3.4 MONITORING RISK

Risk monitoring provides organizations with the means to: (i) verify *compliance*;[64] (ii) determine the ongoing *effectiveness* of risk response measures; and (iii) identify risk-impacting *changes* to organizational information systems and environments of operation. Analyzing monitoring results gives organizations the capability to maintain awareness of the risk being incurred, highlight the need to revisit other steps in the risk management process, and initiate process improvement activities as needed.[65] Organizations employ risk monitoring tools, techniques, and procedures to increase risk awareness, helping senior leaders/executives develop a better understanding of the ongoing risk to organizational operations and assets, individuals, other organizations, and the Nation. Organizations can implement risk monitoring at any of the risk management tiers with different objectives and utility of information produced. For example, Tier 1 monitoring activities might include ongoing threat assessments and how changes in the threat space may affect Tier 2 and Tier 3 activities, including enterprise architectures (with embedded information security architectures) and organizational information systems. Tier 2 monitoring activities might include, for example, analyses of new or current technologies either in use or considered for future use by organizations to identify exploitable weaknesses and/or deficiencies in those technologies that may affect mission/business success. Tier 3 monitoring activities focus on information systems and might include, for example, automated monitoring of standard configuration settings for information technology products, vulnerability scanning, and ongoing assessments of security controls. In addition to deciding on appropriate monitoring activities across the risk management tiers, organizations also decide how monitoring is to be conducted (e.g., automated or manual approaches) and the frequency of monitoring activities based on, for example, the frequency with which deployed security controls change, critical items on plans of action and milestones, and risk tolerance.

STEP 4: RISK MONITORING

Inputs and Preconditions

Inputs to this step include implementation strategies for selected courses of action for risk responses and the actual implementation of selected courses of action. In addition to the risk response step, the risk monitoring step can receive inputs from the risk framing step (e.g., when organizations become aware of an advanced persistent threat reflecting a change in threat assumptions, this may result in a change in the frequency of follow on monitoring activities). The risk framing step also directly shapes the resource constraints associated with establishing and implementing an organization-wide monitoring strategy. In some instances, outputs from the risk assessment step may be useful inputs to the risk monitoring step. For example, risk assessment threshold conditions (e.g., likelihood of threats exploiting vulnerabilities) could be input to the risk monitoring step. In turn, organizations could monitor to determine if such threshold conditions are met. If threshold conditions are met, such information could be used in the risk assessment step, where it could serve as the basis for an incremental, differential risk assessment or an overall reassessment of risk to the organization.

Activities

RISK MONITORING STRATEGY

TASK 4-1: Develop a risk monitoring strategy for the organization that includes the purpose, type, and frequency of monitoring activities.

[64] Compliance verification ensures that organizations have implemented required risk response measures and that information security requirements derived from and traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, and standards/guidelines are satisfied.

[65] Draft NIST Special Publication 800-137 provides guidance on monitoring organizational information systems and environments of operation.

Supplemental Guidance: Organizations implement risk monitoring programs: (i) to verify that required risk response measures are implemented and that information security requirements derived from and traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, and standards/guidelines, are satisfied (*compliance monitoring*); (ii) to determine the ongoing effectiveness of risk response measures after the measures have been implemented (*effectiveness monitoring*); and (iii) to identify changes to organizational information systems and the environments in which the systems operate that may affect risk (*change monitoring*) including changes in the feasibility of the ongoing implementation of risk response measures). Determining the purpose of risk monitoring programs directly impacts the means used by organizations to conduct the monitoring activities and where monitoring occurs (i.e., at which risk management tiers). Organizations also determine the type of monitoring to be employed, including approaches that rely on automation or approaches that rely on procedural/manual activities with human intervention. Finally, organizations determine how often monitoring activities are conducted, balancing value gained from frequent monitoring with potential for operational disruptions due for example, to interruption of mission/business processes, reduction in operational bandwidth during monitoring, and shift of resources from operations to monitoring. Monitoring strategies developed at Tier 1 influence and provide direction for similar strategies developed at Tier 2 and Tier 3 including the monitoring activities associated with the Risk Management Framework at the information system level.

Monitoring Compliance

Compliance monitoring is employed to ensure that organizations are implementing needed risk response measures. This includes ensuring that the risk response measures selected and implemented by organizations in response to risk determinations produced from risk assessments are implemented correctly and operating as intended. Failure to implement the risk response measures selected by organizations can result in the organizations continuing to be subject to the identified risk. Compliance monitoring also includes ensuring that risk response measures required by federal mandates (e.g., legislation, directives, policies, regulations, standards) or organizational mandates (e.g., local policies, procedures, mission/business requirements) are implemented. Compliance monitoring is the easiest type of monitoring to perform because there are typically a finite set of risk response measures employed by organizations usually in the form of security controls. Such measures are typically well-defined and articulated as an output from the risk response step. The more challenging part of compliance monitoring is evaluating whether the risk response measures are implemented correctly (and in some instances continuously). Compliance monitoring also includes, as feasible, analysis as to why compliance failed. The reason for compliance failure can range from individuals failing to do their jobs correctly to the risk response measure not functioning as intended. If monitoring indicates a failure in compliance, then the response step of the risk management process is revisited. A key element of the feedback to the response step is the finding from compliance monitoring indicating the reason for the compliance failure. In some instances, compliance failures can be fixed by simply re-implementing the same risk response measures with little or no change. But in other instances, compliance failures are more complicated (e.g., the selected risk response measures are too difficult to implement or the measures did not function as expected). In such instances, it may be necessary for organizations to return to the evaluation and decision portions of the risk response step to develop different risk response measures.

