Carnegie Mellon University
Software Engineering Institute

Insider Threat Vulnerability Assessment (ITVA)

Trusted Business Partners 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 CERT® Program's definition of insiders includes current and former employees and other trusted business partners (TBPs), including contractors, sub-contractors, suppliers, vendors, and others who have or had authorized access to the networks, systems, or data. This workbook assesses whether the departments that deal with TPBs are actively involved in mitigating insider threat risk. Trusted business partners present unique problems for departments such as legal and human resources because some management tasks are often undertaken by the contracting agency. This workbook exists separately from the *Human Resources* and *Legal* workbooks because TPBs and permanent staff likely have different points of contact with the organization. This workbook addresses several issues in insider risk from TPBs, including documentation and communication of policies, compliance with organizational standards, and key contract provisions. Note that a prime contractor will be responsible for their subcontractors and *their* other trusted business partners.

® 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 # TBP1.1: Background Screenings

The organization ensures that all trusted business partners have successfully completed background screenings before they start work.

Clarification/Intent

The organization should require and verify that the contracting agency has its TBPs undergo background screenings of at least the same level of scrutiny applied to the organization's permanent employees.

If the organization wants to access the information discovered during a TBP's background screening, which may be useful during investigations, it may need to alter the standard background screening release form for TBPs.

Assessment Team Guidance

In some insider threat cases, the organization mistakenly thought that the contracting agency had completed background screenings on its TBPs. The insiders that would have been caught by a background screening were able to gain employment at the organization. Background screenings may include checks for

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

MERIT Example

The insider, a civilian contractor, was employed as computer help desk operator by the victim organization's trusted business partner, a military entity. The victim organization manufactured computer networking products. The victim organization issued field notices (recalls) for various parts. For military contractors, defective products did not have to be returned to the victim organization until after the replacement product was received. The insider created fictitious email accounts to request replacement parts. The victim organization presumed that the requests were coming from different individuals that were authorized to request replacement parts. The insider directed the replacement parts to be shipped to either his home address or to a relative's address. The manufacturer sent the replacements, with the expectation that the original recalled products would be returned after the replacements had been received. The insider could not return original items after having received the replacements because he did not have any recalled products. Over 20 months, the insider received 90+ shipments of 500 products with a retail value of over $8 million. The insider sold 90 of these items through an internet auction site for over $500,000. The insider was arrested, convicted, ordered to pay over $8 million restitution, and was sentenced to 51 months imprisonment followed by 2 years of supervised release. The insider later admitted that he needed money to care for his elderly parents.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

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

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization requires the background screening standards of the contracting agency to be commensurate with those of the organization.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization designates a permanent staff member to ensure that TBP background screening is being performed.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization works with legal counsel to modify the TBP's release form so that the organization can view the TBP's completed background checks, at a commensurate level of the assessed organization, on all TBP employees supporting the organization.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Violations in TBP background check performance are addressed.

Doc Rev _____

Dir Obs _____

Intvw _____

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

Justification

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

Notes (from documentation, observations, and interviews)

Capability Sequence # TBP1.2: Trusted Business Partner Management

The organization ensures that trusted business partner management activities are carried out consistently and by the appropriate parties.

Clarification/Intent

The organization should ensure that it is clear which TBP management activities it will perform itself and which will be performed by the contracting agency. In addition, the organization should verify that the contracting agency's management activities are in line with the organization's own policies and standards.

The organization should ensure that it and the contracting agency share information pertinent to an increased insider risk.

Assessment Team Guidance

According to the Society for Human Resources Management, the contracting agency should handle the following activities:

- recreational or social activities (e.g., holiday parties, social events)
- performance appraisals, salary adjustments, employee benefits
- disciplinary action
- EEO/harassment policies, procedures and interpretation
- recognition programs
- training (although specific, job-related training can be done by the organization)
- travel

While the contracting agency may be responsible for certain management activities, the hiring organization should remain aware of any problem areas that may arise for the TBP. Knowledge of violations in one area might lead to inquires in another that expose insider risk.

