
monitor
customer
research
organization
performance
complex
probability
assessment
data
retention
identification
management
process
risk
plan
analysis
planning
monitor
risk
performance
retention
impact
organization
management
retention
performance
opportunity
assessment
cost
treatment
project
plan
strategy
research
resources
important
organization
sales

STEP 7: MONITOR

The purpose of the Monitor step is to maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions.

TABLE 8: MONITOR TASKS AND OUTCOMES

Tasks	Outcomes
TASK M-1 SYSTEM AND ENVIRONMENT CHANGES	• The information system and environment of operation are monitored in accordance with the continuous monitoring strategy. [*Cybersecurity Framework*: **DE.CM**; **ID.GV**]
TASK M-2 ONGOING ASSESSMENTS	• Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy. [*Cybersecurity Framework*: **ID.SC-4**]
TASK M-3 ONGOING RISK RESPONSE	• The output of continuous monitoring activities is analyzed and responded to appropriately. [*Cybersecurity Framework*: **RS.AN**]
TASK M-4 AUTHORIZATION PACKAGE UPDATES	• Risk management documents are updated based on continuous monitoring activities. [*Cybersecurity Framework*: **RS.IM**]
TASK M-5 SECURITY AND PRIVACY REPORTING	• A process is in place to report the security and privacy posture to the authorizing official and other senior leaders and executives.
TASK M-6 ONGOING AUTHORIZATION	• Authorizing officials conduct ongoing authorizations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions.
TASK M-7 SYSTEM DISPOSAL	• A system disposal strategy is developed and implemented, as needed.

TASK M-1

TASK M-1 SYSTEM AND ENVIRONMENT CHANGES	• The information system and environment of operation are monitored in accordance with the continuous monitoring strategy. [*Cybersecurity Framework*: **DE.CM**; **ID.GV**]

Examples of changes include:

- Upgrades/updates to hardware/software
- Personnel changes
- Changes to physical access
- Location change
- Changes made by external providers (harder to detect)

TASK M-1

If an unauthorized change is detected, the organization can respond accordingly (M-3).

TASK M-1

- Adversarial attack – invoke incident response plan
- Failure of staff – remedial training might be needed

TASK M-2

TASK M-2 ONGOING ASSESSMENTS	• Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy. [*Cybersecurity Framework*: **ID.SC-4**]

Ongoing assessment of the control effectiveness is part of the continuous monitoring activities of the organization.

TASK M-3

TASK M-3 ONGOING RISK RESPONSE	• The output of continuous monitoring activities is analyzed and responded to appropriately. [*Cybersecurity Framework*: **RS.AN**]

Based on the new assessment findings, the authorizing official will decide on the best risk response or may even approve a response provided by the system owner.

TASK M-3

The mitigation response is then implemented by the system owner or control provider however if the risk is accepted, it is documented and will continue to be monitored for any new changes.

TASK M-4

TASK M-4 AUTHORIZATION PACKAGE UPDATES	• Risk management documents are updated based on continuous monitoring activities. [*Cybersecurity Framework*: **RS.IM**]

Updates to the plans of action reflect modifications to controls based on risk mitigation activities carried out by system owners or common control providers. Updates to control assessment reports reflect additional assessment activities carried out to determine control effectiveness based on implementation details in the plans.

TASK M-5

TASK M-5 SECURITY AND PRIVACY REPORTING	• A process is in place to report the security and privacy posture to the authorizing official and other senior leaders and executives.

The results of monitoring activities are documented and reported to the authorizing official and other selected organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy

TASK M-5

Security and privacy posture reports describe the ongoing monitoring activities employed by system owners or common control providers.

TASK M-5

At a minimum, security and privacy posture reports summarize changes to the security and privacy plans, security and privacy assessment reports, and plans of action and milestones that have occurred since the last report.

TASK M-5

The frequency of security and privacy posture reports is at the discretion of the organization and in compliance with federal and organizational policies.

TASK M-6

TASK M-6 ONGOING AUTHORIZATION	• Authorizing officials conduct ongoing authorizations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions.

The findings or results from the continuous monitoring process provides useful information to authorizing officials to support near-real time risk-based decision making.


Identify Change
Evaluate Change Request
Implementation Decision
Implement approved change request
Continuous Monitoring

TASK M-7

TASK M-7 SYSTEM DISPOSAL	• A system disposal strategy is developed and implemented, as needed.

When a system is removed from operation, several risk management actions are required.

- Media sanitization
- Configuration management and control
- Record retention

TASK M-7

Organizational tracking and management systems (including inventory systems) are updated to indicate the system that is being removed from service

TASK M-7

Where applicable, the disposal must comply with federal regulations, standards or policies.