Monitoring Effectiveness

Effectiveness monitoring is employed by organizations to determine if implemented risk response measures have actually been effective in reducing identified risk to the desired level. Although effectiveness monitoring is different than compliance monitoring, failure to achieve desired levels of effectiveness may be an indication that risk response measures have been implemented incorrectly or are not operating as intended. Determining the effectiveness of risk response measures is generally more challenging than determining whether the measures have been implemented correctly and are operating as intended (i.e., meeting identified compliance requirements). Risk response measures implemented correctly and operating as intended do not guarantee an effective reduction of risk. This is primarily due to: (i) the complexity of operating environments which may generate unintended consequences; (ii) subsequent changes in levels of risk or associated risk factors (e.g., threats, vulnerabilities, impact, or likelihood); (iii) inappropriate or incomplete criteria established as an output of the risk response step; and (iv) changes in information systems and environments of operation after implementation of risk response measures. This is especially true when organizations try to determine if more strategic outcomes have been achieved and for more dynamic operating environments. For example, if the desired outcome for organizations is to be less susceptible to advanced persistent threats, this may be challenging to measure since these types of threats are, by definition, very difficult to detect. Even when organizations are able to establish effectiveness criteria, it is often difficult to obtain criteria that are quantifiable. Therefore, it may become a matter of subjective judgment as to whether the implemented risk response measures are ultimately effective. Moreover, even if quantifiable effectiveness criteria are provided, it may be difficult to determine if the information provided satisfies the criteria. If organizations determine that risk response measures are not effective, then it may be necessary to return to the risk response step. Generally, for effectiveness failures, organizations cannot simply return to the implementation portion of the risk response step. Therefore, depending on the reason for the lack of effectiveness, organizations revisit all portions of the risk response step (i.e., development, evaluation, decision, and implementation) and potentially the risk assessment step. These activities may result in organizations developing and implementing entirely new risk responses.

Monitoring Changes

In addition to compliance monitoring and effectiveness monitoring, organizations monitor changes to organizational information systems and the environments in which those systems operate. Monitoring changes to information systems and environments of operation is not linked directly to previous risk response measures but it is nonetheless important to detect changes that may affect the risk to organizational operations and assets, individuals, other organizations, and the Nation. Generally, such monitoring detects changes in conditions that may undermine risk assumptions (articulated in the risk framing step).

- *Information System:* Changes can occur in organizational information systems (including hardware, software, and firmware) that can introduce new risk or change existing risk. For example, updates to operating system software can eliminate security capabilities that existed in earlier versions, thus introducing new vulnerabilities into organizational information systems. Another example is the discovery of new system vulnerabilities that fall outside of the scope of the tools and processes available to address such vulnerabilities (e.g., vulnerabilities for which there are no established mitigations).
- *Environments of Operation:* The environments in which information systems operate can also change in ways that introduce new risk or change existing risk. Environmental and operational considerations include, but are not limited to, missions/business functions, threats, vulnerabilities, mission/business processes, facilities, policies, legislation, and technologies. For example, new legislation or regulations could be passed that impose additional requirements on organizations. This change might affect the risk assumptions established by organizations. Another example is a change in the threat environment that reports new tactics, techniques, procedures, or increases in the technical capabilities of adversaries. Organizations might experience reductions in available resources (e.g., personnel or funding), which in turn results in changing priorities. Organizations might also experience changes in the ownership of third-party suppliers which could affect supply chain risk. Mission changes may require that organizations revisit underlying risk assumptions. For example, an organization whose mission is to collect threat information on possible domestic terrorist attacks and share such information with appropriate federal law enforcement and intelligence agencies may have its scope changed so that the organization is responsible for also sharing some of the information with local first responders. Such a change could affect assumptions regarding the security resources such users may have at their disposal. Changes in technology may also affect the underlying risk assumptions established by organizations. Unlike other types of change, technology changes may be totally independent of organizations, but still affect the risk organizations must address. For example, improvements in computing power may undermine assumptions regarding what constitutes sufficiently strong means of authentication (e.g., number of authentication factors) or cryptographic mechanism.

