Carnegie Mellon University
Software Engineering Institute

Insider Threat Vulnerability Assessment (ITVA)

Information Technology 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 assessment was designed to be completed over a period of three weeks. Week one is the pre-assessment week, where assessment team members review organization-supplied documents to become familiar with organization practices and policies. During week two, the assessment team spends three to five days onsite at an organization. During that time, the assessment team reviews documents, interviews key personnel, and observes processes to substantiate each capability. During the final week, the assessment team prepares an insider threat vulnerability assessment final report, describing how prepared an organization is to prevent, detect, and respond to insider threats.

The purpose of the information technology (IT) capability area is to determine what countermeasures an organization has in its IT infrastructure to reduce its exposure to insider threat vulnerabilities. The Information Technology area is divided into the following areas of focus:

- Access Control
- Audit and Accountability
- Configuration Management/System and Information Integrity
- Identification and Authentication
- Incident Management
- Personnel Termination
- System and Communication Protection

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

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 # IT1.1: Unauthorized Creation of Accounts

The organization has controls to prevent, detect, and respond to the unauthorized creation of accounts permitting access to IT systems.

Clarification/Intent

The organization prevents, detects, and responds to the unauthorized creation of various types of accounts for access to IT systems. These account types may include, for example

- VPN
- shared
- privileged
- DBA
- customer
- partner
- other user
- system
- training
- testing

Assessment Team Guidance

Many insiders created back door accounts, such as VPN, testing, training customer, and partner accounts to set up and conduct their attacks. The controls should address:

- unauthorized accounts created for existing employees but used by someone other than the account owner
- unauthorized accounts created but not intended for an existing employee
- unauthorized generic accounts, as well as application and service accounts, such as email clients and server software

MERIT Example

The insider was employed as an information systems consultant by the victim organization, a manufacturer of pet products. Over 16 months, while on site and during work hours, the insider gained unauthorized access to the organization's computer system on 5 occasions. The insider used the password cracker software 'L0phtCrack' to retrieve 5,000 passwords for user accounts on the system. The insider created a database containing user account passwords and stored it on the organization's server and on his company-issued laptop. The insider also ran one password-recovery utility program (pwdump.exe) and stored the results (i.e. retrieved passwords) in a ZIP file. The insider installed the 'pwdump.exe' program on the organization's system and on his company-issued laptop. The insider used a dial-up connection to remotely access the organization's computer systems and create an unauthorized administrator account. The incident related impact was $10,000, the organization's cost of assessing the damaging, verifying system security, and restoring integrity to its computer systems. The insider was arrested, convicted, ordered to pay $10,000, and sentenced to 3 years' probation and 250 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 a documented policy for the development of enterprise accounts.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization requires continuous monitoring of account creation activity.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization requires a response plan for handling unauthorized accounts.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization responds to unauthorized creation of accounts.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has documented procedures for account management that include separating the duties of authorizing accounts and creating accounts.

Doc Rev

Dir Obs

Intvw

☐ The organization requires account creation standards such as naming convention and appropriate attribute values such as location, phone number, allowed remote access, and group membership.

Doc Rev

Dir Obs

Intvw

☐ The organization requires no use of anonymous accounts.

Doc Rev

Dir Obs

Intvw

☐ The organization has documented procedures that address the creation of privileged accounts.

Doc Rev

Dir Obs

Intvw

☐ The organization has documented procedures that address the creation of VPN accounts.

Doc Rev

Dir Obs

Intvw

☐ The organization has documented procedures that address the creation of contractor accounts.

Doc Rev

Dir Obs

Intvw

☐ The organization has documented procedures that address the creation of shared accounts.

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 # IT1.2: Shared Accounts

The organization controls shared system accounts.

Clarification/Intent

The organization should be able to prevent, detect, and respond to the unauthorized sharing of shared accounts and control the use of authorized shared accounts.

Consider all user, service, and collaborative application accounts, both built-in and user defined.

Assessment Team Guidance

Many insiders have been able to obtain access to shared accounts without the knowledge or approval of the organization and use those accounts to carry out their attacks. There should be processes for :

- tracking employees who have authority to use each shared account
- periodically assessing the continuing need for all shared accounts

MERIT Example

The insider was employed as a supervisory clerk by the victim organization, an administrative court system. The insider and a relative developed a scheme to adjust official records, specifically erasing driving offenses and related fines, in exchange for compensation. The outsider, who had a criminal history and an intimidating demeanor, recruited participants who wanted driving record modifications. Over 18 months, while on site and during work hours, the insider corrupted over 100 driver records by creating false documents and altering electronic court records. The insider used a shared password and identities of several other employees to make changes. The insider was in an accident and modified her own driving record. The organization discovered discrepancies in this record, and an investigation revealed online and offline records connecting the insider to the incident. The insider was arrested, convicted, and sentenced to 3 years imprisonment followed by 4 years of probation. The insider was apparently motivated by financial difficulties; she lived beyond her means and her husband had recently lost his job.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

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

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has a documented policy for creation and use of shared accounts across all system types and levels for enterprise accounts.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented policy for creation and use of shared accounts across all system types and levels for user-generated (not system-generated) accounts.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization detects unauthorized attempts to use shared accounts.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization authorizes, creates, and retires (disables and deletes) shared accounts, consistent with existing policy.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has technical controls to trace all actions performed using shared accounts to the responsible individual.

Doc Rev

Dir Obs

Intvw

☐ The organization tracks and audits who is authorized to use a shared account.

Doc Rev

Dir Obs

Intvw

☐ The organization responds to unauthorized uses of a shared account.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization implements controls for shared account usage, such as a procedure for revoking an entity's right to use the account.

Doc Rev

Dir Obs

Intvw

☐ The organization has technical controls to prevent unauthorized use of shared accounts (e.g., changing passwords regularly, RSA secure ID).

Doc Rev

Dir Obs

Intvw

☐ The organization limits the distribution of credentials for default and built-in accounts.

Doc Rev

Dir Obs

Intvw

☐ The organization observes vendor and industry best practices related to safeguarding default and built-in accounts, such as recommended password policy and naming conventions.

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 # IT1.3: User Attribution

The organization attributes all system activities to individual employees.

Clarification/Intent

The organization should be able to hold users accountable for their actions and track system activities to specific individuals or other entities. Such controls should provide minimal opportunity for repudiation of one's actions

Assessment Team Guidance

Many insiders have been able to avoid detection of malicious activities by using shared accounts, which meant their actions could not be attributed to an individual employee in the organization. The controls should address:

- the use of shared roles and accounts, such as system administrator, DBA, testing, and training
- shared accounts on external systems, such as customer systems
- business partners and directly associated individuals of the partner organization who have authorized access

MERIT Example

The insider used previously stolen identification to get a job at as a data entry clerk/patient account representative for a healthcare billing company. The insider had a previous record of identity theft and identity forgery, but this was not known to her employer. Over the course of four months, she stole personally identifiable information (PII) of approximately 1,200 different patients. She was then able to make purchases using the identities of these patients. The incident was discovered when the victims reported that their identity had been stolen, and law enforcement officials were able to trace back the victims to the same medical billing company. While investigating the company, they were able to attribute the crime to the insider since she was documented to have managed the compromised accounts, and partially due to her history of identity theft.

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 for attribution of activities on critical systems for individual user accounts.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented policy for attribution of activities on critical systems for shared accounts.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization limits the use of default and built-in privileged accounts (i.e., administrator or root) for normal system activities.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization implements granular system auditing that logs not only user account and resources accessed, but also the physical and/or logical location of access attempts (MAC and IP addresses), point of logical system entry (router, VPN, or firewall ID), workstation ID, date, and time.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization institutes a policy prohibiting business partners and customers from using assigned accounts for multiple individuals in their employ.

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 # IT1.4: Expired/Dormant Accounts

The organization manages expired and dormant accounts.

Clarification/Intent

The organization should have controls defining what constitutes expired and dormant accounts and how such accounts should be handled.

Consider the following types of accounts:

- user
- service
- customer
- training
- test

Assessment Team Guidance

Many insiders have exploited expired or dormant computer accounts to set up or carry out their attacks. The controls should address:

- training accounts that are no longer needed
- computer accounts used by customers
- computer accounts used for testing

MERIT Example

The insider was a former student at a public school district. During his time as a student, he shoulder-surfed the password of a school employee who had a privileged account. A few years later, the former student was able to log into the administrative system of the school district using the stolen credentials, which had not expired. The school's information system was hosted by a third party, who hosted many of the information systems of the public school districts in that same area. The insider then used the compromised account to log into the payroll information system of another school district, at which point he stole personally identifiable information (PII) of approximately 5,000 current and former district employees. Using the stolen identities, he started applying for fraudulent credit cards and make fraudulent checks. He was caught when the rightful owners of the stolen identities began noticing strange account activity occurring in their names. The insider was finally arrested at a store where a clerk had noticed that a check he had tried to cash was fake. The former student was sentenced to 10 years in prison for 1st degree computer trespassing, identity theft, forgery, and an unrelated count of drug possession.

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 definition of what is considered a dormant account.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a policy that requires that all accounts be associated with active employees, contractors, or business partners.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented procedure for how dormant accounts should be handled for enterprise accounts.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented procedure for how dormant accounts should be handled for department accounts.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has procedures for controlling accounts of suspended and terminated employees and contractors.

Doc Rev

Dir Obs

Intvw

☐ The organization has procedures for controlling accounts of rotating contractors.

Doc Rev

Dir Obs

Intvw

☐ The organization has procedures for controlling accounts used for testing purposes.

Doc Rev

Dir Obs

Intvw

☐ The organization has procedures for controlling accounts used for training purposes.

Doc Rev

Dir Obs

Intvw

☐ The organization has procedures for controlling accounts of application services (or application-level accounts).

Doc Rev

Dir Obs

Intvw

☐ The organization has implemented a procedure outlining when and how to disable and delete accounts.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization performs account auditing to detect dormant accounts.

Doc Rev

Dir Obs

Intvw

☐ The organization performs account auditing to detect unauthorized accounts.

Doc Rev

Dir Obs

Intvw

☐ The organization performs account auditing to detect expired accounts.

Doc Rev

Dir Obs

Intvw

☐ The organization performs account auditing to detect last log-on date.

Doc Rev

Dir Obs

Intvw

☐ The organization is able to detect attempted use of dormant or expired accounts.

Doc Rev

Dir Obs

Intvw

☐ The organization tracks the usage of testing and training accounts including assigning accountability.

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 # IT1.5: Critical Task Separation

The organization ensures that critical tasks are not completed by a sole individual without the appropriate level of checks and balances.

Clarification/Intent

The organization has one or more mechanisms to ensure that critical tasks are not completed by a single employee without the appropriate level of checks and balances to protect against abuse.

The organization identifies and mitigates risk to critical functions by separating duties and/or using other internal administrative, technical, and physical controls.

Assessment Team Guidance

Many insiders have been able to commit their crimes because a second person was not involved in the approval or management of a business process or application. The controls should:

- address separation of duties in the creation of new payees and the approval of payments
- address separate roles for the development or change of software and the approval for release of software versions
- address the possibility of one person gaining exclusive control over critical systems and/or information, thereby increasing the risk of fraud, extortion, IT sabotage, or revenge
- provide a mechanism of "checking the checker" to detect potential collusion between employees
- provide a means for exception handling in applications and in business processes
- be easily overridden in emergency and crisis situations

MERIT Example

The insider was employed as a network administrator by the victim organization, an IT department for a government entity. The insider, who built the organization's network, was the only person with the passwords to the network as well as true knowledge of how the network functioned. The insider refused to allow or authorize the addition of any new administrators. The insider was reprimanded for poor performance. After being confronted by and subsequently threatening a coworker, the insider was reassigned to a different project. The insider refused to give up the passwords, was subsequently terminated, and arrested. The City was locked out of its main computer network for 12 days. The insider's colleagues discovered that the insider had installed rogue access points in hidden closets, and had set up the organization's system to fail if anyone attempted to reset the system without the proper passwords. The insider provided passwords to police, but none of them worked. The insider later relinquished the passwords in a secret meeting with a city official, who was the one person the insider trusted. The insider defended his actions, claiming that they were in line with standard network security practices. The insider was convicted, sentenced to 4 years imprisonment, and is awaiting a financial penalties hearing. The organization's incident related loss was $200,000 - $900,000. The insider had a prior conviction for aggravated robbery, which occurred 24 years prior to the incident.

