Carnegie Mellon University
Software Engineering Institute

Insider Threat Vulnerability Assessment (ITVA)

Data Owners Capability Area

https://www.sei.cmu.edu

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

DM23-0882

Table of Contents

Introduction 1

Generic Clarifications 2

Capability Sequence # DO1.1: Expired Accounts 3

Capability Sequence # DO1.2: Separation of Duties 7

Capability Sequence # DO2.1: Modification of Critical Software/Data 12

Capability Sequence # DO2.2: Application Exception Handling 17

Capability Sequence # DO2.3: Data Accuracy 21

Capability Sequence # DO2.4: Data Deletion Causing a DoS 26

Capability Sequence # DO3.1: Attempts to Exceed Authorized Access 30

Capability Sequence # DO3.2: Out of Scope Detection 35

Capability Sequence # DO3.3: Data Downloads 40

Capability Sequence # DO4.1: Tracking of Organization IT Assets 46

Capability Sequence # DO4.2: Employee Access Management on Separation 50

Capability Sequence # DO4.3: Communication of IP Ownership 54

Capability Sequence # DO4.4: Monitoring of Customer Complaints 59

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.

This module measures the vulnerability of an organization to the exploits featured in cases in the CERT insider threat database, targeted specifically at data repositories. Data repositories can include databases or any other logical repository of data with common access. A "data owner" is an individual with full custodial and administrative rights over a given set of data. The data owner can authorize or deny access to certain data and is responsible for its accuracy and integrity.[1]

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

[1] From www.businessdictionary.com/definition/data-owner.html

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 # DO1.1: Expired Accounts

The organization manages shared, dormant, and expired accounts.

Clarification/Intent

The organization has controls governing shared, dormant, or expired accounts on systems or applications the data owner is responsible for.

The organization has controls to manage computer accounts used by customers, if applicable.

Assessment Team Guidance

Shared accounts were used in multiple insider cases.

Data owners should pay particular attention to the management of shared, dormant, and expired accounts that are controlled by the data owner, rather relying on the IT department.

If the data owner responds that IT manages all these accounts, the assessment team should ensure that this capability is addressed in the *Information Technology* workbook.

MERIT Example

A director of IT was promoted to VP of technology for a company that published financial market information. The insider was responsible for the computer network and internal email system. Three years after termination, they remotely accessed the internal email system using credentials that were unchanged since termination and spied on email traffic for over 5 months. A Yahoo account was used to notify two employees of their potential terminations, and they reported this to their supervisors.

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 regularly audits user accounts for

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ shared accounts

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ dormant accounts

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ expired accounts

  Doc Rev _____

  Dir Obs _____

  Intvw _____

Level 3

☐ The organization has a procedure that disables shared, dormant, and expired accounts.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has alerts that identify expired and dormant, and potentially shared user 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 # DO1.2: Separation of Duties

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

Clarification/Intent

The organization has business processes governing control of a critical application or database by a single employee.

There are appropriate controls to ensure that a single individual is not responsible for modifying data and checking its integrity.

Assessment Team Guidance

Insiders have often used excessive privileges to commit crimes.

Even if the data owner is the sole custodian of a particular critical repository, the organization should have processes and systems in place requiring other individuals to check the integrity of the data. For example, any changes to critical data should be verified and validated by a party other than the data owner.

MERIT Example

The insider was originally employed as an e-commerce software developer for the victim organization, which produced manufacturing equipment for computer chips. When the insider decided to move to a different state, the organization wanted to retain him as an employee. Due to lack of legal presence in the insider's new domicile, the insider could no longer be a full-time employee for the organization. The insider became a contractor consultant for the organization and was permitted to work from home by remotely logging into the organization's servers during normal working hours. The insider's relationship with the organization continually deteriorated because he considered the benefits he received as a contractor inadequate. The organization notified the insider that his employment would be terminated in one month. A week and a half after receiving notification of his termination, the insider remotely logged into the organization's network, during work hours, and deleted software he was developing as well as other software in development. To conceal his actions, the insider changed the root password, modified system logs, and also reported having problems logging in. The insider resigned at the end of the day. The insider was detected when the organization noticed the lost data. Forensic audits revealed that the server had been accessed from the insider's ISP's domain. The victim organization spent nearly $27,000 to recover the data. The insider was arrested, convicted, ordered to pay $27,000 restitution, 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 identifies which processes are considered critical.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has policy that requires separation of duties (or other methods of checks and balances) for critical processes.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization periodically audits new and existing processes completed by a sole individual whose authority over the repository has no checks and balances.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has IT controls to prevent granting excessive privileges to employees.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Prior to the implementation of new processes, the organization determines if separation of duties is required, and designs and includes them as necessary.

