.1. Retrieved from https://wins.org/document/4-11-effectively-integrating-physical-and-cyber-security/

WINS – World Institute for Nuclear Security. 2019. *Human Reliability as a Factor in Nuclear Security*. Best Practice Guide 3.2, Version 2.1. Retrieved from https://wins.org/document/3-2-human-reliability-as-a-factor-in-nuclear-security/

WINS – World Institute for Nuclear Security. 2019. *Implementing Security by Design at Nuclear Facilities*. Best Practice Guide 4.1, Version 2.1. Retrieved from https://wins.org/document/4-1-security-by-design/

WINS – World Institute for Nuclear Security. 2019. *Managing Internal Threats*. Best Practice Guide 3.4, Version 2.1. Retrieved from https://wins.org/document/3-4-managing-internal-threats/

WINS – World Institute for Nuclear Security. 2019. *Nuclear Material Accountancy and Control in Support of Nuclear Security*. Best Practice Guide 4.4, Version 2.2. Retrieved from https://wins.org/document/4-4-nuclear-material-accountancy-and-control-in-support-of-nuclear-security/

WINS – World Institute for Nuclear Security. 2019. *Nuclear Security Culture*, Best Practice Guide 1.4, Version 3.1. Retrieved from https://wins.org/document/1-4-nuclear-security-culture/

WINS – World Institute for Nuclear Security. 2019. *Security Exercises*. Best Practice Guide 4.6, Version 2.1. Retrieved from https://wins.org/document/4-6-security-exercises/

WINS – World Institute for Nuclear Security. 2019. *Security Performance Metrics*. Best Practice Guide 1.5, Version 2.1. Retrieved from https://wins.org/document/1-5-security-performance-metrics/

## A.6 Glossary

**Assessment** – A review, evaluation, inspection, test, check, surveillance, or audit to determine and document whether items, processes, systems, or services meet specified requirements and perform effectively.

**Event** – A real-time occurrence that adversely affects, or may adversely affect, staff, visitors, the public, property, the environment, or organizational mission. Examples of insider threat events are sabotage, theft, espionage, fraud, and competitive advantage.

**Finding** – An assessment result of noncompliance to procedural, contractual, or regulatory requirements or a failure to meet minimum standards or performance expectations that warrant management attention.

**Good Practice** – An innovative approach or negative experience shared to promote successes or prevent recurrence of negative events; a good practice generally represents a preferred approach that produces desirable results.

**Insider -** An insider is generally defined as a person who has, or once had, authorized access to an organization's critical assets (e.g., network, system, data, materials, or facilities).

**Insider Threat** – A person who has, or once had, authorized access to an organization's critical assets (e.g., network, system, data, materials, or facilities) and uses that access to negatively impact the confidentiality, integrity, and availability of those assets. Insider threats are individuals motivated to act in contravention of law or policy and which can result in an event with adverse effects.

**Issue** – An inclusive term used to define a problem that requires management attention and has a reasonable potential to cause adverse consequences to operations, the environment, safety, security, or quality. Issues include failures, malfunctions, deficiencies, defective items, and non-conformance.

**Opportunity for Improvement** – An assessment result that meets minimal standards or performance expectations. This is not a finding but a recommendation to improve reliability, effectiveness, and/or efficiency of a service, system, policy, or procedure.

**Program Evaluation** – A systematic method for collecting, analyzing, and using information to answer questions about projects, policies, and programs, particularly about their effectiveness and efficiency.

**Self-Assessment** – A periodic, introspective analysis of one's own organization/program/ project to determine whether the activities are properly focused on achieving desired results. Self-assessments can include an evaluation of programmatic compliance, process efficiency, customer satisfaction, whether goals/objectives are being met, or any combination, with the emphasis on issues that affect performance.