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 and procedures for ensuring that employees do not have exclusive ability to access and modify critical information.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has documented policies and procedures for ensuring that employees do not have exclusive ability to perform system activities and functions in financial areas such as sales, payroll, and other accounting processes.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has documented policies and procedures for ensuring that employees do not have exclusive ability to perform software development and quality assurance activities and functions.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has documented policies and procedures for ensuring that employees do not have exclusive ability to perform critical system configuration activities and functions.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has defined change and configuration management processes that check for appropriate separation of duties (e.g., software tester and developer are not the same person).

Doc Rev

Dir Obs

Intvw

☐ The organization has implemented controls to ensure collusion is required to circumvent basic protection (e.g., need approval to install a patch in a server).

Doc Rev

Dir Obs

Intvw

☐ The organization's separation-of-duties controls provide a means for exception handling in applications and in business processes.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has a process that maintains multiparty controls even when activities may need to be expedited, such as in the case of an emergency or crisis.

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 # IT1.6: Remote Access Paths

The organization controls remote access paths into organization systems, ensuring that only authorized personnel can use them.

Clarification/Intent

The organization controls access paths into the organization's systems and ensures that only authorized personnel can use them. Controls address preventing, detecting, and removing rogue devices, software, and other unauthorized (covert) channels.

Assessment Team Guidance

The controls should

- prevent remote access to organization systems by employees' personal equipment
- address the use of remote access tools, such as PC Anywhere, telnet, and remote desktop

MERIT Example

The insider was formerly employed as a network engineer by the victim organization, an aviation leasing and maintenance company. The insider was terminated for undisclosed reasons. Subsequently, the insider gained unauthorized, remote access to the organization's network and destroyed personnel and payroll records. The organization spent $50,000 to repair the damage. The insider was arrested, convicted, ordered to pay over $1,000 restitution, and was sentenced to 6 months in a halfway house and 6 months of house arrest followed by 4 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 a documented definition of authorized and unauthorized points of remote entry (e.g., VPN, modems, terminal services, remote control tools, FTP, HTTP, email forwarding).

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has mechanisms to control which devices are authorized to connect remotely (e.g., mobile devices).

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization audits and reviews remote access attempts and successes.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has processes in place to respond to remote access attempts and successes.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has controls in place to stop unapproved remote access attempts.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization responds to remote access attempts and successes.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization reviews the continued need for remote access by employees.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has done a formal analysis of which assets should and should not be remotely accessible.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has implemented a practice of vulnerability assessment and penetration testing that includes attempts to uncover unauthorized remote access devices or software.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization trains users about acceptable use of remote access paths.

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 # IT1.7: Workstation Inactivity

The organization has policy and controls for protecting logged-in workstations while the user is not present.

Clarification/Intent

The organization has policies and controls for protecting logged-in workstations while the user is not present.

Controls define how to protect systems physically and technologically from unauthorized access while they are logged in.

Assessment Team Guidance

Many insiders have accessed unattended, logged-in workstations to commit their crimes.

MERIT Example

An assistant circulation manager for a newspaper submitted a resignation letter and subsequently left a very rude voicemail for his direct supervisor. He was terminated for gross insubordination. A few days later, a part-time co-worker let him in the office. Using his own password, he accessed a terminal already logged into by another user and deleted 6 months of critical business records. Co-worker let insider into the office after termination.

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 employs mechanisms that allow users to easily lock their workstations when they are physically, but temporarily, absent.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ User workstations automatically lock after a predetermined period of inactivity not to exceed 30 minutes.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization trains users about acceptable use of employee-assigned equipment, including how authorized users should secure their workstations and account 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 # IT1.8: Personal Devices to Store Sensitive Information

The organization prevents, detects, and responds to employees who use their personal (non-company-owned) computers or devices to store confidential organization information.

Clarification/Intent

The organization has implemented an acceptable-use policy, restrictive controls, and mechanisms to detect employees who use their personal computers or devices to store confidential organization information.

Assessment Team Guidance

Some insiders used their own personal computers or devices to store confidential information when committing a crime. The controls should protect against the:

direct connection of personal computers or devices to organization systems

- emailing of the organization's information to an employee's home computer

MERIT Example

Insider was talking with a competitor company during the time that he was illegally downloading proprietary information from his work computer. It is currently unknown if the two incidents are related. Insider was stealing "alpha" info, or proprietary information, by configuring a virtual machine to bypass company security protocols. It is believed that he was using this "alpha" info to have an insider edge on trading. Insider was also downloading certain programs which is in violation of company policy. In addition, insider encrypted information and created passphrases only know to himself. He uploaded hundreds of files from his company computer onto his phone and an external hard drive. He was detected by the company's IT department because they noticed an unusually large quantity of programs and data associated with his user name. When questioned by management at his company, he lied and against their request also destroyed evidence with the help of Individual A, a friend of his. He has not been sentenced yet.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

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

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has an acceptable-use policy for personal, employee-owned hardware.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization can detect unauthorized systems attempting to connect to its network.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has mechanisms to detect unauthorized mass storage devices connected to its systems

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization documents formal disciplinary actions for unauthorized storage, transmission, and transportation of confidential data.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization responds to the unauthorized transmission or storage of confidential data to personal devices.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization prevents unauthorized systems from connecting to its network.

Doc Rev

Dir Obs

Intvw

☐ The organization has mechanisms to prevent the use of mass storage devices on employee-assigned computers unless the employee's job role is authorized for such use.

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 # IT2.1: Log Retention

The organization has policy and controls governing how long audit logs are kept to support the potential investigation of incidents.

Clarification/Intent

The organization defines what content to log and who has access, and it tracks configuration changes to logs.

Assessment Team Guidance

Some organizations destroyed audit logs that were crucial to prosecuting insider crimes.

MERIT Example

The insider was employed as manager of the IT department at the victim organization, a health care provider. 2 days prior to his resignation, the insider downloaded software and customer data from the organization's network. After his resignation, the insider remotely accessed the organization's network and deleted various items, including backups, server logs, and the human resource (HR) director's email. The duration of the incident was 1 month. Access logs connected the insider to the incident. The insider was arrested, but verdict details were unavailable. Based on the insider's decision to target the HR director's email, the insider presumably had an issue with the HR director, but the motive remains unclear. The insider was considered a good employee, had great performance reviews, and a very high security clearance at the organization.

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 definition of audit log content, including email logs, download logs, critical application logs, critical database logs/transactions (e.g., modification/deletion of data in a database and attribution), other properties such as log size and retention, and the period necessary to support investigations of incidents.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has mechanisms to track audit log configuration changes.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization requires multiparty control to clear logs.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a documented definition of which employees can access audit logs.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has documented procedures for archiving audit logs that include use of write-once media and digital signatures.

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 # IT2.2: Log Review

The organization has policies and controls requiring periodic review of log files.

Clarification/Intent

The organization defines what to audit and monitor and when to review the logs. The organization also has automated alerts for detecting abnormal activity and a response process for addressing abnormalities.

Assessment Team Guidance

Many insider threat cases have involved suspicious or malicious access and changes over long periods that were never caught.

MERIT Example

The insider was formerly employed as a system administrator by the victim organization, a retailer. The insider had resigned from the organization. After his resignation, the insider remotely accessed the organization's computer system to access customer's credit card information to make fraudulent purchases online. To conceal his actions, the insider used a public computer that was intended to be used by job seekers. The incident was detected by one of the victims, a state official, who noticed missing funds from a bank account. System log files were used to connect the insider to the incident. The insider received a 2.5 year suspended sentence. If the insider failed to stay out of trouble, the insider would serve 8 years imprisonment followed by 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 a policy for reviewing log files.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization performs routine log reviews.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented definition of which systems, data, job roles, accounts, and access rights should be subject to auditing and monitoring.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has documented procedures for log review in search of deviations from established baseline of normal or anticipated behaviors.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has mechanisms for log aggregation to uncover trends and anomalies.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented response plan for illicit activity as revealed by log reviews.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization continually enhances auditing processes based on previous illicit activity (e.g., when illicit activity is detected, updating the auditing process to automatically detect that particular type of activity.

Doc Rev

Dir Obs

Intvw

☐ The organization has automated alerts to notify personnel of abnormal activities in excess of established thresholds.

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 # IT2.3: Remote Location Logging & Monitoring

The organization has policies and controls governing logging and monitoring activity on remote connections.

Clarification/Intent

The organization has policies and controls governing logging and monitoring activity on remote connections.

Assessment Team Guidance

Most of the IT sabotage cases were remote attacks, sometimes following the employee's termination, and a significant number of thefts for business advantage were conducted remotely.

MERIT Example

The insider was employed as a support technician for a server hosting company. Approximately one month after leaving the company, the insider began remotely accessing the company's systems and modified the network's configuration to create a backdoor which he could use in the future. Over the course of a month, he was able to continually log in and cause over $5,000 of damage to the systems. He modified log files to conceal his activities but was eventually caught and indicted for computer intrusion. The insider was convicted and sentenced to 54 months imprisonment and ordered to pay $3,000 restitution. (The insider's harsh sentence includes a conviction for possession of child pornography.)

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 for monitoring and logging remote connections.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented definition of which systems and remote access technologies should be audited and monitored.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization audits and logs remote access attempts.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The remote access logs track not only user ID and resources accessed, but also the physical and/or logical location of access attempts (MAC and IP addresses), point of logical system entry (router, VPN, or firewall ID), workstation ID, protocols, date, and times.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization performs routine log reviews to determine if there are any anomalous remote connections, such as VPN connections from foreign countries.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a documented response plan for unauthorized remote connections revealed by monitoring.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization responds to unauthorized remote connections revealed by monitoring.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has automated alerts to notify personnel of abnormal activities in excess of established thresholds, (e.g., anomalous remote connections, such as VPN connections from foreign countries).

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has mechanisms to enforce remote access restrictions and logging requirements technologically.

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 # IT2.4: User Authentication Logging

The organization logs user activity for successful, as well as unsuccessful, user authentications to critical systems.

Clarification/Intent

The organization has controls for logging user activity for both successful and unsuccessful attempts at logging in to critical systems.

Assessment Team Guidance

The pattern of login attempts may be a sign of problems to come. The team should investigate the process for monitoring such logs.

MERIT Example

The insider was an inmate at the victim organization, a prison. The insider was serving time for possession of child pornography. The organization permitted inmates to use computers for legal research. Computers used by the inmates could access only a legal research program, which was updated through CD-ROMs. The computer accessed by the insider was "thin client," meaning that it did not run programs or store data itself, but accessed those programs and data over a network from a central legal research computer server that was stored in another part of the organization. The computer accessed by the insider was connected through the organization's network to the Internet solely so that it could obtain updates for the operating system. The insider discovered and exploited an idiosyncrasy in the legal research software. The insider was able to obtain the username and password to a critical management program. The insider unsuccessfully attempted to log in to that program and also unsuccessfully attempted to send two emails outside of the organization. The insider used the Internet to download two short video files, photographs of 2 organizational employees and 2 fellow inmates, and a publicly available aerial shot of the organization itself. The insider was also able to configure the organization's network to provide himself and other inmates access to additional programs and computer files from the organization's network and to obtain personally identifiable information (PII), regarding 1,100 current and former organizational employees. The insider was also to email his fellow inmates. The incident was discovered when organization personnel discovered a piece of paper containing the username and password for the organization's management computer program. The duration of the incident was 5 months. The insider was convicted and sentenced to an additional 18 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 has a policy requiring logging of successful and unsuccessful login attempts to IT systems.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization performs routine log reviews to determine if there is any anomalous login activity.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has procedures for responding to repeated attempts at unauthorized access by employees.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has formal, defined, and enforced disciplinary actions for unauthorized attempts at gaining access to critical IT systems.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization capturesaccess attempt date and time in logs.

Doc Rev

Dir Obs

Intvw

☐ The organization captures access success or failure in logs.

Doc Rev

Dir Obs

Intvw

☐ The organization captures the system from which the attempt was initiated in logs.

Doc Rev

Dir Obs

Intvw

☐ The organization captures the user account in logs.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has mechanisms for log aggregation to uncover trends and anomalies.

Doc Rev

Dir Obs

Intvw

☐ The organization has automated alerts to notify personnel of abnormal activities in excess of established thresholds of IT system 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 # IT2.5: Unauthorized Use of Accounts

The organization can detect employees' unauthorized use of accounts.

Clarification/Intent

The organization has account creation standards and process for auditing all accounts, including for share accounts.