Doc Rev

Dir Obs

Intvw

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

Justification

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

Notes (from documentation, observations, and interviews)

Capability Sequence # DO2.1: Modification of Critical Software/Data

The organization prevents, detects, and responds to unauthorized modification of critical software and data.

Clarification/Intent

To maintain data integrity, the organization has policy and procedures that focus on preventing unauthorized data modification. The organization has controls to maintain nonrepudiation of user actions or transactions in its identified critical systems and databases.

Assessment Team Guidance

Modification, in this workbook, includes any additions, deletions, or revisions.

Insiders have taken advantage of poor integrity controls to insert malicious code or bad data. Assessors should determine how the organization validates changes to data, systems, and software. This could include but not be limited to

- modification of source code
- modification of data in critical systems
- modification of system configuration
- modification of baseline software (new software, disable virus software)
- addition of unauthorized hardware

One of the indicators looks at tracking manual processes. Manual processes usually refer to an "exception" to a normal business process. For example, A DMV that has to manually look up an individual (if they lost their driver's license). A case worker who has to make a phone call to verify the eligibility of someone requesting benefits. Organizations want to be able to identify any steps that could intentionally or unintentionally be skipped or missed causing a business process to not be completed (entirely).

MERIT Example

The insider was employed as an engineer by the victim organization, which developed software for utility companies. As a function of his job, the insider had unlimited access to modify code. Over 75% of the organization's employees were upset that they were not receiving a bonus, and the insider was also upset that he did not receive a promotion. While on site and presumably during work hours, the insider developed two versions of a logic bomb, which were set to self-initiate and randomly insert the letter "i" (octal value 0151) into a communications stream. The logic bombs were designed to affect a specific software package that was crucial to the organization's business operations. The insider shared an office with the lead developer, who often left his workstation on. The insider used the lead developer's workstation to check-in the modified code with the logic bombs. 7 months later, the insider voluntarily left the company. At some point, the insider called the organization and asked a current employee whether anything happened with the software and if "attorneys were involved yet." 5 months after the insider left the company, one of the logic bombs detonated and disrupted communication transmissions. The incident was detected by customers, who reported that they could not use the software. Software developers at the organization discovered the octal code, removed the logic bombs, and re-issued the code, costing the organization over $16,000. The lead developer suspected that the insider was responsible for the incident, which was connected to the insider through audit logs. The insider was arrested, convicted, ordered to pay $16,000 restitution, and sentenced to 180 days of home detention and 80 hours of community service. The duration of the incident, from the creation of the logic bomb to its detonation, was over a year. While employed by the victim organization, the insider was known as the office prankster.

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 identified their critical software and data.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization validates changes to critical data, systems, and software.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization tracks manual processes.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has a documented procedure for handling the modification of critical software or data.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has controls to maintain data integrity for critical manual processes, such as manual data entry.

Doc Rev

Dir Obs

Intvw

☐ *The organization has IT controls to maintain nonrepudiation of user actions and transactions in its systems and 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 # DO2.2: Application Exception Handling

The organization handles exceptions in applications.

Clarification/Intent

The organization has controls governing how data owners build and maintain their systems and applications.

Exceptions in applications can allow end-users to circumvent the controls enforced in the normal business process.

It is important that applications enforce some kind of controls when exception or expedited processing or functions are used.

Assessment Team Guidance

The organization should apply the same, or more, scrutiny to exception handling as it does to normal processing. Many times exception handling (particularly expedited processes) do not include the same level of verification or separation of duties. This could allow an individual to bypass normal validation. The organization should also monitor data auditing. The assessment team should determine if the organization has strategies for exception processing and, if so, their effectiveness.