# Appendix B – Exercise Tables

## Self-Assessment Readiness Checklist

| Collected | N/A | ITEM DESCRIPTION | COMMENTS |
|---|---|---|---|
| DOMAIN 1 – National Legal and Regulatory Framework | | | |
| ☐ | ☐ | Local, regional, or national guidance or directives on mitigating insider threats | |
| ☐ | ☐ | National threat assessment or DBT | |
| ☐ | ☐ | Trustworthiness and reliability regulation and/or requirements | |
| ☐ | ☐ | Legislation regarding criminal offenses and illicit trafficking in nuclear and other radioactive materials | |
| DOMAIN 2 – Facility Management and Planning | | | |
| ☐ | ☐ | ITM policy and program documentation | |
| ☐ | ☐ | Security plan | |
| ☐ | ☐ | Response plan | |
| ☐ | ☐ | Emergency plan | |
| ☐ | ☐ | Operators/material handlers personnel requirements | |
| ☐ | ☐ | Operations schedules | |
| ☐ | ☐ | Operating standards, special procedures, or directives | |
| ☐ | ☐ | Security procedures or directives | |
| DOMAIN 3 – Personnel Security for Trustworthiness and Reliability | | | |
| ☐ | ☐ | Trustworthiness and reliability program criteria and guidance documents | |
| ☐ | ☐ | List of positions with unescorted access and authority to vital areas and nuclear or other radioactive materials | |
| ☐ | ☐ | List of pre-screening measures | |
| ☐ | ☐ | Continuous evaluation policies and procedures | |
| ☐ | ☐ | Insider threat determination procedure | |

| Collected | N/A | ITEM DESCRIPTION | COMMENTS |
|---|---|---|---|
| ☐ | ☐ | Disciplinary policy | |
| ☐ | ☐ | Access revocation policy and procedure | |
| DOMAIN 4 – Physical Protection System | | | |
| ☐ | ☐ | Physical protection system requirements | |
| ☐ | ☐ | Training documentation for overpacks, material containers, delay systems, lock and key control, and shipment vehicles | |
| ☐ | ☐ | Response force training, qualifications, policies, and procedures | |
| ☐ | ☐ | Alarm procedures | |
| ☐ | ☐ | Role-based access control policies | |
| ☐ | ☐ | Search and seizure procedures | |
| ☐ | ☐ | Vehicle and personnel search policy/procedure | |
| ☐ | ☐ | Security incident/Site emergency and site facility plans | |
| DOMAIN 5 – Nuclear Material Accounting and Control | | | |
| ☐ | ☐ | Material inventory monitoring schedule | |
| ☐ | ☐ | Materials segregation procedure | |
| ☐ | ☐ | List of tools, techniques, and procedures implemented to detect unauthorized removal of nuclear material | |
| DOMAIN 6 – Cybersecurity | | | |
| ☐ | ☐ | Facility cybersecurity policy | |
| ☐ | ☐ | Facility cyber incident response plan | |
| ☐ | ☐ | Network system design | |
| ☐ | ☐ | Vendor trustworthiness and reliability conformance | |
| DOMAIN 7 – System Evaluation and Performance Assurance | | | |
| ☐ | ☐ | Performance assurance program plan | |
| ☐ | ☐ | Threat assessment or DBT | |
| ☐ | ☐ | Security performance metrics | |

| Collected | N/A | ITEM DESCRIPTION | COMMENTS |
|---|---|---|---|
| DOMAIN 8 – Nuclear Security Culture | | | |
| ☐ | ☐ | Personnel risk indicators, behavioral observation program guidance, checklists | |
| ☐ | ☐ | Training curriculum and compliance rates | |
| ☐ | ☐ | Recent findings and corrective action plans focused on insiders and insider threat | |
| ☐ | ☐ | Employee assistance program documentation | |
| ☐ | ☐ | Organization security policy and communications plan | |

## Assess Your Organization's Preparedness to Counter Insider Threat

| Characteristic | Strongly Agree 5 points | Agree 4 points | Neutral 3 points | Disagree 2 points | Strongly Disagree 1 point |
|---|---|---|---|---|---|
| The effective implementation of policies, security measures and procedures to manage internal threats is a core organizational value. | | | | | |
| Trustworthiness programs and practices have been implemented. | | | | | |
| The staff believes periodic screening (drugs, alcohol, etc.) is acceptable. | | | | | |
| Cybersecurity forms an integral part of the security program. | | | | | |
| The security program considers cyber-security's impact on physical security. | | | | | |
| A comprehensive vulnerability analysis (VA) has been conducted that clearly defines roles and responsibilities, the separation of duties, and access to sensitive materials and locations. | | | | | |
| Staff and contractors strongly support the management of internal risks and believe it is important for their work, personal safety, and the reputation of the organization. | | | | | |
| Employees quickly notice and report suspicious behavior. | | | | | |
| Management recognizes the value of strong internal controls, encourage a culture of teamwork, and has an established code of conduct including behavioral standards. | | | | | |
| Strong and effective action is taken against individuals who violate the behavioral values of the organization. | | | | | |
| Reassessment of risks and vulnerabilities, including internal threats, is conducted periodically and used as an important input for enhancing the organization's security. | | | | | |
| Security awareness programs, address potential internal threats and the need for constant vigilance. | | | | | |
| There is a good level of access control, and the separation of duties/responsibilities is enforced. | | | | | |
| Staff feel comfortable reporting observations or information that could indicate a potential internal threat. | | | | | |
| **TOTAL** | | | | | |

