IPPF

International Professional Practices Framework

Supplemental Guidance

GTAG®

Global Technology Audit Guide

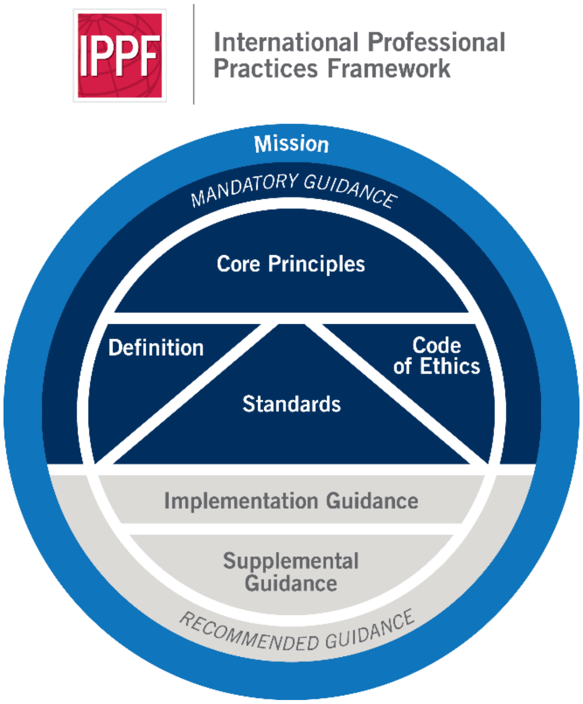
Auditing Insider Threat Programs

UNDER REVIEW

This guide contains some outdated material and references. It remains available while a review is underway.

The Institute of Internal Auditors | Global

About the IPPF



The International Professional Practices Framework® (IPPF®) is the conceptual framework that organizes authoritative guidance promulgated by The IIA. A trustworthy, global, guidance-setting body, The IIA provides internal audit professionals worldwide with authoritative guidance organized in the IPPF as Mandatory Guidance and Recommended Guidance.

Mandatory Guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The mandatory elements of the IPPF are:

- Core Principles for the Professional Practice of Internal Auditing.
- Definition of Internal Auditing.
- Code of Ethics.
- *International Standards for the Professional Practice of Internal Auditing*.

About Supplemental Guidance

Supplemental Guidance is part of the IPPF and provides additional recommended, nonmandatory guidance for conducting internal audit activities. While supporting the *Standards*, Supplemental Guidance is intended to address topical areas, as well as sector-specific issues, in greater procedural detail than the *Standards* or Implementation Guides. Supplemental Guidance is endorsed by The IIA through formal review and approval processes.

Practice Guides

Practice Guides are a type of Supplemental Guidance that provide detailed step-by-step approaches, featuring processes, procedures, tools, and programs, as well as examples of deliverables.

Practice Guides are intended to support internal auditors. Practice Guides are also available to support:

- Financial Services.
- Public Sector.
- Information Technology (GTAG®).

For an overview of authoritative guidance materials provided by The IIA, please visit www.globaliia.org/standards-guidance.

Table of Contents

Executive Summary

In the digital era, organizations must treat data the same way they would treat cash: as an organizational asset that must be protected from insiders and outsiders alike. Protecting the organization's digital assets from catastrophic data breaches should no longer be viewed as the responsibility of information technology (IT) management only. Senior management and the board are ultimately accountable for managing the organization's risks to levels that enable the organization to achieve its objectives.

Whether malicious or unintentional, insider threats often fail to receive the attention they deserve, considering the significance of the risks to which they expose the organization. The key risks associated with insider threats include sabotage, theft of organizational data, espionage, fraud, and criminal acts. Additionally, research trends indicate that the insider threat landscape is growing as organizations become more dependent on information systems (IS), automated processes, web-based applications, digitally transmitted data, and cloud-based data storage.

Organizations are realizing that investments in technology are only part of the solution; it is equally important to assess whether their governance and management controls (e.g., IS policies, training, and awareness campaigns) are capable of addressing insider threats.

Internal auditors are well positioned to help senior management and the board recognize the importance of implementing or strengthening an insider threat program and to help organizations improve their governance, risk management, and control processes related to insider threats.

Introduction

Note: Terms in bold are defined in the glossary in Appendix B. This guidance contains a variety of technical terms for those familiar with information security. If a definition does not appear in the glossary, please consult the references and additional reading sources appearing in Appendix F**.**

An insider threat is defined as the potential for any entity with authorized access (i.e., within the security domain) to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.[1] This definition is broad and includes malicious and nonmalicious (unintentional) attacks to organizational assets, including people.

As opposed to an external threat (i.e., any entity that does not have authorized access to the organization's systems), insiders, such as employees, former employees, contractors, and business associates, already have some level of knowledge and/or access to an organization's systems and data. Therefore, it is much easier for these individuals to bypass many security measures to abuse this access to view, copy, download, corrupt, delete, or transmit sensitive data out of the organization's network.

Risks related to insider threats can include:

- Fraud.
- Sabotage.
- Theft of intellectual property (IP) or trade secrets.
- Disclosure of sensitive data.
- Use of IT resources for illegal activities.

By becoming aware of insider threats and their associated risks and by learning about insider threat programs, internal auditors have a tremendous opportunity to add value by helping the organization strengthen its **governance**, risk management, and **control processes** to manage insider threats.

This Global Technology Audit Guide (GTAG) is intended to help internal auditors understand insider threats and related risks by providing a general overview of insider threats, key risks, and potential impacts. Additionally, the guide presents examples of security frameworks from globally recognized and accepted sources including Carnegie Mellon University Software Engineering Institute, the National Institute of Standards and Technology (NIST), and the U.S. Intelligence and National Security Alliance (INSA), controls, and other resources that can help during the planning and execution of audit engagements. Organizations should base their choice of framework on their unique situation, weighing factors such as their industry, size, complexity, and applicability of the selected framework.

[1] Committee on National Security Systems, *CNSS Instruction No. 4009*, Washington DC: National Security Agency, April 26, 2010: 38. https://www.hsdl.org/?view&did=7447.

For organizations that already have insider threat programs, internal auditors may use this guidance to design assurance engagements to assess the effectiveness of the program.

The guide also describes approaches to consulting engagements, which internal auditors may use to help management identify and assess risks that should be considered when designing and implementing a new insider threat program or to benchmark the maturity of an existing program and help improve it. Finally, the GTAG provides tips for communicating to the **board** about the significance of the risks and the need for responses to identify, prevent, detect, respond to, and recover from **IT security incidents** related to insider threats.

Business Impact

The damage that an insider threat can cause could be quantified in millions. In recent years it was reported that three employees of a superconductors manufacturing organization stole trade secrets and sold them to a competitor over a six-year period. The estimated cost of the trade secrets was $800 million, however the loss of shareholder equity was closer to $1 billion.[2]

Insider Threat Overview

The term threat is sometimes used to refer to the threat actor or an attack. For this reason it is important to define some key terminology that will be used throughout this guide:

Impact is the positive or negative result or effect of a risk.

Threat is any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations.

Threat actor is the entity responsible for the action (or inaction) that adversely impacts the organization.

Threat source is the intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.

Risk is the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

Vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

[2] Christopher Burgess, "Sinovel Wind Group found guilty of IP theft, fined $1.5 million," CSO magazine, July 9, 2018, https://www.csoonline.com/article/3256305/loss-prevention/sinovel-wind-group-found-guilty-of-ip-theft-valued-at-800-million.html.

Insider threats may be *malicious* when the actor intentionally misuses access to an organization's network, system, or data to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems. However, insider threats may also be *nonmalicious* (unintentional) when the actor through action or inaction without malicious intent causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems, such as those outlined in **Figure 1**.

Figure 1: Examples of Insider Threats

Malicious	Nonmalicious
An employee steals trade secrets and later sells them to a competitor.[3]	A systems administrator accidentally turns off a website.
A former employee damages an ex-employer's computer network.[4]	A user accidentally deletes files.
A consultant uses credit card information to commit **fraud**.	Employees fall victim to **social engineering** or phishing emails.

Collusion happens when multiple insider threat actors work together to commit an attack against the organization; when insiders are targeted by malicious outsiders (cybercriminals, hackers, and hacktivists) and end up colluding unknowingly; or when insiders are targeted by malicious outsiders and end up colluding on purpose (many times for a profit).

The potential for collusion creates a larger attack surface and increases the likelihood of a successful attack that is difficult to detect. For small- and medium-size businesses, which often lack the necessary resources to recover from such attacks, the impacts can be especially devastating. Mitigating threats can be an expensive proposition, but when compared with the costs associated with recovering from a major IT security incident, preventing or detecting attacks is a business investment that pays off in the long run.

Adding into the equation data breaches resulting from unintentional acts, the average cost of addressing insider-related damage increases substantially. Moreover, as malicious attackers become more proficient in targeting unsuspecting insiders, the cost is expected to continue to increase.

[3] Kacy Zurkus, "Former Apple Employee Charged with Data Theft," *InfoSecurity Magazine*, July 11, 2018, https://www.infosecurity-magazine.com/news/apple-filed-criminal-complaint-of/.

[4] "Former Employee of Transcontinental Railroad Company Found Guilty of Damaging Ex-Employer's Computer Network," U.S. Department of Justice, October 10, 2017, https://www.justice.gov/usao-mn/pr/former-employee-transcontinental-railroad-company-found-guilty-damaging-ex-employer-s.

Examples of unintentional acts that can result in data breaches include:

Accidental disclosure – An insider unintentionally or erroneously publishes or mishandles sensitive information, or sends it to the wrong party via email, fax, mail, or social media posting.

Phishing/social engineering – An outsider's electronic entry is acquired through social engineering (e.g. phishing email attack, planted or unauthorized USB drive) to acquire an insider's credentials or to plan malware to gain access.

