Carnegie Mellon University
Software Engineering Institute

Insider Threat Vulnerability Assessment (ITVA)

Legal Capability Area

https://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM23-0882

Table of Contents

Introduction 1

Generic Clarifications 3

Capability Sequence # LG1.1: Insider Threat Policies 4

Capability Sequence # LG1.2: Insider Threat Checks & Balances 11

Capability Sequence # LG1.3: Acceptable Use Policies 16

Capability Sequence # LG1.4: Monitoring Policy 21

Capability Sequence # LG1.5: Insider Threat Information Sharing 25

Capability Sequence # LG1.6: Intellectual Property Ownership 32

Capability Sequence # LG1.7: Employee Conduct & Performance Policy 37

Capability Sequence # LG1.8: Employee Management During Organizational Restructuring 46

Capability Sequence # LG1.9: Employee Screening 50

Capability Sequence # LG1.10: Employee Onboarding 55

Capability Sequence # LG1.11: Separation of Employees 60

Capability Sequence # LG1.12: Employee Grievance Process 66

Introduction

The insider threat vulnerability assessment was developed by staff in the CERT® Division at the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University. The assessment, which is based on hundreds of actual insider threat cases, enables organizations to gain a better understanding of insider threat and an enhanced ability to assess and manage associated risks. The assessment was designed to be completed over a period of three weeks. Week one is the pre-assessment week, where assessment team members review organization-supplied documents to become familiar with organization practices and policies. During week two, the assessment team spends three to five days onsite at an organization. During that time, the assessment team reviews documents, interviews key personnel, and observes processes to substantiate each capability. During the final week, the assessment team prepares an insider threat vulnerability assessment final report, describing how prepared an organization is to prevent, detect, and respond to insider threats.

The legal department of an organization is essential to preventing, detecting, and responding to insider threats. This workbook helps assess the legal department's degree of active involvement in mitigating insider threat risk. The legal department is responsible for supporting other departments and enacting safeguards, including negotiating terms and conditions that permit the organization to monitor employees, to protect the organization from insider threat risks. This workbook does **not** help evaluate the legal sufficiency of policies, procedures, or agreements, eliminating organizational concerns that the assessment would affect attorney-client privilege and legal liability. The goal of this workbook is to encourage counsel to examine the organization's potential legal vulnerabilities to insider threat and employ best practices that effectively diminish insider threat risk.

The legal department must ensure that appropriate policy and procedures are in place that enable the organization to take legal and employment actions against insiders. For example, although the information technology department is responsible for logging, monitoring, and auditing employees' use of the organization's information systems and networks, the legal department, working with any privacy officers where appropriate, must verify that the relevant policies and procedures do not violate employee privacy rights.

A single legal point of contact will generally be unable to answer the capabilities in this workbook because oversight and compliance functions are often distributed throughout the organization. The decentralized nature of oversight functions can make determining the appropriate legal points of contact challenging for the assessment team. To ensure the assessment team can identify the appropriate, necessary legal points of contact, the assessment team should ask departments involved in this assessment, specifically human resources and information technology, to direct them to the units that provide their respective departments with legal support and oversight.

® CERT® is a registered mark owned by Carnegie Mellon University.

The assessment team should interview the units responsible for providing legal support to the human resources and information technology departments, but the team needs to recognize the diverse nature of the Office of General Counsel. Some legal issues may require departments to seek legal support outside of their assigned oversight units. The assessment team should also speak with the Officer of the Inspector General, the organization's auditing entity, and the legal unit responsible for advising the Chief Information Officer.

This *Legal* workbook focuses on three primary areas of concern:

- policy that supports organizational action to prevent, detect, and respond to insider threats
- monitoring and privacy
- periods of heightened insider risk within the organization

Capabilities 1.1 through 1.6 address compliance with policy that supports the prevention, detection, and response to insider threats. Capabilities 1.1 and 1.2 present general standards for policy and procedures, particularly those related to separation of duties and information sharing. Capabilities 1.3 through 1.7 concentrate on employee-related policy and procedures, including prohibited usage of systems and networks, protection of intellectual property, and management of employee conduct and performance. The policy and procedures discussed in these capabilities are crucial to taking disciplinary employment and legal actions.

Capability 1.8 is devoted to reorganization. During this period of heightened insider risk, the legal department should ensure that the organization takes adequate measures, including nondisclosure and intellectual property agreements, to protect its intellectual property, systems, and networks.

Capabilities 1.9, 1.10, and 1.11 focus on prescreening, onboarding, and termination, respectively. Because these events pose a heightened insider risk to the organization, the legal team should be involved in developing policy and practices to aid the organization in mitigating risks at these times.

Generic Clarifications

An insider is defined as any person who supports the organization, including contractors, subcontractors, and business partners.

