INSIDER RISK MANAGEMENT PROGRAM EVALUATION (IRMPE)

Question Set and Guidance, Version 1.0

SEPTEMBER 2021

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

This material is based upon work funded and supported by the Department of Homeland Security 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 sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

DM21-0340

Contents

Notification

This document is provided “as is” for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this document, whether or not based upon warranty, contract, tort, or otherwise, whether or not injury was sustained from, or arose out of the results of, or reliance upon the document.

DHS does not endorse any commercial product or service, including the subject of the analysis referred to in this document. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.

The display of the DHS official seal or other DHS visual identities on this document shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.

Program Management

Program Management MIL1

The purpose of the Program Management domain is to determine whether the organization has the management structures, policies, relationships, and communications in place for an Insider Risk Program. Program Management includes

(1) understanding mission critical assets,

(2) defining the Insider Risk policy for the organization,

(3) characterizing the activities associated with insider threat detection, identification, assessment and management,

(4) ensuring communication of insider risk activities and events among responsible participants in the Insider Risk Program,

(5) providing governance and oversight of insider risk activities, and

(6) integrating insider risk management with organizational or enterprise risk management generally.

MIL	Question	Guidance
MIL1	**Goal 1– An insider risk policy exists.** The purpose of this goal is to ensure that the program has been established with the authority, scope, and responsibilities necessary to accomplish its mission.	
	1. Is there an authoritative document that establishes the existence of the Insider Risk Program?	**Question Intent** To determine if the Insider Risk Program was formally established in accordance with the organization's practices and procedures. Examples of authoritative documents include policies, directives, charters, or any other method by which the organization announces and establishes the existence of a program of record. **Typical Work Products** • policy • directive • charter • procedure **Criteria for "Yes" Response** The authoritative document formally established the Insider Risk Program in accordance with the organization's accepted practices. **Criteria for "Incomplete" Response** The authoritative document has been drafted, but has not been formally approved in accordance with the organization's accepted practices.

MIL	Question	Guidance
MIL1	2. Does the authoritative document define the program's: • authority • scope • roles • responsibilities for stakeholders	**Question Intent** To determine if the authoritative document that established the Insider Risk Program contains at least the minimum elements necessary in accordance with best practices. Examples of the minimum necessary elements include: • authority: has the program been empowered with the authority necessary to executive its responsibilities; • scope: describes what part(s) of the organization is covered by the program (entire organization, certain business lines only, all personnel [including contractors], only the organization's employees) and the types of threats that are in-scope for the program (theft of information, sabotage, fraud, workplace violence, etc.); • roles and responsibilities for stakeholders: organization-wide participation is essential for an effective Insider Risk Program. Each stakeholder's roles and responsibilities concerning participation in the Insider Risk Program should be clearly defined. Examples of stakeholders might include: the designated senior official for the program, the program manager, human capital, information technology, cybersecurity, physical security, legal, privacy, and heads of business lines. **Typical Work Products** Authoritative document(s) that formally established the Insider Risk Program. **Criteria for "Yes" Response** The authoritative document contains, at a minimum, the elements listed in the question. **Criteria for "Incomplete" Response** The authoritative document contains, at a minimum, the elements listed in the question, but is still in draft (it has not been formally approved in accordance with the organization's accepted practices).
	Goal 2– There is detect, identify, assess, and manage capability for insider incidents. The purpose of this goal is to ensure sufficient organizational capability exists to detect, identify, assess, and mange insider threats, in support of the Insider Risk program.	
	3. Are the types of insider risks to be addressed identified and documented?	**Question Intent** To determine if the types of insider risks considered by the Insider Risk Program are identified and documented. Being explicit about the threat types addressed is needed for consistent and coherent communication regarding the objective of the Insider Risk program. **Typical Work Products** Document identifying insider risks to be considered in insider risk management. **Criteria for "Yes" Response** A document exists that identifies and describes each insider risk addressed by the organization. **Criteria for "Incomplete" Response** Insider risks are identified but not documented.

MIL	Question	Guidance
MIL1	4. Has a capability been established that supports detection, investigation, and response to insider risk types identified?	**Question Intent** To determine if a capability exists to detect, investigate, and respond to insider incidents important to the organization. Insider incidents cannot always be prevented. Describing detection, investigation, and response capability enables review and refinement of that capability to help understand the extent to which it can be relied. **Typical Work Products** • insider event detection concept of operations, including policies for user monitoring • insider event detection technical architecture, including the audit of user actions insider incident response plan • incident escalation and investigation policy and procedures **Criteria for "Yes" Response** The capability to detect, investigate, and respond to insider incidents is documented in the context of prevention/deterrence capability. **Criteria for "Incomplete" Response** Significant gaps exist in the documentation of the detection, investigation, and/or response to insider incidents, especially in the context of prevention/deterrence capability.
	5. Has a capability been established that supports prevention/deterrence of insider risk types identified?	**Question Intent** To determine if sufficient capability exists to prevent/deter insider risks important to the organization. **Typical Work Products** • insider event prevention/deterrence concept of operations • insider event prevention/deterrence technical architecture **Criteria for "Yes" Response** The capability to prevent/deter insider risks is documented in the context of detect/investigate/respond capability. **Criteria for "Incomplete" Response** Significant gaps exist in the documentation of the prevention/deterrence of insider risks, especially in the context of detect/investigate/respond capability.

MIL	Question	Guidance
MIL1	6. Does the prevention/deterrence capability consider negative deterrence to force or constrain employees to act in the interests of the organization?	**Question Intent** To determine if policies and constraints are in place to help ensure employees act in the interests of the organization. Organizational constraints that forcibly restrict employee behavior are always going to be needed to reduce the risk associated with employees that become unruly, despite the positive aspects of the work environment. **Typical Work Products** • employee code of conduct policy • employee acceptable use policy for technical systems • contractor and trusted business partner agreement on operational constraints • prevention/deterrence security controls implemented as part of the technical architecture **Criteria for "Yes" Response** The policies and constraints on employee behavior to limit insider risk are documented. **Criteria for "Incomplete" Response** While the policies and constraints on employee behavior may be understood, they are not documented.
	7. Does the prevention/deterrence capability consider positive deterrence to attract employees to act in the interests of the organization, including the timely and generally supportive resolution of employee grievances?	**Question Intent** To determine if policies and management practices are in place to help ensure employees maintain goodwill toward and act in the interests of the organization. Employee goodwill is needed because organizations rely on that goodwill in order to accomplish its mission as well as reduce insider risk. A balance of positive and negative deterrence helps ensure effectiveness of insider risk defense and risk mitigation. **Typical Work Products** • confidential employee grievance communication process, supporting the timely and generally supportive resolution of employee grievance • surveys conducted to determine workforce sentiment toward the workplace management and climate, with timely response to employee concerns • manager training on the importance of supervisor supportiveness and organizational justice in reducing insider risk **Criteria for "Yes" Response** Positive deterrence policies and management practices are documented. **Criteria for "Incomplete" Response** While positive deterrence policies and management practices may be commonly used, they are not documented to support consistent application.

MIL	Question	Guidance
MIL1	8. Are employee assistance programs available to help employees with personal and professional stressors that could motivate insider risks or incidents?	**Question Intent** To determine if employees have available professional support for addressing stressors and reducing insider risk. Personal and professional stressors are a common cause of employees behaving in ways counter to organizational interests. **Typical Work Products** • communications about availability of employee assistance programs • documentation of how employee assistance programs work, and the confidentiality that they afford • manager training on how, when and why to refer employees to the employee assistance program. **Criteria for "Yes" Response** Employee Assistance programs exist and are communicated regularly within the organization. **Criteria for "Incomplete" Response** While employee assistance programs exist, there are significant gaps in the communication and documentation.
	Goal 3– Communication about insider risk events happens. The purpose of this goal is to ensure sufficient communication and collaboration to support prevention, detection, and response to insider threats.	
	1. Is there a policy or practice in place that defines what parts of the Insider Risk Program capability are publicly communicated to organizational staff?	**Question Intent** To determine if knowledge of the insider risk capabilities in place in the organization is shared consistently and in line with leadership authorization. **Typical Work Products** • insider risk communication plan • insider risk awareness training • information security awareness training • onboarding materials **Criteria for "Yes" Response** The organization's stance on what information can and cannot be shared with certain groups or individuals regarding insider risk capabilities is documented and executed. **Criteria for "Incomplete" Response** While the organization shares information related to insider risk capabilities in place, there is not documentation on what can and cannot be shared.

MIL	Question	Guidance
MIL1	2. Are there thresholds for when internal teams or groups need to be informed of an insider risk or incident?	**Question Intent** To determine if the organization has identified internal groups or individuals that can receive information related to insider risks and at what point they are notified. **Typical Work Products** • insider risk communication plan • incident response plan(s) • incident response playbook(s) **Criteria for "Yes" Response** The organization has documented policies, practices, or procedures for when and to whom information about insider risk should be communicated. **Criteria for "Incomplete" Response** While the organization engages in ad hoc sharing related to insider risk, there is not a documented process for when this information should be shared.
	3. Is there a defined process in place for internal information sharing about an insider risk or incident?	**Question Intent** To determine if the organization has established internal communication expectation procedures and channels for insider risk. **Typical Work Products** • insider risk communication plan • incident response plan(s) • incident response playbook(s) **Criteria for "Yes" Response** The organization has documented policies, practices, or procedures for how information about insider risk should be communicated. **Criteria for "Incomplete" Response** While the organization engages in ad hoc internal information sharing related to insider risk, there is not a documented process for how information sharing should take place.

MIL	Question	Guidance
MIL1	4. Are there thresholds for when external groups (e.g., law enforcement, legal counsel, or the public) need to be informed of an insider risk or incident?	**Question Intent** To determine if the organization has identified external stakeholders or partners that need to receive information related to insider risks and at what point they are notified. **Typical Work Products** • insider risk program charter • insider risk communication plan • incident response plan(s) • incident response playbook(s) **Criteria for "Yes" Response** The organization has documented policies, practices, or procedures for when and to whom information about insider risk should be communicated. **Criteria for "Incomplete" Response** While the organization engages in ad hoc sharing related to insider risk, there is not a documented process for when this information should be shared.
	5. Is there a defined process in place for external information sharing about an insider risk or incident when escalation thresholds require it?	**Question Intent** To determine if the organization has established external communication expectation procedures and channels for insider risk. **Typical Work Products** • insider risk program charter • incident response playbook(s) • cyber intelligence playbook(s) • situational awareness playbook(s) **Criteria for "Yes" Response** The organization has documented policies, practices, or procedures for how information about insider risk should be communicated. **Criteria for "Incomplete" Response** While the organization engages in ad hoc external information sharing related to insider risk, there is not a documented process for how information sharing should take place.