Unauthorized access to physical records – Lost, discarded, or stolen nonelectronic records, such as paper documents, are accessed by unauthorized or malicious users.

Unauthorized access to portable equipment – Lost, discarded, or stolen data storage devices, such as a laptop, smartphone, portable memory device, CD, hard drive, or data tape are accessed by unauthorized or malicious users.

Cost of Insider Related Incidents Reported Over a 12-Month Period

- Total number of insider incidents: 3,269.
- Total average cost: $8.76 million.
- Incidents relating to negligence: 64%.
- Incidents relating to criminal insider: 23%.
- Incidents relating to user credential theft: 13%.

Source: Research: Ponemon Institute©, and Sponsorship: ObserveIT, 2018 Cost of Insider Threats: Global, April 2018.

Anatomy of an Insider Threat

To build the profile of an insider threat, it is important to consider multiple factors (dimensions) such as who represents the threat, what assets can be targeted, the motivation for the attack, and the potential effects on the organization.

Threat Source or Actor

Insider threats are not necessarily hackers or cybercrime experts, which makes the task of identifying them difficult. Insiders by definition are individuals or entities that have or had authorized access to the organization's information and information systems (physical or logical). Common threat actors that should be considered when building insider threat profiles or risk scenarios include:

- Current or former employees.
- Full-time or part-time employees.
- Temporary employees or contractors.
- Trusted business partners.

While it is difficult to identify the individuals that are at the highest risk of performing malicious activities, it may be helpful to understand some of the characteristics that may be used to develop a behavioral baseline for identifying insider threat actors. **Figure 2** displays a list of "red flag" behavioral characteristics issued by the National Cybersecurity and Communications Integration Center. Note that the listing of these characteristics does not represent importance or likelihood.

Figure 2: Characteristics of Insiders at Risk of Becoming a Threat

Introversion.	Overly concerned with avoiding, concealing, or fixing mistakes.
Greed/financial need.	Inability to assume responsibility for actions.
Vulnerability to blackmail.	Intolerance of criticism.
Compulsive and destructive behavior.	Self-perceived value exceeding performance.
Rebellious, passive aggressive behavior.	Lack of empathy.
Ethical "flexibility."	Pattern of frustration and disappointment.
Entitlement – narcissism (ego/self-image).	History of managing crisis ineffectively.

Source: National Cybersecurity and Communications Integration Center, *Combating the Insider Threat*, 1.

Target

Targets include assets or any items of value to the organization that can be affected by the threat and result in negative impact to the organization, including:

- People.
- Information.
- Technology.
- Facilities.

Motivation

The motivations for an insider threat actor to engage in nonmalicious activities are significantly varied and numerous. Anything from personal issues outside of the office to issues with colleagues and management, as well as opportunity and boredom could lead an individual to engage in these activities.

Possible Indicators That a Vulnerability Is Being Exploited

- Cloud storage uploads.
- Removable storage use.
- Working odd hours without authorization.
- Email to external agent or personal email account.
- Excessive printing or copying proprietary or classified material.
- Requesting access to previously denied areas or systems.

Motivations for malicious attacks may include, but are not limited to:

- Financial gain.
- Fraud.
- Mischief.
- Malice.
- Revenge.
- Espionage.
- Theft.
- Association with criminals.

Negative Impact

The impact of insiders exploiting a vulnerability can be categorized following the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Enterprise Risk Management Framework* as financial, operational, compliance, and customer. It is common that one attack can result in more than one impact category; for example, sabotage of critical information systems can result in financial (cost to restore systems), operational (loss of productivity), and customer (poor service during outage) impacts.

Insider threat profiles can be developed using the dimensions described in the previous sections as shown in **Figure 3.**

Figure 3: Building an Insider Threat Profile

	Profile 1	Profile 2
Threat	IT sabotage	Theft of IP
Threat actor	Former employee	Current employee
Target	Computer network	Trade secrets
Motivation	Malice (revenge)	Financial gain
Negative Impact	Disruption to operations	Loss of competitive advantage

In addition, it is important that organizations rank potential risks related to insider threats using factors such as likelihood of occurrence, velocity, and persistence to build a risk profile that reflects the organization's **risk appetite** and tolerance.

Risks should also be cross-referenced with potential actors to build inherent risk profiles for job functions — such as system administrators, help desk operators, service providers — that require access to data classified as sensitive, critical, or confidential. Creating risk profiles by function should enable management to implement controls that may help prevent and detect intentional or unintentional attacks in a cost-effective way.

The Role of Internal Audit in Insider Threat Management

The **internal audit activity** uses a systematic, disciplined, and risk-based approach to provide objective assurance, advice, and insight. As it relates to insider threat management, the primary responsibility of the internal audit activity is to provide **assurance** and **consulting services** that help the organization accomplish its objectives by evaluating and contributing to the improvement of the organization's risk management, control, and governance processes, as described in Standard 2100 – Nature of Work.

Assurance engagements are intended to assess the effectiveness of control and may outline opportunities for improvement. They may also help senior management and the board better understand risks and the need for response. On the other hand, consulting engagements may help the organization develop or enhance a program to manage insider threats (i.e., early intervention), or may be used to assess the program's adequacy (i.e., benchmarking).

Consulting Engagements

Standard 2010.C1 requires the **chief audit executive** (CAE) to consider accepting proposed consulting engagements if they have the potential to add value by improving the organization's risk management and operations.

Consulting engagements may provide value when the IT operations staff cannot dedicate time and resources to assess the risks related to insider threats and identify the necessary controls. Internal auditors may support system and network administration staff in performing risk assessments concerning insider threats, identifying issues that systems and security administrators may have missed, or areas where policies are not followed properly. In a consulting capacity, internal auditors may make recommendations for addressing such gaps and provide objective insight and knowledge.

IT Governance

For more information about IT governance, see IIA GTAG "Auditing IT Governance."

Independent of the type of engagement, internal auditors must assess and make appropriate recommendations to improve the organization's governance processes (Standard 2110 – Governance). In many cases organizations may have technology controls in place, but do not have formalized governance frameworks to direct, manage, and monitor activities critical to the organization's success. One example of this scenario would be the absence of policies or consistent procedures for provisioning and managing access to users, which could result in unnecessary privileges and increase the risk of insider threats in spite of having technology controls to manage user access.

At least annually or when major changes in technology or business practices occur, risks should be assessed and insider threat programs should be reevaluated. Depending on the size of the organization and the complexity of the IT environment, assessing an entity-level program may be difficult; therefore, internal auditors may perform multiple engagements to assess different components of the program (e.g., governance, information security, physical security, or hiring practices) or may include those components in internal audit engagements that include critical digital assets in the scope. For example, internal auditors may assess whether the security monitoring functions have the necessary mechanisms to detect anomalies from within that could indicate compromised credentials or authorized users abusing their privileges. If the organization has already implemented mechanisms to monitor the external and internal environment, internal auditors may assess the effectiveness and efficiency of such control processes and may help promote continuous improvement (Standards 2120 – Risk Management and 2130 – Control).

The CAE must consider whether the internal audit activity collectively possesses the appropriate knowledge, skills, and other competencies to perform such engagements (Standard 1210 – Proficiency). For assurance engagements, internal auditors are expected to have sufficient knowledge of key IT risks and controls; however, they are not expected to have the expertise of internal auditors whose primary responsibility is IT auditing (Standard 1210.A3). If the internal audit activity lacks the necessary competencies to perform an assurance engagement involving insider threats, the CAE must obtain competent assistance and advice, according to Standard 1210.A1. Internal auditors should collaborate with personnel in IT operations and information security to leverage the required technical expertise to ensure a comprehensive assessment of insider threats. Additionally, the CAE should coordinate activities and share information with these functions to leverage capabilities, ensure proper assurance coverage, and minimize duplication of efforts, as described in Standard 2050 – Coordination and Reliance.

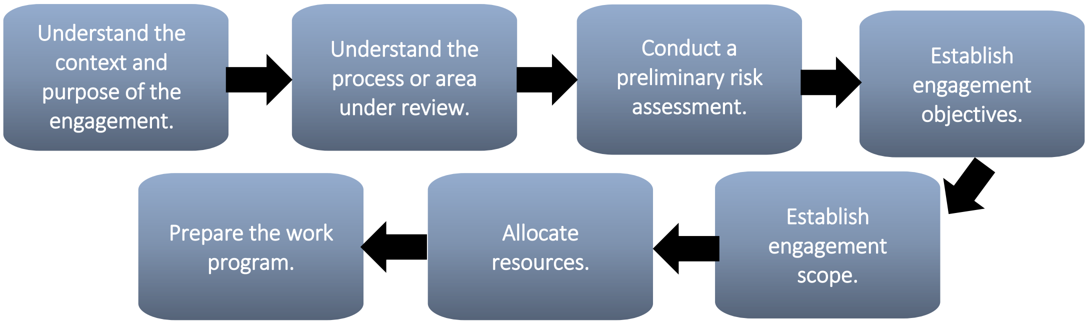
Planning Engagements to Assess Insider Threat Programs

Standard 2200 – Engagement Planning instructs that internal auditors must develop and document a plan for each engagement. Standard 2201 – Planning Considerations adds that internal auditors must consider:

- The strategies and objectives of the activity being reviewed and the means by which the activity controls its performance.
- The significant risks to the activity's objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level.
- The adequacy and effectiveness of the activity's governance, risk management, and control processes compared to a relevant framework or model.
- The opportunities for making significant improvements to the activity's governance, risk management, and control processes.

Engagement planning typically includes several steps, as **Figure 4** depicts, that help internal auditors gain an understanding of the area or process that will be reviewed and document the information that supports the engagement plan and work program. Because reviewing and documenting information is an ongoing process, the steps may not be completely distinct and linear.