## Compare Capacity Across Domains

| Domain | Domain Total | | Number of Statements | Average |
|---|---|---|---|---|
| 1. National, Legal, and Regulatory Framework | | ÷ | 10 | |
| 2. Facility Management and Planning | | ÷ | 10 | |
| 3. Personnel Security | | ÷ | 10 | |
| 4. Physical Protection | | ÷ | 10 | |
| 5. Nuclear Material Accounting and Control | | ÷ | 10 | |
| 6. Cybersecurity | | ÷ | 11 | |
| 7. System Evaluation and Performance Assurance | | ÷ | 10 | |
| 8. Nuclear Security Culture | | ÷ | 11 | |
| **Total** | Sum the above | ÷ | Sum the above (82) | |

## Domain 1 – National, Legal, and Regulatory Framework

| | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| | **5 points** | **4 points** | **3 points** | **2 points** | **1 point** |
| **1.1** The country has established national-level legislation and requirements for the protection of nuclear and other radioactive materials, facilities, and/or activities. | | | | | |
| **1.2** The country has a designated nuclear regulator and/or competent authority responsible for oversight and implementation of nuclear security requirements. | | | | | |
| **1.3** The country encourages cooperation between nuclear regulator/competent authority and other agencies (law enforcement, border security, commerce, etc.) for safety and security of nuclear and other radioactive materials. | | | | | |
| **1.4** Nuclear regulator/competent authority develops regulations and requirements to establish trustworthiness and reliability for all persons with access to sensitive data, information, materials, or facilities. | | | | | |
| **1.5** The country or regulator has developed and periodically revises a national threat assessment or design-basis threat (DBT). | | | | | |
| **1.6** The country has established domestic laws for prosecution of criminal or intentional acts involving or directed at nuclear and other radioactive materials, facilities, and/or activities. | | | | | |
| **1.7** The country has established laws, policies, and guidance to combat illicit trafficking in nuclear and other radioactive materials. | | | | | |
| **1.8** The country cooperates with and seeks assistance from nuclear security-oriented organizations (e.g., International Atomic Energy Agency) on nuclear security matters. | | | | | |
| **1.9** The country uses a risk-informed, graded approach to nuclear security. | | | | | |
| **1.10** The country is a subscriber to INFCIRC/908 | | | | | |
| **Domain 1 Total** | | | | | |

**Notes:**

## Domain 2 – Facility Management and Planning

| | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| | **5 points** | **4 points** | **3 points** | **2 points** | **1 point** |
| **2.1** Organization/facility has an ITM policy based on regulatory requirements and the national threat assessment or DBT. | | | | | |
| **2.2** The ITM policy documents are incorporated into the overall facility security plan. | | | | | |
| **2.3** ITM preventive and protective security measures use a graded approach to protect targets with the highest consequence. | | | | | |
| **2.4** Administrative and operational measures provide defense-in-depth and serve a key role in the development and implementation of the ITM program. | | | | | |
| **2.5** Facility uses “separation of duties” to limit an insider’s ability to obtain access, authority, and/or knowledge needed to conduct a malicious act. | | | | | |
| **2.6** Facility standard operating procedures allow deviations in procedure to be readily detected and challenged | | | | | |
| **2.7** The implementation of corrective actions is based on security incidents. | | | | | |
| **2.8** Facility security, contingency, and emergency plans focus on preventing further negative consequences and securing nuclear material and facilities after malicious activities. | | | | | |
| **2.9** Security plans and programs, (including ITM) are updated regularly to reflect changes in threat, operations, legislation, and regulation. | | | | | |
| **2.10** Facility has a formal ITM program as a distinct function to support nuclear security. | | | | | |
| **Domain 2 Total** | | | | | |

