STANDARDS PREPARATION CHECKLIST

Incident Response and Evidence Readiness

Line up the decisions, access, records and recovery arrangements a cybersecurity incident will demand, organized by the CSF 2.0 outcomes in NIST SP 800-61 Revision 3.

Edition 2026-11-03 · Updated November 3, 2026 · miami-computer-forensics.com/guides/incident-response-readiness-checklist/

Baseline: NIST SP 800-61 Rev. 3 and CSF 2.0. Updated November 3, 2026.

Use the questions to prepare the review

These eighteen questions cover the response outcomes that decide the first days of an incident. If an incident is already under way, call the 24/7 hotline at (800) 868-8189 first and return to the checklist afterward. Counsel applies the notification and preservation obligations that fit your organization.

For this incident response preparation, distinguish records you can locate from answers awaiting confirmation. Mark an answer verified once someone has checked the record behind it. Assign an owner to unresolved questions and explain exclusions.

Keep incident evidence, access tokens and personal data out of ordinary email and web forms; we arrange secure transfer on the first call. Identify the record holder and discuss a suitable evidence handoff.

Use these incident response preparation questions to prepare the discussion. Each question cites the NIST section it comes from, so your team can check the source directly.

© 2026 Global Digital Forensics, Inc. All rights reserved.

IR-01

Are incident roles and decision authorities clear?

Identify the incident lead, technical responders, business owner and people authorized to approve disruptive actions. Include outside providers where they have response duties.

Evidence to gather

Role assignments, decision authority, escalation contacts and service arrangements.

If something is missing

Resolve ambiguous approval responsibilities before an incident forces a rushed decision.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, GV.RR-02; PDF page 21.

Answer:

Owner, evidence reference and follow up date:

IR-02

Does the response plan match the business and its dependencies?

Connect response to business continuity and the services needed to keep operating. A generic procedure may omit the cloud provider, outside administrator or operational system the organization relies on.

Evidence to gather

Current response/continuity plans, critical services and dependency records.

If something is missing

Review the plans together and identify assumptions about external support.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, ID.IM-04 and GV.OC-05; PDF page 28. Additional source pointer: GV.OC-05 (PDF page 20).

Answer:

Owner, evidence reference and follow up date:

© 2026 Global Digital Forensics, Inc. All rights reserved.

IR-03

Can a reported event reach someone who can assess it?

Include reports from employees, customers and service providers. Identify how reports are monitored and triaged, including when normal working arrangements are disrupted.

Evidence to gather

Reporting channels, duty arrangements and representative triage records.

If something is missing

Confirm the route using an authorized exercise.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, RS.MA-02; PDF page 35.

Answer:

Owner, evidence reference and follow up date:

IR-04

Are severity and escalation decisions based on impact?

Evaluate affected functions, data, asset criticality and recoverability. Handling incidents strictly in arrival order can direct attention away from a more consequential event.

Evidence to gather

Severity criteria, escalation thresholds and example decisions.

If something is missing

Agree on risk factors and who can raise the incident to a higher response level.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, RS.MA and RS.MA-03/04; PDF page 34.

Answer:

Owner, evidence reference and follow up date:

© 2026 Global Digital Forensics, Inc. All rights reserved.

IR-05

Can responders identify the affected assets and service owners?

Keep current hardware, software, service and data flow records accessible to the response team. Include external hosting and SaaS systems rather than limiting the list to office devices.

Evidence to gather

Inventories, owners, service providers and authorized network/data flow records.

If something is missing

Resolve the most important ownership or visibility gaps before an emergency.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, ID.AM-01/02/03; PDF page 24.

Answer:

Owner, evidence reference and follow up date:

IR-06

Are the right records available when an event is examined?

Identify identity, email, endpoint, network and cloud records actually retained. Access rights, licensing and retention can affect availability. Record which sources each search covered, so a blank result is read against that coverage.

Evidence to gather

Logging coverage, example exports, retention, administrator contacts and known gaps.

If something is missing

Arrange approved access and document where each remaining source is held and how to reach it.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, DE.CM-06 and DE.CM-09; PDF page 32.

Answer:

Owner, evidence reference and follow up date:

© 2026 Global Digital Forensics, Inc. All rights reserved.

IR-07

Can adverse events be analyzed in context?

An alert or anomaly is an observation that needs interpretation. Define how technical evidence, threat information and business context are evaluated before an event is declared an incident.

Evidence to gather

Analysis workflow, available context, escalation criteria and representative case records.

If something is missing

Identify where specialized analysis is needed and how it can be obtained.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, DE.AE-02 and DE.AE; PDF page 33.

Answer:

Owner, evidence reference and follow up date:

IR-08

Are cloud, vendor and insurer response handoffs understood?

Bring relevant third parties into planning and exercises. Confirm contractual contacts, access arrangements and any conditions on engaging outside assistance. Check whether your IT support contract covers forensic collection and analysis or only restoration.

Evidence to gather

Provider agreements, response contacts, handoff responsibilities and relevant policy conditions.

If something is missing

Clarify the missing handoffs with the authorized business and legal contacts.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, GV.SC-05 and GV.SC-08; PDF page 23.

Answer:

Owner, evidence reference and follow up date:

© 2026 Global Digital Forensics, Inc. All rights reserved.

IR-09

Are response actions and decisions recorded as they happen?

Keep an incident chronology that identifies actions, responsible people, timing and known effects. Protect those records from unauthorized alteration or disclosure.

Evidence to gather

Incident log template, record owner, storage/access controls and time basis.

