CTRL THE FUTURE LLC

INCIDENT RESPONSE READINESS CHECKLIST

A practical self-review for preparing to identify, manage, contain, recover from, and learn from cybersecurity incidents

Purpose: This checklist helps organizations review foundational incident-response capabilities before an incident occurs. It is designed as a practical readiness resource and is informed by contemporary incident-response and cybersecurity risk-management concepts, including NIST CSF 2.0. It should be tailored to the organization's environment, risks, legal and contractual obligations, technology, and business priorities.

Organization: _____

Completed by: _____

Date: _____

How to Use This Checklist

Review each statement with appropriate technology, security, operations, legal/compliance, communications, privacy, leadership, and third-party stakeholders. Select the response that best reflects current readiness and record supporting evidence or follow-up actions.

READY	PARTIAL	NOT READY	N/A
Established and usable	Some elements exist	Absent, incomplete, or unknown	Not applicable

1. Governance, Policy & Authority

Incident response readiness statement	Ready	Partial	Not Ready	N/A	Notes
An incident response policy or equivalent governing document is approved and current.	■	■	■	■	
Incident response roles, responsibilities, authorities, and decision rights are defined.	■	■	■	■	
Leadership understands when and how significant cybersecurity incidents are escalated.	■	■	■	■	
The incident response capability is coordinated with relevant cybersecurity, privacy, legal/compliance, business continuity, and operational processes.	■	■	■	■	
Criteria exist for activating the incident response plan and escalating major incidents.	■	■	■	■	

2. Incident Response Team & Contacts

Incident response readiness statement	Ready	Partial	Not Ready	N/A	Notes
Primary and alternate incident response personnel are identified.	■	■	■	■	
Current contact information is maintained for internal responders, leadership, legal/compliance, communications, and other critical stakeholders.	■	■	■	■	
External contacts such as cyber insurance, outside counsel, forensic support, key technology providers, and law enforcement are identified where appropriate.	■	■	■	■	
On-call, after-hours, or emergency contact procedures are established for significant incidents.	■	■	■	■	
Team members understand their responsibilities and have access to the tools and information needed to perform them.	■	■	■	■	

3. Detection, Reporting & Initial Triage

Incident response readiness statement	Ready	Partial	Not Ready	N/A	Notes
Personnel know how to report suspected cybersecurity events and incidents.	■	■	■	■	
Security monitoring and alerting capabilities are defined for important systems and services.	■	■	■	■	
Reported events can be triaged to determine severity, scope, urgency, and required response.	■	■	■	■	
Incident categories and severity levels are defined sufficiently to support consistent handling.	■	■	■	■	
Processes distinguish routine technical issues from events requiring formal incident response.	■	■	■	■	

4. Analysis & Investigation

Incident response readiness statement	Ready	Partial	Not Ready	N/A	Notes
Responders have procedures for collecting and analyzing relevant logs, alerts, system information, and other evidence.	■	■	■	■	
Important data sources and log locations are known before an incident occurs.	■	■	■	■	
Investigation activities can establish affected assets, accounts, data, users, and business processes.	■	■	■	■	
Procedures support development of an incident timeline and documentation of investigative findings.	■	■	■	■	
Evidence preservation and chain-of-custody considerations are addressed when legal, regulatory, disciplinary, insurance, or forensic needs may apply.	■	■	■	■	

5. Containment & Mitigation

Incident response readiness statement	Ready	Partial	Not Ready	N/A	Notes
Containment strategies are defined for common incident scenarios.	■	■	■	■	
Responders have authority or escalation paths to isolate systems, disable accounts, block malicious activity, or take other urgent protective actions.	■	■	■	■	
Containment decisions consider operational impact, evidence preservation, safety, and business continuity.	■	■	■	■	
Temporary mitigations are tracked until permanent corrective actions are implemented.	■	■	■	■	
Actions taken during containment are documented with responsible personnel and timestamps where appropriate.	■	■	■	■	

6. Eradication & Recovery

Incident response readiness statement	Ready	Partial	Not Ready	N/A	Notes
Procedures exist to remove malicious artifacts, unauthorized access, compromised credentials, and identified persistence mechanisms.	■	■	■	■	
Recovery activities include validation that affected systems are safe to return to operation.	■	■	■	■	
Backups and restoration processes are available and periodically tested for critical systems and data.	■	■	■	■	
Recovery priorities are aligned with business continuity and operational requirements.	■	■	■	■	
Enhanced monitoring is considered after restoration to identify recurrence or remaining compromise.	■	■	■	■	