Assessment Team Guidance

Some insiders have used accounts for which they were not authorized to commit their crimes. The controls should be able to detect:

- the use of expired or inactive accounts
- a newly terminated contractor or subcontractor accessing organization systems

MERIT Example

The insider was originally employed in the human resources (HR) department of the victim organization, an insurance company. A female employee at the victim organization claimed that the insider was harassing her because she rebuffed his romantic advances. The insider was terminated and obtained employment at another organization that was not a competitor to the victim organization. For nearly 5 months, the insider used a password belonging to another employee at the victim organization to remotely access the victim organization's database. The insider used the unauthorized access to delete 800 files relating to the compensation of managing directors and 150 files relating to compensation of other employees. The insider also altered the female employee's compensation record to reflect a $40,000 increase in her salary and a $100,000 bonus. A month later, senior managers at the organization received an email with an attachment containing information from the deleted salary files. The email appeared to have been originally sent from an email account established at hotmail.com that contained the female employee's last name. After the female employee denied establishing the account, a forensic image of the insider's computer at his new employer revealed the source of the emails to the senior managers at the victim organization. The insider was arrested, convicted, ordered to pay $91,000 restitution, and sentenced to 18 months imprisonment followed by 3 years of supervised release. The victim organization expended thousands of dollars to secure its system from future unauthorized access and to re-enter deleted data.

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 account creation standards for naming and attribute values that assist in employee identification, like location, phone number, and group membership.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a process for monitoring and reviewing account activity and inactivity by logging account creation date.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a process for monitoring and reviewing account activity and inactivity by logging account last login date.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization detects and responds to users who attempt to exceed their authorization.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization performs regular account audits to determine if user privileges match job roles. The audit process should address file access privileges, group memberships, and role-based access controls.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The audit process addresses shared accounts, such as
- training accounts
- application-specific accounts
- development accounts
- testing accounts

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 # IT2.6: Abnormal Process Monitoring

The organization audits and monitors for processes that deviate from normal activity.

Clarification/Intent

The organization audits and monitors for processes that deviate from normal performance.

The organization audits and monitors remote access to critical systems or data outside normal business hours.

The organization audits and monitors irregular alterations of data.

Assessment Team Guidance

Some malicious activities involved changes and additions to data that were inconsistent with other data. The controls should be able to detect:

- financial discrepancies that might indicate fraud
- the addition of data inconsistent with external data sources, such as current address data

Many insiders committed their malicious activities remotely and outside of normal business hours, possibly because they felt less vulnerable to detection.

MERIT Example

The insiders, contractors and foreign nationals, were employed as part of the investment services team of a foreign financial institution. The primary insider was a day trader with a computer programming background. The secondary insider was the head of the trading department. The insiders' employer organization was a customer and trusted business partner (TBP) of the victim organization, a commercial news distribution service. One of the victim organization's services was a proprietary, web-based, press release submission system that was available only to clients. The insider's employer organization became a client of this service because the organization had never issued a press release. To publicly disseminate a news release, clients would begin the process by logging on to the victim organization's website and submitting their press release. Prior to publication, a submitted news release would be edited and proofread by the victim organization. This process generally took 15 minutes. The insiders used a "spider" program, ran for several hours a day, to access the confidential information of the victim organizations' other clients, specifically press releases that were not yet available to the public. The press releases included the identity of the issuing organization, the purpose and substance of the press release, the scheduled time of public dissemination, and distribution routing instructions. Within minutes of a clients' submission of a press release to the victim organization's website, the insiders made trades based on the information. The insiders obtained over 360 confidential press releases issued by over 200 companies. The insiders made over $7.8 million in related trades. The incident was detected when the victim organization's technical team noticed unusual trading the day before a merger announcement. The insiders' IP address from their employer organization was recorded in the victim organization's web log files, and connected the insiders to the incident. The insiders were arrested, convicted, and ordered to pay financial penalties. The primary insider's financial penalties included a $13 million disgorgement and a $1,300 penalty. The secondary insider's financial penalties were $551,000 disgorgement with $10,000 interest and a $15,000 penalty. The insiders' employer organization was also penalized $650,000.

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 collects metrics for online activity (e.g., email traffic, web traffic, number of downloads) that provide an understanding of baseline or normal activity.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has documented procedures for log review in search of deviations from established baseline of normal or anticipated behavior.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a practice of auditing and monitoring process activity for deviations from baseline activity (e.g., vulnerability scanners, network mapping).

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has mechanisms for log aggregation to uncover trends and anomalies.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has procedures for identifying and responding to abnormal after-hours activity.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has automated mechanisms that detect and raise an alert for abnormal activity patterns based on established baselines.

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 # IT2.7: Alterations of Critical Data

The organization audits and monitors alterations of critical data.

Clarification/Intent

The organization reviews data modification logs to detect deviations from the baseline.

Assessment Team Guidance

Insiders have exploited lack of validation controls to add, delete, or modify data to commit their crimes, for example, changing identification information of customers, such as addresses.

MERIT Example

The insider was formerly employed by the victim organization, a court document subscription service. The insider became disgruntled when a new CEO was hired and refused to honor a verbal agreement between the former CEO and the insider regarding compensation and vacation time. The insider resigned and took a series of malicious actions with the intent that customers would be unable to access the database without making a call to the organization's helpdesk. The insider was able to bypass system front-ends to obtain unauthenticated access to a customer database. The insider remotely accessed the database, outside of work hours, and made malicious changes to customer information, including changing usernames by a single character to and changing what access customers had once they logged in. The insider made complex queries intended to reduce system performance for all logged-on customers. The insider also updated the source code of web pages by making small changes to the database queries including commenting out code or changing the query to use a slower method. The changes were relatively minor and were not incredibly damaging to the organization, but the organization had to handle multiple customer complaints and had to troubleshoot each problem individually. The insider was detected when the organization recognized that an apparent intruder had changed some web site related files. To identify the insider, the organization created a duplicate of its servers and routed calls from the attacker into the duplicate servers. The organization worked with the internet service provider who managed the source IP of the attacks to tie the attacks back to the insider's home computer. The incident took place over a week. The insider was arrested, convicted, and sentenced to 2 years of unsupervised probation. The insider was also allowed to apply for diversion. (If the insider complied with the terms of probation, the incident could be removed from his record.) The incident cost the organization over $7,000.

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 reviews data modification logs for deviations from established baseline or anticipated values.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization routinely reviews data modifications for potential malicious activity.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

There is no Level 3 for this capability.

Level 4

☐ The organization has automated integrity checks built into critical databases.

Doc Rev _____

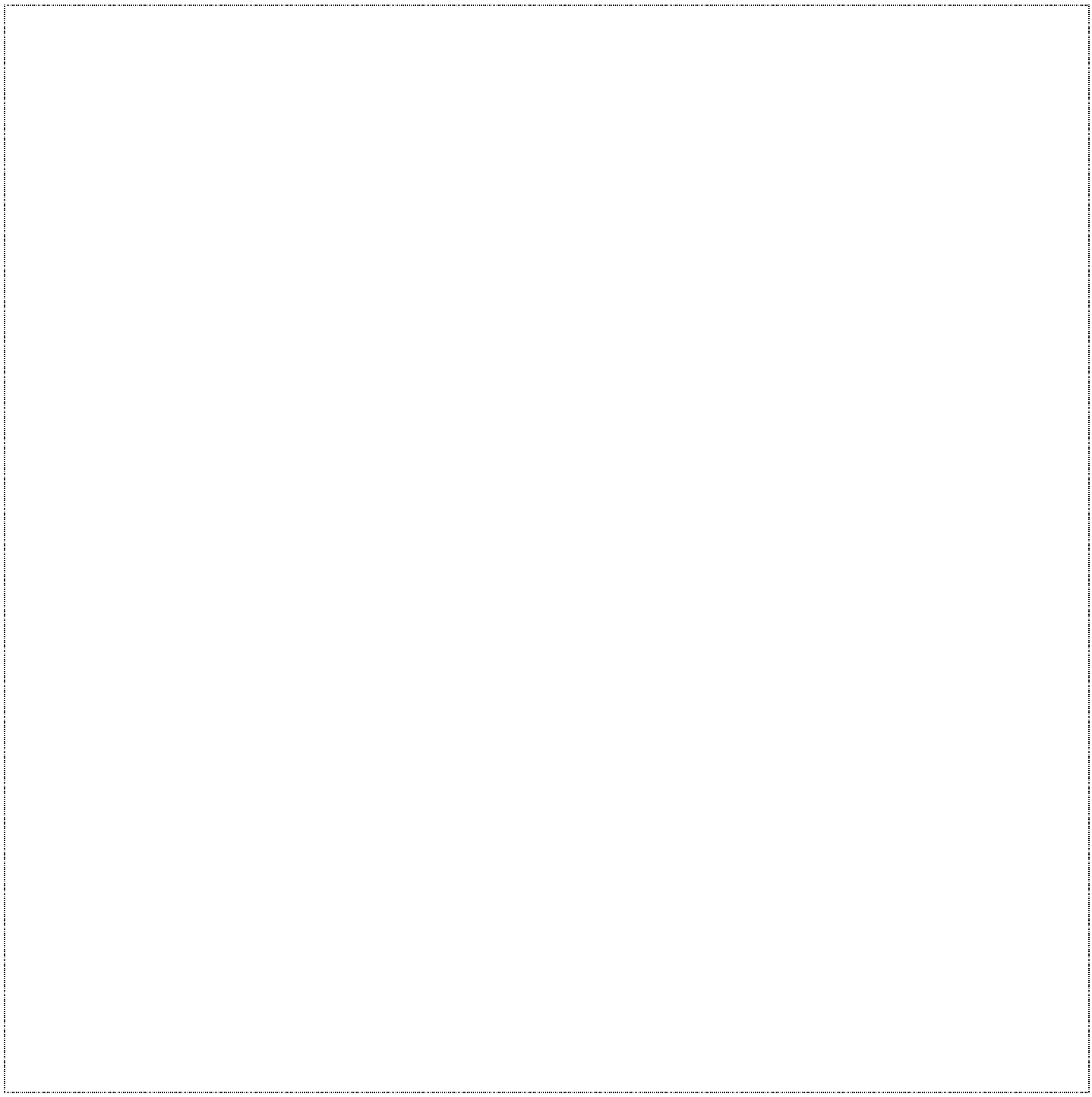
Dir Obs _____

Intvw _____

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

Justification

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



Capability Sequence # IT2.8: Exception/Expedited Process Monitoring

The organization audits and monitors expedited processes that bypass critical checks.

Clarification/Intent

The organization defines, tracks, and reviews procedures for bypassing or expediting processes.

Assessment Team Guidance

Some insiders have used the ability to expedite a process to facilitate their insider activities.

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 defines when and how business processes may be expedited or by-passed.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has documented procedures for bypassing or expediting processes that include multiparty approval and implementation.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization tracks usage of the exception process.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization routinely reviews exception reports for anomalies and abuse.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has an automated notification whenever an employee bypasses normal business processes.

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 # IT3.1: Modification or Deletion of Critical Data

The organization prevents, detects, and responds to the unauthorized modification or deletion of critical data.

Clarification/Intent

The organization prevents, detects, and responds to the unauthorized modification or deletion of critical files (non-executables).

Controls define and control how and when critical files may be modified or deleted.

Assessment Team Guidance

Many insiders have modified or deleted computer files critical to their employer's operation maliciously and without authorization. The controls should protect:

- customer information, accounts, systems, operating files, and computer registries
- websites, contact information, products, and services
- log files that support detection of malicious activity and identification of imposters

Critical and sensitive data must include

- customer information including PII
- employee, customer, and partner accounts
- financial records
- systems operating and registry files
- public website content
- audit logs

MERIT Example

The insider was formerly employed as an internet technology (IT) manager by the victim organization, a multimedia software development company. For undisclosed reasons, the insider's employment was terminated by the organization. The insider was being investigated and the investigation continued after the insider left the organization. The incident took place over 5 days and the motivation for the incident was revenge. Two weeks after his termination, the insider remotely accessed the organization's systems from his residence, outside of working hours. During this unauthorized access, the insider removed SSL libraries, deleted all root domains, deleted an email server domain, accessed the email account of the CEO of the organization, changed account passwords, and configured an email server to reject all incoming emails. IT administrators detected the attack. The IT administrators noticed that emails were accessed by non-account holders, passwords were changed by non-account holders, and the email servers had been reconfigured. The IT administrators also noticed that these actions were performed by someone with privileged access. Web and internet service provider (ISP) log files from the victim organization, the insider's ISP, and the insider's home computer connected him to the incident. The insider was arrested, convicted, and sentenced to 3 years of probation. The insider later admitted that he accessed the organization's CEO's email to determine what was going on with his investigation.

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 formally defines what is considered critical and sensitive data. (See Assessment Team Guidance.)