Figure 4: Internal Audit Engagement Planning Steps


Understand the context and purpose of the engagement.
Understand the process or area under review.
Conduct a preliminary risk assessment.
Establish engagement objectives.
Establish engagement scope.
Allocate resources.
Prepare the work program.

Note: Several of the steps depicted in Figure 4 have been addressed in detail in other practice guides issued by The IIA (see Appendix A).

Understanding Engagement Context and Purpose

This step is necessary to ensure that the goals and objectives set forth in the internal audit plan are accomplished and that stakeholders' expectations are properly included in the engagement plan. For ad hoc engagements, or engagements requested by senior management or the board after a significant change in the business or technology environment, this step is critical to ensure that internal auditors understand fully the expectations of senior management. For example, after a merger or acquisition, senior management may need to understand whether the acquired organization has introduced new risks to the environment and whether those risks are being addressed by the existing insider threat program.

Understanding the Process or Area Under Review

There are two critical areas the internal auditor must understand clearly when planning an engagement to assess how well the organization is managing risks related to insider threats. Internal auditors should first understand the nature of insider threats and the practices that may be implemented to identify, protect, detect, respond to, and recover from an IT security incident. To build their knowledge, internal auditors may consider using established security frameworks, programs, and recommendations. Appendix E lists resources and agencies that provide guidance and assistance related to information security, and Appendix F offers additional resources. Internal auditors may start with this information but should identify specific frameworks and recommendations applicable to the industry, market, and geographical location in which their organization operates.

Fraud Risk

Because fraud is one of the key risks related to insider threats, it is important to obtain information about fraud allegations, occurrences, and investigations.

For detailed instructions on how to incorporate fraud risk into engagement planning, see IIA Practice Guide "Engagement Planning: Assessing Fraud Risks."

In addition, internal auditors should understand the organization and its objectives. Understanding the business objectives provides a basis for internal auditors to identify risks that should be included in the preliminary engagement-level risk assessment (as required by Standard 2210.A1).

Insider Threat Management

Insider threats cannot be completely eliminated, but they can be managed to prevent or reduce their impact if they materialized. An insider threat program is a combination of policies, procedures, and controls to identify, prevent, detect, respond to, and recover from an IT security incident.

The primary purpose of implementing an insider threat program is to protect critical assets, which can be physical and logical and include people, facilities, systems, and information. Trying to protect everything the organization considers an asset can be a daunting and expensive proposition; thus it is important that the first step in the process is to identify and classify critical assets.

Developing an Insider Threat Program

To improve the rate of success, the organization should formalize the program and manage its development and implementation in a systematic way (similar to any other project) that clearly documents expectations, roles and responsibilities, timing and activities. By having a formal project plan or road map, the organization can identify the current state (gap analysis) and determine the resources needed to complete the project (e.g., people, money, time, and technology). One key to a successful insider threat management process is collaboration among functions that provide oversight (e.g., senior management and the board) and those responsible for implementing the program (e.g., human resources, legal, operations, data owners, information security, and software engineering).

Addressing the Human Factor

Effective insider threat programs consider human and technology controls. Robust IT governance and enterprise risk management programs can provide the foundation to manage and control the human factor.

Rather than starting from the ground up, organizations can benefit from customizing existing insider threat management frameworks developed by private, public and not-for-profit organizations to fit their specific needs. By doing so, the organization can speed the development and implementation of the insider threat program.

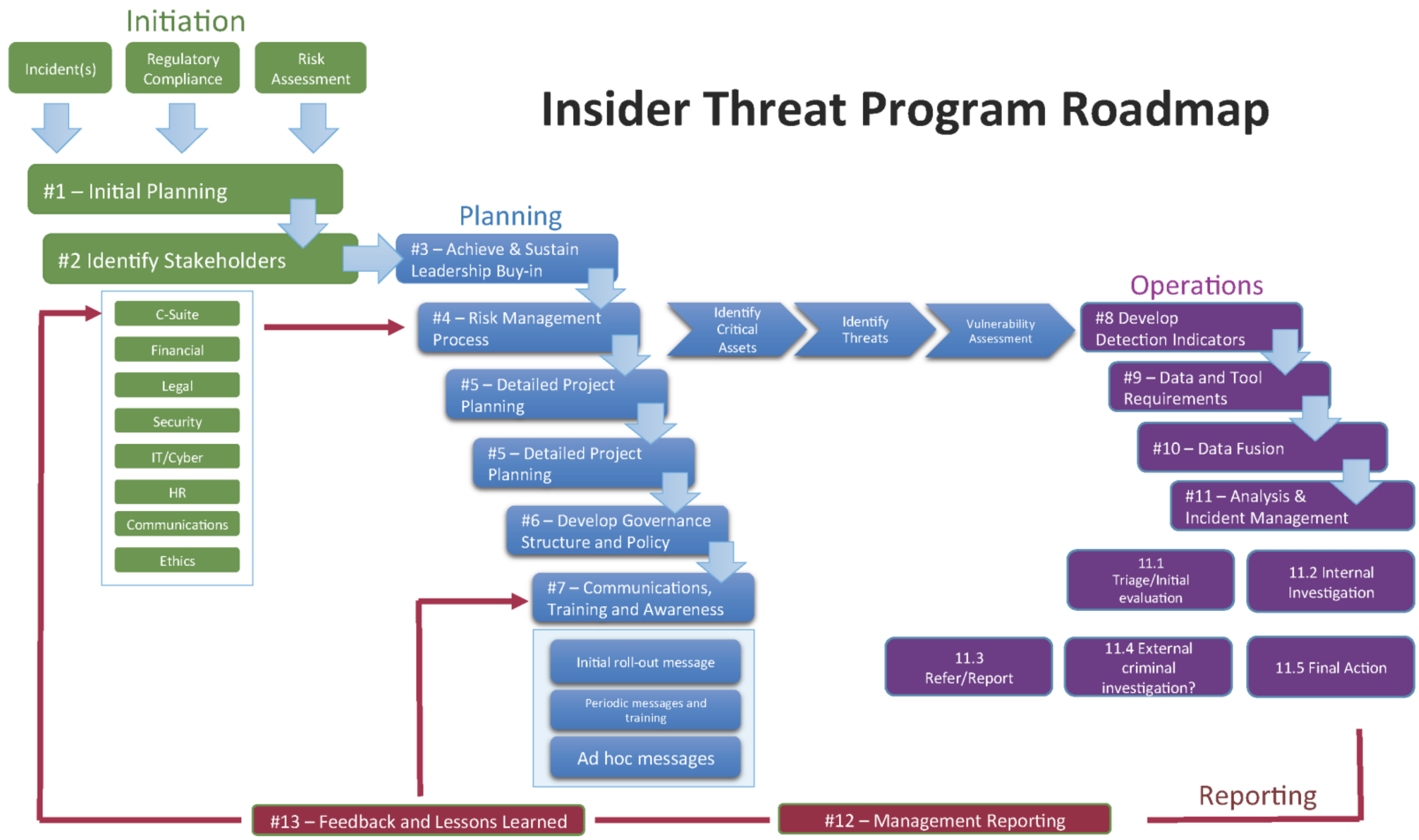
Examples of frameworks that can be used to develop an insider threat program include:

- NIST "Framework for Improving Critical Infrastructure Cybersecurity" (shown in Appendix C), which provides a set of activities to identify, protect, detect, respond and recover from cyberattacks. This framework was developed with the main goal of helping organizations manage cybersecurity programs, however the activities are also applicable to managing insider threats.
- The "Common Sense Guide to Mitigating Insider Threats, Fifth Edition" published by Carnegie Mellon University shown in Appendix D, which provides 20 recommended practices that can help any organization develop an insider threat program to mitigate (deter, detect, and respond to) insider threats.
- The U.S. Intelligence and National Security Alliance (INSA) "Identifying and Countering Insider Threats Study," which provides a 13 step road map (or essential elements) to develop, implement, and monitor an insider threat program as shown in **Figure 5.**

Frameworks Used by Internal Audit

Internal auditors can use similar frameworks as part of the criteria to evaluate the capability of their organization's insider threat program during assurance or consulting engagements.

Figure 5: INSA Insider Threat Program Road Map


Initiation
Incident(s)
Regulatory Compliance
Risk Assessment
Insider Threat Program Roadmap
#1 – Initial Planning
#2 Identify Stakeholders
C-Suite
Financial
Legal
Security
IT/Cyber
HR
Communications
Ethics
Planning
#3 – Achieve & Sustain Leadership Buy-in
#4 – Risk Management Process
Identify Critical Assets
Identify Threats
Vulnerability Assessment
#5 – Detailed Project Planning
#5 – Detailed Project Planning
#6 – Develop Governance Structure and Policy
#7 – Communications, Training and Awareness
Initial roll-out message
Periodic messages and training
Ad hoc messages
Operations
#8 Develop Detection Indicators
#9 – Data and Tool Requirements
#10 – Data Fusion
#11 – Analysis & Incident Management
11.1 Triage/Initial evaluation
11.2 Internal Investigation
11.3 Refer/Report
11.4 External criminal investigation?
11.5 Final Action
Reporting
#12 – Management Reporting
#13 – Feedback and Lessons Learned

Source: U.S. Intelligence and National Security Alliance in partnership with DHS, FBI, and ODNI, Insider Threat Program Roadmap, https://www.insaonline.org/insider-threat-roadmap/. Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

Initiation Phase

During this phase the organization identifies the need for an insider threat program, defines the scope for the program, and identifies the main stakeholders. Some of the questions that may help the organization to identify and prioritize the protection of its critical assets include:

- What critical assets do we have?
- Do we know the current state of each critical asset?
- Do we understand the importance of each critical asset and can we explain why it is critical to our organization?
- Can we prioritize our list of critical assets?
- Do we have the authority, money, and resources to effectively monitor our critical assets?