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

☐ If exception handling is permitted, the organization logs those transactions.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Each transaction is attributable to a single user in the organization.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization audits data logged by exception handling processes.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ If exception handling is permitted, the organization monitors transactions for improper usage.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Alerts are automatically raised when exceptions processing occurs.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Alerts are reviewed on a regular basis.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Unauthorized exception transactions are identified.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Unauthorized exception transactions are investigated and remediated.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has a process for incorporating exceptions into normal business processes.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Prior to the completion of an exception transaction, review and approval is obtained.

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 # DO2.3: Data Accuracy

The organization prevents, detects, and responds to incorrect data before it is entered into critical applications.

Clarification/Intent

The organization has controls allowing for the prevention of, detection of, and response to a situation where critical data is incorrectly entered or modified. Incorrect, in this instance refers to invalid, incomplete, or inaccurate data.

Assessment Team Guidance

Examples of the types of controls that might be in place include but are not limited to

- controls to detect or prevent the processing of incomplete data, where essential information is missing. Examples could include customer names where there are not both first and last names, phone numbers that do not have all the required numbers.
- Controls to detect or prevent invalid data from being accepted and processed Examples could be alpha data entered into a numeric field or data larger than the value being requested.
- Controls to detect or prevent inaccurate data from being accepted and processed such as credit card charges against an account where the owner is deceased.

MERIT Example

The insider was employed as an administrator in the human resources (HR) department of the victim organization, a business telecommunications technology provider. Prior to the incident, the insider had recently changed job roles within the organization. The organization failed to deactivate the insider's access to payroll systems. The insider was able to exploit this access and defraud the organization. The insider used records of the organization's terminated employees to falsely indicate that they were rehired at a higher pay rate. The insider funneled the pay into personal bank accounts. An internal audit revealed the fraudulent activity. The insider was arrested, convicted, sentenced to 15 months imprisonment followed by 3 years or probation, and the insider was prohibited from working in financial institutions. The incident related impact was $200,000.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

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

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has controls in place that prevent the entry of incorrect data including:

Doc Rev _____

Dir Obs _____

Intvw _____

☐ preventing the entry of invalid data.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ preventing the entry of incomplete data

Doc Rev _____

Dir Obs _____

Intvw _____

☐ preventing the entry of inaccurate data.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has detection mechanisms in place that alert if incorrect data entry is attempted.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a response mechanism in place in cases where attempts to enter incorrect data is identified.

Doc Rev

Dir Obs

Intvw

Level 4

☐ Employees and trusted business partners are trained to understand what type of data is invalid, incomplete, and inaccurate.

Doc Rev

Dir Obs

Intvw

☐ Employees and trusted business partners are trained how to address attempts to enter incorrect data.

Doc Rev

Dir Obs

Intvw

☐ Controls to prevent incorrect data entry are included in requirements for any new software or business processes.

Doc Rev

Dir Obs

Intvw

☐ Controls to prevent incorrect data entry are periodically reviewed for effectiveness and revised as needed.

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 # DO2.4: Data Deletion Causing a DoS

The organization prevents, detects, and responds to data deletion that would result in denial of service.

Clarification/Intent

The organization protects data from deletion that may cause a denial of service (for example, loss of data that could cause customer areas to be offline).

The organization has controls governing physical and digital destruction, modification that results in deletion, and other actions on data that would result in denial of service.

Denial of service in this case means that because the data is unavailable, a critical business process, service, or system could not operate.

Assessment Team Guidance

The organization should have controls to prevent and detect physical destruction of critical data. For example critical data for a manufacturing company may be customer, payment, or billing information.

Such data deletion resulting in unavailability of services or processes might also be done as an act of sabotage.

MERIT Example

The insider, a computer programmer for a hospital, inserted a logic bomb on two separate occasions while employed there. The insider worked on a computer based training program for hospital employees. After resigning, the logic bomb went off approximately 2 months after the insider's departure. The victim organization noticed that they were unable to use the training program and contacted law enforcement.