MIL	Question	Guidance
MIL1	**Goal 4– Insider risk is integrated with the enterprise risk program (ERP) and/or security risk management program.** **The purpose of this goal is to ensure that threats from trusted insiders are considered in the enterprise risk management program as factors that affect tracked risk, and that those threats are considered their own category of risk.** The purpose of this goal is to ensure that threats from trusted insiders are considered in the enterprise risk management program as factors that affect tracked risk, and that those threats are considered their own category of risk.	
	1. Are there procedures for conducting trusted insider risk assessments?	**Question Intent** To determine if the method for conducting trusted insider risk assessments is repeatable and consistent from assessment to assessment. **Typical Work Products** • standard operating procedure • assessment report template • assessment checklist **Criteria for "Yes" Response** The methodology for conducting trusted insider risk assessments is documented. **Criteria for "Incomplete" Response** While the method for conducting a trusted insider risk assessment is understood, it is not documented.
	2. Is a trusted risk assessment done on a yearly basis, and are the results integrated with the organization's Enterprise Risk Program (ERP) or security risk program?	**Question Intent** To determine the interval between risk assessments, and if the results are used for risk mitigation across the enterprise. **Typical Work Products** • risk assessment reports • insider risk references in the ERP **Criteria for "Yes" Response** There is some form of work product that substantiates that insider risk assessments are performed yearly and integrated with the ERP or security risk program. **Criteria for "Incomplete" Response** One or more insider risk assessments have been performed, but either not yearly, or have not been integrated with the ERP or security risk program.

MIL	Question	Guidance
MIL1	3. Have criteria been defined for trusted insider risks (probability, impact, priority, tolerance) that are consistent with ERP risk criteria	**Question Intent** To determine if there is defined criteria for measuring trusted insider risk that are consistent with the ERP risk criteria. The trusted insider risk criteria should be patterned after to the ERP risk criteria to provide for seamless integration. **Typical Work Products** • list of trusted insider risk criteria • list of ERP risk criteria **Criteria for "Yes" Response** Trusted insider risk criteria is documented and consistent with ERP risk criteria. **Criteria for "Incomplete" Response** The criteria for insider risk is generally consistent with ERP risk criteria, but is not documented and verified.
	4. Are trusted Insider risks treated as a category of risk in the ERP?	**Question Intent** To determine if insider risk is tracked as its own category within the ERP. Even if trusted insider actions are considered as risk factors within the ERP tracked risks, it should also be its own standalone category of risk tracked within the ERP. **Typical Work Products** • ERP policy, procedures, or guidance • list of categories tracked by the ERP **Criteria for "Yes" Response** There is documentation that shows that the ERP has a defined category dedicated to risks from trusted insiders. **Criteria for "Incomplete" Response** Although the ERP considers risks from trusted insiders across all ERP categories, there is no standalone category for trusted insider risk.

MIL	Question	Guidance
MIL1	5. Are trusted insider risks identified and integrated into the ERP on a continuous basis?	**Question Intent** To determine if newly identified trusted insider risks can be integrated into the ERP at any time (not just during a scheduled review). **Typical Work Products** • procedures for identifying new risks in ERP • policy for ERP risk identification **Criteria for "Yes" Response** A new trusted insider risk can be integrated into the ERP when it is identified. **Criteria for "Incomplete" Response** While new trusted insider risks can be integrated into the ERP, it is only during regularly scheduled reviews (i.e. only during quarterly, semi-annual, annual reviews).
	Goal 5– Mission-critical assets are known. The purpose of this goal is to ensure that the organization has identified and maintains a record of its indispensable hardware and software, and the users of those assets, within the organization and with third parties, and that the organization has appropriately identified the roles which are accountable for operating the Insider Risk program.	
	1. Is an inventory of critical assets maintained to support the Insider Risk Program?	**Question Intent** To determine whether a record of the organization's critical IT hardware and software assets exists. **Typical Work Products** Formal documentation that represents a record, based on observation of critical assets including IT hardware and software. **Criteria for "Yes" Response** Confirmation that an inventory exists and is maintained. **Criteria for "Incomplete" Response** An inventory that does not reflect an accurate record of all of organization's critical IT hardware and software.

MIL	Question	Guidance
MIL1	2. Are critical assets associated with key or primary users who may pose particular insider risk?	**Question Intent** To determine if critical IT hardware or software is associated with specific users such that, for users who may pose particular insider risk, activity may be observed and related to critical assets. **Typical Work Products** A register that identifies those users who may have access to or use critical hardware or software. **Criteria for "Yes" Response** Confirmation that a register exists and is maintained. **Criteria for "Incomplete" Response** A register that does not reflect an accurate record of associations between users and critical hardware and software assets.
	3. Have critical software platforms and applications within the organization been identified in support of detection, investigation, and response to insider incidents?	**Question Intent** To determine whether software IT assets (particular applications, for example) that may be critical to the organization have been identified to facilitate the organization's ability to identify and respond to insider risk. **Typical Work Products** Evidence of a process. This process may be indicated by a record of past use or by currently observed activity. **Criteria for "Yes" Response** All formal agreements with suppliers that support the critical service contain requirements for the suppliers to report incidents that may negatively affect the critical service. **Criteria for "Incomplete" Response** Partial evidence of some related activity (partial classification of assets or undetermined method for defining ‘critical assets,' for example).
	4. Have critical physical IT assets been identified in support of detection, investigation, and response for insider incidents?	**Question Intent** To determine if physical IT assets (PC's, for example) that may be critical to the organization have been identified to facilitate the organization's ability to identify and respond to insider risk. **Typical Work Products** Evidence of a process that works to identify critical physical IT assets, using elements obtained according to observation, user, department, function, hardware-stored or managed data, or other elements of identification. **Criteria for "Yes" Response** Existence of a process. This process may be indicated by a record of past use or by currently observed activity. **Criteria for "Incomplete" Response** Partial evidence of some related activity (partial classification of assets or undetermined method for defining 'critical assets,' for example).

MIL	Question	Guidance
MIL1	5. Are critical services associated with third parties that may represent insider risk?	**Question Intent** To determine if critical IT services performed by third parties have been identified to facilitate the organization's ability to identify and respond to insider risk. **Typical Work Products** Evidence of a process that works to identify critical third party services, using elements obtained according to observation, user, department, function, stored or managed data, or other elements of identification. **Criteria for "Yes" Response** Existence of a process. This process may be indicated by a record of third party associations with critical services or currently observed activity. **Criteria for "Incomplete" Response** Partial evidence of some activity related to identifying third parties that may be associated with critical services.
	6. Are cybersecurity roles and responsibilities established to define organizational accountability for addressing insider risk?	**Question Intent** To determine whether the organization's cyber security function is organized such that accountability for addressing insider risk is certain. **Typical Work Products** A current organization chart or other document that defines organizational accountability for addressing insider risk. **Criteria for "Yes" Response** Confirmation that the organization has established a formal function, role, or group of roles that is accountable for addressing insider risk. **Criteria for "Incomplete" Response** Evidence that only partial accountability has been assigned for insider risk, or that evidence itself is incomplete, inaccurate, or not current.

Program Management MIL2 – MIL5

MIL	Question	Guidance
MIL2 – Planned	1. Is there a plan for performing program management activities?	**Question Intent** To determine if a plan for performing program management activities exists. • The plan defines program management within the organization and prescribes how asset management activities will be performed. • The plan may be a stand-alone document, embedded in a more comprehensive document, or be distributed across multiple documents. **The plan, which may be in the form of an Insider Risk Program charter, typically includes:** • standards and requirements • assignments of responsibility • resources funding • identification of stakeholders • measurement and reporting requirements • training requirements oversight **Criteria for "Yes" Response** There is a documented plan for performing program management. **Criteria for "Incomplete" Response** A plan is in development and partially documented.

MIL	Question	Guidance
MIL2 – Planned	2. Is there a documented policy for program management?	**Question Intent** To determine if a policy for performing program management activities exists. • A policy is a written communication from the organization's senior management to employees. • It establishes the organizational expectations for planning and performing the functions of an Insider Risk program and communicates those expectations to the organization. **The policy should address:** • responsibility, authority, ownership, and the requirement to perform asset management activities • establishment of procedures, standards, and guidelines • establishing and maintaining an Insider Risk Program • measuring adherence to policy, exceptions granted, and policy violations • compliance with legal, regulatory, contractual, and government obligations **Criteria for "Yes" Response** The organization has a documented policy for performing Insider Risk Program management. **Criteria for "Incomplete" Response** A policy is in development and partially documented.

MIL	Question	Guidance
MIL2 – Planned	3. Have stakeholders for program management activities been identified and made aware of their roles?	**Question Intent** To determine if stakeholders for program management activities have been identified and made aware of their roles. **Stakeholders of the program management process have the following responsibilities:** • creating an Insider Risk Program mission statement and scope • overseeing the program management process • managing the risk resulting from out-of-scope use cases or controls (gaps in monitoring or response, lack of tooling or staff, etc.) **Examples of stakeholders include:** • critical service owners • asset management staff • owners and custodians of assets that underpin the service (to include facility security personnel) • critical service staff • external entities responsible for some part of asset management, monitoring, or response • information technology staff • human resources • internal auditors **Criteria for "Yes" Response** All stakeholders for the program management activities have been identified and made aware of their roles. **Criteria for "Incomplete" Response** • Some stakeholders for the program management activities have been identified and made aware of their roles; • Or, stakeholders are identified but have not been made aware of their roles.

MIL	Question	Guidance
MIL2 – Planned	4. Have program management standards and guidelines been identified and implemented?	**Question Intent** To determine if standards and guidelines for performing program management activities have been implemented. • Standards establish expectations for performance. • Guidelines are issued by an organization to ensure the performance of program management activities meets standards and is predictable, measurable, and repeatable. **Standards and guidelines typically address:** • establishing an insider risk appetite statement for the organization (e.g., use cases, scope, etc.) • critical assets protected by the Insider Risk Program • designating or allowing access to data sources used by the program • sensitivity categorization for information assets • documenting program management requirements • defining escalation and change management processes **Criteria for "Yes" Response** The organization has implemented documented standards and guidelines for performing program management activities. **Criteria for "Incomplete" Response** Some standards and guidelines have been implemented.
MIL3 – Managed	1. Is there oversight of the Insider Risk Program?	**Question Intent** To determine if oversight exists for the Insider Risk Program. The intent of the practice is to ensure that an appropriate level of oversight is performed for the management of the program. Oversight may include having a designated steering committee, working group, or other group of senior managers who provide oversight of the Insider Risk Program. These types of groups should have regular meetings, receive written or oral status updates about the program, and conduct auditing or spot checks. **Typical Work Products** • policy or charter establishing oversight committees, working groups, etc. • assignment of responsibility in job description • organizational communications and memoranda • inclusion of activity tasks in staff performance management goals and objectives, with measurement of progress against these goals **Criteria for "Yes" Response** Management oversight of all the day-to-day activities of the Insider Risk Program is being performed. **Criteria for "Incomplete" Response** Management oversight covers some aspects of the program, or there is insufficient oversight, or the activity is otherwise incomplete.