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has mechanisms to detect unauthorized modification and deletion of critical and sensitive data.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a procedure providing for critical and sensitive data redundancy.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has the ability to restore data that has been modified or deleted.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ There are physical and technical controls for protecting critical and sensitive data.

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 # IT3.2: Data Integrity Handling During an Exception

Organization controls ensure the integrity of data entered when normal processing is bypassed.

Clarification/Intent

The organization ensures the integrity of data entered when normal processing is bypassed.

Controls address integrity of data in motion and at rest.

The organization ensures the integrity of any data entered from an external system.

Controls should define the handling of data accessible through external systems.

Assessment Team Guidance

To further their fraud, many insiders have bypassed normal processing as a means to get around data integrity checks.

MERIT Example

Three insiders were employed as data entry clerks by the victim organization, an agricultural products firm. Over 5 months, while on site and during work hours, the insiders manipulated data to fraudulently issue 19 rebate checks to their relatives. During the incident, a supervisor's password was compromised and the insider also illegally entered the system with a temporary credentials. The incident was detected when the organization's accountant's conducted an internal audit. The audit revealed that some end or information had been changed or deleted, and some rebate recipients were receiving excessively large rebate amounts, and those recipients were outside the geographic restrictions on the program. The insiders were identified by the names of their relatives on the account and the passwords. The primary insider was arrested, convicted, and sentenced to 8 months imprisonment followed by 3 years of supervised release, including community service and fines.

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 procedures describing how data is to be entered, modified, and/or deleted.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization formally defines trusted external systems from which data may be collected.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization prevents external systems from bypassing controls for entering, modifying, and deleting data.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization prevents bypassing procedures for data modification or entry, especially in the case of expedited processes, such as emergencies.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization automatically validates data input from internal and external sources.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization technically validates the trustworthiness of external sources (e.g., certificates, IP address).

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 # IT3.3: Unauthorized OS or Production Software Configuration

The organization prevents, detects, and responds to unauthorized modification of its operational systems and deployed production software, even if performed by system administrators.

Clarification/Intent

The organization prevents, detects, and responds to unauthorized modification of its operational systems and deployed production software, even if performed by system administrators.

Controls define authorized means of systems and production software modifications.

Controls include checks and balances for updating and modifying systems and production software.

Assessment Team Guidance

Many insiders have modified an organization's computer systems and software to exact revenge for a perceived wrong or to enable them to steal information. The controls should:

- protect against the creation, testing, and insertion of malicious code, such as logic bombs and viruses
- protect against the illicit use of password crackers
- protect against the use of a malicious script set up in "crontab" or other schedulers
- address potential modification of the operating system script to trigger malicious code
- protect against the modification of critical software programs and the purposeful misconfiguration of system applications
- protect against the installation of unauthorized software onto a user's desktop

MERIT Example

The insider was formerly employed as a network administrator by the victim organization, which developed networking and communications technologies. The organization reprimanded the insider for poor performance and general unavailability. The organization later discovered that the insider was frequently unavailable because the insider was simultaneously employed by another organization. In response to the written reprimand, the insider attempted to resign, but was asked by his supervisor to take 3 days to reconsider. The organization immediately changed the insider's administrative passwords. 3 days later, the insider entered the organization, mentioned to another employee that his passwords had been changed, and asked to see his supervisor regarding his resignation. The insider's exit interview was performed. Subsequently, while on site and during work hours, the insider installed a malicious file deletion script and a backdoor on the server. The insider's malicious file deletion script went off on 3 separate occasions over the week after his termination. The incident deleted file systems from 2 servers and the file servers went down. Another system administrator at the company discovered that a script called "findit" was on the system in cron that was used to delete the files. The organization was able to restore some data, but not all, because of a backup software issue. During his employment, the insider was responsible for the organization's backup software. The insider was connected to the incident through log on times and location records. The organization's incident related loss was approximately $238,000. The insider was arrested and convicted, but sentencing details were unavailable. The insider's supervisor also believed that the insider was running a scam by selling memory owned by the organization.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

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

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has an acceptable-use policy for its IT systems, which prohibits downloading malicious code and unauthorized modification to systems.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization clearly defines what is authorized and unauthorized software and data.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization is able to detect unauthorized modifications to production systems (e.g., registry changes).

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has the capability to detect unauthorized downloads and installations of applications.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has procedures for responding to unauthorized modifications to production systems.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization is able to return systems and software configurations to a known reliable state

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has technical controls to prevent unauthorized downloads and installations of software.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented change management process for IT systems.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented configuration management process for IT systems.

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 # IT3.4: Unauthorized Hardware

The organization prevents, detects, and responds to the unauthorized addition of new hardware to its computer and network systems.

Clarification/Intent

The organization prevents, detects, and responds to the unauthorized addition of new hardware to its computer and network systems.

Controls define allowable equipment and peripherals, and they help the organization detect the presence of unauthorized equipment and peripherals in use.

The organization has policies and controls for employees attaching removable media, including compact USB drives and portable machines owned by the organization, to organization systems and downloading to that media.

Assessment Team Guidance

Some insiders have modified the hardware configuration of organizational systems. The controls should protect against:

- the addition of a modem
- the attachment of a USB-based hardware keystroke logger to a workstation or server

Many insiders have stolen large quantities of information by downloading to removable media. The controls should address:

- downloads to thumb drives
- downloads to compact disks
- insiders who bring their own drives to work

MERIT Example

The insider was employed as a claims manager at the victim organization, an insurance company. The insider considered the organization's practice of canceling policies when customers were one day late with payment to be unjust and illegal. The insider gave company documents about canceled policies to lawyers representing plaintiffs in a class-action lawsuit against the organization. The insider installed a keystroke logger on the organization's vice-president's secretary's computer in order to eavesdrop on her emailing. The insider was terminated for failing to report time he spent in the office. It was later discovered that the time the insider failed to report was when he was secretly gathering documents. The day after his termination, the insider asked another employee to remove the keystroke logger. Instead of complying with the insider's request, the employee notified the organization. Forensic investigators recovered the device and found files of intercepted keystrokes on the insider's office computer, proving that the insider obtained the files from the keystroke logger at least once. After his arrest, the insider claimed that he was a whistle-blower working at the behest of the state Department of Insurance, whose representatives denied the claim. The case against the insider was dismissed. An appellate court ruled against the organization in the class-action suit involving the policies disputed by the insider.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

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

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has an acceptable-use policy for its IT systems, including employee-assigned hardware.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The acceptable-use policy clearly states what is authorized and unauthorized hardware and peripherals.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization clearly defines (via a policy or other document) which employees are authorized to use removable storage hardware and peripherals.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has mechanisms to detect unauthorized hardware installations or use.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a documented response plan for unauthorized hardware.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization defines which storage hardware and peripherals are authorized for use.

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 # IT3.5: System Vulnerability Exploits

The organization prevents, detects, and responds to a system administrator exploiting an unpatched or known system vulnerability.

Clarification/Intent

The organization has formal, documented patch, configuration, and change management processes. The organization has identified critical systems and reviews logs of these systems to track access.

Assessment Team Guidance

MERIT Example

The insider was employed as a system administrator and computer security officer by a court. As a function of his job, the insider subscribed to a private mail list service that was restricted to court computer system administrators. The mail list server was operated by another court, the victim organization. The insider wanted to prove that the victim organization's server was vulnerable to outside attacks. The method of attack was an electronic mail flood that overwhelmed the server with inappropriate email. The server was subscribed to numerous other mail list servers on the Internet. When those other mail list servers sent an acknowledging email, the server was flooded with email messages. There were at least 5 attacks on the server over a month long period. The insider initiated at least one of these attacks, but it is believed that the insider repeated the attacks after his attempts went unnoticed. The incident was detected after the electronic mail flood made the server unavailable. The insider was arrested, convicted, ordered to pay $5,300 restitution, sentenced to 3 months imprisonment followed by 3 months of home confinement, and 1 year of supervised release, including 240 hours of community service and monitored computer activity.

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 list of critical systems.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization reviews logs of critical systems to track access and activity of system administrators.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization performs regular vulnerability scans of critical systems.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization remedies vulnerabilities within organization-defined time frames in accordance with configuration management and risk assumption policy and procedures.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has a documented patch management process.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented configuration management process.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented change management process.

Doc Rev _____

Dir Obs _____

Intvw _____

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

Justification

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

Notes (from documentation, observations, and interviews)

Capability Sequence # IT4.1: Role Based Access Control (RBAC)

The organization controls account privileges as they relate to job function.

Clarification/Intent

The organization should control user account privileges based on initial job function and role changes.

The controls should prevent and detect excessive privileges being granted to an employee. Excessive privileges are any privileges an employee can exercise that are not required to perform his or her job function.

The organization should control who is granted administrator-level privileges based on job function. Controls should address temporary assignments and partial administrative capabilities (i.e., the ability to reset account passwords and make group membership assignments, but not to create new accounts).

Job roles that should be considered include the following:

- conditional employees
- programmers and system developers
- technicians
- system maintenance personnel
- help desk representatives

The organization should be able to prevent, detect, and respond to unauthorized changes to system access that would result from an account being added to the membership of a system group that has additional privileges.

Assessment Team Guidance

Some insiders who were not authorized system administrators have been able to set up and conduct their attacks because they had obtained administrative system- and/or application-level privileges. The controls should:

- address programmers and/or system developers who may need administrative system- and/or administrative-level privileges
- address technicians, system maintenance personnel, and help desk representatives

Some organizations have allowed insiders unfettered access to information and systems before the insiders were fully vetted. The controls should address the risk of granting access prior to the completion of background checks,

Insiders have sometimes exploited system administrator privileges to harm an organization or steal information, even though they were not the system administrator or trained in system administration. The controls should address users whose core responsibilities are not system administration

Many insiders have been able to escalate their own privileges, or have someone else escalate privileges, which allowed them to carry out their attacks. The controls should

- address operating-system-level groups and privileges
- address application-level groups and privileges
- address escalation of access to a privilege level, such as administrator or root

MERIT Example

The insider was employed as a system administrator by the victim organization, an internet service provider (ISP). The insider, dissatisfied with this job, quit and began writing threatening e-mails to the organization. The organization had poor access controls; even the receptionist had the ability to add new accounts. As a paying ISP customer, the insider was able to retain partial access to the organization. The insider used his knowledge of a company tool to elevate his privileges on the system to that of an employee. The unauthorized access was detected when log files showed the attempts at elevating access, and the organization terminated the insider's customer account. The insider was able to continue attacking the organization using two other bogus accounts he had created. The insider changed all administrative passwords, altered the billing system, modified the registry, and deleted two internal billing databases. The duration of the incident was 4 days. It took an entire weekend to recover from the attack, costing the organization $45,000. The insider was arrested, convicted, and sentenced to 6 months in a halfway house followed by 3 years 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 a documented policy and procedure for assigning each new account the appropriate set of privileges. (User template is acceptable provided this template does not have administrator privileges.)

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization tracks creation of group accounts.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization regularly audits group membership.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented policy for periodically reassessing and recertifying the continued need for an account to have specific system and application access.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has policies and procedures that specifically address the privileges for conditional employees.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has policies and procedures that specifically address the privileges for programmers and system developers.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has policies and procedures that specifically address the privileges for technicians.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has policies and procedures that specifically address the privileges for system maintenance personnel.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has policies and procedures that specifically address the privileges for help desk representatives.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a process for handling job role changes (e.g., change in position results in audit of current privileges).

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization periodically assesses the continued need for group system permission and rights as well as group membership.

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 # IT4.2: Password Management

The organization manages passwords.

Clarification/Intent

The organization should have controls to provide password management in accordance with widely accepted guidelines addressing password

- Initial settings and issuance
- strength
- history and change frequency
- storage and transmission
- sharing

Consider all system types, including computer- and network-based systems, phone systems (PBX), voicemail, and subscribed third-party application services.

Also consider all password types, including passphrases, personal identification numbers, and access codes.