MERIT Example

The insider, a contractor, was employed by as a system administrator by a data-mining company that was a trusted business partner (TBP) of the victim organization. The victim organization processed consumer data, including customer information for credit-card issuers, banks, automotive manufacturers, retailers, etc. As a TBP organization, the insider's employer had access to the victim organization's FTP server. A lack of proper oversight and access management resulted in the insider having unnecessary privileged access to this server. On the server, the insider discovered an unprotected file containing encrypted passwords. The insider used a password cracking program to brute force the passwords and access data belonging to 200 large companies, approximately 10% of the victim organization's customer database. The insider cracked 300 passwords, including a master key that the insider used to download the personal data for millions of the victim organization's customers. Over a 6 month period, the insider used remote access, outside of working hours, to download the information and burn it to discs. In an IRC chat room, the insider disclosed to a local hacker that he had accessed a great deal of sensitive information. When the hacker's home was raided, authorities discovered a log of the conversation. The insider was arrested after dozens of discs containing the personal data for the victim organization's customers were found at his residence. The insider apparently liked to collect data and did not use the stolen data for commercial or criminal purposes. The insider had a criminal history of illegally accessing computers. The insider was arrested, convicted, ordered to pay $2.7 million restitution, and sentenced to 45 months imprisonment followed by 3 years of supervised release, including a 500 hour substance-abuse program and a mental health assessment and treatment. The insider was prohibited from accessing the internet without his probation officer's permission. The incident cost the victim organization $5.8 million, including the value of the stolen information, employee time, travel expenses, and costs incurred from security audits and new encryption software.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

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

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has a policy which documents which management activities will be carried out by the contracting agency and which the organization will perform itself.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization ensures that any management activities carried out by the contracting agency are in line with the hiring organization's own policies and standards.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization ensures that it and the contracting agency share information pertinent to an increased insider risk.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization communicates its contractor management policy to the trusted business partners.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization designates a permanent staff member to ensure that these management activities are being performed.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization uses a vendor management system to ensure consistent application of policy across TBPs.

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 # TBP1.3: Onboarding for Trusted Business Partners

The organization provides employee onboarding tailored for trusted business partners.

Clarification/Intent

The Society for Human Resource Management states the TBP should be familiar with the organization's missions, culture, policies, and procedures. However, unlike permanent employees, TBPs need onboarding that gives them just enough organizational information to perform their tasks. In addition, TBPs should be aware of workplace behavioral requirements.

Assessment Team Guidance

Setting a TBP's expectations can help prevent disgruntlement, a motivator of insider crime.

Relevant policies and procedures include behavioral policies, such as those in Capability 1.12 of the *Human Resources* workbook.

Areas covered should include but not be limited to

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

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

MERIT Example

The insider, a contractor, was employed as a systems administrator by the victim organization, a government entity. The insider was responsible for monitoring 3 INOMS system servers that the organization relied on. Shortly after being hired

and not long after an employee onboarding process would have concluded, the insider was reprimanded for his frequent tardiness, absences, and unavailability. The insider's supervisor repeatedly warned the supervisor that his poor performance was cause for dismissal. The insider responded by sending threatening and insulting messages to his supervisor. The incident took place for approximately 2 weeks, on site and during work hours. The insider, who had root access on one server and no root access on another server, used his privileged account to create a rhost file that enabled him to access the second server. The insider inserted malicious code into the victim's INOMS servers, which would delete all of the organization's files when the volume reached a certain point. To conceal his activity, the insider turned off system logs, removed history files, and attempted to overwrite the malicious code after execution. After the insider was terminated, he repeatedly contacted the system administrators to ask if the machines and servers were functioning properly, which aroused suspicion at the organization. The organization discovered the malicious code and shut down the system to remove the code and restore system security and integrity, costing the organization at least $5,000. The insider did not succeed in deleting the data. The insider was arrested, convicted, ordered to pay $108,000 restitution, and sentenced to 15 months imprisonment followed by 3 years supervised release. On his job application, the insider had concealed previous arrests related to drug charges and failed to report that he had been fired for misuse of his previous employer's computer system; the insider said he had never been arrested and had voluntarily left his previous employer.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

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

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has defined policy or procedures for TBP onboarding.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization communicates TBP roles and responsibilities.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization provides TBPs copies of all relevant policies and procedures.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization obtains TBP's acknowledgement of receipt and understanding of policy.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization communicates its missions and culture to TBPs.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization or contracting agency trains TBPs about policy and procedures, particularly behavioral requirements.

