

SELF ASSESSMENT

Incident Response Maturity Checklist

A quick review of how mature and test-ready your incident response capability is today. This does not replace a formal IR program assessment. Scoring: Yes = 2 pts | Partial = 1 pt | No = 0 pts.

Plan Documentation

Control	Yes – 2	Partial – 1	No – 0
A written incident response plan exists and is version-controlled	☐	☐	☐
Plan defines severity levels and corresponding response timelines	☐	☐	☐
Plan covers ransomware, BEC, data breach, and insider threat scenarios	☐	☐	☐

Roles & Responsibilities

Control	Yes – 2	Partial – 1	No – 0
A designated incident commander is identified for each response	☐	☐	☐
Legal, communications, HR, and executive roles are clearly defined	☐	☐	☐
Cyber insurance carrier and breach counsel contacts are documented	☐	☐	☐

Detection & Escalation

Control	Yes – 2	Partial – 1	No – 0
24/7 monitoring capability exists to detect potential incidents	☐	☐	☐
Clear escalation path exists from detection to leadership notification	☐	☐	☐

Communication & Legal

Control	Yes – 2	Partial – 1	No – 0
Internal and external communication templates are pre-drafted	☐	☐	☐
Regulatory breach notification timelines and obligations are documented	☐	☐	☐

Testing & Improvement

Control	Yes – 2	Partial – 1	No – 0
---------	---------	-------------	--------

IR plan tested via tabletop exercise at least annually	☐	☐	☐
Lessons-learned / post-incident review process is documented and followed	☐	☐	☐

Add the total of each column

TOTAL

*Anything less than **80% of the maximum possible score** suggests your organization would face avoidable confusion and delay during a real incident — the leading driver of extended downtime and increased breach cost.*

Want a Professional Review?

Contact Cenova Cyber at cenovacyber.com to build or stress-test your incident response plan.

www.cenovacyber.com