Planning Phase

The planning phase usually starts by obtaining senior management buy-in, and identifying the assets that must be protected. Some of the steps the organization may take to complete this phase include:

- Identify systems and digital assets.
- Identify regulatory requirements.
- Conduct a risk assessment.
- Develop a formal implementation project plan.
- Create (if needed) governance structure and policies.
- Develop communication, training, and reporting plans.

Operations Phase

During this phase the organization analyzes needs and gaps and prioritizes activities to address them. Some of the typical activities that take place during this phase include:

- Cost/benefit analysis.
- Develop insider threat profiles.
- Identify/implement the necessary controls to address insider threats (examples of common IT security controls are shown in **Figure 6**).
- Develop key performance indicators.
- Formalize IT security incident management procedures.

Figure 6: Common IT Security Controls

Administrative	Physical	Technical
Policies and procedures. Personnel policies. Password policies. Service level agreements (SLAs). Security related awareness and training. Change management. Configuration management. Patch management. Archival, backup, and recovery procedures.	Fire suppression. Heating, ventilation, and air conditioning (HVAC). Electromagnetic shielding (EMI). Environmental monitoring. Video monitoring. Fences, gates, and walls. Lighting. Access cards. Guards. Locks, turnstiles, and mantraps.	Cryptography. Virtual private networks (VPNs). Demilitarized zone (DMZ). Firewalls. Access control lists. Proxy servers. Address translation. Intrusion detection/prevention (IDS/IPS). Honeypots. Network segmentation.

Source: CERT, Model-Driven Insider Threat Control Selection and Deployment.

Reporting Phase

Monitoring and reporting are very important to ensure the organization is addressing risks related to insider threats as the internal and external environments change. The organization can repeat the steps in the implementation plan as many times as needed as part of a continuous improvement approach.

Engagement Planning Information

Activities internal auditors may perform to gain an understanding of the organization's insider threat program include but are not limited to:

Reviewing Documentation

- Review current business plans and risk assessment results.
- Review prior assessments (internal and external).
- Review organizational charts to identify relevant stakeholders.
- Review any policies or procedures related to user management, access management, remote administration and access (e.g., vendor), and system configuration manuals.
- Review asset and data inventories to identify the organization's critical systems and data.

Legal Considerations

Employee monitoring controls are critical to managing insider threats, but they can expose the organization to legal risk related to state, federal, and cross-border laws protecting personal privacy. One example is the European Union's (EU) general data protection regulation (GDPR) intended to protect the privacy of all individuals living in the EU.

To manage this type of legal risk it is important to coordinate activities with legal and HR to make sure that individual rights are taken into account when considering monitoring practices.

- Review access control lists and firewall restrictions that limit access to sensitive systems and data located on the internal network.
- Identify and review applicable laws and regulations that influence the context of the audit engagement.

Interviewing Relevant Stakeholders

To gather information, internal auditors may interview employees who perform tasks associated with the insider threat program, the management responsible for oversight, and the individuals with authority to make decisions. Some of the stakeholders to include are listed in **Figure 7.**

Audit Considerations

CERT's list of 20 practices included in Appendix D may be used to develop internal control questionnaires (ICQs) to gather information about control activities during the engagement planning phase, or to develop stakeholder interview questions.

Figure 7: Stakeholders in the Insider Threat Program

Business Stakeholders	IT Stakeholders
C-level managers.	Information technology (CIO, CTO).
Security (physical, personnel, and information).	Data architect (or functionality).
Human resources (HR).	System network architect.
Legal/privacy.	Information assurance specialists.
Ethics and compliance.	IT security investigation specialists.
Acquisition/contracting/purchasing.	IT operations.
Critical lines of business (products, services, data owners, trusted business partners as appropriate).	Software development.
Public relations.	Computer incident response team (CIRT).

As part of the interviews or separately, internal auditors may lead brainstorming sessions with stakeholders to identify inherent risks. Later, the resulting list can be input into a more detailed risk assessment to determine the residual risk and prioritize risks according to significance.

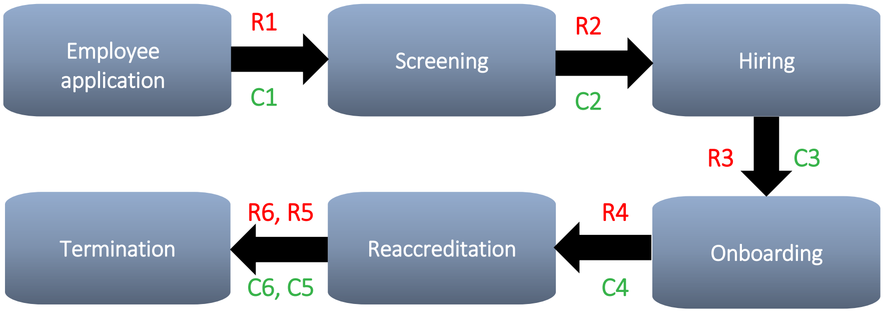
Staying Ahead of Threats

Because the threat landscape changes rapidly, internal auditors should check the resources in Appendices C through E frequently for updates.

Mapping the Process or Subprocesses Flow

One way to identify risks and controls is to develop a high-level process map that depicts inputs, outputs, interfaces, and controls. Mapping an entire insider threat management program may be difficult, but internal auditors can focus the mapping exercise on high-risk processes. To gain an understanding of key risks and controls, for instance, internal auditors may map processes for employee management; vendor management; mergers and acquisitions; identity management and access control; and asset classification and prioritization. **Figure 8** provides an example of a high-level process map.

Figure 8: Example of a High-level Process Map: Employee Management



Subprocess	Risks	Controls
Employee application	R1: Employees from major competitors are hired, increasing the likelihood of IP theft and loss of competitive advantage.	C1: Employment history is evaluated as part of the employment application process, and additional screening is conducted to determine if they may pose a threat.
Screening	R2: Employees with criminal backgrounds are hired, increasing the likelihood of fraud.	C2: Criminal and financial background checks are conducted as allowed by privacy laws.
Hiring	R3: Employees with stakes in major competitive organizations are hired for positions that handle critical data.	C3: Employees must declare conflicts of interest during the hiring process and every 12 months thereafter.
Onboarding	R4: The onboarding process does not include awareness training about insider threats and protocols to address potential IT incidents.	C4: Every employee must complete awareness training as part of the onboarding process. Access to the network should be granted only when the employee can prove completion of compulsory training.
Reaccreditation	R5: Employees are not reaccredited after changing jobs within the organization resulting in unnecessary access to systems.	C5: Employee access is reviewed at least every six months and any time the employee changes jobs. Access is automatically revoked if the employee is not properly reaccredited.
Termination	R6: During employment termination, the organization does not revoke network access immediately.	C6: HR notifies the help desk immediately after an employee resigns or is terminated. Help desk employees trigger a workflow to remove access from all systems applicable.

Conducting a Preliminary Risk Assessment

Due to time and resource constraints, not all risks can be reviewed during an engagement. Therefore, internal auditors must conduct a preliminary risk assessment and prioritize risks according to significance, which is measured as a combination of risk factors. Figure 9 shows a risk assessment of the most common types of insider threats.

Figure 9: Examples of Insider Threats and Resulting Risks

Threat	Risk	Potential Impact
Fraud	Insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data for personal gain, or theft of information that leads to an identity crime (e.g., credit card fraud).	Loss of shareholder trust resulting from financial misstatements. Reputational damage.
IT sabotage	Insider's use of IT to direct specific harm at an organization or an individual.	System downtime and productivity loss. Denial of service.
Theft of intellectual property	Insider's use of IT to steal intellectual property from the organization. This includes industrial espionage involving insiders.	Loss of competitive advantage. Loss of potential revenue.
Theft or disclosure of sensitive/critical data	An insider's use of IT to steal confidential, proprietary, or private data for financial gain.	Loss of customer trust. Financial loss resulting from restitution payments to customers.
Theft of personal data	An insider's use of IT to steal or disclose personal data.	Loss of customer trust. Financial loss resulting from restitution payments to customers. Financial loss resulting from legal expenses.
Illegal activities	Insider's use of digital assets for monetary gain (e.g., sending spam), to gamble or engage in other activities that may not be sanctioned by the law.	Reputational damage. Financial loss resulting from legal expenses.

Establishing Engagement Objectives

The objectives of the engagement depend on the context and purpose of the engagement. For compliance audits, the objectives are derived from the compliance requirements that must be reviewed. For risk-based assurance engagements, objectives are based on the initial purpose of the engagement and the results of the risk assessment. For consulting engagements, objectives must address governance, risk management, and control processes to the extent agreed upon with the client (Standard 2210.C1).

Help with Engagement Planning

For detailed instructions on developing the elements below, see IIA Practice Guide "Engagement Planning: Establishing Objectives and Scope":

- Risk scenarios.
- Risk and control matrix.
- Risk prioritization maps (i.e., heat maps).

Engagement Objective Examples

Assurance engagement (Compliance) – This engagement will evaluate compliance with the GDPR that requires protection of personally identifiable information (PII). In this example, the criteria for evaluation, required by Standard 2210.A3, are the applicable privacy requirements and controls defined in GDPR.[5]

Assurance engagement (Risk-based) – This engagement will evaluate the effectiveness of the insider threat management program using as a reference the Framework for Improving Critical Infrastructure Cybersecurity published by NIST. In this example, the criteria for evaluation, as required by Standard 2210.A3, is the NIST framework, presented in Appendix C as an engagement work program.

