Vulnerability Assessment Checklist

For cloud and hybrid environments

Scope. Validate coverage. Prioritize. Remediate. Verify.

A working record for security engineers, cloud and platform teams.

01 SCOPE 02 RUN CHECKS 03 PRIORITIZE 04 REMEDIATE 05 VERIFY

Turn each check into a reviewable decision

Define the assessment scope and reporting cutoff, then link each answer to the underlying inventory, scan results, or remediation records.

ASSESSMENT CONTEXT

Assessment name / ID: _____

Review period: _____ Reporting cutoff & timezone: _____

Inventory snapshot: _____

Assessment owner: _____ Reviewer: _____

Evidence repository: _____

SLA policy & version: _____ Exclusions register: _____

RESULT ≠ COMPLETION

Mark Performed Y/N and then record the result. An approved exception does not turn a failed criterion into Pass. A Pass confirms this checklist criterion; it does not mean the environment has no vulnerabilities.

PASS	Criterion met across assessed scope, with supporting evidence.
GAP	Missing requirement, failed result, or unsupported closure.
NOT ASSESSED	Check not completed or evidence insufficient.
N/A	No relevant target or case; record reason and reviewer approval.

For every Gap or Not assessed result, link the action owner and due date in the follow-up register.

Define the rules before checking

Set the required assessment method and freshness rule for each asset group. A material deployment or configuration change may invalidate earlier evidence.

ASSET GROUP & SCOPE	REQUIRED CHECK & SOURCE	FRESHNESS & CHANGE RULE
_____	_____	_____
_____	_____	_____
_____	_____	_____

KEEP TWO BOUNDARIES DISTINCT

An approved scope exclusion is disclosed outside the denominator. An in-scope asset with an accepted scanning gap stays in the denominator and remains uncovered.

Use a snapshot at the reporting cutoff for live-asset coverage. Assess short-lived workloads across the review period under check 04, without mixing terminated assets into a live snapshot.

A COMPLETED CHECK CAN STILL REPORT A GAP

120 production VMs in scope. 103 have all required checks current and successful; 4 have no result, 3 are stale, and 10 have partial checks. Asset coverage = 103 / 120 = 85.8%.

Check 03 • Performed Y • Result GAP • Evidence INV-01 / COV-01 / GAP-01 • Owner Platform Engineering

Group result: use Gap if any applicable target fails. Use N/A only when the entire check is inapplicable.

Make the scope measurable

Preserve the inventory and the evidence used to decide what was assessed.

01 Approve the boundaries and testing conditions

PASS WHEN

Every in-scope account, subscription, project, environment, and Region has a responsible owner. Authorized assessment methods, scan windows, a stop contact, and approved scope exclusions are recorded before testing.

EVIDENCE

Approved assessment plan, scope IDs, exclusion decisions, and named owners. [1]

IF THERE IS A GAP

Resolve unclear ownership or authorization. Keep unresolved boundaries visible; do not silently drop them from scope.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

02 Reconcile and preserve the asset inventory

PASS WHEN

A current inventory covers every scoped boundary, reconciles with the account or subscription roster, and is preserved as a dated snapshot with stable resource IDs. Empty responses and failed reads have been investigated.

EVIDENCE

Provider inventory export, collection timestamp, permissions or collection errors, and reconciliation record.

IF THERE IS A GAP

Restore collection access or use an approved alternative source. Report the unverified scope as an inventory limitation.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

03 Check every required asset and scan type

PASS WHEN

Inventory and coverage records are matched by stable asset ID and required check type. Every required pair has successful evidence meeting the agreed freshness rule. Missing, stale, failed, and partial results remain visible.

EVIDENCE

Inventory snapshot, coverage export, required-check matrix, and the list of gaps. AWS Inspector exposes separate coverage details for Lambda standard and code scanning. [2]

IF THERE IS A GAP

Record the affected IDs, missing check, owner, and due date. An accepted scanning exception remains uncovered while the asset stays in scope.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

Inventory into testing

Tie inventory decisions to the methods that will test each target.

04 Include workloads that disappeared during the period

PASS WHEN

Launch, deployment, and termination history is reconciled with the review window. The identity and relevant check evidence are preserved for short-lived instances, container digests, and deployed function versions that were in scope.

EVIDENCE

Lifecycle or deployment export linked to resource IDs, image digests or function versions, and timestamps.