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 data that, if deleted, might impact operations or institutional knowledge.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization monitors data that has been identified as impacting operations if deleted. This includes monitoring for

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ physical destruction

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ digital destruction

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ modification that results in deletion

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ other actions on data that would result in denial of service

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a policy which outlines when and how data can be destroyed both physically and digitally.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has data controls which detect modifications and deletions of data which could result in a denial of service or impact to operations.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a response plan for when data is deleted and causes denial of service.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Employees and trusted business partners are trained to properly handle and protect data that has been identified as causing a denial of service or impact to operations if deleted.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Data that has been identified as causing a denial of service or impact to operations if deleted, is backed up on a daily basis.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Data that has been identified as causing a denial of service or impact to operations if deleted, is readily available from backups.

Doc Rev

Dir Obs

Intvw

☐ Backups of data that has been identified as causing a denial of service or impact to operations if deleted, are tested on a regular basis to ensure integrity.

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 # DO3.1: Attempts to Exceed Authorized Access

The organization has the ability to detect employee and trusted business partner attempts to exceed authorized access.

Clarification/Intent

Exceeding authorized access includes activities such as hacking, escalating operational system account privileges, exceeding role-based access control (RBAC) levels, and so on.

The organization should have controls in place that prevent and detect employees or trusted business partners from exceeding their authorized access to systems or applications. Alerts to appropriate personnel about the unauthorized attempts should then be responded to.

Assessment Team Guidance

The organization should restrict and monitor employees' access when they transfer jobs within the organization and require different privileges to data and systems.

If the organization allows data-owner-controlled systems that may not have standard security controls, the organization should ensure that such systems are secured to the same level as standard systems.

MERIT Example

The insider, a subcontractor, was employed by an organization that was contracted to set up and support a network for the victim organization, a government agency. Midway through the project, the contractor decided to employ another subcontractor, effectively terminating the insider's employment. The disgruntled insider used remote access, outside of work hours, to access the organization's network. The insider increased the privileges of a user's account to create a backdoor and began sabotaging the organization's network. The insider had system administrator access to the organization's entire computer system, either as a function of his former job or through the escalation of privileges on the user account. The insider deleted employee's passwords and potentially accessed email. To conceal his tracks, the insider attempted to delete all system logs, but this action crashed the system. IT staff detected the incident and performed forensic analysis. The insider was arrested, but details regarding the verdict 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 checks logs or has a detection mechanism for employees' and trusted business partner attempts to exceed authorized access.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization executes their response plan or policy regarding employees who are discovered exceeding their authorized access.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has controls to prevent employees and trusted business partners from exceeding their authorized access to systems or applications controlled by data owners.

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 # DO3.2: Out of Scope Detection

The organization has the ability to monitor employees' activities in order to detect usage inconsistent with their job responsibilities.

Clarification/Intent

The organization monitors critical systems in an attempt to identify activity inconsistent with employee and trusted business partner's job responsibilities.

The organization provides mechanisms for data owners to monitor employees' usage of their systems and applications.

Assessment Team Guidance

The organization should be able to detect employees' attempts to

- query data outside job responsibilities
- access files, applications not required for job
- access others email

The organization should have a process that restricts and updates employees' access when they transfer jobs within the organization and require different privileges to access or work with data and systems due to changing job responsibilities.

MERIT Example

The insider, a contractor, was formerly employed as a software developer and tester by the victim organization. The insider was terminated for poor performance and was subsequently employed by a non-competitor organization. The organization failed to change a shared account password upon the insider's departure. The insider used his company laptop assigned to him by his new employer to remotely access 24 of the victim organization's user accounts. The insider ignored banner warnings indicating that unauthorized access or attempted access was a criminal violation and that the computer system was subject to audit and that federal laws provided penalties for unauthorized use. To conceal his actions, the insider edited rhost files. An employee at the victim organization discovered that she had been logged on to her machine just a few hours earlier when in fact she had not, prompting a cooperative investigation by both the insider's current and previous employers' security divisions. Security personnel at the insider's current employer traced the intrusions to the insider's laptop and confronted him. The insider made several claims, including that he only logged on to check on a program he wrote; that he had not been fired from the victim organization, but just had not had his contract renewed; that he was asked to login by an ex-coworker to help with a problem, and that he was playing a break-in game/contest with his ex-coworkers to find flaws in the victim organization's network. The insider was arrested, convicted, and sentenced to two concurrent 2 year terms of probation, as well as unspecified fines and penalties. The insider exploited 13 systems storing trade secrets valued at approximately $1.3 million.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

