# Discussion Draft of the Preliminary Cybersecurity Framework Illustrative Examples

The Cybersecurity Framework emphasizes processes/capabilities and supports a broad range of technical solutions. While organizations and sectors may develop overall Profiles, these Threat Mitigation Profile examples that illustrate how organizations may apply the Framework to mitigate specific threats. These scenarios include cybersecurity intrusion, malware, and insider threat.

## Threat Mitigation Examples

A threat is characterized as any circumstance or event with the potential to have an adverse impact on an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service (DoS). Threats continue to evolve in sophistication, moving from exploitation (collection and interception of information) to disruption (denial of service attacks) to destruction, with physical damage to a main operating component, whether it is destruction of information or incorrect commands causing damage to computer-controlled systems. The following examples describe Profiles crafted to address specific known threats.

## Example 1: Mitigating Cybersecurity Intrusions

This example Profile is intended to describe key activities that address the cybersecurity risk associated with a Cybersecurity Intrusion event. The Profile was crafted based on the activities performed by adversaries during the life cycle of a cybersecurity intrusion. The cybersecurity intrusion life cycle consists of three general phases: Gain Access, Maintain Access, and Act.

> **Gain Access:** The goal of this phase is to achieve limited access to a device on a target network. Adversaries often gain initial access to networks by exploiting a single vulnerability in a product or by prompting user action. Techniques used include: spear phishing, malicious e-mail content, Web browser attacks, exploitation of well-known software flaws, and distribution of malware on removable media.
>
> **Maintain Access:** During this phase the adversary takes steps to ensure continued access to the targeted network. This is often accomplished by the installation of tools and/or malware to allow the adversary to maintain a presence on the network. Malware components establish command and control capabilities for the adversary and enable additional attacks to be performed, such as capturing keystrokes and credentials. Example actions taken during this phase include the installation of rootkits/backdoor programs and execution of BIOS exploits.
>
> **Act:** In the final phase the adversary focuses on gaining access privileges that enable them to move, compromise, disrupt, exploit, or destroy data. Using the previously established command and control capabilities and compromised accounts, adversaries take steps to access and control additional data and resources. This includes establishing communications channels to the adversary's servers that facilitate remote access. Privilege escalation and lateral movement enable an enterprise-wide compromise by an adversary. The adversary is able to use the access gained to internal networks, where security protections may not be as robust, to gain access to critical resources.

43 # Threat Mitigation Profile: Cybersecurity Intrusion
44

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| Identify | Risk Assessment | • Identify threats to organizational assets (both internal and external)<br>• Identify providers of threat information | **NIST SP 800-53** Rev. 4 PM-16<br>**ISO/IEC 27001** A.13.1.2 | Allows the organization to identify current known IP addresses for adversary servers and block inbound and outbound connections to this source. |
| Protect | Awareness and Training | • Provide awareness and training that ensures that general users understand roles & responsibilities and act accordingly<br>• Provide awareness and training that ensures that privileged users (e.g. system, network, industrial control system, database administrators) understand roles & responsibilities and act accordingly<br>• Provide awareness and training that ensures that third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities and act accordingly<br>• Provide awareness and training that ensures that senior executives understand roles & responsibilities and act accordingly<br>• Provide awareness and training that ensures that physical and information security personnel understand roles & responsibilities and act accordingly | **CCS CSC**9 | Training that is shaped by the existing threat landscape provides employees with an awareness of active threats and the basic cybersecurity knowledge needed to identify suspicious applications and not to open unknown email attachments. The benefit of awareness and training can be extremely high and has a relatively low cost. |
| Protect | Information Protection Processes and Procedures | • Develop, document, and maintain under configuration control a current baseline configuration of information technology / operations technology systems | **NIST SP 800-53** Rev. 4 CM-2 | An effective patch management process provides another potential defense against malware. Many exploits use well-known software flaws for which patches are available. A mature patch management process makes it harder |