IF THERE IS A GAP

Record workloads whose activity or scan history cannot be reconstructed. Assign a fix for evidence collection in the next cycle.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

05 Confirm the business context with the service owner

PASS WHEN

Each asset or documented asset group has an owner, service, environment, criticality, and relevant data classification. Verify exposure through the network or application path, including public load balancers and gateways.

EVIDENCE

CMDB or inventory fields, owner confirmation, and network or application configuration supporting the exposure decision.

IF THERE IS A GAP

Flag unknown fields for triage and assign an owner to resolve them. Do not infer low risk from missing context.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

06 Match the assessment method to the target

PASS WHEN

The required-check matrix names the method and target for each asset group: host, network, web or API, image, cloud configuration, or IaC. Network tests have the intended source vantage; application tests have the intended role and routes.

EVIDENCE

Scan policy or configuration ID, target set, scanner location, enabled check families, and tool or feed version where available.

IF THERE IS A GAP

Correct the policy or add a complementary method. Record unsupported asset types and the alternative assessment needed.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

Verify what ran

Confirm access, deployed versions, and change-triggered coverage.

07 Verify access and the checks that actually ran

PASS WHEN

Every target requiring authentication has confirmed access and successful completion of the intended local or protected checks. API and agent methods show successful collection with the required permissions. A successful login alone is insufficient.

EVIDENCE

Per-target authentication and collection output. In Nessus, review plugin 19506 and relevant privilege or collection errors. [3]

IF THERE IS A GAP

Correct credentials, permissions, agent health, or session handling and rerun. Preserve the partial result as a coverage gap.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

08 Assess managed services and the deployed configuration

PASS WHEN

Required checks cover applicable databases, storage, serverless deployments, image dependencies, and live cloud settings. Link IaC findings to the commit and compare relevant deployed settings. Confirm the scanner supports the actual version or artifact serving traffic.

EVIDENCE

Service configuration export, deployed version or digest, IaC commit, and matching result IDs. Inspector Lambda eligibility is limited to $LATEST. [4]

IF THERE IS A GAP

Add the missing check or approved alternative. A result for another version does not establish coverage for the deployed target.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

09 Check scheduled and deployment triggered coverage

PASS WHEN

A scheduled cadence exists for each required check, with relevant deployment or configuration changes triggering reassessment. Confirm a recent applicable change produced a successful result for the affected target within the agreed interval.

EVIDENCE

Schedule, change or deployment ID, trigger log, result timestamp, and artifact or resource ID.

IF THERE IS A GAP

Repair the trigger and run the missing check. Mark previous evidence stale when the change invalidated what it tested.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

From results to risk

Resolve partial scans, then establish real exposure and threat evidence.

10 Resolve incomplete scans and validate disputed findings

PASS WHEN

Required runs have completed successfully for their targets. No unresolved skipped, failed, partial, or stale result is counted as covered. False-positive decisions have evidence for the exact affected component and version.

EVIDENCE

Job and target logs, retry results, package versions, vendor advisory, and documented finding disposition.

IF THERE IS A GAP

Assign and rerun failed checks. Keep unsupported dismissals open for validation; do not treat an older version string alone as proof of vulnerability or remediation.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

11 Establish whether the vulnerable feature is reachable

PASS WHEN

The affected feature and version, who or what can reach it, and the relevant network, identity, or application controls are recorded. Configuration evidence and authorized validation support the access path.

EVIDENCE

Source and destination, relevant access rules, authentication requirements, validation date, and finding ID.

IF THERE IS A GAP

Record reachability as unknown and assign investigation. A private address alone does not establish isolation.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

12 Add dated vulnerability and exploitation evidence

PASS WHEN

CVE findings include applicable CVSS data, dated EPSS probability when available, and the KEV lookup result. Unavailable scores are distinct from zero. Findings without a CVE retain their own technical evidence.

EVIDENCE

CVE or rule ID, score source and version, lookup date, and vendor or scanner evidence. EPSS is a threat input, not a complete risk score. [5, 6]

IF THERE IS A GAP

Refresh missing or stale inputs. Document unavailable data without treating it as evidence of low risk.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

Prioritize with context

Preserve the impact, component, and due-date rationale.

13 Trace the potential business impact

PASS WHEN

The triage record explains what exploitation could affect: service availability, sensitive data, privileged identities, or dependent systems. Record compensating controls and the evidence that they currently operate.

EVIDENCE

Service criticality, data classification, dependency or permission path, and control validation date.