All capabilities containing the phase ***"prevent, detect, and respond to"*** require that the organization can do all three: prevent insider threat incidents, detect incidents if they occur, and respond to incidents when they occur.

A ***policy*** is an administrative control commonly used as a prevention method. However, for an organization to achieve a capability involving a policy, the policy's existence is not sufficient on its own. The assessment team will be looking for the following attributes of a policy:

- documented
- communicated
- maintained
- routinely and consistently applied
- enforced
- monitored

Without defined policies and procedures, it can be difficult to discipline, terminate, or prosecute employees who engage in insider threat activity. To be effective, the policies and procedures must be consistently and routinely enforced.

Capability Sequence # LG1.1: Insider Threat Policies

The organization has a development and review process for policies and procedures that support the organization in preventing, detecting, and responding to insider threats.

Clarification/Intent

The organization should have a process for developing new policies and procedures that would support preventing, detecting, and responding to an insider threat. The organization should also have a process for periodically reviewing existing policies and procedures. Such policy should form the basis for employee screening, monitoring, discipline, termination, and legal action regarding insider activity.

Without defined insider threat policies and procedures, it can be difficult to discipline, terminate, or prosecute employees who engage in insider threat activity. To be effective, defined policy and procedures must be routinely and consistently enforced. In most cases, the organization must also communicate these policies to employees.

Assessment Team Guidance

The human resources department or the legal department generally maintains such policies and procedures.

Policies on employee screening, monitoring, and discipline (including legal actions) are examples of policies for preventing, detecting, and responding to insider threats, respectively.

MERIT Example

The insider had several decades of experience within the chemical industry and had spent time with multiple employers. While at the insider's latest company, the insider requested time off in alternating months in order to travel to the insider's native country and another foreign country to complete a charitable project. After several trips, management informed the insider that the trips were impacting the insider's work performance and requested that the insider focus more on company projects. A few weeks later, the insider indicated that they had secured employment as a consultant with a competitor in one of the foreign countries being visited and promptly resigned. This triggered an audit of the insider's company email account (per established company procedure) which revealed that the insider had been selling proprietary information belonging to a previous employer (and competitor of the current company) to another competitor in a foreign country. The management of the insider's soon to be former company contacted the management of the insider's former company to inform them that the insider had been selling their trade secrets to the foreign competitor. The victim organization performed their own investigation and determined that the information sold closely resembled their own proprietary recipes. They then passed the information on to the FBI. The insider was charged, pled guilty, and was fined and sentenced to time in prison.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has a documented process for developing and reviewing policies that support actions against insider threats.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a mechanism for communicating these policies to employees.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has policies with uniform compliance language that would allow the organization to enforce the policies and hold employees accountable.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has procedures that support policies for preventing, detecting or responding to an insider threat.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization designates an individual to continually verify that organizational actions with respect to insider threat are done in accordance with the organization's documented policies and procedures.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The procedures identify the triggers for creating new policies and procedures:

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ changes to the external operating environment

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ changes in the law

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ The organization regularly reviews policies even if procedures do not require it to do so.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The procedures define a regular review cycle for policies.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The procedures specify a minimum time (typically 3 years) and maximum time (such as 5 years) between policy reviews.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization periodically evaluates the effectiveness of and compliance with their insider threat policies.

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

Capability Sequence # LG1.2: Insider Threat Checks & Balances

The organization has policy that ensures that checks and balances, appropriate to preventing, detecting, and responding to insider threats to business-critical tasks, are implemented and enforced.

Clarification/Intent

The organization should have policy that requires it to identify business-critical tasks and mitigate risk of their disruption by separating duties and using internal controls.

Assessment Team Guidance

Separation of duties is one of the key concepts of internal control to support the prevention of fraud and insider threats. Approving, carrying out, and monitoring an action should each be conducted by separate entities or individuals.

Traditionally, identifying business-critical tasks and ensuring appropriate levels of checks and balances is a senior management function. The legal department may not have responsibility for this function. If not, request the identity of the senior manager responsible for this capability.

