Funded by the European Union

CBRN Centres of Excellence
An initiative of the European Union

Information Security Management System Planning for CBRN Facilities

With the support of

United Nations Interregional Crime and Justice Research Institute

Action Implemented by

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Funded by the European Union

CBRN Centres of Excellence
An initiative of the European Union

UNICRI Project 19

Information Security Management System Planning for CBRN Facilities

Prepared by the Pacific Northwest National Laboratory within the framework of the Project 19 of the European Union Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative (EU CBRN CoE) entitled:

“Development of procedures and guidelines to crate and improve security information management systems and data exchange mechanisms for CBRN materials under regulatory control.”

December 2015

unicri
United Nations
Interregional Crime and Justice
Research Institute

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

The document has been produced with the assistance of the EU. The information and views set out in this document are those of the author(s) and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

The contents of this document do not necessarily reflect the views or policies of the United Nations, UNICRI or contributory organizations, or do they imply any endorsement. While reasonable efforts have been made to ensure that the contents of this document are factually correct and properly referenced, UNICRI does not accept responsibility for the accuracy or completeness of the contents, and shall not be liable for any loss or damage that may be occasioned directly or indirectly through the use of, or reliance on, the contents of this publication. The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations and UNICRI concerning the legal status of any country, territory or boundaries. This publication has not been formally edited by UNICRI.

Summary

Information assets, including data and information systems, need to be protected from security threats. To protect their information assets, chemical, biological, radiological, and nuclear (CBRN) facilities need to design, implement, and maintain an information security program. An information security management system (ISMS) is at the core of an information security program. The ISMS is a set of policies, practices, and technologies that work together to protect the security of information. The ISMS implements security controls that cover the management, operational, and technical aspects of security. To achieve its security goals, an information security program needs to adopt a life cycle perspective that incorporates security concepts during the design, acquisition, installation, operation, maintenance, and decommissioning phases of information assets and systems.

The guidance provided in this document is based on international standards, best practices, and the experience of the information security, cyber security, and physical security experts on the document writing team. The document was developed within the scope of Project 19 of the European Union Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative.

This document is the second in a series of three documents produced by Project 19. The first document in the series, *Information Security Best Practices for CBRN Facilities*[1], provides recommendations on best practices for information security and high-value security controls. The third document in the series, *How to Implement Security Controls for an Information Security Program at CBRN Facilities*[2], provides risk-based guidance on selecting security controls to implement the ISMS.

The current document focuses on ISMS planning. It describes a risk-based approach for information security that is based on the sensitivity of the data developed, processed, communicated, and stored on facility information systems. The sensitivity of the information it contains (e.g., unrestricted, restricted, confidential, or secret), or might contain, determines the sensitivity of the information asset. The greater the sensitivity of the information asset, the more rigorous should be the application of security controls. However, not all facilities can afford to purchase, install, operate, and maintain expensive security systems; therefore, decisions on information security have to balance considerations of security risk and resource constraints. When resources are limited, information security investments should focus on what provides the greatest risk reduction, given the available resources.

Two major types of plans govern an ISMS: risk management and security. The risk management plan identifies and tracks threats and vulnerabilities to the CBRN facility, identifies how these threats will be responded to, and documents the organization's risk monitoring approach. The risk management plan has three components:

- Risk Assessment
- Risk Response
- Risk Monitoring.

[1] UNICRI - United Nations Interregional Criminal Justice Research Institute. 2015a. *Information Security Best Practices for CBRN Facilities*. United Nations Interregional Criminal Justice Research Institute, Turin, Italy.
[2] UNICRI - United Nations Interregional Criminal Justice Research Institute. 2015b. *How to Implement Security Controls for an Information Security Program at CBRN Facilities.* United Nations Interregional Criminal Justice Research Institute, Turin, Italy.

The security plan provides a framework for implementing the organization’s information security strategies. The security plan covers:

- Business Environment
- Asset Management
- Security Control Implementation
- Configuration Management
- Contingency Planning and Disaster Recovery
- Incident Response
- Monitoring and Auditing
- Awareness and Training.

Acknowledgments

This document was prepared by a team of cyber and information security researchers from the Pacific Northwest National Laboratory in the United States, the National Nuclear Laboratory in the United Kingdom, and the University of Glasgow in the United Kingdom. The U.S.-based members of the team are:

Joseph Lenaeus
Pacific Northwest National Laboratory

Lori Ross O'Neil
Pacific Northwest National Laboratory

Rosalyn Leitch
Pacific Northwest National Laboratory

Cliff Glantz
Pacific Northwest National Laboratory

Guy Landine
Pacific Northwest National Laboratory

Janet Bryant
Pacific Northwest National Laboratory

The European-based members of the team are:

John Lewis
National Nuclear Laboratory

Gemma Mathers
National Nuclear Laboratory

Robert Rodger
National Nuclear Laboratory

Christopher Johnson
University of Glasgow

The document's technical editor was Cornelia Brim (Pacific Northwest National Laboratory). Administrative and management support was provided by Emily Davis, Josh Byrd, Monica Chavez, Keith Freier (all of Pacific Northwest National Laboratory), and other members of the authors' organizations.

This document was produced within the scope of Project 19 of the European Union Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative. The initiative is implemented in cooperation with the United Nations Interregional Crime and Justice Research Institute and the European Commission Joint Research Center. The initiative is developed with the technical support of relevant international and regional organizations, the European Union Member States, and other stakeholders, through coherent and effective cooperation at the national, regional, and international level.

Special thanks to Odhran McCarthy and the staff at the United Nations Interregional Crime and Justice Research Institute for their support, patience, and technical guidance during this project.

Acronyms and Abbreviations

CBRN	chemical, biological, radiological, and nuclear
DMZ	demilitarized zone
DNS	domain name system
FIPS	Federal Information Processing Standard
HIDS/HIPS	host intrusion detection system and host intrusion prevention systems
IDS	intrusion detection systems
IP	Internet protocol
IPsec	Internet protocol security
ISMS	information security management system
ISO/IEC	International Organization for Standardization (ISO) and the International Electrotechnical Commission
IT	information technology
LAN	local area network
NIDS/NIPS	network intrusion detection system and network intrusion prevention systems
NIST	U.S. National Institute of Standards and Technology
SIEM	security information event management
SME	subject matter expert
SSL	secure sockets layer
syslog	event logging system
TLS	transport layer security
UNICRI	United Nations Interregional Crime and Justice Research Institute
USB	universal serial bus
VPN	virtual private networks

Contents

Figures

1.0 Introduction

This document is designed to assist organizations in developing plans for a risk-based, cost-effective information security program. In particular, this guidance is intended for facilities that are tasked with creating, using, storing, or disposing of chemical, biological, radiological, and nuclear (CBRN) materials. This document may be used by management, planners, and other workers at CBRN facilities and their contractors (including suppliers). It may be used by managers with parent organizations that have supervisory responsibilities for CBRN facilities. It may also be used by competent authorities that have regulatory responsibilities for CBRN facilities. The guidance provided in this document may also be used to support information security at other types of facilities (i.e., those that do not involve CBRN materials), that support critical infrastructure or provide other business functions that involve sensitive information and information systems.

The systematic protection of information requires a comprehensive information security program that is implemented through an information security management system (ISMS). An ISMS is a set of policies, procedures, practices, technologies, and responsibilities that protect the security of information. The protection of information involves cyber security (i.e., computer security), physical security, and personnel security. Attacks on information security may involve an attempt to exploit just one type of security or it may involve blended attacks (i.e., hybrid attacks) that attempt to exploit vulnerabilities in more one type of security (e.g., a cyberattack to exploit a personnel security database or a physical security system). Information security also involves protecting infrastructure resources upon which information security systems rely (e.g., electrical power, telecommunications, and environmental controls).

Two major types of plans make up the organization's ISMS: risk management and security. The risk management plan identifies and tracks threats and vulnerabilities to the CBRN facility (i.e., the organization), identifies how these threats will be responded to, and documents the organization's risk monitoring approach. It has three components:

- Risk Assessment
- Risk Response
- Risk Monitoring.

The security plan provides a framework for implementing the organization's information security strategies and covers:

- Business Environment
- Asset Management
- Security Control Implementation
- Configuration Management
- Contingency Planning and Disaster Recovery
- Incident Response
- Governance
- Monitoring and Auditing
- Awareness and Training.

In this document, the reader will be introduced to risk management and security plans and the key components of these plans. Guidance is provided on the structure and content of these plans. Examples are provided to illustrate, though incompletely, the type of language various sections of the planning documents might contain. These examples are not intended to provide word-for-word guidance for an actual CBRN facility. Their purpose is to illustrate how plan authors might begin to develop information security plans for a hypothetical CBRN facility

The guidance provided in this document for information security planning is presented from a risk management perspective. Not all facilities can afford to purchase, install, operate, and maintain expensive security systems; therefore decisions on information security have to balance considerations of security risk and resource constraints. When resources are limited, information security investments should focus on what provides the greatest risk reduction for the available resources.

1.1 Document Context

This document is the second in a series of three information security guidance documents produced within the framework of Project 19 of the European Union CBRN Risk Mitigation Centres of Excellence Initiative. The initiative is implemented in cooperation with the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the European Commission Joint Research Center. The initiative is developed with the technical support of relevant international and regional organizations, the European Union Member States and other stakeholders, through coherent and effective cooperation at the national, regional, and international level.

Project 19 is tasked with providing guidance on the security of information technology (IT) structures and data exchange mechanisms for CBRN facilities. This includes providing information on the management, operational, and technical security controls needed to address threats, characterize adversaries, identify vulnerabilities, and enhance defense and mitigation capabilities. The key objective of the project is to help CBRN security managers, IT/cyber security managers, and other decision makers typically involved in acquiring, auditing, regulating, and disposing of information to develop and implement appropriate and cost-effective information security programs.

The first of the three documents in the Project 19 Information Security series is *Information Security Best Practices for CBRN Facilities* (UNICRI 2015a) and is referred to as the "Best Practices" document. This document provides a high-level description of the best practices that support the development of an effective information security program. It provides a description of high-value security controls. The third document in the series, *How to Implement ISMS Security Controls Using a Risk Based Approach at CBRN Facilities* (UNICRI 2015b), is referred to as the "How-to" document. It provides a guide for selecting security controls that can be used to implement information security plans and policies.

In addition to the three documents, a two-day teach-the-teacher workshop on information security for CBRN facilities has been prepared. That workshop is designed to introduce the need for information security to CBRN facility decision makers and others with oversight responsibilities for CBRN materials and facilities.

1.2 Sources of Information Security Planning Guidance

The guidance provided in this document is informed by a number of generally accepted standards and guidance documents. These include a comprehensive series of guidance documents prepared by the U.S. National Institute of Standards and Technology (NIST) and standards produced by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), typically shown as ISO/IEC (listed below).

- NIST Special Publication 800-30 Revision 1 *Information Security: Guide for Conducting Risk Assessments.* (http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf) (NIST 2012a)

- NIST Special Publication 800-53 Revision 4 *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST 2013)
- NIST SP 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View* (NIST 2011c)
- NIST SP 800-53A *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans* (NIST 2014)
- NIST "Cybersecurity Framework" (NIST 2015)
- ISO/IEC 27001 *Information security management* (ISO/IEC 2015a)
- ISO/IEC 27002:2013 *Information Technology—Security techniques—Code of practice for information security controls* (ISO/IEC 2015b)
- ISO/IEC 27005:2011 *Information Technology—Security techniques—Information security risk management* (ISO/IEC 2015c).

The ISO/IEC standards provide a comprehensive approach for establishing an ISMS. However, these standards are expensive to acquire (they are not freely available to CBRN facilities) and can be difficult to understand by those who are not information security specialists. In contrast, the NIST information security guidance is free, easily downloadable from the publicly available NIST webpages, and provides more in-depth explanations. We rely heavily on the NIST guidance in this document because all our readers will be able to quickly review these publications without cost.

1.3 How to Use Information Security Plans

Information security programs should be risk-based. While the same general outline for information security planning documents is followed regardless of the security risk, the level of detail will vary according to the risk level. It is up to the CBRN facility, in consultation with its competent authorities and any parent organization under which the facility operates, to determine the appropriate level of detail and length of its information security planning documents to support its information security plans.

For example, a CBRN facility with a low level of information security risk (e.g., it possesses little or no sensitive information, and would experience minimal consequences if its information security were compromised) may prepare short and simple risk management and security plans. These may be quite easy and inexpensive to develop and implement. In contrast, an organization with a high level of information security risk (e.g., it creates, processes, or stores sensitive or classified information, and would experience substantial consequences if its information security were compromised) may divide its risk management and security plans into multiple planning documents, some of which may be lengthy and detailed. For example, the risk management plan may be broken up into separate risk assessment, risk response, and risk monitoring planning documents and each section of the security plan may be a standalone planning document.

In the following sections, guidance is provided on the structure and content of information security plans. Examples are provided to illustrate, though incompletely, the type of language various sections of the planning documents might contain. As noted earlier, these examples are **not** intended to provide word-for-word guidance for an actual CBRN facility. Their purpose is to illustrate how plan authors might begin to develop information security plans for a hypothetical CBRN facility. Because that hypothetical facility does not exist, and has not been fully characterized by our team of authors, it was impossible to prepare complete plans for that facility. Even if our team could, the differences between our imaginary facility and real-world facilities would ensure that our examples would not be applicable to many real facilities. Readers are requested to use the structure of our plans as guidance for their facilities, but use their own risk- and resource-based assessments and insider knowledge of their CBRN facility to determine the appropriate content for their plans.

In the examples presented in this document, we list specific facility job titles such as ISMS manager, IT manager, physical security manager, facility security director, and others. Large facilities may have individuals with these or similar position titles. Smaller facilities, with fewer staff members, routinely assign multiple roles and the corresponding responsibilities to designated individuals. In Figure 1.1, we illustrate the key information security positions for two small CBRN facilities and one large CBRN facility. For the large CBRN facility—which in this example could be a nuclear power plant or a large chemical manufacturing facility—there are separate positions established for the facility security director, physical security manager, cyber security manager, IT manager, and ISMS manager. For the two small facilities in Figure 1.1, which might be a small pharmaceutical facility and a small biological laboratory, there might only be two people assuming the responsibilities assigned to five people at the large facility. The ways those roles are combined may vary from facility to facility, as illustrated in Figure 1.1.

