
ASSESSMENT
IMPROVEMENT
QUALITY
COMPLIANCE
RATING
FEEDBACK
CONTROL
RESULT
SURVEY
CRITERIA
PROGRESS
SCORE
NALYSIS
RESEARCH
REVIEW
EVALUATION
MANAGEMENT
EXCELLENT
MEASURE
SUCCESS
TIME
DEVELOPMENT
GOAL
AUDIT
PLAN
FAIL

LAB CYBER

STEP 5: ASSESS CONTROLS

The purpose of the Assess step is to determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.

STEP 5: ASSESS CONTROLS

Are the controls:

- Implemented correctly?
- Operating as intended?
- Producing the desired outcome?

TABLE 6: ASSESS TASKS AND OUTCOMES

Tasks	Outcomes
TASK A-1 ASSESSOR SELECTION	• An assessor or assessment team is selected to conduct the control assessments. • The appropriate level of independence is achieved for the assessor or assessment team selected.
TASK A-2 ASSESSMENT PLAN	• Documentation needed to conduct the assessments is provided to the assessor or assessment team. • Security and privacy assessment plans are developed and documented. • Security and privacy assessment plans are reviewed and approved to establish the expectations for the control assessments and the level of effort required.
TASK A-3 CONTROL ASSESSMENTS	• Control assessments are conducted in accordance with the security and privacy assessment plans. • Opportunities to reuse assessment results from previous assessments to make the risk management process timely and cost-effective are considered. • Use of automation to conduct control assessments is maximized to increase speed, effectiveness, and efficiency of assessments.
TASK A-4 ASSESSMENT REPORTS	• Security and privacy assessment reports that provide findings and recommendations are completed.
TASK A-5 REMEDIATION ACTIONS	• Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken. • Security and privacy plans are updated to reflect control implementation changes made based on the assessments and subsequent remediation actions. [*Cybersecurity Framework*: **Profile**]
TASK A-6 PLAN OF ACTION AND MILESTONES	• A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed. [*Cybersecurity Framework*: **ID.RA-6**]

TASK A-1

TASK A-1 ASSESSOR SELECTION	• An assessor or assessment team is selected to conduct the control assessments. • The appropriate level of independence is achieved for the assessor or assessment team selected.

It is extremely important that the assessors are independent and can make truthful judgements. They could be in-house or contracted assessors.

TASK A-2

TASK A-2 ASSESSMENT PLAN	• Documentation needed to conduct the assessments is provided to the assessor or assessment team. • Security and privacy assessment plans are developed and documented. • Security and privacy assessment plans are reviewed and approved to establish the expectations for the control assessments and the level of effort required.

- Develop security assessment policy
- Prioritize and schedule assessment
- Select and customize testing techniques
- Develop the assessment plan
- Address legal considerations

TASK A-3

TASK A-3 CONTROL ASSESSMENTS	• Control assessments are conducted in accordance with the security and privacy assessment plans. • Opportunities to reuse assessment results from previous assessments to make the risk management process timely and cost-effective are considered. • Use of automation to conduct control assessments is maximized to increase speed, effectiveness, and efficiency of assessments.

- Observe
- Interview
- Test

TASK A-3 (Observe)

Screen lock was set to 2 minutes of inactivity

TASK A-3 (Interview)

Are you aware of our security policies and what the best practices for using removable media are?

TASK A-3 (Test)

Usually technical and involves activities like penetration testing and logging.

NIST 800-53 CONTROLS

Access Control & Identification & Authentication :

Ensures the system is using proper key management techniques, tokens, correct and verified authentication methods, passwords are managed etc

NIST 800-53 CONTROLS

Auditing, Accountability and System Communications Protection :

Ensures the system is

- Being audited and monitored to identify security incidents
- Secured so that access is based on a need-to-know basis and least privilege
- Appropriately managing privileged accounts
- Using malware protection
- Implementing an effective network device control program e.g router, firewalls

NIST 800-53 CONTROLS

Physical & Environmental (PE) Controls:

Ensures the system is protected against fire, humidity and physical intrusions using guards, detectors, safes, alarms etc.

TASK A-4

TASK A-4 ASSESSMENT REPORTS	• Security and privacy assessment reports that provide findings and recommendations are completed.

Document everything that isn't optimal and those can serve as recommendations for improvement.

TASK A-5 & A-6

TASK A-5 REMEDIATION ACTIONS	• Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken. • Security and privacy plans are updated to reflect control implementation changes made based on the assessments and subsequent remediation actions. [*Cybersecurity Framework*: **Profile**]
TASK A-6 PLAN OF ACTION AND MILESTONES	• A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed. [*Cybersecurity Framework*: **ID.RA-6**]