MERIT Example

The insider was employed as president and manager of the victim organization, a financial institution, for 17 years. For at least 15 years, the insider embezzled funds from the victim organization. As a function of her job, the insider had access to and could internally control loans and check writing. The insider misused this access to write multiple checks to herself, including checks written as “add-ons” to existing loans belonging to others without their knowledge or consent, checks posted as “share withdrawals” from other member accounts, and internal checks from other member’s accounts. To conceal the activity, the insider created fraudulent teller entries and also purposefully failed to post many of the checks written to herself to the organization’s records. The insider used multiple accounts to perpetrate the fraud, including the accounts of family members, a non-profit, and another organization. The insider was able to embezzle money from the non-profit account because she was a board member of the non-profit and had sole signatory authority at the financial institution. The insider refinanced her mother-in-law’s existing vehicle loan several times and kept the extra funds. The insider did this by making unauthorized advances for a new loan, which she then rolled into her mother-in-law’s existing loan. There were no loan documents to support any of the loans made or modified, only the canceled checks evidenced the loan advances. The incident was detected after the organization performed a forensic audit of its financial records, which revealed detailed spread sheets and bond claims that evidenced the insider’s illegal transactions. 1 month after the incident was discovered, the insider resigned, citing health problems. The U.S. Attorney’s Office declined to prosecute the insider, in lieu of local charges. However, local charges were never brought against the insider because she was gravely ill at the time. The insider admitted to defrauding her mother-in-law, but denied responsibility for the other fraudulent activities. The insider, who filed for bankruptcy after the incident, made an agreement with the financial institution to pay $355 a month toward the money stolen from the insider's mother-in-law, approximately $22,000.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has policy requiring that it identify business-critical tasks.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has policy requiring that it implement checks and balances for business-critical tasks.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization implements and enforces such policy.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ An individual is tasked with verifying that business-critical tasks are regularly reviewed for compliance with such policy.

Doc Rev _____

Dir Obs _____

Intvw _____

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

Capability Sequence # LG1.3: Acceptable Use Policies

The organization has policy for acceptable use of organization-owned networks and employee-owned devices used on organization-owned networks that allows the organization to effectively prevent, detect, and respond to usage violations.

Clarification/Intent

The organization has a policy describing the acceptable usage of organization-owned devices and networks as well as employee-owned and organization provisioned devices used on the organization's network that clearly defines what constitutes a violation of the policy as well as consequences for an infraction.

Assessment Team Guidance

Acceptable use policy should cover all organization-owned resources and employee-owned resources that may be connected to the organization's network. Employee-owned devices, such as cell phones and laptops, are part of a bring-your-own device policy.

The assessment team should be cautious when making recommendations about what to include in a social media policy. Policy that is too broad or vague may violate the National Labor Relations Board's standards, which require that employees must be able to discuss work conditions.

This capability focuses on the existence of a policy, which should be drafted, reviewed, and/or approved by General Council, and the enforcement of the policy (granting access, provisioning, and detection of unauthorized use) is a capability under the control of the Information Technology department.

MERIT Example

To Be Supplied

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev

Dir Obs

Intvw

Level 2

☐ The organization has an acceptable-use policy that considers

Doc Rev

Dir Obs

Intvw

- ☐ organization-owned devices

  Doc Rev

  Dir Obs

  Intvw

- ☐ employee-owned devices that may be connected to the organization's employer's network

  Doc Rev

  Dir Obs

  Intvw

☐ The organizational acceptable-use policy encompasses

Doc Rev

Dir Obs

Intvw

- ☐ work- and non-work-related use

  Doc Rev

  Dir Obs

  Intvw

☐ the transmission and receipt of confidential information

Doc Rev _____

Dir Obs _____

Intvw _____

☐ transmitting and receiving discriminatory, harassing, sexually oriented, offensive, or other illegal or improper messages[1]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ downloading unauthorized software onto an organization-owned system

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a social media policy that encompasses

Doc Rev _____

Dir Obs _____

Intvw _____

☐ employee use of social media on organization technology or during work time

Doc Rev _____

Dir Obs _____

Intvw _____

☐ employee respect of copyright and other IP laws

Doc Rev _____

Dir Obs _____

Intvw _____

☐ harassment of other employees

Doc Rev _____

Dir Obs _____

Intvw _____

[1] Smith, Shawn A. & Mazin, Rebecca A. *The HR Answer Book.* American Management Association, 2004.

☐ discrimination

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a social media policy that notifies employees that

Doc Rev _____

Dir Obs _____

Intvw _____

☐ posting anything known to be false about the employer, associates, or customers online is prohibited

Doc Rev _____

Dir Obs _____

Intvw _____

☐ employees are prohibited from representing any opinion or statement online on behalf of the employer

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has clearly defined consequences for violations of the acceptable use policy.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization addresses and handles any violations of the acceptable use policy.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization trains its staff about acceptable use of systems and networks.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization trains its staff about acceptable use of social media.

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected

Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

Capability Sequence # LG1.4: Monitoring Policy

The organization has policy and procedures that allow the organization to monitor employee actions on its systems and networks.

Clarification/Intent

Organizations should notify employees of any monitoring to lessen employees' expectations of privacy on the organization's systems and networks.