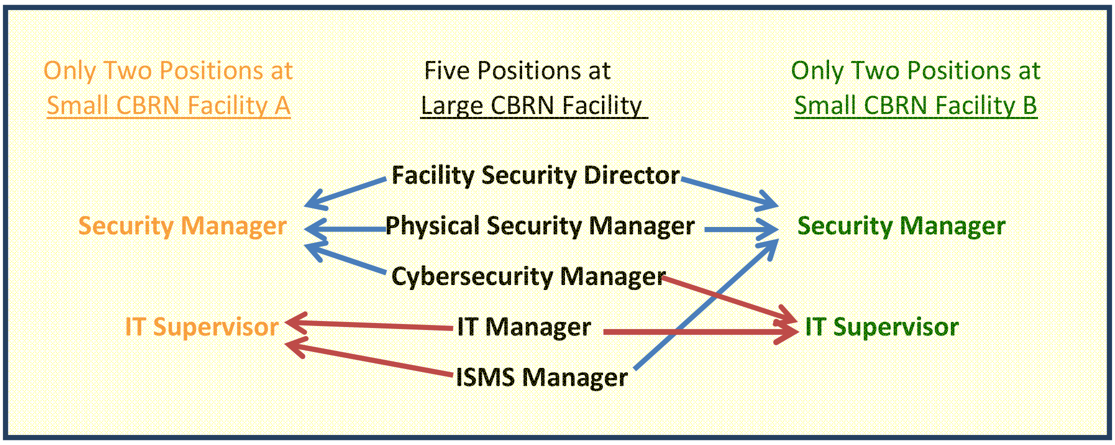

Figure 1.1. Combining Roles at Small Facilities with Limited Staffing

In this document, we refer to a variety of "teams" operating at the CBRN facility. For example, we explicitly mention the following:

- Risk assessment team
- Risk monitoring team
- Risk response team
- Asset management team
- ISMS team
- Cyber security team
- Physical security team
- Configuration management team
- Disaster recovery planning team
- Cyber security incident response team
- Physical security incident response team

- Security monitoring and auditing team.

The word “team” is used loosely. The team concept is employed because assigned activities require either a multidisciplinary skill set or multiple staff members are needed to tackle a large assignment. At large facilities, where there are many information assets, teams typically consist of multiple individuals. At small facilities, there might be too few staff members or too small a scope of work for assignments to be addressed by multiple individuals. In such cases, a team may consist of only one individual. In addition, that one individual may take on the roles and responsibilities assigned to a number of multi-person teams at large facilities. The names of teams and their size may vary significantly from facility to facility. The terminology offered in this document should therefore be modified by each CBRN facility to suit its unique characteristics.

2.0 Risk Management Plan

All computer systems are made up of digital assets. If a digital asset is compromised, it could potentially affect the ability of a system or network to perform its intended function and jeopardize information security. A loss of confidentiality, integrity, or availability of a data system or the information it contains could potentially result in grave impacts for the facility, its parent organization, employees, the government, and/or the public.

The purpose of the risk assessment plan is to identify and characterize potential information security risks. To do this, a facility needs to understand the types of information security threats it may face, the vulnerabilities that may exist in its current information security program, and the consequences of a compromise of its information or information assets[1].

In the Best Practices document (UNICRI 2015a), the following brief discussion is provided on risk:

> ***Risk,*** *specifically* ***information security risk,*** *is the product of the likelihood that something adverse will happen to information and the resulting consequences of that adverse event on those who need to use that information.* ***Likelihood*** *is a function of the characteristics and intentions of the threat agent and the vulnerability of the information and/or information systems.*

However, estimating the likelihood of risk can be difficult. Even the best estimates typically have huge uncertainties. There are a number of reasons for this:

- Lack of an adequate historical database on attacks on information systems, particularly those at CBRN facilities
- Rapid evolution of information security threats, including the advent of new adversaries and the rapid development of new forms of attack (e.g.; new types of malware, new forms of social engineering)
- Rapid sharing of information on the Internet about recently detected vulnerabilities in the hardware, firmware, operating systems, and other software that are used to develop, process, communicate, and store information
- Lag time between identifying a security vulnerability and the time it takes to develop, test, and implement patches or replacements to alleviate that vulnerability.

For these reasons and others, most CBRN facilities feel most comfortable estimating risk based on a general characterization of threats, vulnerabilities, and consequences without attempting to prepare a numerical (i.e., quantitative) estimate of the likelihood of a successful attack.

There are a number of ways to measure risk in simple, qualitative terms. For example, risk can be characterized using three levels—low, medium, and high risk. Alternatively, a semi-quantitative approach using a greater number of risk categories can be used. One approach involves using multiple risk levels ranging from very low to very high. Risk can also be measured in a quantitative manner if there is sufficient quantitative data available to support this type of numerical assessment.

A **threat** represents the intent, capability, and opportunity of an adversary to attack or inflict harm. The magnitude of a threat is dependent on an attacker's motivation, capability, and opportunity. Attackers' motivations include nationalistic, political, economic, social, cultural, religious, and emotional factors. Their capability refers to

[1] In generic terms, an information asset is a collection of information, defined and managed as a single unit so it can be understood, shared, protected and used effectively (The National Archives 2015). For information and cyber security purposes, an information asset is defined as any data, device, or other infrastructure that supports information-related activities. This includes information, hardware, firmware, software, devices, systems, and networks software.

the knowledge, skills, and tools at their disposal to support an attack. Opportunity represents the circumstances that would support the initiation of an attack. For example, an adversary that has a strong motivation to attack (e.g., a group believes that the CBRN facility is harming the health of their families), considerable attack capabilities (e.g., ready access to cyberattack technologies, knowledge of operations at the facility), and ample opportunity to mount an attack (e.g., time and resources) would represent a serious threat. In contrast, an attacker that has limited motivation, minimal capabilities, and few opportunities to mount an attack would represent a minimal threat.

It is important to recognize that the relative interest levels of potential adversaries in attacking a CBRN facility can greatly vary over time. In some cases this variance can be linked to the evolving risk-effort-reward mindset (e.g., Is the payoff for conducting an attack at this point in time worth the effort involved? Am I likely to be caught by law enforcement?). As hinted at earlier, it is also important to recognize that the emergence of new tools and methods, the disclosure of vulnerabilities, motivational changes, and other occurrences can quickly elevate the threat posed by an adversary.

For an attack to succeed, it must exploit some inherent **vulnerability** within the target. The term vulnerability is defined to be a weakness in the physical, electronic, or human factor that could allow a compromise of an asset. If an attack is poorly executed or it attempts to exploit an asset that is adequately defended, the attack will likely be unsuccessful. This basic concept holds true regardless of whether the attack takes place within the physical domain, the cyber domain, or both.

For an attack to have a negative impact on information security there must be **consequences.** Consequences may involve the loss of:

- Confidentiality. This occurs when the attacker gains access to sensitive information, and could result in the disclosure or misuse of that sensitive information.
- Integrity. This occurs when the attacker can modify information and affect its accuracy or reliability. This includes information used by people, IT systems, or control systems that operate facility processes.
- Availability. This occurs when the attacker is able to prevent authorized individuals, IT, or controls systems from accessing facility information in a timely and uninterrupted manner.

Consequences resulting from the loss of confidentiality, integrity, or availability can have tangible impacts on the CBRN facility and the public. The compromise of information assets could contribute to the theft of hazardous materials, the environmental release of hazardous materials, curtailment of facility operations and other business impacts, damage to facility equipment, impacts to the health or safety of workers and the public, damage to the facility's reputation and public image, and regulatory impacts (e.g., increased regulatory oversight, new legal restrictions on facility operations).

One way to quickly evaluate consequences is to use a classification of the sensitivity of the information that needs to be protected. One potential classification scheme for information uses four different levels of sensitivity. The follow are the four example sensitivity levels:

- Secret. Unauthorized access to the information could cause ***severe adverse*** effects.
- Confidential. Unauthorized access to the information could cause ***serious adverse*** effects (but not rising to the level of severe adverse effects).
- Restricted. Unauthorized access to the information could cause ***adverse*** effects (but not rising to the level of serious or severe adverse effect).
- Unrestricted. Unauthorized access to the information could **not** cause ***adverse*** effects.

The adverse effects may be evaluated in terms of their impact on the facility, parent organization, local region, or nation.

Figure 2.1 illustrates this classification method in the form of a pyramid. Secret information is typically the least common type of information at a facility and it needs the most protection. There is often a greater amount of confidential information than secret information. The confidential information requires a slightly reduced level of protection. Restricted information is typically more prevalent than confidential information and the level of protection it requires is somewhat less. Unrestricted information is at the bottom of the pyramid and requires the least amount of security.

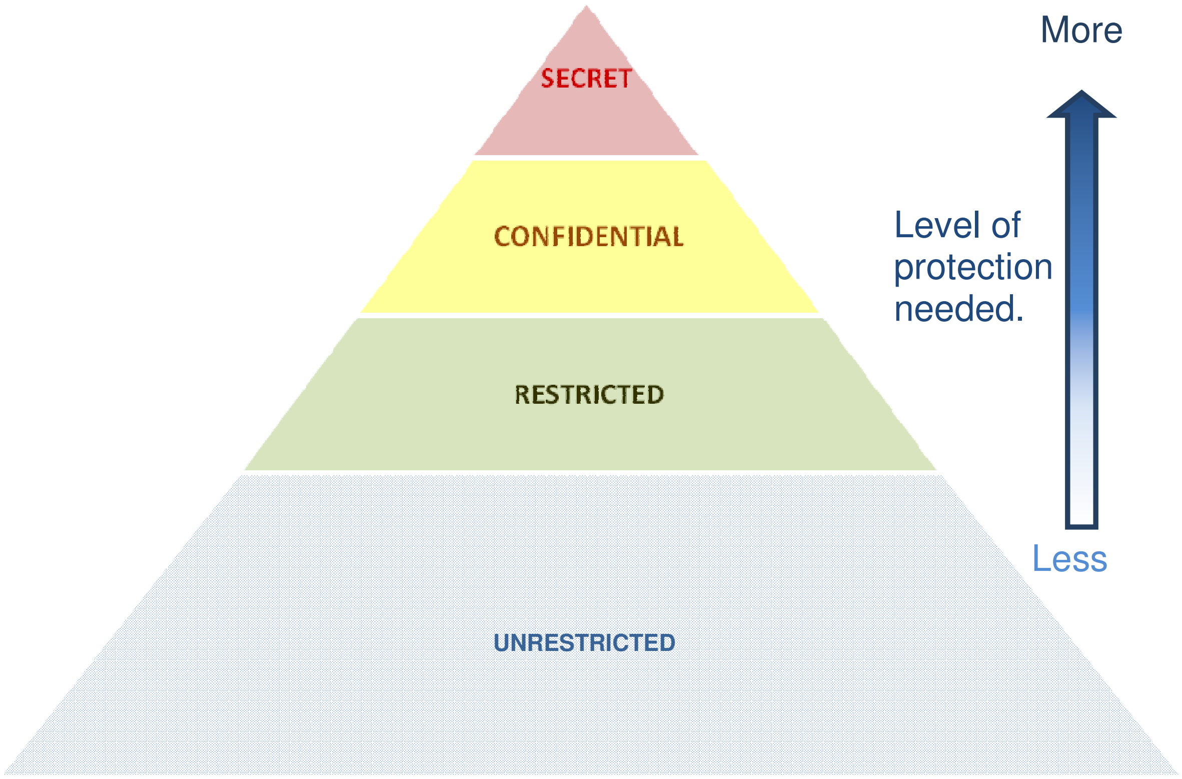

Figure 2.1. The Information Classification Pyramid

As a result of their different classification levels, not all information assets within a CBRN facility are of equal importance. While the compromise of some types of information assets may have a negligible impact, the compromise of others may pose serious consequences. For example, information on the configuration and operation of safety and security systems, which might have a Secret or Confidential designation, poses greater risks than information associated with routine business functions, which may have a Restricted or Unrestricted designation.

The level of digital and physical protection afforded to information assets should be based on classification level. The use of a graded approach ensures that an appropriate share of security resources are applied to information assets based on their risk level. Systems that represent higher levels of risk should receive proportionally more attention and resources than systems that represent comparatively low risks.

The remainder of Section 2 covers the three components of the Risk Management Plan: risk assessment, risk response, and risk monitoring. These components are referred to as separate plans in the following section. These components can be developed as separate planning documents to support risk management planning, or they can be sections in a single risk management planning document.

For each planning component, guidance is provided for developing an introduction, describing the applicability and scope of the plan, the roles of responsibilities for managers and facility staff members, specific policies for implementing the plan, and sources of additional information. Many of these sections contain examples of plan language. As stated at the end of Section 1, these examples are provided to illustrate, though incompletely, the type of language various sections of the planning documents might contain. These examples are not intended to provide word-for-word guidance for an actual CBRN facility.

The management-approved Risk Management Plan, and any associated plans, should be treated as a sensitive documents and protected in accordance with it security classification level. The Risk Management Plan should be reviewed and updated periodically (e.g., once every three years is a common practice). Components of the plan may need to be reviewed and updated more frequently.

2.1 Risk Assessment Plan

2.1.1 Introduction

A risk assessment is a process to identify and estimate risks. It involves characterizing threats, vulnerabilities, and consequences. The introduction to the risk assessment plan presents

- The purpose of the risk assessment activities.
- An outline of the risk assessment process. Figure 2.2 presents an example of the steps in a typical information security risk assessment.
- An introduction to the elements in the risk assessment plan.

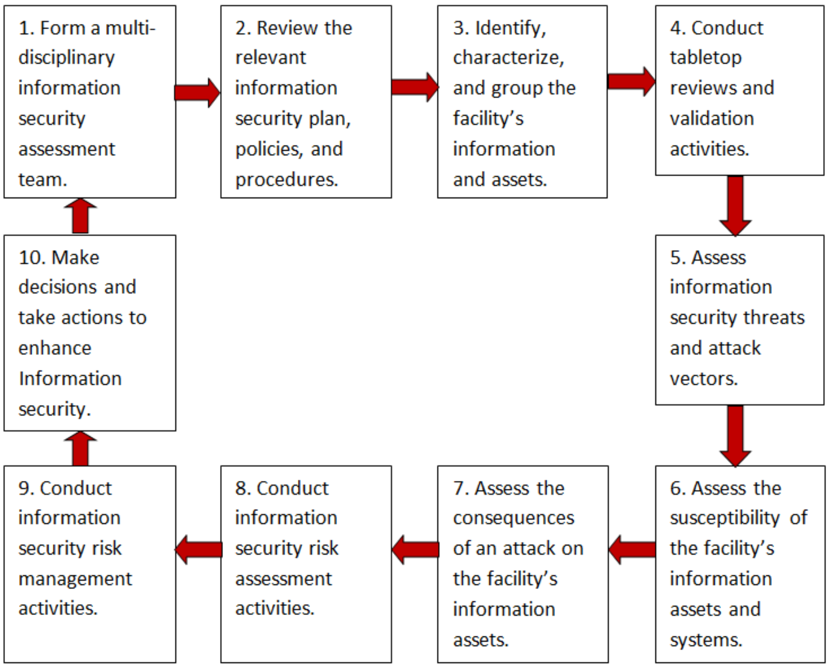
1. Form a multi-disciplinary information security assessment team.
2. Review the relevant information security plan, policies, and procedures.
3. Identify, characterize, and group the facility's information and assets.
4. Conduct tabletop reviews and validation activities.
5. Assess information security threats and attack vectors.
6. Assess the susceptibility of the facility's information assets and systems.
7. Assess the consequences of an attack on the facility's information assets.
8. Conduct information security risk assessment activities.
9. Conduct information security risk management activities.
10. Make decisions and take actions to enhance Information security.

Figure 2.2. The Steps in a Risk Assessment and Management Program

The following is an example:

The risk assessment plan is designed to provide guidance for conducting periodic risk assessments of information assets and systems, with an emphasis on those assets that involve sensitive information. Information from the risk assessment plan will be used to make risk-based, cost-effective risk management decisions in support of the ISMS.