MIL	Question	Guidance
MIL3 – Managed	2. Have qualified staff been assigned to perform program management activities?	**Question Intent** To determine if qualified staff have been assigned to the Insider Risk Program. The intent of this question is to evaluate the qualifications of the staff, not the completeness of the plan. Qualified means that staff are appropriately skilled to perform Insider Risk Program activities, and have been assigned responsibility and given authority for performing those activities. **Examples of qualified staff include personnel responsible for:** • performing activities directly associated with or in support of Insider Risk Program activities. • monitoring the program to ensure alignment with expected performance and outcomes. • knowledge of tools, techniques, and methods that can be used to identify, analyze, mitigate, and monitor operational impacts resulting from or incurred by insider risk. • managing relationships with the program's stakeholders and related organizational functions. **Typical Work Products** • documented skills required for Insider Risk Program activities. • staffing and succession plans for Insider Risk Program activities. **Criteria for "Yes" Response** Sufficient, appropriately skilled staff have been assigned to perform planned Insider Risk Program roles. **Criteria for "Incomplete" Response** Some but not all staff have the skills necessary to perform their roles, or the practice is otherwise incomplete.
	3. Is there adequate funding to perform program management activities as planned?	**Question Intent** To determine if adequate funding is provided to operate and support the Insider Risk Program. The intent of the question is to evaluate the completeness of the funding, not the completeness of the plan. **Typical Work Products** Budgets to support the Insider Risk Program. **Criteria for "Yes" Response** Adequate funding has been provided to perform all planned Insider Risk Program activities. **Criteria for "Incomplete" Response** Activities have only been partially funded, or some related functions in the organization are not considered in the funding, or the activity is otherwise incomplete.

MIL	Question	Guidance
MIL3 – Managed	4. Are risks related to the performance of planned program management activities identified, analyzed, disposed of, monitored, and controlled?	**Question Intent** To determine if the organization identifies and manages risks to the performance of program activities. This practice refers to identifying risks to the performance of the insider risk program. Examples of risks to an Insider Risk Program include: • insufficient standards or activity definition, resulting in an incorrect understanding and prioritization of risk. • variability or inaccuracy in observable or quantifiable data. • inadequate linkage/communication between the Insider Risk Program and related organizational functions or stakeholders. **Typical Work Products** • documented Insider Risk Program review procedures and evidence of a risk assessment. • reports and communications about specific insider risks and about the functions and activities of the program. **Criteria for "Yes" Response** Risks to the performance of activities are identified, analyzed, disposed of, monitored, and controlled. **Criteria for “Incomplete” Response** Risks to the performance of activities are reviewed and identified but not controlled, or risks to the program's performance are sporadically reviewed, or funding is otherwise incomplete.

MIL	Question	Guidance
MIL4 – Measured	1. Are program management activities periodically reviewed and measured to ensure they are effective and producing intended results?	**Question Intent** To ensure the program management activities remain effective and produce intended results by conducting periodic review and measurement. Periodic review and tracking of measures over time allow detection of variance and correction of activities that may not be performing well. An example of a measurement is the percentage of program management activities that have undergone some form of assessment, risk assessment, or audit. Other examples of measurements include the count or percentage of program management activities in the following categories: • by number or type of unforeseen or disruptive program management functional changes • by performance problems reflected for example through variance of performed activities • by insider incidents that reflect gaps in program management level prevention and deterrence goals • by insider incidents that reflect gaps in program management level detection and response goals • by problems relating to responsiveness or timeliness of incident response activities **Typical Work Products** • documented list of measures for program management • list of identified weaknesses in program management function • exception reports – areas out of compliance with activity standards **Criteria for "Yes" Response** All program management activities are periodically (as defined by the organization) reviewed and measured, and the results evaluated. **Criteria for "Incomplete" Response** The organization has not established a frequency for review of program management activities, or review and measurement addresses some of the program management activities, or program management activities are reviewed but not measured, or the activity is otherwise incomplete.

MIL	Question	Guidance
MIL4 – Measured	2. Are program management activities periodically reviewed to ensure they are adhering to the plan?	**Question Intent** To periodically determine if program management activities are being performed as planned. Adherence to the plan ensures that activities are not only performing well, but that activities are improving at the planned rate. **Examples of possible periodic (as defined by the organization) plan review items:** • percentage of program management activities without designated organizational owners • count of new insider risk management functions formed without program management oversight • percentage of program management records or database entries with old or incomplete information **Typical Work Products** • designation of responsibility for periodic reviews • exception reporting • stakeholder communication regarding reviews of program management activities **Criteria for "Yes" Response** All program management activities are periodically (as defined by the organization) reviewed to ensure that these activities are performed as planned. **Criteria for "Incomplete" Response** The organization has not established a frequency for reviews, or some program management activities are reviewed, or the activity is otherwise incomplete. If MIL2.Q1 is Incomplete (can’t be a yes if there is no/incomplete Plan).

MIL	Question	Guidance
MIL4 – Measured	3. Is higher-level management aware of issues related to the performance of program management?	**Question Intent** To determine if the performance of program management is communicated to higher-level managers to provide visibility and facilitate the resolution of issues. Higher-level managers include those in the organization above the immediate level of management responsible for the program management activity. Communications are expected to be performed periodically (as defined by the organization) and may be event-driven when escalation is needed. **Typical Work Products** • reviews of status of program management activities • reporting of issues identified in activity and plan reviews • documented reporting of risks associated with program management activities • recommendations for improvement **Criteria for "Yes" Response** Higher-level management is made aware of issues related to the performance of program management. **Criteria for "Incomplete" Response** The organization has not established a frequency for communication to higher-level management, or communications address some issues, or some stakeholders are not included in the communications, or the activity is otherwise incomplete.
MIL5 – Defined	1. Has the organization adopted a standard definition of program management activities from which operating units can derive practices that fit their unique operating circumstances?	**Question Intent** Programs within large and diverse organizations often need the ability to adapt policies, procedures, and practices to meet the needs of individual lines of business, or subsidiary operating units. The program should provide enough structure and guidance to allow for subordinate programs to successfully adapt to their own business needs. **Typical Work Products** • publication of policies, procedures and practices of the program • regular reviews of subordinate program's policies, procedures and practices. **Criteria for "Yes" Response** Lines of business and subsidiary operating units are aware of the current state of the organization's program and are able to use that information to adapt to their own requirements. **Criteria for "Incomplete" Response** The organization has not fully communicated the current state of the organization's program, but lines of business and subsidiary operating units are able to adapt the organization's program to meet their own requirements.

MIL	Question	Guidance
MIL5 – Defined	2. Are improvements to program management documented and shared across the organization?	**Question Intent** Programs within large and diverse organizations often need the ability to adapt policies, procedures, and practices to meet the needs of individual lines of business, or subsidiary operating units. The program should regularly communicate changes in the organization's program to allow for subordinate programs to successfully adapt to their own business needs. **Typical Work Products** Regular meetings with lines of business and subsidiary operating units to discuss the current and potential future state of the organization's program. **Criteria for "Yes" Response** Lines of business and subsidiary operating units are aware of the current and potential future state of the organization's program and are able to use that information to adapt to their own requirements. **Criteria for "Incomplete" Response** Although lines of business and subsidiary operating units can adapt the organization's program to meet their own requirements, the program does not proactively ensure that updates to shared.

Personnel and Training

Personnel and Training MIL1

The purpose of the Personnel and Training domain is to determine if the organization has instituted the appropriate levels of insider risk awareness and training throughout the employee lifecycle. Personnel and Training includes

(1) insider risk awareness training for all personnel,

(2) role-based training for employees working with the Insider Risk Program,

(3) role-based training for Insider Risk Program team members, and

(4) incorporation of insider risk training in the onboarding process.

MIL	Question	Guidance
MIL1	**Goal 1– Participation in the Insider Risk Program is organization-wide.** The purpose of this goal is to ensure that the organization has included all of the key stakeholders in the governance, oversight and staffing of the Insider Risk Program.	
	1. Is there cooperation from components, divisions, or departments across the organization with the Insider Risk Program?	**Question Intent** To determine whether the Insider Risk Program has coverage on, and input from, the entirety of the organization. If the Insider Risk Program does not effectively collaborate with all stakeholders, then the program and organization runs the risk of incomplete coverage of risk scenarios or critical assets under the program's scope **Typical Work Products** • documentation of participating members of an Insider Risk Working Group or Council (as applicable) • documentation of roles and responsibilities for individual components, divisions, or departments as they relate to Insider Risk Program operations, e.g., reporting, communication, etc. • evidence of recurring collaboration between the Insider Risk Program and other components of the organization, such as meeting minutes or co-authored documentation **Criteria for "Yes" Response** Confirmation that the Insider Risk Program has participation from all stakeholders, including senior leadership, Human Resources (HR), Information Technology (IT), cyber security or information security/assurance (if separate from IT), legal, privacy (if separate from legal), physical security / facilities, behavioral sciences (if applicable), financial, contracts/acquisitions/purchasing, union representation (if applicable), and lines of business. **Criteria for "Incomplete" Response** Confirmation that the Insider Risk Program has participation from some but not all stakeholders listed above. Alternatively, the Insider Risk Program may have participation from all identified groups, but may lack documentation enforcing or codifying participation from those groups.

MIL	Question	Guidance
MIL1	**Goal 2– The Insider Risk Mitigation Team is composed of multi-disciplinary members with the appropriate skills and abilities.** The purpose of this goal is to ensure that the organization has created a multi-disciplinary team that can detect, identify, assess, and manage all insider related risks that are within the scope of the Insider Risk Program.	
	1. Are the work and tasks to be done by the Insider Risk Mitigation Team identified for all roles so that the organization can effectively build a set of required qualifications (knowledge and skills) for Insider Risk Mitigation Team members?	**Question Intent** If Insider Risk Mitigation Team member work tasks are not mapped and aligned with the required qualifications, the team may run the risk of being composed of overqualified or underqualified members. **Typical Work Products** A list or descriptions of all Insider Risk Mitigation Team roles along with their responsibilities or typical functions, tasks, or activities **Criteria for "Yes" Response** The organization identifies the roles and responsibilities (tasks or activities) of all Insider Risk Mitigation Team members, from which required qualifications (knowledge and skills) can be derived. **Criteria for "Incomplete" Response** The organization identifies roles and responsibilities for some, but not all, Insider Risk Mitigation Team members.
	2. Are Insider Risk Mitigation Team member qualifications—such as required knowledge, skills, competencies, education, certifications, and experience—identified based on the noted tasks to be done?	**Question Intent** If Insider Risk Mitigation Team member work tasks are not mapped and aligned with the required qualifications, the team may run the risk being composed of overqualified or underqualified members. **Typical Work Products** A role-based list, description, or mapping of Insider Risk Mitigation Team member qualifications for each work role, which identifies the expected knowledge and skills (or competencies) needed to perform typical work tasks. **Criteria for "Yes" Response** The organization identifies the qualifications (knowledge and skills) for all Insider Risk Mitigation Team member roles, based on their respective responsibilities (typical tasks or activities). **Criteria for "Incomplete" Response** Some, but not all, Insider Risk Mitigation Team members are assessed on their knowledge, skills, competencies, or other identified qualifications that are needed for them to perform their respective roles and responsibilities (or tasks).