Targeted monitoring of individuals has implications for all organizations. Targeting specific employees may lead to allegations of violations of the Equal Employment Opportunity Act. Government employers are often subject to additional regulations and policy. Targeted monitoring policies should be documented and uniformly enforced.

Assessment Team Guidance

While linked to the acceptable use policy, monitoring policy and notifications are maintained separately by many organizations.

Courts may look to an organization's monitoring policy for several purposes, such as to determine whether to allow evidence, obtained through monitoring, of an insider crime or to defend an organization against privacy lawsuits brought by employees.

In addition, at least two states currently require notification of monitoring.

MERIT Example

To Be Supplied

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has documented policy that informs employees that the organization is logging, monitoring, and auditing employee actions on organization systems and networks.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has documented policy that requires employees to consent to logging, monitoring, and auditing.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented plan that describes when and how targeted monitoring of specific employees takes place. (This plan does not have to be distributed to all employees).

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The monitoring policy or procedure specifies how logging, monitoring, and auditing will be routinely and consistently conducted.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The policy indicates that communications will be monitored for content.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization trains appropriate personnel about the rules and boundaries of monitoring online behavior.

Doc Rev

Dir Obs

Intvw

☐ The organization has a web banner, appearing every time employees log on to organization systems or networks, that informs employees that their activity is being monitored.

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

Capability Sequence # LG1.5: Insider Threat Information Sharing

The organization has policy and processes for sharing information among departments when there are insider risk factors that can or do entail an employment action or legal liability for the organization.

Clarification/Intent

The organization has a process for sharing and considering information in the aggregate to improve the likelihood of identifying insider risk factors.

The organization's information-sharing policy should appropriately facilitate the sharing of information, including technical and behavioral precursors that may indicate potential insider threat activity.

The organization's information-sharing policy and procedures enable employees with an authorized purpose to access information in the performance of their duties.

The organization's information-sharing policy and procedures protect employee privacy and civil rights.

Assessment Team Guidance

Organizations often fail to connect vital information and evidence that, if shared and considered in the aggregate, could identify impending or present insider risks.

Due to additional regulations, organizations must be cautious when deciding whether to share information that could be considered confidential, such as criminal, credit, or medical history.

MERIT Example

The insider was employed by the victim organization, a manufacturer of electronic equipment. The insider had access to privileged information, including passwords. The insider used this information, and remote access, to fraudulently purchase a computer and other items, which were billed to the organization. The organization's accounting department detected the fraudulent purchases and used shipping records to connect the insider to the fraud. The insider wanted to use the fraudulently purchased items to for his financially failing side business. The insider was arrested, convicted, ordered to pay $700 restitution, and sentenced to one year of probation with 100 hours of community service. The insider had a history of poor performance and had been reprimanded on several occasions.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has documented policy and processes for sharing and aggregating risk information.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization notifies affected departments about terminations, new hires, and resignations.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has designated an individual to coordinate information sharing among departments.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has identified key individuals who need to share information.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has policy in place to protect the privacy of employee information, particularly information that could be considered confidential (i.e., health or criminal records).

Doc Rev

Dir Obs

Intvw

☐ The organization conducts a postmortem on insider threat discoveries to improve policies and processes.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The identified key individuals for information sharing meet on a regular basis.

Doc Rev

Dir Obs

Intvw

☐ The designated lead has created a formalized team.

Doc Rev

Dir Obs

Intvw

☐ The organization follows up on suggested improvements to policy and processes.

Doc Rev

Dir Obs

Intvw

☐ The organization periodically reviews the performance of the information sharing schema.

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

Capability Sequence # LG1.6: Intellectual Property Ownership

The organization has policy regarding ownership of the organization's intellectual property (IP) to reduce the likelihood of disputes and insider threats.

Clarification/Intent

Organization policy should indicate that employees have no ownership interest in any of the organization's IP and that employees who use the organization's IP inappropriately will be subject to discipline, termination, and legal action.

The policy should allow the organization to detect employees' attempts to steal, sell, market, or personally use business resources.

IP procedures should require appropriate marking, such as ownership and limited distribution instructions.

Assessment Team Guidance

To manage the ownership of IP effectively, organizations must have relevant policies that have been communicated to employees.

The organization may require employees to sign agreements that enable the organization to take legal action if the integrity of its IP is compromised.

MERIT Example

The insider was employed as a senior website developer and software engineer by the victim organization, which produced financial software. The organization relied heavily on its website to market its products. The insider was working on a computer operating framework that supported the victim organization's website. For four months, the insider discussed possible employment with a beneficiary organization, which marketed products online. The insider accepted a position with the beneficiary organization without notifying the victim organization. Shortly after, the insider stole the victim organization's trade secret and intellectual property–the computer operating framework he had been working on. The insider worked for both organizations simultaneously for at least 3 months. It is unclear how the insider stole the intellectual property, but the insider worked on site and remotely from home, providing great opportunity. The insider made a $35,000 profit by using the victim organization's intellectual property to develop websites for the beneficiary organization. The insider was arrested, convicted, and sentenced to 2 years of probation and $50,000 in restitution.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev

Dir Obs

Intvw

Level 2

☐ The organization has a policy which governs intellectual property ownership and use.