The risk assessment will involve the following steps:

- Select a multidisciplinary team to conduct the risk assessment.
- Acquire information on appropriate information security laws, requirements, technical guidance, policies, and procedures.
- Identify and characterize the facility information assets.
- Conduct a tabletop review of the hardware, firmware, software, connectivity, and security measures for each information asset or system.
- Conduct an inspection of each information asset and its digital connectivity.
- Assess information security threats.
- Assess the security vulnerabilities.
- Assess the consequences of an exploitation of each information asset or system.

In this risk assessment plan, we review the applicability and scope of the risk assessment, roles and responsibilities, risk assessment policies, and sources of information.

2.1.2 Applicability and Scope

In this section, describe the applicability and scope of the risk assessment plan. This includes a summary of key items that are within the scope of this plan and an explicit mention of items that are out of scope. For example, the risk assessment plan's applicability statement should list all the systems that can affect information security and are therefore covered by this plan. Typically, all information systems should be subject to the risk assessment. If a system that contains or may contain sensitive information is excluded from the assessment, it should be noted and the reason for this exclusion justified. Information systems that do not contain sensitive information and are excluded from this risk assessment should also be noted. This section should also define the level of detail of the assessment. For example, it might note that the assessment will involve a review of documentation, the interview of subject matter experts (SMEs), the visual inspection of information system hardware, an examination of software versions (to determine which security updates are installed), a review of which ports are available for use on digital devices, and a review of the configuration of security devices (e.g., firewall and their rule sets). If electronic scanning or penetration testing is permitted or excluded, this should also be noted.

2.1.3 Roles and Responsibilities

In this section, define the staff roles and responsibilities for the risk assessment. This includes the roles and responsibilities of the multidisciplinary team conducting the risk assessment and other personnel who have management responsibilities for the assessment or need to provide information to support the assessments. This includes, but is not limited to, the ISMS manager, the facility's security manager, the IT manager, other senior managers who have oversight for the information security program or whose programs may be affected by risk assessment activities, cyber security specialists, and the SMEs contributing to the assessment. If a parent organization is involved in the risk assessment, their roles and responsibilities should be defined.

The following are examples of the roles and responsibilities for the ISMS manager under this plan.

- The ISMS manager is responsible for the management of the information security program, oversight of program staff, and allocating resources to program activities. This includes the development and execution of the risk assessment plan.

- The ISMS manager shall oversee the development of any procedures required to efficiently implement risk assessment policies.

- The ISMS manager is responsible for ensuring that risk assessments are carried out according to the risk assessment plan. This includes ensuring that an appropriate risk assessment team is selected, is provided with appropriate training and resources to perform their assessment function, and perform their assessments in a timely and appropriate manner.

- The ISMS manager is responsible for reviewing the results of the risk assessment and ensuring it meets the requirements of the risk assessment plan.

- The ISMS manager is responsible for reporting the results of the information security risk assessment to the facility security director and other senior facility managers.

- The ISMS manager is responsible for ensuring that significant findings in the risk assessment are addressed in a timely manner and that the ISMS program meets its risk management objectives.

2.1.4 Policy

In this section, outline the policies governing the risk assessment. Policies may cover such items as how to select the assessment team, establish of rules of engagement between the assessment team and the facility's SMEs, determine what is permitted and what is excluded in the assessment, define the security classification level of the risk assessment report, capture the role of a parent organization in the assessment, and establish budget and schedule constraints for the assessment.

The following are examples of policies that could be established to cover the risk assessment of information assets.

- For each information asset or system under review, the assessment team shall:
    - Review findings from any previous risk assessment and identify corrective actions taken by the facility.
    - Identify and characterize all associated digital hardware, firmware, and software.
    - Obtain network connectivity diagrams from the appropriate SMEs.
    - Trace each digital pathway into or out of the information asset to its termination point (be it another digital device, a link to an external network, a link to the Internet).
    - Identify potential vulnerabilities in the security of the information asset.
    - Identify potential consequences to the asset and the facility if the confidentiality, integrity, or availability of the asset were compromised.
    - Identify the security controls in place to restrict access to the information asset and the configuration setting of these security controls.
    - Record observations in the risk register (or risk log)1.
- Any obstruction or hindrance by facility managers, staff members, contractors, or vendors in performing an assessment of an information asset shall be promptly reported to the ISMS manager.
- If the assessment of an information asset cannot be completed, the unassessed or partially assessed assets and their connectivity shall be listed it in the risk assessment as being “not determined to be secure.”
- The ISMS manager will ensure that the risk assessment is kept current. Major changes in system connectivity or equipment shall warrant a timely reassessment of risk. Even if no changes are reported, the risk assessment shall be repeated at least once every other year, though annually is often preferred, to ensure that new security vulnerabilities have not been inadvertently introduced into the system.

Formal attack tree analyses (see UNICRI 2015a for a description) are typically associated with information security programs and information assets that require a high level of protection. The following are examples of the policies that could be established to govern the use of attack trees analyses for assets requiring a high level of protection.

[1]. The “risk register” is also called the “risk log.” It is a collection of risk information recorded for the facility. It should contain a list of each identified risk, the person who characterized that risk, the nature of the risk, the risk level to the facility, treatment options, existing security controls that address (at least in part) this risk, and potential new security controls that could further reduce this risk.

- Attack tree analyses will be conducted to identify potential methods of attack against key information assets and systems.
- The attack tree analyses will consider cyberattacks, physical attacks, and blended cyber-physical attacks.
- The attack tree analysis will consider scenarios in which there is no intentional malicious action by a facility insider and scenarios in which there is at least one malicious insider participating in the attack.
- The attack tree analyses will assume that the attackers may get facility staff members to perform actions that could support the attack. This may involve social engineering of plant staff members (e.g., getting them to unknowingly download malware on facility computers) or the theft of information from staff members (e.g., steal the staff member's username and password for system access).
- Nodes in the attack tree may be labeled as having a low, medium, or high likelihood of success of compromise if sufficient information is available to approximate this likelihood. Otherwise, the attack tree may be prepared without any likelihood metrics.
- A sufficient number of attack trees will be generated to provide a representative sample of the risks that key information assets and systems may encounter. The attack tree analyses do not have to consider every possibility.

2.1.5 Sources of Information and References

In this section, list the sources of information and references to be used in the risk assessment plan. This might include laws, regulations, standards, company or facility policies and procedures, and other publications. For example, this section might note that NIST Special Publication 800-30, Revision 1, *Information Security: Guide for Conducting Risk Assessments* (NIST 2012a) is a recommended reference to use in the formulation of the risk assessment plan.

2.2 Risk Response Plan

2.2.1 Introduction

An information security program cannot eliminate all information security risks. The purpose of risk response planning according to NIST (2012a) is to:

- Develop alternative courses of action for addressing risk.
- Evaluate these alternative courses of action.
- Determine appropriate courses of action consistent with the organization's security goals, requirements, and resource constraints.
- Prepare to implement appropriate risk responses using selected courses of action.

The risk response plan involves prioritizing, evaluating, and implementing the appropriate security controls to deter, delay, detect, and deny attempts to subvert information security and minimize the consequences of a successful attack. Risk response is achieved through the following options, as outlined in NIST (2012a):

- Risk Acceptance. To accept the potential risk and continue operating the information system as is, or implement security controls to lower the risk to an acceptable level.
- Risk Avoidance. To avoid the risk by eliminating identified vulnerabilities or taking actions that reduce the potential consequences of a successful attack (e.g., promptly turn off certain functions or shut down the system as soon as a potential attack is detected).
- Risk Transfer/Sharing. To transfer or share the risk by enabling options to compensate for the loss. This may involve purchasing insurance or spreading the cost of the consequences resulting from a successful attack over a number of departments, facilities, or consortium of companies.
- Risk Mitigation. To limit the risk by implementing security controls that minimize the adverse consequences (e.g., design systems to fail in a safe and secure manner, develop procedures to allow information systems to be quickly restored from a previous stored and safe configuration).

The goals and mission of an organization should be carefully considered before selecting any single risk response option or set of options.

In this section, introduce the concept of risk response/mitigation and outline the purpose of this plan. For example,

> The facility shall develop, document, and implement a comprehensive and diverse set of protective strategies capable of the timely detection, isolation, and neutralization of attempts to compromise information security. The goal of this risk response plan is to provide an approach that will work to ensure that the design-based functions and capabilities of information systems are maintained. The protective strategies shall exhibit defense-in-depth characteristics ensuring that the failure of any single element of a strategy does not result in successful compromise of an information system. The strategies developed need to protect information systems from various vectors of attack that involve both physical and cyber compromise.
>
> The controls implemented within each layer of security need to be capable of detecting unauthorized activities. Detection shall trigger preplanned security response mechanisms that act to delay or prevent the advance of an attack toward the target of interest. The developed strategies must consider vectors of attack involving both physical and digital compromise of information systems.
>
> In this risk response plan, we review the applicability and scope of risk response activities, roles and responsibilities, risk response policies, and sources of information.

2.2.2 Applicability and Scope

In this section, describe the scope and applicability of the risk response plan. This includes a summary of key items that are within the scope of this plan and an explicit mention of items that are out of scope. For example, the risk response plan's applicability statement should list all the information systems that may be potential targets for risk response activities. Typically, all information assets should be subject to risk response activities, though assets will be prioritized for risk reduction based on the finding of the risk assessment. Information assets or systems that are excluded from risk reduction should be listed and reasons for their exclusion justified.

2.2.3 Roles and Responsibilities

In this section, define the roles and responsibilities for performing risk response and mitigation activities. This includes, but is not limited to, the roles and responsibilities for the ISMS manager, the facility's security manager, the IT manager, other senior managers who have oversight for the information security program or whose programs may be affected by risk response activities, the staff conducting risk response activities, and the SMEs supporting these activities.

The following presents examples of the roles and responsibilities of the ISMS manager under this plan.

- The ISMS manager is responsible for the management of the information security program, oversight of program staff, and allocating resources to program activities. This includes the development and execution of the risk response plan.
- The ISMS manager shall oversee the development of any procedures required to efficiently implement risk response policies.
- The ISMS manager is responsible for ensuring that risk reduction activities are carried out according to the risk response plan. This includes ensuring that an appropriate risk response team is selected, are provided with appropriate training and resources to perform their work, and develop risk response planning options in a timely and appropriate manner.
- The ISMS manager is responsible for reviewing the results of the risk response activities and ensuring they meet the requirements of the risk response plan.
- The ISMS manager is responsible for reporting the results of risk response activities to the facility security director, the cyber security manager and other senior facility managers.
- Responsibility for risk response activities may be shared with the cyber security manager (for issues involving the protection of information assets from cyberattack) and the physical security manager (for issues involving the physical protection of information assets). Shared responsibilities are not an excuse for inactivity. Unresolved disputes between the managers involving risk reduction activities will be resolved by the senior facility manager with oversight responsibility for security.
- The ISMS manager is responsible for ensuring that the risk response recommendations are addressed in a timely manner so that the ISMS program meets it risk management objectives.

2.2.4 Policy

In this section, outline the policies governing the risk response/mitigation activities. These policies should:

- Set the criteria to use for selecting the risk response team
- Set the rules of engagement between the risk response team, the risk assessment team, and the facility's SMEs, and facility managers
- Document information security requirements
- Outline the types of risk responses that are acceptable to the organization (e.g., Is risk transfer/sharing feasible and acceptable at this facility?).
- Select an appropriate set of security controls based on risk and resources
- Provide guidance on how to factor in budget and schedule constraints
- Assign overall responsibility for the facility's risk response to the designated senior manager.

The following are examples of policies that could be established to cover the first two bullets presented above.

- Staff performing risk response and mitigation activities shall:
    - Understand the function and structure of the information assets and systems on which they will perform risk response and mitigation actions; this includes safety, security, and operational functions
    - Have an appropriate level of knowledge of information security, cyber security, and physical security
    - Be trained in facility policies and procedures for making risk-based decisions when selecting and implementation security controls.

- Risk response and mitigation actions will be reviewed by another team member and the ISMS manager prior to implementation.

- The information security risk response team will coordinate all proposed action on digital systems with members of the cyber security team. It is recognized that in some cases, the two teams may have overlapping or identical membership. Any disagreements between the two teams will be moderated by the ISMS manager and the cyber security manager. Any issues that remain unresolved will be decided by the facility security director.

- The risk assessment team shall make all of its assessment information available to the risk response team to support informed risk decisions.

- The risk response team will inform the risk assessment team of all security modifications made to an information system. That will allow these security enhancements to be efficiently captured for future risk assessments.

- All facility SMEs shall cooperate fully with the information security team. Disputes between an SME and an information security team member will be moderated by the ISMS manager and the SME's manager. Any issues that remain unresolved will be decided by the facility security director.

2.2.5 Sources of Information and References

In this section, list the sources of information and references to be used in this risk response plan. This might include laws, regulations, standards, company or facility policies and procedures, and other publications. Inputs from other facility processes and investigations should also be included.

2.3 Risk Monitoring Plan

2.3.1 Introduction

The purpose of risk monitoring is to detect changes in information security risk levels that could occur as a result of changes in the threat environment, the identification of new vulnerabilities, changes in information system operations (e.g., change in the classification level of information on the system, the introduction of new information assets, a change in communication pathways), changes in operational practices, changes in personnel, and changes to deployed security controls. Risk monitoring makes sure that the security controls in place are effective and that any emerging risks are identified so that they can be handled according to the risk management plan (as described in Section 3).

In this section, introduce the concept of risk monitoring and reporting and outline the purpose of the risk monitoring plan. For example, The facility shall develop a risk monitoring plan to detect changes in information security risk levels. These may occur as a result of changes in the threat environment, the identification of new vulnerabilities, changes in facility operations, changes in personnel access requirements or training, identification of new consequences, the deployment of new technologies or the removal of existing technologies, etc. Risk monitoring bridges the gap between periodic risk assessments. It highlights important changes in risk that may occur between the scheduled assessments; particularly those changes that warrant timely action to maintain an appropriate level of information security.

In this plan we discuss the scope and applicability, roles and responsibilities, facility policies, and information sources related to planning for risk monitoring activities.

2.3.2 Applicability and Scope

In this section, the facility describes the applicability and scope of the risk monitoring plan. This includes a summary of key items that are within the scope of this plan and an explicit mention of items that are out of scope. For example, the risk monitoring plan's applicability statement should list all the information systems for which risk monitoring will be conducted. Typically, all information assets should be subject to risk monitoring activities, though some information assets and systems will require a greater level of risk monitoring based on the higher classification level of its information or elevated risk level. Information assets or systems that are excluded from risk monitoring should be listed and the reasons for their exclusion justified.

2.3.3 Roles and Responsibilities

In this section, define the roles and responsibilities for performing risk monitoring and reporting activities. This includes, but is not limited to, the roles and responsibilities for the ISMS manager, the facility's security manager, the IT manager, other senior management who have oversight for the information security program or whose programs may be affected by risk monitoring activities, the staff conducting risk monitoring response activities, and the SMEs supporting these activities.