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| | | | | for an adversary to craft an initial exploit. It is important that critical infrastructure install updated patches; test patches for potential operational impacts; and ensure that the patches do not introduce new vulnerabilities. |
| Protect | Protective Technology | • Implement and maintain technology that enforces policies to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on organizational systems (i.e., Whitelisting of applications and network traffic)<br>• Determine, document, and implement physical and logical system audit and log records in accordance with organizational auditing policy | **CCS CSC** 6<br>**COBIT** APO11.04 | Application whitelisting ensures that only approved applications may run. This mitigation approach can also prevent the installation of known malicious code.<br>Auditing and logging operates in direct support of other Detect, Respond, and Recover Framework Functions. |
| Detect | Security Continuous Monitoring | • Perform network monitoring for cybersecurity events flagged by the detection system or process<br>• Perform physical monitoring for cybersecurity events flagged by the detection system or process<br>• Perform personnel monitoring for cybersecurity events flagged by the detection system or process<br>• Employ malicious code detection mechanisms on network devices and systems to detect and eradicate malicious code<br>• Detect the use of mobile code and implement corrective actions when unacceptable mobile code is detected<br>• Perform personnel and system monitoring activities over external service providers | **NIST SP 800-53** Rev. 4 CM-1, CA-7, AC-2, SC-5, SI-4<br>**NIST SP 800-53** Rev. 4 CM-1, CA-7, PE-3, PE-6, PE-20<br>**NIST SP 800-53** Rev. 4 CM-1, CA-7<br>**ISO/IEC 27001** A.10.4.2<br>**ISO/IEC 27001** 10.2.2<br>**NIST SP 800-53** Rev. 4 CM-1, CA-7, PE-3, PE-6, PE-20 | Monitoring can detect and quarantine email that contains malware prior to delivery. Malware can be identified using signatures that uniquely identify specific malware components. Malware signatures must be frequently updated to ensure that emerging malware threats can be identified and eradicated before users within the organization can launch them.<br>Monitoring also allows the organization to detect unusual or anomalous system behaviors that may indicate that a system has been infected with malware.<br>Automated malware detection solutions can be configured to block connections to servers that are known to host malware or that malware |

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| | | • Perform periodic checks for unauthorized personnel, network connections, devices, software<br>• Perform periodic assessments to identify vulnerabilities that could be exploited by adversaries (aka Penetration testing) | **NIST SP 800-53** Rev. 4 CM-1, CA-7 | software is known to communicate with. |
| Respond | Planning | • Execute the organization's incident response plan | **CCS CSC** 18<br>**NIST SP 800-53** Rev. 4 IR-1, IR-2 | After an attack is recognized, the security team should use the organization's response plan to determine the appropriate, coordinated response to the type of attack. |
| Respond | Analysis | • Investigate anomalies, including cybersecurity events (from network, physical, or personnel monitoring) flagged by the detection system or process<br>• Conduct an impact assessment (damage/scope)<br>• Perform forensics<br>• Classify the incident | **ISO/IEC 27001** A.06.02.01<br>**ISO/IEC 27001** A.06.02.01<br>**ISO/IEC 27001** A.13.02.02 A.13.02.03<br>**ISO/IEC 27001** A.13.0 A.13.02 A.03.06 A.07.4.2.1 | It is important to understand the scope of the incident, the extent of damage, the level of sophistication demonstrated by the adversary, and the stage the attack is in. This knowledge helps to determine if an attack is localized on an organization's machine or if the adversary has a persistent presence on the network and the scope is enterprise-wide. Organization should compare attack data against current and predicted attack models to gain meaningful insight into the attack. |
| Respond | Improvements | • Incorporate lessons learned into plans<br>• Update response strategies | **ISO/IEC 27001** A.13.02.02<br>**NIST SP 800-53** Rev. 4 PM-9 | Document the lessons learned from the intrusion and use them to enhance organizational cybersecurity processes. |

45
46

## Example 2: Malware

It has been shown that critical infrastructure can be susceptible to low-level threats that cause ancillary disruption. Recent attacks suggest that malware infections pose a significant threat to organizational assets. Key features of malware attacks include the exploitation of outdated patches, ingress through back channels, denial of service based on exploited systems and failing network hardware, escalation of presence, and the prevalence of a 'fortress mentality.'

## Threat Mitigation Profile: Malware

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| Identify | Asset Management | • Inventory and track physical devices and systems within the organization<br>• Inventory software platforms and applications within the organization<br>• Identify organizational network components and connections<br>• Identify external information systems including processing, storage, and service location<br>• Identify classification/ criticality/business value of hardware, devices, and software | **ISO/IEC 27001** A.7.1.1, A.7.1.2<br>**COBIT** BAI03.04, BAI09.01, BAI09, BAI09.05<br>**ISO/IEC 27001** A.7.1.1<br>**NIST SP 500-291** 3, 4 | Understanding of the network architecture must update with changes. Potential backdoors must be identified and mitigated. |
| Protect | Access Control | • Perform identity and credential management (including account management, separation of duties, etc.) for devices and users<br>• Enforce physical access control for buildings, stations, substations, data centers, and other locations that house logical and virtual information technology and operations technology<br>• Protect remote access to organizational networks to include telework guidance, mobile devices access restrictions, and cloud computing policies/procedures | **NIST SP 800-53** Rev. 4 AC Family<br>**ISO/IEC 27001** A.9.1, A.9.2, A.11.4, A.11.6,<br>**COBIT** APO13.01, DSS01.04, DSS05.03 | Access control should be risk informed, should be updated, and should anticipate threats. |