Doc Rev

Dir Obs

Intvw

☐ The organization requires relevant employees to sign

Doc Rev

Dir Obs

Intvw

- ☐ IP agreements

  Doc Rev

  Dir Obs

  Intvw

- ☐ nondisclosure agreements

  Doc Rev

  Dir Obs

  Intvw

- ☐ nonsolicitation of client and co-worker agreements

  Doc Rev

  Dir Obs

  Intvw

☐ noncompetition agreements

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization monitors e-mail content for illegal transfer of IP.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization provides a confidential mechanism for employees to report potential IP policy violations.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has detailed Controlled Information Management (CIM) policy and procedures that all employees follow when handling proprietary or sensitive information.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The CIM policy and procedures specify how documents should be marked to identify ownership and limited distribution.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization's CIM policy and procedures identify and track how sensitive information is received, created, accessed, used, modified, disclosed, stored, processed, or destroyed.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization's IP policy references applicable laws and penalties regarding theft of the organization's IP, including an employee's attempts to sell, market, or personally use business resources.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization's CIM policy and procedures identify all critical information on IT systems that may be harmful to the organization if divulged.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization verifies employee compliance with CIM policies.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization gives employees an opportunity to lodge IP ownership disputes.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization promptly and thoroughly investigates IP ownership disputes.

Doc Rev _____

Dir Obs _____

Intvw _____

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

Capability Sequence # LG1.7: Employee Conduct & Performance Policy

The organization has employee conduct and performance policy to support employment and/or legal actions that effectively prevent, detect, and respond to insider threats.

Clarification/Intent

The organization should have policy and procedures that define unacceptable employee conduct and performance and their consequences, including discipline, termination, and legal action.

The organization should also have policy and procedures for managing unacceptable employee conduct and performance.

The organization should have policy stating that employees engaging in behavior that harms the organization will be subject to discipline, termination, and legal action. Such policy and any supporting procedures should define the process for disciplinary actions, termination, or resignation.

In addition, the organization's policy should define an employee's obligation to report or otherwise deal with violations of its workplace behavioral rules, including online and interpersonal behavior, and extortion or other types of threats. The organization should also have policy for unacceptable conduct outside the workplace (such as felony and DUI convictions).

Assessment Team Guidance

To manage employee conduct and performance effectively, including preserving the right to take disciplinary and legal action, the organization must have relevant policies that have been communicated to employees.

MERIT Example

The insider was employed as a salesman by the victim organization, a manufacturer. The organization had a proprietary system to store customer data, including related leads and progress. The organization's salesmen were responsible for updating this information and typically devoted 6 hours a week to this task. The insider failed to sufficiently update customer data and was warned that he would be fired if he did not enter more detailed customer information. The insider failed to improve his performance and was penalized with a $2,500 salary deduction. The insider became disgruntled and sought employment with a competitor organization. The insider contacted a former colleague from the victim organization who currently worked for the competitor organization. (The victim organization also sued this employee for violating his employment agreement.) The insider informed the competitor organization that he planned to bring customer information with him if he was hired. The victim organization became suspicious of the insider. Consequently, the insider asked his contact at the beneficiary organization to delete all email correspondences; the insider's contact deleted the emails, but said he planned to tell the truth if he were ever subpoenaed. The insider received an offer from the competitor organization. Two weeks later, the insider accessed the victim organization's customer records and downloaded them to his home computer. The external connection failed to arouse suspicion by network administrators. Two days later, the insider sent an email to the victim organization, informing that he was resigning, effective immediately. The next day, the insider went to work for the beneficiary organization. The insider immediately began contacting customers from the victim organization and recruiting them for the beneficiary organization. Once the victim organization discovered the insider's actions, they notified law enforcement. Law enforcement examined the insider's computers and noticed that 60 MB of data had been deleted and that the computer had been defragmented several times. The victim organization filed civil suits against the insider and the beneficiary organization. The outcome of those civil suits is unknown.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has policies defining unacceptable behavior both in and out of the workplace.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization communicates what is or is not acceptable behavior in the workplace.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization requires employees and contractors to sign a code of ethics.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a policy in place that identifies actions that can result in employee termination.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has policy that defines an employee's obligation to report or otherwise deal with violations of workplace behavioral rules, including extortion and other types of threats.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization ensures that supervisors conduct effective performance reviews that are kept on file.

