IR.L2-3.6.3

Incident Response

Incident Response Testing

"Test the organizational incident response capability."

Objectives

[a]
The incident response capability is tested.

Key Discussion Points

Test Types:
Checklists, tabletop exercises, parallel simulations, and full-interrupt exercises all qualify — tabletop is the most common DIB approach.

Beyond IT:
The guide lists legal, public affairs, HR, and law enforcement as participants — an IT-only test does not satisfy the intent.

Document the Results:
Test results must be documented and used to improve the IRP — a tabletop with no after-action report does not close the loop.

Frequency Matters:
No specific frequency is mandated, but the guide implies regular testing — annual tabletop exercises are the standard DIB practice.

Assessment Methods

EXAMINE

Incident response policy; contingency planning policy; procedures addressing incident response testing; incident response testing material; incident response test results; incident response test plan; incident response plan; contingency plan; system security plan.

INTERVIEW

Personnel with incident response testing responsibilities; personnel with information security responsibilities; personnel with responsibilities for testing plans related to incident response.

TEST

Mechanisms and processes for incident response.

IR.L2-3.6.3

INCIDENT RESPONSE — Incident Response Testing

Plain English

What this control is really saying:

Having a written IRP (3.6.1) isn't enough — this control requires that you actually test it. Put your team in a room, run a scenario, and find out what breaks before a real incident does. The test validates whether your plan works, identifies gaps in roles and procedures, and ensures people know what to do when it counts.

How it is used:

- An annual tabletop exercise is conducted with IT, management, and legal — a simulated ransomware scenario is used to walk through the IRP step by step.
- Test results are documented in an after-action report that identifies gaps and assigns remediation owners with due dates.
- The IRP is updated after each test — tabletop findings drive changes to roles, escalation contacts, and procedures before the next exercise.
- Test records (scenario, participants, results, action items) are retained and available as evidence for assessors.

Real World Example

The Scenario

Acme Defense wrote an incident response plan 18 months ago. The IT admin is confident the plan is adequate. No tabletop exercise has ever been conducted. The plan has never been tested in any form since it was written.

What the assessor finds

No test has ever been performed. The IRP lists a phone number for the previous IT vendor — who left the contract 14 months ago. The IRP references a backup system that was replaced. Nobody other than the IT admin has ever read the plan. All gaps would have been found in a one-hour tabletop exercise.

SPRS Score Impact

3.6.3 carries a point value of 3. An untested IRP is a false sense of security — testing reveals outdated contacts, undefined roles, and procedural gaps that only appear when pressure is applied.

What Good Looks Like

Annual tabletop exercise conducted with cross-functional participation, scenario-based test drives the IRP step by step, after-action report documents findings, IRP updated based on test results, test records retained as evidence.

Common Gaps

What assessors actually find in the field:

✗ **IRP never tested**

The organization wrote an IRP two years ago but has never conducted any form of exercise — the plan has never been validated.

✗ **IT-only test**

Tabletop exercises only involve the IT admin — legal, HR, and management have never participated, leaving key roles untested.

✗ **No after-action documentation**

Informal tabletop discussions happen but no results are documented — no evidence exists and improvements are never tracked.

✗ **Test did not challenge the plan**

The 'test' consisted of the IT admin reading through the IRP alone — no scenario, no team, no gaps identified.

✗ **Test results not acted on**

A tabletop exercise identified three procedure gaps 18 months ago — none have been addressed and the IRP is unchanged.