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 # TBP1.4: TBP Reporting of Policy Violations

Clarification/Intent

Trusted business partners should understand that they are an important source of information and concerns regarding the safety and security of the workplace. The organization or contracting agency should provide TBPs with specific mechanisms and instructions for reporting violations of workplace behavioral rules or concerns about their own or other's behavior. There should also be a policy or procedure in place documenting the responsibility and requirements for reporting, and corresponding training for TBPs to better understand their obligations. Reporting can be anonymous or confidential. The TBP should also receive information on how their reports are handled.

Assessment Team Guidance

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

Areas that should be specified for reporting should include but not be limited to

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

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

MERIT Example

The insider, a contractor and consultant, was employed to upgrade the network at the victim organization, a government agency. On 4 occasions over a 9 month period, the insider breached the organization's computer systems and obtained the encrypted passwords of over 38,000 employee accounts. The insider used two pieces of password-cracker freeware to decrypt the passwords. The insider had unauthorized access to sensitive, and potentially classified, information. The organization temporarily shut down its network and spent millions of dollars plus thousands of hours to ensure no sensitive data had been misused. The insider was disgruntled by the organization's bureaucratic processes that hindered his ability to work. The insider used stolen names and passwords to speed up his access to the computer system because he was tired of having to seek written permission even for such mundane tasks as adding printers, workstations, user accounts, and moving machines from one operating system to another. The insider also claimed that two of the organization's officials were aware of what he was doing and that one actually provided his personal password so that the insider could do his job more efficiently. The insider had previously exceeded his authorized access during his employment with another government agency. The insider was arrested, convicted, and sentenced to 6 months of home detention.

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 that describes the TBP's obligation to report policy violations.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The policy outlines specific reporting options and procedures.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization or contracting agency trains TBPs on the reporting procedures and requirements.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization follows-up on policy violation reports from TBPs.

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 # TBP1.5: Updated Background Screenings

The organization requires updated background screenings for trusted business partners.

Clarification/Intent

Concerning behaviors and stressors are not always present at the beginning of employment. Updating background screenings allows the organization or contracting agency to remain aware of potential risks.

Assessment Team Guidance

Periodic reevaluation may include screenings for

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

MERIT Example

The insider, a contractor, was employed as a programmer by the victim organization, a telecommunications firm. The insider was deeply interested in math, and was involved in a competitive and collaborative effort to find the next prime number. To help in this endeavor the insider placed specialized code on the organization's machines, taking advantage of the computing power of the victim organization. The code ran for 8 months on approximately 2,500 of the organization's computer systems. It wasn't detected until an error in the code caused it to run during peak daytime hours (previously it had only run during off-hours when system traffic was low) which significantly impacted normal business operations. The organization's offices began to experience wide-scale lag in the computer systems making them unable to serve customer requests. The situation was so severe that the organization considered simply deactivating the entire site and routing operations through other offices to mitigate the incident related loss of the event. The organization discovered that the unidentified code running on its systems was sending information to an external ISP owned by the insider. The insider never intentionally planned to disrupt the computer systems of the victim organization, but had knowingly taken advantage of computing resources he was not supposed to have access to. It was later determined that the insider previously worked, and been fired by, the victim organization. At that time, the insider was working with a different contractor, using a different name, and working in a different location within the victim organization. It is unknown if the victim organization did any sort of background screening on the insider. The FBI raided the insider's home, but he was never arrested or charged.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

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

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization requires updates of background screenings for TBPs.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has communicated their standards for detecting and responding to changes in TBP behavior so that the contracting agency can take appropriate action.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization designates a permanent staff member to ensure that TBP background screening updates are being performed.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization is able to access the information in updated TBP background screenings.

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 # TBP1.6: IP Ownership Rights

The organization has policy that defines its ownership rights to intellectual property (IP) created by trusted business partners.

Clarification/Intent

Organizations should establish policy that describes what ownership rights, if any, a TBP has related to organizational IP created by the TBP. If the organizational policy states that TBPs have no ownership interest in any of the organization's IP, including IP created by TBPs for the organization, appropriate documentation and training for the TBP should be available describing this situation. The policy should also include actions to be taken if a TBP uses the organizational IP in an inappropriate manner. It should describe consequences for TBPs who use the organization's intellectual property inappropriately such as disciplinary actions, termination, and legal actions. TBP IP policy should give the organization the authority or jurisdiction to detect the TBP's attempts to steal, sell, market, or personally use business resources. Controlled information management (CIM) is the process by which authorized access is determined, provisioned, and revoked to/from an information asset determined to have restricted access, which includes IP.