Automated Versus Manual Monitoring

Broadly speaking, organizations can conduct monitoring either by automated or manual methods. Where automated monitoring is feasible, it should be employed because it is generally faster, more efficient, and more cost-effective than manual monitoring. Automated monitoring is also less prone to human error. However, not all monitoring can take advantage of automation. Monitoring conducted at Tier 3 generally lends itself to automation where activities being monitored are information technology-based. Such activities can usually be detected, tracked, and monitored through the installation of appropriate software, hardware and/or firmware. To ensure that automated processes, procedures, and/or mechanisms supporting monitoring activities are providing the information needed, such processes, procedures, and mechanisms should be appropriately validated, updated and monitored. Compliance monitoring can be supported by automation when the risk mitigation measures being validated are information technology-based (e.g., installation of firewalls or testing of configuration settings on desktop computers). Such automated validation can often check whether risk mitigation measures are installed and whether the installations are correct. Similarly, effectiveness monitoring may also be supported by automation. If the threshold conditions for determining the effectiveness of risk response measures are predetermined, then automation can support such effectiveness monitoring. While automation can be a supporting capability for Tiers 1 and 2, generally automation does not provide substantive insight for non-information technology-based activities which are more prevalent at those higher tiers. Activities that are not as likely to benefit from automation include, for example, the use of multiple suppliers within the supply chain, evolving environments of operation, or evaluating the promise of emerging technical capabilities in support of missions/business functions. Where automated monitoring is not available, organizations employ manual monitoring and/or analysis.

Frequency of Monitoring

The frequency of risk monitoring (whether automated or manual) is driven by organizational missions/business functions and the ability of organizations to use the monitoring results to facilitate greater situational awareness. An increased level of situational awareness of the security state of organizational information systems and environments of operation helps organizations develop a better understanding of risk. Monitoring frequency is also driven by other factors, for example: (i) the anticipated frequency of changes in organizational information systems and operating environments; (ii) the potential impact of risk if not properly addressed through appropriate response measures; and (iii) the degree to which the threat space is changing. The frequency of monitoring can also be affected by the type of monitoring conducted (i.e., automated versus procedural approaches). Depending on the frequency of monitoring

required by organizations, in most situations, monitoring is most efficient and cost-effective when automation is employed. Monitoring can provide significant benefits, especially in situations where such monitoring limits the opportunities for adversaries to gain a foothold within organizations (either through information systems or the environments in which those systems operate). When manual monitoring is employed by organizations, it is generally not efficient to perform the monitoring with the frequency that automation allows. In some instances, infrequent monitoring is not a major issue. For example, missions/business functions, facilities, legislation, policies, and technologies tend to change on a more gradual basis and as such, do not lend themselves to frequent monitoring. Instead, these types of changes are better suited to condition/event-based monitoring (e.g., if missions and/or business functions change, then monitoring of such changes is appropriate to determine if the changes have any impact on risk).

RISK MONITORING

TASK 4-2: Monitor organizational information systems and environments of operation on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes.

Supplemental Guidance: Once organizations complete the development of their monitoring strategies, the strategies are implemented organization-wide. Because there are so many diverse aspects of monitoring, not all aspects of monitoring may be performed, or they may be performed at different times. The particular aspects of monitoring that are performed are dictated largely by the assumptions, constraints, risk tolerance, and priorities/trade-offs established by organizations during the risk framing step. For example, while organizations might desire to conduct all forms of monitoring (i.e., compliance, effectiveness, and change), the constraints imposed upon the organizations may allow only compliance monitoring that can be readily automated at Tier 3. If multiple aspects of monitoring can be supported, the output from the risk framing step helps organizations to determine the degree of emphasis and level of effort to place on the various monitoring activities.

As noted above, not all monitoring activities are conducted at the same tiers, for the same purpose, at the same time, or using the same techniques. However, it is important that organizations attempt to coordinate the various monitoring activities. Coordination of monitoring activities facilitates the sharing of risk-related information that may be useful for organizations in providing early warning, developing trend information, or allocating risk response measures in a timely and efficient manner. If monitoring is not coordinated, then the benefit of monitoring may be reduced, and could undermine the overall effort to identify and address risk. As feasible, organizations implement the various monitoring activities in a manner that maximizes the overall goal of monitoring, looking beyond the limited goals of particular monitoring activities. Risk monitoring results are applied in performing incremental risk assessments to maintain awareness of the risk being incurred, to highlight changes in risk, and to indicate the need to revisit other steps in the risk management process, as appropriate.

Outputs and Post Conditions

The output from the risk monitoring step is the information generated by: (i) verifying that required risk response measures are implemented and that information security requirements derived from and traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, and standards/guidelines, are satisfied; (ii) determining the ongoing effectiveness of risk response measures; and (iii) identifying changes to organizational information systems and environments of operation. Outputs from the risk monitoring step can be useful inputs to the risk framing, risk assessment, and risk response steps. For example, compliance monitoring results may require that organizations revisit the implementation portion of the risk response step, while effectiveness monitoring results may require that organizations revisit the entire risk response step. The results of monitoring for changes to information systems and environments of operation may require organizations to revisit the risk assessment step. The results of the risk monitoring step can also serve the risk framing step (e.g., when organizations discover new threats or vulnerabilities that affect changes in organizational risk assumptions, risk tolerance, and/or priorities/trade-offs).