

Jennifer Thibodeau
[REDACTED]

Nov 13, 2025, 1:00:19 PM
to 800-171comments@list.nist.gov

To Whom It May Concern:

Please find Wiz's feedback for SP 800-172 and SP 800-172A attached.

Thank you. Happy to answer or further discuss any questions you may have.

Jennifer Thibodeau

--

Jennifer Thibodeau
Director of Government Affairs
[REDACTED]

Mobile: [REDACTED]

Wiz Feedback: SP 800-172A Rev. 3 Assessing Enhanced Security Requirements for Controlled Unclassified Information

Providing standardized assessment procedures is critical for ensuring that the enhanced requirements are implemented consistently and effectively. The decision to align the structure with NIST SP 800-53A is a welcome one, as it provides a familiar format for assessors and organizations already working within the NIST Risk Management Framework. The clear breakdown of each procedure into an assessment objective, determination statements, and potential methods and objects is excellent.

The primary challenge with this document is its application to the dynamic, ephemeral, and interconnected nature of the cloud. The assessment methods of "Examine, Interview, Test" are timeless, but the "Objects" they act upon have fundamentally changed. The procedures often imply a manual, document-centric review process. **In a cloud environment with thousands of resources and constant change, this is not scalable or effective.**

Our core recommendation is to emphasize automated evidence collection through direct analysis of cloud and hybrid environments. Modern Cloud Native Application Protection Platforms (CNAPPs) can programmatically and continuously perform the "Examine" and "Test" functions, providing assessors with real-time, data-backed evidence rather than static documentation. The guidance should encourage this modern approach to assessment.

Section 2: The Fundamentals

For 2.1 Assessment Procedures, the description of Assessment Objects—specifications, mechanisms, activities, and individuals—does not translate well to cloud environments. **We recommend adding a fifth category or expanding the definitions to include "Live Environmental Configuration Data."** In the cloud, the actual configuration of a resource is the ultimate source of truth, not a design document that may be months out of date. This can be

done in near-real time leveraging APIs or lightweight agents with little to no impact on system compute.

The Examine method is defined as "reviewing, studying, inspecting, or analyzing assessment objects". **The discussion should clarify that for cloud environments, this "examination" should be achieved by programmatically querying the cloud control plane.** This shifts the focus from reviewing a static document to analyzing live, verifiable data about the system's security posture.

Section 3: The Procedures

For 03.04.03E (Automated Maintenance of System Component Inventory): The "Potential Assessment Objects" section includes examining a system component inventory document.

Recommendation: **The most effective assessment object for cloud and hybrid environments is not a document, but direct access to a Cloud Native Application Protection Platform (CNAPP) or successive technology.** An assessor should be able to query this platform to get a real-time, comprehensive inventory of all cloud resources (VMs, containers, serverless functions, storage buckets, IAM roles, etc.). The "Test" method should involve the assessor asking the organization to provide access to or a feed from their CNAPP environment. This provides far greater assurance than a static list.

3.11 Risk Assessment (RA)

For 03.11.10E (Criticality Analysis): The assessment objective is to determine if a criticality analysis has been performed. The assessment objects include the criticality analysis itself and analysis reports.

Recommendation: The assessment procedure should guide the assessor to look for evidence of attack path analysis. The most powerful evidence of an effective criticality analysis is a live demonstration showing how the organization identifies critical assets and their methodology to assess the risk to these assets. **An assessor should be able to see a visual graph that shows a vulnerable, internet-exposed virtual machine and the toxic combination of permissions and network paths that allow it to access a critical CUI data store. This validates that the organization's criticality analysis is dynamic, context-aware, and based on effective risk, not just a predefined label.**

3.17 Supply Chain Risk Management (SR)

For 03.17.05E (Supply Chain Integrity – Pedigree): The assessment objects include SBOMs and software identification tags.

Recommendation: Simply examining an SBOM is insufficient. The Test method should be to verify the organization's capability to rapidly produce and operationalize this data. The assessor

should ask: "A new critical vulnerability (a new "Log4j") was just announced in this open-source package. How do you assess your risk?" A successful test would be the organization using its tooling to immediately identify every single running cloud resource that uses the vulnerable package and prioritizing remediation based on which of those resources are exposed or have sensitive access. This is the true assessment of supply chain resiliency.

Appendix D: Security Requirement Assessments

In section D.1 Preparing for Assessments, the list of preparatory activities includes providing artifacts like policies, plans, and system documentation to assessors.

Recommendation: **We suggest adding an item specifically for cloud environments: Providing assessors with read-only access to the organization's centralized cloud security platform (e.g., a CNAPP). This allows for direct, efficient, and comprehensive evidence gathering and validation of controls against the live environment.** This single step can drastically improve the accuracy and efficiency of an assessment compared to a manual review of potentially outdated documents.

As always, we at Wiz appreciate the opportunity to provide feedback and commend NIST for its thorough and forward-looking work on this crucial guidance.