Consulting engagement – This engagement will evaluate the effectiveness of the process to identify and classify digital assets. The internal audit activity will provide recommendations on how to improve the process (if necessary). In this example, the criteria for evaluation, as required by Standard 2210.A3, is determined by the stakeholder who requested the review.

Establishing Engagement Scope

The engagement scope sets the boundaries of the engagement and outlines what will be included in the review. The scope may define such elements as the specific processes and/or areas, geographic locations, and time period (e.g., point in time, fiscal quarter, or calendar year) that will be covered by the engagement, given the available resources.

Once engagement objectives have been established, the internal auditor must establish a scope sufficient to achieve the engagement objectives (Standard 2220 – Engagement Scope), taking into

[5] For more information about GDPR see, https://gdpr-info.eu.

account the relevant systems, records, personnel, and physical properties, including those under the control of third parties (Standard 2220.A1).

Engagement Scope Examples

Based on the engagement objectives established in the previous section, the following examples of engagement scope have been established.

Assurance engagement (Compliance) – The scope for this engagement will include all facilities, systems, and processes that handle customer data for European Union residents.

Assurance engagement (Risk-based) – The scope for this engagement will be limited to reviewing the design documentation for the insider threat program at the entity level. The program will be evaluated using the NIST Framework for Improving Critical Infrastructure Cybersecurity.

Consulting engagement – The scope for this engagement will be limited to the process implemented to identify and classify digital assets in the engineering function.

Allocating Resources

Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources (Standard 2230 – Engagement Resource Allocation). The interpretation of this standard clarifies that *appropriate* refers to the mix of knowledge, skills, and other competencies needed to perform the engagement, and *sufficient* refers to the quantity of resources needed to accomplish the engagement with due professional care.

Internal Auditor Competence

The minimum skills an internal auditor must have include knowledge and understanding of the four IPPF mandatory elements: Core Principles, Definition of Internal Auditing, Code of Ethics, and the *International Standards for the Professional Practice of Internal Auditing*.

The most important skill for internal auditors assessing insider threat management is knowledge of the organization and its strategic objectives, threats, risks, vulnerabilities, and the potential impacts on the organization’s ability to achieve its objectives.

Due to the technical nature of some of the controls used to identify, protect, detect, respond, and recover from an IT incident, it may be necessary to employ internal auditors who understand principles of IS security. If the organization does not have any internal auditors with the necessary competencies, the CAE may need to supplement resources through cosourcing or working with IT employees in the organization as subject matter experts that can provide information without compromising the internal audit activity’s ability to provide objective assurance.

Preparing the Work Program

The engagement work program is the product of the engagement planning phase. For assurance engagements, the work program should describe the engagement objectives, scope, risks, controls, and the procedures that will be used to identify, analyze, evaluate, and document the information while performing the engagement (Standard 2240 – Engagement Work Program and Standard 2240.A1). For consulting engagements, work programs may vary in form and content depending upon the nature of the engagement (Standard 2240.C1).

For the purpose of auditing an insider threat program, the following list includes activities and controls (**Figure 10**) recommended to implement an insider threat program following the Insider Threat Program Road Map described in the section titled "Developing an Insider Threat Program." The activities and controls have been mapped to CERT's 20 practices (in Appendix D) and the control function definitions provided in the cybersecurity framework developed by NIST in Appendix C to show their correlation.

The list of activities and controls to implement an insider threat program is not comprehensive and is intended to demonstrate the use of multiple resources available to prepare a program that fits the organization's needs. Organizations should develop a road map that fits their specific needs, based on size, industry, regulations, geographic location, and other factors related to addressing insider-related risks.

In addition, Appendix C shows a chart of control objectives and controls, based on the NIST Cybersecurity Framework. This framework along with CERT's 20 practices included in Appendix D can be helpful to develop a risk assessment specific to an organization, determine the controls to be tested further, and identify the testing procedures to be used to evaluate the effectiveness of those controls. For organizations that already have functional insider threat programs, these resources can be used to benchmark performance.

Figure 10: Insider Threat Program's Key Activities and Controls

Initiation Phase		
Activity/Controls	CERT Practice	Function
Gain senior management's endorsement.	2	Identify
Identify insider threat frameworks that can be used as a baseline or benchmark.	2	Identify
Evaluate the current state of information security.	2	Identify
Leverage programs that cover information security, corporate security, and data governance to identify and understand critical assets.	2	Identify
Identify key stakeholders and establish governance mechanisms.	2	Identify

Planning Phase		
Activity/Controls	CERT Practice	Function
Assess and scope the project.	2	Identify
Know and protect your critical assets.	1	Identify
Ensure integration with organizationwide risk management.	2, 6	Identify
Develop policies, procedures, and practices that have buy-in from key stakeholders, and take into account organizational culture. Examples of policies include: ▪ Acceptable use policy. ▪ Code of conduct. ▪ HR termination procedures. ▪ Nonrealization policy. ▪ "See something; say something" policy. ▪ Suspicious activity reporting procedures. ▪ Incident response procedures. ▪ Segregation of duties policy. ▪ Incident severity level definitions. ▪ Protocol for communicating with law enforcement.	3	Identify Protect Respond
Beginning with the hiring process, monitor and respond to suspicious or disruptive employee behavior.	4	Identify Respond
Coordinate with HR to implement a monitoring process that covers 30 days before and 30 days after when a key employee with information to critical assets leaves the organization. This 60-day window has been identified as the period when the most damage seems to occur.	9	Protect
Coordinate with human resources to develop a training curriculum to create awareness about insider threats, their related risk, and their potential impacts on the organization.	9	Protect
Coordinate with legal counsel early and often to address privacy data protection and cross-border data transfer compliance requirements.	4	Protect
Anticipate and manage negative issues in the work environment in coordination with legal and human resources.	5	Identify
Coordinate with stakeholders to develop a communications plan.	2	Identify Respond Recover
Identify business partner and third-party providers that have access to the organization's digital assets.	6	Identify
Implement clearly defined investigation and resolution processes to ensure that all incidents are handled following a consistent process.	20	Identify Protect Respond Recover

Planning Phase (continued)		
Activity/Controls	CERT Practice	Function
Screen employees and vendors on a regular basis, especially personnel in high-risk job roles or who have access to critical digital assets.	4, 6	Protect
Develop repeatable processes for identifying, protecting, and detecting insider threats and responding to and recovering from incidents.	2	Identify Protect Detect Respond Recover
– Asset and data classification and governance processes are implemented to prioritize those assets deemed critical/sensitive to the organization. These critical assets should be a top priority when applying insider threat controls.	1	Identify
– Compliance with state, federal, and cross-border regulations over the protection of sensitive data (e.g., HIPAA[6], FERPA[7], GDPR, or PCI DSS[8]) should be considered and implemented accordingly. These regulations often require controls focused on least privilege, or "need to know" type of access levels. Performing these types of assessments or reviews may reveal areas where an insider threat actor could abuse excessive privileges to expose data they do not have a business need to access.	2	Identify Protect Detect
– Define explicit security agreements for cloud service providers, especially access restrictions and monitoring capabilities.	16	Protect
– Monitoring of internal network traffic, similar to monitoring of external inbound network traffic, should be implemented. Often organizations deploy monitoring resources to account for external threats, but do not take internal traffic into account. When coupled with improper network segmentation of critical systems from general purpose staff workstations, organizations could potentially miss network-based insider threat attacks.	12	Detect
– Awareness campaigns to let employees know that the organization is monitoring.	5, 9	Protect
– Social media awareness campaigns to educate employees about potentials risks of disclosure.	7	Protect

[6] The Health Insurance Portability and Accountability Act is a U.S. federal law that contains privacy standards to protect patient medical records and any other health information provided to health care providers.

[7] The Family Educational Rights and Privacy Act is a U.S. federal law designed to protect the privacy of student education records.

[8] The Payment Card Industry Data Security Standard, issued by the PCI Security Standards Council, is a global security standard designed to protect cardholder data.

Planning Phase (continued)

Activity/Controls	CERT Practice	Function
– Privileged access management (PAM). To prevent insider attacks and comply with regulations organizations must proactively monitor and manage privileged access. PAM can help the organization monitor and restrict accounts that have privilege levels far beyond what most users have. In general this type of account is used by system administrators, database administrators, and other personnel who must have the ability to perform administrative or operational tasks. Because these accounts can bypass some controls, the organization must implement policies, processes, and technology to prevent and detect misuse or abuse. The main purpose of PAM is to establish automated management for privileged accounts and credentials, and repeatable processes to track the provision and retirement of critical account entitlements. Examples include deprovisioning all access to development and production systems, and granting one-time-access using an emergency change process that includes login for all activities.	10, 11, 15	Protect
– Structure management and document job descriptions to minimize unintentional insider stress and mistakes.	8	Protect
– Incident response is an organized approach to addressing and managing the aftermath of an IT security incident. Typically, a document that contains instructions and protocols for addressing IT incidents is known as an incident response plan (IRP), and the group of professionals responsible for addressing, analyzing, and reporting IT incidents is known as a computer security incident response team (CSIRT).	2	Respond Recover

Operations Phase

Activity/Controls	CERT Practice	Function
Implement physical and logical controls to protect, detect, respond, and recover. For example:		Protect Detect Respond Recover
– Physical controls include building access management systems and video surveillance that can be used to detect irregular or unauthorized access to areas where critical information is accessible. For example: ▪ Fire suppression. ▪ HVAC. ▪ Video monitoring. ▪ Access cards. ▪ Locks, turnstiles, and mantraps.	2	Protect Detect
– Strong identity and access management controls to govern access to applications, systems, and data (hard copy or digital assets). This includes user provisioning and deprovisioning activities; user access reviews based on business needs; remote access review and approval (vendor and staff); non-shared access policies and controls of internal users, vendors, and third parties.	10, 11, 12, 15	Protect