7. Communications & Notification

Incident response readiness statement	Ready	Partial	Not Ready	N/A	Notes
Internal communication responsibilities and escalation channels are defined for incidents.	■	■	■	■	
External communication is coordinated with authorized leadership, legal/compliance, privacy, communications, or other responsible functions.	■	■	■	■	
Potential contractual, regulatory, customer, partner, insurer, or law-enforcement notification requirements can be identified and evaluated promptly.	■	■	■	■	
Incident communications protect sensitive investigative information and avoid unauthorized disclosure.	■	■	■	■	
Predefined communication templates or procedures are available for significant incident scenarios where useful.	■	■	■	■	

8. Third-Party & Supply Chain Incidents

Incident response readiness statement	Ready	Partial	Not Ready	N/A	Notes
Critical vendors, service providers, cloud providers, and other third parties relevant to incident response are identified.	■	■	■	■	
Contracts or agreements are reviewed for incident reporting, cooperation, access, evidence, and notification expectations where appropriate.	■	■	■	■	
Processes exist to evaluate incidents originating from or affecting third parties.	■	■	■	■	
Third-party incidents can be incorporated into the organization's internal severity, escalation, and response processes.	■	■	■	■	
Alternate services, continuity options, or escalation contacts are identified for critical supplier disruptions where appropriate.	■	■	■	■	

9. Documentation, Exercises & Readiness

Incident response readiness statement	Ready	Partial	Not Ready	N/A	Notes
An incident record captures key decisions, actions, evidence, communications, owners, and status.	■	■	■	■	
Incident response plans, playbooks, contact lists, and supporting procedures are stored where responders can access them during disruptions.	■	■	■	■	
Tabletop exercises or simulations are conducted periodically for relevant incident scenarios.	■	■	■	■	
Exercise findings and readiness gaps are assigned owners and tracked to resolution.	■	■	■	■	
Incident response documentation is reviewed after significant organizational, technology, threat, or regulatory changes.	■	■	■	■	

10. Lessons Learned & Continuous Improvement

Incident response readiness statement	Ready	Partial	Not Ready	N/A	Notes
Post-incident reviews are conducted for significant incidents or other events where lessons can improve readiness.	■	■	■	■	
Root causes, contributing factors, control gaps, and response challenges are documented.	■	■	■	■	
Corrective actions are prioritized based on risk and assigned accountable owners and target dates.	■	■	■	■	
Lessons learned are used to update controls, policies, training, playbooks, architecture, monitoring, and recovery practices as appropriate.	■	■	■	■	
Leadership receives meaningful information about significant incidents, recurring trends, response performance, and unresolved risks.	■	■	■	■	

Incident Response Readiness Summary

Use this page to document the most important readiness gaps. Prioritize weaknesses that could materially delay detection, decision-making, containment, investigation, communication, or restoration during a real incident.

Priority Area	Gap / Observation	Owner	Target Date
1.			
2.			
3.			
4.			
5.			

Suggested Next Steps

1. Confirm incident-response ownership, decision authority, escalation paths, and current contact information.
2. Develop or update practical playbooks for the incident scenarios most relevant to the organization.
3. Validate access to logs, backups, administrative tools, external support, and critical documentation before an incident occurs.
4. Conduct a tabletop exercise and track identified gaps through remediation.
5. Review the plan after significant incidents, exercises, technology changes, supplier changes, or changes in applicable obligations.

Need to strengthen incident response readiness?
CTRL The Future LLC can help evaluate incident-response capabilities, develop policies and playbooks, facilitate tabletop exercises, identify gaps, clarify roles and escalation paths, and build a prioritized readiness improvement roadmap.

Framework note: This readiness resource is informed by cybersecurity incident-management concepts reflected in NIST CSF 2.0 and should be tailored to the organization's specific environment and obligations.

Disclaimer: This checklist is provided for general informational and readiness purposes only. It is not legal advice, a formal audit, certification, forensic investigation, or determination that an organization can prevent, detect, contain, or recover from every cybersecurity incident.