The following presents examples for the roles and responsibilities of the ISMS manager under this plan.

- The ISMS manager is responsible for the management of the information security program, oversight of program staff, and allocating resources to program activities. This includes the development and execution of the risk monitoring plan.

- Responsibility for risk monitoring activities may be shared with the cyber security manager (e.g., issues involving the protection of information assets from cyberattack) and the physical security manager (e.g., issues involving the physical protection of information assets). Shared responsibilities are not an excuse for inactivity. Unresolved disputes between the managers involving risk reduction activities will be resolved by the senior facility manager with oversight responsibility for security.

- The ISMS manager is responsible for ensuring that risk monitoring activities are carried out according to the risk monitoring plan. This includes the formation of a risk monitoring team, providing personnel with appropriate training and resources to perform their risk monitoring functions, and ensuring risk monitoring activities are performed in a timely and appropriate manner.

- The ISMS manager is responsible for reviewing the results of the risk monitoring activities and ensuring they meet the requirements of the risk monitoring plan.

- The ISMS manager is responsible for reporting the results of risk monitoring activities to the facility's cyber security manager, physical security manager, and facility security director.

- The ISMS manager is responsible for ensuring that appropriate and timely risk reduction activities are taken in response to risk monitoring observations. Problems shall be addressed in a timely manner so that the ISMS program meets it risk management objectives.

2.3.4 Policy

In this section, outline the policies governing the risk monitoring development, implementation, and analysis. The policies should cover changes in the external and internal environment that may change information security risk levels.

The following are a few examples of risk monitoring policies:

- Personnel assigned risk monitoring responsibilities shall receive appropriate training before undertaking these duties.

- Risk monitoring may be performed by different individuals with different areas of responsibility. Areas of responsibility include

    - Monitoring changes in the threat environment. This shall involve reviewing information provided from publicly available sources. It shall also include soliciting and reviewing information that can be provided by local law enforcement, national and international cyber security organizations, national law enforcement and security agencies, hardware and software product manufactures, etc.

    - Monitoring for new information security vulnerabilities. This shall involve reviewing information provided from publicly available sources. It shall also include soliciting and reviewing information that can be provided by national and international cyber security organizations, hardware and software product manufactures, industry peers, etc.

    - Monitoring changes in the consequences of a compromise of information security. This shall involve reviewing information on equipment and process changes from facility managers, system operators, and other facility personnel. It shall also include input from facility and parent organization business experts. It shall include the review of consequence-related information from safety and security organizations, including international, national, and industry organizations.

- Information gathered by different members of the risk monitoring team shall be shared within the team and in particular with those assigned the duties of integrating the information to identify potential changes in risk that might be significant.

- Risk monitoring of information systems is a shared responsibility among staff members with information security, cyber security, and physical security responsibilities. Risk monitoring activities will be coordinated within the facility to provide consistency and continuity in risk monitoring and reporting.

2.3.5 Sources of Information and References

In this section, list the sources of information and references to be used in this risk monitoring plan. This might include laws, regulations, standards, company or facility policies and procedures, and other publications. Inputs from other facility processes, investigations, business offices, etc., should also be included.

3.0 ISMS Security Plan

The purpose of the ISMS security plan is to provide direction for implementing the information security program at the facility. The ISMS security plan provides a framework for presenting security strategies and the roles, responsibilities, and the policies needed to implement those strategies. The components of an integrated ISMS security plan are

- Business environment
- Asset management
- Security control implementation
- Configuration management
- Contingency planning and disaster recovery
- Incident response
- Monitoring and auditing
- Awareness and training.

This section discusses each of these components in the ISMS security plan. These components are referred to as separate plans throughout the remainder of Section 3. These components can be developed and released as separate planning documents to support ISMS security planning, or they can be sections in a single ISMS security planning document.

For each planning component, guidance is provided for developing an introduction, describing the applicability and scope of the plan, the roles of responsibilities for managers and facility staff members, specific policies for implementing the plan, and sources of additional information. In many of these sections examples of plan language are provided. As stated at the end of Section 1, these examples are provided to illustrate, though incompletely, the type of language various sections of the planning documents might contain. These examples are not intended to provide word-for-word guidance for an actual CBRN facility.

The ISMS security plan should be treated as a sensitive document and protected in accordance with its security classification level. The ISMS security plan should be reviewed and updated periodically (e.g., once every three years is a common practice). Components of the plan may need to be reviewed and updated more frequently.

3.1 Business Environment Plan

3.1.1 Introduction

This plan describes the business environment under which the information security program operates. Business environment planning includes:

- Defining the mission and goals of the information security program.

- Defining the types of information (i.e., their sensitivity) that need to be protected by the information security program.
- Identifying the location of the information security program within the overall structure of the organization.
- Identifying the laws, regulations, and parent organization requirements that must be addressed by the information security program.
- Providing sufficient authority to the ISMS manager and staff to conduct their activities.
- Establishing internal enforcement mechanisms for addressing violations of information security requirements.
- Identifying internal stakeholders within the CBRN facility.
- Identifying external stakeholders within the parent company, with the competent authorities, and with outside interest groups.
- Acquiring the resources needed to operate a successful ISMS.

In the introduction, provide a brief explanation of the role the business environment plays in maintaining an information security program. The following is an example.

> To have an effective information security program, the business environment in which the facility and ISMS operates needs to be defined. This includes specifying the mission of the information security program, the legal and organizational requirements it must meet, and its defined objectives. To do this, management needs to understand the sensitivity of the information that is being created, used, transmitted, and stored.
>
> The information security program requires a structure and a place within the organizational framework of the facility. Its manager and staff need to have the authority to access and assess information assets and to provide information security direction to personnel assigned to other groups within the facility. Adequate enforcement mechanisms are required to address violations of information security requirements. The ISMS must have adequate resources to fulfill its information security mission. This includes having an adequate level of staffing, to perform required information security duties, resources to fund the necessary work, and sufficient time to meet objectives.
>
> Another aspect of a successful business environment for the ISMS involves the identification and involvement of internal stakeholders. These are managers and personnel within the facility who should have an interest in information security or might be affected by information security decisions. In addition, external stakeholders (i.e., those who are not part of the facility staff) need to be identified and involved in information security activities. These include groups and individuals within our parent organization. This is likely to include information technology, cyber security, and information security personnel. External stakeholders also include appropriate competent authorities. This might include national, regional, and local regulatory agencies, other government ministries, and law enforcement. External stakeholders also include suppliers, contractors, and customers. Finally, external stakeholders may include vendor public interest groups, academia, the media, and local businesses.

3.1.2 Applicability and Scope

In this section, describe the applicability and scope of the business environment plan. This includes a summary of key items that are within the scope of this plan and an explicit mention of items that are out of scope.

The business environment plan's scope statement should list all the organizations within the facility and the parent company that are involved in information security and whose contributions and cooperation are needed to prepare or implement the business environment plan. For example, does it apply only to the CBRN facility, perhaps leaving parent organization responsibilities to be covered by the parent organization's own information security-related governance plan? Does it overlap or reference the physical security and cyber security plans that also cover aspects of information security? Most effective information security governance plans reference the facility's other applicable governance plans and smoothly integrates with these other plans.

This plan should also specify the types of external stakeholders who need to be addressed in the plan. Excluded from the plan are organizations that have no role in information security and external stakeholders that are not concerned with information security issues or consequences.

3.1.3 Roles and Responsibilities

In this section, define the roles and responsibilities involving the business environment. This includes, but is not limited to, the roles and responsibilities for the ISMS manager, IT manager, physical security manager, cyber security manager, facility security director, regulatory compliance organization, external communications organization, and other senior managers.

For example, the ISMS manager is responsible for ensuring that the Business Environment Plan is carried out. The following presents examples of the roles and responsibilities of the ISMS manager under this plan.

- The ISMS manager is responsible for the management of the information security program, oversight of program staff, and allocating resources to program activities. This includes the development and execution of the business environment plan.

- The ISMS manager is responsible for ensuring that sufficient business environment information is gathered to support this plan. The ISMS manager is responsible for ensuring that information-gathering activities are conducted within and outside of the facility, including outreach to external stakeholders.

- The ISMS manager is responsible for ensuring that business environment data are periodically reviewed and kept current to support the appropriate functioning of the information security program.

- The ISMS manager is responsible for ensuring that business environment information is gathered in a timely manner and is used to provide a framework for information security-related activities.

- The ISMS manager is responsible for presenting all information security plans to the facility security director and other senior managers for approval.

- The ISMS manager shall work with the facility security director and other facility staff to develop an enforcement policy for information security that defines penalties for the violations of the facility's information security policies.

- The ISMS manager is responsible for requesting adequate resources, including funding and personnel, to maintain an adequate information security program.

3.1.4 Policy

In this section, outline policies for the business environment as it relates to the information security program. Policies should specify the authority of the ISMS manager and the ISMS team in conducting its information security activities. This includes developing, implementing, and enforcing information security policies. The location of the ISMS program within the facility organizational structure should be defined. The allocation of financial and personnel resources for conducting the information security program should also be covered by policies. These policies should define the rules of engagement for involving internal and external stakeholders in developing this plan.

The following are examples of policies that could be established to support the business environment plan:

- The facility is committed to maintaining a risk-based information security program to protect its information assets, particularly its sensitive information assets.
- The information security program shall comply with all applicable laws and regulations.
- The information security program shall operate under the direct authority of the facility security director.
- The information technology department and facility operations groups shall not have direct authority over the information security program because that would represent a potential conflict of interest between the facility's productivity objectives and the facility's security mission.
- The ISMS manager shall have the authority to remove from service, and secure the data of, any information system that is out of compliance with the facility's information security policies.
- The information security program, its policies, and procedures shall be approved by the ISMS manager and the facility security director.

3.1.5 Sources of Information and References

In this section, list the sources of information and references to be used in this business environment plan. This might include laws, regulations, standards, company or facility policies and procedures, and other publications. It also includes inputs from other facility processes and investigations.

Potentials sources of information include ISO 27002, *Information Technology—Security techniques—Code of practice for information security controls* (ISO/IEC 2015b) and NIST SP 800-12, *An Introduction to Computer Security – The NIST Handbook* (NIST 1995).

3.2 Asset Management Plan

3.2.1 Introduction

Asset management is a systematic process for identifying and characterizing the digital assets that make up information systems. It is a useful tool in providing for the secure deployment, operation, maintenance, and disposal of assets. In information security, asset management involves conducting and maintaining a comprehensive inventory of all digital assets and systems. This includes computer hardware, firmware, software, and communication pathways. Asset management provides a solid foundation that can be used to search for computer system-related security vulnerabilities. In the introduction to the asset management plan, provide a brief explanation of why asset management is an important component in an information security program and outline what will be done to support asset management. The following is an example:

Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, searching for unprotected or partially protected assets to be attached to the network. If they find devices that do not contain the latest security updates, and therefore contain known vulnerabilities, these devices may be easy to exploit. Even devices that are not visible from the Internet can be used by attackers who have already gained access to a facility workstation or network and are hunting for higher-value targets within the facility.

A critical step in establishing an appropriate level of information security is to have accurate information on the configuration, connectivity, and other security properties of every device or asset that is part of an information system. The next step involves developing and implementing an effective set of security requirements that need to be followed before any device or asset is modified, reconfigured, added, or removed from the information system. Requirements are also needed to govern the timely implementation of security updates that address known vulnerabilities (e.g., operating system or software updates that are released to address vulnerabilities that may be exploited by malware). These activities are key elements in asset management.

3.2.2 Applicability and Scope

In this section, describe the applicability and scope of asset management. This includes a summary of key items that are within the scope of this plan and an explicit mention of items that are out of scope. For example, the asset management plan’s scope statement should describe the general types of hardware, firmware, and software that can affect information security and therefore need to be included in a program of asset management. In general, all devices that are part of an information system, or connected to an information system, should be included in the asset management program. In the risk-based approach that is at the core of ISMS security planning, different requirements can be specified for information assets and systems based on the sensitivity of the information that is associated with the system. Any information system that is determined to be out of scope for the asset management plan should be identified and the reason for its exclusion thoroughly justified.

3.2.3 Roles and Responsibilities

In this section, define the roles and responsibilities for asset management. This includes, but is not limited to, the roles and responsibilities for the ISMS manager, the staff conducting asset management activities, the system administrators for information systems, the program managers responsible for those systems, and senior managers who have oversight and resource allocation responsibilities for facility assets and their operation.

For example, the ISMS manager is responsible for ensuring that the asset management plan is carried out. Work activities to identify and track information assets may be performed by other departments, such as the IT organization, security department, facility inventory group, and facility operations groups. Regardless of who performs this activity, the ISMS security manager is responsible for ensuring this information is acquired to support the asset management program. The following presents examples of the roles and responsibilities of the ISMS manager under this plan:

- The ISMS manager is responsible for the management of the information security program, oversight of program staff, and allocating resources to program activities. This includes the development and execution of the asset management plan.

- The ISMS manager is responsible for ensuring that asset management information, either the acquisition of data from other groups performing asset management activities or asset inventory information gathered by the information security asset management team, are collected and analyzed according to the asset management plan.

- The ISMS manager is responsible for assigning asset management team roles and responsibilities, providing personnel with appropriate training and resources to perform their asset management activities, and ensuring activities are performed in a timely and appropriate manner.

- The ISMS manager is responsible for coordinating asset management activities with the IT manager, cyber security team, or other facility organizations that are also engaged in asset management activities.

- The ISMS manager is responsible for evaluating the asset management data collected to ensure it meets the requirements of the asset management plan.

- The ISMS manager is responsible for ensuring that asset management information is periodically reviewed and kept current to maintain an accurate and acceptable level of information security risk.

- The ISMS manager is responsible for summarizing the results from asset management activities and reporting any unusual and significant observations or findings to the facility security director, IT manager, and other senior facility managers.

- The ISMS manager is responsible for ensuring that asset management information is provided in a timely manner to the other information security teams that will use this information to perform their security-related activities.

3.2.4 Policy

In this section, outline the policies governing asset management. Policies may include:

- Criteria for selecting the asset management team
- Requirements to follow organizational procedures when modifying, reconfiguring, adding, or removing a digital asset on an information system
- Criteria for selecting the information assets and systems to be included in asset management
- Coordination with other facility groups (e.g., IT and cyber security) that may also have asset management responsibilities
- The rules of engagement for gathering asset information from system administrators and SMEs
- The extent of the review of assets
- Requirements and limitations on electronic probing to search for system assets and gather configuration information

- Budgeting, scheduling, and assessment frequency.

The following are examples of policies that could be established to support electronic scanning as part of asset management.

- The information security program shall ensure that periodic scans are conducted to detect new devices installed on information systems. Scanning may be part of routine automated security monitoring or a separate scanning activity.
- Scanning to support asset management shall be coordinated with other facility groups (e.g., cyber security, IT) that are conducting asset management activities.
- Scanning tools will be thoroughly tested before their operational use to minimize potential interference with system or process operations.
- Scanning activities will be coordinated with system operators to minimize the likelihood of potential disruptions. Scanning will be a cooperative rather than an adversarial process.
- Scans that register new assets (i.e., ones that have not been previously documented as part of the system), will be flagged for additional investigation. Prompt action is required to confirm that newly identified assets are legitimate.
- Devices determined to have been added without appropriate authorizations will be reported to the ISMS manager and appropriate countermeasures will be implemented as necessary. This may include removing the device or implementing security controls to maintain an appropriate level of information security.
- Findings that indicate a potential violation of information security requirements shall be tracked and reported to the ISMS manager, cyber security manager, IT manager, and facility security director.