The organization should also have procedures requiring appropriate marking of IP, such as ownership markings and limited distribution instructions.

Assessment Team Guidance

To effectively manage the ownership of IP, the organization should have relevant policy and communicate it to TBPs.

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

MERIT Example

The insider, a foreign national, and his co-conspirator, were both contractors. The insiders were formerly employed as software developers for the victim organization, which provided news filtering and distribution services to websites. In response to their termination, legal counsel for the insiders faxed a letter to the organization. The letter insisted that the insiders owned software they created during their employment and demanded that the organization stop using the software and return all copies to the insiders. On the evening prior to a holiday, the insiders used the insider's home computer, and their own credentials, to remotely access the victim organization's network to download software and proprietary files, including secret business plans. The insiders were arrested after the organization discovered the unauthorized access, and connected the insiders to the theft through user ID's, passwords, and activity logs. The insider was found not guilty.

Organization Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

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

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The organization has a defined policy on ownership of IP created by the TBP for the organization.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization requires TBPs to sign (if applicable) nondisclosure agreements.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization requires TBPs to sign (if applicable) IP agreements.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization requires TBPs to sign (if applicable) noncompete agreements.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization requires TBPs to sign (if applicable) nonsolicitation agreements.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization informs TBPs of controlled-information management (CIM) policy.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has an IP dispute resolution process available to TBPs.

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 # TBP1.7: Insider Threat TBP Terms

The organization negotiates contract terms and conditions that allow it to prevent, detect, and respond to insider threats from trusted business partners as effectively as it would insider threats from permanent staff.

Clarification/Intent

Contracts should have terms and conditions that allow the organization to monitor TBP behavior as necessary and require mandatory flow-down clauses to protect the organization's intellectual and physical assets.

Assessment Team Guidance

To protect itself from fraud and insider threats effectively, the organization should set contract terms and conditions that allow for adequate monitoring, notifications, and control.

MERIT Example

The insider, a foreign national and subcontractor, was formerly employed by the victim organization, which developed and marketed a digital interactive video service. The day after his termination, the insider remotely accessed the organization's network and disabled 14 routers that controlled the organization's wide area network across the United States. The organization's network failed and required extensive repairs. The organization spent 18 days fully restoring the network. The insider was motivated by revenge. The insider claimed that the organization failed to honor a verbal agreement between the insider and management and that the organization owed him money. The insider was arrested, released on bail, fled to a foreign country, and failed to appear in court. The insider assumed a false identity and returned to the United States and was arrested again on an outstanding warrant. At the time of his arrest, the insider possessed numerous false identification materials. The insider was convicted and sentenced to 46 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 considered, and uses as appropriate, contract terms and conditions including but not limited to those that

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ allow thorough information security assessment of TBPs and their TBPs as part of routine due diligence

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ require proof of fraud insurance

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ allow auditing of books and records of all TBPs

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ require TBPs to be subject to the same policies and execute the same agreements as the organization's permanent staff, such as code of conduct, nondisclosure, noncompetition, IP, and other agreements

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ require TBPs to consent to logging, monitoring, and auditing

Doc Rev _____

Dir Obs _____

Intvw _____

☐ allow TBP background screenings or proof of background screenings

Doc Rev _____

Dir Obs _____

Intvw _____

☐ require contracting agency to notify the organization before terminating a TBP or their TBPs

Doc Rev _____

Dir Obs _____

Intvw _____

☐ require notification when a breach occurs

Doc Rev _____

Dir Obs _____

Intvw _____

☐ require return of intellectual and physical assets upon contract termination

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Experts from the following departments have reviewed the contract terms and conditions for adequate requirements and procedures:

Doc Rev _____

Dir Obs _____

Intvw _____

☐ information technology

Doc Rev _____

Dir Obs _____

Intvw _____

☐ security

Doc Rev _____

Dir Obs _____

Intvw _____

☐ human resources

Doc Rev _____

Dir Obs _____

Intvw _____

☐ facilities

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has a process that formalizes execution of all contracts and modifications.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has all executed contracts and modifications on file and accessible to those with a need to know.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has preapproved templates with contract terms and conditions.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has a process for approving negotiated terms and conditions that deviate from contract templates.