MIL	Question	Guidance
MIL1	3. Are Insider Risk Mitigation Team members assessed on their knowledge and skills (or competencies) and any other identified qualifications?	**Question Intent** Qualifications should be identified for each role prior to hiring or assigning individuals to the Insider Risk Mitigation Team. Team members' qualifications should periodically be reviewed/updated as needed. Insider Risk Mitigation Team members who lack any of the required qualifications should be provided appropriate training or assistance in meeting the minimum qualifications. The outcome of this Goal and Question should feed into the related Goal: "The Insider Risk Mitigation Team receives training to enable them to handle their roles and tasks." **Typical Work Products** • documentation or tracking of Insider Risk Mitigation Team members' qualifications • documentation or tracking of periodic performance reviews or evaluations or Insider Risk Mitigation Team members. **Criteria for "Yes" Response** The organization reviews, assesses, or evaluates all Insider Risk Mitigation Team members on their qualifications. **Criteria for "Incomplete" Response** Some, but not all, Insider Risk Mitigation Team members are assessed on their knowledge, skills, competencies, or other identified qualifications that are needed for them to perform their respective roles and responsibilities (or tasks).

MIL	Question	Guidance
MIL1	**Goal 3– The Insider Risk Mitigation Team receives training to enable them to handle their roles and tasks.** The purpose of this goal is to ensure that the members of the Insider Risk Mitigation Team are fully trained and equipped to handle all of their roles and responsibilities within the Insider Risk Program.	
	1. Is training identified and provided to Insider Risk Mitigation Team members to enable them to effectively carry out their roles and tasks?	**Question Intent** The organization should be able to map the identified role tasks and competencies (knowledge/skills) to appropriate training resources. **Typical Work Products** • information or other resources (website, catalog, listings, etc.) that identify available or recommended training • identification or descriptions of recommended training resources that are designed to provide specific knowledge or skills • documentation of team members' learning, training, or education opportunities, which may include internal mentoring **Criteria for "Yes" Response** The organization provides training opportunities to all members of the Insider Risk Mitigation Team to enable them to effectively perform their work tasks. **Criteria for "Incomplete" Response** Training is provided inconsistently or to some (but not all) Insider Risk Mitigation Team members.
	2. Is the identification and completion of Insider Risk Mitigation Team member training tracked?	**Question Intent** Completion of training and professional development activities should be tracked and recorded. **Typical Work Products** • documentation or a tracking system that identifies the completion of team members' significant training activities • evidence of team members' goals setting or training or professional development plans that identify requested or recommended training • copies of team members' training certificates of completion Criteria for "Yes" Response **Criteria for "Yes" Response** The organization identifies and tracks the completion of all, significant training for all members of the Insider Risk Mitigation Team, including any mandatory training requirements. **Criteria for "Incomplete" Response** • The organization identifies or tracks the completion of some, but not all, significant training for all Insider Risk Mitigation Team members; or • The organization identifies and tracks the completion of training by some, but not all, members of the Insider Risk team.

MIL	Question	Guidance
MIL1	**Goal 4– New employees are made aware of the Insider Risk Program during the onboarding process.** The purpose of this goal is to ensure that all new personnel–employees, contractors, vendors, consults, etc.–receive the training necessary to recognize and report indicators of potential insider risk.	
	1. Is insider risk awareness training provided for all organizational personnel?	**Question Intent** To determine whether awareness training is provided organization-wide in support of the insider risk program. **Typical Work Products** A training regime that is provided to all personnel to support the insider risk program. Evidence may include documentation of the process, the training program itself, or records regarding its deployment and operation. **Criteria for "Yes" Response** Confirmation that insider risk awareness training is delivered to all personnel exists. **Criteria for "Incomplete" Response** Insider risk training exists, but has not been deployed or is not in operation or there is no confirmation of delivery.
	Goal 5– Insider risk awareness training is provided for all organizational personnel. The purpose of this goal is to ensure that all personnel–employees, contractors, vendors, consults, etc.–receive the training necessary to recognize and report indicators of potential insider risk.	
	1. Does the onboarding process for new employees inform the employee of the Insider Risk Program and provide guidance for how the employees should interact with that team?	**Question Intent** Determine whether the organization's new employee onboarding process includes information about the organization's Insider Risk Program, so that new employees are aware of the role and contact details of the team and are encouraged to report. **Typical Work Products** • documentation in the onboarding process of the inclusion of the Insider Risk Program information • a sample of the information that is communicated about the Insider Risk Program during onboarding **Criteria for "Yes" Response** Confirmation that all new personnel are made aware of the Insider Risk Program, so that new personnel know that the team exists, and new personnel are provided with contact details. **Criteria for "Incomplete" Response** The onboarding process provides information about the existence of the Insider Risk Program, but no resources or information are provided on how or to whom to report any observed, suspicious activities.

MIL	Question	Guidance
MIL1	**Goal 6– Role-based insider risk awareness training is provided to staff (HR, Security, IT, Legal, Contracts, Finance, etc.) regarding detection, identification, assessment, and management of insider risk behaviors and events.** The purpose of this goal is to ensure that the organization has tailored its training to the specific needs of staff. These staff roles are most likely to come into contact with specific indicators of insider risk behavior that may be unique only to their role.	
	1. Are roles that require role-based insider risk training identified?	**Question Intent** To determine if insider risk training needs have been identified for personnel who operate in parts of the organization that cooperate and support insider risk activities. **Typical Work Products** • evidence may include documentation of the training process, the training program itself, or records regarding its deployment and operation. Examples may include: • directives related to which roles are subject to insider risk training • procedures for training • training modules or other materials **Criteria for "Yes" Response** The organization has identified all of the role-based insider risk training needs for personnel supporting insider risk activities. **Criteria for "Incomplete" Response** The organization has identified some of the role-based insider risk needs for personnel supporting insider risk activities. Alternatively, the organization may have identified training needs for personnel supporting insider risk activities, but these are not yet tailored at the role-based level.
	2. Are staff/resources assigned to manage, coordinate, and support role-based insider risk training?	**Question Intent** To determine if responsibilities and resources have been allocated for addressing the insider risk training needs for personnel who operate in parts of the organization that cooperate and support insider risk activities. **Typical Work Products** Evidence may include documentation of the training process, the training program itself, or records regarding its deployment and operation. **Criteria for "Yes" Response** Confirmation that there are personnel responsible for the coordination and deployment of role-based insider risk training. **Criteria for "Incomplete" Response** While role-based insider risk training may take place, it is deployed on an ad hoc or decentralized manner.

MIL	Question	Guidance
MIL1	3. Is role-based insider risk awareness training provided to staff (HR, Security, IT, Legal, Contracts, Finance, etc.) regarding detection, identification, assessment, and management of insider risk behaviors and events?	**Question Intent** To determine whether personnel who operate in parts of the organization that cooperate and support insider risk activities receive targeted training to support the organization's Insider Risk Program. **Typical Work Products** A training regime that is targeted to support the Insider Risk Program specifically for parts of the organization that cooperate or support insider risk activities. Evidence may include documentation of the process, the training program itself, or records regarding its deployment and operation. **Criteria for "Yes" Response** Confirmation that a program designed for and delivered to personnel in HR, Physical Security, IT, Legal, Contracts, Finance, etc. exists. **Criteria for "Incomplete" Response** Role-based insider risk training is provided to only some parts of the organization; or the training is only partially developed; or not fully developed yet.
	Goal 7– Managers and supervisors receive training regarding prevention, detection, and response to insider risk behaviors and events. The purpose of this goal is to determine whether the organization includes awareness of insider risk behaviors and responses in the training necessary to recognize and report indicators of potential insider risk.	
	1. Do managers and supervisors receive training regarding detection, identification, assessment, and management of insider risk behaviors and events?	**Question Intent** To determine whether personnel who lead other personnel receive training to support the organization's Insider Risk Program. **Typical Work Products** A training regime that is targeted to support the Insider Risk Program among supervisors and management. Evidence may include documentation of the process, the training program itself, or records regarding its deployment and operation. **Criteria for "Yes" Response** Confirmation that a program designed for and delivered to supervisory personnel exists. **Criteria for "Incomplete" Response** Insider risk training for supervisory personnel does not cover all supervisors, or this training has not yet been deployed or is not yet in operation.

Personnel and Training MIL2 – MIL5

MIL	Question	Guidance
MIL2 – Planned	1. Is there a plan for performing personnel and training activities?	**Question Intent** To determine if a plan for performing personnel and training activities exists. • The plan defines training expectations within the organization and prescribes how personnel and training activities will be performed. • The plan may be a stand-alone document, embedded in a more comprehensive document, or be distributed across multiple documents. The plan may be in the form of an Insider Risk Program charter's training requirements, or in an organization's training program charter, typically includes: • overview of the content to be covered • learning objectives and outcomes • assignments of responsibility, resources, and funding for delivery and tracking of training • identification of audience for each training **Criteria for "Yes" Response** There is a documented plan for performing personnel and training activities. **Criteria for "Incomplete" Response** A plan is in development and partially documented.

MIL	Question	Guidance
MIL2 – Planned	2. Is there a documented policy for personnel and training activities?	**Question Intent** To determine if a policy for performing training activities exists. • A policy is a written communication from the organization's senior management to employees. • It establishes the organizational expectations for planning and performing the functions of an insider risk training program and communicates those expectations to the organization. The policy should address: • responsibility, authority, ownership, and the requirement to perform insider risk training activities • establishment of procedures, standards, and guidelines • establishing and maintaining an insider risk training program • measuring adherence to policy, exceptions granted (i.e., employees exempt from certain training requirements), and policy violations (i.e., failure to complete training requirements) • compliance with legal, regulatory, contractual, and government obligations **Criteria for "Yes" Response** The organization has a documented policy for performing Insider Risk training activities. **Criteria for "Incomplete" Response** A policy is in development and partially documented.

MIL	Question	Guidance
MIL2 – Planned	3. Have stakeholders for personnel and training activities been identified and made aware of their roles?	**Question Intent** To determine if stakeholders for insider risk training activities have been identified and made aware of their roles. Stakeholders of the insider risk training process have the following responsibilities: • creating insider risk learning objectives, training goals, and scope • overseeing the insider risk training process • determining courses of action and remedial training for failures to complete or "pass" learning goals, effectively managing the risk resulting from under- or un-trained workforce Examples of stakeholders include: • human resources • workforce development/training services staff • information technology staff supporting IT-enabled training delivery • Insider Risk Program manager or senior official • enterprise risk management • ethics and compliance • senior leadership **Criteria for "Yes" Response** All stakeholders for the insider risk training activities have been identified and made aware of their roles. **Criteria for "Incomplete" Response** • Some stakeholders for the insider risk training activities have been identified and made aware of their roles; or • Stakeholders are identified but have not been made aware of their roles.