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

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization provides mechanisms for data owners to monitor employees' usage of their critical systems and applications and detect anomalies.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a policy that defines access to the organization's critical assets commensurate with job responsibilities.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Employees have clearly defined position descriptions that outline roles and responsibilities within the organization.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Position descriptions define access to the organization's critical assets.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ .When access beyond job responsibilities is detected, it is addressed and handled.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ When personnel changes occur (e.g., promotion, demotion, transfer, hire, resignation, or termination), access to critical assets is reviewed to ensure appropriate privileges are granted to/revoked from the individual impacted by the personnel change.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization provides mechanisms for data owners to monitor employees' usage of all systems and applications and detect anomalies.

Doc Rev

Dir Obs

Intvw

☐ The organization creates employee baselines based on employee usage 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 # DO3.3: Data Downloads

The organization monitors data downloads.

Clarification/Intent

The organization monitors data downloads to as part of their process to prevent data exfiltration. Downloads of proprietary or sensitive information could indicate that an employee or trusted business partner is obtaining information that it might exfiltrate. By collecting information on downloads, an organization may see the potential for malicious actions.

The organization has controls governing downloads both onto employees' and trusted business partners such as contractors' workstations and external media.

The organization's policy and procedures with respect to downloads applies to all systems and applications controlled by data owners.

Assessment Team Guidance

The organization should be able to monitor downloads to desktops, removable media, and portable machines. It should also be able to monitor downloads to and from home, downloads printed to paper, and downloads to external sites.

The organization should have special procedures to detect downloads close to the date of employees' termination (within 30 days before).

The organization should be able to prevent and detect downloads of confidential information outside employees' domains of responsibility or within their domains of responsibility but involving a greater quantity of information than usual.

Examples of the types of things the organization should be able to detect include but are not limited to

- large downloads over short periods of time
- downloads before or after normal working hours
- downloads of employee or customer lists and personal information
- downloads of materials shared with business partners
- downloads of materials targeted for disposal
- downloads of intellectual property (IP): strategic plans, source code, scientific designs and formulas, and merger and acquisition plans

MERIT Example

The insider was an executive at a financial organization and was responsible for managing the accounts of some of the larger clients in the region. In an abrupt fashion, the insider and some fellow conspirators resigned from the victim organization, all on the same day. Each reported that they had accepted a new position with the same competitor. A few hours before resigning, the insider had been observed using a mobile device to take photographs of a computer screen but it was not clear why. Computer records demonstrated that the insider had attempted to download confidential customer information a few days prior to resigning, but had been denied due to security measures put in place by the victim organization. One of the conspirators was successfully able to download confidential information and customer lists. Additionally, the insider and conspirators were known to have kept physical copies of customer files in their offices. These files were unable to be recovered after their resignations. "The insider used authorized access to the customer data and attempted to take the data along with physical customer files to a new position. When download restrictions prevented the insider from exfiltrating the customer data, the insider took photos of the computer screen using a mobile device."

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 controls governing downloads both onto employees' trusted business partner workstations and external media.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization monitors for data downloads within 30 days before an employee's termination.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has controls governing downloads via FTP from IPs outside the United States.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has procedures for responding to unauthorized data downloads.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Unauthorized data downloads when detected are addressed and handled.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization monitors for sudden increases of downloads.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization can access employee baseline behavior for use in response activities.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization periodically audits for downloads before or after working hours.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization monitors customer lists for exfiltration.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization monitors personal information for exfiltration.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization monitors materials shared with trusted business partners.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization monitors materials slated for disposal.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization monitors sensitive IP for exfiltration.

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 # DO4.1: Tracking of Organization IT Assets

The organization tracks organization property loaned to employees.

Clarification/Intent

The organization tracks organization property loaned to its employees, including data-owner-owned equipment that IT may not be aware of.

This policy includes all types of removable media, software, and hardware.

