IR.L2-3.6.1

Incident Response

Incident Handling

"Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities."

Objectives

[a]
An operational incident-handling capability is established.

[b]
The operational incident-handling capability includes preparation.

[c]
The operational incident-handling capability includes detection.

[d]
The operational incident-handling capability includes analysis.

[e]
The operational incident-handling capability includes containment.

[f]
The operational incident-handling capability includes recovery.

[g]
The operational incident-handling capability includes user response activities.

Key Discussion Points

Six Phases Required:
Preparation, detection, analysis, containment, recovery, and user response — all six must be addressed. Missing one is a gap.

Plan + Training:
An IRP on paper is not enough — user response activities require that personnel are trained on roles and reporting procedures.

Indicators to Know:
Sensor alerts, unusual filenames, and suspicious log entries are the three detection indicators explicitly named in the guide.

Spans the Organization:
Effective IR involves HR, legal, procurement, and operations — not just IT. The IRP must address coordination across all affected parties.

Assessment Methods

EXAMINE

Incident response policy; contingency planning policy; procedures addressing incident handling; incident response plan; contingency plan; system security plan; incident response training curriculum and materials; incident response training records.

INTERVIEW

Personnel with incident handling responsibilities; personnel with contingency planning responsibilities; personnel with incident response training and operational responsibilities; personnel with information security responsibilities.

TEST

Incident-handling capability for the organization; organizational processes for incident response assistance; mechanisms supporting or implementing incident response assistance.

IR.L2-3.6.1

INCIDENT RESPONSE — Incident Handling

Plain English

What this control is really saying:

When an incident happens — a breach, a ransomware hit, a data spill — you need a plan. This control requires that you build that capability before you need it: a documented IRP, defined roles, a way to report and track incidents, and trained users who know what to do. The six phases cover the full incident lifecycle from prep to recovery.

How it is used:

- The Incident Response Plan (IRP) is documented and reviewed annually — it covers all six phases and includes named roles and escalation contacts.
- All employees complete annual IR awareness training covering how to recognize and report an incident — the IT admin and security officer receive additional tabletop training.
- Incidents are reported to a dedicated email address and tracked in a simple ticketing log — every incident is recorded from first report to closure.
- The IRP includes contact lists for legal counsel, HR, and the prime contractor's security team — cross-functional coordination is built into the plan.

Real World Example

The Scenario

Acme Defense has never experienced a documented security incident. The IT admin handles all security issues informally. There is no written incident response plan, no designated reporting email, and no user training on incident recognition.

What the assessor finds

No IRP exists. No incident reporting mechanism exists. When asked how they would respond to a ransomware attack, the IT admin says 'I'd call our IT vendor' — no defined roles, no contact list, no containment procedure, no recovery plan. User training on incident recognition has never been conducted.

SPRS Score Impact

3.6.1 carries a point value of 5. No incident response capability is among the most consequential gaps in a CMMC assessment — DFARS 252.204-7012 reporting obligations exist regardless of assessment status, and an organization without an IRP cannot meet them.

What Good Looks Like

Documented IRP covering all six phases, named roles and escalation contacts, incident reporting mechanism established, all users trained on recognition and reporting, tabletop exercises conducted, plan reviewed and updated annually.

Common Gaps

What assessors actually find in the field:

✗ No incident response plan

The organization has no documented IRP — when an incident occurs, response is improvised with no defined roles or procedures.

✗ No user training

Employees have never been trained on how to recognize or report a security incident — users are the first line of detection.

✗ No reporting mechanism

There is no designated way to report a suspected incident — employees have no clear path to alert the IT admin or security team.

✗ Plan exists but not tested

An IRP was written but has never been reviewed, updated, or tested — key contacts are wrong and procedures are outdated.

✗ Missing phases

The IRP covers detection and containment but has no recovery procedures or lessons-learned process — [f] and parts of [g] not met.