MIL	Question	Guidance
MIL2 – Planned	4. Have personnel and training standards and guidelines been identified and implemented?	**Question Intent** To determine if standards and guidelines for performing personnel and training activities have been implemented. Standards establish expectations for performance, for both learners and instructors/facilitators. Guidelines are issued by an organization to ensure the performance of training activities meets standards and are predictable, measurable, and repeatable. Standards and guidelines typically address: • format and delivery method • expectations for knowledge checks, assessments, or testing • expectations for passing scores of any knowledge checks (if applicable) • measurement and reporting requirements to management and/or supervisors • recurrence of training and any refreshers • length of training • consequences for failure to complete training • consequences for failing scores on any knowledge checks (if applicable) • time allotted for an individual user to complete the training **Criteria for "Yes" Response** The organization has implemented documented standards and guidelines for performing personnel and training activities. **Criteria for "Incomplete" Response** Some standards and guidelines have been implemented.

MIL	Question	Guidance
MIL3 – Managed	1. Is there oversight of personnel and training activities?	**Question Intent** To determine if oversight exists for personnel and training activities. The intent of the practice is to ensure that an appropriate level of oversight is performed for these activities. Oversight may include having a designated steering committee, working group, or other group of senior managers who provide oversight. These groups should have regular meetings, receive written or oral status updates about the program, and conduct auditing or spot checks. **Typical Work Products** • policy or charter establishing oversight committees, working groups, etc. • assignment of responsibility in job description • organizational communications and memoranda • inclusion of activity tasks in staff performance management goals and objectives, with measured of progress against these goals **Criteria for "Yes" Response** Oversight of all personnel and training activities is being performed. **Criteria for "Incomplete" Response** Oversight covering only some activities is performed.
	2. Have qualified staff been assigned to perform personnel and training activities?	**Question Intent** To determine if qualified staff have been assigned in support of the program's personnel and training activities. The intent of this question is to evaluate the qualifications of the staff, not the completeness of the plan. "Qualified" means that staff are appropriately skilled to perform Insider Risk Program activities, and have been assigned responsibility and given authority for performing those activities. Examples of qualified staff include personnel who: • perform activities directly associated with or in support of personnel and training activities. • monitor activities to ensure alignment with expected performance and outcomes. • have knowledge of tools, techniques, and methods that can be used in support of personnel and training activities. • maintain relationships with the program's stakeholders and related organizational functions. **Typical Work Products** • documented skills required for personnel and training activities. • staffing and succession plans for Insider Risk Program activities. **Criteria for "Yes" Response** Sufficient, appropriately skilled staff have been assigned to perform planned personnel and training activities. **Criteria for "Incomplete" Response** Some but not all staff have the skills necessary to perform their roles, or the practice is otherwise incomplete.

MIL	Question	Guidance
MIL3 – Managed	3. Is there adequate funding to perform personnel and training activities as planned?	**Question Intent** To determine if adequate funding is provided for personnel and training activities. The intent of the question is to evaluate the completeness of the funding, not the completeness of the plan. **Typical Work Products** budgets to support the Insider Risk Program. **Criteria for "Yes" Response** Adequate funding has been provided to perform personnel and training activities. **Criteria for "Incomplete" Response** Activities have only been partially funded, or some related functions in the organization are not considered in the funding, or funding is otherwise incomplete.
	4. Are risks related to the performance of personnel and training activities identified, analyzed, disposed of, monitored, and controlled?	**Question Intent** To determine if the organization identifies and manages risks to the performance of its personnel and training activities. This practice refers to identifying risks to the performance of those activities. Examples of risks to these activities include: • insufficient standards or activity definition, resulting in an incorrect understanding and prioritization of risk. • variability or inaccuracy in observable or quantifiable data related to personnel and training activities. • inadequate linkage/communication about personnel and training activities with related organizational functions or stakeholders. **Typical Work Products** • evidence of a risk assessment/review of data collection and analysis activities. • reports and communications about the status of personnel and training activities **Criteria for "Yes" Response** Risks to the performance of personnel and training activities are identified, analyzed, disposed of, monitored, and controlled. **Criteria for "Incomplete" Response** Risks to the performance of activities are reviewed and identified but not controlled, or risks to the program's performance are sporadically reviewed, or the activity is otherwise incomplete.

MIL	Question	Guidance
MIL4 – Measured	1. Are personnel and training activities periodically reviewed and measured to ensure they are effective and producing intended results?	**Question Intent** To ensure personnel and training activities remain effective and produce intended results by conducting periodic review and measurement. Periodic review and tracking of measures over time allow detection of variance and correction of activities that may not be performing well. An example of a measurement is the percentage of the workforce having taken required insider risk awareness education. Other examples of training based measurements include: • the frequency of training course material audit, update and refreshing. • the frequency of train-the-trainer course material audit, update and refreshing • the percentage of passing grades for training courses. **Typical Work Products** • documented list of measures for Personnel and Training • list of identified weaknesses in Personnel and Training courses and training processes **Criteria for "Yes" Response** All Personnel and Training activities are periodically (as defined by the organization) reviewed and measured, and the results evaluated. **Criteria for "Incomplete" Response** The organization has not established a frequency for review of training course materials, or review and measurement addresses some of the training conducted but not others, or training conducted is reviewed but not measured for effectiveness.

MIL	Question	Guidance
MIL4 – Measured	2. Are personnel and training activities periodically reviewed to ensure they are adhering to the plan?	**Question Intent** To periodically determine if personnel and training activities are being performed as planned. Adherence to the plan ensures that activities are not only performing well, but that activities are improving at the planned rate. Examples of possible periodic (as defined by the organization) plan review items: • percentage of training courses without designated organizational owners • count of new training courses developed without Personnel and Training oversight • percentage of Personnel and Training records or database entries with old or incomplete information **Typical Work Products** • designation of responsibility for periodic reviews • exception reporting • stakeholder communication regarding reviews of Personnel and Training activities **Criteria for "Yes" Response** All Personnel and Training activities are periodically (as defined by the organization) reviewed to ensure that these activities are performed as planned. **Criteria for "Incomplete" Response** The organization has not established a frequency for reviews, or some training courses are not reviewed for needed updates, or the activity is otherwise incomplete.
	3. Is higher-level management aware of issues related to the performance of personnel and training activities?	**Question Intent** To determine if the performance of personnel and training activities is communicated to higher-level managers to provide visibility and facilitate the resolution of issues. Higher-level managers include those in the organization above the immediate level of management responsible for the Personnel and Training activity. Communications are expected to be performed periodically (as defined by the organization) and may be event-driven when escalation is needed. **Typical Work Products** • reviews of status of Personnel and Training activities • reporting of issues identified in activity and plan reviews • documented reporting of risks associated with Personnel and Training activities • recommendations for improvement **Criteria for "Yes" Response** Higher-level management is made aware of issues related to the performance of Personnel and Training. **Criteria for "Incomplete" Response** The organization has not established a frequency for communication to higher-level management, or communications address some issues, or some stakeholders are not included in the communications, or the activity is otherwise incomplete.

MIL	Question	Guidance
MIL5 – Defined	1. Has the organization adopted a standard definition for personnel and training activities from which operating units can derive practices that fit their unique operating circumstances?	**Question Intent** Programs within large and diverse organizations often need the ability to adapt policies, procedures, and practices to meet the needs of individual lines of business, or subsidiary operating units. The program should provide enough structure and guidance to allow for subordinate programs to successfully adapt their personnel and training requirements to meet their own business needs. **Typical Work Products** • publication of policies, procedures and practices concerning insider risk personnel and training requirements • regular reviews of subordinate program's policies, procedures and practices around their insider risk personnel and training. **Criteria for "Yes" Response** Lines of business and subsidiary operating units are aware of the current state of the organization's insider risk personnel and training standards and are able to use that information to adapt to their own requirements. **Criteria for "Incomplete" Response** The organization has not fully communicated the current state of the organization's insider risk personnel and training standards, but lines of business and subsidiary operating units are able to adapt the organization's standards to meet their own requirements.
	2. Are improvements to personnel standards and training content documented and shared across the organization?	**Question Intent** Programs within large and diverse organizations often need the ability to adapt policies, procedures, and practices to meet the needs of individual lines of business, or subsidiary operating units. The program should regularly communicate changes in the organization's insider risk personnel standards and training content to allow for subordinate programs to successfully adapt to their own business needs. **Typical Work Products** • publication of updates to the insider risk program's personnel standards and training content. • regular meetings with lines of business and subsidiary operating units to discuss the current and potential future state of the organization's insider risk personnel standards and training content. **Criteria for "Yes" Response** Lines of business and subsidiary operating units are aware of the current and potential future state of the organization's insider risk program personnel standards and training content and are able to use that information to adapt to their own requirements. **Criteria for "Incomplete" Response** Although lines of business and subsidiary operating units can adapt the organization's program to meet their own requirements, the program does not proactively ensure that updates are shared.

Data Collection and Analysis

Data Collection and Analysis MIL1

The purpose of the Data Collection and Analysis domain is to identify the elements and processes necessary for the purpose of providing timely, accurate, complete, relevant, and actionable information about and response to an organization's insider risk environment. Key elements and processes include incident reporting, forensics and behavioral analytics, response mechanisms, time-focused actions, staff augmentation and organizational support, and other elements and procedures required to support an effective Insider Risk Program. The aim of all of the above is alignment with an organization’s standards and policy, and compliance with relevant law and regulation.

MIL	Question	Guidance
MIL1	**Goal 1– The organization responds to and mitigates identified potential or ongoing insider risks and incidents.** The purpose of this goal is to determine if the organization has developed the necessary capabilities to effectively manage insider risk incidents.	
	1. Are identified insider risks and incidents mitigated and resolved?	**Question Intent** To determine whether the organization mitigates the harmful effects of and resolves as part of the incident management process those insider threat behaviors and activities identified as important. **Typical Work Products** • documentation of insider incidents with associated behaviors and activities • actions taken to clean up after incident • actions taken to mitigate harmful effects of incident • actions take to prevent the incident in the future • actions taken to close out the incident **Criteria for "Yes" Response** Confirmation that identified insider risk behaviors and activities are tracked through the incident management process to resolution and that mitigation actions are taken. **Criteria for "Incomplete" Response** Incomplete tracking of the incidents through the incident management process or lack of mitigation of those incidents.

MIL	Question	Guidance
MIL1	2. Does the organization follow established procedures or guidelines for responding to and mitigating insider risks and incidents?	**Question Intent** To determine whether incident response procedures/guidelines are followed during the operational practice of incident resolution and mitigation. **Typical Work Products** • validation of collected alerts and reports • inquiries or investigations to clarify or resolve insider risk matters • documenting each reported insider risk behavior or activity documenting each confirmed insider risk activity • handing off investigations • inquiries, and mitigations to appropriate internal or external entities • coordinating and communicating insider risk mitigation and response tasks across the organization to contain and resolve the activity, including IT, HR, physical and personnel security, counterintelligence, Insider Risk Mitigation Team, and data owners. **Criteria for "Yes" Response** Confirmation that documented processes/guidelines are followed as described. **Criteria for "Incomplete" Response** Incomplete adherence to documented processes, for example by not following the process completely for identified incidents, or not tracking all incidents identified.
	3. Does resolution of insider risk matters occur in a timely fashion, as defined by organizational or federal criteria?	**Question Intent** To determine whether insider incidents are resolved according to timeliness requirements. **Typical Work Products** • documentation of the timeliness requirements for incident management specified either by internal or external criteria • tracking of the insider incident resolution timeline **Criteria for "Yes" Response** Confirmation that insider incidents are resolved according to the timeliness requirements. **Criteria for "Incomplete" Response** Lack of identification of incident response timeliness requirements or incomplete tracking of the incident resolution timeline.

