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.

Edition 2026-11-03 · Online at newyorkcomputerforensics.com/guides/incident-response-readiness-checklist/

Use the questions to prepare the review

These questions cover the readiness outcomes that matter most in the first hours of an incident. If an incident is under way now, call the 24/7 hotline at (800) 868-8189.

For this incident response preparation, distinguish records you can locate from answers still to be confirmed. Assign an owner to each open question and explain exclusions.

Keep incident evidence, access tokens and personal data out of a public form. Identify the record holder and discuss a suitable evidence handoff.

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 this item

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:

© 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. Name the cloud provider, outside administrator and operational systems the organization relies on in the procedure.

Evidence to gather

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

To complete this item

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:

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 this item

Confirm the route using an authorized exercise rather than sending a fabricated production incident.

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. 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.

To complete this item

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:

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 this item

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:

© 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. Record the access rights, licensing and retention behind each source, so every search result reads against its actual coverage.

Evidence to gather

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

To complete this item

Arrange approved access and list the sources still to be located.

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 this item

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 this item

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:

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 this item

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:

© 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.

Evidence to gather

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

To complete this item

Discuss the evidence scope and secure transfer with the response lead and the legal contact.

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 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.

To complete this item

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, limitations and open hypotheses.

To complete this item

Assign the next evidence gathering steps instead of declaring closure from one clean device.

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. Record each reporting deadline that applies to your organization and who owns it.

Evidence to gather

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

To complete this item

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:

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

IR-14

Can the team separate containment from removing the cause?

Containment leads into eradication of persistence and 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 this item

Keep open 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:

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.

To complete this item

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:

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

IR-16

Does recovery demonstrate that the business function works?

Confirm the order of restoration, system integrity and operating status of each essential service with the owner.

Evidence to gather

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

To complete this item

Record 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 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.

To complete this item

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. Assign improvements to plans, monitoring, access or recovery rather than stopping at a lessons learned meeting.

Evidence to gather

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

To complete this item

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:

All five checklists are also in one editable workbook: GDF Standards Readiness Checklists (XLSX).

Get Incident Help Now

Call the 24/7 hotline now if an incident is under way. A responder will help contain it and preserve the records your response depends on, and the first consultation is free. Requests are handled in confidence.

Call (800) 868-8189, 24/7 · New York office (212) 561-5860

Email info@evestigate.com or request your consultation at newyorkcomputerforensics.com/contact.