**Notes:**

## Domain 3 – Personnel Security for Trustworthiness and Reliability

| | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| | **5 points** | **4 points** | **3 points** | **2 points** | **1 point** |
| **3.1** Facility operators implement state-, regulator-, and competent authority-defined personnel security measures. | | | | | |
| **3.2** The facility/organization's Personnel Security Program is developed in line with nuclear regulator/competent authority guidance using a graded approach, based on risk and commensurate to the category of the nuclear material and the consequences that could result from a malicious act of theft or sabotage. | | | | | |
| **3.3** Guidelines for trustworthiness assessments and reliability determinations clearly define the criteria for conducting assessments and making determinations and provides well-defined procedures for facility implementation. | | | | | |
| **3.4** Pre-screening measures (e.g., background check) are used to verify an individual's credibility and reliability before hire. | | | | | |
| **3.5** Facility/organization periodically reviews and evaluates backgrounds of personnel with access to sensitive information, materials, equipment, or facilities. | | | | | |
| **3.6** Facility/organization periodically reviews and evaluates backgrounds of personnel with authorized unescorted access to risk-significant materials, systems, or information. | | | | | |
| **3.7** Continuous evaluation policies and procedures enable identification of new personnel issues or circumstances that might represent a reliability, safety, and/or security concern (e.g., stress, physical or emotional impairment, illegal substance use, substance or alcohol abuse). | | | | | |
| **3.8** Individuals identified as potential insider threats are denied unescorted access to facilities, risk-significant materials, systems, or information. | | | | | |
| **3.9** Facility procedures/policies contain processes for identifying and implementing corrective actions and for invoking disciplinary actions, when appropriate. | | | | | |
| **3.10** Access revocation policies and procedures are documented and applied to potential insider threats, individuals changing job roles/functions, and individuals who are separating from the facility/organization (e.g., retirement, termination). | | | | | |
| **Domain 3 Total** | | | | | |

**Notes:**

## Domain 4 – Physical Protection System

| | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| | 5 points | 4 points | 3 points | 2 points | 1 point |
| **4.1** The facility physical protection system includes technical, administrative, and operational measures designed to provide defense-in-depth to secure materials while in use, storage, or transit. | | | | | |
| **4.2** Engineered and automated access controls (e.g., two-person, multifactor biometrics) are implemented to permit only authorized individuals into the facility, vital areas, risk-significant materials, systems or information. | | | | | |
| **4.3** Alarm systems provide automated notifications for high-priority alarms and unauthorized access attempts via short message service (SMS)/text message, email, and/or auto-dialer to at least two individuals responsible for alarm adjudication. | | | | | |
| **4.4** Role-based access control authorizations are based on the principle of least privilege. | | | | | |
| **4.5** Multiple, complementary detection technologies are used for surveillance, identification of unauthorized access/intrusion, and to indicate tampering of critical assets and system components. | | | | | |
| **4.6** Tie-downs, restraints, anchors, in-device delay kits (device hardening), high-security locks, and other barriers are used to minimize unauthorized removal. | | | | | |
| **4.7** Response force policies and procedures are documented and included in the overall facility security plan. | | | | | |
| **4.8** Security personnel routinely conduct vehicle and personnel searches at critical ingress/egress points and procedures include use of metal and radiation detectors. | | | | | |
| **4.9** Location and status of materials in transit/shipment is continuously updated, with appropriate personnel and procedures for transit/shipment in place for emergency/incident response. | | | | | |
| **4.10** Facility/organization has a multi-year security exercise plan derived from the threat assessment or DBT, and the plan includes performance testing of administrative, technical, and operational measures. | | | | | |
| **Domain 4 Total** | | | | | |

**Notes:**

## Domain 5 – Nuclear Material Accounting and Control

| | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| | **5 points** | **4 points** | **3 points** | **2 points** | **1 point** |
| **5.1** Nuclear material handling and transportation activities are only conducted by trained and authorized personnel. | | | | | |
| **5.2** All nuclear materials are secured in a locked and alarmed room/facility when not in use. | | | | | |
| **5.3** Nuclear materials are physically monitored between regularly scheduled inventories. | | | | | |
| **5.4** Accountancy balances are maintained in near real-time. | | | | | |
| **5.5** Alarms, service denial, and lockdowns are initiated as soon as anomalies or nonconformances are detected. | | | | | |
| **5.6** Facility/organization promptly detects, investigates, and issues corrective actions to resolve irregularities. | | | | | |
| **5.7** Random spot checks and targeted audits are conducted on both physical materials and data stored in the NMAC system. | | | | | |
| **5.8** Empty and non-nuclear material containers are segregated and removed from the accounting balance area. | | | | | |
| **5.9** Tags, bar codes, and readers are used to track material movement and facilitate rapid stock inventories. | | | | | |
| **5.10** NMAC system provides information on the isotopic composition, quantity, type, location, use and movement of nuclear materials. | | | | | |
| **Domain 5 Total** | | | | | |