IF THERE IS A GAP

Ask the service owner to confirm impact and dependencies. Retain the uncertainty in the priority rationale until resolved.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

14 Group duplicates without losing separate fixes

PASS WHEN

Observations of the same issue link to a canonical asset and vulnerability or rule ID. Source evidence and affected package, path, port, image, or version remain distinct when they require different remediation or retesting.

EVIDENCE

Canonical finding record, source finding IDs, affected component list, and linked remediation units.

IF THERE IS A GAP

Correct asset matching or split distinct affected components. Closing one component must not close other unresolved instances.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

15 Set a defensible priority and remediation deadline

PASS WHEN

Each finding has a priority, rationale, and due date under the agreed SLA policy. Record the clock start rule and any authorized pause rules. Specify what change in exposure, threat evidence, or controls would trigger reprioritization.

EVIDENCE

Triage decision, policy version, detection and SLA-start timestamps, original due date, and reviewer.

IF THERE IS A GAP

Assign unresolved decisions to the risk or service owner. Escalate urgent applicable threats under the agreed policy without waiting for every score.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

Assign and remediate

Make ownership and rollout scope actionable.

16 Assign actionable work to the remediation owner

PASS WHEN

Every finding requiring treatment links to a ticket in the responsible team's workflow. The ticket names an assignee who can coordinate the fix, affected IDs and components, priority, due date, and evidence required for closure.

EVIDENCE

Ticket ID, named assignee, affected finding links, and acceptance criteria.

IF THERE IS A GAP

Route unassigned work to the service owner and record an assignment deadline. Retain the original SLA start.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

17 Make aging and overdue work visible

PASS WHEN

Open findings display age and due date. An escalation route exists and is tested or evidenced by actual alerts. Reassignments and replacement tickets retain the original finding history and SLA clock.

EVIDENCE

Aging report, original deadline, handoff history, and escalation configuration or alert record.

IF THERE IS A GAP

Restore missing dates or links, notify the accountable lead, and record the next action on overdue work.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

18 Prepare a change that covers the affected scope

PASS WHEN

The approved change identifies the fixed version or configuration, all affected targets, deployment sequence, health checks, and rollback plan. Schedule the window against the remediation deadline.

EVIDENCE

Change ID, target list, planned artifact or configuration, window, and rollback criteria.

IF THERE IS A GAP

Resolve missing targets or deployment prerequisites. If the window exceeds the deadline, request an exception before it expires.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

Treat then verify

Keep exceptions distinct from fixes and retest the original finding.

19 Track deployment through completion

PASS WHEN

Deployment records show which affected targets received the change and which failed, were skipped, or await action. Link the deployed artifact or configuration to the original findings; successful deployment still requires verification.

EVIDENCE

Rollout log, applied version or digest, target outcomes, and change-to-ticket links.

IF THERE IS A GAP

Keep unresolved targets open and assign follow-up work. Do not close a group because the first target was patched.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

20 Control exceptions and temporary mitigations

PASS WHEN

Each exception names exact findings and assets, rationale, validated temporary controls, an authorized approver, remediation owner, review date, and expiry. Accepted risk and mitigation remain distinct from a verified fix.

EVIDENCE

Approval record, control evidence, exception ID, expiry, and linked treatment plan.

IF THERE IS A GAP

Escalate expired or unapproved exceptions. Return affected findings to the active queue; accepted scanning gaps remain visible in coverage.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

21 Retest every finding proposed for fixed closure

PASS WHEN

A successful retest after the change checks the original vulnerability on the relevant asset or deployed artifact and confirms it is resolved. Authentication, target identity, and check coverage are sufficient to support that conclusion.

EVIDENCE

Original finding, change ID, before-and-after result IDs, target or digest, and verification timestamp.

IF THERE IS A GAP

Keep or reopen the finding. A scan that lost access, skipped the check, or tested another target cannot verify a fix.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

Prove closure

Confirm the running fleet and preserve traceable evidence.

22 Verify the fixed version reached the running fleet

PASS WHEN

The affected deployment scope is reconciled with running instances, tasks, or replicas. Every affected target has the verified version or configuration, or remains explicitly open. Where relevant, running image digests match the tested digest.

EVIDENCE

Dated runtime inventory, instance or task IDs, running versions or digests, and matching verification results.

IF THERE IS A GAP

Identify remaining old versions, failed rollout targets, or replacements lacking evidence. Track these until verified.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

23 Classify closure and detect regressions

PASS WHEN

Closure records distinguish verified fix, retirement, approved scope removal, false positive, mitigation, and accepted risk. Loss of coverage remains unresolved. Redeployment or rollback checks can reopen or link a recurring finding to its history.