Assessment Team Guidance

Many insiders have been able to carry out and conceal malicious activity by compromising an account of another employee. There should be a process to ensure that the organization issues strong default passwords when creating and resetting accounts. The controls should:

- address easily guessed or cracked passwords
- ensure that initial passwords are changed
- address physical storage of passwords
- address sharing of passwords among employees
- address passwords for subscribed third-party applications, such as domain name service (DNS), internet-based customer relationship management (CRM), and mass marketing

MERIT Example

The insider was formerly employed as a system administrator by the victim organization, a government agency. The insider resigned from the organization and was very unhappy at the time of resignation. The incident took place outside of working hours, using remote access to a Gopher program. The insider remotely accessed the organization's network from his home and changed the Domain Name Service (DNS) tables. The following day, the insider attempted to gain unauthorized access from his home and was denied. Subsequently, the insider used backdoors that he had created prior to resignation to access the root access program, Gopher. The insider wanted to see if his password was still working. The following day, the organization's network administrator removed the insider's username and passwords from the systems. The next day, the insider, using Gopher, created a new user ID and password. The day after this, the insider remotely accessed the network and set up a secure shell for a second computer to have access to the organization's network via his home computer. The following day, the insider again obtained unauthorized access to the organization's systems. The day after, the organization's network administrator detected the intrusions and deleted the insider's new username and password. A week later, the insider was denied access to the organization's network. Two months later, the insider accessed the network, and transferred files from the organization's network to his home computer using FTP. The insider created secure shell and several directories. The insider also hid several files. The insider deleted 2 hours of logs, but was unsuccessful at concealing his actions. Log files connected the insider to the incident - through his IP address and entries indicating that he had visited his personal website. The duration of the incident was 3 months. The insider was arrested, but details regarding the verdict were unavailable. The investigation revealed that a former co-worker was acting as an accomplice. The accomplice stated that the insider was motivated to access the system by poor treatment he felt he received while employed by the organization and at the time of his resignation.

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 for how passwords should be managed.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization uses security controls that implement the password management policy (e.g., password strength, password age and history).

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a technological and/or administrative implementation of complex, default password generation.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization changes applicable passwords upon employee role changes, suspension, and/or termination.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has a secure process for initial password distribution.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization encrypts stored and transmitted passwords and hashes.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization ensures that stored passwords and hashes are accessible only to privileged users and account owners.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has implemented a practice of assessing password vulnerability.

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 # IT4.3: Access to Backup Media

The organization has policy and controls governing employee access to backup media or services.

Clarification/Intent

The organization has policy covering data backups; access, storage, and transportation of backups; and disposal of physical media.

Assessment Team Guidance

Some insiders have accessed backup media to steal or sabotage information.

MERIT Example

The insider was formerly employed as a network engineer and technical services manager by the victim organization, a non-profit that stored data for community health clinics. After receiving a negative performance evaluation, the insider resigned. 2 months after resigning, the insider remotely accessed the organization's network and disabled the automatic process that created backups of patient information for the area's largest clinic. 6 days later, the insider attacked the system again and systematically deleted data and software on several of the victim organization's servers, including software used by all of the area clinics and additional patient data for the area's largest clinic. The insider was arrested, convicted, ordered to pay $41,000 restitution, and sentenced to 63 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 data backup policy.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has documented procedures on how to store and transport backup media.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has documented procedures for properly disposing of physical media.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has physical and technological access logs to track employees and/or trusted business partners who attempt to access backup copies.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has physical and technological mechanisms to prevent unauthorized access to backup copies.

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 # IT5.1: Account Compromise

The organization prevents, detects, and responds to account compromise.

Clarification/Intent

The organization should have controls that provide employees an understanding of potential account compromises and how to address such incidents.

Controls should provide guidance on preventive measures for protecting accounts from unauthorized use, detecting unauthorized account use or attempts at such use, and how to respond to suspected account compromise (such as an exposed password or evidence of unauthorized account use).

Assessment Team Guidance

The controls should:

- provide means of reporting
- provide penalties for unauthorized attempts to obtain account or password information
- include means of authentication beyond the use of traditional passwords

MERIT Example

The insider, presumably a foreign national, was employed by a foreign division of the victim organization, a construction and mining company. At the time of the incident, the insider was also working for a foreign internet technology organization. The insider used another employee's user ID and password to access the organization's server, which was located in the organization's headquarters in the United States. The insider downloaded over 4,000 confidential documents. Closer circuit cameras captured visuals of the insider accessing the server at the time the files were downloaded. User logs also indicated the password and user ID used for gaining entry into the server. The insider was arrested and convicted, but sentencing details were unavailable. Authorities discovered storage media, specifically a hard disk and a flash drive, that stored the stolen files.

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 procedures for reporting potential account/password compromises.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has incident management procedures and methods to detect potential account/password compromises.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a documented response plan for compromised accounts.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has procedures to take disciplinary action against employees who attempt to gain unauthorized account password information.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has an awareness program for all employees, conveying basic password and account protection.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Current and backup instances of account databases are secured, both technologically and physically.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Login traffic is encrypted.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization requires multifactor authentication for remote account 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 # IT5.2: System Privilege Abuse

The organization prevents, detects, and responds to systems privilege abuse.

Clarification/Intent

The organization should have controls to address excessive privilege use, such as mass password changes, other unauthorized account management activities, and audit log activities. Controls should define normal activity levels and how to prevent, detect, and respond to excessive activity.

Assessment Team Guidance

There should be controls to:

- track manual alteration to accounts, such as password resets
- implement protection from malicious script execution
- address all password types, such as administrative, user login, VPN, phone system/PBX, and customer and partner passwords
- address monitoring of nonprivileged and nonadministrative accounts for users with responsibility to manage customer and/or user accounts
- address administrative accountability

MERIT Example

The insider worked as a branch manager for a banking institution. After running into gambling issues, family health issues, and unforeseen expenses, he used his privileged access to the bank's computer systems to withdraw money from a friend's business accounts. This access gave him the ability to change the billing addresses of accounts to his own registered PO box for the purpose of hiding the true bank statements from the accounts' owner. Eventually, the insider began stealing money from others' business accounts as well, until he had stolen a total of over $225,000. While the insider claimed to have intentions of paying the full amount back, he was caught after his friend and the other account holders notified authorities of fraudulent withdrawals from their accounts. The authorities traced the paper trail back to the insider, who admitted to the criminal scheme. He was indicted for Bank Fraud, and sentenced to 27 months imprisonment, 5 years supervised release, and restitution of the full amount stolen.

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 defining who is authorized to perform privileged system activities (e.g., only help desk and system administrator staff can change user passwords).

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has procedures for verifying and/or validating changes made to critical systems.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has mechanisms to detect privilege abuse and mass changes of critical data (such as system passwords).

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has procedures for taking disciplinary action against employees who attempt to perform unauthorized activities.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has procedures and/or mechanisms to correct unauthorized mass changes (e.g., system restores).

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has controls (e.g., separation of duties, change management) to prevent unauthorized changes made to critical systems.

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 # IT5.3: Detection of Access Abuse

The organization detects employees' attempts to exceed their authorized access, successful or not.

Clarification/Intent

Assuming right-sized privileges are initially granted, the organization has controls to detect an employee who gains greater access than given or authorized.

Assessment Team Guidance

The team should determine if the controls can detect unauthorized access to information and detect misconfigured system utilities.

-

MERIT Example

The insider was formerly employed as a system administrator by the victim organization, a government agency. The insider resigned from the organization and was very unhappy at the time of resignation. The incident took place outside of working hours, using remote access to a Gopher program. The insider remotely accessed the organization's network from his home and changed the Domain Name Service (DNS) tables. The following day, the insider attempted to gain unauthorized access from his home and was denied. Subsequently, the insider used backdoors that he had created prior to resignation to access the root access program, Gopher. The insider wanted to see if his password was still working. The following day, the organization's network administrator removed the insider's username and passwords from the systems. The next day, the insider, using Gopher, created a new user ID and password. The day after this, the insider remotely accessed the network and set up a secure shell for a second computer to have access to the organization's network via his home computer. The following day, the insider again obtained unauthorized access to the organization's systems. The day after, the organization's network administrator detected the intrusions and deleted the insider's new username and password. A week later, the insider was denied access to the organization's network. 2 months later, the insider accessed the network, and transferred files from the organization's network to his home computer using FTP. The insider created secure shell and several directories. The insider also hid several files. The insider deleted 2 hours of logs, but was unsuccessful at concealing his actions. Log files connected the insider to the incident - through his IP address and entries indicating that he had visited his personal website. The duration of the incident was 3 months. The insider was arrested, but details regarding the verdict were unavailable. The investigation revealed that a former co-worker was acting as an accomplice. The accomplice stated that the insider was motivated to access the system by poor treatment he felt he received while employed by the organization and at the time of his resignation.

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 implemented a practice of granting entities only the rights and permissions necessary to access systems and data relevant to their job function and needs.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization grants access permissions and rights required per job role through the use of user account templates, systems roles, and/or groups.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization baselines systems activities and monitors for deviations.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has implemented multiparty controls to prevent the abuse of privileged access capabilities and authority (i.e., separation of duties).

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 # IT5.4: Abnormal Activity Outside Working Hours

The organization detects and responds to abnormal technical activity outside normal working hours.

Clarification/Intent

The organization defines normal working hours for the various employee types and is able to detect and respond to employee access outside normal working hours.

Assessment Team Guidance

Many insiders have conducted their crimes outside normal working hours, perhaps feeling that their activity would be less scrutinized. The organization should define normal working hours for each employee type, such as staff, contractors, subcontractors, and temporary workers. There should be temporal technical access controls.

-

MERIT Example

The insider was formerly employed as a computer support technician by the victim organization, an information technology support business. As part of his duties, the insider had administrator-level password controlled access to the organization's network. The insider did not have authorization to access the organization's computer after his departure. Three months after leaving the organization, on a late weekend night, the insider used his administrator account and password to remotely access the organization's network. The insider changed the passwords of all of the organization's IT system administrators and shut down nearly all of the organization's servers. The insider deleted files from backup tapes that would have enabled the organization to promptly recover from the intrusion. The organization and its customers experienced system failure for several days. The incident was traced to the insider's home network. The insider was arrested, convicted, ordered to pay $31,000 restitution, and sentenced to 12 months and 1 day imprisonment, followed by 3 years of supervised release. The insider was also ordered to perform 100 hours of community service by lecturing young people on the implications of hacking.

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 definition of normal business hours.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization formally sets working hours for the different types and roles of employee.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a system monitoring abnormal (deviations from the baseline) behavior as it relates to after-hours access.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization reviews audit logs daily or utilizes a security information and event management (SIEM) system to alert on abnormal activity.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a documented response plan for investigating suspicious technical activity outside normal working hours.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has technical controls to enforce after-hours access restrictions.

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 # IT5.5: Physical Security Violations

The organization has controls to support detection and reporting of physical security policy violations and problems.

Clarification/Intent

The organization has mechanisms to detect and report physical security policy violations and problems.

The organization defines which employees are authorized and unauthorized to access specific areas and provides for physical separation of such spaces.

Controls alert authorized personnel to physical security breaches and allow for auditing of attempted and successful breaches that may have gone unnoticed.

Assessment Team Guidance

Controls should support reporting of direct violations of policy, as well as suspicious or concerning behaviors, especially outside of normal working hours.

-

MERIT Example

Two insiders were currently employed as engineers at a tire equipment manufacturing company. Their organization was an international company with locations in the US and China, among others. They had manufactured equipment for the victim organization, and held a contract with a Chinese company to manufacture a piece of equipment that they were struggling to design. The victim organization (who they supplied equipment to) had their own trade secret version of the equipment that the insiders' organization needed to design to fulfill their own contract. The insiders scheduled a visit to the victim's manufacturing plant under the pretense of inspecting their (the insiders' org.) own equipment for potential repairs. The victim's plant had restricted access behind several secure doors, and signs stating that cameras were prohibited. Visitors were required to sign in and out, and be escorted at all times. The victim organization also asked visitors to sign an NDA, however the insiders falsely stated that they had already signed one the previous year. While one insider kept a lookout, the other insider proceeded to take several pictures of the trade secret equipment with the camera on his cell phone. After the insiders left the victim's facility, one insider downloaded the images from his camera and emailed them from his personal account to his work email. Later, he proceeded to send the images from his work account to other co-workers in another plant who were tasked with actually manufacturing their version of the trade secret equipment.

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 identifies sensitive areas throughout the organization.

Doc Rev

Dir Obs

Intvw

☐ The organization controls physical access to all sensitive areas.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization employs mechanisms to alert security personnel to unauthorized physical access and attempted access.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has documented procedures for responding to incidents of unauthorized physical access and attempted 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 # IT5.6: Theft of Organization Property

The organization prevents, detects, and responds to the theft of organization property and software, especially property that may be useful for an employee's personal use.

Clarification/Intent

The organization has policies and controls in place to prevent, detect, and respond to the theft of organization property and software, especially property that may be useful for an employee's personal use.

A starting point for this capability is that the organization should maintain an inventory of all organization property and software.

The organization should also define and label property it considers proprietary. Controls should be in place to protect property from theft. This includes mechanisms for tracking property and restricting access to property and software to only those who need to use it.