Doc Rev

Dir Obs

Intvw

☐ The organization ensures that performance issues are communicated to employees.

Doc Rev

Dir Obs

Intvw

☐ The organization assigns responsibility to an organizational unit, such as human resources, to advise and assist units with performance management activities.

Doc Rev

Dir Obs

Intvw

☐ The organization develops appropriate level of documentation to support taking disciplinary action if desired.

Doc Rev

Dir Obs

Intvw

☐ The organization has a documented procedure for developing performance improvement plans and periodically assesses, discusses, and documents employee progress.

Doc Rev

Dir Obs

Intvw

☐ The organization provides employee assistance programs.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization has clearly defined consequences for violations of its unacceptable employee behavior policy.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has appropriate procedures in place to ensure that appropriate documentation is developed to support taking disciplinary action if desired.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a procedure for documenting unacceptable conduct and indicators of poor performance.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has conflict-of-interest and conflict-of-commitment policies and procedures.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization requires employees to submit for review potential conflicts of interest and conflicts of commitment.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a process for reviewing and approving (or disapproving) conflicts of interest and conflicts of commitments.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization provides a confidential mechanism for employees to report potential violations of unacceptable conduct policy.

Doc Rev

Dir Obs

Intvw

☐ The organization ensures confidentiality to those participating in employee assistance programs.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization trains supervisors to refer employees to employee assistance programs.

Doc Rev

Dir Obs

Intvw

☐ The organization trains employees to recognize and report a coworker's unacceptable conduct and performance.

Doc Rev

Dir Obs

Intvw

☐ The organization promotes employee assistance programs.

Doc Rev

Dir Obs

Intvw

☐ The organization provides supervisors sample scripts referring employees to employee assistance programs, to avoid protected class assertions.

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

Capability Sequence # LG1.8: Employee Management During Organizational Restructuring

The organization has policy for managing employees during major organizational restructuring to minimize disruption, support employment actions, and reduce the likelihood of insider threat activity.

Clarification/Intent

The organization should have policy and procedures for minimizing employee disruption and dissatisfaction during the restructuring process. Such policy should also allow the restructuring team to assess information security and vulnerability risks and threats

Assessment Team Guidance

To effectively manage any major organizational restructuring, the organization should have policy and procedures to minimize disruption and preserve its right to take disciplinary and legal action.

Organizational restructuring activities include mergers, acquisitions, large reductions in force and outsourcing. The organization being taken over or eliminated is even more likely to disgruntle employees.

MERIT Example

The insider was employed as a cell development technologist by the victim organization, a battery manufacturer. Over a 3 month period, while on site and during work hours, the insider copied, downloaded, and emailed research to his computer and also physically carried information from the organization's offices. The insider sent the information, in 3 mailings on 2 separate occasions, to 2 of the victim organization's competitors. Both competitors returned the information they received to the victim organization. The insider's motivation was anger directed toward the victim organization. The insider was enraged because, when lower level employees were receiving meager raises or being laid off, executives were receiving what the insider regarded as exorbitant executive bonuses and compensation. The insider was arrested, convicted, fined $7,500, and sentenced to 5 years probation with 200 hours of community service. The victim organization estimated the incident related loss at $3 million.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has policy that ensures that new employees hired as part of a merger, acquisition, or outsourcing have signed the relevant agreements, including

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ IP ownership agreements

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ nondisclosure agreements

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ nonsolicitation-of-employees agreements

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ nonsolicitation-of-client agreements

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ noncompetition agreements

Doc Rev _____

Dir Obs _____

Intvw _____

☐ a code of ethics

Doc Rev _____

Dir Obs _____

Intvw _____

☐ acceptable use policy

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a communication plan for informing staff of changes such as major internal restructuring, layoffs, mergers, acquisitions, and group resignations.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization's communication plan has a mechanism for employees to voice their concerns during such major organizational changes.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has an employee outplacement service during the change process.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization reviews all third-party contracts of the acquired or merging organization to ensure no lapses of security occur during the change process.

Doc Rev

Dir Obs

Intvw

☐ The organization has a change management expert to ensure policy and procedures are in place and to minimize employee disruption and dissatisfaction during the change process.

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected

Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

Capability Sequence # LG1.9: Employee Screening

The organization has policy and procedures that support the organization in the candidate and employee screening process.

Clarification/Intent

The organization should document and consistently enforce screening policy and procedures to protect candidates' and employees' rights, thereby protecting the organization from liability.

Assessment Team Guidance

Criminal background screenings can be tricky for some employers: at least two states now at least partially prohibit initially asking candidates about their criminal history. In addition, all employers must comply with equal employment law. The Equal Employment Opportunity Commission has produced guidance about criminal background screenings to help employers avoid violations in this area, generally suggesting that employers avoid prohibiting anyone with a criminal history from being considered as a candidate.