EVIDENCE

Closure reason and evidence, scope or retirement decision where applicable, and regression handling rule.

IF THERE IS A GAP

Correct unsupported closure records and investigate unexplained disappearances. Reopen affected work when the vulnerable state returns.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

24 Make the evidence and metrics reproducible

PASS WHEN

A reviewer can follow a finding from asset identity through triage, treatment, and verification. Calculate coverage, SLA attainment, and remediation time using the definitions below; retain the underlying records and cutoff date.

EVIDENCE

Evidence index, source exports, calculation inputs, reporting cutoff, and open-gap register.

IF THERE IS A GAP

Repair broken evidence links and recalculate inconsistent measures. Label unavailable metrics and the reason; do not substitute checklist completion.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

Close the assessment

The report records what was checked and what remains open.

25 Sign off the assessment with remaining work assigned

PASS WHEN

The reviewer records the assessment outcome, limitations, uncovered scope, overdue findings, and active exceptions. Every unresolved item has an action owner and due or review date. Schedule the next assessment and relevant change-triggered checks.

EVIDENCE

Reviewer and date, approved report, action register, exception register, and next review date.

IF THERE IS A GAP

Return unowned gaps or unsupported conclusions for resolution. Assessment sign-off does not close open findings.

Performed Y / N Result _____ Evidence ref _____ Checked by / date _____

ASSESSMENT RECORD

In-scope assets: _____ Fully covered: _____ Asset coverage: _____%

Required asset–check pairs: _____ Covered pairs: _____ Check coverage: _____%

Unassessed scope / limitations:
_____

Open overdue findings: _____ Active exceptions: _____ Expired: _____

Action register: _____ Next assessment date: _____

Outcome: Complete / Complete with recorded gaps / Incomplete

Reviewer and date: _____ Risk acceptance references:
_____

Sign-off records the assessment outcome. Open findings, coverage gaps, and exceptions retain their own status and review dates.

Calculate and review the outcome

Use the same cutoff, asset identity, and freshness policy across periods. Disclose changes to scope or calculation rules beside the trend.

COVERAGE

Asset coverage

Assets with every required check current and successful / all in-scope assets at the cutoff × 100. Report by asset class. Accepted scanning gaps remain in the denominator.

Check coverage

Current successful required asset–check pairs / all required asset–check pairs in scope × 100. A pair is one asset and one required check type. Multiple historical runs do not add pairs.

REMEDIATION

Original-deadline attainment

Findings due during the period that reached verified fix by the original due date / all findings due in that period × 100. Include open and late findings; show exceptions separately.

Mean time to remediate

Average elapsed time from initial detection to verified fix for findings verified fixed in the period, grouped by priority. Show the count and the age of still-open findings alongside it.

Report N/A when a denominator is zero. Exclude retirement, accepted risk, false positives, and mitigation-only dispositions from the verified-fix calculation.

Keep the next action traceable

For every Gap or Not assessed result, retain the check ID, affected resources, evidence reference, blocker, next action, accountable owner, due date, and exception ID where applicable.

A REVIEWER SHOULD BE ABLE TO FOLLOW

Asset identity → required checks → original finding → priority decision → remediation ticket → dated verification result.

Preserve exports and artifact IDs. For compliance reviews, attach the applicable control mapping and additional required evidence. This worksheet alone does not establish PCI DSS or ISO 27001 compliance.

TECHNICAL REFERENCES

1 NIST SP 800-115 — planning and conducting technical assessments
https://csrc.nist.gov/pubs/sp/800/115/final

2 AWS — assessing Amazon Inspector coverage
https://docs.aws.amazon.com/inspector/latest/user/assessing-coverage.html

3 Tenable — Nessus Scan Information plugin 19506
https://www.tenable.com/plugins/nessus/19506

4 AWS — scanning Lambda functions and eligibility
https://docs.aws.amazon.com/inspector/latest/user/scanning-lambda.html

5 FIRST — EPSS frequently asked questions
https://www.first.org/epss/faq

6 CISA — Known Exploited Vulnerabilities Catalog
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

7 Cloudaware — Vulnerability Management documentation
https://docs.cloudaware.com/modules/vulnerability-management/

Documentation checked on 20 November 2026. Follow the current guidance for the tools and targets in your own assessment.

BOOK A FREE 30-MINUTE DEMO

Tell us about your environment and current vulnerability workflow. A Cloudaware expert will show how scanner findings, asset context, ownership, and remediation could work together for your team.