Assessment Team Guidance

Many insiders have stolen organization property either in the direct commission of the attack or as setup for the attack.

The scope of the inventory of organization property and software could include but is not limited to

- laptops loaned to employees as part of their job
- removable media
- information that exists on paper during the lifecycle of creation, use, storage, and disposal

Controls or policies should address

- the appropriate use of company property
- employees who do not return company equipment upon termination
- measures for maintaining and auditing an inventory of organization-owned property and software

MERIT Example

The insider, a foreign national and contractor, was employed as a programmer by a foreign beneficiary organization, an oil company. The victim organization developed software for surveying land for oil and natural gas. The beneficiary organization had an agreement with the victim organization to train the insider for 6 months. During the last month of his training, the insider gained unauthorized access to the victim organization's systems via a compromised password, either through observing an employee enter his password or using a crack program. The insider stole the victim organization's software and source code by initially copying it to an employee's laptop and then to his own laptop. After the victim organization's employee reported that his computer had been tampered with, the insider was ordered to vacate the premises and his laptop was confiscated. The insider was arrested while waiting to board a plane to his home country. The insider was arrested, convicted, and sentenced to 24 months imprisonment followed by 2 years of supervised release. A few years prior to the incident, another employee from the beneficiary organization had stolen the victim organization's software during training at the victim organization's facility.

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 maintains an inventory of company property, including but not limited to software, laptops, and removable media.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization tracks what property has been assigned to employees or trusted business partners.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a policy that defines the appropriate use of organization property and software and consequences for violation.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a mechanism for reporting missing property.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has procedures for responding to missing property.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a procedure for tracking the return and recovery of organization property assigned to employees who are separating from the organization.

Doc Rev

Dir Obs

Intvw

☐ The organization has a procedure for auditing the inventory of organization-owned property and software to ensure accuracy and quality control.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization trains employees on how to properly use, secure, and maintain company property, including software, laptops, and removable media.

Doc Rev

Dir Obs

Intvw

☐ The organization tracks and controls software license usage.

Doc Rev

Dir Obs

Intvw

☐ The organization has controls in place to track and protect information that exists on paper during the lifecycle of creation, use, storage, and disposal.

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 # IT5.7: Access to Information Out of Scope

The organization prevents, detects, and responds to employees' attempts to access information inconsistent with their job responsibilities.

Clarification/Intent

The organization prevents, detects, and responds to employees' attempts to access information inconsistent with their job responsibilities.

Controls address access protections to ensure that employee authority is defined congruent to information and that technological mechanisms enforce such protection.

Assessment Team Guidance

To carry out their crimes, some insiders have accessed information that was beyond their need to know. Controls should protect against attempts to query databases beyond the employee's responsibility and reading executive email.

The mechanism for lockout in Level 3 can be manual (e.g., if after reviewing the logs in Level 2, the organization determines a suspicious user, they can disable or lock the account).

MERIT Example

The insider, a foreign national, was employed as a senior engineer by the victim organization, an automobile parts manufacturer. The insider's co-conspirators were his wife, who was the former vice-president of sales at the victim organization; another former co-worker and foreign national; and an employee from a competitor beneficiary organization. The insider, the former employees, and the employee from the beneficiary organization conspired to steal the victim organization's secret manufacturing process and use it to aid a foreign competitor organization. The goal was to displace the victim organization as the supplier of various automobile parts to United States companies. The insider and his co-conspirators set up a company to act as a commercial agent for the beneficiary organization. The insider remained employed at the victim organization while his accomplices negotiated with foreign competitors. The insider's wife contacted a friend and current employee at the victim organization via email. Prior to her resignation, the insider's wife had asked the friend to move her user files somewhere "safe" to hide them from another employee. In the email, the insider's wife asked the friend to move the hidden files back to her private network user folder so that her husband, the insider, could access them. In the email, the insider's wife disclosed that she was working with foreign competitors. The friend willfully complied with the insider's request and moved the files so that the insider was able to access them. It is unknown whether all of the stolen confidential files were obtained in this manner. Regardless, all of the information was outside of the insider's need-to-know. At the time of the incident, the insider was a project manager and was only permitted to access information pertaining to the project. The insider copied hundreds of confidential files, to a disc, which he gave to his wife. This information was passed on to the co-conspirator from the beneficiary organization, who emailed confidential information pertaining to the victim organization's manufacturing processes to 2 of the organization's suppliers. The suppliers reported the emails to the victim organization. The insider was arrested, convicted, sentenced to 6 months imprisonment followed by 6 months house arrest and 18 months of probation. The insider and his co-conspirators signed confidentiality agreements when they began their employment with the victim organization. The insider's wife may have stolen trade secrets prior to leaving the victim organization. Prior to her resignation, the insider's wife had several disputes with the victim organization's executive level management team, which likely contributed to her motivation for the incident.

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 definition of what access and permissions are granted to employees per job role.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization performs periodic audits of each job role's continued need for specific access rights and permissions.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization performs at least monthly reviews of access logs to uncover unauthorized access attempts or uses a SIEM to alert on unauthorized access attempts.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has mechanisms to alert security staff to excessive attempts at access beyond an account's given rights and permissions.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization employs lockout mechanisms for technical access controls when thresholds of unauthorized access attempts are reached.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization documents disciplinary actions to be taken against insiders who attempt unauthorized access.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization trains employees on acceptable access to information consistent with their job responsibilities.

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 # IT5.8: Unauthorized Workstation Usage

Workstations and other user accessible network endpoints are configured to prevent locally stored information from unauthorized access.

Clarification/Intent

The intent of this control is to ensure that data that is moved or copied from a protected network share is afforded the same or greater security permissions on the endpoint or destination.

Assessment Team Guidance

Some insiders have used computers other than their usual workstations to carry out and hide their malicious actions. The team should determine how the organization detects or controls sensitive data on user workstations and whether access control lists (ACLs) follow data that is copied to a local workstation.

-

MERIT Example

The insider was employed in the auditor/accounting office of the victim organization, a local government entity. The insider became disgruntled when he did not receive an expected promotion to finance director. While on site and outside of working hours, the insider deleted several official documents from the incoming finance director's workstation. After deleting the files, the insider went on vacation. The organization's internet technology (IT) director discovered the deleted files in the recycle bin. The organization agreed not to prosecute the insider if he agreed to replace the files at no cost to the organization and to resign. Although the new finance director stated the files were not recovered, the police officer said everything was recovered.

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 defines acceptable locations for the storage of company information.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has technical mechanisms for monitoring and logging workstation local access attempts.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization ensures that workstation endpoints are properly configured to enforce access control lists.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization ensures users are not able to access files stored on an endpoint to which they do not have permissions.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization regularly scans network endpoints for company data.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a data classification policy that defines how different levels of data are to be handled and provides training on the policy to employees.

Doc Rev

Dir Obs

Intvw

☐ The organization has a data classification policy that defines how data is to be protected on network endpoints and on standalone or unmanaged equipment.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has technical mechanisms to enforce appropriate ACLs on company data on all network endpoints.

Doc Rev

Dir Obs

Intvw

☐ The organization has technical controls in place to protect company data regardless of where the data is stored (Data Loss Prevention [DLP]).

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 # IT5.9: Suspicious Downloads of Info or Code

The organization can detect suspicious downloads of information or code.

Clarification/Intent

The organization should be able to detect suspicious downloads of information, such as information that could be used maliciously or illegally and for which the employee is not authorized.

The organization prevents, detects, and responds to the downloading of code that can be used maliciously, such as known hacking tools.

Assessment Team Guidance

Insider theft of information has often not been very well hidden. Controls should address downloads close to employee termination, downloads of confidential information outside the employee's realm of responsibility, and large downloads over short periods of time. The controls should be able to distinguish between confidential information of the organization, including intellectual property (IP), and open information.

Many insiders have downloaded malicious code used in their crimes. There should be controls to address code downloaded from websites as well as those embedded in emails as well as controls for known and suspected viruses, worms, Trojan horse programs, logic bombs, hacking tools, password crackers, remote access tools, and keystroke loggers. The organization should be able to prevent, detect, and respond to the downloading of code that can be used maliciously.

-

MERIT Example

The insider, a foreign national, was employed as a technical operations associate by the victim organization, a pharmaceutical company. During the course of his nearly 3 and a half year employment, the insider systematically and continuously downloaded the organization's confidential and proprietary information. The insider planned to use the information to start a competing organization in his home country. The insider, while on site and during work hours, downloaded 45 GB of information, including 1300 confidential and proprietary documents, onto an external drive. The insider emailed some of these documents to potential foreign investors. The incident was discovered when an internal audit of the insider's computer revealed the insider's application to start a beneficiary organization in a foreign country. During the investigation, a conversation was taped between the insider and a potential foreign investor. This conversation led investigators to a meeting between the insider and a potential foreign investor. During this meeting, the insider showed the investor some of the organization's trade secrets, including those related to a drug that the organization spent over $500 million to develop. The insider was arrested and convicted, but sentencing details 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 defines acceptable use of assigned employee equipment and IT systems.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has mechanisms to detect unauthorized downloads and installations of applications.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has mechanisms to detect known malicious software on systems.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a practice of increased monitoring of the activity of accounts belonging to terminating and suspended employees.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has procedures for responding to unauthorized download and installation attempts and successes.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has technical controls to prevent unauthorized downloads and installation of software.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has an automated means of removing unauthorized software.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a mechanism for alerting personnel to abnormal download traffic patterns.

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 # IT5.10: Monitor Encrypted Traffic

The organization has the ability to monitor encrypted traffic.

Clarification/Intent

The organization has the ability to decrypt and inspect the contents of encrypted traffic, such as https, SSH, and other channels encrypted via SSL. This organization does not require decryption of email traffic that is secured via private keys.

Assessment Team Guidance

Many insiders have used encrypted channels to exfiltrate data from their organization. In these cases, the organizations did not have the ability to decrypt and inspect this traffic and were therefore unable to prevent and/or detect this activity.

MERIT Example

The insider, a naturalized U.S. citizen, was employed as a computer programmer by the victim organization, an investment banking firm. Prior to the incident, the insider had submitted a letter of resignation. The duration of the incident was 5 days and the insider used both on-site and remote access, outside of working hours, to carry out the attack. The insider used a swipe card to access the building. The insider used a Bash script that copied, compressed and merged the files containing the source code, then encrypted, renamed and uploaded the files to the external file host. On 4 separate occasions, the insider uploaded 32 MB of files to a foreign file host. The insider deleted the encryption program and attempted to erase the Bash history, but the organization retained back-up copies of the Bash history. The insider claimed that the upload was accidental and that the intent was to transfer only "open source" information. The information was not passed to any third parties. The organization had some safeguards in place, including monitoring outgoing email attachments, disallowing outgoing FTP, monitoring HTTPS, and requiring the insider to sign an intellectual property (IP) agreement. The incident was detected was detected through regular auditing of HTTPS traffic. The insider was arrested, but verdict details 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 policy that allows information security staff to intercept and inspect encrypted traffic.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has security devices, such as proxies, to intercept SSL and other channels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization sends encrypted traffic logs to a central log correlation engine, such as a SIEM.

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 # IT5.11: Info Tech Complaints

The organization has a process to accept and handle employee complaints related to information technology and systems.

Clarification/Intent

The organization has a process to accept and handle employee complaints related to IT and systems, especially those that may indicate an integrity problem or system compromise.

Assessment Team Guidance

Many insiders had complained about the management or use of IT prior to committing their malicious activities. There should be controls that deal with complaints about:

- the quality of software development processes
- the information security within the organization
- inability to do technical tasks

MERIT Example

The insider, a contractor, was employed as a software developer by the victim organization, which produced flight simulation software. The insider complained about the organization's lack of security policies. When his complaints were unresolved, the insider copied the organization's password file to his machine and used a password cracker on that file to crack 40 of 160 passwords, including the system administrator's password as well as the root password. The insider reported the cracked passwords to his manager. The insider was arrested, convicted, ordered to pay a $5,000 fine, and sentenced to 1 year probation and 80 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 procedures for employees to report issues regarding IT and systems.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has documented procedures for handling complaints related to IT and systems with escalation triggers to ensure issues are addressed in a timely fashion.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization tracks progress of IT issues.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The above tracking process allows for escalation or elevation of issues to management.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization routinely performs quality assurance checks to confirm procedure adherence and issue resolution.

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 # IT5.12: Disaster Recovery

The organization has a formal disaster recovery or business continuity plan in place.

Clarification/Intent

This capability focuses on establishing resilience for critical assets by ensuring a business continuity or disaster recovery plan has been developed and tested. Such plans provide for the capability to restore assets and data that may be destroyed through malicious insider actions such as sabotage or theft.

The organization should be able to recover within a time frame that minimizes disruption should its systems be completely destroyed.

Assessment Team Guidance

Many organizations have been completely devastated by insider IT sabotage, partly due to the lack of contingency planning.

The assessment team should look for evidence that the organization

- can recover quickly
- implements hot backups or redundant systems for critical systems or data
- has controls that include testing backups or redundant systems to ensure they meet contingency plan recovery objectives and survivability goals?

MERIT Example

The insider was formerly employed as a software engineer by the victim organization, a high-technology company that developed and manufactured computer chips. The insider was responsible for managing an automated manufacturing system. During the work week, the insider maintained a constant remote access connection from his home to the organization's network. The insider, who had previously worked in another department at the organization, was terminated due to poor performance. Prior to informing the insider of his termination, the organization terminated the insider's network access, but failed to check if the insider's remote access connection was active. The incident occurred the day after the insider's termination, outside of working hours. While under the influence of alcohol, the insider used the open remote access connection to attempt to completely shut down the organization's manufacturing system by deleting critical files. Due to the insider's actions, the organization lost 4 hours of manufacturing time and had to load backup data to restart the manufacturing process. The incident cost the organization $20,000 to remedy. Connection and activity logs connected the insider to the incident. The insider was arrested and convicted, but sentencing details 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 a formal and documented business continuity plan (BCP) or disaster recovery (DR) plan.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented data backup process.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented configuration backup process, especially for critical systems such as core routers and mail servers.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has hot standbys or load-balanced configurations for critical network equipment, especially core and internet routers and perimeter firewalls.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has off-site backup for critical data.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a list of critical systems and services.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization maintains service level agreements (SLAs) with internet service providers (ISPs), service providers (if applicable), or hardware support vendors.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has tested their DR and/or BC plan.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization is able to recover from a disaster based on the DR/BCP plan.

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 # IT5.13: Incident Management Readiness

The organization has incident management capabilities to ensure that incidents are handled quickly and do not reoccur.

Clarification/Intent

Even the best information security infrastructure can't guarantee that intrusions or other malicious acts won't happen. When computer security incidents occur, it's critical for organizations to have an effective way to identify that something has happened and conduct a response. The speed with which an organization can recognize, analyze, and respond to an incident will limit the damage and lower the cost of recovery. This is the basis for an organizational incident management capability. Incident management requires organizations to establish processes for detecting, analyzing, responding to, and learning from incidents that threaten the confidentiality, availability, and integrity of critical systems and data. Supporting these functions are processes for communication, coordination, documentation, and tracking of incident details and response actions.

This capability focuses on the organization having a documented incident management process including a defined set of incident handlers with appropriate skills and knowledge to handle malicious or unintentional activities that might harm the organization's assets and data.

Assessment Team Guidance

Some organizations have suffered repeated attacks, sometimes by the same insider and sometimes by different insiders.

The team should look for evidence that a general incident management process is in place that defines how to detect, analyze, response, and recovery from security incidents.

At level four (4) the team should look for evidence that a specific process is in place to handle incidents perpetrated by an insider. This process can be part of the general incident management plan or a stand-alone plan just for insider activities.

MERIT Example

The insider was employed as deputy director of the computer department by the victim organization, a financial institution. Over 6 days, the insider stole 1.5 million records from the organization by downloading them to a disc. The records contained personally identifiable information (PII), including names, addresses, telephone numbers, birth dates, professions, annual incomes, and employer's names. The insider attempted to conceal his actions by using a co-worker's credentials. (2 months prior to the incident, the co-worker had been transferred to another division, but the co-worker's access rights had not been updated and the credentials remained valid). The insider, a manager, instructed a subordinate to copy the information to a disc. The insider acted as if the task was part of official business. The insider copied the information to his home computer and subsequently sold the data to over 80 telemarketing companies. 3 months after the data was sold, the incident was detected when customers began complaining that they were being spammed over their phones. The organization responded by conducting an internal investigation. The insider was fired. The insider was arrested and convicted, but sentencing details were unavailable. The insider had a considerable amount of debt, which likely contributed to his motivation for the incident.

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 incident management process or plan.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The above incident management process includes assigned staff and defined roles and responsibilities

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has mechanisms in place to detect or report security incidents.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization responds to incidents.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization performs a postmortem of the response performed on significant incidents.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization collects lessons learned from the postmortem to ensure similar incidents are prevented from re-occurring.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has a specific incident management process for handling incidents perpetrated by an insider.

Doc Rev

Dir Obs

Intvw

☐ The organization provides incident management training to members of the assigned team.

Doc Rev

Dir Obs

Intvw

☐ The organization conducts exercises for the team.

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 # IT6.1: Redundant Employee Roles

The organization assures redundancy in roles and responsibilities in the event an employee is terminated or otherwise unavailable.

Clarification/Intent

The organization should have controls that provide redundancy in roles and responsibilities within the organization in the event an employee is terminated or otherwise unavailable.

In support of continuity of operations, the organization should have plans to handle unscheduled (sudden) employee termination or unavailability.

Assessment Team Guidance

The damage to some organizations due to insider actions has been magnified because of the organization's sole reliance on the insider. There should be controls to address:

- sensitive information employees have access to, such as others' passwords
- unique technical skills or knowledge possessed by the employee

MERIT Example

To Be Supplied

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

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

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has documented definitions of roles and responsibilities for each member of its staff.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a documented policy requiring redundancy in roles and responsibilities.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization provides the necessary training to ensure redundancy in particular positions.

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 # IT6.2: Return of IT Assets on Separation

The organization has policy and controls to ensure that the organization's IT property and software are returned upon employee termination.

Clarification/Intent

The organization has a documented policy that requires the return of the organization's property as well as technical controls to delete data and track the location of the property.

Assessment Team Guidance

Many insiders have exploited organization-owned property following termination. Controls for IT property should address the following:

- company laptops that may be used to enter organization systems
- software products that may have national security implications
- products on which the organization's competitiveness depends

MERIT Example

The insider, a foreign national, was formerly employed as a systems analyst, database administrator, and project manager by the victim organization, a government entity. The insider filed a complaint with Human Resources (HR) against her supervisor for harassment and discrimination, but the complaint was unaddressed. Subsequently, the insider's work performance declined. Consequently, she received negative performance reviews, was demoted by the removal of her project manager status, and suspended for 4 calendar days. The insider filed a complaint with the Equal Employment Opportunity Commission (EEOC), but the complaint was denied. The insider was also being treated for depression and insomnia. The insider resigned, did not return the organization's equipment or software, and took a position with another government entity. The insider was upset that the victim organization forwarded her negative performance reviews to her new employer. 2 months after her resignation, the insider remotely dialed in to the victim organization's systems and used a former colleague's ID and password to authenticate and enter a database. The insider deleted 2 weeks' worth of critical data and dropped 11 out of 30 table spaces from the database. The incident was detected when the system failed. Remote access, database, and ISP logs connected the insider to the incident. The insider was arrested, convicted, ordered to pay $35,000 restitution, and sentenced to 5 months home detention 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 has a documented policy and procedure for employee termination that includes immediate return of assigned IT property, hardware, and software.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has technical mechanisms to perform remote deletion of any unrecovered software and data from the organization's property.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has technical mechanisms for location tracking of mobile IT property, including laptops and PDAs.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has a procedure to pursue legal avenues to recover IT property (e.g., warning letters).

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 # IT6.3: Enhanced Monitoring

The organization has policies and controls to restrict employees' access and monitor their online activity after they announce their pending resignation or termination.

Clarification/Intent

The organization has policies and controls for restricting the access of employees with known pending termination, whether voluntary or involuntary. The organization has policy allowing monitoring of departing employees.

Assessment Team Guidance

Many insiders have exploited unfettered access to their organization's systems to harm the organization after they announced or were informed of their pending termination. Policies and controls to look for include restrictions on the terminating employee's access outside normal working hours and limiting the employee's access to only those areas needed during transition.

Additional controls that might exist could also address an employee who is leaving to work for a competitor or a company that could be initiating a new product line to compete with the organization; or controls to address temporary workers who are told that their employment will be ending.

MERIT Example

The insider, a foreign national, was employed as a computer engineer by the victim organization, an enterprise networking company. As a team leader, the insider had access to the victim organization's proprietary information. After accepting a position with a competitor, the insider announced his resignation. The night before his last day of employment, the insider evaded the victim organization's card access system, presumably by walking in behind another employee. The insider used another employee's workstation to download personal files and company proprietary information onto discs. A co-worker reported this incident, leading to the insider's detection. The insider subsequently used his remaining vacation time to finish out his employment term. During this time, the insider had continued access to the company's network. Approximately a month after his last day, the insider had an exit interview and signed a non-disclosure agreement. The insider was eventually arrested, convicted, and sentenced to 3 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 a policy to restrict employees' access before pending termination.

Doc Rev

Dir Obs

Intvw

☐ The organization has controls to restrict employees' access before pending termination.

Doc Rev

Dir Obs

Intvw

☐ The organization has a policy to increase monitoring of a terminating employee's account activity.

Doc Rev

Dir Obs

Intvw

☐ The organization has controls to increase monitoring of a terminating employee's account activity.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization is able to respond to abnormal account activity.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has documented procedures in place limiting access of terminating employees to only those areas needed during transition.

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 # IT6.4: Notification of Employee Separation

The organization has a process for notifying others when an employee terminates.

Clarification/Intent

The organization has a process for notifying all internal departments and external entities within 24-48 hours of when an employee terminates.

Assessment Team Guidance

Inadequate notification of employee termination has sometimes facilitated malicious insider actions. The termination process should include notification of business partners and applicable third parties.

-

MERIT Example

The insider was employed as a design engineer by the victim organization, a high technology company that developed and manufactured computer chips.. The insider's wife was also employed by the victim organization, but at a different location in another state. The insider was seeking employment with a competitor organization while his wife was in the process of transferring to the location where the insider worked. A month later, the insider received and accepted an offer from the competitor organization. The insider delayed his start at the competitor organization for nearly 4 months. The month after receiving the offer from the competitor organization, the victim organization gave the insider a poor performance review. 2 months later, the insider's wife's transfer request was approved. Within hours, the insider announced his plan to resign from the victim organization and to use accrued vacation time to close out the remainder of his employment there. The insider told the victim organization that he would be working in a different industry, and falsely stated that he had returned the victim organization's intellectual property (IP), including documents and data. Around this time, the insider began his employment with the competitor organization and was briefly simultaneously employed by both organizations. During the insider's vacation, the insider remotely accessed the victim organization's network and downloaded trade secret documents. The insider accessed the victim organization's network twice over a 2 day period. After rumors began circulating that the insider had gone to work for the competitor, an investigation began and the incident was detected. Access logs connected the insider to the incident. At the insider's residence, authorities discovered over 100 of the victim organization's confidential and proprietary documents stored on an external hard drive. One of the documents explained how the victim organization's encrypted intellectual property could be reviewed when not connected to the network. The insider was arrested and convicted. The insider, who pleaded not guilty, said that he was motivated by curiosity and because he was mentoring his wife. The organization responded that the insider's wife would not have been working on that specific project. The organization claimed that the stolen documents were worth $1 billion. The competitor organization was not involved in the incident.

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 procedures that ensure that all internal departments, including IT, HR, and physical security, are made aware of the impending departure of terminating employees within 48 hours of announcement.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization has documented procedures that ensure that all relevant external entities, such as customers, vendors, and business partners, are made aware of the impending departure of terminating employees within 48 hours of announcement.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization has documented procedures that ensure that all internal departments and all relevant external entities are made aware of the impending departure of terminating employees within 24 hours of announcement.

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 # IT6.5: Termination Procedures for TBP

The organization has a process for responding to the termination of a contractor or employee of a trusted business partner.

Clarification/Intent

The organization should have a process for responding when a contractor or employee of a trusted business partner is terminated.