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| | | • Enforce access restrictions including implementation of Attribute-/Role-based access control, permission revocation, network access control technology<br>• Protect network integrity by segregating networks/implementing enclaves | **CCS CSC** 12, 15<br>**ISO/IEC 27001** A.10.1.4, A.11.4.5 | |
| Protect | Awareness and Training | • Provide awareness and training that ensures that general users understand roles & responsibilities and act accordingly<br>• Provide awareness and training that ensures that privileged users (e.g. system, network, industrial control system, database administrators) understand roles & responsibilities and act accordingly<br>• Provide awareness and training that ensures that third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities and act accordingly<br>• Provide awareness and training that ensures that senior executives understand roles & responsibilities and act accordingly<br>• Provide awareness and training that ensures that physical and information security personnel understand roles & responsibilities and act accordingly | **COBIT** APO07.03, BAI05.07<br>**ISO/IEC 27001** A.8.2.2<br>**NIST SP 800-53** Rev. 4 AT-3<br>**CCS CSC** 9<br>**ISO/IEC 27001** A.8.2.2 | Partners must be educated as to the impact they or their systems may have on critical infrastructure. Employees must have ongoing understanding of malware that reflects the current threat landscape. |
| Protect | Information Protection Processes and Procedures | • Develop, document, and maintain under configuration control a current baseline configuration of information technology / operations technology systems | **CCS CSC** 3, 10 | Aggressive patch management is particularly important in the critical infrastructure setting. Patches should be thoroughly tested prior to deployment to ensure that the patch does not negatively |

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| | | | | affect critical systems. Rapid testing and installation of new patches is critical to hardening the network from malicious code should it penetrate existing barriers. |
| Protect | Protective Technology | • Implement and maintain technology that enforces policies to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on organizational systems (i.e., Whitelisting of applications and network traffic)<br>• Restrict the use of removable media (including writable portable storage devices), personally/externally owned devices, and network accessible media locations<br>• Determine, document, and implement physical and logical system audit and log records in accordance with organizational auditing policy<br>• Protect wireless network security including monitoring for unauthorized devices/networks, processes for authorization and authentication for wireless networks, adequate encryption to protect information transmitted wirelessly<br>• Protect operational technology (to include ICS, SCADA, DCS) | **CCS CSC** 6<br>**NIST SP 800-53** Rev. 4 AC-19<br>**CCS CSC** 14<br>**ISO/IEC 27001** 10.10.2<br>**COBIT** APO13.01, BAI03.02 | Protection of operational technology is critically important. These devices should be separated from all non-necessary devices. Architecture and security measures must be updated with changes to the network and the cybersecurity landscape. |
| Detect | Anomalies and Events | • Identify and determine normal organizational behaviors and expected data flow of personnel, operations technology, and information systems | **NIST SP 800-53** Rev. 4 SI-4 AT-3 CM-2 | The organization should have solid understanding of the events that occur on their operational networks. |

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| | | • Characterize detected events (including through the use of traffic analysis) to understand attack targets and how a detected event is taking place | **NIST SP 800-53** Rev. 4 SI-4 | |
| | | • Perform data correlation among to improve detection and awareness by bringing together information from different information sources or sensors. | **NIST SP 800-53** Rev. 4 SI-4 | |
| | | • Assess the impact of detected cybersecurity events to inform response & recovery activity | **NIST SP 800-53** Rev. 4 SI-4 | |
| Detect | Security Continuous Monitoring | • Perform network monitoring for cybersecurity events flagged by the detection system or process | **ISO/IEC 27001** A.10.10.2, A.10.10.4 A.10.10.5 | Monitoring should be adjusted to detect not only presently understood threats but also predicted threats. Organizations should test systems for vulnerabilities that may expose them to current or predicted threats. |
| | | • Perform physical monitoring for cybersecurity events flagged by the detection system or process | **NIST SP 800-53** Rev. 4 CM-1, CA-7, PE-3, PE-6, PE-20 | |
| | | • Perform personnel monitoring for cybersecurity events flagged by the detection system or process | **NIST SP 800-53** Rev. 4 CM-1, CA-7 | |
| | | • Employ malicious code detection mechanisms on network devices and systems to detect and eradicate malicious code | **COBIT** DSS05.01 | |
| | | • Detect the use of mobile code and implement corrective actions when unacceptable mobile code is detected | **ISO/IEC 27001** A.10.4.2 | |
| | | • Perform personnel and system monitoring activities over external service providers | **ISO/IEC 27001** 10.2.2 | |
| | | • Perform periodic checks for unauthorized personnel, network connections, devices, software | **NIST SP 800-53** Rev. 4 CM-1, CA-7, PE-3, PE-6, PE-20 | |

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| | | • Perform periodic assessments to identify vulnerabilities that could be exploited by adversaries (aka Penetration testing) | **NIST SP 800-53** Rev. 4 CM-1, CA-7 | |
| Respond | Mitigation | • Contain the incident<br>• Eradicate the incident (includes strengthening controls to prevent incident recurrence) | **ISO/IEC 27001** A.03.06 A.13.02.03 | It is crucial that incidents be contained and eradicated. Organizations should be prepared for both existing threats and anticipated threats. |
| Recover | Recovery Planning | • Execute recover plan | **ISO/IEC 27001** A.14.1.3 A.14.1.4 A.14.1.5 | Organizations should have viable recovery options for both currently understood threats and predicted threats. |

## Example 3: Mitigating Insider Threats

Insider threats present a significant danger to organizations. In many cases personnel may act as a conduit for a cybersecurity attack. This may occur through the inadvertent installation of malware, installation of unauthorized software, the loss of organizational assets, accidental data exposure or loss, and other unintentional actions. Occasionally, organizational insiders may actively seek to subvert an organization through corporate espionage or corporate sabotage. In these cases an insider may pose a significant threat, particularly within critical infrastructure.

### Threat Mitigation Profile: Insider Threat

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| Identify | Asset Management | • Identify business value of workforce functions by role | **NIST SP 800-53** Rev. 4 PM-11 | Organizations should have understanding of current workforce, their positions, and the assets to which they have access. |
| Identify | Governance | • Identify organizational information security policy<br>• Identify information security roles & responsibility, coordination<br>• Identify legal/regulatory requirements | **COBIT** APO01.03, EA01.01<br>**ISO/IEC 27001** A.15.1.1 | Organizations should have understanding of policies, procedures, and requirements employees must adhere to. Organizations should understand the lines of communication employees currently use and may use in the future, to include social media, email, and mobile networks. |
| Protect | Access Control | • Perform identity and credential management (including account management, separation of duties, etc.) for devices and users<br>• Enforce physical access control for buildings, stations, substations, data centers, and other locations that house logical and virtual information technology and operations technology<br>• Protect remote access to organizational networks to include telework guidance, mobile devices access restrictions, and cloud computing policies/procedures | **NIST SP 800-53** Rev. 4 AC Family<br>**COBIT** DSS01.04, DSS05.05<br>**ISO/IEC 27001** A.11.4, A.11.7 | Organizations should monitor and maintain constant control of credentials, access to facilities and assets, as well as remote access to assets. Furthermore, organizations should continue to search for and mitigate the damage caused by unknown possible points of entry. |

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| | | • Enforce access restrictions including implementation of Attribute-/Role-based access control, permission revocation, network access control technology | **ISO/IEC 27001** A.11.1.1 | |
| | | • Protect network integrity by segregating networks/implementing enclaves | **ISO/IEC 27001** A.10.1.4, A.11.4.5 | |
| Protect | Awareness and Training | • Provide awareness and training that ensures that general users understand roles & responsibilities and act accordingly | **COBIT** APO07.03, BAI05.07 | Organizations should have ongoing security training that mirrors current and potential threats. Employees should be trained to identify misuse of assets. |
| | | • Provide awareness and training that ensures that privileged users (e.g. system, network, industrial control system, database administrators) understand roles & responsibilities and act accordingly | **ISO/IEC 27001** A.8.2.2 | |
| | | • Provide awareness and training that ensures that third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities and act accordingly | **NIST SP 800-53** Rev. 4 AT-3 | |
| | | • Provide awareness and training that ensures that senior executives understand roles & responsibilities and act accordingly | **CCS CSC** 9 | |
| | | • Provide awareness and training that ensures that physical and information security personnel understand roles & responsibilities and act accordingly | **ISO/IEC 27001** A.8.2.2 | |
| Protect | Data Security | • Protect data (including physical records) during storage (aka "data at rest") to achieve confidentiality, integrity, and availability goals | **ISO/IEC 27001** A.15.1.3, A.15.1.4 | Organizations should seek to protect organizational data at rest from both outside threats and inside threats in a manner that reflects current understanding of the value of the information. |
| | | • Protect data (including physical records) during transportation/ transmission (aka "data in | **NIST SP 800-53** Rev. 4 SC-8 | |

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| | | motion") to achieve confidentiality, integrity, and availability goals | | |
| | | • Protect organizational property and information through the formal management of asset removal, transfers, and disposition | **ISO/IEC 27001** A.9.2.7 | |
| | | • Protect availability of organizational facilities and systems by ensuring adequate capacity availability (physical space, logical storage/memory capacity) | **ISO/IEC 27001** A.10.3.1 | |
| | | • Protect confidentiality and integrity of organizational information and records by preventing intentional or unintentional release of information to an unauthorized and/or untrusted environment (information/data leakage) | **CCS CSC** 17 | |
| | | • Protect intellectual property in accordance with organizational requirements | **ISO/IEC 27001** A.15.1.2 | |
| | | • Reduce potential for abuse of authorized privileges by eliminating unnecessary assets, separation of duties procedures, and least privilege requirements | **NIST SP 800-53** Rev. 4 AC-5, AC-6 | |
| | | • Establish separate development, testing, and operational environments to protect systems from unplanned/unexpected events related to development and testing activities | **COBIT** BAI07.04 | |
| | | • Protect the privacy of individuals and personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by organizational programs and systems | **ISO/IEC 27001** A.15.1.3 | |

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| Protect | Information Protection Processes and Procedures | • Develop, document, and maintain under configuration control a current baseline configuration of information technology / operations technology systems | **NIST SP 800-53** Rev. 4 CM-2 | Organizations should have well-established processes that address the potential damage to operations and business that an insider threat may cause. Processes must also exist to protect data from insiders such as limiting attack surfaces and properly disposing of assets. Processes should also integrate with human resources to ensure that employees are properly screened and adhere to organizational security requirements. |
| | | • Develop, document, and maintain a System Development Life Cycle (including secure software development and system engineering and outsourced software development requirements) | **CCS CSC** 6 | |
| | | • Protect organizational information by conducting backups that ensure appropriate confidentiality, integrity, and availability of backup information, storing the backed-up information properly, and testing periodically to ensure recoverability of the information | **NIST SP 800-53** Rev. 4 CP-9 | |
| | | • Ensure appropriate environmental requirements are met for personnel and technology | **COBIT** DSS01.04, DSS05.05 | |
| | | • Destroy/dispose of assets (to include data destruction) in a manner that prevents disclosure of information to unauthorized entities | **ISO/IEC 27001** 9.2.6 | |
| | | • Achieve continued improvement (lessons learned, best practices, feedback, etc.) | **COBIT** APO11.06, DSS04.05 | |
| | | • Develop, document, and communicate response plans (Business Continuity Plan(s), Disaster Recovery Plan(s), Incident Handling Plan(s) that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance | **ISO/IEC 27001** A.14.1 | |

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| | | • Plan for what it takes to deliver critical infrastructure services for which the organization is responsible, including the identification of dependencies that might prevent delivery of those services | **ISO/IEC 27001** 9.2.2 | |
| | | • Integrate cybersecurity practices / procedures with human resources management (personnel screenings, departures, transfers, etc.) | **COBIT** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05, | |
| Protect | Protective Technology | • Implement and maintain technology that enforces policies to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on organizational systems (i.e., Whitelisting of applications and network traffic) | **CCS CSC** 6 | Organizations should ensure continuous security of applications, networks, and devices from insider threats. |
| | | • Restrict the use of removable media (including writable portable storage devices), personally/externally owned devices, and network accessible media locations | **NIST SP 800-53** Rev. 4 AC-19 | |
| | | • Determine, document, and implement physical and logical system audit and log records in accordance with organizational auditing policy | **CCS CSC** 14 | |
| | | • Protect wireless network security including monitoring for unauthorized devices/networks, processes for authorization and authentication for wireless networks, adequate encryption to protect information transmitted wirelessly | **ISO/IEC 27001** 10.10.2 | |
| | | • Protect operational technology (to include ICS, SCADA, DCS) | **COBIT** APO13.01, BAI03.02 | |