**Notes:**

## Domain 6 – Cybersecurity

| | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| | **5 points** | **4 points** | **3 points** | **2 points** | **1 point** |
| **6.1** Computer-based systems and networks are monitored, inspected, and assessed regularly to validate compliance with policies and procedures and to detect suspicious activities. | | | | | |
| **6.2** Security measures such as firewalls, anti-virus and malware detection software, intrusion detection, and network segmentation are implemented to prevent or detect unintentional or malicious incidents. | | | | | |
| **6.3** Logical access controls are implemented (passwords, two- or three-factor authentication, managed user rights) to impede unauthorized access to a system and prevent security incidents. | | | | | |
| **6.4** Facility enforced "separation of duties" compartmentalizes and prevents employees from accessing computer-based information and services that are not required for their job/role. | | | | | |
| **6.5** Sensitive computer-based systems are monitored, controlled, and send event notification alerts to cybersecurity response personnel. | | | | | |
| **6.6** Facility conducts computer security training, education, and awareness. | | | | | |
| **6.7** Network traffic is characterized. Baselines are established to detect internal and external anomalies indicative of unintentional or malicious activities to sensitive data and systems. | | | | | |
| **6.8** Cyber and physical security teams coordinate event response and investigation. | | | | | |
| **6.9** Facility/organization computing infrastructure is designed with multiple zones that provide an increasing number of barriers (cyber, physical, procedural). | | | | | |
| **6.10** System design incorporates redundancy or other fault-tolerant design approach. | | | | | |
| **6.11** Information technology vendors and contractors are subject to trustworthiness and reliability requirements. | | | | | |
| **Domain 6 Total** | | | | | |

**Notes:**

## Domain 7 – System Evaluation and Performance Assurance

| | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| | **5 points** | **4 points** | **3 points** | **2 points** | **1 point** |
| **7.1** Facility/organization conducts performance testing based on approved performance test plans. | | | | | |
| **7.2** Performance assessment tests are informed by and derived from the threat assessment or DBT. | | | | | |
| **7.3** Performance testing realistically evaluates and verifies the effectiveness of the protection program, trains personnel, identifies areas requiring system improvements, validates improvements, and motivates personnel. | | | | | |
| **7.4** The assessment process includes establishing and documenting key performance metrics and quality assurance practices for people, processes, technologies, and the operating environment. | | | | | |
| **7.5** Security performance metrics are used to evaluate and recommend security improvement options. | | | | | |
| **7.6** Vulnerabilities or nonconformances identified during performance tests are addressed through corrective actions. | | | | | |
| **7.7** Evaluation and assessment are used at all phases of the facility life cycle to optimize physical protection during operations and decommissioning. | | | | | |
| **7.8** Regular tests, assessments, and inspections verify that the physical system reflects security-by-design documents and that the effectiveness of the insider protection program is as expected based on the nuclear security assessment program. | | | | | |
| **7.9** Security performance assessments data and reporting supports regulatory inspections and audits. | | | | | |
| **7.10** Sensitive/confidential performance assessment data and analysis are properly safeguarded and limited to personnel with a documented need-to-know. | | | | | |
| **Domain 7 Total** | | | | | |

**Notes:**

## Domain 8 – Nuclear Security Culture

| | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| | **5 points** | **4 points** | **3 points** | **2 points** | **1 point** |
| **8.1** Security policy is documented, accessible and familiar to personnel. | | | | | |
| **8.2** Senior manager commitment to security is demonstrated through their words and actions. | | | | | |
| **8.3** Security roles and responsibilities for all personnel are well defined and understood. | | | | | |
| **8.4** Facility/organization holds both initial and periodic training on the potential for unintentional and malicious insider threats and their consequences. | | | | | |
| **8.5** Facility/organization has developed a security communication program to educate staff and reinforce organizational values and expectations. | | | | | |
| **8.6** Management monitors staff coping skills, stress, and fatigue levels. | | | | | |
| **8.7** Personnel are encouraged to report security concerns. | | | | | |
| **8.8** The organization has a formal process for handling employee grievances. | | | | | |
| **8.9** The organization has a well-developed employee assistance program (access to counseling, educational services, etc.). | | | | | |
| **8.10** Management holds personnel accountable for their behavior. | | | | | |
| **8.11** Personnel at the organization adhere to security procedures. | | | | | |
| **Domain 8 Total** | | | | | |

**Notes:**