Assessment Team Guidance

An organization needs to respond quickly to notification that one of its contracting agencies has terminated an employee working at the organization, to prevent that employee from taking out his or her disgruntlement on the organization. Controls should, for example, immediately revoke computer accounts of business partners when the relationship is terminated

-

MERIT Example

The insider, a contractor, was formerly employed as an information technology (IT) technician by the victim organization, an oil-exploitation company. The organization hired the insider as a temporary consultant to assist in setting up a Supervisory Control And Data Acquisition (SCADA) system. SCADA enables the organization to communicate with its offshore platforms and to detect pipeline leaks. The insider's contract was about to expire when he filed a request for permanent employment. The organization rejected the request and the insider's employment subsequently ended. The organization failed to disable the insider's administrative accounts and remote access. During the 2 months following his termination, the insider planted malicious programs on the organization's systems that temporarily disabled the organization's SCADA system. The insider was arrested, convicted, order to pay $50,000 restitution, and sentenced to 5 years of probation including 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 a process for notifying relevant IT staff of termination of vendors or trusted business partners employee.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a response mechanism to terminate access rights and permissions after receiving notice of a vendor's or trusted partner's employee termination.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ IT staff are notified and access and permissions are removed within 24 hours of a vendor or trusted business partner employee termination.

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 # IT6.6: Disabling Computer Accounts on Termination

The organization has policies and controls for disabling computer accounts and changing shared account passwords upon suspension, resignation, or termination of employees.

Clarification/Intent

The organization has policy and controls for disabling computer accounts and changing shared account passwords upon suspension, resignation, or termination of employees as well as the ability to track all accounts.

Assessment Team Guidance

Many insiders have used system access paths that were unknown to, or forgotten by, the organization to commit their malicious activities. Teams should look for the following types of information:

- All computer accounts associated with a terminated employee are known.
- Controls address system administrator accounts, DBA accounts, network administration accounts, voice mail systems, administration accounts, user accounts, VPN accounts, and remote access applications.
- Controls address company accounts used for purchasing.
- Controls address company accounts to third-party systems, for example, customer sites.
- Controls address accounts for individuals who have been suspended but not terminated.
- Controls address accounts that may have been set up temporarily, such as accounts for training or to test system functionality.
- Controls address revocation of authorized access to external organization systems, especially access that is infrequently used.

MERIT Example

The insider was formerly employed as a doctor by the victim organization, a hospital. The insider was terminated by the organization. Over the course of a month, the insider accessed 957 patient records and downloaded 339 of the patients' medical images. The patient records contained medical images, name, exam dates, exam details, gender, age, medical record number and date of birth, did not include social security numbers (SSNs) or financial information. To conceal his actions, the insider used a former colleague's credentials to remotely access the organization's network outside of work hours. The organization did not alert employees to change any passwords they may have shared with the insider. The insider used the information to contact former patients and offer his services at a competitor organization. Patients reported the insider's activities to the victim organization, which investigated the matter. It is unknown whether any legal actions were taken against the insider.

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 and procedure for disabling computer accounts for employees upon suspension, resignation, or termination.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has the ability to track all accounts—both individual and shared—to which specific employees have access.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The above policy calls for account disabling immediately on the effective date of the employee's departure.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a policy and procedure for changing passwords to all the shared accounts departing employees has access to.

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 # IT6.7: Device Modification by Terminated NetAdmins

The organization prevents, detects, and responds to terminated network administrators who access and modify network device configurations.

Clarification/Intent

The organization prevents, detects, and responds to terminated network administrators who access and modify router and/or switch configurations after termination.

Assessment Team Guidance

MERIT Example

The insider was formerly employed as a network administrator by the victim organizations, jointly owned transportation companies. For unknown reasons, the insider was terminated. During his employment, the insider had administrator-level passwords and privileges for all of the companies' computer operations. The computer network was used for both organizations and no outside services were performed. The exact location and time of the attack are unknown, but the attack was presumably remote and took place at the insider's residence. During a 2 week period, the insider hacked into the victim organizations' computer systems, changed passwords; and deleted specialized software, the companies' customer database, and other records. The insider's actions shut down the organizations' servers, websites, and internet-based credit card processing system. Employees detected the attack when they were unable to use their computers. The organizations reported the attack. During a search of the insider's home, investigators found information related to the organizations' computer systems, a file folder marked "retaliation," and several computers. The insider was arrested and convicted, but sentencing details were unavailable. The organizations lost thousands of dollars because they were unable to dispatch drivers without their computer systems.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

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

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has a configuration management tool that specifically addresses changes to network device configurations (e.g., Tripwire).

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented policy and procedure that requires revocation of access rights to departing network administrators immediately upon change of their employment status.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization detects unauthorized device access or access attempts.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization responds to unauthorized device access or access attempts.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization ensures that retained network administration staff have the same requisite skills as departing network administrators.

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 # IT6.8: Disable Connections on Termination

The organization disables remote connections that might be open to terminated employees.

Clarification/Intent

The organization should have policies and procedures for disabling remote connections that might be open to terminated employees.

Assessment Team Guidance

Organizations may overlook remote connections that are not closed when a terminated employee's account is disabled.

MERIT Example

The two insiders were formerly employed as managers by the victim organization, a parts manufacturer. At the time of the incident, the insiders were employed by a competitor organization. The insiders used outdated credentials to remotely access the victim organization's systems and obtain proprietary information. Systems administrators at the victim organization changed the credentials, but the insiders were able to guess the new credentials and access the system again. The insiders accessed the organization's systems on at least 12 occasions. The insiders were arrested, convicted, ordered to pay $72,000 restitution, and sentenced to 3 years of probation including 6 months of work 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 documented policy and procedures for disabling any form of network connectivity for terminated employees, including opening remote connections.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Upon employee termination, the organization audits existing remote or VPN connections to ensure accounts of terminated employees are no longer active.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a procedure for preserving logs and other evidence so that it may take legal action against terminated employees attempting to exploit unauthorized, open connections to the organization's network.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization disables connections of terminating employees and contractors.

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 # IT7.1: Resource DoS

The organization prevents, detects, and responds to a user who, either accidentally or deliberately, executes system programs that are resource-intensive enough to disable a server.

Clarification/Intent

The organization prevents, detects, and responds to a user who, either accidentally or deliberately, executes system programs that are resource-intensive enough to disable a server.

Controls address mechanisms to provide availability of critical resources by understanding normal activity levels and alerting personnel to deviations.

Assessment Team Guidance

Some insiders have executed programs that disrupted their employer's operations.

MERIT Example

The insider was formerly employed as a systems administrator by the victim organization, a blogging service. The organization discovered that the insider had been stealing from the company and terminated his employment. Subsequently, while on site and during working hours, the insider did a slash-and-burn on some servers and wiped out the organization's SQL database. The organization discovered the incident and attempted to recover the data. A data recovery service discovered not only that the data had been overwritten, but also that the insider relied on RAID as the only backup mechanism for the SQL server. The insider set up automated backups for the HTTP server which contains the PHP code, but had no backup system in place for the SQL data. The data loss was permanent and essentially destroyed the organization's business. It is unknown whether criminal charges or a civil suit was filed against the insider.

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 establishes baselines of normal system activity levels.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization detects deviations from normal system activity levels and alerts the appropriate security personnel.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has procedures for containing and analyzing resource-intensive processes.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization responds to the discovery of resource-intensive processes when they are found to be undesirable.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has controls to prevent resource-intensive processes from disabling a server.

Doc Rev

Dir Obs

Intvw

☐ The organizational risk assessments identify resources which could affect business processes if victimized by DoS activities.

Doc Rev

Dir Obs

Intvw

☐ The organizational IT and security staff receive training on how to establish baselines and properly interprete identify resources which could affect business processes if victimized by DoS 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 # IT7.2: Public Access to Sensitive Information

The organization has policy and controls governing download of sensitive information by external entities not associated with an employee or business partner.

Clarification/Intent

The organization has policy governing download of sensitive information from external sites not associated with an employee or business partner. The organization also has the ability to detect and respond to unauthorized external entities attempting to gain access to information via internet capabilities.

Assessment Team Guidance

Some insiders have participated in, or facilitated theft of, information from sites not connected with the organization. The controls should provide restrictions on downloads from sites associated with known competitors, for example,

-

MERIT Example

To Be Supplied

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

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

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has a documented definition of what information is authorized to be accessible via internet capabilities.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has mechanisms to detect unauthorized external entities attempting to gain access to information via internet capabilities.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has an incident response plan to address unauthorized external entities attempting to gain access to information via internet capabilities.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has controls that prevent downloads from sites associated with known competitors.

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 # IT7.3: Release of Sensitive Information

The organization prevents, detects, and responds to employees' unauthorized communication of IP, classified information (CI), and other confidential information to external parties, including competitors and foreign governments.

Clarification/Intent

The organization prevents, detects, and responds to employees' unauthorized communication of IP, CI, and other confidential information to external parties, including competitors and foreign governments.

Assessment Team Guidance

Some communications, both internal and external, have signaled insiders' intent or motivation to steal information. The team should determine the following:

- Controls protect against communicating confidential information to primary competitors.
- Controls address internal communications that might involve plans to communicate information externally.
- Controls address unauthorized communications with company customers.

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.

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 data classification system that clearly indicates which data are sensitive or confidential.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization formally defines which employees are allowed to access and transmit sensitive information.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a documented definition of official usage, including specific restrictions, regarding sensitive information.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has mechanisms that scan for sensitive information that is illegally stored on employee workstations, stored in electronic mail formats on network servers, and transmitted over the network (i.e., by keyword, file name, etc.).

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization detects abnormal mass-data transfers (i.e., greater than 1 GB), including email attachments.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has alerting mechanisms to notify staff of suspicious activity.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has documented procedures regarding storage and destruction of sensitive information and any media that held such data.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization defines disciplinary actions for unofficial use of sensitive information and its unauthorized storage, transmission, and transportation.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has controls to prevent employees from sending sensitive information to external parties.

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 # IT7.4: Communication Applications

The organization has policies and controls on using communication applications, such as IRC chat, at work.

Clarification/Intent

The organization has policy to address the use of communication applications, such as IRC chat, at work and controls that detect and prevent unauthorized communication methods.

Assessment Team Guidance

Some insiders have used IRC chat at work to pass confidential system information.

MERIT Example

The insider was employed as a technical support employee by the victim organization, an internet service provider (ISP). The insider and an outsider, a friend, used customer accounts, which were expired but not disabled, to access the organization's network and communicate via IRC chat. The insider's internet access was suspended because his supervisor discovered unauthorized programs on his machine, specifically a credit card number verification program and a network sniffer. The outsider accessed company systems, perused email, monitored the network, and ran a sniffer, which emailed him results every morning. The outsider obtained multiple other user IDs and passwords, which he used to attack the organization's systems. The insider worked with the outsider to deface the organization's website, specifically by changing a picture. The outsider obtained root access via a buffer overflow. The insider and outsider, who had several aliases, had extensive ties to hacker groups, attended organized hacker meetings, and discussed their activities at length in online IRC chat sessions. A co-worker of the insider discovered that the insider was attending organized hacker meetings. The insider responded by threatening his co-worker's health via IRC chat. Access logs connected the insider and outsider to the incident. During the investigation, the insider asked a friend to keep discs with company information on them. The duration of the incident was approximately 1 month. The insider was arrested, convicted, ordered to pay a $4,000 fine, and sentenced to 1 year 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 clearly stating which internet communication methods are authorized and which are unauthorized.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The above policy restricts internet chat and/or instant messaging services.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The above policy discusses appropriate and inappropriate uses of internet social networking services, including the need to keep trade secrets, confidential information, or attorney-client information private.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization detects network connections that use unauthorized communication methods.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization prevents network connections that use unauthorized communication methods.

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 # IT7.5: External DoS Prevention

The organization has controls in place to limit the damage from an external denial-of-service (DoS) attack.

Clarification/Intent

The organization has the ability to detect and respond to external DoS attacks.

Assessment Team Guidance

One insider tried to prove that his organization was vulnerable by initiating an external flood attack on his organization's systems.

MERIT Example

The insider was formerly employed as a data communications manager by the victim organization, a retailer. The organization terminated the insider's employment due to problems with an email server. The insider posted employees' login credentials and detailed instructions on how to use those passwords to hack into the organizations network onto an online internet hacking group posting board. Over a period of several days, the insider also remotely accessed the organization's network and made multiple attempts to conduct a denial of service attack (DoS). The insider's goal was to deny the organization computer services at the beginning of the holiday shopping season. Personnel at the organization detected problems in the network that were obstructing online sales and promptly responded to the incident. The insider was arrested, convicted, sentenced to 18 months imprisonment, and ordered to pay $64,000 restitution. The duration of the incident was approximately 1 week and the incident related impact was $70,000.

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 records a baseline of normal network activity.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a firewall or intrusion protection system (IPS) in its perimeter that can detect DoS or distributed denial-of-service (DDoS) attacks

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has agreements in place with an ISP to block DoS packets before they reach the organization's perimeter.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has the ability to automatically detect deviations from the above baseline.

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)