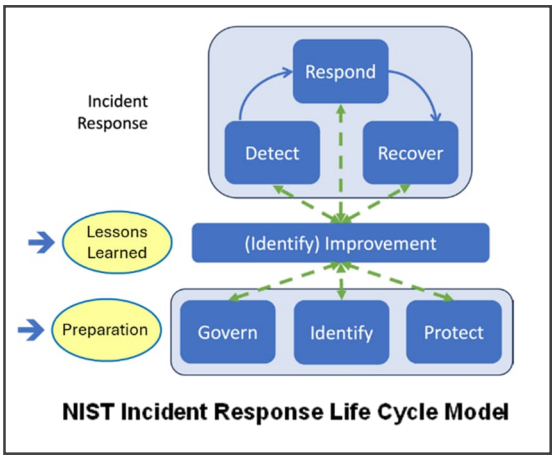
Cyber Incident Response (CIR) Planning Checklist

This checklist is designed to help organizations improve their preparedness to respond to cyber incidents. The steps of this checklist also create the foundation upon which the Cyber Incident Response (CIR) Plan is built. This checklist is *not a substitute* for a CIR Plan.

The checklist consists of specific action items organized by the Incident Response Life Cycle Model of the National Institute of Standards and Technology (NIST)[1]. This Life Cycle Model, shown in the inset figure, is structured around the components of cybersecurity incident response; it has three broad categories that align with the Subcategories of the NIST Cybersecurity Framework (CSF):

- ***Incident Response***. Includes actions in the response operations-related Subcategories in NIST CSF Functions Detect, Respond, and Recover.
- ***Lessons Learned***. Represents opportunities for improving preparedness based on the organization's experience in actual incidents or exercises. The actions in this category generally align with the CSF Identify Function.
- ***Preparation***. Defines actions to build robust incident response capability; actions are in CSF Functions Govern, Identify, Protect, and Detect.



NIST Incident Response Life Cycle Model

The checklist items are grouped in the *Preparation* and *Lessons Learned* components of the NIST Incident Response Life Cycle Model. Each checklist item includes references to the NIST CSF Functions and Subcategories to which it aligns.

In cybersecurity, a distinction is made between a cyber *event* and a cyber *incident*.[2] Events can be expected to occur frequently with relatively small impact; incidents have potentially high impact and require a coordinated response. The organization's Cyber Incident Response Plan should describe the process for escalating events to incidents when warranted.

How to use this checklist

1. Follow the steps in the **Preparation** section to establish and maintain a baseline of capability and operational preparedness. Review at least twice yearly. Some steps are more difficult to accomplish than others.
2. Follow the steps in the **Improvement** section to capture and document lessons learned during and after the response. Update plans, processes, and capabilities accordingly, and review at least twice yearly.
3. This checklist only addresses actions that are related to incident response readiness. To respond to an actual cyber incident, activate your organizational Cyber Incident Response Plan and use it to guide your actions.

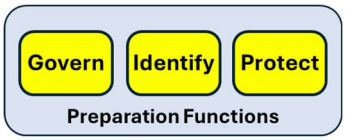
---

[1] NIST SP 800-61r3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

[2] **Definitions** [Source: NIST Computer Security Resource Center Glossary, https://csrc.nist.gov/glossary]

- *event*: Any observable occurrence in a network or system.
- *incident*: An occurrence that actually or potentially jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Cyber Incident Response (CIR) Planning Checklist



Preparation

- ○ 1. **ID.IM-04** Establish, communicate, maintain, and improve incident response plans and other cybersecurity plans that affect operations.
    - a. Develop a Cyber Incident Response (CIR) Plan that contains the guidance and resources needed to respond to cyber incidents in a systematic manner.
        - i. Consult with your cyber insurance broker and carrier to identify third parties with specialized cyber incident response services, such as cybersecurity forensic analysis, external legal counsel, communications advisor, and others.
        - ii. Develop a roster of names and contact information of internal and external (third party) members of the Cyber Incident Response team, including:

            Internal

            - IT representative (CIR Team Leader)
            - County leadership
            - Cybersecurity Operations Leader
            - Representatives of County functional leaders (Legal, HR, Finance, etc.)