3.2.5 Sources of Information and References

In this section, list the sources of information and references to be used in this asset management plan. This might include laws, regulations, standards, company or facility policies and procedures, and other publications. Inputs from other facility processes and investigations should also be included.

3.3 Security Control Implementation Plan

3.3.1 Introduction

This plan covers key categories of security controls used to maintain information security. Security controls are management, operation, or technical safeguards or countermeasures that act to deter, delay, detect, and deny attempts to subvert information security and minimize the consequences of a successful attack. Specific categories of security controls covered in this plan include:

- Access control
- Baseline configuration security

- Communications security
- Cryptography
- Information sanitization and destruction
- Human resource security
- Operational security
- Physical and environmental security
- Security in supplier and third-party relations
- Security throughout the asset life cycle.

In this introduction, provide an overview of the framework for the facility's security control program. This begins by introducing the overarching protective strategies for information security that are addressed by security controls. Briefly introduce each of the major security control categories to be covered in the plan.

The following is an example:

> In designing an information security program, the facility shall develop and implement a comprehensive and diverse set of protective strategies capable of detecting, isolating, and neutralizing unauthorized activities in a timely manner. The protective strategies shall exhibit defense-in-depth characteristics ensuring that the failure of any single element of a strategy does not result in successful compromise of an information system. The strategies developed need to protect information systems from various vectors of attack that involve a physical, cyber, or combined attack. These strategies are implemented through a variety of management, operational, and technical security controls.
>
> This plan highlights the categories of security controls that support and implement protective strategies. Security controls are designed to deter, delay, detect, and deny attempts to subvert information security or minimize the consequences of a successful attack. The categories of security controls covered in this plan are access control, configuration security, communications security, cryptography, information sanitization and destruction, human resource security, operational security, physical and environmental security, security in supplier and third-party relations, and security throughout the asset life cycle.

Guidance for the specific security controls to be used at the facility is presented in *How to Implement Security Controls for an Information Security Program at CBRN Facilitie*s (UNICRI 2015b).

3.3.2 Applicability and Scope

In this section, the facility describes the scope and applicability of its security control implementation plan. This includes a summary of key items within the scope of this plan and an explicit mention of items that are out of scope.

For example, the security control implementation plan's applicability statement should list all the information systems and the support IT environment for which the security controls apply. It should also list any information systems or supporting IT networks that are not subject to this plan (typically this would involve systems that do not contain any sensitive information or systems on which their compromise would only result in acceptable risks). The reason for this exclusion should be appropriately documented to support any future review of this decision.

For some types of information systems covered under this plan, certain security controls or categories of security controls might not be applicable. For example, it may not be practical to institute access controls on information systems when those access controls might potentially interfere with critical processes. In those cases, compensating security controls based on the risk level of the information assets would be required. These compensating controls might involve applying principles of physical and digital isolation that would reduce the need for traditional access-based security controls. In these cases, the plan should call for appropriate documentation to justify the exclusion of certain security controls.

3.3.3 Roles and Responsibilities

In this section, define the roles and responsibilities associated with designing, implementing, maintaining, reviewing, and updating security controls. This includes, but is not limited to, the roles and responsibilities for the ISMS manager and team, cyber security manager and team, IT manager and staff, and the facility security director. This should include the roles and responsibilities for mangers and staff members involved in designing, acquiring, developing, and maintaining information assets, systems, and related infrastructure. Emphasis should be placed on information assets that are designated as sensitive.

For example, the ISMS manager is responsible for ensuring that the security control implementation plan is carried out. Work activities associated with most aspects of the security control program are part of the ISMS manager's responsibility. This includes the design and implementation of security controls, maintenance of existing security controls, monitoring of security control performance, security control assessments, and security control updates. The ISMS manager has oversight responsibilities for all information security-related activities at the facility. The ISMS manger is also responsible for coordinating activities with other groups (e.g., cyber security, IT, physical security) that have overlapping responsibilities involving the facility's security controls.

The following presents examples of the roles and responsibilities of the ISMS manager under this plan:

- The ISMS manager is responsible for the management of the information security program, oversight of program staff, and allocating resources to program activities. This includes the development and execution of the asset management plan.
- The ISMS manager is responsible for ensuring that for each information system covered by this plan, the security controls are evaluated in accordance with this plan.
- The ISMS manager is responsible for ensuring that those evaluating and selecting security controls have the appropriate knowledge and training to make these determinations.
- The ISMS manager is responsible for reviewing for appropriateness the selection of security controls for each information system covered by this plan. The security controls selected for application must, as a result of working together to cover various areas of concern, result in overall, acceptable risk levels.
- The ISMS manager is responsible for coordinating activities related to security controls with other facility and parent organization managers who have overlapping security controls responsibilities. Others working on information security-related controls are likely to include representatives from cyber security, IT, and physical security groups.
- The ISMS manager is responsible for assuring that application of security controls is effectively carried out and the security controls are working as designed. These may involve the ISMS security manager arranging for appropriate spot checks and assessing the results provided by assessment teams.
- The ISMS manager is responsible for summarizing the status of security controls and results and providing this report to the facility security director, IT manager, cyber security manager, and other senior facility managers.
- The ISMS manager is responsible for reporting any unusual and significant observations or findings regarding the application of security controls to the facility security director, IT manager, cyber security manager, and physical security manager.

3.3.4 Policy

In this section, outline the policies governing the selection, installation, operation, and maintenance for various types of security controls. In the following sections, policy guidance is presented for each of the major security control categories.

Policy for Access Controls

Access control is the process of managing access to certain systems, information, functions, tools, locations, components, or resources. Access control limits individual users and processes by implementing the "principle of least privilege." This means that every process, program, or user shall only be granted access to information and resources for which authorization has been granted, and then only when there is a legitimate business purpose for that access. This reduces the number of potential entry points for an attempt to compromise information security. Access control is designed to enforce security policies and streamline security management processes. For example, it can allow the grouping of users based on their role within the organization, rather than separately evaluating each individual identity (ESCSWG 2014).

The following are examples of policies that could be established to support security controls for access to information systems:

- Privileged accounts shall only be granted to staff members who have both the knowledge necessary to administer the information system and a business need to modify the configuration of the underlying system.
- Accounts on information systems deemed sensitive, shall only be granted to staff members who have a business need to access the system.
- All accounts shall be reviewed a minimum of once every two years.
- System accounts that cannot be associated with a business process or owner must be disabled.
- Prohibit the use of default passwords for applications and operating systems.
- Ensure that users cannot reuse their last 12 passwords.
- Implement and enforce appropriate restrictions on password minimum length and strength.
- All accounts shall be monitored for usage. At a minimum, the log on and log off time will be recorded for each account. Any failed log on attempts and other anomalies shall be recorded and unusual behaviors assessed to identify potential security issues.
- Any logged on account left idle for 15 or more minutes will be logged off or require positive authentication before the session is resumed.

Policy for Baseline Configuration Controls

Security controls are needed to ensure that assets, including hardware, software, and data sets, are free from tampering. An effective set of security controls that can maintain the facility's established baseline configuration is required. A baseline configuration is a set of specifications for an information system that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures established by the facility. A configuration management process is used to make changes to the baseline configuration (NIST 2011a). A baseline configuration will vary based on the system type (i.e., server vs. workstation) as well as information classification level.

The following are examples of policies that could be established to support security controls for the baseline configuration:

- The ISMS shall maintain a list of authorized operating systems, versions, and applications that are used within each information system. This covers workstations, servers, routers, switches, firewalls, laptops, and other digital devices.
- Any operating system or application that is no longer being maintained by the vendor requires ISMS approval to remain on the network. Additional security controls will likely be needed to compensate for the lack of upgrades to address newly discovered security vulnerabilities.
- All digital devices and other equipment connected to an information system shall be uniquely identified and approved by the ISMS program for use on that information system.
- For each digital asset within an information system or its supporting infrastructure, the ISMS program will ensure that the following security requirements are met:
    - Remove or disable unnecessary services.
    - Close unused network ports.
    - Disable auto-run from universal serial bus (USB) tokens, USB hard drives, CD/DVDs, FireWire devices, and other such devices.
    - Monitor the use of external devices.
    - Establish a default-deny rule set on all host-based firewalls.
    - Use a reliable source of network time.
    - All assets capable of running anti-malware must have anti-malware software installed. At a minimum the assets must be able to:
        - Receive updates automatically from a centralized infrastructure.
        - Automatically conduct an anti-malware scan of removable media when inserted.
        - Use whitelist applications based on the authorized software and version list provided by the ISMS manager.
        - Implement intrusion detection.
- Maintain an active program to patch vulnerabilities. Once a vulnerability is discovered in hardware, firmware, or software and a patch becomes available, testing on that patch shall begin within one week of the receipt of the patch. All patches that do not interfere with essential information system functionality shall be promptly installed.

Policy for Communications Security Controls

The network architecture is how a network is designed and segmented into logical, smaller functional subnets (i.e., network security zones) for the purpose of communication. Poorly designed network architectures that lack a defense-in-depth approach to security may be vulnerable to cyber exploitation. Hardware, software, and firmware that restrict communications are important tools in establishing an appropriate cyber security defensive architecture for networks. Security can be enhanced by partitioning networks into multiple segments and placing technical security controls (e.g., firewalls, unidirectional communication devices, or virtual private network [VPN] concentrators) between the network segments.

The following are examples of policies that could be established to support security controls for communications:

- Information security networks shall be segmented. Any assets accessible from the Internet shall be in a demilitarized zone (DMZ)[5]. DMZ systems shall never contain sensitive data. Sensitive data shall reside on a private network that is not directly connected to the DMZ. Communication between the DMZ and the private network shall occur through an interface managed in the middleware segment.

- Deploy a domain name system (DNS)[6] in a hierarchical, structured fashion.

    a. Internal network client systems shall be configured to send requests to intranet DNS servers.

    b. Intranet DNS servers shall be configured to send requests to the DMZ DNS servers.

    c. DMZ DNS servers shall be configured to send requests to the Internet.

- Deploy a reliable source of network time.

- An intrusion detection system shall be deployed at key interfaces throughout the enterprise.

- All remote privileged access of servers, workstations, network devices or like equipment shall be performed over secure channels such as secure sockets layer (SSL)/transport layer security (TLS) or Internet protocol security (IPsec).

- Perimeter boundary security mechanisms (firewalls, routers) shall meet the following requirements:

    a. Be configured to allow communication to and from known and approved Internet protocol (IP) addresses and domains.

    b. Network engineers, in order to support a rapid response to an attack, shall be able to quickly propagate new firewall and router rule sets throughout the facility. The goal is for network engineers to distribute enhanced rule sets within an hour of notification of a potential attack.

    c. The ISMS manager shall authorize each type of communication that is to be permitted to pass through boundary security mechanisms.

    d. Any VPN or tunneled remote access requires two-factor authentication.

    e. Perimeter boundary security mechanisms shall deny by default.

Policy for Cryptography

Cryptography is the application of mathematical techniques for encrypting and decrypting data in order to keep it private when electronically transmitted or stored. A cryptographic-based security system involves both

[5] In computer networks, a demilitarized zone (DMZ) is a physical or logical sub-network that separates an internal local area network (LAN) from other untrusted networks, usually the Internet. External-facing servers, resources, and services are located in the DMZ so they are accessible from the Internet but the rest of the internal LAN remains unreachable. This provides an additional layer of security as it restricts the ability of hackers to directly access internal servers and data via the Internet. (Tech Target 2015a).

[6] The domain name system (DNS) is the way that Internet domain names are located and translated into Internet protocol (IP) addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address (Tech Target 2015b).

cryptographic methods (e.g., primitives/algorithms) and cryptographic key management (methods of creating, distributing, maintaining, validating, and updating cryptographic keys). Publicly accessible guidance on setting requirements for cryptography are provided in Federal Information Processing Standard (FIPS) 140-2 (FIPS 2001) and NIST 800-57 (NIST 2012b).

The following are examples of policies that could be established to support security controls for cryptography:

- Any cryptographic algorithms shall provide acceptable levels of protection and be based on commonly accepted guidance or standards documents (e.g., based on FIPS 140-2 or an equivalent standard).
- All systems shall be configured to authenticate using channel-level encryption[7]. If possible, data shall be transmitted using channel-level encryption.
- If passwords are stored digitally, they shall be protected using cryptography.
- Wireless traffic shall be encrypted using a technology that conforms to current "good practice" expectations for information systems.

Policy for Information Sanitization and Destruction

Information sanitization is the cleaning or sanitizing of an information system for reuse without resorting to the destruction of the asset. Sanitization removes information such that it cannot be retrieved or reconstructed. Information sanitization and destruction focuses on maintaining security of information assets at all phases of their life cycle. This includes the appropriate disposal and/or destruction of information assets when they are no longer needed.

The following are examples of policies that could be established to support security controls for information sanitization and destruction:

- Any information assets being redeployed for another purpose need sufficient sanitization to ensure their prior use or function cannot be determined or their data recovered.
- All information assets must be sanitized prior to disposal, unless they are slated for complete destruction.
- The facility employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
- Hard copies of sensitive data and electronic storage media shall be stored in locked rooms and/or containers when not in use to restrict access to authorized personnel only.
- When no longer needed, hard copies of sensitive data shall be shredded and disposed of using a trusted method (e.g., incineration or secure recycling).
- Electronic storage media (e.g., memory cards, hard drives, USB drives, disks) shall be sanitized using a method that ensures that the data cannot be retrieved. As an added security measure for information that is extremely sensitive, the electronic storage media shall be destroyed after erasure.

[7] Channel encryption is a security layer that resides between the application and the transport layers, the most common forms are SSL and HTTPS (Netlingo 2015).

Policy for Human Resources

Human resource security is an important element in information security. Breeches of information security are frequently linked to inappropriate, often inadvertent, actions by facility personnel. Examples of inadvertent actions include accidental disclosures of information, failure to follow security policies or requirements, and falling prey to social engineering. Intentional and malicious actions are also a concern. Staff members or former staff members may undertake malicious actions for a variety of reasons. Examples include being paid to provide sensitive information or to open a venue for a cyberattack; voluntarily providing information to adversaries because of a perceived mistreatment of the individual by the facility or its parent organization; or providing information or services to an attacker because of personal threats made by against the individual, their family, or others by the attacker.

The following are examples of policies that could be established to support security controls for human resources:

- Background security checks are required for personnel who handle sensitive information assets.
- Background security checks are required prior to personnel being authorized to access or maintain information assets upon which sensitive information is created or resides.
- Background checks shall be renewed at prescribed intervals (e.g., every five to seven years).
- Background checks shall identify potential items of concern such as a criminal history, mental illness, abusive behavior, excessive alcohol consumption, use of illegal drugs, etc.
- A continuous behavioral observation program shall be established so that facility personnel are trained to detect and report behaviors of concern exhibited by other staff members (e.g., alcohol or drug addiction; mental illness; intentional violation of regulations, policies, or procedures).
- Develop an information security briefing for personnel who are concluding their employment at the facility or transferring to a different position that does not involve access to sensitive information systems. The purpose of the briefing is to remind personnel that their responsibilities to protect sensitive information do not end after they leave their current job. Civil and criminal penalties for violating information security shall be reviewed as part of this briefing.
- Present the outgoing briefing described above to all staff members who are about to leave their current position and have access to sensitive information or the operation of facility information systems.
- If there is sufficient advance warning, access to sensitive information or systems shall be terminated two weeks prior to an outgoing staff member’s last day of employment at the facility.

Policy for Operations

Information security is highly dependent on operational security. The system administrators, maintenance personnel, and users of information systems play important roles in information security. The adherence of personnel to security policies and procedures, and the adequacy of those policies and procedures, are important elements in information security. Checks and balances are needed to ensure information security is maintained at an adequate level. No single individual should have sole, unchecked control over an information asset or system.

Among the elements of operations policy are the setting of appropriate passwords and maintaining password security, properly configuring security logging for each information asset, setting appropriate user authentication requirements, and performing timely and appropriate system backups.

The following are examples of policies that could be established to support security controls for the operation and administration of information assets:

- All administrative or privileged passwords shall be of sufficient complexity to thwart automated password cracking programs. For example, the password shall:
  - have a minimum length of 10 characters
  - contain lower- and upper-case letters, numbers, and special characters
  - exclude common words, names, or dates.
- Privileged users shall not share accounts. Each user shall have their own unique user identification and password for tracking and auditing purposes.
- Privileged accounts shall change their passwords every 30 days.
- Passwords shall never be repeated and shall meet organizational requirements for length and complexity.
- All logs shall include a date and timestamp. Where possible, systems shall record logs in a standardized format, such as syslog.
- At least one common time source shall be available for systems to retrieve the time, to provide for consistency in the times used in the audit logs. For sensitive information assets, it is recommended that a second time source also be used to ensure consistency.
- Audit logs shall be retained for at least one year. Each system must have storage space available for one year of logs or a method of backing up logs to another system to preserve these logs.
- No single individual shall have total or unsupervised control over the operation or administration of a sensitive information system. Having two or more personnel responsible for the operation of a sensitive information system or task provides checks and balances on the primary operator's actions. This is done to deter behavior or actions by an operator that are not consistent with facility information security policies. It also enhances continuity of operations in the event the primary administrator abruptly leaves his or her current assignment.

Policy for Physical and Environmental Security

To maintain information security, a facility needs to guard against a loss of confidentiality, integrity, and availability of its information assets. Physical security and cyber security need to operate in tandem to protect information security. Performing adequately in only one of these major security components will not provide sufficient protection for information assets. Environmental security can be another important area to maintain the security and availability of information assets. Fire, water, extreme temperatures, and other environmental conditions can damage or destroy information assets. Protecting information assets from these environmental hazards is an element of information security.

The following are examples of policies that could be established to support security controls for physical and environmental security:

- The ISMS manager and ISMS team shall work with the physical security team to document and implement a physical security plan for information systems.
- Ensure that attempts to physically access information assets are detectable. If electronic logging of access attempts is available, access attempts shall be automatically logged to a central logging server and that information shall be retained for a prescribed period (e.g., one year or longer).
- Ensure that all physical security systems protecting information assets are periodically tested (e.g., once every year). More frequent testing is required for highly sensitive information assets. Records of physical security system tests shall be maintained for a prescribed period (e.g., one year or longer).
- Ensure that the locations where backup copies of sensitive information are stored meet the same requirements for physical protection as the primary information assets.
- Ensure that information security assets are appropriately protected from environmental hazards. This includes hazards of internal origin (e.g., water, fire, and temperatures outside of prescribed ranges) and external origin (e.g., tsunamis, earthquakes, or severe storms).

Policy for Supplier and Third-party Relationships

The life cycle security program for suppliers and contractors is an important element in information security. Information security vulnerabilities can result from faulty architecture; poor security design; and vulnerabilities in hardware, firmware, and software in products provided, installed, or maintained by suppliers and contractors. Vulnerabilities can also occur from inadequate security training or poor security practices by supply and contractor staff members. Many security vulnerabilities are the result of software developed with inadequate attention to secure coding practices. Life cycle security programs provide a structured way for developing robust products with fewer weaknesses and vulnerabilities. Supplier post-production support is critical for maintaining secure software and systems, including remediating newly discovered vulnerabilities. It is also important to have validation of hardware, firmware, and software to ensure that they have adequate security and were not tampered with or otherwise modified during transport to the facility or maintenance at the facility (ESCSWG 2014). As a result of the above issues, it is important to incorporate information security in the process of procuring products and services from suppliers and other third parties.

The following are examples of policies that could be established to support security controls supplier and third-party relationships:

- The ISMS manager and the facility's procurement personnel shall work with suppliers and contractors to ensure that information assets, as well as other products and provided services, comply with the facility's information security plans, policies, and requirements.
- Prior to acquiring and deploying information assets and services from suppliers and contractors, the ISMS manager shall arrange for a review of the supplier or contractor's information security program and the application of that program to the product or service being offered to the facility.
- Service-level agreements or similar tools shall be used to ensure that partners live up to their obligations to protect the information security at the facility.
- Any software developed for use at the facility shall be developed using a security-aware software development life cycle.

Policy for the System Development Life Cycle

The system development life cycle for information security involves incorporating information security in the design, acquisition, installation, operation, maintenance, and disposal of information assets. As part of the life cycle nature of information security, a CBRN facility should employ a process that actively maintains and evaluates information security. Results from risk assessment and risk management activities and lessons learned during routine observations should be incorporated in a continuous improvement process.

The following are examples of policies that could be established to support security controls for the system development life cycle:

- Software developed at the CBRN facility, or by its parent organization, for use with information assets (particularly those involved with sensitive information) shall be developed using a security-aware software development life cycle.
- Perform information security and cyber security testing on all information system products (hardware and software) before deploying the new products and after major updates.
- Maintain a separate environment for the development and testing of information system products (hardware and software) that is not connected to the information system operational environment.
- Information products that will operate on systems that contain highly sensitive data may require independent information security and cyber security assessments before operational deployment. This is needed when routine in-house testing may not be sufficient to reduce the risks of potential vulnerabilities to an acceptable level.

3.3.5 Sources of Information and References

In this section, list the sources of information and references used in this Security Control Implementation Plan. This might include laws, regulations, standards, parent company or facility policies and procedures, technical publications, and other sources of information. Inputs from other facility processes and investigations should also be included. A varied set of information sources should be used because security controls cover so many different areas of importance for information security.

3.4 Configuration Management

3.4.1 Introduction

Configuration management establishes and maintains the integrity of hardware and software products throughout their life cycle. Configuration management involves identifying the configuration of assets, controlling this configuration and changes to it, and recording and reporting the status activity of these configurations (NIST 2011a). The introduction to the section on configuration management should provide a brief explanation of why configuration management is important in maintaining information security and a summary of what it entails. The following is an example:

Configuration management is a collection of activities focused on establishing and maintaining the integrity of assets, through control of the processes for initializing, changing, and monitoring the configurations of those assets throughout their life cycle (NIST 2011a).

Configuration management is used to eliminate the confusion and error brought about by the existence of different versions of hardware, firmware, and software products. Product change occurs throughout the life cycle of all information assets. Changes are made to enhance products, correct errors, or improve system performance and security. Configuration management works to control these changes. This includes ensuring that major changes are reviewed and approved by a change control board. All changes shall be made only by those authorized to do so, changes and the reason for them shall be documented. The current and proper version of a product shall be used and that product shall have passed the established quality control checks. An appropriate configuration management program requires a well-defined set of policies and controls that define:

- What products are covered by the configuration management program
- How products and their versions are identified
- How products enter and leave the authorized set of products that are available for use
- How products may be used and by whom
- The different versions of a product available for use and when these products may be used
- How to select and deploy security controls for configuration management (DOE 2014).

3.4.2 Applicability and Scope

In this section, describe the applicability and scope of the configuration management plan. This includes a summary of key items that are within the scope of this plan and an explicit mention of items that are out of scope. For example, the configuration management plan applicability statement should list all the systems on which hardware, firmware, and software are governed by the configuration management plan. It should also list any information systems that are not subject to this plan (typically this would involve systems that do not contain any sensitive information or systems on which their compromise would only result in acceptable risks). The reason for this exclusion should be appropriately documented to support any future review of this decision.

3.4.3 Roles and Responsibilities

In this section, define the roles and responsibilities associated with the configuration management plan. This includes, but is not limited to, the roles and responsibilities for the ISMS manager, IT manager, information system acquisition personnel, system administrators, software developers, system maintenance personnel, change control board members and others. For example, the ISMS manager is responsible for ensuring that the configuration management plan is appropriately applied to information assets and supports products on systems containing sensitive information. In so doing, the ISMS manager has responsibilities for the staff members under his or her direct management and must ensure appropriate coordination with other groups that are performing information asset procurement, development, testing, and maintenance.

The following list is an example of the roles and responsibilities of the ISMS manager for asset management:

- The ISMS manager is responsible for establishing a change control board made up of stakeholders from the IT department, information system owners, and information system users who may be affected by changes to information systems.
- The ISMS manager is responsible for the management of the information security program, oversight of program staff, and allocating resources to program activities. This includes the development and execution of the configuration management plan.
- The ISMS manager is responsible for ensuring that those performing configuration management activities on information systems have the appropriate knowledge and training to perform their configuration management functions and are authorized to perform these activities.
- The ISMS manager is responsible for ensuring that configuration management policies, procedures, and associated security controls are kept current.
- The ISMS manager is responsible for reviewing configuration management documentation for information systems to ensure required policies and practices are being appropriately carried out.
- The ISMS manager is responsible for summarizing the status of the configuration management program and periodically providing this report to the facility security director, IT manager, and other senior facility managers.
- The ISMS manager is responsible for reporting any unusual and significant observations regarding the application of configuration management to the facility security director, IT manager, and other relevant personnel.

3.4.4 Policy

In this section, outline the policies governing configuration management and the change control board. Policies may involve criteria for selecting personnel to perform configuration management duties, training requirements, procedures for identifying information assets that require configuration management, determining the level of configuration management that is required for particular products, the rules of engagement between the configuration management team and operational programs, recordkeeping procedures, testing procedures, maintaining independent testing and operational environments, problem reporting, and other areas of concern.

The following are examples of policies that could be established to support the configuration management program:

- The change control board shall be presented with proposed major changes to information systems that could have an adverse effect on an information system or ISMS program. This board will review the proposed changes and determine if security mitigation and contingency planning is sufficient prior to allowing the change to occur. All proposed changes shall be tracked and reviewed to identify any potential impacts on the facility.
- All servers, workstations, network devices, and any policies or procedures supporting the ISMS are under configuration control.
- Modifications to items under configuration management must follow the configuration management process. A modification may involve a maintenance or a change activity, where:
    - A maintenance activity is defined as patching software or minor updates to documentation.
    - A change is defined as any action that is not maintenance.
- The change control process shall be monitored by checking for unrecognized or altered versions of operating systems, firmware, or software.

3.4.5 Sources of Information and References

In this section, list the sources of information and references to be used in the configuration management plan. This might include laws, regulations, standards, parent company or facility policies and procedures, and other publications. It also includes inputs from other facility processes and investigations.

3.5 Contingency Planning and Disaster Recovery

3.5.1 Introduction

A contingency planning and disaster recovery process is an important element for information security. Contingency planning and disaster recovery seek to identify problems, implement corrective actions, and return any information system by a major event to normal operations in a timely manner. An issue of interest for a CBRN facility that is not found in other facility types is the potential for contamination of information system equipment as a result of the release of chemical, biological, or radiological material within the facility.

The introduction to this section should provide a brief explanation of why contingency planning and disaster recovery is important to maintain information security. The following is an example.

> Information assets are vulnerable to a variety of disruptions, ranging from mild to severe. These disruptions may involve natural or human-caused events including earthquakes, severe weather, war, cyberattacks, physical attacks, labor strife, etc. Risk can be minimized through the application of various types of defensive controls, including security controls. Contingency planning is designed to anticipate the negative impact that may occur to information assets, despite defensive controls, and outline actions that can reduce or mitigate adverse effects (NIST 2010).
>
> Disaster recovery is a component of contingency planning, and involves plans for responding to events that can result in major disruptions. For information systems, this often involves plans to replace damaged information system hardware, restore information that has been corrupted or lost, or finding alternative ways to conduct facility operations when primary information systems are unavailable. This planning emphasizes the importance of identifying the problem, implementing corrective actions, and returning the facility to normal operations in a timely manner. It includes communications and coordination with an array of stakeholders such as the parent organization’s suppliers, contractors, competent authorities, local emergency services personnel, other government officials, and the news media.

3.5.2 Applicability and Scope

In this section, describe the scope and applicability of the contingency planning and disaster recovery plan. Recovery from an information security event can be as simple as restoring the systems from off-site backup or as challenging as maintaining an isolated backup system that can be activated quickly. The level of recovery is unique to each facility, based on its mission and how critical the information system is for facility operations. For example, a hospital could experience loss of life if critical information systems are unavailable for an extended period of time. In contrast, many retail businesses may be able to rely on paper and pen for extended periods if their information systems (e.g., accounting or inventory systems) were unavailable. CBRN facilities will probably fall somewhere between these two examples and follow their facility-specific contingency plan to perform disaster recovery.

The description of the scope and applicability should include a summary of key items that are within the scope of this plan and an explicit mention of items that are out of scope. For example, the contingency planning and disaster recovery plan should list all the information systems covered by the plan, particularly those whose compromise could significantly affect the facility. It should also list any information systems that are not subject to this plan (typically this would involve systems that do not contain any sensitive information or systems for which their loss or compromise would only result in acceptable risks). The reason for this exclusion should be appropriately documented to support any future review of that decision. Further, the contingency planning and disaster recovery plan should list the types of natural and man-made incidents that are within scope of this plan (e.g., cyberattacks, hurricanes, earthquakes, and severe storms that are within the design basis for the facility) and those plausible events that are intentionally excluded (e.g., military strikes by a nation state, or earthquakes that exceed the facility's design basis).

3.5.3 Roles and Responsibilities

In this section, define the roles and responsibilities associated with the contingency planning and disaster recovery plan. This includes, but is not limited to, the roles and responsibilities for the ISMS manager, IT manager, facility security director, IT support staff, equipment acquisition personnel, maintenance personnel, and others.

For example, the ISMS manager is responsible for ensuring that appropriate contingency planning and disaster recovery plans are in place to safeguard the security of sensitive information after an event and restore overall information security capabilities in a timely manner. In so doing, the ISMS manager has responsibilities for staff under his or her direct management. The ISMS manager also needs to ensure appropriate coordination with other facility groups and the parent organization that have their own contingency planning and disaster recovery plans.