MIL	Question	Guidance
MIL1	4. Are additional staff identified and called in if needed to assist with resolving and remediating insider risk events?	**Question Intent** To determine whether the organization has the flexibility to scale up the insider incident management processes during times of higher than normal volume of insider risk events. **Typical Work Products** • process that establishes conditions for calling in additional staff, including individuals identified and contact information • agreements with on-call individuals and their management for the provided contingent service **Criteria for "Yes" Response** Confirmation that scale-up processes are in place, individuals identified, and agreements for contingent services obtained. **Criteria for "Incomplete" Response** Incomplete documentation of scale-up processes, lack of individuals identified, or uncertainty regarding the agreements for contingency services provided.
	5. Is the established chain-of-command followed to effect a disposition of all insider risk cases?	**Question Intent** To determine whether the disposition of all insider risk cases is authorized by the critical decision makers. **Typical Work Products** • policy that establishes the chain-of-command for all classes of insider risk identified as important to the organization • sign offs by those identified with command authorization as incidents are responded to during incident management processes **Criteria for "Yes" Response** Confirmation chain-of-command policies exist and processes are followed. **Criteria for "Incomplete" Response** Incomplete documentation of the chain-of-command for certain incident types, or lack of sign off by command authorities in the incident management process.

MIL	Question	Guidance
MIL1	6. Is forensic evidence collected, if necessary?	**Question Intent** To determine whether the organization collects forensic evidence as needed during the incident management process. Forensic evidence may be necessary to gain sufficient confidence about what actually happened in an insider incident. **Typical Work Products** Process for collecting forensic evidence, including when such evidence should be collected and how the evidence should be handled. **Criteria for "Yes" Response** Documentation of the forensic evidence collection process and staff identified with forensic collection capabilities. **Criteria for "Incomplete" Response** Incomplete documentation of the forensic collection processes or lack of capable staff identified.
	7. Is digital media analyzed, if necessary?	**Question Intent** To determine whether the organization analyzes digital media as needed during the incident management process. **Typical Work Products** Process for analyzing digital media, including when such media should be analyzed and how collected evidence should be handled. **Criteria for "Yes" Response** Documentation of the digital media analysis process and staff identified with digital media analysis capabilities. **Criteria for "Incomplete" Response** Incomplete documentation of the digital media analysis processes or lack of capable staff identified.
	8. Do documented procedures specify the process and mechanisms to reconstitute and recover critical systems that are affected by insider risk events?	**Question Intent** To determine whether the organization has the processes and mechanisms documented to reconstitute and recover critical systems in the event they are compromised by insider incidents. **Typical Work Products** Documentation of critical system reconstitution and recovery processes and mechanisms. **Criteria for "Yes" Response** Confirmation that a document exists that describes the process of reconstituting and recovering critical systems to full operational capability. **Criteria for "Incomplete" Response** Documentation does not cover all critical systems or does not extend to full operational capability.

MIL	Question	Guidance
MIL1	**Goal 2– Processes exist to minimize barriers to the Insider Risk Mitigation Team's access to relevant information in an efficient and secure manner.** The purpose of this goal is to determine if processes are in place that ensure that data elements needed by the Insider Risk Mitigation Team are provided by data owners.	
	1. Has senior or executive management directed components of the organization to provide data sources and other information to the Insider Risk Mitigation Team that are necessary to identify, analyze, and resolve insider risk matters?	**Question Intent** To determine whether senior or executive management has directed components of the organization to provide data sources and other information to the Insider Risk Mitigation Team that are necessary to identify, analyze, and resolve insider risks and incidents. Such direction is necessary to show senior support for the Insider Risk Program mission and to facilitate data sharing internally. **Typical Work Products** • policy that establishes senior or executive management support for data sharing with the Insider Risk Mitigation Team • documentation of the data sources needed by the Insider Risk Mitigation Team and the reasons and conditions for needing the data • regular communications that direct organization components to share data with the Insider Risk Mitigation Team. **Criteria for "Yes" Response** Evidence of senior or executive management support for the Insider Risk Program mission in terms of documented policy directing organizational components to share data sources with the Insider Risk Program. **Criteria for "Incomplete" Response** Support for data sharing with Insider Risk Mitigation Team expressed but not documented in policy, and/or direction does not include data owned by other components that is needed to identify, analyze, or resolve insider risks and incidents.

MIL	Question	Guidance
MIL1	2. Are data sources and other relevant information provided in a secure manner?	**Question Intent** To determine whether data sources provided to Insider Risk Mitigation Team are sufficiently protected in their communication. **Typical Work Products** • security policy for handling data provided to the Insider Risk Mitigation Team • documentation of the procedures for transferring data sources to Insider Risk Mitigation Team. **Criteria for "Yes" Response** Confirmation that all security policies and procedures are followed in transfer of data sources to the Insider Risk Mitigation Team. **Criteria for "Incomplete" Response** Some lapses in protecting data transfer to the Insider Risk Mitigation Team according to security policies and procedures.
	3. Are data sources and other relevant information provided in a timely manner, according to organizational requirements?	**Question Intent** To determine whether data sources provided to Insider Risk Mitigation Team are provided in time to handle insider events efficiently and effectively. **Typical Work Products** • timeliness requirements for provision upon data request • data provision agreements with organization components that stipulate timeliness requirements **Criteria for "Yes" Response** Confirmation that all data provision agreements are in force and adhered to. **Criteria for "Incomplete" Response** Incomplete coverage of, adherence to, or lack of documentation of timeliness requirements for data provided by organization components to the Insider Risk Mitigation Team.

MIL	Question	Guidance
MIL1	4. Are procedures established for the Insider Risk Mitigation Team to request access to organizational components that maintain or handle sensitive or protected information?	**Question Intent** To determine whether a means is established for requesting access to needed sensitive or protected information from organizational components. **Typical Work Products** Data request procedures and forms **Criteria for "Yes" Response** Documentation of established procedures for requesting all data sources needed by the Insider Risk Mitigation Team. **Criteria for "Incomplete" Response** Lack of coverage or documentation of request procedures.
	5. Does the organization have guidelines for all components—such as IT and HR—to report information about insider threats directly to the Insider Risk Team?	**Question Intent** To determine whether organizational components have guidance on how to report information about insider risks directly to the Insider Risk Program. Organization components may be the first to have information critical to the timely response to insider incidents. **Typical Work Products** • documented guidance on reporting information about insider risks directly to the Insider Risk Program • report format templates. **Criteria for "Yes" Response** Documentation of procedures for reporting information directly to the Insider Risk Program. **Criteria for "Incomplete" Response** Identification of reporting procedures without documentation, or documentation does not adequately cover the variety of information reported by organization components.

MIL	Question	Guidance
MIL1	6. Does the Insider Risk Mitigation Team have timely access to analytic products pertaining to adversarial threats, based on organizational requirements?	**Question Intent** To determine whether analytic products produced by others can be obtained by Insider Risk Mitigation Team in time to handle insider events efficiently and effectively. **Typical Work Products** • identification of analytic products produced by others needed by the Insider Risk Mitigation Team • timeliness requirements for provision of analytic products once produced • data provision agreements with sources of analytic products that stipulate timeliness requirements **Criteria for "Yes" Response** Documentation of analytic products needed and confirmation that all data provision agreements are in force. **Criteria for "Incomplete" Response** Incomplete coverage of or lack of documentation of timeliness requirements for analytic product provided to the Insider Risk Mitigation Team.
	7. Are all information-sharing activities conducted in accordance with applicable laws, whistleblower protections, civil liberties, and privacy policies?	**Question Intent** To determine whether information sharing is conducted on a strong legal basis and in accordance with applicable policies. **Typical Work Products** • identification of regulation and policies to which information sharing activities must conform • regular review of current laws and policies, noting those that are new or have been modified • argument that information sharing activities are in conformance with current applicable laws and policies **Criteria for "Yes" Response** Confirmation that all applicable laws and policies are followed in all information sharing activities. **Criteria for "Incomplete" Response** Some information sharing activities are conducted in violation of identified laws and policies, or review of the applicability of laws and policies to information sharing activities is outdated.

MIL	Question	Guidance
MIL1	8. Are new data sources reviewed for applicability to the Insider Risk Program?	**Question Intent** To determine whether data sources that are newly available within the organization are reviewed to determine whether they provide useful input to resolve insider risk concerns. **Typical Work Products** • process for identifying new data sources as they arise • criteria for when a new data source is deemed applicable to the Insider Risk Program • document describing review procedures for new data sources • documented justification for deeming new data sources as applicable (or not) to the Insider Risk Program **Criteria for "Yes" Response** Confirmation that new data sources are reviewed and judged to be applicable or not to the Insider Risk Program. **Criteria for "Incomplete" Response** Gaps in identifying new data sources exist, or in the process of judging new data sources for their applicability to the Insider Risk Program.
	9. Do documented policies and procedures specify the processes and mechanisms used by the Insider Risk Mitigation Team to gain access to new data sources?	**Question Intent** To determine whether there are documented means for the Insider Risk Mitigation Team to gain access to new data sources. **Typical Work Products** • process by which Insider Risk Mitigation Team can gain access to a new data source • justification of the need for new or additional data access • sign-off from legal and management to permit access to the new data source • in-motion and at-rest security requirements for the new data to be collected **Criteria for "Yes" Response** Documentation of established procedures for requesting access to new data sources needed by the Insider Risk Mitigation Team. **Criteria for "Incomplete" Response** Established procedures for requesting access are identified but not documented.

MIL	Question	Guidance
MIL1	**Goal 3– Relevant organizational components securely provide the Insider Risk Mitigation Team with the information necessary to detect, identify, assess, and manage insider risk activities.** The purpose of this goal is to ensure that the appropriate data elements needed by the Insider Risk Mitigation Team are shared, processed, and stored using the proper protections.	
	1. Is the data that must be sent to the Insider Risk Mitigation Team or for which access is to be allowed defined in policy or guidance?	**Question Intent** To determine whether the data to be supplied when a data source is requested is specified in policy or guidance. **Typical Work Products** Data specification for each data source **Criteria for "Yes" Response** Documentation of the data to be sent for each data source relevant to the Insider Risk Program. **Criteria for "Incomplete" Response** Data is not specified for all data sources.
	2. Does data reported to the Insider Risk Mitigation Team or for which access is allowed include the following categories? • Personnel usernames • Levels of network access • Audit data • Unauthorized use of removable data • Print logs	**Question Intent** To determine whether data supplied to the Insider Risk Mitigation Team includes specific data items. **Typical Work Products** A specification of the data provided to the Insider Risk Mitigation Team including the following: • personnel usernames and aliases • levels of network access • audit data • unauthorized use of removable media • print logs **Criteria for "Yes" Response** Documentation of the data to be sent to the Insider Risk Mitigation Team includes all of the required field. **Criteria for "Incomplete" Response** Data to be sent to the Insider Risk Mitigation Team does not include all of the required fields.