MERIT Example

The insider was employed as a bookkeeper by the victim organization, a restaurant. Over a 25 month period, the insider wrote 75 checks from the organization's account to pay for her personal expenses. The insider also obtained a credit card in the organization's name. To conceal her actions, the insider used her privileged access to alter the organization's computer accounting records to show a different payee. The insider embezzled $175,000 from the organization. The insider's activity was detected when a manager at the victim organization noticed irregularities in the electronic check ledger. The insider was terminated. The insider was arrested, convicted, ordered to pay $20,000 restitution, and sentenced to 15-months imprisonment followed by 3 years of supervised release. The insider was also referred to a mental health program. 6 years prior to this incident, the insider was convicted of a similar fraud. The insider used the stolen money to purchase expensive collectible dolls.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization requires candidates to consent to criminal and financial background screenings during hiring and after hire to detect any criminal activity.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has hiring policy that differentiates between arrest and conviction records when making employment decisions.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has documented policies for keeping candidates' information confidential during the hiring process.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization considers the business justification of background screening for each position.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ If a candidate does have a criminal history, the organization considers individual circumstances (i.e., nature of the crime, how long ago the crime occurred, and the nature of the job).

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization conducts periodic or event-driven background reviews that follow the targeted practices in Level 2.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Relevant staff are trained how to comply with employment laws relevant to the hiring process.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization verifies its compliance with candidate and employee screening processes and addresses noncompliance.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has documented procedures for keeping candidates' information confidential during the hiring process.

Doc Rev _____

Dir Obs _____

Intvw _____

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

Capability Sequence # LG1.10: Employee Onboarding

The organization has policy and procedures that support employee onboarding.

Clarification/Intent

Employees should know what to expect of the organization and what the organization expects of them prior to their start date. Setting employee expectations is one way to mitigate disgruntlement, which is a motivator for insider crimes. Setting of these expectations usually occurs during the onboarding process. This process is usually handled by Human Resources or a specific training group.

Legal's involvement should be in ensuring there are appropriate policies and/or procedures in place to ensure the onboarding occurs in a standardized fashion for each employee and that the appropriate steps, training, or document signing occurs before the employee starts their actual work.

Procedures should outline which documents or agreements must be signed prior to the employee's start date and which ones should be signed during the onboarding process.

Assessment Team Guidance

Onboarding is covered as a capability in the HR workbook. It is capability 1.10 and states: *The organization has an employee onboarding process to inform new hires of the organization's policy, procedures, values, and culture and establish expectations.* The focus of this capability within the Legal workbook is to ensure that the onboarding process has supporting policies and procedures that have been reviewed by Legal and are institutionalized to ensure consistency.

The assessment team should look for a policy that requires a standardized onboarding for all employees and trusted business partners. It is possible that specific roles and responsibilities will require additional special onboarding.

MERIT Example

The insider was employed as a computer engineer by a trusted business partner (TBP) organization, an IT company that managed computer systems for a foreign government, the victim organization. One month prior to the incident, the insider resigned from the TBP. In his resignation letter, the insider expressed that he felt "'isolated' and 'stressed' due to his physical segregation from the rest of his team." The insider also stated that he felt he was inappropriately disciplined for the team's mistakes because he was new to the team. The incident occurred after the insider's fiancée broke off their engagement and the insider proceeded to get intoxicated. At the time, the insider was living with a former colleague, who was still employed by the TBP organization. The insider used his colleague's work computer and credentials to open a VPN connection. The insider crashed multiple government servers and deleted 11,000 accounts for government employees at those victim organizations. The incident related impact was $1.2 million. The insider was arrested, convicted, and sentenced to 3 years imprisonment. The insider claimed he was trying to expose security vulnerabilities in the government's IT systems.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has a policy that all employees and trusted business partners complete the required onboarding process.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has identified which employment agreements and requirements must be met prior to an employee's start date and which must be meet during the onboarding process.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has procedures which define the process for onboarding for all employees and trusted business partners.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has an individual designated to verify that all employment agreements and requirements are met prior to the employee's start date and to address noncompliance.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization tailors onboarding to the level of the employee's position, including tailoring any relevant employment agreements.

Doc Rev

Dir Obs

Intvw

☐ The organization verifies that onboarding activities are performed according to the policy and procedures and addresses noncompliance.

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

Capability Sequence # LG1.11: Separation of Employees

The organization has policy and procedures that facilitate preventing, detecting, and responding to insider threats when an employee is leaving the organization.

Clarification/Intent

Whether an employee is separating from the organization voluntarily or not, there should be policies and procedures in place to ensure that employees do not harm the organization during or after the separation process. Mechanisms, controls, and processes should be in place to remind the employee of their obligations regarding IP agreements, non-disclosures, and non-compete agreements. Controls can also involve increased user monitoring.

The scope of this capability is for both employees and trusted business partners. The scope also includes voluntary separation or organizational directed termination.

Assessment Team Guidance

Employee termination or resignation poses increased risk to the organization. Cases in the CERT insider threat database show that such events have led to disgruntlement and sabotage. Other cases also indicate a heightened risk of theft of IP during this time.

MERIT Example

The insider was formerly employed as a support person in the IT department of the victim organization, a casino. Two weeks after leaving the organization, over a 6 day period, the insider remotely accessed the victim organization's systems via VPN from his residence. The insider used a former colleague's credentials to access the organization's sever that controlled the casino players' club cards. Club cards stored players' slot usage for rewards and comps. During the incident, players were unable to access their rewards and comps, and the casino was unable to track existing club cards or to issue new cards. After a search warrant was executed at the insider's home, police discovered a hard drive containing the organization's employee's usernames and passwords. The insider was arrested and purportedly admitted that he accessed the casino's private network with the employee information stored on the hard drive. The insider was convicted, ordered to pay $5,000 restitution, and sentenced to 1 year of house arrest followed by 2 years of probation. The insider perpetrated the attack because he was unhappy with how he left his job.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ There is a policy in place that defines the type of actions that can be taken when an employee or trusted business partner separates from the organization so that organizational assets and services are protected.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization protects the privacy and civil liberties of the separating employee.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has procedures that define a process for employee separation, including but not limited to having

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ the legal department send a warning letter reminding the employee of continuing obligations pursuant to signed agreements

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ the legal department take immediate action to contain actual or potential damage inflicted by competitors or conspirators, such as copying them on the warning letter to the employee

Doc Rev

Dir Obs

Intvw

☐ requiring an HR representative to accompany employees from their termination notice through their escort out of the building

Doc Rev

Dir Obs

Intvw

☐ terminating all IT system access accounts such as e-mail and databases

Doc Rev

Dir Obs

Intvw

☐ collecting physical assets such as laptops, thumb drives, PDAs, and mobile phones

Doc Rev

Dir Obs

Intvw

☐ disabling access to the organization's system from employee owned devices

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization trains relevant staff to carry out practices related to the exit process.

Doc Rev

Dir Obs

Intvw

☐ The organization periodically audits their exit process to ensure any new requirements are addressed.

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	
Notes (from documentation, observations, and interviews)					

Capability Sequence # LG1.12: Employee Grievance Process

The organization has policy and procedures that establish an employee grievance process.

Clarification/Intent

The organization should establish a documented employee grievance process, including how employees initiate a grievance as well as the investigation and remediation process.

Assessment Team Guidance

The CERT insider threat database contains cases where unaddressed grievances have led to disgruntled employees. Disgruntlement is a motivation for insider crimes.

MERIT Example

The insider was employed as a systems administrator by the victim organization, a financial services firm. The organization announced to employees that bonuses would be half of what they normally were. The insider had complained about the lower bonus to his supervisor. The insider responded to this news by building and distributing a logic bomb on the organization's Unix-based network, which took down nearly 2000 servers in the head office and 370 servers at branch offices around the country. Prior to the logic bomb's detonation, the insider purchased put options on the company, expecting the subsequent detonation of the logic bomb to drive the firm's stock price lower. The insider quit when the organization became suspicious of him. Although the stock price did not drop, the logic bomb cost the victim organization $3.1 million in repairs and caused mass chaos that the firm never fully recovered from. A forensics investigation connected the insider to the incident through VPN, access, and code snippets between his home computer and the organization's network. The insider was arrested, convicted, and sentenced to 97 months imprisonment.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev

Dir Obs

Intvw

Level 2

☐ The organization has documented policy that enables employees to file formal grievance reports.

Doc Rev

Dir Obs

Intvw

☐ The organization has a confidential mechanism in place that enables employees to file formal grievance reports.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization ensures the privacy of employees who file a grievance, ensuring they are not targeted for additional monitoring or employee actions based on their grievance.

Doc Rev

Dir Obs

Intvw

☐ The organization ensures that it promptly and thoroughly investigates grievances.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization trains supervisors in how to handle employee grievances and how to refer employees to the grievance policy and process.

Doc Rev

Dir Obs

Intvw

☐ The organization tracks grievances, including their number, cost, cause, and time taken to remediate.

Doc Rev

Dir Obs

Intvw

☐ The organization periodically evaluates the effectiveness of their grievance-filing system.

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)