Operations Phase (continued)		
Activity/Controls	CERT Practice	Function
– Firewalls located in front of critical systems and configured to restrict workstation connection to only those authorized.	13	Protect Detect
– Internal network segmentation and network control restrictions require attention. Information systems that house sensitive organizational data should have access restricted to only those with a business need for the information. This segmentation could include separate virtual local area network (VLAN) assignments, access controls lists or firewall rule sets that isolate those systems, and physically secure locations to house the servers from direct tampering or obstruction.	13	Protect
– External network segmentation and network access restrictions. This segmentation could include the use of demilitarized zones (DMZs), virtual private networks (VPNs), honeypots, and proxy servers to control the interaction between trusted and untrusted environments.	13	Protect Detect
– Security information and event management (SIEM) software solutions combine security information management (SIM) and security event management (SEM) to retroactively examine and log unique user actions against an individual system, data set, or general network activities (shared connections) and create alerts. The resulting logs should be actively reviewed and assessed for abnormalities. Further, these logs should be comprehensive enough to support incident response activities in the event of an IT security incident.	13	Detect Respond
– Security monitoring programs augmented by data analytics tools such as user and entity behavior analytics (UEBA) to determine standard business operational activities on an individual system, data set, or network resources. Understanding routine, common tasks performed on the network on a daily basis will help administrative staff to identify abnormalities or unusual behavior that may indicate malicious activity (red flags).	12, 14	Detect
– Alerting technologies that effectively capture changes, additions, or modifications to network resources, systems, applications, or security controls should be in place. These alerts should go directly to staff responsible for the management of each technology to quickly identify legitimate threats from false positives. These technologies include intrusion detection/prevention systems (IDS/IPS).	17, 19	Detect Respond
– Escalation policies and procedures to ensure those alerts related to credible threats are communicated to key organizational groups to minimize impact. For example, if an alert is received from an application administrator that a new super user account has been created without going through the normal vetting/approval process, this should be immediately communicated to responsible staff such as business owners, data owners, and security groups to prevent threats from gaining deeper, unauthorized access.	3	Respond Recover

Operations Phase (continued)		
Activity/Controls	CERT Practice	Function
– Data loss prevention technologies implemented at the network edge and within email technologies to identify instances when sensitive data is being sent outside of the organization. Further, there should also be a review or assessment of security controls governing data upload/download access to any cloud services in use by the organization, and whether those services can be accessed over a public network, such as the internet. This can be abused by an insider threat actor who could leverage this legitimate business activity to upload sensitive data to the cloud, and then retrieve it from an offsite location that is not under monitoring by the organization.	19	Protect Detect
– Other technology controls include any logical and physical mechanisms used to protect, detect, and respond to IT incidents. For example: ▪ Change management. ▪ Configuration management. ▪ Patch management. ▪ Archival, backup, and recovery procedures. ▪ Penetration testing.	17, 18, 19	Protect Detect Recover
Use data analytics to strengthen the program.	12	Respond
Execute the incident response playbook.	2	Respond Recover
Collect evidence and document lessons learned.	12	Identify

Reporting Phase		
Activity/Controls	CERT Practice	Function
Evaluate the program periodically and update as necessary. These are areas and key performance indicators (KPIs) that are typically evaluated on a maturity scale to determine if the organization is doing the right things.	2	Recover
– Governance, oversight, and development.	2	Recover
– Assessments (threat risks, third parties, and assets).	2	Recover
– Monitoring. ▪ Number or anomalies investigated. ▪ High or increasing rates of data egress. ▪ Number of false positives. ▪ Number of false negatives. ▪ Number of security policies violations by IT personnel.	2	Recover
– Asset protection.	2	Recover

Reporting Phase (continued)

Activity/Controls	CERT Practice	Function
– Performance. ▪ Team overall performance. ▪ Employee turnover. ▪ Budget management. ▪ Internal self-assessments. ▪ External assessments. ▪ Improvement recommendations that have not been acted upon. ▪ Employees placed on performance improvement plans. ▪ Employees or areas with excessive HR claims files against.	2	Recover
– Incident management and response. ▪ Type and quantity of investigations within a specific period of time. ▪ Number of investigations closed satisfactorily. ▪ Number of investigations closed within 30 days. ▪ Quality of communications with internal stakeholders and law enforcement.	2	Identify Recover
– Education and awareness. ▪ Number of users, administrators, investigators, and senior management that have attended training within a specific time period. ▪ Percentage of people that pass a validation questionnaire at the end of the training session. ▪ Frequency of training offered. ▪ Percentage of reoccurrence. ▪ Number of IT incidents reported. ▪ Number of IT incidents detected using monitoring mechanisms.	2	Identify Recover
Ensure lessons learned exercises are conducted after an event to determine areas of improvement.	2	
Implement remediation or improvement plans.	2	Respond Recover

Providing Assurance to the Board

To effectively communicate risks related to insider threats to the board, internal auditors must translate audit findings into terms of financial loss, reputational damage, operational disruption, and other organizational performance indicators.

To illustrate risks in terms that are meaningful for management, internal auditors may find it helpful to leverage existing industry reports describing data compromises and breaches throughout the world that resulted from insider threats. Using real world data helps communicate the breadth and depth of the impacts and helps remove the illusion that insider threats and resulting breaches cannot happen to the organization.

Audit Reports

For detailed instructions on preparing internal audit reports, see IIA Practice Guide "Audit Reports: Communicating Assurance Engagement Reports."

Educating the board includes helping them understand that "absolute security" is not possible; therefore, it is critical to focus on strengthening the organization's IT security incident response capabilities and ensuring balance between security and efficiency (security is managed based on the risk appetite established by the organization). Other key elements for providing assurance to the board include:

- Develop a collaborative reporting approach with parties such as the chief information security officer (CISO) and chief risk officer (CRO) to demonstrate the level of maturity of the organization's security posture related to insider threats.
- Ensure that insider threat risks are included in the organizationwide risk assessment and communicating the effort and results to the board.
- Agree on a framework that all assurance parties can use to assess the maturity and effectiveness of insider threat mitigation efforts.
- Develop possible risk scenarios to describe the potential actors and the likelihood and impact in a language that clearly relates to business objectives.
- Determine whether the internal audit activity possesses the competencies needed to assess insider threat management or can be trained, and if not, outsourcing the expertise.
- Develop the internal audit plan to leverage the work of other assurance functions (compliance, management self-assessments, and risk management results).

To leverage the work of other assurance functions, it is critical to define clear roles and responsibilities among business owners, risk management, compliance, and other assurance stakeholders, and to determine what information can be used and how the internal audit activity will evaluate the reliability of the work done by the first and second lines of defense.

Reliance on Assurance Functions

For instructions on how to create an assurance map, see IIA Practice Guide “Coordination and Reliance: Developing an Assurance Map.”

Appendix A. Relevant IIA Standards and Guidance

The following IIA resources were referenced throughout this practice guide. For more information about applying the *International Standards for the Professional Practice of Internal Auditing*, please refer to The IIA's Implementation Guides.

Standards
Standard 1210 – Proficiency
Standard 2010 – Planning
Standard 2050 – Coordination and Reliance
Standard 2100 – Nature of Work
Standard 2110 – Governance
Standard 2120 – Risk Management
Standard 2130 – Control
Standard 2200 – Engagement Planning
Standard 2201 – Planning Considerations
Standard 2210 – Engagement Objectives
Standard 2220 – Engagement Scope
Standard 2230 – Engagement Resource Allocation
Standard 2240 – Engagement Work Program

Guidance
Practice Guide "Coordination and Reliance: Developing an Assurance Map," 2018.
Practice Guide "Engagement Planning: Assessing Fraud Risk," 2017.
Practice Guide "Engagement Planning: Establishing Objectives and Scope," 2017.
GTAG "Assessing Cybersecurity Risks: Roles of the Three Lines of Defense," 2016.
GTAG "Auditing IT Governance," 2018.

Appendix B. Glossary

Terms identified with an asterisk (*) are taken from The IIA's *International Professional Practices Framework®* Glossary.

Assurance Services* – An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization.

Board* – The highest level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable. Although governance arrangements vary among jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word "board" in the *Standards* refers to a group or person charged with governance of the organization. Furthermore, "board" in the *Standards* may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee).

Business Partners – Any third-party organization that has been given authorized access to the organization's customers, clients or suppliers networks, systems, and data.

Chief Audit Executive* – Describes the role of a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the mandatory elements of the International Professional Practices Framework. The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title and/or responsibilities of the chief audit executive may vary across organizations.

Consulting Services* – Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

Control Processes* – The policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept.

Fraud* – Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

Governance* – The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

IT Security Incident[9] **–** An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Internal Audit Activity* – A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.

Risk* – Is the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

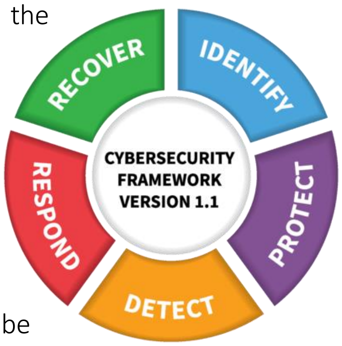
Risk Appetite* – The level of risk that an organization is willing to accept.

Social Engineering [10]**–** In the context of information security, the manipulation of people to get them to unwittingly perform actions that cause harm (or increase the probability of causing future harm) to the confidentiality, integrity, or availability of the organization's resources or assets, including information, information systems, or financial systems.

[9] Committee on National Security Systems Glossary Working Group, *CNSS Instruction No. 4009: National Information Assurance Glossary*, (Washington, D.C.: National Security Agency, 2010), 35.

[10] The CERT® Insider Threat Center, "Unintentional Insider Threats: Social Engineering," https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_77459.pdf, p. xi.