The following presents examples of the roles and responsibilities of the ISMS manager for contingency planning and disaster recovery:

- The ISMS manager is responsible for the management of the information security program, oversight of program staff, and allocating resources to program activities. This includes the development and execution of the contingency planning and disaster recovery plan.

- The ISMS manager is responsible for ensuring that those performing contingency planning and disaster recovery planning for information security have the appropriate knowledge and training to perform their functions and are authorized to do this work.

- The ISMS manager is responsible for ensuring that contingency planning and disaster recovery policies are kept current.

- The ISMS manager is responsible for coordinating contingency planning and disaster recovery policies with other facility groups (e.g., IT, operations, physical security) and the parent organization to ensure that information security-related activities are coordinated and consistent with the planning of other groups.

- The ISMS manager is responsible for summarizing the status of the contingency planning and disaster recovery policies and providing this report to the facility security director, IT manager, and other senior facility managers on a periodic basis.

- The ISMS manager is responsible for reporting any unusual and significant observations regarding the application or testing of contingency planning and disaster recovery policies to the facility security director, IT manager, and other relevant senior facility managers.

- The ISMS manager is responsible for periodically testing the contingency planning and disaster recovery plan.

3.5.4 Policy

In this section, outline the policies governing contingency planning and disaster recovery activities. Policies may involve criteria for selecting personnel to perform contingency planning and disaster recovery planning, severe event identification, event likelihood analysis, consequence analysis, and event mitigation measures. Policies should cover the coordination and integration of contingency planning and disaster recovery activities with other groups.

The following are examples of policies that could be established to support the contingency planning and disaster recovery program:

- General categories of severe events that can affect information security will be identified. This categorization may be derived from work already conducted by the information security risk assessment team, or be conducted in conjunction with that team.
- The approximate likelihood of severe events that can affect information security will be estimated. This information may be derived from work already conducted by the information security risk assessment team, or be conducted in conjunction with that team. If insufficient data exist for a quantitative estimate, a non-quantitative assessment will be prepared.
- The consequences to information security from severe events will be estimated. This information may be derived from work already conducted by the information security risk assessment team, or be conducted in conjunction with that team.
- The contingency planning and disaster recovery planning team will coordinate their activities with other groups within the facility that perform contingency planning and disaster recovery planning for other aspects of facility operations.
- The contingency planning and disaster recovery plan will be reviewed and updated at a minimum of once every two years and more frequently as circumstances warrant.
- The contingency planning and disaster recovery plan shall be tested a minimum of once every two years.

3.5.5 Sources of Information and References

In this section, list the sources of information and references to be used in the contingency planning and disaster recovery plan. This might include laws, regulations, standards, governmental or industry guidance, parent company or facility policies and procedures, and other publications.

3.6 Incident Response

3.6.1 Introduction

An incident response and recovery process is an important element for information security. If an incident involves information assets and systems at a CBRN facility, an immediate goal is to identify the problem, implement corrective actions, and return the information assets to a secure status in a timely manner. It is also important to safeguard the forensic data necessary to better understand the nature of an information security compromise and counter future threats. A description of the components of an incident response program are found in our Information Security "Best Practices" document (UNICRI 2015a, Section 3.11).

The following is an example of introductory language for an Incident Response Plan:

> Incident response is a structured approach for addressing an active or recent attempt to compromise information security. An incident response plan provides guidance for detecting, responding to, and limiting the adverse effects of an information security compromise. Incident response for an information security event shall be integrated with the incident response planning for other types of cyber and physical security events. If there is a cyber component to the compromise of an information asset, a cyber security incident response team will be involved. If there is a physical or personnel security component to the compromise, a physical security incident response team will be involved. For many potential events, both incident response teams will need to coordinate operations. Fortunately, membership on these teams often overlaps, so consolidated activities are easy to implement.
>
> An incident response plan shall be designed to meet national and international requirements, particularly reporting requirements. Facilities are encouraged to reach out to appropriate national and international organizations (e.g., computer emergency response team) to report attacks on information security. These organizations are designed to provide assistance to organizations victimized by an attack.
>
> An information security incident response plan shall include the following components:
>
> - Preparation
> - Identification
> - Containment
> - Eradication
> - Recovery
> - Post-incident analysis
> - Forensics activities
> - Information security awareness training.

3.6.2 Applicability and Scope

In this section, describe the scope and applicability of the Incident Response Plan. This includes a summary of key items that are within the scope of this plan and an explicit mention of items that are out of scope. For example, the Incident Response Plan should list all the information systems that are covered by the plan. It should also list any information systems that are not subject to this plan (typically this would involve systems that do not contain any sensitive information or systems on which their compromise would only result in acceptable risks). The reasons for the exclusion of any information system should be appropriately documented to support any future review of that decision.

In addition, the Incident Response Plan should list the types of incidents that are within scope of this plan. For example, a cyberattack that disables an information system would fall within the scope of the incident response plan. The detection and automated quarantine of a common type of malware product may be treated as a routine matter and not involve the activation of an incident response team.

3.6.3 Roles and Responsibilities

In this section, define the roles and responsibilities associated with the incident response plan. This includes, but is not limited to, the roles and responsibilities for the ISMS manager, the IT managers and support staff, the physical security group, the facility security director, facility operations staff, and others. For example, the ISMS manager is responsible for ensuring that appropriate incident response recovery plans are in place to minimize any loss of information security resulting from an adversary's actions, assist in the investigation of the event, and restore overall information security capabilities in a timely manner. In doing this, the ISMS manager has responsibilities for staff under his/her direct management. The ISMS manager also needs to ensure appropriate coordination with other facility groups that have their own incident response plans and responsibilities.

The following are examples of the roles and responsibilities of the ISMS manager for incident response.

- The ISMS manager is responsible for the management of the information security program, oversight of program staff, and allocating resources to program activities. This includes the development and execution of the incident response plan.
- The ISMS manager is responsible for ensuring that those performing incident response recovery planning for information security have the appropriate knowledge and training to perform their functions and are authorized to do this work.
- The ISMS manager is responsible for ensuring that incident response policies are kept current.
- The ISMS manager is responsible for coordinating incident response policies with other facility groups (e.g., IT, operations, physical security) to ensure that information security-related activities are coordinated and consistent with the planning of other groups.
- The ISMS manager is responsible for summarizing the status of the incident response policies and providing this report to the facility security director, IT manager, and other senior facility managers on a periodic basis.
- The ISMS manager is responsible for reporting any unusual and significant observations regarding the application or testing of incident response capabilities to the facility security director, IT manager, and other relevant senior facility managers.
- The ISMS manager is responsible for reviewing and updating the incident response plan a minimum of once every two years.
- The ISMS manager is responsible for reviewing and testing the Incident Response Plan annually either as a table-top exercise or more actively if the plan has not been activated in the last 12 months to address an actual incident.

3.6.4 Policy

In this section, outline the policies governing incident response activities. Policies may involve criteria for selecting personnel to perform incident response planning and selecting personnel for incident response teams. Policies also cover activities during the preparation, identification, containment, eradication, recovery, post-incident analysis, forensics, and training components of the incident response program. Policies should also cover the coordination and integration of incident response activities with other groups.

The following are examples of policies that could be established to support the incident response program:

1. An individual detecting a potential unauthorized intrusion into an information system, compromise of information security, or any security breech that could affect information security shall promptly notify the facility security office and the ISMS program office.

2. The facility security office and ISMS program office shall coordinate their incident response activities.

3. A designated information security first responder who is on duty will be promptly assigned to assess the situation. The ISMS manager will also be notified.

4. The information security first responder shall perform a prompt assessment of the situation. If the incident appears to be of potential concern, the first responder will activate the incident response team. Otherwise, the ISMS manager will arrange for the prompt review of the results of the initial assessment to confirm that it does not rise to a level requiring an activation of the incident response team.

5. If activated, the incident response team will promptly convene to assess the situation and provide their own initial assessment to the ISMS manager and other affected program managers

6. The ISMS manager and the facility security director will determine if the incident under investigation may potentially jeopardize facility, regional, or national security. If either believes this threat exists, a prompt notification will be made to the appropriate government agencies (e.g., law enforcement, the competent authority). The facility's overall manager and the parent organization's security director will also be notified.

3.6.5 Sources of Information and References

In this section, list the sources of information and references to be used in the incident response plan. This might include laws, regulations, standards, governmental or industry guidance, parent company or facility policies and procedures, and other publications.

3.7 Security Monitoring and Auditing

3.7.1 Introduction

An information security monitoring and auditing process is an essential element of an information security program. A description of security monitoring (including auditing) is provided in our information security "Best Practices" document (UNICRI 2015a, Section 3.14). The following is an example of introductory language for a security monitoring and auditing plan.

Information security monitoring and analysis is the collection and analysis of data that can be used to detect and respond to attempts to compromise information security. A robust information security program will include capabilities for the collection and analysis of data to detect and respond to intrusions and unauthorized activities. Security monitoring data can be obtained from many different types of digital devices and applications (e.g., routers, firewalls, operating system security event logs, and application logs).

Event logging systems (i.e., syslogs) are a key component within an information security system or network. Syslog information is used to detect active information security threats and perform post-event forensics analyses. A challenge that exists with the logging of event data is the vast number of events that can be generated by syslog reporting. Depending upon the types of operating systems, the reporting agents involved, and the granularity of reporting, a typical information system network is quite capable of generating thousands or tens of thousands of events per day. Manual inspection of this number of events is well beyond the capabilities of even a fair-sized team of information security or cyber security analysts. To effectively monitor and respond to logged events on information system networks or any reasonable size, it is necessary to use an automated security information and event management (SIEM) product that is capable of analyzing events, prioritizing each event by severity, and elevating those events which shall be acted upon in a timely fashion. SIEMs also provide the capabilities to aggregate event data, search on stored data, derive baselines of analyzed activity, and produce reports. Even on small information system networks or individual devices, automated monitoring can be an invaluable tool for detecting potential information security problems. Another advantage of a SIEM is its ability to integrate data from network intrusion detection systems and network intrusion prevention systems (NIDS/NIPS), host intrusion detection systems and host intrusion prevention systems (HIDS/HIPS), anti-virus systems, file integrity systems, and others.

Some SIEM applications are capable of taking automated action in response to some identified security incidents. Other SIEM-flagged events require analyst evaluation to distinguish between false positives and actual security events. Frequent examinations of SIEM reports are therefore required.

3.7.2 Applicability and Scope

In this section, describe the scope and applicability of the security monitoring and auditing plan. This includes a summary of key items that are within the scope of this plan and an explicit mention of items that are out of scope. For example, the security monitoring and auditing plan should list all the information systems that are covered by the plan. It should also list the any information systems that are not subject to this plan (typically this would involve systems that do not contain any sensitive information or systems on which their compromise would only result in acceptable risks). The reason for the exclusion of any information assets or systems should be appropriately documented to support any future review of this decision.

In addition, the security monitoring and auditing plan should list the types of security events that are within the scope of this plan. For example, plans may focus the electronic monitoring of information systems against cyberattack or the physical security of information assets. In this guidance, we are assuming the focus of the security monitoring and auditing plan is primarily the cyber security of information systems. Physical security risks are assumed to be addressed in the security monitoring plans of the physical security group. If this is true, it should be noted that most physical security risks are outside the scope of the current plan.

3.7.3 Roles and Responsibilities

In this section, define the roles and responsibilities associated with the security monitoring and auditing plan. This includes, but is not limited to, the roles and responsibilities for the ISMS manager and team members, the physical security manager and staff, the facility and parent organization IT managers and staff, the facility security director, facility operations and maintenance personnel, and others.

For example, the ISMS manager is responsible for ensuring that appropriate security monitoring and auditing plans are in place to safeguard the security of all information assets, particularly those involving sensitive information. In doing this, the ISMS manager has responsibilities for staff under his or her direct management. The ISMS also has responsibilities to ensure appropriate coordination with the physical and cyber security teams that have their own security monitoring and auditing plans.

The following presents examples of the roles and responsibilities of the ISMS manager under this plan:

- The ISMS manager is responsible for the management of the information security program, oversight of program staff, and allocating resources to program activities. This includes the development and execution of the security monitoring and auditing plan.

- The ISMS manager is responsible for ensuring that those performing security monitoring and auditing recovery planning for information security have the appropriate tools, knowledge and training to perform their functions and are authorized to do this work. The ISMS manager is responsible for ensuring that security monitoring and auditing policies are kept up-to-date.

- The ISMS manager is responsible for coordinating security monitoring and auditing policies with other facility groups (e.g., IT, operations, physical security) to ensure that information security-related activities are coordinated and consistent with the planning of other groups.

- The ISMS manager is responsible for summarizing the status of the security monitoring and auditing activities and providing this report to the facility security director, IT manager, and other senior facility managers on a periodic basis.

- The ISMS manager is responsible for reporting any unusual and significant observations regarding the security monitoring and auditing to the facility security director, IT manager, and other relevant senior facility managers.

- The ISMS manager is responsible for reviewing the security monitoring and auditing plan and updating as needed.

3.7.4 Policy

In this section, outline the policies governing security monitoring and auditing. Policies may involve criteria for selecting personnel to perform security monitoring and auditing, training requirements, procedures for identifying information assets that require security monitoring and auditing, determining the level of security monitoring and auditing that is required for particular products, the implementation and maintenance of system logging, the deployment of SIEMs, the analysis of SIEM data, the rules of engagement between the security monitoring and auditing team and other facility personnel or teams, and other areas of concern.

In this section, outline the policies governing the security monitoring and auditing program. The following are a few selected examples.

- The information system and cyber security program teams shall establish processes to continuously monitor all information systems within the scope of the ISMS. Monitoring shall cover workstations, servers, mobile devices, firewalls, network intrusion detection and prevention systems, host intrusion detection and prevention systems, anti-virus systems, file integrity systems, and other components connected to the information system.

- A central repository for security-relevant events (e.g., event logs, vulnerability scan data, etc.) shall be maintained.

- Security-related event logs shall be sent to a central repository for assessment by a SIEM product. The use of automated security monitoring tools is recommended to improve the accuracy and reliability of security monitoring.

- As part of security monitoring, the outer perimeter of the facility's information system networks shall be monitored for potentially dangerous file types (e.g., exe, zip, msi), specifically within email attachments. The ISMS manager in cooperation with the cyber security team and IT manager shall determine the types of files that shall be blocked at the external boundaries of the networks.

- Information or cyber security team members shall conduct periodic reviews of security logs and SIEM output to identify anomalies. Logs and SIEM output shall be reviewed at least once a week. Systems containing sensitive information shall be reviewed with a greater frequency.

- At a minimum information system scanning shall include:
    - Scan for unauthorized software. Any unauthorized software shall generate an alert requiring prompt investigation.
    - Scan for vulnerabilities. Vulnerability scans shall be performed in both authenticated and unauthenticated mode. A report of the vulnerabilities shall be provided to the ISMS manager and the cyber security team.
    - Scan for open ports. Any unauthorized open ports that are identified shall be reported to the appropriate system administrator, cyber security team, and the ISMS program team. Prompt action is required to either close unauthorized port or add them to the approved list if the appropriate justification can be provided.
    - Scan for inadequate passwords. The facility has established requirements for password length, strength, and duration of use. Passwords that do not meet these requirements shall generate an alert and the owners of those passwords shall be contacted by the ISMS team and issued a deadline to bring their passwords into compliance. Information system passwords not in compliance by the deadline shall be disabled.
    - Scan for information assets that lack required technical security controls. Information system resources that lack required technical security controls shall generate an alert and their system administrators will be contacted by the ISMS team and issued a deadline to bring its information system into compliance. Information assets not in compliance by the deadline shall be reported to the security and operations managers and scheduled for disconnection unless facility baseline security requirements are promptly met.