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| Detect | Anomalies and Events | Identify and determine normal organizational behaviors and expected data flow of personnel, operations technology, and information systems | **NIST SP 800-53** Rev. 4 SI-4 AT-3 CM-2 | Organizations should assess anomalies within the organizational network. |
| | | • Characterize detected events (including through the use of traffic analysis) to understand attack targets and how a detected event is taking place | **NIST SP 800-53** Rev. 4 SI-4 | |
| | | • Perform data correlation among to improve detection and awareness by bringing together information from different information sources or sensors. | **NIST SP 800-53** Rev. 4 SI-4 | |
| | | • Assess the impact of detected cybersecurity events to inform response & recovery activity | **NIST SP 800-53** Rev. 4 SI -4 | |
| Detect | Security Continuous Monitoring | • Perform network monitoring for cybersecurity events flagged by the detection system or process | **ISO/IEC 27001** A.10.10.2, A.10.10.4, A.10.10.5 | Organizations should have ongoing monitoring of assets to include employee interactions with assets. |
| | | • Perform physical monitoring for cybersecurity events flagged by the detection system or process | **NIST SP 800-53** Rev. 4 CM-1, CA-7, PE-3, PE-6, PE-20 | |
| | | • Perform personnel monitoring for cybersecurity events flagged by the detection system or process | **NIST SP 800-53** Rev. 4 CM-1, CA-7 | |
| | | • Employ malicious code detection mechanisms on network devices and systems to detect and eradicate malicious code | **COBIT** DSS05.01 | |
| | | • Detect the use of mobile code and implement corrective actions when unacceptable mobile code is detected | **ISO/IEC 27001** A.10.4.2 | |
| | | • Perform personnel and system monitoring activities over external service providers | **ISO/IEC 27001** 10.2.2 | |

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| | | • Perform periodic checks for unauthorized personnel, network connections, devices, software<br>• Perform periodic assessments to identify vulnerabilities that could be exploited by adversaries (aka Penetration testing) | **NIST SP 800-53** Rev. 4 CM-1, CA-7, PE-3, PE-6, PE-20<br>**NIST SP 800-53** Rev. 4 CM-1, CA-7 | |
| Detect | Detection Processes | • Ensure accountability by establishing organizational roles, responsibilities for event detection and response<br>• Perform policy compliance and enforcement for detect activities (internal, external constraints)<br>• Conduct exercises (e.g., tabletop exercises) to ensure that staff understand roles/responsibilities and to help provide quality assurance of planned processes<br>• Communicate and coordinate cybersecurity event information among appropriate parties | **ISO/IEC 27001** A.10.4.2<br>**ISO/IEC 27001** A.10.2.2<br>**NIST SP 800-53** Rev. 4 CM-1, CA-7, PE-3, PE-6, PE-20 | Organizations should establish roles, responsibilities, and privileges for employees. They should also ensure employees adhere to organizational policies. Organizations should conduct testing to ensure employees are adhering to policies and procedures, and that new methods of accessing and communicating organizational data are found and controlled. |
| Respond | Analyze | • Conduct an impact assessment (damage/scope)<br>• Perform forensics<br>• Classify the incident | **ISO/IEC 27001** A.06.02.01<br>**ISO/IEC 27001** A.13.02.02 A.13.02.03<br>**ISO/IEC 27001** A.13.0 A.13.02 A.03.06 A.07.4.2.1 | Organizations should conduct a thorough analysis to better understand the impact of insider threat incidents, to help prepare for recovery efforts, and to craft an effective containment and eradication strategy. |
| Respond | Mitigation | • Contain the incident<br>• Eradicate the incident (includes strengthening controls to prevent incident recurrence) | **ISO/IEC 27001** A.03.06 A.13.02.03 | Organizations should implement the steps necessary to manage the insider threat incident and engage law enforcement, as needed, to ensure that the threat is contained and eradicated. |
| Respond | Improvements | • Incorporate lessons learned into plans | **ISO/IEC 27001** A.13.02.02 | Organizations should document the lessons learned from insider |

| Function | Category | Subcategories | IR | Comment |
|---|---|---|---|---|
| | | • Update response strategies | **NIST SP 800-53** Rev. 4 PM-9 | threat incidents and incorporate them into response plans and strategy. |
| Recover | Recovery Planning | • Execute recover plan | **CCS CSC** 8 | Organizations should have recovery plans that account for current and predicted insider threats. |