MIL	Question	Guidance
MIL1	3. Does data reported to the Insider Risk Mitigation Team or for which access is allowed include incident reports?	**Question Intent** To determine whether data supplied to the Insider Risk Mitigation Team includes incident reports. **Typical Work Products** A specification of incident reports **Criteria for "Yes" Response** Documentation of the data to be sent to the Insider Risk Mitigation Team includes incident reports, or incident reports are otherwise available to the Insider Risk Mitigation Team. **Criteria for "Incomplete" Response** Some incident reports, or parts of incident reports, are not sent or not available to the Insider Risk Mitigation Team.
	Goal 4– The organization monitors user activity on its networks and systems to identify concerning behaviors that are within the scope of the Insider Risk Program. The purpose of this goal is to ensure the organization collects the user activity data that will be needed for analytics that can identify concerning behaviors.	
	1. Does the Insider Risk Mitigation Team have access to the necessary user activity data on its networks and systems to allow it to identify concerning behaviors that are within the scope of the Insider Risk Program?	**Question Intent** To determine if the Insider Risk Mitigation Team has user activity data available that can contain concerning behaviors that are within the scope of the Insider Risk program. Examples of user activity data include (but are not limited to): • email logs • chat logs • phone logs • web browsing activity • facility access logs **Typical Work Products** • various user activity monitoring logs • access to User Activity Monitoring tool(s) interface(s), or aggregated data that results from monitoring. **Criteria for "Yes" Response** Access to the necessary user activity monitoring data to identify concerning behaviors that are within the scope of the Insider Risk Program. **Criteria for "Incomplete" Response** The Insider Risk Mitigation Team has access to some of the user activity monitoring data, but not everything that is needed to cover the scope of the Insider Risk Program.

MIL	Question	Guidance
MIL1	**Goal 5– The organization has an insider risk analytic capability to gather, review, and analyze information for concerning behaviors that are within the scope of the Insider Risk Program.** The purpose of this goal is to ensure the organization has the ability to conduct analytics on the user activity data that it collects.	
	1. Is there a defined and established insider risk analytic capability?	**Question Intent** To determine if the Insider Risk Mitigation Team can identify and analyze concerning behaviors that are within the scope of the Insider Risk Program. **Typical Work Products** • policy, charter, or procedure establishing an analytic capability • standard operating procedures defining analytics **Criteria for "Yes" Response** Evidence of a defined and established insider risk capability exists and is approved (see typical work products). **Criteria for "Incomplete" Response** Evidence of a defined and established insider risk capability is in draft but is not approved (see typical work products).
	2. Have analysts been identified and trained to perform required insider risk analytical activities?	**Question Intent** To determine if the Insider Risk Mitigation Team has insider risk analysts assigned and trained to identify concerning behaviors that are within the scope of the program. **Typical Work Products** • documents that delineate the roles and responsibilities of insider risk analyst. Some examples of such documents could include: • policies, charters, concepts of operations, or procedures • position descriptions • performance goals and objectives • training records for insider risk analysts **Criteria for "Yes" Response** There is evidence (documents, as described in typical work products) that insider risk analysts are assigned and trained to identify concerning behaviors that are within the scope of the program. **Criteria for "Incomplete" Response** There is evidence of either insider risk analysts being assigned, or of the training necessary to identify concerning behaviors that are within the scope of the program, but not both of these elements.

MIL	Question	Guidance
MIL1	3. Does the analytical capability sufficiently allow for the integration, review, and assessment of user activity to identify concerning behaviors that are within the scope of the Insider Risk Program?	**Question Intent** To determine if the Insider Risk Mitigation Team can integrate, review, and assess the data collected by the organization to identify concerning behaviors. **Typical Work Products** • procedures for conducting analysis on collected data • analytic reports • referrals of incidents **Criteria for "Yes" Response** Analysis if performed on all data that is collected and aggregated. **Criteria for "Incomplete" Response** Analysis can be performed on some of the data, but not all. This could be because of not being able to properly normalize or aggregate some of the data, or some other reason why not all of the data that can identify concerning behaviors is being analyzed.
	Goal 6– The Insider Risk Mitigation Team leverages employee background screening data. The purpose of this goal is to ensure that the Insider Risk Mitigation Team has access to the background screening data necessary to support risk-based hiring decisions and the analysis of insider activity anomalies and allegations.	
	1. Is there a defined process in place for sharing background screening data about an employee with the Insider Risk Program (if applicable)?	**Question Intent** To determine if efforts to share employee background screening data is shared with the Insider Risk Program in a repeatable and consistent manner. **Typical Work Products** Evidence may include Standard Operating Procedures (SOPs), guidelines, or tools that facilitate sharing of background screening data **Criteria for "Yes" Response** The organization has defined and established processes for sharing employee background screening data with the Insider Risk Program. Alternatively, the organization may have documented any justification(s) for why this information may not be made available to the Insider Risk Program at certain stages of an inquiry or investigation. **Criteria for "Incomplete" Response** Employee background screening data may be shared with the Insider Risk Program on an ad hoc basis; the process for sharing background screening data is not documented; or, the data may be shared with the Insider Risk Program in an inconsistent manner.

MIL	Question	Guidance
MIL1	2. Are there thresholds for sharing employee background screening data with the Insider Risk Program when potential incidents or escalation thresholds require them?	**Question Intent** To determine if employee background screening data is shared in accordance with formally established guidelines and policies maintained by the organization. **Typical Work Products** Evidence may include Memorandum of Understanding (MOU) between departments collecting and analyzing data, Standard Operating Procedures (SOPs), guidelines, templates for making data requests, or analyst workflows. **Criteria for "Yes" Response** Confirmation that there are thresholds for when employee background screening data may be shared with the Insider Risk Program, to include at what stage in an inquiry or investigation individual data points may be shared (if applicable). **Criteria for "Incomplete" Response** Employee background screening data is shared on an inconsistent or ad hoc basis; or, thresholds for how employee background screening data may be shared do not accurately reflect the data source or the escalation/investigation process in place.
	Goal 7– The Insider Risk Mitigation Team supports the employee separation processes. The purpose of this goal is to determine whether the Insider Risk Mitigation Team is involved in the organization's secure employee separation process, proactively identifying potential insider risk behaviors related to personnel leaving the organization.	
	1. Is there a defined process in place for notifying the Insider Risk Program when an employee is going to separate (or be separated from) the organization?	**Question Intent** To determine if efforts to notify the Insider Risk Program about departing employees occurs in a repeatable and consistent manner. **Typical Work Products** Evidence may include sample or template notifications related to employee separations, such as a list or dashboard of departing employees **Criteria for "Yes" Response** Confirmation that there is a defined process for notifying the Insider Risk Program of employee separations. **Criteria for "Incomplete" Response** Processes for employee separations are not documented or occur on an ad hoc basis.

MIL	Question	Guidance
MIL1	2. Is there a formal or written procedure with accountability for compliance by which the Insider Risk Program is notified in a timely manner when an employee is going to separate (or be separated from) the organization??	**Question Intent** To determine if the Insider Risk Program is positioned to detect, identify, assess, and manage insider risk posed by departing employees before they formally separate from the organization. **Typical Work Products** Evidence may include policies related to when the Insider Risk Program should be notified, or tools or techniques that automate notifications to the Insider Risk Program about employee separations **Criteria for "Yes" Response** Confirmation that there is a defined threshold for when the Insider Risk Program is notified of an employee separation, which would, at minimum, take place on or before the day of the employee's departure. **Criteria for "Incomplete" Response** While the Insider Risk Program may be notified about employee separations, it may take place inconsistently or after the employee has already separated from the organization.
	3. Is there a defined offboarding process in place for separating employees that includes affirmation of continuing adherence to insider risk training, non-disclosure agreements, etc.?	**Question Intent** To determine if insider risk posed by departing employees is considered and consistently mitigated as part of the offboarding process. **Typical Work Products** Evidence may include documentation of and justification for a formal employee separation process, which may take the form of a policy, directive, or procedure. **Criteria for "Yes" Response** Confirmation that there is a documented employee separation process and that it is applied in accordance with the scope identified in any relevant policies or procedures. **Criteria for "Incomplete" Response** While documentation may exist on the employee separation process, it is not consistently applied; or, documentation on the employee separation process is not in place or does not reflect the entire process.

MIL	Question	Guidance
MIL1	4. Are staff/resources assigned to manage, coordinate, and support the employee separation process?	**Question Intent** To determine if responsibilities and resources have been allocated for addressing the insider risk posed by departing employees. **Typical Work Products** Evidence may include documentation of the employee separation / offboarding process, an offboarding checklist, or records regarding its execution and operation. **Criteria for "Yes" Response** Confirmation that there are personnel responsible for the coordination and execution of the employee separation process. **Criteria for "Incomplete" Response** While activities related to employee separation may take place, it is deployed on an ad hoc or decentralized manner.
	Goal 8– The Insider Risk Mitigation Team can identify acceptable and unacceptable employee behavior. The purpose of this goal is to ensure that the Insider Risk Program can distinguish between acceptable (i.e., expected) and unacceptable behavior in its analytics. Being able to tell this difference will help reduce workload on the analysts by providing more relevant alerts for review.	
	1. Does the Insider Risk Program incorporate the organization's policies that define acceptable and unacceptable workplace behavior into its analytical capabilities?	**Question Intent** To determine if the Insider Risk Program has the ability to distinguish between expected user behavior and anomalous or unacceptable workplace behavior. The ability to quickly disregard expected behavior can help to reduce alerts produced by tools and time needed by analysts. **Typical Work Products** • ingest of acceptable use policy • ingest of code of conduct • ingest of conflict of interest • ingest of code of ethics **Criteria for "Yes" Response** Insider risk tools and analysts are able to recognize acceptable behaviors and not alert on them. **Criteria for "Incomplete" Response** Analysts or insider risk tools can sometimes, but not always, recognize and ignore acceptable behaviors.

Data Collection and Analysis MIL2 – MIL5

MIL	Question	Guidance
MIL2 – Planned	1. Is there a plan for performing data collection and analysis activities?	**Question Intent** To determine if a plan for performing data collection and analysis activities exists. • The plan defines accepted data collection and analysis within the organization and prescribes how data collection and analysis activities will be performed. • The plan may be a stand-alone document, embedded in a more comprehensive document, or be distributed across multiple documents. The plan, which may be in the form of a Standard Operating Procedure (SOP), typically includes: • purpose and scope of data collection and analysis activities • roles, assignments of responsibility, resources, and funding • identification of technology and resources • measurement, escalation, and reporting/communication requirements • training requirements (e.g., for analysts) • management oversight **Criteria for "Yes" Response** There is a documented plan for performing data collection and analysis. **Criteria for "Incomplete" Response** A plan is in development and partially documented.