Appendix C. Insider Threat Assessment Using NIST Cybersecurity Framework



N. Hanacek/NIST

In accordance with Standard 2240.A1, "Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement." As a starting point for building a work program, internal auditors may use an existing risk and control framework. The chart below uses NIST's Cybersecurity Framework as the criteria against which an insider threat program may be compared. Internal auditors may adapt this chart to suit their organization and specific engagement. Based on the chart, auditors may develop a risk and control matrix and risk assessment, which may then be expanded into a work program.

NIST's Cybersecurity Framework was created to provide a common language to understand, manage, and express cybersecurity risk both internally and externally. The framework helps users identify and prioritize actions for reducing cybersecurity risks that include insider threats, which can be easily translated into actions for reducing insider threat risks.

The framework is organized into functions (identify, protect, detect, respond, and recover), categories, and subcategories. Categories are used in this work program to represent control objectives, and the subcategories are used to represent control activities. Internal auditors may use the last column to document the controls that exist in their organizations. (*Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.*)

Function: Identify	
Risk Area: Asset Management	
Control Objective: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	
Control Activities	Assessment
Physical devices and systems within the organization are inventoried.	
Software platforms and applications within the organization are inventoried.	
Organizational communication and data flows are mapped.	
External information systems are cataloged.	
Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value.	
Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, and partners) are established.	

Function: Identify (continued)	
Risk Area: Business Environment	
Control Objective: The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	
Control Activities	Assessment
The organization’s role in the supply chain is identified and communicated.	
The organization’s place in critical infrastructure and its industry sector is identified and communicated.	
Priorities for organizational mission, objectives, and activities are established and communicated.	
Dependencies and critical functions for delivery of critical services are established.	
Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).	
Risk Area: Governance	
Control Objective: The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	
Control Activities	Assessment
Organizational information security policy is established.	
Information security roles and responsibilities are coordinated and aligned with internal roles and external partners.	
Legal and regulatory requirements regarding cybersecurity, including privacy, and civil liberties and obligations are understood and managed.	
Governance and risk management processes address cybersecurity risks.	
Risk Area: Risk Assessment	
Control Objective: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	
Control Activities	Assessment
Asset vulnerabilities are identified and documented.	
Cyber threat intelligence and vulnerability information is received from information sharing forums and sources.	
Threats, both internal and external, are identified and documented.	
Potential business impacts and likelihoods are identified.	
Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	
Risk responses are identified and prioritized.	

Function: Identify (continued)

Risk Area: Risk Management Strategy

Control Objective: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Control Activities	Assessment
Risk management processes are established, managed, and agreed to by organizational stakeholders.	
Organizational risk tolerance is determined and clearly expressed.	
The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.	

Risk Area: Supply Chain Risk Management

Control Objective: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess, and manage supply chain risks.

Control Activities	Assessment
Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.	
Identify, prioritize, and assess suppliers and partners of critical information systems, components, and services using a cyber supply chain risk assessment process.	
Suppliers and partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan.	
Suppliers and partners are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted.	
Response and recovery planning and testing are conducted with critical suppliers/providers.	

Function: Protect

Risk Area: Identity Management, Authentication and Access Control

Control Objective: Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Control Activities	Assessment
Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	
Physical access to assets is managed and protected.	
Remote access is managed.	
Access permissions and authorizations are managed, incorporating the principle of least privilege and separation of duties.	
Network integrity is protected, incorporating network segregations where appropriate.	
Identities are proofed and bound to credentials, and asserted in interactions when appropriate.	

Function: Protect (continued)

Risk Area: Awareness and Training

Control Objective: The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

Control Activities	Assessment
All users are informed and trained.	
Privileged users understand roles and responsibilities.	
Third-party stakeholders (e.g., suppliers, customers, and partners) understand roles and responsibilities.	
Senior executives understand roles and responsibilities.	
Physical and information security personnel understand roles and responsibilities.	

Risk Area: Data Security

Control Objective: Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.

Control Activities	Assessment
Data-in-transit is protected.	
Assets are formally managed throughout removal, transfers, and disposition.	
Adequate capacity to ensure availability is maintained.	
Protections against data leaks are implemented.	
Integrity checking mechanisms are used to verify software, firmware, and information integrity.	
The development and testing environment(s) are separate from the production environment.	
Integrity checking mechanisms are used to verify hardware integrity.	

Risk Area: Information Protection Processes and Procedures

Control Objective: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Control Activities	Assessment
A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g., concept of least functionality).	
A system development life cycle to manage systems is implemented.	
Configuration change control processes are in place.	
Backups of information are conducted, maintained, and tested periodically.	
Policy and regulations regarding the physical operating environment for organizational assets are met.	
Data is destroyed according to policy.	

Function: Protect (continued)	
Control Activities	Assessment
Protection processes are continuously improved.	
Effectiveness of protection technologies is shared with appropriate parties.	
Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	
Response and recovery plans are tested.	
Cybersecurity is included in human resources practices (e.g., deprovisioning, and personnel screening).	
A vulnerability management plan is developed and implemented.	
Risk Area: Maintenance	
Control Objective: Maintenance and repairs of industrial control and information system components is performed consistently with policies and procedures.	
Control Activities	Assessment
Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools.	
Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	
Risk Area: Protective Technology	
Control Objective: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	
Control Activities	Assessment
Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	
Removable media is protected and its use restricted according to policy.	
The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	
Communication and control networks are protected.	
Systems operate in pre-defined functional states to achieve availability (e.g., under duress, under attack, during recovery, and normal operations).	

Function: Detect

Risk Area: Anomalies and Events

Control Objective: Anomalous activity is detected in a timely manner and the potential impact of events is understood.

Control Activities	Assessment
Detected events are analyzed to understand attack targets and methods.	
Event data are aggregated and correlated from multiple sources and sensors.	
Impact of event is determined.	
Incident alert thresholds are established.	

Risk Area: Security Continuous Monitoring

Control Objective: The information systems and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

Control Activities	Assessment
The network is monitored to detect potential cybersecurity events.	
The physical environment is monitored to detect potential cybersecurity events.	
Personnel activity is monitored to detect potential cybersecurity events.	
Malicious code is detected.	
Unauthorized mobile code is detected.	
External service provider activity is monitored to detect potential cybersecurity events.	
Monitoring for unauthorized personnel connections, devices, and software is performed.	
Vulnerability scans are performed.	

Risk Area: Detection Processes

Control Objective: Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Control Activities	Assessment
Roles and responsibilities for detection are well defined to ensure accountability.	
Detection activities comply with all applicable requirements.	
Detection processes are tested.	
Event detection information is communicated to appropriate parties.	
Detection processes are continuously improved.	

Function: Respond

Risk Area: Response Planning

Control Objective: Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.

Control Activities	Assessment
Response plan is executed during or after an event.	

Risk Area: Communications

Control Objective: Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

Control Activities	Assessment
Personnel know their roles and order of operations when a response is needed.	
Events are reported consistent with established criteria.	
Information is shared consistent with response plans.	
Coordination with stakeholders occurs consistent with response plans.	
Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	

Risk Area: Analysis

Control Objective: Analysis is conducted to ensure adequate response and support recovery activities.

Control Activities	Assessment
Notifications from detection systems are investigated.	
The impact of the incident is understood.	
Forensics are performed.	
Incidents are categorized consistent with response plans.	

Risk Area: Mitigation

Control Objective: Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

Control Activities	Assessment
Incidents are contained.	
Incidents are mitigated.	
Newly identified vulnerabilities are mitigated or documented as accepted risks.	

Risk Area: Improvements

Control Objective: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Control Activities	Assessment
Response plans incorporate lessons learned.	
Response strategies are updated.	

Function: Recover	
Risk Area: Recovery Planning	
Control Objective: Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	
Control Activities	Assessment
Recovery plan is executed during or after an event.	
Risk Area: Improvements	
Control Objective: Recovery planning and processes are improved by incorporating lessons learned into future activities.	
Control Activities	Assessment
Recovery plans incorporate lessons learned.	
Recovery strategies are updated.	
Risk Area: Communications	
Control Objective: Restoration activities are coordinated with internal and external parties, such as coordinating centers, internet service providers, owners of attacking systems, victims, other computer security incident response teams, and vendors.	
Control Activities	Assessment
Public relations are managed.	
Reputation after an event is repaired.	
Recovery activities are communicated to internal stakeholders and executive management teams.	

Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce.
Not copyrightable in the United States.

Appendix D. CERT Best Practices to Mitigate Insider Threats

The following table appears in the “Common Sense Guide to Mitigating Insider Threats, Fifth Edition,” authored by the CERT® Insider Threat Center of Carnegie Mellon University’s Software Engineering Institute. The 20 best practices are intended to be a reference for organizations that need to create or update an insider threat program and should be customized to suit the organization’s needs, culture, and risk appetite. The order in which CERT has arranged the practices is intended to make the process of implementing an insider threat program easier.

These 20 best practices are high-level statements or control objectives and each best practice is broken down into more specific control activities in the guide.

Order	Best Practice
1	Know and protect your critical assets.
2	Develop a formalized insider threat program.
3	Clearly document and consistently enforce policies and controls.
4	Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
5	Anticipate and manage negative issues in the work environment.
6	Consider threats from insiders and business partners in enterprise-wide risk assessments.
7	Be especially vigilant regarding social media.
8	Structure management and tasks to minimize unintentional insider stress and mistakes.
9	Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.
10	Implement strict password and account management policies and practices.
11	Institute stringent access controls and monitoring polices on privileged users.
12	Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
13	Monitor and control remote access from all end points, including mobile devices.
14	Establish a baseline of normal behavior for both networks and employees.
15	Enforce separation of duties and least privilege.
16	Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
17	Institutionalize system change controls.
18	Implement security backup and recovery processes.
19	Close the doors to unauthorized data exfiltration.
20	Develop a comprehensive employee termination procedure.