If something is missing

Agree on a recording method that remains usable if normal collaboration tools fail.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, RS.AN-06; PDF page 37.

Answer:

Owner, evidence reference and follow up date:

IR-10

Can incident data be preserved with its origin and integrity?

Plan how relevant data and metadata will be collected and retained. The method and handling record should remain explainable. Sensitive material travels through an agreed transfer process.

Evidence to gather

Preservation procedure, collection authority, source references and handling records.

If something is missing

Discuss the evidence scope and secure transfer with the response lead and counsel where appropriate.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, RS.AN-07; PDF page 37.

Answer:

Owner, evidence reference and follow up date:

© 2026 Global Digital Forensics, Inc. All rights reserved.

IR-11

Is containment authorized and suited to the affected service?

Isolation, account restrictions and service shutdowns can prevent further damage but may also disrupt essential activity. Define decision criteria, authority and the treatment of urgent exceptions.

Evidence to gather

Containment playbooks, approval rights, operational dependencies and temporary measure expiry.

If something is missing

Walk through a representative containment decision with the service owner.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, RS.MI-01; PDF page 40.

Answer:

Owner, evidence reference and follow up date:

IR-12

Does the scope review look beyond the first affected device?

An incident can include persistence, additional accounts and other systems. Define how the team will assess magnitude, distinguish confirmed observations from assumptions and revisit the scope as evidence changes.

Evidence to gather

Scope assessment, examined sources, open questions and hypotheses under review.

If something is missing

Assign the next evidence gathering steps across the affected devices before closure.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, RS.AN-08; PDF page 37.

Answer:

Owner, evidence reference and follow up date:

© 2026 Global Digital Forensics, Inc. All rights reserved.

IR-13

Are notification and communication decisions assigned?

Identify who determines applicable obligations, approves messaging and informs affected stakeholders. Reporting deadlines differ by industry, state and contract, so list the ones that apply to you before an incident starts the clock.

Evidence to gather

Communication plan, counsel contact, approval route and relevant contractual obligations.

If something is missing

Have authorized legal and business owners confirm the applicable decisions and timetable.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, RS.CO-02 and RS.CO-03; PDF page 38.

Answer:

Owner, evidence reference and follow up date:

IR-14

Can the team separate containment from removing the cause?

Containment stops the spread; eradication removes persistence and the weakness that let the attacker in, and each needs its own evidence. Track eradication work and the evidence supporting each completed action.

Evidence to gather

Remediation records, affected asset list, verification results and unresolved issues.

If something is missing

Keep incomplete actions visible and agree on the checks that clear recovery to proceed.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, RS.MI-01 and RS.MI-02; PDF page 40.

Answer:

Owner, evidence reference and follow up date:

© 2026 Global Digital Forensics, Inc. All rights reserved.

IR-15

Are recovery materials checked before restoration?

A backup or installation image may contain corruption or signs of compromise. Define who checks the materials and how they are accepted for use.

Evidence to gather

Recovery source checks, known good references and acceptance records.

If something is missing

Resolve unexplained integrity findings before using the material in production.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, RC.RP-03; PDF page 42.

Answer:

Owner, evidence reference and follow up date:

IR-16

Does recovery demonstrate that the business function works?

A restored file or a running server is the start; the service owner confirms that the business function actually works. Confirm the order of restoration, system integrity and operating status with the owner.

Evidence to gather

Functional acceptance criteria, service owner confirmation and post restore monitoring.

If something is missing

Record the open items and who can approve the return to service.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, RC.RP-04 and RC.RP-05; PDF page 42.

Answer:

Owner, evidence reference and follow up date:

© 2026 Global Digital Forensics, Inc. All rights reserved.

IR-17

Have response and recovery been exercised with relevant partners?

Exercises can reveal missing contacts, inaccessible records or conflicting authority without waiting for a live incident. Include critical providers and the scenarios relevant to the business.

Evidence to gather

Exercise plan, attendance, observations and assigned follow up actions.

If something is missing

Run an authorized tabletop or other suitable exercise and track the resulting work.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, ID.IM-02; PDF page 27.

Answer:

Owner, evidence reference and follow up date:

IR-18

Do closure criteria and lessons produce specific improvements?

Declare the end of recovery using agreed criteria and complete the incident record. Assign improvements to plans, monitoring, access or recovery, each with an owner who carries it past the lessons learned meeting.

Evidence to gather

Closure criteria, after action record, owners and follow up dates.

If something is missing

Review outstanding actions with the accountable owner and schedule the next reassessment.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, RC.RP-06 and ID.IM-03; PDF page 42. Additional source pointer: ID.IM-03 (PDF page 27).

Answer:

Owner, evidence reference and follow up date:

Bring Your Readiness Answers to a Free Consultation

Bring the completed checklist to a free consultation with a GDF incident response lead. On that first call we walk through your answers, mark the gaps that would slow a response and set out the preparation work, from playbooks and evidence handling to a tabletop exercise. If an incident is under way, call the

© 2026 Global Digital Forensics, Inc. All rights reserved.

hotline now. Call (786) 219-1210 or the 24/7 hotline at (800) 868-8189, or write to info@evestigate.com. To keep preparing, browse the cybersecurity guide library.

Get Incident Help Now

If an incident is under way, call the 24/7 hotline first. For readiness work, bring this guide to a free consultation and we will set out the response plan, the evidence to preserve and the deliverables.

Miami office: (786) 219-1210 · **24/7 hotline:** (800) 868-8189 · **Email:** info@evestigate.com

miami-computer-forensics.com

© 2026 Global Digital Forensics, Inc. All rights reserved.