It is important to track such assets to ensure equipment is returned upon termination and also that equipment is not taken offsite without approval.

Assessment Team Guidance

Insiders sometimes steal or keep organization property when terminated.

MERIT Example

The insider was formerly employed in the internet technology (IT) department of the victim organization, a cable company. The insider's employment was terminated by the organization. After termination, the insider retained his company laptop and 2 cell phones. The insider used remote access and his own systems administrator account, which the organization failed to disable, to delete software he had written as well as critical data. The deleted software prevented the organization from broadcasting local commercials. The insider left a suicidal voicemail for his former supervisor and claimed that he had shot the company laptop full of holes. The insider had a history of mental illness and was on a variety of psychiatric medications at the time of the incident. The victim organization's systems sustained irreparable damage and were costly to replace. The insider was arrested, convicted, ordered to pay $88,000 restitution, and sentenced to 2 years probation with required participation in mental health and drug rehabilitation programs.

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 hardware inventory.

Doc Rev

Dir Obs

Intvw

☐ The organization has a software inventory.

Doc Rev

Dir Obs

Intvw

☐ The organization has a policy for hardware and software loans.

Doc Rev

Dir Obs

Intvw

☐ The organization has a policy for tracking employee equipment.

Doc Rev

Dir Obs

Intvw

☐ The organization tracks employee provided or loaned equipment.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization requires approval before taking equipment offsite.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization verifies all property is returned upon termination of an employee.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization periodically audits itself for lost or stolen property.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has policies in place to prevent equipment from being taking to international locations without appropriate safeguards and approvals.

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 # DO4.2: Employee Access Management on Separation

The organization manages employees' access after they announce their pending resignation or termination.

Clarification/Intent

The organization restricts access to systems and applications no longer needed by separating employees upon announcement of resignation or termination.

Assessment Team Guidance

In most cases of IP theft, insiders commit their crimes within 30 days before termination.

The organization should restrict terminating employees' physical, local, and remote access to proprietary business information.

MERIT Example

The insider was employed as a specialist by the victim organization, an internet technology marketing firm. After the insider failed to receive a raise and his request for a transfer was rejected, the insider submitted his resignation. The insider subsequently downloaded proprietary information from the victim organization and transferred the information to his home computer via FTP. The insider used both remote and on-site access to download the information. The insider thought the information might be useful at his new job. The insider was arrested, convicted, and sentenced to 180 days in jail followed by 3 years probation. The insider was also required to forfeit his computer.

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 restricts employee access upon resignation or termination to the following, as appropriate:

Doc Rev

Dir Obs

Intvw

- ☐ facilities and sensitive areas

  Doc Rev

  Dir Obs

  Intvw

- ☐ local and remote connections to network and systems

  Doc Rev

  Dir Obs

  Intvw

- ☐ proprietary business information

  Doc Rev

  Dir Obs

  Intvw

Level 3

☐ The organization communicates the employment status of employees to relevant data owners, security guards, IT, and anyone with the potential of being socially engineered.

Doc Rev

Dir Obs

Intvw

☐ Data owners restrict access to systems appropriately when an employee is placed on administrative leave.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization audits access for 30 days before resignation or termination.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization audits access for 30 days after resignation or 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 # DO4.3: Communication of IP Ownership

The organization communicates its policies regarding the ownership of IP.

Clarification/Intent

Data owners reiterate organizational policies regarding the ownership of IP to employees using their systems.

Assessment Team Guidance

Many insiders believed they owned the software they were developing. Clear communication regarding IP ownership can clear up misunderstandings.

The intent of the level 4 indicator related to data owner acknowledgement of IP Ownership Policy, was to be sure that the owners of the data are aware of the policies put in place to protect their data. If the owner acknowledge they are aware of what is in the policy and the employees agree to the policy, there should be no confusion about what should be enforced.