MIL	Question	Guidance
MIL2 – Planned	2. Is there a documented policy for data collection and analysis activities?	**Question Intent** To determine if a policy for performing data collection and analysis activities exists. • A policy is a written communication from the organization's senior management to employees. • It establishes the organizational expectations for planning and performing the functions associated with insider risk detection and response, as well as communicating those expectations to the organization. The policy should address: • responsibility, authority, ownership, and the requirement to perform data collection and analysis activities • establishment of procedures, standards, and guidelines • expectations for individuals performing data collection and analysis activities (e.g., conflict of interest reporting, additional privacy or non-disclosure agreements) • measuring adherence to policy, exceptions granted, and policy violations • compliance with legal, ethical, regulatory, contractual, and government obligations **Criteria for "Yes" Response** The organization has a documented policy for performing data collection and analysis activities. **Criteria for "Incomplete" Response** A policy is in development and partially documented.

MIL	Question	Guidance
MIL2 – Planned	3. Have stakeholders for data collection and analysis activities been identified and made aware of their roles?	**Question Intent** To determine if stakeholders for data collection and analysis activities have been identified and made aware of their roles. Stakeholders of the data collection and analysis process have the following responsibilities: • formalizing scope and use cases for monitoring related to insider risk • overseeing the data collection and analysis process • overseeing the individuals performing data collection and analysis activities • granting access to individuals performing data collection and analysis activities on a need-to-know basis • restricting access to information sources or tools used for data collection and analysis to only those with a need-to-know Examples of stakeholders include: • data source owners and custodians • external entities responsible for some part of data collection, monitoring, or response • information technology staff, including those responsible for identity and access management • human resources • internal auditors • cyber or information security staff, including those responsible for tools and/or monitoring **Criteria for "Yes" Response** All stakeholders for the data collection and analysis activities have been identified and made aware of their roles. **Criteria for "Incomplete" Response** • Some stakeholders for the data collection and analysis activities have been identified and made aware of their roles; or • Stakeholders are identified but have not been made aware of their roles.

MIL	Question	Guidance
MIL2 – Planned	4. Have data collection and analysis standards and guidelines been identified and implemented?	**Question Intent** To determine if standards and guidelines for performing data collection and analysis activities have been implemented. • Standards establish expectations for performance. • Guidelines are issued by an organization to ensure the performance of data collection and analysis activities meets standards and is predictable, measurable, and repeatable. Standards and guidelines typically address: • establishing the use cases and scope (in terms of employees and data sources) of data collection and analysis activities • documenting critical assets protected and subject to monitoring by the Insider Risk Program • designating or allowing access to data sources or tools used for data collection and analysis • sensitivity categorization for information assets and tools • documenting data collection and analysis requirements • defining escalation and response processes **Criteria for “Yes” Response** The organization has implemented documented standards and guidelines for performing data collection and analysis activities. **Criteria for “Incomplete” Response** Some standards and guidelines have been implemented.

MIL	Question	Guidance
MIL3 – Managed	1. Is there oversight of data collection and analysis activities?	**Question Intent** To determine if oversight exists for data collection and analysis activities. The intent of the practice is to ensure that an appropriate level of oversight is performed. Oversight may include having a designated steering committee, working group, or other group of senior managers who provide oversight of the Insider Risk Program. These types of groups should have regular meetings, receive written or oral status updates about the program, and conduct auditing or spot checks. **Typical Work Products** • policy or charter establishing oversight committees, working groups, etc. • assignment of responsibility in job description • organizational communications and memoranda • policy describing data collection and analysis activities, including rules and guidance, limits and prohibition, and awareness of compliance requirements for data collection and analysis. **Criteria for "Yes" Response** Oversight of all day-to-day data collection and analysis activities is being performed. **Criteria for "Incomplete" Response** Oversight covers some aspects of data collection and analysis activities, or there is insufficient oversight, or the activity is otherwise incomplete. Written or oral status updates about the program, and conduct auditing or spot checks.

MIL	Question	Guidance
MIL3 – Managed	2. Have qualified staff been assigned to perform data collection and analysis activities?	**Question Intent** To determine if qualified staff have been assigned to perform data collection and analysis activities. The intent of this question is to evaluate the qualifications of the staff, not the completeness of the plan. "Qualified" means that staff are appropriately skilled to perform Insider Risk Program activities, and have been assigned responsibility and given authority for performing those activities. Examples of qualified staff include personnel who: • meet the requirements as established by the organization's job descriptions. • are evaluated to ensure they are capable of performing expected functions. • have knowledge of tools, techniques, and methods that can be used to identify, analyze, mitigate, and monitor operational impacts resulting from or incurred by insider risk. **Typical Work Products** • documented skills required for data collection and analysis activities. • staffing and succession plans for Insider Risk Program activities. **Criteria for “Yes” Response** Sufficient, appropriately skilled staff have been assigned to perform planned data collection and analysis activities. **Criteria for “Incomplete” Response** Some but not all staff have the skills necessary to perform their roles, or the practice is otherwise incomplete.
	3. Is there adequate funding to perform data collection and analysis activities as planned?	**Question Intent** To determine if adequate funding is provided to operate and support data collection activities. The intent of the question is to evaluate the completeness of the funding, not the completeness of the plan. **Typical Work Products** budgets to support the Insider Risk Program. **Criteria for “Yes” Response** Adequate funding has been provided to perform data collection and analysis activities. **Criteria for “Incomplete” Response** Activities have only been partially funded, or some related functions in the organization are not considered in the funding, or funding is otherwise incomplete.

MIL	Question	Guidance
MIL3 – Managed	4. Are risks related to the performance of planned data collection and analysis activities identified, analyzed, disposed of, monitored, and controlled?	**Question Intent** To determine if the organization identifies and manages risks to the performance of its data collection and analysis activities. This practice refers to identifying risks to the performance of those activities. Examples of risks to these activities include: • insufficient standards or activity definition, resulting in an incorrect understanding and prioritization of risk. • variability or inaccuracy in observable or quantifiable data related to data collection and analysis activities. • inadequate linkage/communication about data collection and analysis activities with related organizational functions or stakeholders. **Typical Work Products** • evidence of a risk assessment/review of data collection and analysis activities. • reports and communications about the status of data collection and analysis activities **Criteria for “Yes” Response** Risks to the performance of activities are identified, analyzed, disposed of, monitored, and controlled. **Criteria for “Incomplete” Response** Risks to the performance of activities are reviewed and identified but not controlled, or risks to the program's performance are sporadically reviewed, or the activity is otherwise incomplete.

MIL	Question	Guidance
MIL4 – Measured	1. Are data collection and analysis activities periodically reviewed and measured to ensure they are producing intended results?	**Question Intent** To ensure the Data Collection and Analysis activities remain effective and produce intended results by conducting periodic review and measurement. Periodic review and tracking of measures over time allow detection of variance and correction of activities that may not be performing well. An example of a measurement is the percentage of data requests responded to within the time required. Other examples of Data Collection and Analysis measurements include: • the percentage of analytic products requests responded to within the time required. • the percentage of new data sources reviewed for their relevance to the Insider Risk Program mission. • the percentage of responses to data requests that contain required information. **Typical Work Products** • documented list of measures for Data Collection and Analysis • list of identified weaknesses in Data Collection and Analysis processes **Criteria for "Yes" Response** All Data Collection and Analysis activities are periodically (as defined by the organization) reviewed and measured, and the results evaluated. **Criteria for "Incomplete" Response** The organization has not established a frequency for review of Data Collection and Analysis activities, or review and measurement addresses some of the activities conducted but not others, or activities are reviewed but not measured for effectiveness.

MIL	Question	Guidance
MIL4 – Measured	2. Are data collection and analysis activities periodically reviewed to ensure they are adhering to the plan?	**Question Intent** To periodically determine if Data Collection and Analysis activities are being performed as planned. Adherence to the plan ensures that activities are not only performing well, but that activities are improving at the planned rate. Examples of possible periodic (as defined by the organization) plan review items: • percentage of Data Collection and Analysis activities without designated organizational owners • count of Data Collection and Analysis activities developed without oversight • percentage of Data Collection and Analysis records or database entries with old or incomplete information **Typical Work Products** • designation of responsibility for periodic reviews • exception reporting • stakeholder communication regarding reviews of Data Collection and Analysis activities **Criteria for “Yes” Response** All Data Collection and Analysis activities are periodically (as defined by the organization) reviewed to ensure that these activities are performed as planned. **Criteria for “Incomplete” Response** The organization has not established a frequency for reviews, or some activities are not reviewed for needed updates, or the activity is otherwise incomplete.

MIL	Question	Guidance
MIL4 – Measured	3. Is higher-level management aware of issues related to the performance of data collection and analysis?	**Question Intent** To determine if the performance of Data Collection and Analysis is communicated to higher-level managers to provide visibility and facilitate the resolution of issues. Higher-level managers include those in the organization above the immediate level of management responsible for the Data Collection and Analysis activity. Communications are expected to be performed periodically (as defined by the organization) and may be event-driven when escalation is needed. **Typical Work Products** • reviews of status of Data Collection and Analysis activities • reporting of issues identified in activity and plan reviews • documented reporting of risks associated with Data Collection and Analysis activities • recommendations for improvement **Criteria for “Yes” Response** Higher-level management is made aware of issues related to the performance of Data Collection and Analysis. **Criteria for “Incomplete” Response** The organization has not established a frequency for communication to higher-level management, or communications address some issues, or some stakeholders are not included in the communications, or the activity is otherwise incomplete.
MIL5 – Defined	1. Has the organization adopted a standard definition of data collection and analysis activities from which operating units can derive practices that fit their unique operating circumstances?	**Question Intent** Programs within large and diverse organizations often need the ability to adapt policies, procedures, and practices to meet the needs of individual lines of business, or subsidiary operating units. The program should provide enough structure and guidance to allow for subordinate programs to successfully adapt data collection and analysis activities to meet their own business needs. **Typical Work Products** • Publishing of policies, procedures and practices of the program's data collection and analysis activities • Regular reviews of subordinate program's policies, procedures and practices for data collection and analysis activities. **Criteria for “Yes” Response** Lines of business and subsidiary operating units are aware of the current state of the program's data collection and analysis activities and are able to use that information to adapt to their own requirements. **Criteria for “Incomplete” Response** The organization has not fully communicated the current state of the program's data collection and analysis activities, but lines of business and subsidiary operating units are able to adapt the program's activities to meet their own requirements.

MIL	Question	Guidance
MIL5 – Defined	2. Are improvements to the program's data collection and analysis activities documented and shared across the organization?	**Question Intent** Programs within large and diverse organizations often need the ability to adapt policies, procedures, and practices to meet the needs of individual lines of business, or subsidiary operating units. The program should regularly communicate changes in the program's data collection and analysis activities to allow for subordinate programs to successfully adapt to their own business needs. **Typical Work Products** Regular meetings with lines of business and subsidiary operating units to discuss the current and potential future state of the program's data collection and analysis activities. **Criteria for "Yes" Response** Lines of business and subsidiary operating units are aware of potential future state of the program's data collection and analysis activities and are able to use that information to adapt to their own requirements. **Criteria for "Incomplete" Response** Although lines of business and subsidiary operating units can adapt the program's data collection and analysis activities to meet their own requirements, the program does not proactively ensure that updates to shared.

CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY