Carnegie Mellon University
Software Engineering Institute

Insider Threat Vulnerability Assessment (ITVA)

Human Resources 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

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 ITVA assesses organizational capabilities across seven workbook areas: Human Resource, Data Owners, IT, Legal, Physical Security, Software Engineering, and Trusted Business Partners.

The assessment was designed to be completed over a period of six to eight weeks. The initial weeks are spent on planning and pre-assessment work. The week before the on-site assessment is the pre-assessment week, where assessment team members review organization-supplied documents to become familiar with organization practices and policies. During the on-site week, the assessment team spends three to five days at an organization. During that time, the assessment team reviews additional documents, interviews key personnel, and observes processes to substantiate each assessment capability. During the final weeks, 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.

This workbook has not been separated to address public and private sectors. Rather, it captures information in a way that accommodates the different regulatory regimes that often apply to the public and private sectors (and even among different private sectors). However, the assessment team should also be cognizant of any additional regulations that apply to particular industries (e.g., financial or health care sectors), which may subject a subset of employees to additional scrutiny throughout the employment lifecycle. Government employees, particularly those who have security clearances, may also be subject to additional scrutiny. The assessment team must keep these employee differences in mind when applying the capabilities and indicators presented in this workbook.

The chart below highlights the capabilities for which the assessment team needs to be the most cautious and provides recommendations based on the organization's score. The Assessment Team Guidance for these capabilities also highlights some of the regulations that the assessment team needs to be aware of to understand the organization's possible operational constraints.

Human Resource Capability	**Common practice**	**Caution: major differences exist by**	**Additional scrutiny likely applies to**	**Comments**
1.1 Job History Confirmation	x		x	While this is a common practice, employees under greater scrutiny will likely have to supply a longer address history and more information about employment.

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

Human Resource Capability	Common practice	Caution: major differences exist by	Additional scrutiny likely applies to	Comments
1.2 Interview Professional References	x		x	Level 4 may be more applicable to positions of additional scrutiny, such as candidates in the security clearance process.
1.3 Interview Personal References	x		x	Level 4, interviewing additional personal references, may be more applicable to positions of additional scrutiny, such as candidates in the security clearance process.
1.4 Candidate Criminal History	x		x	While criminal history screenings are recommended for all job candidates, the law generally allows organizations to put greater scrutiny on candidates for positions of trust.
1.5 Candidate Civil Litigation & Judgments	x		x	While civil litigation history screenings are recommended for all job candidates, the law generally allows organizations to put greater scrutiny on candidates for positions of trust.
1.6 Candidate Credit History	x		x	While credit rating screenings are recommended for all job candidates, the law generally allows organizations to apply greater scrutiny to candidates for positions of trust.
1.7 Candidate Medical Testing		x		The Department of Health and Human Services has published guidance for executive branch agencies on which positions random drug testing should be required for or disallowed.
1.8 Candidate Behavioral Interview	x			
1.9 Candidate Psychological Testing		x	x	Psychological testing may be considered medical testing under the Americans with Disabilities Act, which would require the organization to show that the relevant job requirement is job-related and consistent with business necessity. Positions of trust are more likely to fall within this definition. Also, polygraphs, another part of the capability, are highly regulated and often used only in specific industries or during employee investigations.
1.10 Onboarding Process	x			

Human Resource Capability	Common practice	Caution: major differences exist by	Additional scrutiny likely applies to	Comments
1.11 Increased Monitoring During Probationary Period	x			
1.12 Policies for Workplace Behaviors	x			
1.13 Employee Obligation to Report Behavioral Violations		x		It is mandatory for many government employees to report fraud, waste, and abuse.
1.14 Follow-Up of Employee Violations	x			
1.15 Investigation Results Usage	x			
1.16 Sharing of Policy Violation Information	x			
1.17 Monitor, Log, Audit Policy	x			
1.18 Targeted Monitoring Policy		x		Government employers may have to open an inquiry or investigation prior to targeted monitoring.
1.19 IP Policy	x			
1.20 Facility & Employee Physical Security	x			
1.21 Good-Conduct Policy	x			
1.22 Employee Benefits & Compensation	x			
1.23 Employee Assistance Programs	x			

Human Resource Capability	Common practice	Caution: major differences exist by	Additional scrutiny likely applies to	Comments
1.24 Insider Threat Security Awareness Training	x			
1.25 Rewarding Employees for Good Behaviors	x			
1.26 Identifying High-Risk Employees	x			
1.27 Notification of Employee Status Change	x			
1.28 Insider Threat Risk Evaluation Teams		x		The government sector is less likely to have merger and acquisition policies, so assessors should focus on reorganizations, layoffs, and termination policies.
1.29 Employee Screening Updates	x		x	Organizations should update their screening tools for all employees, but some employees in positions of trust may require more specific updates based on policy or regulations.
1.30 Insider Threat Incident Review	x			

Policies and other evidence necessary for a full assessment of human resources capabilities may be distributed throughout the organization. The assessment team may want to ask the organization to send the following policy and pieces of evidence prior to their onsite visit:

- acceptable use of IT resources policy
- monitoring policy for IT resources
- monitoring policy for physical spaces (i.e., video, badging, etc.)
- bring-your-own-device policy
- intellectual property policy
- social media policy
- conflict of interest and commitment policy and review procedures
- candidate screening policy
- controlled-information management policy
- employee reporting policy
- good conduct policy
- drug testing policy

- employee grievance policy
- employee performance policy
- employee resignation policy
- employee separation from employment policy
- employee handbook and code of ethics
- benefits and compensation policy
- onboarding policy
- targeted monitoring policy
- human resource merger and acquisition policy

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 # HR1.1: Job History Confirmation

The organization confirms the identities as well as personal and professional histories of job candidates.

Clarification/Intent

The organization needs to confirm that candidates for positions of concern are who they claim to be. Candidates might be hiding their identities or background to gain access to the organization for hostile motives involving fraud, espionage, sabotage, or other insider risks. Even candidates without such motives might lie about their background, qualifications, or histories to hide past problems or exaggerate their qualifications. Such individuals can place the organization at risk. In addition, the address information obtained in this capability can then be used in determining where to perform a criminal background screening as set out in HR 1.4.

Assessment Team Guidance

Candidates for "positions of concern" will most likely be identified and defined by the organization. However, what we mean by this term is positions with greater responsibility and access to key data and critical assets; staff who have privileged access; or staff who can make changes to proprietary data, such as software or IP.

The assessment team should verify that the organization confirms a candidate's identity.

MERIT Example

The insider, a foreign national, was employed as programmer by the victim organization, a Department of Motor Vehicles (DMV). Originally, the insider was working on an e-Development system for the victim organization. The insider was granted a family leave to purportedly seek medical care for his ailing father. Upon his return, the insider was re-assigned to another project. The insider began working exclusively from home, via remote access. 3 months after his reassignment, the insider remotely accessed the e-Development project. For 12 days, outside of work hours, the insider remotely logged in, undetected, and downloaded data from the e-Development project. After an IT security employee detected the insider's presence on the e-Development system, the insider attempted to download files from the organization's database and conceal his activity. The insider's access to the e-Development project was subsequently terminated. Six days after his access was terminated, the insider logged into the e-Development system from 2 different IP addresses. The insider was arrested after a search of his home revealed unusual data storage on his home computer. The next day, the insider's employment was terminated. The insider was connected to the incident through remote access logs and logs from the insider's ISP. The insider was arrested and convicted, but sentencing information was unavailable. The insider did not go through a background check before hiring. The insider had falsely claimed to be a U.S. citizen for over 2 years, lied about being a U.S. citizen on pilot's license applications, and previously filed a lawsuit against a government entity, which he claimed had interfered with his attempt to gain U.S. citizenship.

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 confirms candidate's name and Social Security number.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization confirms candidate's date and location of birth.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization confirms candidate's employment history for the last 5–6 years.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization confirms candidate's educational history.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization confirms candidate's certifications, licenses, or other specialized training.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization confirms candidate's address history for the last 5–6 years.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization confirms candidate's identity, qualifications, history, and trustworthiness while protecting the candidate's privacy by seeking only information relevant to the position.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ A standardized process is in place to confirm the identities as well as personal and professional histories of job candidates.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Staff are assigned the job responsibility for performing confirmation activities.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization confirms candidate's employment history for the last 7–9 years.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization confirms candidate's address history for the last 7–9 years.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Staff responsible for background checks and screenings are properly trained how to confirm the identities as well as personal and professional histories of job candidates.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Documented procedures or guidance exists detailing how the confirmation process should be executed; including handling exceptions.

Doc Rev

Dir Obs

Intvw

☐ The organization confirms candidate's employment history for the last 10 or more years.

Doc Rev

Dir Obs

Intvw

☐ The organization confirms candidate's address history for the last 10 or more years.

Doc Rev

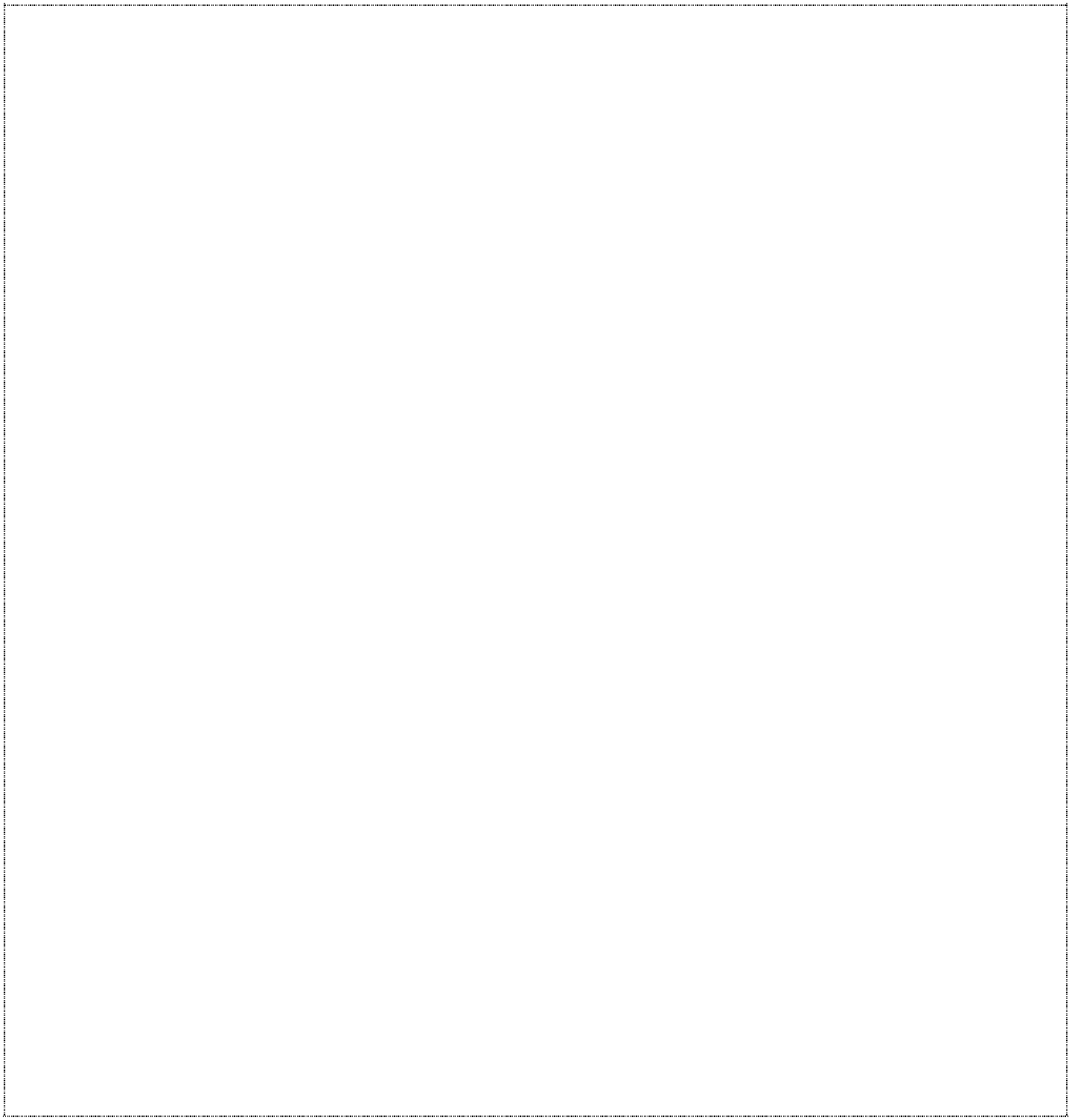
Dir Obs

Intvw

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

Justification

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



Capability Sequence # HR1.2: Interview Professional References

The organization interviews the professional references of job candidates.

Clarification/Intent

An important step in confirming the identity, qualifications, professional history, and trustworthiness of job candidates is interviewing their professional references. In addition, the organization should use these interviews to generate additional professional references not supplied by the candidate. A request for references might also deter potentially concerning candidates from applying to the organization.

Assessment Team Guidance

Previous studies have shown that insiders who acted against their employer had sometimes committed the same or similar offenses against previous employers or had significant problems with them. Candidates might not report these issues themselves, or they might count on their former employers to refrain from reporting them.

MERIT Example

The insider was originally employed as a system administrator by the victim organization, a telecommunications company. The insider resigned without providing any advance notice to the organization. The insider refused to provide the system administrator passwords to the organization until he received payment for his last two days of work. The insider used remote access, during working hours, to attack the organization's network for a month. The insider remotely accessed the organization's key files and email. The insider also modified systems to prevent the organization from performing administrative functions. Two days later, the insider remotely accessed the DNS server and changed the name resolution settings to point to a malicious DNS name. The next day, the organization finally received passwords from the insider and promptly changed them for all administrative functions. Several days later, the organization contacted law enforcement for assistance. The insider ran several attacks in the next few days, including running a sniffer on the network for several hours, running port scans from the organization's systems, downloading internal files to his home computer. The insider also used the organization's systems to scan government systems. While on the company network, the insider, who was associated with the internet underground, chatted with other hackers, bragged about the damage he could inflict on the organization, and claimed that he installed an EEPROM password on the organization's systems. The insider had a history of psychological and psychiatric problems. The insider also had an extensive criminal history, including burglary, theft, credit card fraud, and weapons violations. A search of the insider's home revealed bomb making materials, terrorist manuals, and child pornography stored on his home computer. The insider was arrested, convicted, ordered to pay a $3,000 fine, and sentenced to 2 years supervised probation. Three years later, the insider committed another act of insider sabotage against a different former employer.

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 interviews professional references to confirm candidate's identity, qualifications, history, and trustworthiness, including interviews with at least two to three candidate-supplied professional references.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization confirms candidate's identity, qualifications, professional history, and trustworthiness while protecting the candidate's privacy by seeking only information relevant to the position.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ A standardized process is in place for performing professional reference checks.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization interviews professional references to confirm candidate's identity, qualifications, history, and trustworthiness, including interviews with at least three additional professional references generated by candidate-supplied references.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Documented procedures or guidance exists detailing how professional reference checks should be executed.

Doc Rev

Dir Obs

Intvw

☐ Staff performing professional reference checks have received organizational training or guidance on how to execute such functions.

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 # HR1.3: Interview Personal References

The organization interviews the personal references of job candidates.

Clarification/Intent

An additional step in confirming the identity, qualifications, personal and professional history, and trustworthiness of job candidates is interviewing their personal references. In addition, the organization should use these interviews to generate additional personal references not supplied by the candidate. The organization should also review a candidate's social networking records for concerning contacts or activities. A request for references might also deter potentially concerning candidates from applying to the organization.

Assessment Team Guidance

Previous studies have shown that insiders who acted against their employer had sometimes committed the same or similar offenses against previous employers or had significant problems with others. Candidates might not report these issues themselves, or they might count on their personal references to refrain from reporting them.

The assessment team should look for evidence that personal references and social media use by the candidate are checked as part of the hiring process.

MERIT Example

The insider was employed as a language specialist by the victim organization, a law enforcement agency. Over 2 years and 4 months, the insider accessed the organization's computer on 6 occasions for the purpose of private financial gain. Presumably, the insider accessed a sensitive law enforcement database. Additional details regarding the unauthorized access were unavailable. The insider also lied to authorities regarding other employment, debt, providing confidential information to unauthorized individuals, and the insider's association with a convicted felon. Over a 4 month period, the insider also resold stolen mobile phones for $1,000. The insider possessed child pornography on his home computer. The insider was arrested, convicted, and sentenced to 60 months imprisonment followed by 3 years of supervised release.

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 confirms candidate's identity, qualifications, history, and trustworthiness by interviewing at least two to three candidate-supplied personal references.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization confirms candidate's identity, qualifications, history, and trustworthiness while protecting the candidate's privacy by seeking only information relevant to the position.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization confirms candidate's identity, qualifications, history, and trustworthiness by reviewing candidate's participation on social networking sites, including the type and function of site, regular site contacts, and participants.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization confirms candidate's identity, qualifications, history, and trustworthiness by interviewing at least three additional personal references generated by candidate-supplied references.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Documented procedures or guidance exists detailing how personnel reference checks should be executed.

Doc Rev

Dir Obs

Intvw

☐ Documented procedures or guidance exists detailing how social media checks should be executed.

Doc Rev

Dir Obs

Intvw

☐ Staff performing personnel reference checks and social media checks have received organizational training or guidance on how to execute such functions.

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 # HR1.4: Candidate Criminal History

The organization screens job candidates for a criminal history.

Clarification/Intent

The organization should review a candidate's criminal history to ensure the organization is aware of potential risks.

Assessment Team Guidance

According to previous CERT insider threat studies, many organizations were unaware of previous criminal acts committed by their malicious insiders.

The U.S. Equal Employment Opportunity Commission (EEOC) has published guidance on criminal background screenings. Ensuring compliance with these best practices is part of the Legal workbook, in LG1.9: Employee Screening. The Federal Credit Reporting Act also imposes restrictions on employers who obtain criminal history reports as part of a consumer report, including notice and consent requirements.

Several states and cities have also instituted so-called "ban the box" laws, which typically prohibit the organization from asking for the criminal history of job candidates until a specific time in the hiring process (e.g., after the first interview).

The assessment team should note that many of the indicators in this capability are also included in LG1.9 in the Legal Workbook. This ensures these questions are asked to both HR and Legal relevant stakeholders.

MERIT Example

The insider was employed as a sales associate by the victim organization, a financial institution. The insider worked at the victim organization's call center and was responsible for changing accounts or ordering new credit cards. For approximately a year, while on site and during work hours, the insider printed screen captures of customer data, including social security numbers (SSNs) and account numbers. The insider sold 300 accounts to an outsider for approximately $1,000 - $1,500. The insider also telephoned the outsider with information. The insider's activity was detected when consumers reported the fraudulent charges and an investigation connected the insider to the fraud. The insider was arrested and convicted, but sentencing information was unavailable. The victim organization's incident related loss was $200,000. The insider associated with criminals, specifically counterfeiters, and had a prior criminal history. The organization had no acceptable usage policy and did not perform background checks.

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 runs a criminal record screening for job candidates.

Doc Rev _____

Dir Obs _____

Intvw _____

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

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 _____

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

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ A standardized process is in place for performing criminal history reviews.

Doc Rev

Dir Obs

Intvw

Level 4

☐ Documented procedures or guidance exists detailing how criminal history reviews should be executed.

Doc Rev

Dir Obs

Intvw

☐ Staff performing criminal history reviews have received organizational training or guidance on how to execute such functions.

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 # HR1.5: Candidate Civil Litigation & Judgments

The organization screens job candidates for a history of civil litigation and judgments.

Clarification/Intent

The organization needs to determine if job candidates have a history of

- rule violations that have resulted in legal actions against them
- personal conflicts that have led to legal actions, including those initiated by the candidates

Legal actions of concern might include protection orders, injunctions, financial suits, certain aspects of divorce cases, bankruptcies, or other civil actions that raise concern about a candidate's decision-making abilities or interpersonal behavior. Such behaviors might be predictive of future violations.

Assessment Team Guidance

A selection of insiders from past research had a history of civil actions against them that should have raised concerns about their trustworthiness. Those actions included injunctions against the use of intellectual property (IP) from a previous employer, foreclosures, and protection orders.

The Fair Credit Reporting Act generally prohibits consumer reports containing lawsuits and judgments that are more than 7 years old.

MERIT Example

The insider was employed as a senior database analyst by the victim organization, a financial institution. For over 5 years, the insider and a co-conspirator systematically downloaded over 8.4 million consumer records, including bank account information for over 5.6 million consumers and credit/debit account information for over 1.4 million consumers. Downloads took place during on-site, presumably during work hours. To avoid detection, the insider removed the data using physical processes. The insider was one of only five employees who had access to the data. The organization created a company as a front to sell the stolen data to a broker for $580,000. The data broker re-sold the information to 7 marketing companies. The theft was discovered when several of the victim organization's customers reported a correlation between check transactions and an influx of telephone and mailed marketing solicitations. To track down the data source, authorities contacted the marketing firms, who were unaware that the data was stolen. The firms identified the insider's company as the source of the data. The insider was terminated the week after the theft was discovered. The insider was subsequently arrested, convicted, ordered to pay $3.2 restitution, and sentenced to 57 months imprisonment. The victim organization successfully obtained an injunction to bar the marketing firms from using the information, and with the cooperation of those firms, the organization managed to recover most of the stolen data. A judge also granted an order permitting the seizure of the insider's data storage devices, office and home computers. The organization maintained that there was no evidence that the stolen information was used for other than marketing purposes, but some affected consumers alleged that they were victims of identity theft. The organization spent a minimum of $5 million in settlement fees related to the data theft, not including attorney's fees. Although the victim organization had been acquired by another organization, this was not a motivating factor for the insider because the purchase occurred only a year before the discovery of the 5 year theft. The insider had a history of financial problems, including bankruptcy and liens. The insider also had been previously arrested for petty theft and driving under the influence (DUI).

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 runs civil record screenings for job candidates.

Doc Rev

Dir Obs

Intvw

Level 3

☐ A standardized process is in place for performing civil record screenings for job candidates.

Doc Rev

Dir Obs

Intvw

Level 4

☐ Documented procedures or guidance exists detailing how civil record screenings for job candidates should be executed.

Doc Rev

Dir Obs

Intvw

☐ Staff performing civil record screenings have received organizational training or guidance on how to execute such functions.

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 # HR1.6: Candidate Credit History

The organization screens the credit rating and history of job candidates.

Clarification/Intent

The organization should screen the credit rating and history of job candidates to determine whether they are under unusual financial stress that might increase their vulnerability to outside coercion or indicate problems with judgment or self-control.

Assessment Team Guidance

Financial stress among insiders has been linked to incidents of fraud, IP theft, and espionage.

Several states have regulations limiting the use of credit checks in employment decisions.

Under the Fair Credit Reporting Act, generally a consumer report cannot include

- bankruptcies more than 10 years old
- other information related to credit more than 7 years old, such as accounts placed for collection, paid tax liens, and judgments

It is possible that some organizations may outsource such screening activities. If so, it may be difficult to determine what processes are in place. If the assessment team can easily identify the processes they should try to include them for review in this assessment.

MERIT Example

A financial analyst and 2 accomplices were employed by a developer of enterprise networking hardware. They were disgruntled with their perceived low pay in comparison to the organization's executives. The insiders questioned co-workers about vulnerabilities in the stock disbursement system. Two of the insiders exploited vulnerabilities in the system to issue fraudulent disbursement orders valued at over $4 million to their personal accounts, some of which went to pay off prior debts as well as cars and jewelry.

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 screens job candidate's credit history.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ A standardized process is in place for performing civil record screenings for job candidates.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Documented procedures or guidance exists detailing how credit history reviews for job candidates should be executed.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Staff performing credit history reviews have received organizational training or guidance on how to execute such functions.

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 # HR1.7: Candidate Medical Testing

The organization conducts medical testing of job candidates for substance abuse, including the abuse of alcohol and prescription drugs.

Clarification/Intent

The organization administers medical tests to screen candidates for illegal substance use, unreported prescription drug use, and alcohol abuse.

Assessment Team Guidance

The organization should avoid hiring candidates whose performance and judgment might be compromised by substance abuse problems.

For all drug testing, employers must generally comply with state drug testing laws. For prescription drug and alcohol testing, employers must be aware that the American Disabilities Act may apply.

MERIT Example

The insider, a subcontractor, was employed as a systems administrator by victim organization. The contractor organization provided computer support to the victim organization, specifically by using a local area network (LAN) that allows employees to create and edit documents, access databases, and to send e-mails to co-workers. The victim organization was a government agency. The insider helped to maintain the connection between the victim organization's file server and the LAN. As a function of his job, the insider was given remote access to the victim organization's network, allowing him to remotely control server operations. The contractor organization offered the insider a full-time position, but rescinded the offer after the insider failed a mandatory drug test. The contractor organization informed that he could no longer work for the victim organization and his employment was terminated. The contractor organization failed to notify the victim organization of the insider's termination. Security personnel escorted the insider out of the building. The insider was characterized as "angry" at the time of his termination, but a technical supervisor had previously raised concerns regarding the insider's agitated demeanor and short temper. The insider was terminated on a Friday and the attack occurred over the weekend following the insider's dismissal. The insider used a previously-created bogus account, which was an abbreviated version of his wife's name, to remotely attack the victim organization. The insider disabled the server, changed passwords and deleted printers from the network system. The victim organization's systems manager discovered the attack after the organization's employees could not log on to the file server. The victim organization's systems were down for 12 hours and the incident related loss was $60,000. The insider attempted to conceal his actions by clearing system error logs, but was connected to the incident via remote dial-in logs. The insider was arrested, ordered to pay $5,000 restitution, and sentenced to 4 months imprisonment followed by 3 years supervised release.

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 in place that explains when and why medical testing is required as part of the employee hiring process (as allowed under applicable laws).

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization develops a business case to justify any medical testing that is required as part of the employee hiring process (as allowed under applicable laws).

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization administers medical tests to screen candidate's recent alcohol use and use of a range of illegal drugs (as allowed under applicable laws).

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a standard process in place for conducting medical tests to screen candidate's recent alcohol use and use of a range of illegal drugs (as allowed under applicable laws).

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization administers medical tests to screen candidate's recent use of a range of prescription medications (as allowed under applicable laws).

Doc Rev

Dir Obs

Intvw

☐ The organization has a standard process in place for conducting medical tests to screen candidate's recent use of a range of prescription medications (as allowed under applicable laws).

Doc Rev

Dir Obs

Intvw

☐ Documented procedures or guidance exists detailing how medical testing for candidates should be executed.

Doc Rev

Dir Obs

Intvw

☐ Staff performing medical testing have received organizational training on how to execute such functions.

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 # HR1.8: Candidate Behavioral Interview

The organization conducts an in-person behavioral interview with job candidates to evaluate their attitudes, interpersonal skills, and technical skills.

Clarification/Intent

Individuals trained in behavioral interviewing might be able to detect any of the candidates' attitudes and personality issues that could lead to problems at work and foster disgruntlement.

Assessment Team Guidance

CERT studies indicate that problems with mental health and social skills can create a vulnerability to insider risk. HR personnel trained in behavioral interviewing might be able to detect such risks through specific interview protocols. Behavioral interviews might also provide an opportunity to

- screen the candidate's reactions to personal and professional stressors
- screen the candidate's reactions to negative references or work experiences
- identify the candidate's patterns of decision making, including on ethical issues
- validate information in the candidate's application
- verify the candidate's technical skills and training

Employers should be aware that certain behavioral tests can be considered medical tests and are regulated by the Americans with Disabilities Act. In addition, employers should ensure that the testing does not cause a disparate impact to a protected class, which would violate equal employment laws.

MERIT Example

The insider, a contractor, was formerly employed as a help desk specialist by the victim organization, a publishing company. As a function of his job, the insider was able to create, modify, or delete programs on the organization's systems. The organization terminated the insider's employment because they were generally unhappy with him, specifically due to supervisor conflict, coworker complaints, and the insider's abrasive attitude. The night after his termination, the insider, whose accessed had been revoked, purportedly used another employee's credentials to remotely access the organization's networks. The next day, the system crashed. Phone records indicated that a 55 minute phone call was made from the insider's home phone to an organization computer line. A search of the insider's home uncovered the organization's confidential documents, including planning documents, salary information, and an internal security analysis. The investigation also revealed that the insider possessed a library of documents related to computer hacking and sabotage, including a Trojan horse construction kit. The insider revealed later that although he felt highly qualified for his position at the organization, his job was that of a low-level technician and he received no respect from his colleagues. The insider denied involvement in the incident. The insider was arrested, convicted, ordered to pay $20,000 restitution, and sentenced to 5 years of probation - including 4 months of monitored home confinement and 200 hours of community service.

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 covering which positions are subject to personal interviews.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization conducts personal interviews to determine candidate's interpersonal strengths and weaknesses in accordance with documented policy.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization conducts personal interviews to explore candidate's past challenges at work, including negative references and ethical decision making in accordance with documented policy.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a standard process in place for conducting personal interviews.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has documented procedures covering how to appropriately conduct personal interview activities, including

Doc Rev

Dir Obs

Intvw

- ☐ how to confirm information provided in the application

  Doc Rev

  Dir Obs

  Intvw

- ☐ how to protect candidate's rights

  Doc Rev

  Dir Obs

  Intvw

- ☐ which employees can administer this type of interview

  Doc Rev

  Dir Obs

  Intvw

- ☐ how to verify technical abilities and training during the personal interview

  Doc Rev

  Dir Obs

  Intvw

☐ Staff performing personal interviews have received organizational training on how to execute such functions.

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 # HR1.9: Candidate Psychological Testing

The organization uses some form of formal psychological testing to verify the honesty, personal characteristics, and integrity of job candidates.

Clarification/Intent

Formal psychological testing can be used to assess the attitudes and beliefs correlated with theft and dishonesty in the workplace. Doing so can screen out candidates with serious psychological problems or characteristics associated with counterproductive work behaviors. It can also identify and reinforce the value of candidates with personal characteristics that have demonstrated advantages for specific jobs. For select positions of significant trust in specific industries and government, the polygraph may be used to verify the integrity and intentions of candidates, consistent with Federal regulations.

Assessment Team Guidance

Honesty testing is widely used in retail and other fields in which theft, fraud, or embezzlement is a risk. Psychological screening tools such as the Minnesota Multiphasic Personality Inventory-2 (MMPI-2) are commonly used to screen candidates for high-stress or high-trust positions to rule out major psychological problems. Specific test batteries are frequently designed to identify personal characteristics prior research has found to be adaptive for particular positions. The polygraph may be used for positions of trust within classified environments, the pharmaceutical industry, and other industries exempt from the Federal ban on its use.

Psychological testing may be considered as falling within the definition of medical testing and therefore may be regulated under the Americans with Disabilities Act. As a result, psychological testing likely only applies to trusted positions within certain sectors.

If such testing is not considered warranted or appropriate within the organization, this capability should be marked as not applicable and removed from the assessment process.

MERIT Example

The insider, a foreign national, was employed as a design engineer by the victim organization, which designed semiconductors. A few months prior to resigning from the victim organization, the insider emailed design data sheets to a direct competitor, the beneficiary organization. The insider subsequently accepted a position with the beneficiary organization and resigned from the victim organization. The insider provided a false reason for his resignation and told the victim organization that he did not have a job lined up. After the insider's resignation, two of his former colleagues reported that they directly observed, or had knowledge of, the insider downloading data from the victim organization's network. The insider downloaded the information on-site, during work hours, for 3 months. The insider stole data both before and after accepting the position with the beneficiary organization. A forensic exam revealed email correspondence between the insider and the beneficiary organization, including email transfers of the victim organization's confidential information and a job offer with salary and benefits information. The stolen datasheet was valued at $100,000. The insider was arrested, convicted, fined $3,500, and sentenced to 6 months of community confinement and 6 months home confinement followed by 5 years of probation. The insider's sentence was relatively light because semiconductor data sheets generally have no standalone value and are often publicly disclosed.

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 covering which positions are subject to psychological testing.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization uses formal psychological testing to screen out or select candidates for attitudes empirically associated with honesty or psychopathology and for personal characteristics empirically associated with work success or integrity and honest motivation.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Documented procedures or guidance are in place on how to conduct psychological testing.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Staff performing psychological testing have received organizational training on how to execute such functions.

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 # HR1.10: Onboarding Process

The organization has an employee onboarding process to inform new hires of the organization's policy, procedures, values, and culture and establish expectations.

Clarification/Intent

The organization should set clear expectations with new employees about their roles, responsibilities, and contribution.

Onboarding processes enable alignment of new hires to the organization, their roles, and their responsibilities to reduce misunderstanding regarding expectations.

Assessment Team Guidance

CERT studies indicate that employee disgruntlement is a motivating factor of insider crime. Disgruntlement can occur when an employee's expectations do not match those of the organization. The onboarding process is one way to set expectations and mitigate disgruntlement.

MERIT Example

The insider was employed as a hardware engineer by the victim organization, which served as a middleman broker between farmers and grocery stores. The organization was experiencing some reorganization, believed to be one source of the insider's motivation for the attack. The insider was unhappy with his new boss, because the boss modified the organization's bonus system. The insider later claimed his job was not challenging and about the lack of upward mobility in the company. The insider was formally reprimanded for absenteeism. Prior to the attack, the insider left work at lunch time without notifying his supervisor. 10 days after receiving the formal reprimand, the insider used a shared administrative account to remotely access 5 of the organization's systems. The insider uploaded a virus that damaged 2 systems. Following the attack, the insider did not return to work. After calling in sick several times, the insider finally faxed his resignation. The insider was connected to the incident through remote access logs. The insider was arrested and convicted, but the conviction was overturned due to a legal loophole concerning the exact amount of damages. The incident related loss was $75,000 - $85,000.

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 a documented policy or process for onboarding new hires.

Doc Rev

Dir Obs

Intvw

☐ The organization follows the onboarding process for all new hires or transfers.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The onboarding process lasts more than a day, and provides insight into the organizational unit the employee will be joining.

Doc Rev

Dir Obs

Intvw

☐ The onboarding process includes

Doc Rev

Dir Obs

Intvw

☐ an overview of policy and procedures

Doc Rev

Dir Obs

Intvw

☐ an overview of organizational culture attributes

Doc Rev

Dir Obs

Intvw

☐ an overview of the performance management process

Doc Rev

Dir Obs

Intvw

☐ a review of roles and responsibilities

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization follows the standard onboarding process for all trusted business partners.

Doc Rev

Dir Obs

Intvw

☐ The organization has staff dedicated to employee engagement, development, or effectiveness, whose task it is to integrate new hires into the organization.

Doc Rev

Dir Obs

Intvw

☐ The organization has documented processes and procedures for onboarding new hires.

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 # HR1.11: Increased Monitoring during Probationary Period

For new hires, the organization implements a probationary period of increased monitoring of online and workplace behavior.

Clarification/Intent

Many employee offenses occur early in the employment period when rules and policy are unclear or poorly understood. In addition, some groups of potential insiders—especially those involved in the internet underground—habitually deploy devices or disable logging early in their employment. Early surveillance can reduce these risks before they become more damaging. The interpersonal or social skill deficits of new hires might not be clear until they are in the workforce. The deficits can be rapidly assessed and dealt with by using a probationary period that gives the organization greater flexibility and options with new hires than with longer-term employees.

Assessment Team Guidance

The following behaviors should be closely monitored:

- involvement with the internet underground
- fraud
- information/privacy violations
- timecard and other financial reporting
- information theft
- disruptive interpersonal behavior

Interpersonal monitoring should be addressed through performance management activities.

MERIT Example

Supervisor at a bank downloaded a Trojan horse program when individual clicked on a photo on a website. The program recorded keystrokes, erased security files and emailed recorded information. Unknown individuals were able to access the customer information of over 30,000 accounts in the banking area. The organization was vulnerable because of the back door method which they used to allow new employees (that were part of an acquisition of a different bank) access to the system. Over the course of about a month, the hackers looked through the accounts, determining which to compromise. Four wire transfers were attempted from the victim organization to other bank accounts outside of the organization. The attempts were unsuccessful. Another supervisor within the victim organization first noticed the fraud. Investigation did not uncover the culprits. Information about the bank accounts outside of the organization did not help identify the culprits because: foreign information was unavailable, one of the bank accounts was created through ID theft and the holder of another of the accounts could not be located.

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 performance management process.

Doc Rev

Dir Obs

Intvw

☐ The organization has a documented probationary period policy or process.

Doc Rev

Dir Obs

Intvw

☐ The organization conducts performance reviews at least annually.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization actively monitors, records, and evaluates employee online behavior for an established probationary period of at least 3 months.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization actively monitors, records, and evaluates employee online behavior for an established probationary period of at least 6 months.

Doc Rev

Dir Obs

Intvw

☐ The organization institutes a period of close behavioral monitoring of new employees' workplace behavior during the probationary period (i.e., regularly checking in with the new employee).

Doc Rev

Dir Obs

Intvw

☐ Staff engaged in monitoring, recording, and evaluating employee behavior have received training or guidance on how to conduct such activities.

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 # HR1.12: Policies for Workplace Behaviors

The organization has policy and practices that describe acceptable and unacceptable workplace behaviors, including interpersonal activities.

Clarification/Intent

The organization has both hard-copy and online materials that describe acceptable and unacceptable behaviors and that include activities related to

- interpersonal, legal, regulatory, and ethical issues
- privacy
- security
- outside employment
- organizational values
- employee privileges
- compensation
- organizational property use

Assessment Team Guidance

To intervene in unacceptable workplace behaviors and enforce its policy and practices, the organization must establish, communicate, and uniformly enforce these rules and have employees acknowledge them. Areas covered should include but not be limited to

- violence and threats
- theft of company or personal property
- sexual harassment
- damaging, unproductive, or offensive behavior
- Equal Employment Opportunity rules
- attendance
- timecard and other financial reporting
- vacation and leave
- drug and alcohol use
- weapons
- dress and hygiene
- fraternization and relationships at work
- respect and treatment of others
- protection of privacy and proprietary and personal information
- nonbusiness use of organizational resources
- granting physical or digital access to unauthorized personnel
- outside business contacts and reporting
- refusal to document work or perform other work-related tasks

MERIT Example

The insider was formerly employed as a laboratory system administrator by the victim organization, a university cancer institute. The insider decided to continue his education, forcing him to change to part-time status. The insider was primarily disgruntled with the organization because his change in status substantially lowered his benefits. The insider also had financial issues. The insider was hostile toward his co-workers, who characterized the insider as lazy. The organization deemed the insider to be a "necessary evil" because of his skills. At work, the insider displayed numerous instances of aggressive and malicious behavior. The insider resigned from his position, primarily because of personality and work ethic differences. Subsequently, the insider launched two attacks on the organization's systems. 2-3 days after his resignation, the insider returned to the work site after working hours. The insider's badge had been disabled, so he asked an employee who recognized him to let him in. Once the insider gained access to the building, he used a key, which should have been confiscated according to university policy, to enter the office. In the first attack, the insider used computer access (no accounts or passwords were necessary and no auditing was done) and user commands to defeat policy (a design vulnerability) by deleting the cancer research (data) in order to create a denial of service attack (DoS). In the second attack, the insider again used his computer access and user commands to violate policy (a design vulnerability) by modifying what remained of the research group's deleted information and modifying operating systems to depict/display both derogatory and arrogant statements about co-workers and his own technical abilities, respectively, in order to corrupt information. The incident modified the file system to display his statements (i.e. when someone viewed the root drives directory users could read a message by reading the modified directories names in sequence, in a left to right and top to bottom manner.) The insider also sent angry e-mails to his supervisor and co-workers. The organization had no backup copies of the 18 months of research, valued at $90,000. The insider was arrested, convicted, ordered to pay $3,000 restitution, and sentenced to 3 years of probation with 100 hours of community service.

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 practices describing appropriate and inappropriate workplace behavior.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization communicates the policy and practices to employees.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization obtains employee acknowledgement and agreement to adhere to the policy and practices.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization makes both hard-copy and online materials that describe acceptable and unacceptable behaviors easily available to employees.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization enforces the policy and practices.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization requires the employee to sign the relevant policy and practices.

Doc Rev

Dir Obs

Intvw

☐ The organization periodically trains employees on the policy and practices.

Doc Rev

Dir Obs

Intvw

☐ The organization periodically reviews the policy and practices for effectiveness.

Doc Rev

Dir Obs

Intvw

☐ The organization updates the policy and practices as necessary.

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 # HR1.13: Employee Obligation to Report Behavioral Violations

The organization has a policy that encourages and/or describes an employee's obligation to report or otherwise deal with violations of its workplace behavioral rules and interpersonal violations.

Clarification/Intent

Employees and their families understand that they are the most important source of information and concern regarding the safety and security of their workplace. The organization provides employees specific mechanisms and scripts to report violations of workplace behavioral rules or concerns about their own or others' behavior. Options for anonymous reporting may be included.

Areas covered should include but not be limited to

- violence and threats
- theft of company or personal property
- sexual harassment
- damaging, unproductive, or offensive behavior
- Equal Employment Opportunity rules
- attendance
- timecard and other financial reporting
- vacation and leave
- drug and alcohol use
- weapons
- dress and hygiene
- fraternization and relationships at work
- respect and treatment of others
- protection of privacy and proprietary and personal information
- nonbusiness use of organizational resources
- granting physical or digital access to unauthorized personnel
- outside business contacts and reporting
- refusal to document work or perform other work-related tasks

Assessment Team Guidance

Past CERT insider threat studies have found that a significant number of coworkers and others in the employee's family or social network were aware of the insider's disgruntlement and specific plans for attack. Coworkers were also aware of the damaging and potentially fatal impact these attacks could have on the organization and the job security of other workers.

Team members should be careful to distinguish between policy that requires reporting (MUST) versus policy that suggests reporting (SHOULD).

It should be noted that the following capability, HR1.14: Follow-Up of Employee Violations, contains the indicators related to handling of any reported violations.

MERIT Example

Subject was in a management position at a local bank. For almost 5 years, the Subject committed a lapping scheme at the bank. Subject would steal money from one account and then use money from another account to hide theft. Subject's co-workers had noticed security/policy violations, but had not reported them. For example, Subject was noted using co-workers' computers and often the teller's drawers would be out of balance. Subject also covered her tracks by sending out false bank statements of victim's accounts and changing the addresses of the account so that the real statement would not reach victim. Subject's activities were discovered when she was sick in the hospital and a customer was unable to locate his account. The bank then started an audit. The Subject's relative stated that the Subject had a "spending problem", perhaps based on the grief over the death of a relative. The Subject was arrested, plead guilty to bank fraud and sentenced to 37 months in prison and 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 policy that requires employee action when the employee becomes aware of violations of work-place rules or suspicious actions by employees and trusted business partners.

Doc Rev

Dir Obs

Intvw

☐ The organization has mechanisms and processes in place that allow confidential reporting of workplace violations or suspicious behavior.

Doc Rev

Dir Obs

Intvw

Level 3

☐ All reports that are submitted are reviewed and handled.

Doc Rev

Dir Obs

Intvw

☐ The organization has mechanisms and processes in place that allow anonymous reporting of workplace violations or suspicious behavior.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has documented procedures available to employees and trusted business partners that.

Doc Rev

Dir Obs

Intvw

☐ describe specific reporting options and corresponding processes

Doc Rev

Dir Obs

Intvw

☐ are reviewed and updated on a periodic basis

Doc Rev

Dir Obs

Intvw

☐ The organization educates and trains employees on the policies, including the reasons for these rules and their potential benefits for workplace safety and security.

Doc Rev

Dir Obs

Intvw

☐ The organization has training that takes into accounts the organization's actual risks and threats (i.e., the training is customized to the organization's threat environment and mission).

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 # HR1.14: Follow-Up of Employee Violations

The organization has policy and practices for following up on employee reports of violations and risks.

Clarification/Intent

The organization has policy and practices to fully handle, protect, and effectively deal with employee reports of risky behavior or violations of policy. Such reports are recorded and tracked by qualified multidisciplinary professionals who follow established procedures. The results are stored safely so they can be used for future individual, group, and organizational risk assessments.

Assessment Team Guidance

The organization should have policy and practices to assure that

- reports of risk or violations submitted by employees and others are tracked in a standardized manner
- anonymous and other reporting sources are protected
- the persons investigating these reports are qualified to do so and have no conflict of interest (e.g., they do not supervise the employees involved) and have access to support from multidisciplinary personnel trained to assist them (e.g., physical security, information security, mental health, legal, HR resources)

The results of investigations should be stored securely.

MERIT Example

The insider was employed as a property room (evidence) manager by the victim organization, a law enforcement agency. While on site and during work hours, the insider abused her access to a database to obtain information regarding her former daughter-in-law's new husband. The insider passed the information onto her son, who subsequently murdered his ex-wife's new husband. There was no evidence to suggest that the insider had prior knowledge that her son was going to commit murder, but the insider was apparently concerned that her grandchildren were going to be raised by a man of Islamic faith. The insider had numerous behavioral precursors, specifically erratic behavior and becoming overly excited about trivial issues. The insider was receiving treatment for lupus, so colleagues attributed this behavior to her medication. The insider had been reprimanded for policy violations, specifically by leaving evidence on her desk and allowing her family in the property room. Over the course of the investigation, the organization discovered that the insider had been taking items from the property home with her for several years. The insider was not prosecuted for the incident, which was discovered during the related murder investigation. The insider was connected to the incident through access logs.

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 detailed, established policy and practices governing how employee reports of risk or violations will be followed up.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has policy and practices that protect the identity and avoid exposure of reporting employees and other sources of information.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has policy and practices that protect the privacy and civil liberties of any person accused of work-place violations or suspicious, risky behavior.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization follows up and handles all reports of risk or workplace violations

Doc Rev _____

Dir Obs _____

Intvw _____

  ☐ in accordance with the above policy and practices

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ in accordance with all legal mandates, laws, and regulations

Doc Rev

Dir Obs

Intvw

☐ in a fair and timely manner

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization has a standardized process in place for tracking and responding to all reports of risk or workplace violations.

Doc Rev

Dir Obs

Intvw

☐ The organization securely stores and protects all materials related to reports and follow-up.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has documented procedures or guidance that assures that

Doc Rev

Dir Obs

Intvw

☐ persons investigating these reports meet established qualifications

Doc Rev

Dir Obs

Intvw

☐ investigators are free of any conflict of interest

Doc Rev

Dir Obs

Intvw

☐ investigators have access to qualified, multidisciplinary professionals who can help assess risk and other issues

Doc Rev

Dir Obs

Intvw

☐ The organization has designated staff who handle the investigations and follow-up activities.

Doc Rev

Dir Obs

Intvw

☐ Staff who perform investigations and follow-up activities receive appropriate training on how to conduct those activities.

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 # HR1.15: Investigation Results Usage

The organization has policy and procedures for using the results of the investigation of employee violations and other risk reports, including clear options for consequences when significant insider risks are found.

Clarification/Intent

The results of investigations are documented for analysis regardless of their outcome and are accessible to future investigators. Clear and varied options (beyond immediate termination) are available to deal with employees who present significant insider risk. In addition, boards, groups, or decision makers have been established to decide how the organization deals with repeated concerns. The organization uses these procedures and consequences consistently.

Assessment Team Guidance

Insider threat research has found that abrupt termination without significant evaluation was often followed by an insider action by the terminated employees. Keeping detailed records and allowing employee records to be used for employee evaluation prior to personnel actions, especially termination, may reduce the likelihood of insider attacks.

The results of investigations should be stored securely but be available to future investigators assessing the risk of individuals, groups, situations, or outside threats.

MERIT Example

The insider was formerly employed as a supervisor in the internet technology (IT) department of the victim organization, an educational institution. The organization terminated the insider's employment after numerous violations of the organization's conduct policy. A few hours after his termination, the insider used another employee's credentials to remotely access the organization's fiscal computer. For over 2 months, the insider continued to remotely access and delete records from this computer. An internal audit detected the incident and the insider was connected to the incident through his IP address. The insider was arrested, convicted, and sentenced to an alternative rehabilitation program.

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 clearly defined options and consequences for handling investigations that result in findings of significant insider risks.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has policies or practices in place that requires

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ maintaining records of past investigations, regardless of their outcome, of employees who presented possible risk factors

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ making reports available to investigators looking into current concerns

  Doc Rev _____

  Dir Obs _____

  Intvw _____

Level 3

☐ The organization has varied options beyond simple termination for dealing with persons presenting repeated concerns.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has established adjudication groups and procedures for evaluation and decision making regarding consequences for at-risk employees.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has documented procedures that detail how proven violations and risks should be handled.

Doc Rev

Dir Obs

Intvw

☐ The organization consistently follows its policy and procedures regarding handling of employee violations and other risk reports.

Doc Rev

Dir Obs

Intvw

☐ Staff responsible for investigations and handling risks and workplace violations are trained on techniques and procedures for performing such activities.

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 # HR1.16: Sharing of Policy Violation Information

The organization has a method for sharing reports of security and policy violations and other risk indicators among concerned groups, including HR, Legal, physical security, IT security, and other departments.

Clarification/Intent

The organization should have policy and practices that mandate the regular sharing of information on employee risk indicators among HR, Legal, physical and IT security, and other concerned departments. This information should encompass individual employee risk as well as organizational and environmental risk factors that have possible implications for insider risk.

Assessment Team Guidance

Past insider research has indicated that behavioral and IT risk indicators might co-occur. For example, two noted insiders were both cited by HR for shoving female employees around the same time the insiders were violating IT policy and safeguards. Knowledge of violations in one area might lead to inquiries in another that expose insider risk. In addition, it is important that departments share information about organizational or environmental developments that can influence insider risk. For example, during one recent insider risk audit, an organization's HR department did not inform the IT security department about a series of recent layoffs. As a result, the employees' access was not terminated in a timely fashion. Strikes, mergers, and acquisitions are examples of organizational and environmental developments that should be shared across departments.

If the organization has a formalized insider threat program or an analytic hub – the team should take this into account and count this towards meeting some of the information sharing indicators. However, the team should still look to see that information about risks and threats are actually shared with relevant stakeholders, including information about employee separation or problem behavior. Any information sharing must be in keeping with the organizational policies and relevant laws, regulations, and mandates. Employee privacy and civil rights must also be protected.

MERIT Example

The insider, a resident alien, was employed as a senior research scientist by the victim organization, a chemical manufacturing company. The insider was working on a multi-million dollar project related to chemicals used to produce a new electronic technology. The insider and the beneficiary organization, a foreign university where the insider was an alumnus, wanted to use the technology to develop a commercial product. In direct violation of his employment agreement, the insider accepted a job from the beneficiary organization without notifying the victim organization. During this time, the insider was listed as a faculty member on the beneficiary organization's website and made multiple presentations regarding his plans for the victim organization's technology, including a presentation at a prestigious American university. Several months later, the insider provided a 1 month notice to the victim organization that he planned to resign and transfer to a position with a foreign branch of the victim organization, which was located in his home country. In the month following announcing his resignation, the insider emailed a Microsoft Word document, which detailed the chemical procedure, to his email account at the beneficiary organization. The insider repeatedly inquired about transferring the data from his company laptop to the victim organization's foreign branch. The insider was consistently informed that the transfer would require approval and that he was prohibited from transferring any information from his laptop in the absence of an approval. The insider attempted to force the transfer by emailing the IT department, falsely stating that his transfer had been approved, and asking how to perform the transfer. Prior to the insider's departure from the victim organization, the victim organization performed a forensic examination on the insider's computer, which was standard procedure for transferring employees. The day after the insider's laptop was returned, while on site and during early morning hours, the insider downloaded 543 documents from the laptop to an external storage device. A few days later, the victim organization confronted the insider about downloading confidential documents and his connection to the beneficiary organization. The insider initially confessed that he had downloaded documents to an external drive, but denied any additional actions or connections to the beneficiary organization. The insider considered the documents to be "reference materials." A subsequent examination of the insider's personal computer revealed that he had copied the documents to his personal computer, and there was evidence that the insider had transferred information to his personal yahoo email account. The incident was detected before the information could be shared with the beneficiary organization. The insider was arrested, convicted, and sentenced to 14 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 a defined process for the regular sharing among HR, physical security, Legal, and IT security of information on individual and organizational risk factors.

Doc Rev

Dir Obs

Intvw

☐ The organization regularly shares information among HR, physical security, Legal, and IT security on individual and organizational risk factors as appropriate.

Doc Rev

Dir Obs

Intvw

☐ Any organizational information sharing among HR, physical security, Legal, and IT security of information on individual and organizational risk factors is done in accordance with all relevant policies, laws, regulations, and mandates.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization has established communication mechanisms for information sharing among HR, physical security, Legal, and IT security regarding individual and organizational risk factors.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization schedules regular information sharing sessions among HR, physical security, Legal, and IT security regarding individual and organizational risk factors.

Doc Rev

Dir Obs

Intvw

☐ The organization has established a formal Insider Threat Program and team to share information and collect data across relevant parts of the enterprise.

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 # HR1.17: Monitor, Log, Audit Policy

The organization has established policy and practices that allow it to monitor, log, and audit all personnel activities on its proprietary IT and communications systems.

Clarification/Intent

The organization has established a policy that allows it to monitor, log, and audit all employee activity on its systems regardless of the origin of the communication or its personal or professional nature.

Assessment Team Guidance

The organization has established its right to monitor, log, and audit both the technical and interpersonal conduct of employees on its digital media, networks, and other computerized communication media. The goal is to enforce the organization's policy regarding online interpersonal and technical conduct.

MERIT Example

The insider, a clerk, was employed by the victim organization, a child support office. While on site and during work hours, the insider modified computer entries to issue child support checks to her mother. The insider's mother had Alzheimer's and resided in an assisted care facility. An employee at the assisted care facility reported the first check dispersed, for over $3,000. The insider resigned after an internal investigation revealed logs directly linking her to the fraud. The insider was arrested, convicted, and sentenced to 5 years 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 a policy in place that allows it to monitor, log, and audit all personnel activity on its systems and networks.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Any employee monitoring, logging, and auditing of personnel activity is done in accordance with all relevant policies, laws, regulations, and mandates.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a standardized process in place for monitoring, logging, and auditing all personnel activity on its systems and networks

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization securely stores and protects all artifacts from its employee monitoring, logging, and audit activities.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization periodically trains or teaches employees about the policy (this does not have to include specifics of what is monitored).

Doc Rev

Dir Obs

Intvw

☐ The organization institutionalizes the policy in its official media and communications.

Doc Rev

Dir Obs

Intvw

☐ The organization tests employee knowledge of the policy.

Doc Rev

Dir Obs

Intvw

☐ The organization requires employee acknowledgement of the policy as an requirement for employment.

Doc Rev

Dir Obs

Intvw

☐ The organization posts the policy on its computerized media or makes the policy available in an alternative manner.

Doc Rev

Dir Obs

Intvw

☐ The organization has established a policy for intensified monitoring of employees when violations or other risk indicators suggest it is necessary or when there is evidence of other threats.

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 # HR1.18: Targeted Monitoring Policy

The organization has documented policy for targeted monitoring.

Clarification/Intent

The organization should have a clearly documented targeted monitoring policy prior to placing additional scrutiny on any single employee.

Assessment Team Guidance

An organization may want to more closely monitor any employee exhibiting particularly concerning behavior. For the private sector, policy for placing additional monitoring on an employee is recommended to avoid discrimination suits. Such policy is also recommended for the public sector to address any prerequisite inquiry or investigation required by additional regulations.

IT teams, instead of the human resources department, may be the owners of targeted monitoring policy. This capability only looks to see there is a policy in place, the actually targeted monitoring of employees is addressed in the IT workbook.

MERIT Example

The insider, a foreign national, was employed as a researcher at the victim organization, a chemical company. The victim organization specialized in the research and synthesis of large quantities of chemical compounds. The insider used a personal computer to access files containing four recipes on the victim organization's network. The insider then sent the files to an outsider, a family member, who worked for a competitor. The insider and the outsider had also started a website for a new business that would directly compete with the victim organization, but did not officially register the business in a foreign country. The insider was caught when a co-worker saw the insider download, convert, and e-mail files containing trade secrets using a personal computer. The co-worker reported the action to management, who worked with IT to set up logging and monitored the insider's activity more closely. The next day, the insider sent another e-mail to the outsider including company confidential chemical production methods, and was put on administrative leave.

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 in place allowing for targeted monitoring of employees.

Doc Rev

Dir Obs

Intvw

☐ Any targeted employee monitoring is done in accordance with all relevant policies, laws, regulations, and mandates.

Doc Rev

Dir Obs

Intvw

☐ Any targeted employee monitoring is done with the knowledge and consent of legal and human resources.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization has a standardized process in place for targeted employee monitoring.

Doc Rev

Dir Obs

Intvw

☐ The organization securely stores and protects all artifacts from targeted employee monitoring.

Doc Rev

Dir Obs

Intvw

Level 4

☐ If the organization uses risk scores to determine whom to monitor, the organization documents how the risk scores are calculated.

Doc Rev

Dir Obs

Intvw

☐ If the organization uses risk scores to determine whom to monitor, the organization has the legal and human resources departments review risk score criteria to ensure employee rights are protected.

Doc Rev

Dir Obs

Intvw

☐ The organization partitions the individuals responsible for performing different functions such as monitoring and investigation (i.e., those responsible for monitoring the network may not legally investigate an individual case).

Doc Rev

Dir Obs

Intvw

☐ The organization considers the time frame of the occurrence.

Doc Rev

Dir Obs

Intvw

☐ The organization considers the employee's risk factors separately from the employee's degree of access.

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 # HR1.19: IP Policy

The organization has clearly defined policies regarding the definition, ownership, use, and sharing of its intellectual property (IP).

Clarification/Intent

The organization has rules and regulations defining the ownership of all organizational intellectual property including all employee work products. The organization also has supporting procedures which describe processes for answering questions regarding ownership, benefits from IP and contingencies for rule violations. These procedures explicitly address scenarios in which employees may seek to take IP or other sensitive data for personal business advantage or for use at another organization.

Assessment Team Guidance

A subset of insider violations stems from misunderstanding and conflict regarding ownership of IP, especially due to unclear definitions of IP and arrangements for shared ownership prior to its creation. These difficulties extend to contractors as well as direct employees. In addition, numerous cases involve former employees who take or use their organization's IP or other sensitive proprietary data for personal business advantage.

This capability is also included in the Legal workbook.

MERIT Example

The insider, a contractor, was employed as a computer consultant by the victim organization, which managed client data and business operations for other companies. The insider had a verbal contract with the organization and was the principal software developer for the organization. Agreements between the organization and the insider indicated that the organization retained ownership and related intellectual property rights in the insider's work product. Over the course of a year, the insider repeatedly demanded that the organization grant him 20% of the company in consideration of his services. The organization decided to demote the insider because of his behavior. The organization informed the insider that in 5 months he would be reduced to part-time status, lowering his compensation and benefits. The insider continued to demand a 20% interest in the company. The incident took place over a 21 day period. The day after his demotion to part time status, the insider, during work hours, remotely logged into the organization's computer system. The insider removed critical code from the system, preventing employees and authorized users from accessing software he created, specifically a program that was used to manage client data and business operations. The organization detected the attack when customers reported their inability to access the system. The organization connected the insider to the attack when an employee contacted the insider for technical support and the insider revealed that he had taken the program down in order to acquire 20% of the company. 4 days later, the organization drafted a document purported to grant the insider his desired interest in the company, and the insider remotely accessed the organization's computer system and restored access to the program. The owner of the organization, accompanied by corporate counsel, contacted the insider via telephone. The insider admitted that he had taken down the computer system, intended to disrupt the organization's business operations, and indicated the he would not cause any more disruptions if the organization met his demands. 3 days later, the organization had not met the insider's demands, so the insider remotely accessed the system and modified passwords, preventing employees and authorized users from accessing the computer system. The insider was arrested, convicted, ordered to pay $10,000 restitution, and sentenced to 6 months of home detention followed by 2 years of probation. The insider was also required to notify future consulting clients of his conviction and to provide his client list to his probation officer. The victim organization's damages were estimated at $5,000.

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 a policy that clearly defines what is considered intellectual property (IP).

Doc Rev

Dir Obs

Intvw

☐ The organization has a policy that clearly defines the ownership of all organizational intellectual property (IP).

Doc Rev

Dir Obs

Intvw

☐ The organization has a policy against theft of IP or other proprietary data by employees for personal business or other advantages.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization has a policy that includes clear descriptions of ownership of employee work products, including rules for sharing or not sharing ownership.

Doc Rev

Dir Obs

Intvw

☐ The organization requires employee acknowledgement of the IP policy.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization requires employees to minimally sign the IP policy upon hiring and separation.

Doc Rev

Dir Obs

Intvw

☐ The organization has a designated procedure for resolving questions regarding IP ownership, including a specific point of contact for questions.

Doc Rev

Dir Obs

Intvw

☐ The organization has procedures for ensuring employee understanding and acknowledgment of IP policies and privileges.

Doc Rev

Dir Obs

Intvw

☐ The organization has specific contingencies for violation of IP policies and practices and consequences for the theft of IP or other sensitive proprietary data for personal business advantage.

Doc Rev

Dir Obs

Intvw

☐ The organization has education or training programs for employees regarding these policies and practices.

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 # HR1.20: Facility & Employee Physical Security

The organization has policies and practices for the adequate protection of facilities' and employees' physical security.

Clarification/Intent

Insiders may use weaknesses in physical security measures to access information storage and computerized systems. The organization should have policy that governs the facility access and egress of persons, information, equipment, and property. This policy should be scaled to the organization's assessed risk and threats relevant to a facility and its personnel. The organization should also have policy that governs physical access to different sections of a facility according to employee group, based on need and qualification.

Assessment Team Guidance

In past insider cases, employees have

- smuggled information-containing media from facilities
- allowed confederates into facilities to assist them in insider acts
- inadvertently allowed unauthorized individuals access to critical information, subsequently taken, within the facility
- failed to safely dispose of printed materials that were then taken from dumpsters
- violated internal physical access policy to steal or damage property

The assessment team should look for evidence of documented procedures or a physical security plan that outlines how facilities are protected. They can also collect evidence by observing the process they must follow to enter facilities and areas within facilities.

MERIT Example

The insider was employed as an administrative assistant to a general partner of the victim organization, a venture capitalist firm. Prior to the incident, the insider had been misusing corporate credit cards to purchase expensive personal items, which she shipped to her home. The insider had made fraudulent charges in excess of $100,000 dollars. The insider's credit card fraud was discovered after she mistakenly shipped a fraudulent purchase to the billing address on the credit card, which was the organization's office. Initially, the organization believed the fraudulent charges to be less than $10,000. The insider paid a little over $8,000 in restitution and was subsequently terminated. The organization gave the insider permission to return after the work day had ended, but before 9:00 PM, to clear out her desk. The insider entered the organization's facilities at an unknown time that evening. Beginning at approximately 11:00 PM, the insider used her still active computer and network logon accounts to access the organization's networks. The insider downloaded sensitive files, including trade secrets potentially valued at $1 million; e-mailed several files to herself at different personal accounts, and copied several files to discs. To conceal her actions, the insider deleted copies of her sent email. The insider was arrested, convicted, and ordered to repay the $100,000 credit charges, but sentencing details related to the trade secret theft were unavailable.

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 policies or practices governing

Doc Rev

Dir Obs

Intvw

- ☐ facility access and egress of persons, information, equipment, and property

  Doc Rev

  Dir Obs

  Intvw

- ☐ the scaling of these practices to the organization's assessed risk and threats relevant to a facility and its personnel

  Doc Rev

  Dir Obs

  Intvw

- ☐ physical access to different sections of a facility according to employee group based on need and qualification

  Doc Rev

  Dir Obs

  Intvw

- ☐ physical access of non-employees to the facility

  Doc Rev

  Dir Obs

  Intvw

Level 3

☐ The organization implements and tests its physical security policies and practices.

Doc Rev

Dir Obs

Intvw

☐ The organization considers insider threat risks to facilities as part of its risk management activities.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization trains employees on the policies and procedures related to the protection of facilities and their obligations to comply.

Doc Rev

Dir Obs

Intvw

☐ The organization documents how employees are trained, tested, and monitored for compliance.

Doc Rev

Dir Obs

Intvw

☐ The organization has a plan to augment policies during emergencies to cope with increased threats to physical facilities.

Doc Rev

Dir Obs

Intvw

☐ The organization can show how the policies extends to the protection of personnel and resources outside of its facilities.

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 # HR1.21: Good-Conduct Policy

The organization has a good-conduct policy that allows it to terminate an employee for major legal violations or personal acts outside of work that present insider risk factors or tarnish the reputation or credibility of the organization.

Clarification/Intent

Some employee acts outside of work are associated with insider risk factors, such as

- poor judgment
- lack of personal ethics or behavioral control
- close associations with individuals who have a known criminal or adversarial affiliation
- other risk indicators

When these insider risks are found, the organization should be able to sever its relationship with the employee without being constrained by contractual or other obligations.

Assessment Team Guidance

The policy should give the organization the option to terminate the employee for insider risk behaviors outside of work that involve criminal acts or significant ethical violations, or for scandalous personal behavior that reflects poorly on the organization.

In light of recent Equal Employment Opportunity enforcement guidance, employers should consider business justifications and the specific circumstances of the violation when they weigh arrests and convictions in decisions about employment.

MERIT Example

The insider, a contractor, was formerly employed as a consultant to the victim organization, a medical supply facility. The insider, who owned a consulting firm with a partner, was hired to set up networks at the organization. While working for the victim organization, the insider was observed probing its network, but no disciplinary actions were taken. One of the victim organization's clients also reported that insider was gathering information about him. The insider was bought out of the consulting partnership due to drug use. After the partnership dissolved, the insider threatened to get revenge against his former partner. At the time of the incident, the insider's former partner was employed as an information systems manager at the victim organization. Over the course of a month, the insider used unauthorized remote access to attack the organization. The insider installed remote control applications (PC Anywhere), deleted and modified data, and changed administrative passwords to prevent access to the network. The insider also copied files from his previous partner's business. The incident was detected when the organization discovered that server passwords had changed. Remote access logs and ISP logs connected the insider to the incident. The insider was arrested and convicted, but committed suicide prior to his sentencing.

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 good-conduct policy.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization can terminate an employee for criminal violations outside work or acts outside work that discredit the organization, in compliance with all applicable laws and regulations.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization considers business justifications and the specific circumstances of the violation when they weigh arrests and convictions in decisions about employment.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization sponsors education or training programs for employees regarding the policy and practices.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Employees involved in these types of terminations have received training on how to do so in accordance with organizational policy and legal rules and regulations.

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 # HR1.22: Employee Benefits & Compensation

The organization has published policy describing how it determines employee benefits and compensation and how it communicates any changes.

Clarification/Intent

The organization has clear, specific, and published rules for evaluating and making decisions about promotion, demotion, and assigning compensation and benefits. Employees acknowledge these rules, such acknowledgment is documented, and adherence to the rules is recorded. Employers should ensure this information is easily available to all employees and any changes are communicated.

Assessment Team Guidance

A significant number of insider actions appear motivated by insiders' perception of injustice regarding compensation, promotion, and benefits.

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 of 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 published policies for evaluating and making decisions about promotion and demotion.

Doc Rev

Dir Obs

Intvw

☐ The organization has published policies for evaluating and making decisions about assignment of compensation and benefits.

Doc Rev

Dir Obs

Intvw

☐ The organization communicates any changes or updates to promotion and demotion policies at least annually.

Doc Rev

Dir Obs

Intvw

☐ The organization communicates any changes or updates to employee benefits and compensation at least annually.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization obtains employees' acknowledgment of the policy and practices across all areas of compensation, advancement, and benefits.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization sponsors employee education or training programs regarding the policy and practices.

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 # HR1.23: Employee Assistance Programs

The organization provides access to employee support services.

Clarification/Intent

The organization has services, policy, and procedures to assist employees and their families with personal, psychological, financial, legal, and other stressors that have been related to insider risk. These services, policy, and procedures are accessible to employees and include provisions for privacy, voluntary and involuntary referral, and referral by others. The organization should provide procedures describing access to and benefits of employee assistance programs and other employee support services.

Assessment Team Guidance

According to CERT research on the personal predispositions of insiders, a significant percentage of insiders suffer from problems related to physical health, mental health, financial matters, legal matters, or related problems that increased their risk of insider activity. Internal mechanisms and services for identifying and addressing these risks can reduce the probability of insider attacks.

The organization can provide these services either internally or through its benefits program to address problems associated with known insider risks, including problems with physical health, mental health, and financial matters. If it does not provide them itself, it is still acceptable and meeting the intent of the capability if the services are provided externally but the access and support comes from within the organization.

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 sanctions and supports employee use of employee assistance programs and related services.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has in place or makes available an employee assistance programs and/or related services.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization communicates information about the available services to the employees.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization makes electronic or hardcopy information on the services easily available to employees.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization provides clear procedures for employee access to these programs.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization provides training to managers and supervisors on the available services and employee assistance program and how to help employees get access to such services.

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 # HR1.24: Insider Threat Security Awareness Training

The organization has policy and practices mandating initial and ongoing information security awareness training relevant to insider risk.

Clarification/Intent

The organization provides employees at all levels with security awareness training. This training considers the organization's specific risk environment context, specific insider risk history, and the full range of insider policies and practices aimed at preventing, deterring, detecting, and managing insider risk.

Assessment Team Guidance

Security awareness programs should not be overly general. They should be based on organization-specific insider risks presented or experienced and the organization's risk or threat environment. They should be appropriately structured for the needs of different employee groups and updated according to new information or conditions. The training programs should require attendees to demonstrate some level of competence in the course content as a condition for continued employment. In addition, a program-effectiveness evaluation and feedback mechanism should be in place that can lead to program changes.

Information security policy encompasses

- acceptable use
- password policy
- reporting vulnerabilities, suspicious emails, and other security concerns

MERIT Example

The insider was employed as a product engineer by the victim organization, an automobile manufacturer. As a function of his job, the insider had access to the organizations' trade secrets and design specification documents. 2 years prior to leaving the organization, the insider downloaded a sample of the victim organization's trade secrets, specifically design specification documents. The insider used this information to aid him in acquiring employment with a foreign competitor. A year and a half later, the insider accepted a job offer from a U.S. based company that manufactured automotive electronics in China, the primary beneficiary organization. The acceptance took place 2 months before the insider officially left the victim organization. The night prior to leaving the victim organization, the insider downloaded 4,000 documents onto an external hard drive, including sensitive design documents. The insider downloaded design specifications for the engine/transmission mounting subsystem, electrical distribution system, electric power supply, electrical subsystem and generic body module, etc. The documents were valued at $24-$32 million. The majority of these documents were not related to the insider's job. The insider traveled to the primary beneficiary organization in China. 2 weeks later, the insider submitted his resignation via e-mail. Subsequently, the insider began working for the primary beneficiary organization. 15 months later, the insider began working for the victim organization's direct foreign competitor, the secondary beneficiary organization. 9 months later, the insider returned to the U.S. and was arrested at the airport. The insider was convicted and is awaiting sentencing in February 2011. At the time of his arrest, the insider was carrying a laptop he acquired from the secondary beneficiary organization. A forensic examination of the laptop revealed that the insider had stolen thousands of confidential, proprietary documents from the victim organization and another unnamed organization. The insider was arrested and convicted, and sentenced to 70 months imprisonment, 2 years of supervised release, and fined $12,500. The victim organization did take steps to protect the system design specification documents, including maintaining unspecified security features on site. With respect to electronic information, the victim organization provided training to employees on information security measures, required the execution of non-disclosure agreements, and marked documents according to information protection policies. The insider had signed an employee agreement, in which he agreed that he would not disclose the victim organization's proprietary information or retain copies of the information after the termination of his employment. The insider was reminded of this obligation when he resigned.

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 mandating initial and ongoing information security awareness training related to insider risk.

Doc Rev

Dir Obs

Intvw

☐ The organization has a security awareness training program that

Doc Rev

Dir Obs

Intvw

- ☐ is based on the specific level of threat to employees and the organization

  Doc Rev

  Dir Obs

  Intvw

- ☐ accounts for the organization's actual experience with insider risk

  Doc Rev

  Dir Obs

  Intvw

- ☐ is appropriately structured for different employee groups

  Doc Rev

  Dir Obs

  Intvw

Level 3

☐ The organization has a security awareness training program that is modified or updated according to new information or developments.

Doc Rev

Dir Obs

Intvw

☐ The organization has a security awareness training program that requires attendees to demonstrate their competence in the material presented.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has a security awareness training program that is evaluated for effectiveness.

Doc Rev

Dir Obs

Intvw

☐ The organization has a security awareness training program whose evaluation measures are used as feedback to modify the training.

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 # HR1.25: Rewarding Employees for Good Behaviors

The organization has personnel policy and procedures for rewarding and increasing loyalty and personnel security while reducing the risk of insider activity.

Clarification/Intent

Organizations may reduce insider risk by rewarding employees for

- periods without security or other risk violations or indicators
- ideas on improving personnel security

Organizations may also improve loyalty by providing rewards for tenure or by providing shared profits such as stock options or profit-sharing accounts.

Assessment Team Guidance

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.

Level 2

☐ The organization has policy or practices that meet ANY TWO of the following:

Doc Rev

Dir Obs

Intvw

☐ reward employees for good security behavior

Doc Rev

Dir Obs

Intvw

☐ reward employees for ideas on improving security

Doc Rev

Dir Obs

Intvw

☐ increase employee investment in successful organizational performance

Doc Rev

Dir Obs

Intvw

☐ encourage employees to stay in the organization

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization has policy or practices that meet ANY THREE of the following:

Doc Rev

Dir Obs

Intvw

☐ reward employees for good security behavior

Doc Rev

Dir Obs

Intvw

☐ reward employees for ideas on improving security

Doc Rev

Dir Obs

Intvw

☐ increase employee investment in successful organizational performance

Doc Rev

Dir Obs

Intvw

☐ encourage employees to stay in the organization

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has policies or practices that meet ALL of the following:

Doc Rev

Dir Obs

Intvw

☐ reward employees for good security behavior

Doc Rev

Dir Obs

Intvw

☐ reward employees for ideas on improving security

Doc Rev

Dir Obs

Intvw

☐ increase employee investment in successful organizational performance

Doc Rev

Dir Obs

Intvw

☐ encourage employees to stay in the organization

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 # HR1.26: Identifying High-Risk Employees

The organization has policy, procedures, and personnel for identifying and evaluating employees at risk for insider actions, prior to management intervention up to and including termination.

Clarification/Intent

The organization should have policy, procedures, and trained personnel that can

- identify employees who are at risk before managerial interventions that could cause negative employee reactions and increase insider risk
- show coworkers and supervisors how to deal with identified at-risk colleagues across a range of scenarios
- refer these at-risk employees facing negative personnel actions to appropriate teams for evaluation; these teams should
- include human resources, legal, employee assistance program, physical and IT security, and behavioral science members who can evaluate the risk of insider espionage, sabotage, and theft, as well as interpersonal risks such as violence and harassment
- be trained, exercised, and prepared to execute such assessments
- have established relationships and liaisons with members of law enforcement, the judiciary, specialized medicine, social services, and other community groups whose assistance and collaboration may be important for case management
- be supported by policy and practices to implement team recommendations and reduce identified risks

Assessment Team Guidance

The results of research on insider threats show that the risk of insider acts prior to management intervention is greatly underappreciated. Consistent with this concern is the finding that a significant number of insider acts occur after some type of escalation with management or an intervention attempt by management. For example, the number of insiders who attacked their organization after termination was highly significant. Employee disputes over salary, IP ownership, and promotion can also increase insider risk and merit investigation and assessment.

MERIT Example

The insider, a contractor, was formerly employed as a helpdesk and network technician by the victim organization. While working for the company, the insider had superuser and remote access to the network, in order to perform maintenance and to troubleshoot problems from home. The insider was a temporary employee hoping to be hired into the organization full-time, but his application for full-time employment was rejected. The insider had received a poor performance review from his supervisor, who characterized the insider as not a team player, volatile, angry, and inflexible on issues. The insider, who was trying to gain full custody of his daughter, also had financial issues. Due to cutbacks at the organization and rules surrounding temporary employment, the insider was informed that his employment would be terminated in 2 months. After learning of his pending termination, the insider wrote several threatening emails to the organization's human resources (HR) department, specifically threatening to sue the organization for unfair labor practices. As a result of the e-mails, the insider was immediately terminated. The insider had also installed backdoors into the organization's network. The insider used a generic administrative login and password and remote access channels to dial-in to the organization's network. The insider removed access to systems, changed administrative passwords, deleted system event logging, and modified accounts associated with individuals who were involved with his termination. The insider's actions were discovered the following day when employees could not enter the system. The insider failed to delete all logs that connected him to the incident. The insider admitted responsibility for the incident, acknowledged that he made a mistake, and wanted to help minimize damages. Additional details regarding the outcome of the case are unknown. The organization's incident related loss was $5,000.