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 # TBP1.8: Monitoring of Trusted Business Partners

The organization monitors and manages trusted business partners sufficiently to prevent, detect, and respond to insider threats from contractors as effectively as it would insider threats from permanent staff.

Clarification/Intent

The organization has policy and procedures for monitoring TBP behavior and ensuring that TBPs have no right or access to organizational assets upon termination.

Assessment Team Guidance

To effectively protect itself from fraud and insider threats once appropriate contract terms and conditions are established, the organization should monitor and manage TBPs sufficiently to prevent, detect, and respond to TBP threats as effectively as it would internal threats.

Separate policies covering TBPs are not required if the organization extends its policies covering permanent staff to TBPs.

MERIT Example

The insider, a contractor, was formerly employed as an engineer by an organization, which specialized in developing and managing Supervisory Control and Data Acquisition Systems (SCADA) for utility companies. The insider's employer was a trusted business partner (TBP) of the victim organization, a municipality. The insider's employer organization installed a SCADA system that allowed the victim organization to use radio signals to control sewage equipment. The insider, who had a very strained relationship with his employer, resigned and sought employment with the victim organization. After his termination, the insider retained devices that his employer organization used to control the victim organization's SCADA systems, including a 2-way radio and a PDS compact 500 computer control device. A month later, the insider was rejected by the victim organization. After another month had passed, the insider decided to seek revenge against the victim organization for not hiring him and reloaded the software that controlled the victim organization's SCADA system onto his laptop. The insider attacked the victim organization's SCADA system for over 3 months. On at least 46 occasions, the insider issued radio commands to the victim organization's SCADA systems. The insider used the 2-way radio to issue commands, ran the SCADA control on his computer at least 31 times, set the computer control device to spoof a pumping station, disabled alarms at 4 pumping stations, and ultimately released 800,000 liters of raw sewage into water and parks located in a popular tourist area. The insider's actions polluted the water, killed marine life, and repelled local citizens and tourists with its repugnant smell. The insider was pulled over by the police, who conducted a vehicle search and discovered the computer equipment used to control the victim organization's systems. The insider was subsequently arrested, sentenced to concurrent sentences of 12 months imprisonment for the environmental harm, and 2 years for related computer hacking and theft charges.

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 and procedures for terminating all TBP access to the organization's online and physical assets before or on the day of their termination or the contract's termination.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization routinely identifies and monitors all TBPs whose potential misuse of sensitive and confidential information could harm the organization.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization has defined processes, policy, practices, and/or multidisciplinary groups assigned to plan and assess the range of risks associated with transferring TBPs out of the organization, either at the agreed-upon end of the contract period or at contractor termination.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization has conflict of interest and commitment policy and procedures for TBPs.

Doc Rev _____

Dir Obs _____

Intvw _____

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

Doc Rev

Dir Obs

Intvw

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

Doc Rev

Dir Obs

Intvw

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

Doc Rev

Dir Obs

Intvw

☐ The organization promptly and thoroughly investigates IP ownership disputes.

Doc Rev

Dir Obs

Intvw

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

Justification

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

Notes (from documentation, observations, and interviews)

Capability Sequence # TBP1.9: Trusted Business Partner Scope Review

The organization periodically reviews contracts and their assigned scope of work to ensure it has not given trusted business partners additional duties beyond the original scope.

Clarification/Intent

The organization should not assign TBPs additional duties outside the scope of the contract.

Assessment Team Guidance

Exceeding the original scope of work in a contract could create opportunities for insider threat as TBP employees gain additional access or privileges beyond what is being monitored or managed. The organization should have policies to prevent this from occurring and should review contracts periodically against the actual scope of assigned work to ensure that it has not occurred.

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 policy that TBPs will not be assigned work beyond the original scope of the contract.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The organization communicates its policy on scope of work with TBPs.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The organization periodically reviews contracts and their assigned scope of work to ensure it has not given TBPs additional duties beyond the original scope of work.

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)