- Information system records shall be sent to a central repository for secure storage.

3.7.5 Sources of Information and References

In this section, list the sources of information and references to be used in the Security Monitoring and Auditing Plan. This might include laws, regulations, standards, governmental or industry guidance, parent company or facility guidance, and other publications.

One publicly available source of information is NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (NIST 2011b).

3.8 Awareness and Training Plan

3.8.1 Introduction

Threats to information security could originate from within or outside a CBRN facility. Threats originating from within, by disgruntled workers or spies, may be the most dangerous because the attackers have inside knowledge about the information security infrastructure. Even when threats originate from the outside, non-malicious actions by facility personnel may assist an attack on information security. There are a number of ways non-malicious actions can support an attack. Personnel may inadvertently circumvent information security controls by visiting websites infected with malware, clicking links, or opening malware provided in phishing emails, storing their system login information in an unsecured location, or sharing valuable information in response to social engineering.

One of the more cost-efficient ways to reduce the likelihood that personnel will inadvertently compromise information security is to institute facility security-awareness training initiatives. These may include classroom-style training for all personnel, the posting of security awareness information (e.g., on-line messages, hard copy announcements and posters), sending helpful hints via email, and conducting informal awareness testing. These methods can help ensure staff members have a solid understanding of information security policies, procedures, and best practices (SANS 2009). The following is an example of introductory language for an information security awareness and training plan:

The greatest threat to a CBRN facility's information security is often not a weakness in its security technology but the actions of personnel. This may involve the non-malicious disclosure of information as a result of social engineering, a failure to report unusual activity, or the failure to follow information security policies and procedures. It is therefore vital that our facility have a security training and awareness program in place to ensure personnel working within the facility, or having access to its information systems, are aware of the importance of protecting sensitive information assets and understand their role in maintaining information security (PCI 2014).

An information security awareness and training plan is needed to ensure personnel are trained on:

- The importance of protecting facility information assets, and particularly sensitive information assets
- What they need to do to maintain information security
- How to identify and avoid attempts by adversaries to use facility personnel in attempts to compromise information security (e.g., social engineering, phishing emails)
- How to identify and report suspicious behaviors
- The consequences of an information security compromise to the facility, its parent organization, public safety, and national security.

Awareness programs reinforce the lessons learned in training. This is especially important given the long gap between training and retraining sessions. Awareness programs can involve informational emails, informative posters, and awareness testing. Examples of awareness testing include sending facility personnel fake phishing emails to evaluate their response and incorporating information security incidents into facility security drills.

The information security awareness and training plan will provide guidance for selecting training topics, identifying and training instructors, developing awareness and training materials, determining the depth of training required by different categories of personnel (e.g., general staff, information system operators, information system administrators and security personnel), conducting training courses and awareness activities, evaluating the effectiveness of the program, and updating the program as the threat and technology environment evolves.

3.8.2 Applicability and Scope

In this section, describe the scope and applicability of the information security awareness and training plan. This includes a description of items that are within the scope of this plan and an explicit mention of items that are out of scope. For example, the information security awareness and training plan might specify the following training items are in-scope:

- Training will be provided to all personnel.
- Different training classes will be provided based on the risk associated with various positions at the facility.
- Training may be integrated with cyber security and physical security training.

The plan may specify the following as out-of-scope:

- Requirements for training courses conducted by academic institutions and external security training organizations for information security and cyber security specialists
- Training and awareness activities that could jeopardize facility operations as a result of actions taken by personnel while performing these educational activities.

3.8.3 Roles and Responsibilities

In this section, define the roles and responsibilities associated with the information security awareness and training plan. This includes, but is not limited to, the roles and responsibilities for the ISMS manager, the facility's training office, cyber security and physical security training teams that have complementary training programs, the facility security director, and others.

For example, the ISMS manager is responsible for ensuring that all personnel that have access to information systems, particularly those that involve sensitive information, receive appropriate information security training. In doing this, the ISMS manager has responsibilities for staff members under his or her direct management, must coordinate the review of training records with the facility's training office, and must ensure that only those who have completed their information security training are authorized to use the facility's information systems.

To support the development and maintenance of the information security awareness and training program, the plan could call for establishing an information security training steering committee. The committee could take over the responsibilities for setting learning objectives, coordinating the development of the training curriculum, determining the level of training required for various roles within the facility, and deciding how often training materials need to be reviewed and updated.

The following list is an example of the roles and responsibilities of the ISMS manager for training and awareness:

- The ISMS manager is responsible for the management of the information security program, oversight of program staff, and allocating resources to program activities. This includes the development and execution of the information security awareness and training plan.
- The ISMS manager is responsible for ensuring that those planning and conducting information security awareness and training have the appropriate knowledge and capabilities to perform their functions and are authorized to do this work.
- The ISMS manager is responsible for ensuring that information security awareness and training materials are reviewed periodically and kept current with changing threats, security technologies, and facility operations.
- The ISMS manager is responsible for coordinating information security awareness and training policies with other facility groups (e.g., cyber security, physical security) to ensure that information security-related training and awareness activities are consistent and complementary with other security training.
- The ISMS manager is responsible for summarizing the status of the information security awareness and training programs for the facility security director, IT manager, and other senior facility managers on a periodic basis.
- The ISMS manager is responsible for reporting any unusual and significant observations regarding the information security awareness and training program to the facility security director, IT manager, and other relevant senior facility managers.
- The ISMS manager is responsible for auditing the effectiveness of the training and awareness program.

3.8.4 Policy

In this section, outline the policies governing information security awareness and training. Policies should cover the following areas:

- Setting learning objectives for the training and awareness program.
- Identifying the gaps that may exist in current information security knowledge and practice.
- Developing and implementing a training curriculum for at least three levels of training:
  - Basic training for all personnel
  - Supplementary training for those using information systems that contain sensitive data or are connected to systems that contain sensitive information
  - Advanced training for information security specialists, information system owners and system administrators for sensitive information networks.
- Developing and implementing an awareness program to reinforce information security learning and monitoring the ability of personnel to appropriately identify and address attempts to compromise information security.
- Developing a review program to ensure that the training and awareness materials evolve to match changes in the threat environment, available security technologies, and the nature of facility operations.

The following are examples of policies that could be established to support information security awareness and training.

- All facility personnel are required to receive information security training at least annually.
- At a minimum, information security awareness training will include:
  - Information security objectives, management expectations, programmatic authority, roles and responsibilities, key policies, and consequences for noncompliance.
  - Information security threats (e.g., what constitutes a threat, who are potential attackers, how they work, how they are manifested, what are the typical consequences of threats).
  - General attack methodologies including social engineering techniques.
  - Appropriate and inappropriate information security practices.
  - Organizational contacts to report violations of information security policies, procedures, or practices.
- Senior facility management, including the facility security director and the IT manager, will receive an awareness briefing (at least annually and more frequently depending on the threat environment) emphasizing evolving vectors of attack that could affect the facility.
- The following personnel have roles of additional responsibility for sensitive information assets and shall receive additional training:
  - Personnel involved in the development, use, or storage of sensitive information.
  - Personnel involved in the design, configuration, implementation, use, or administration of information systems, component digital assets, or networks.
- The information security training for the personnel identified in Item 4 will at a minimum include:
  - Information security and engineering procedures, practices, and technologies. .
  - General information on information security vulnerabilities, potential consequences to systems and networks of successful attacks, and information security risk reduction methods
  - The use of tools and techniques to harden information systems and related digital assets to reduce vulnerabilities to cyber threat.
- The following personnel require even more detailed training in information security:

  a. Information security specialist.

  b. System administrators for sensitive information systems

  c. Those involved in the configuration, installation, operation, maintenance, or administration of technical security controls.
- The training for the personnel identified in Item 6 will at a minimum include:
  - Data security
  - Operating system security
  - Application security

- Network security
- access controls
- Intrusion analysis
- Incident management and response
- Digital forensics
- Penetration testing.

3.8.5 Sources of Information and References

In this section, list the sources of information and references to be used in the information security training and awareness plan. This might include laws, regulations, standards, governmental or industry guidance, parent company or facility guidance, and other publications.

Key references might include NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (NIST 1998), and NIST SP-50, *Building an Information Technology Security Awareness and Training Program* (NIST 2003).

Resources for planning a security awareness program can be found at the *SANS Resources: Planning Your Awareness Program* (SANS 2015).

4.0 Glossary

Readers can find definitions of common terms in a number of online references, including but not limited to:

- Internet Engineering Task Force (IETF) Glossary (IETF 2015)
- National Information Assurance (IA) Glossary (CNSS 2006).

5.0 References

CNSS – Committee on National Security Systems. 2006. National Information Assurance (IA) Glossary. CNSS Secretariat, Ft. Meade, Maryland. Accessed December 1, 2015 at http://jitc.fhu.disa.mil/pki/documents/committee_on_national_security_systems_instructions_4009_june_2006.pdf.

DOE - U.S. Department of Energy. 2014. *Electricity Subsector Cybersecurity Capability Maturity Model Version 1.1*, 2012. U.S. Department of Energy, Washington, D.C. Accessed September 2015 at http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012.

ESCSWG – Energy Sector Control Systems Working Group. 2014. *Cybersecurity Procurement Language for Energy Delivery Systems*. Energy Sector Control Systems Working Group, Washington, D.C. Available at http://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf.

FIPS - Federal Information Processing Standards. 2001. *Security Requirements for Cryptographic Modules. National Institute of Standards and Technology*, Gaithersburg, Maryland. Accessed September 2015 at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

IETF – Internet Engineering Task Force. 2015. "Glossary." Accessed December 1, 2015 at http://www.ietf.org/glossary.html.

ISO/IEC - International Standards Organization/International Electrotechnical Commission. 2015a. *ISO/IEC 27001 Information security management.* Accessed November 30, 2015 at http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

ISO/IEC - International Standards Organization/International Electrotechnical Commission. 2015b. *Information Technology—Security techniques—Code of practice for information security controls*. ISO/IEC 27002:2013. Accessed November 30, 2015 at http://www.iso.org/iso/catalogue_detail?csnumber=54533.

ISO/IEC - International Standards Organization/International Electrotechnical Commission. 2015c. ISO/IEC 27005:2011 *Information Technology—Security techniques—Information security risk management.* Accessed November 30, 2015 at http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56742.

Netlingo. 2015. "channel encryption." Accessed December 1, 2015 at http://www.netlingo.com/word/channel-encryption.php.

NIST - National Institute of Standards and Technology. 1995. *An Introduction to Computer Security – The NIST Handbook*. NIST Special Publication 800-12, National Institute of Standards and Technology, Gaithersburg, Maryland. Accessed September 2015 athttp://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

NIST - National Institute of Standards and Technology. 1998. *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. NIST Special Publication 800-16, National Institute of Standards and Technology, Gaithersburg, Maryland. Accessed September 2015 at http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.

NIST - National Institute of Standards and Technology .2003. *Building an Information Technology Security Awareness and Training Program.* NIST Special Publication 800-50, National Institute of Standards and Technology, Gaithersburg, Maryland. Accessed September 2015 at http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

NIST - National Institute of Standards and Technology. 2010. *Contingency Planning Guide for Federal Information System*s. NIST Special Publication 800-34, National Institute of Standards and Technology, Gaithersburg, Maryland. Accessed September 2015 at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=905266.

NIST - National Institute of Standards and Technology. 2011a. *Guide for Security-Focused Configuration Management of Information Systems.* NIST Special Publication 800-128, National Institute of Standards and Technology, Gaithersburg, Maryland. Accessed September, 2015 at http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf.

NIST - National Institute of Standards and Technology. 2011b. *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. NIST Special Publication 800-137, National Institute of Standards and Technology, Gaithersburg, Maryland. Accessed September, 2015 at http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.

NIST - National Institute of Standards and Technology. 2011c. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication 800-39, National Institute of Standards and Technology, Gaithersburg, Maryland. Accessed November 30, 2015 at (http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf).

NIST - National Institute of Standards and Technology. 2012a. *Information Security: Guide for Conducting Risk Assessments*. NIST Special Publication 800-30, Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland. Accessed September 2015 at http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

NIST - National Institute of Standards and Technology. 2012b. *Recommendation for Key Management – Part 1: General*. NIST Special Publication 800-57 Rev 3, National Institute of Standards and Technology, Gaithersburg, Maryland. Accessed September , 2015 at http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf.

NIST - National Institute of Standards and Technology. 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST Special Publication 800-53 Revision 4, National Institute of Standards and Technology, Gaithersburg, Maryland. Accessed November 30, 2015 at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

NIST - National Institute of Standards and Technology. 2014. *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans.* NIST Special Publication 800-53A, National Institute of Standards and Technology, Gaithersburg, Maryland. Accessed November 30, 2015 at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

NIST - National Institute of Standards and Technology. 2015. "Cybersecurity Framework." Accessed November 30, 2015 at http://www.nist.gov/cyberframework/.

PCI Security Standards Council. 2014. *Information Supplement: Best Practices for Implementing a Security Awareness Program.* Security Awareness Program Special Interest Group, PCI Security Standards Council, Accessed September 2015 at https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf.

SANS. 2009. *The Importance of Security Awareness Training.* SANS Institute InfoSec Reading Room. Accessed September 2015 at https://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013.

SANS 2015. Resources: Planning Your Awareness Program. Accessed December 1, 2015 at http://www.securingthehuman.org/resources/planning.

Tech Target. 2015a. "DMZ (demilitarized zone) definition." Accessed December 1, 2015 at http://searchsecurity.techtarget.com/definition/DMZ.

Tech Target. 2015b. "domain name system (DNS) definition." Accessed December 1, 2015 at http://searchnetworking.techtarget.com/definition/domain-name-system.

The National Archives. 2015. "What is an information asset?" Accessed November 30, 2015 at http://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf.

UNICRI. 2015a. *Information Security Best Practices for CBRN Facilities*. United Nations Interregional Criminal Justice Research Institute. Turin, Italy. http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-25112.pdf.

UNICRI. 2015b. *How To Implement Security Controls for an Information Security Program at CBRN Facilities*. United Nations Interregional Criminal Justice Research Institute. Turin, Italy. http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-ACT-10019.pdf.

Contact:
UNICRI
Viale Maestri del Lavoro, 10,
10127, Turin, Italy
Tel: (+39) 011 6537 111
Fax: (+39) 011 63133 68
information@unicri.it
www.unicri.it

Clifford Glantz
Pacific Northwest National Laboratory
P.O. Box 999, MSIN K9-30, Richland, WA 99352
Tel: 001-509-375-2166
cliff.glantz@pnnl.gov
www.pnnl.gov