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 tries to actively identify at-risk employees before management interventions that might cause negative employee reactions and increase insider risk.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has practices or guidance in place to actively identify at-risk employees before management interventions that might cause negative employee reactions and increase insider risk.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has practices or guidance in place for referring these at-risk employees facing negative personnel actions to appropriate teams for evaluation.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has policies or standardized processes in place to address at-risk employees.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has documented procedures for identifying at-risk employees and referring them to appropriate teams for evaluation.

Doc Rev

Dir Obs

Intvw

☐ The organization has teams that

Doc Rev

Dir Obs

Intvw

- ☐ include human resources, legal, employee assistance program, physical and IT security, and behavioral science members who can evaluate the risk of insider espionage, sabotage, and theft as well as interpersonal risks such as violence and harassment

  Doc Rev

  Dir Obs

  Intvw

- ☐ are trained, exercised, and prepared to execute such assessments

  Doc Rev

  Dir Obs

  Intvw

- ☐ have established relationships and liaisons with members of law enforcement, specialized medicine, social services, and other community groups whose assistance and collaboration may be important for case management

  Doc Rev

  Dir Obs

  Intvw

- ☐ are supported by policy and practices to implement team recommendations for reducing identified risks

  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 # HR1.27: Notification of Employee Status Change

The organization has a means of notifying data owners, IT security, physical security, and other concerned departments when an employee's change in position impacts his or her access to IT and physical assets.

Clarification/Intent

The organization should communicate to ensure that an employee's access to IT and physical assets are disabled or granted as appropriate to that employee's change in position or status influencing his or her access.

Assessment Team Guidance

Notification should also include discussion of relevant aspects of an employee's work history and any other aspects that may pertain to the new position. For example, if an employee no longer needs access to a specific building, then physical security should be notified so they can terminate the employee's access rights to that building.

MERIT Example

The insider, a foreign national, worked as a programmer for 4 years at a domestic banking and finance institution. Prior to her termination, she was reprimanded for poor performance and a negative attitude. Coworkers complained that she stated that "something's going to explode", that she would disrupt the whole group, and that she would make her manager's life miserable. Eventually, the organization fired the insider and immediately escorted her out of the facility. Later that night, she called the third-shift help-desk and requested that they reset her remote login credentials. The help desk employee recognized her voice and was not informed of her earlier termination, so he complied. Once she regained her remote access ability, she accessed the organization's network three times between 1:00 AM and 7:00 AM and deleted files and propriety source code from the network's servers. Once the next workday started, the organization's network staff detected the absence of the source code and used log files to discover the insider's malicious activities. The insider later admitted to her activities, which cost the organization $15,000. The insider was sentenced to two years of probation, mandatory mental health treatment, and ordered to pay full restitution and a $500 fine.

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 notifies data owners, IT security, physical security, and other concerned departments when an employee's change in position impacts his or her access to IT and physical assets.

Doc Rev

Dir Obs

Intvw

☐ The organization has a documented policy requiring a transferring employee's previous department to discuss pertinent employee history.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization has a standardized process and mechanisms in place to notify data owners, IT security, physical security, and other concerned departments when an employee's change in position impacts his or her access to IT and physical assets.

Doc Rev

Dir Obs

Intvw

☐ The organization discusses pertinent employee history (e.g., performance reviews, disciplinary actions) with the employee's new department.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has documented procedures for interdepartmental communication when an employee transfers roles.

Doc Rev

Dir Obs

Intvw

☐ The organization provides training to involved stakeholders on the process for notification of employee position changes.

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 # HR1.28: Insider Threat Risk Evaluation Teams

The organization has policies, practices, and/or multidisciplinary groups assigned to plan and assess the range of risks associated with employee terminations, layoffs, and other exits as well as major organizational changes such as reorganizations, mergers, acquisitions.

Clarification/Intent

Termination planning is essential to reducing insider risk because terminated employees are among the most at risk for insider acts.

Policies and practices should document the reasons for termination, communicate the termination to concerned departments, and address insider risk issues common to this group of departing employees. In addition, policies and practices should address the possible increased insider risk across the workforce during organizational changes such as reorganizations.

Assessment Team Guidance

Policies and practices regarding individual risk should encompass

- screenings for insider risk indicators of sabotage, espionage, and violence
- communication of IP and confidentiality requirements with departing employees
- potential communications between the employee and competitors and other insider risk behaviors, especially copying IP, downloading IP, or other efforts to acquire IP prior to departure
- means to monitor the activities of at-risk employees for violations of agreements after departure
- coordination of digital, physical, and personnel access control during and after the termination period
- special risks associated with groups of formerly associated employees leaving around the same time and with undisclosed or deceptive plans
- communication of how current employees should respond to requests from terminated employees
- assurance that employees terminated for cause do not successfully reapply to the organization under any name

Another thing to consider when making organizational changes is how employees who are leaving and those who are staying in the organization both affect insider risk.

MERIT Example

In response to an uncharacterized dispute, the employer suspended the insider's security access. The insider's employer failed to notify the victim organization of the suspension, and the insider's physical security clearance was not removed. 6 days later, on a Sunday evening, the insider attempted an unsuccessful remote attack against the victim organization's data center. Later that night, the insider, using a security card key and biometric hand reader, gained access to the victim organization's facility. The insider used a hammer to break glass and hit an "emergency power off button," shutting down computer systems, including computers that regulate the exchange of electricity between power grids in the western United States, for approximately 2 hours. The shutdown denied the victim organization access to the energy trading market, but did not directly affect the transmission grid. While at the facility, the insider encountered another contract employee and attempted at least twice to log on to the victim organization's systems. The day following the shutdown, the insider emailed a bomb threat to his supervisor. The email prompted the evacuation of 500 employees for 6 hours. To restore the system, the victim organization had to transfer control to another facility and utilize 20 computer specialists for approximately 7 hours. Employee security access codes as well as computer access, system, and video surveillance logs were used to identify the insider. The insider was arrested, convicted, ordered to pay sentenced $34,000 restitution, and sentenced to 6 months of house arrest and 5 years of probation.

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 and procedures for complete risk assessment and planning that cover individual exits and terminations as well as major organizational changes.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization can demonstrate its adherence to the above guidelines.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has teams that

Doc Rev

Dir Obs

Intvw

☐ include human resources, legal, employee assistance program, physical and IT security, and behavioral science members who can evaluate the risk of insider espionage, sabotage, and theft as well as interpersonal risks such as violence and harassment

Doc Rev

Dir Obs

Intvw

☐ are trained, exercised, and prepared to execute such assessments

Doc Rev

Dir Obs

Intvw

☐ have established relationships and liaisons with members of law enforcement, specialized medicine, social services, and other community groups whose assistance and collaboration may be important for case management

Doc Rev

Dir Obs

Intvw

☐ are supported by policy and practices to implement team recommendations for reducing identified risks

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 # HR1.29: Employee Screening Updates

The organization periodically updates and reapplies important employee screening measures to warn of any increase in an employee's insider risk factors.

Clarification/Intent

Although new hires may be subject to rigorous screening, the personal and professional lives of employees may change after they are hired. Employee disgruntlement and corresponding insider risk can arise from personal and professional developments as well as outside influence. Employee vulnerability to psychological, medical, financial, social, and other stressors should be reevaluated regularly after hiring.

Assessment Team Guidance

Periodic reevaluation may include screenings for

- criminal activity
- civil violations or lawsuits
- medical problems such as substance abuse
- conflicts of interest
- financial behavior such as credit issues or financial abuses at work
- misuse of IT resources
- reports of interpersonal problems

MERIT Example

The insider was employed as a network administrator by the victim organization, a manufacturer of measurement and control devices. Prior to and at the time of the incident, the organization was going through a major expansion; the insider was not interested in expansion. Prior to the incident, the insider had been promoted to management. After his promotion, the insider was reprimanded twice for bad behavior and subsequently demoted. The insider behaved aggressively and abusively toward his coworkers by purposely bumping into people and downplaying their achievements, bragging about his own abilities, taking credit for others' work, bottlenecking projects, and loading faulty programs to make others look bad. The insider stole the organization's equipment for personal use and also ran a side business. Prior to his termination, the insider interviewed with competitor companies. The insider also systematically centralized the critical manufacturing programs for one of the organization's plants to prepare for the release of a logic bomb. The insider tested the logic bomb on the system 3 times. After his termination, the insider set up the logic bomb to execute 21 days later. The logic bomb, designed to execute at first login, used an unauthorized account to delete many crucial programs that the plant relied on for its manufacturing process. Although the malicious software was never found, reformatted backup tapes and malicious programs were found in the insider's possession. The organization's damages were estimated at $10 million. The insider was arrested, convicted, and sentenced to 41 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 a policy governing the updating and reapplying of employee screening measures.

Doc Rev

Dir Obs

Intvw

☐ The organization performs reevaluations of screening measures, as appropriate.

Doc Rev

Dir Obs

Intvw

☐ The organization updates employee information in areas of concern including

Doc Rev

Dir Obs

Intvw

- ☐ criminal and civil litigation or procedures

  Doc Rev

  Dir Obs

  Intvw

- ☐ substance abuse

  Doc Rev

  Dir Obs

  Intvw

- ☐ financial or credit status

  Doc Rev

  Dir Obs

  Intvw

☐ conflicts of interest

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization has a standardized process in place for performing employee screening reevaluations and updating areas of concern.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The trains assigned staff on how to conduct employee screening re-evaluations.

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 # HR1.30: Insider Threat Incident Review

The organization performs incident review and lessons-learned evaluations following reports of significant insider violations.

Clarification/Intent

The organization engages groups from across the enterprise to diagnose and address insider vulnerabilities revealed by insider incidents.

Assessment Team Guidance

Representatives across organizational departments should participate in investigations of insider incidents, which should examine individual case facts and the organization's relevant policy, practices, data, and processes in order to discover vulnerabilities that could be addressed and mitigated.

MERIT Example

The insider was formerly employed as a supervisor in the internet technology (IT) department of the victim organization, an educational institution. The organization terminated the insider's employment after numerous violations of the organization's conduct policy. A few hours after his termination, the insider used another employee's credentials to remotely access the organization's fiscal computer. For over 2 months, the insider continued to remotely access and delete records from this computer. An internal audit detected the incident and the insider was connected to the incident through his IP address. The insider was arrested, convicted, and sentenced to an alternative rehabilitation program.

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 informal process for performing multidisciplinary reviews of significant insider incidents, including evaluation of lessons learned and mitigation of related insider vulnerabilities.

Doc Rev

Dir Obs

Intvw

☐ The organization conducts multidisciplinary reviews of significant insider incidents, including evaluation of lessons learned and mitigation of related insider vulnerabilities.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization has a standardized process for performing multidisciplinary reviews of significant insider incidents that includes criteria or definitions to identify "significant" insider incidents (i.e., incidents that should warrant a review and lessons-learned evaluation).

Doc Rev

Dir Obs

Intvw

☐ The organization documents the results from post-incident reviews and lessons learned evaluations to identify potential process changes or controls to mitigate insider vulnerabilities.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization tracks and acts upon the feedback from post-incident reviews and lessons learned evaluations to improve their processes or mitigate insider vulnerabilities in the future.

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)