Source: CERT, “Common Sense Guide to Mitigating Insider Threats, Fifth Edition,” 2016, Table 1, pg. xii.

Appendix E. Organizations and Agencies That Issue Advice

The resources below may provide information to help the organization identify, monitor, and manage insider threats. While not exhaustive, the list is provided to help internal auditors expand their knowledge and skills. Additionally, local and industry security standards and regulations must be considered during the audit engagement planning phase to ensure resources are allocated to the risks that are most significant to the specific organization.

American National Standards Institute/International Society of Automation
ANSI is the voice of the U.S. standards and conformity assessment system and the official U.S. representative to the International Organization for Standardization and, via the U.S. National Committee, the International Electrotechnical Commission (IEC). ANSI's mission is to enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity. https://www.ansi.org/cyber/

Australian Government: Attorney-General's Department
The Protective Security Policy Framework (PSPF) comprises the Australian government's security risk management approach and guidance to support effective implementation. The PSPF includes three personnel security core requirements essential for mitigating the threat posed by trusted insiders. https://www.protectivesecurity.gov.au/personnel/Pages/default.aspx

Center for Internet Security
CIS is a nonprofit entity that establishes global standards and best practices for securing IT systems and data to safeguard private and public organizations against cyber threats based on the work of a global IT community. https://www.cisecurity.org

CERT Australia
CERT Australia is the national computer emergency response team. Established in 2010, CERT is the primary government contact point for major Australian businesses to:

- Receive and respond to cybersecurity incident reports.
- Receive support and advice in responding to and mitigating cyber incidents.
- Monitor cybersecurity incidents or attacks to develop a threat picture.
- Provide advice and alerts to its partners to enhance their cybersecurity resilience.

https://www.cert.gov.au/

CERT - SEI

CERT is a division of the Carnegie Mellon University Software Engineering Institute that studies and solves problems with widespread cybersecurity implications, researches security vulnerabilities in software products, contributes to long-term changes in networked systems, and develops cutting-edge information and training to help improve cybersecurity. The CERT Insider Threat Center provides resources to help organizations develop and implement insider threat management programs. http://www.cert.org

CSA Singapore

The Cyber Security Agency of Singapore (CSA) is a national agency overseeing cybersecurity strategy, operation, education, outreach, and ecosystem development in Singapore. It is part of the Prime Minister's Office and is managed by the Ministry of Communications and Information. Among other activities, CSA is dedicated to:

- *Engagement and outreach –* Nurturing ties with local and global industry and thought leaders, heightening cybersecurity awareness through public outreach programs, and promoting security-by-design.
- *Ecosystem development –* Developing a robust cybersecurity ecosystem (i.e., a vibrant industry equipped with the manpower to respond to and mitigate cyberattacks).
- *Protecting critical sectors –* Strengthening cybersecurity in our critical sectors, such as energy, water, and banking.
- *Operations –* Ensuring effective coordination and deployment in our response to cyber threats.

https://www.csa.gov.sg

Intel® Corporation

Insider Threat Field Guide is a white paper report that identifies 60 most likely insider threat attack vectors to give organizations a consistent way to share information internally and externally and enable more effective security strategies and responses to attacks from within the organization. https://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/a-field-guide-to-insider-threat-paper.html

Intelligence and National Security Alliance

In partnership with the Department of Homeland Security, Federal Bureau of Investigation, and Office of the Director of National Intelligence, INSA facilitates collaborative partnerships between members of the private sector and teams of experienced intelligence community analysts. Guidance on identifying and countering insider threats is among the top priorities for this agency. https://www.insaonline.org

International Organization for Standardization/International Electrotechnical Commission

ISO is an independent, nongovernmental international organization with a membership of 161 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant international standards that support innovation and provide solutions to global challenges. IEC is the world's leading organization for the preparation and publication of international standards for electrotechnologies (electrical, electronic and related technologies). When appropriate, IEC cooperates with ISO to ensure that international standards fit together seamlessly and complement each other. https://www.iso.org

INTERPOL

INTERPOL is the world's largest international police organization, with 192 member countries. INTERPOL publishes general guidance on cybercrime and cyber-enabled crime. https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

National Institute of Standards and Technology

NIST's Cybersecurity Framework is a set of standards and best practices, created through the collaboration between the public and private sector, to help organizations manage cybersecurity risks. The framework uses a common language to address and manage cybersecurity risks in a cost-effective way based on business needs. https://www.nist.gov/cyberframework

Appendix F. References and Additional Resources

The resources below may provide information to help the organization identify, monitor, and manage insider threats. While not exhaustive, the list is provided to help internal auditors expand their knowledge and skills. Additionally, local and industry security standards and regulations must be considered during the audit engagement planning phase to ensure resources are allocated to the risks that are most significant to the specific organization.

References

CERT Insider Threat Center. *Common Sense Guide to Mitigating Insider Threats, Fifth Edition*. Pittsburgh, PA: Carnegie Mellon University, 2016. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf.

CERT Insider Threat Center. Unintentional Insider Threats: Social Engineering. Pittsburgh, PA: Carnegie Mellon University, 2014. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_77459.pdf.

INSA. "Insider Threat Program Roadmap." https://www.insaonline.org/insider-threat-roadmap/.

National Cybersecurity and Communications Integration Center. U.S. Department of Homeland Security, *Combating the Insider Threat*. Washington, DC: DHS/US-CERT, 2014. https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf.

Ponemon Institute ©. *2018 Cost of Insider Threats: Global*. New York, NY: ObservIT 2018. https://www.observeit.com/ponemon-report-cost-of-insider-threats/.

Stoneburner, Gary; Alice Goguen, and Alexis Feringa. National Institute of Standards and Technology (NIST), Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

International Professional Practices Framework, 2017 Edition. Lake Mary, FL: The Institute of Internal Auditors, 2017.

Trzeciak, Randy, and Dan Costa. *Model-Driven Insider Threat Control Selection.* Pittsburgh, PA: Carnegie Mellon University, 2017. https://resources.sei.cmu.edu/asset_files/presentation/2017_017_001_509187.pdf.

Additional Resources

American National Standards Institute/International Society of Automation. ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program. https://tinyurl.com/ANSI-ISA-62443-2-1.

American National Standards Institute/International Society of Automation. ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels. https://tinyurl.com/ANSI-ISA-62443-3-3.

A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector. https://www.insaonline.org/a-preliminary-examination-of-insider-threat-programs-in-the-u-s-private-sector/.

Australian Government Attorney-General's Department. 13 Ongoing assessment of personnel. Accessed June 27, 2018, https://www.protectivesecurity.gov.au/personnel/ongoing-assessment-of-personnel/Pages/default.aspx.

Center for Internet Security. CIS Critical Security Controls™ for Effective Cyber Defense (CIS Controls). https://www.cisecurity.org/controls/.

CERT Australia. Insider threat: Beyond technical controls. March 26, 2018. https://www.cert.gov.au/news/insider-threat-beyond-technical-controls.

Costa, Daniel. "CERT Definition of 'Insider Threat' – Update." *Insider Threat Blog*, Carnegie Mellon University Software Engineering Institute, SEI Insights. March 7, 2017. https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html.

Intel® Corporation. *Insider Threat Field Guide*. https://www.intel.com/content/www/us/en/it-management/intel-it-best-practices/a-field-guide-to-insider-threat-paper.html.

International Organization for Standardization/International Electrotechnical Commission. ISO/IEC 27001: 2013, Information Technology — Security Techniques — Information Security Management Systems — Requirements. https://www.iso.org/standard/54534.html.

Miller, Sarah. ""The Frequency and Impact of Insider Collusion," *Insider Threat Blog*, Carnegie Mellon University Software Engineering Institute, SEI Insights, June 22, 2016. https://insights.sei.cmu.edu/insider-threat/2016/06/the-frequency-and-impact-of-insider-collusion.html.

National Institute of Standards and Technology. NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (including updates as of January 15, 2014). http://dx.doi.org/10.6028/NIST.SP.800-53r4.

Ponemon Institute©. 2017 Cost of Cyber Crime Study. New York, NY: Accenture, 2017. https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50.

Ponemon Institute©. 2016 Cost of Cyber Crime Study. Traverse City, MI: Ponemon Institute, 2016. https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf.

Acknowledgments

Guidance Development Team

Himi Tina Kim, CIA, CGAP, CRMA, United States (Chairman)
Joseph Keating, United States
Michael Lynn, CRMA, United States
Sajay Rai, United States
Terence Washington, CIA, CRMA, United States

Global Guidance Contributors

Jared Hoffman, United States
Yadeli Ibarra, CISA, Mexico
Brad McGary, United States
Phillip Nemmers, CISA, United States
Patricia Rowe Seale, CIA, CRMA, CISA, CRISC, Barbados
Andriy Rybalchenko, CISA, CISM, Ukraine
Deb Snyder, United States

IIA Global Standards and Guidance

Eva Sweet, CISA, CISM, IT and PS Director, (Project Lead)
Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, Vice President
Debi Roth, CIA, Managing Director
Anne Mercer, CIA, QIAL, Director
Jeanette York, CCSA, FS Director
Shelli Browning, Technical Editor
Lauressa Nelson, Technical Editor

The IIA would like to thank the following oversight bodies for their support: Information Technology Guidance Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and International Professional Practices Framework Oversight Council.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession’s most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from more than 170 countries and territories. The association’s global headquarters are in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

The IIA publishes this document for informational and educational purposes and, as such, is only intended to be used as a guide. This guidance material is not intended to provide definitive answers to specific individual circumstances. The IIA recommends that you always seek independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this guidance.

Copyright

August 2018

The Institute of Internal Auditors | Global

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.theiia.org