            External (third parties) as applicable

            - Cybersecurity forensics service provider
            - External legal counsel
            - Law Enforcement (FBI)
    - b. Create playbooks as part of documenting cyber incident response procedures. Playbooks provide actionable steps or tasks for people to perform during various scenarios or situations.
    - c. **GV.SC-08** Include relevant suppliers and other third parties in incident planning, response, and recovery activities.
- ○ 2. **GOVERN** Conduct regular (at least twice yearly) Cyber Tabletop Exercises to develop the readiness of the organization to execute the Cyber Incident Response Plan and respond to cyber incidents. (supports **ID.IM-02**)
- ○ 3. **ID.AM-01** Document and maintain inventories of information technology hardware managed by the organization.
- ○ 4. **ID.AM-02** Document and maintain inventories of software, services, and systems managed by the organization.
- ○ 5. **ID.AM-04** Document and maintain inventories of services provided by suppliers for use in finding and addressing vulnerabilities, monitoring operations, and identifying “shadow IT” usage.
- ○ 6. **PR.DS-11** Create, protect, maintain, and test backups of data, including network and system log data.

Cyber Incident Response (CIR) Planning Checklist
a. Test data and system restoration on a regular basis, adjusting test objectives to cover a broad range of scenarios over time. Include testing of processes for verification of data integrity. (supports **RC-RP-03**)
○ 7. **ID.RA-08** Establish processes for receiving, analyzing, and responding to vulnerability disclosures.
○ 8. **ID.RA-02** Receive cyber threat intelligence from information sharing forums and sources and integrate it into cybersecurity event detection and analysis.
○ 9. **DETECT** Develop and implement capability to adjust the extent and verbosity of network and system logging that can be selectively activated if preliminary analysis of cyber events and incidents warrant. (supports **PR.PS-04**)
○ 10. Develop the capability to monitor the environment to detect cyber events. Specifically, develop the capability and processes to: a. **DE.CM-01** Monitor networks and network services to detect potentially adverse events. b. **DE.CM-02** Monitor the physical environment to detect potentially adverse events. c. **DE.CM-03** Monitor personnel activity and technology usage to detect potentially adverse events. d. **DE.CM-06** Monitor external service provider activities and services to detect potentially adverse events. e. **DE.CM-09** Monitor computing hardware and software, runtime environments, and their data to detect potentially adverse events.
○ 11. Develop the capability to analyze and understand cyber events to determine the actions to be taken, including capability and associated processes to: a. **DE.AE-02** Analyze potentially adverse events to better understand associated activities. b. **DE.AE-03** Correlate cybersecurity event information from multiple sources to better understand the estimated impact and scope of the event. c. **DE.AE-07** Integrate cyber threat intelligence and other contextual information into cybersecurity event analysis. d. **DE.AE-08** Declare an incident when adverse events meet the defined incident criteria. e. Perform initial analysis promptly upon cyber event detection; use the results of the analysis to inform actions. (supports **DE.AE**)
○ 12. **DETECT** Establish and exercise a process for escalating detected cybersecurity events to higher levels within the organization as warranted by the potential impact of the event and the need for more senior management decision making. The escalation process should define the conditions that would designate the cybersecurity event as a cybersecurity incident. (supports **DE.AE-08**, **RS.MA-04**)

Cyber Incident Response (CIR) Planning Checklist
○ 13. **PR.AT-02** Provide awareness and training to individuals in specialized roles so they possess the knowledge and skills to perform relevant tasks with security risks in mind.

Cyber Incident Response (CIR) Planning Checklist
(Identify) Improvement **Lessons Learned**
○ 1. **ID.IM-01** Identify improvements by periodically evaluating incident response program performance to identify problems and deficiencies that should be corrected.
○ 2. **ID.IM-02** Improve the Cyber Incident Response Plan and associated procedures based on: a. Results of security tests and exercises, including those done in coordination with suppliers and relevant third parties. b. **ID.IM-03** Learnings from the execution of operational processes, procedures, and activities.
○ 3. **GV.RR** Ensure that cybersecurity roles, responsibilities, and authorities are established to foster accountability, performance assessment, and continuous improvement. a. **GV.RR-01** Ensure that organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving. b. **GV.RR** Ensure that cybersecurity roles, responsibilities, and authorities include incident response.
○ 4. **GV.OV** Improve and adjust cybersecurity risk management strategy by: a. **GV.OV-01** Reviewing cybersecurity risk management strategy outcomes to inform and adjust strategy and direction. b. **GV.OV-02** Reviewing and adjusting the cybersecurity risk management strategy to ensure coverage of organizational requirements and risks. c. **GV.OV-03** Evaluating and reviewing organizational cybersecurity risk management performance and adjusting as needed.