Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/incident-response-readiness-checklist/

STANDARDS PREPARATION CHECKLIST

Incident Response and Evidence Readiness

Prepare the decisions, access, records and recovery arrangements needed for a cybersecurity incident. Uses selected CSF 2.0 outcomes from the incident response profile.

Baseline: NIST SP 800-61 Rev. 3 and CSF 2.0. Prepared November 1, 2026.

Use the questions to prepare the review

An incident may require immediate specialist support.

For this incident response preparation, mark each answer as backed by a record you can locate or as still being confirmed. Put an owner against every open question and give the reason for any exclusion.

Incident evidence, access tokens and personal data move through the secure channel agreed on the first call. Identify the record holder and discuss a suitable evidence handoff.

Use these selected incident response preparation questions to prepare a discussion. The references support the topics.

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.

To complete the record

Settle approval responsibilities now, so each decision during an incident goes straight to the right person.

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

Answer:

Owner, evidence reference and follow up date:

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

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 plan tailored to the business names the cloud provider, outside administrator and operational systems the organization relies on.

Evidence to gather

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

To complete the record

Review the plans together and identify assumptions about external support.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, ID.IM-04; PDF page 28. Secondary topic reference: NIST SP 800-61 Rev. 3; Section 3, GV.OC-05; PDF page 20; printed page 12.

Answer:

Owner, evidence reference and follow up date:

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.

To complete the record

Confirm the route using an authorized exercise, clearly labeled as a test.

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

Answer:

Owner, evidence reference and follow up date:

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

IR-04

Are severity and escalation decisions based on impact?

Evaluate affected functions, data, asset criticality and recoverability. Ranking by impact directs attention to the most consequential event first, whatever order the reports arrive in.

Evidence to gather

Severity criteria, escalation thresholds and example decisions.

To complete the record

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, RS.MA-03 and RS.MA-04; PDF pages 34 to 36.

Answer:

Owner, evidence reference and follow up date:

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 alongside office devices.

Evidence to gather

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

To complete the record

Settle the most important ownership and visibility questions ahead of any emergency.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, ID.AM-01, ID.AM-02 and ID.AM-03; PDF pages 23 and 24.

Answer:

Owner, evidence reference and follow up date:

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

IR-06

Are the right records available when an event is examined?

Identify identity, email, endpoint, network and cloud records actually retained. Confirm the access rights, licensing and retention behind each one.

Evidence to gather

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

To complete the record

Arrange approved access and document the sources outside current logging coverage, so the analysis plan accounts for them.

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:

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.

To complete the record

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:

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

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. Confirm which forensic tasks the IT support contract covers.

Evidence to gather

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

To complete the record

Clarify each open handoff 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:

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.

To complete the record

Agree on a recording method that stays available through any outage of the normal collaboration tools.

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

Answer:

Owner, evidence reference and follow up date:

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

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 moves through an agreed transfer process, and the inquiry form carries only general details.

Evidence to gather

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

To complete the record

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:

IR-11

Is containment authorized and suited to the affected service?

Isolation, account restrictions and service shutdowns contain damage, and each is weighed against the essential activity it touches. Define decision criteria, authority and the treatment of urgent exceptions.

Evidence to gather

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

To complete the record

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:

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

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, scope notes and open hypotheses.

To complete the record

Assign the next evidence gathering steps across the wider environment, and decide closure on the full scope.

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

Answer:

Owner, evidence reference and follow up date:

IR-13

Are notification and communication decisions assigned?

Identify who determines applicable obligations, approves messaging and informs affected stakeholders. Requirements depend on the organization and incident, so each reporting deadline is confirmed for the specific matter.

Evidence to gather

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

To complete the record

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 pages 38 and 39.

Answer:

Owner, evidence reference and follow up date:

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

IR-14

Can the team separate containment from removing the cause?

Stopping immediate spread is the first step, and eradication then addresses persistence and the underlying weaknesses. Track eradication work and the evidence supporting each completed action.

Evidence to gather

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

To complete the record

Keep open actions visible and agree on the checks that clear the way for recovery.

Topic reference: NIST SP 800-61 Rev. 3; Section 3, RS.MI-01 and RS.MI-02; PDF pages 40 and 41.

Answer:

Owner, evidence reference and follow up date:

IR-15

Are recovery materials checked before restoration?

Each backup or installation image is checked for integrity and signs of compromise. Define who performs the check and how the materials are accepted for use.

Evidence to gather

Recovery source checks, known good references and acceptance records.

To complete the record

Explain every integrity finding, then use 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:

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

IR-16

Does recovery demonstrate that the business function works?

A recovery test confirms that the essential service itself operates correctly once files are restored and servers are running. 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.

To complete the record

Record the remaining conditions and who approves 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:

IR-17

Have response and recovery been exercised with relevant partners?

Exercises confirm contacts, record access and lines of authority ahead of 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.

To complete the record

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:

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

IR-18

Do closure criteria and lessons produce specific improvements?

Declare the end of recovery using agreed criteria and complete the incident record. Carry the lessons learned meeting through to assigned improvements in plans, monitoring, access or recovery.

Evidence to gather

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

To complete the record

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; PDF page 42. Secondary topic reference: NIST SP 800-61 Rev. 3; Section 3, ID.IM-03; PDF page 27; printed page 19.

Answer:

Owner, evidence reference and follow up date:

Web Addresses for the Sources Cited

1. NIST SP 800-61 Rev. 3; Section 3, GV.RR-02; PDF page 21: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf#page=21
2. NIST SP 800-61 Rev. 3; Section 3, ID.IM-04; PDF page 28: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf#page=28
3. NIST SP 800-61 Rev. 3; Section 3, GV.OC-05; PDF page 20; printed page 12: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf#page=20
4. NIST SP 800-61 Rev. 3; Section 3, RS.MA-02; PDF page 35: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf#page=35
5. NIST SP 800-61 Rev. 3; Section 3, RS.MA, RS.MA-03 and RS.MA-04; PDF pages 34 to 36: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf#page=34
6. NIST SP 800-61 Rev. 3; Section 3, ID.AM-01, ID.AM-02 and ID.AM-03; PDF pages 23 and 24: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf#page=23
7. NIST SP 800-61 Rev. 3; Section 3, DE.CM-06 and DE.CM-09; PDF page 32: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf#page=32
8. NIST SP 800-61 Rev. 3; Section 3, DE.AE-02 and DE.AE; PDF page 33: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf#page=33
9. NIST SP 800-61 Rev. 3; Section 3, RS.AN-06; PDF page 37: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf#page=37
10. NIST SP 800-61 Rev. 3; Section 3, RS.MI-01; PDF page 40: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf#page=40
11. NIST SP 800-61 Rev. 3; Section 3, RS.CO-02 and RS.CO-03; PDF pages 38 and 39: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf#page=38
12. NIST SP 800-61 Rev. 3; Section 3, RC.RP-03; PDF page 42: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf#page=42

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

13. NIST SP 800-61 Rev. 3; Section 3, ID.IM-02; PDF page 27: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf#page=27

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 1, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

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