MERIT Example

The insider was employed as a sales representative by the victim organization, a computer manufacturer. A competitor, the beneficiary organization, offered the insider a job. The insider spent 2 months systematically emailing the victim organization's critical, confidential information to his home computer, including customer lists, passwords, and credit reports; marketing and sales plans and promotions, staff commission and incentives paid, quotes requested by customers, material costs and profit margins, and a computer program designed to configure quotations for customers. The insider also accessed accounts assigned to other employees, specifically 4 of the victim organization's largest accounts. The majority of the information was accessed outside of the insider's need-to-know, and the victim organization did not have any restrictions on the disclosure of confidential information. To conceal his systematic theft, the insider deleted the contents of his work computer hard drive at the victim organization. Prior to leaving the victim organization, the insider used a stolen password and a computer at the beneficiary organization to remotely access the victim organization's website and download additional proprietary information. After receiving a formal offer from the beneficiary organization, the insider used email to transfer the victim organization's intellectual property (IP) to a former customer of the victim organization. After beginning his employment with the beneficiary organization, the insider used stolen passwords to continue accessing protected areas of the victim organization's website. Even though the employee handbook prohibited sending documents home, the insider claimed that it was common practice at the victim organization. The insider claimed that the program he "stole" was his own creation, and filed for copyright four months after the victim organization had claimed ownership. The insider also recruited another employee to work for the beneficiary organization. The victim organization obtained an injunction to recover the stolen IP and to prohibit the beneficiary organization from using the stolen IP.

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 regarding the ownership of intellectual property.

Doc Rev

Dir Obs

Intvw

☐ The organization communicates this policy to employees upon hiring and termination.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization requires signed acknowledgement of the intellectual property agreement upon hiring.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization requires signed acknowledgement of the intellectual property agreement upon separation.

Doc Rev

Dir Obs

Intvw

☐ The organization requires trusted business partners to sign acknowledgement of the intellectual property agreement upon hiring and separation.

Doc Rev

Dir Obs

Intvw

☐ The organization communicates this policy to data owners and requires periodic acknowledgement.

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 # DO4.4: Monitoring of Customer Complaints

The organization monitors communications with its customers to see if they have complaints or concerns that might indicate an internal problem.

Clarification/Intent

The organization monitors communications with its customers for complaints or concerns that might indicate an internal problem.

The intent of this capability is to capture input from customers external to the organization, but there may be cases in which customers are internal to the organization. For instance, satellite offices may be considered customers of a parent organization.

Assessment Team Guidance

System administrators and other privileged users sometimes abused their access to harm an organization.

MERIT Example

The insider, a contractor and a foreign national, was employed as a technical support representative by the victim organization, which designed software used to access consumer credit records. The insider's position allowed him to access passwords and codes that enabled him to download individual credit reports. The insider was recruited by an outsider, who was part of a foreign organized crime ring that was unrelated to the insider's home country. The incident was part of a larger organized crime scheme, which continued after the insider resigned from his position. The insider's involvement with the scheme continued for 3 years. The insider used his pre-programmed laptop to download consumers' credit-history records, both on-site and off-site using remote access. The insider's accomplice then re-sold the credit history records, for $60 each, to others involved in the organized crime ring. The members of the crime ring used the information to drain consumers' bank accounts and make fraudulent credit card purchases. At one point, the insider moved out of state, but returned to the victim organization to download credit reports. Eventually, the insider gave his computer to the accomplice, and taught him how to remotely access the organization's network and download the records. The insider continued to provide technical support to the accomplice. The incident was detected when one of the victim organization's corporate customers had received numerous complaints from customers who had become victims of credit card and bank fraud. The corporate customer reviewed bills sent by one of the credit agencies and discovered that thousands of credit reports had been downloaded without permission. The credit agency reviewed database log files and discovered that many passwords and subscriber codes had been compromised. The insider was arrested, convicted, ordered to pay an undetermined amount in restitution, sentenced to 14 years imprisonment, and required to forfeit $1 million he received in profits from the scheme. Financial institutions sustained an approximate loss of $11 million. The incident affected 30,000 consumers, who sustained an estimated $50-$100 million loss. The insider was experiencing financial problems, which motivated him to participate in the scheme.

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 procedure for collecting customer complaints that includes escalation triggers.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has routine quality assurance checks to confirm procedure adherence and issue resolution.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Customer complaints are addressed in a timely fashion.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has an automated process that tracks customer issues.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Customer issues are brought to the attention of appropriate data owners and management in case there is a deeper internal problem.

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)