Applying the NIST Cybersecurity Framework (CSF)

What is the NIST CSF?

The NIST Cybersecurity Framework is a flexible, repeatable model for managing and reducing cybersecurity risk. It's broken down into five core functions, each with categories and subcategories.

Use this framework to:
- Respond to incidents
- Build or assess security programs
- Guide tabletop exercises
- Communicate risks clearly

1. IDENTIFY – Know what you have and what's at risk.

Purpose: Understand the business context, critical assets, data flows, and known vulnerabilities.

Key Activities:
- Inventory hardware, software, users
- Classify systems by criticality
- Map data flow and access rights
- Identify high-risk assets or gaps in visibility

Questions to Ask:
- What systems or data are at risk?
- Who has access to them?
- Are there any known vulnerabilities?
- What is normal behavior in this environment?

Example: Before responding to a breach, identify what the attacker could access — and which assets are most valuable.

2. PROTECT – Reduce the likelihood of an incident.

Purpose: Put safeguards in place to limit or contain the impact of a potential event.

Key Activities:
- Apply least privilege and access controls

- Enable MFA
- Patch systems and enforce configuration baselines
- Encrypt sensitive data
- Provide user awareness training

Questions to Ask:
- Are systems up-to-date and securely configured?
- Do we have access controls and backup plans?
- Is sensitive data encrypted?
- Are users trained on common threats?

Example: Blocking external RDP access and applying MFA can prevent credential-based attacks.

3. DETECT – Know when something goes wrong.

Purpose: Quickly identify when an attack or anomaly is occurring.

Key Activities:
- Monitor logs, endpoints, and network traffic
- Use IDS/IPS, SIEM, or threat intelligence feeds
- Establish alerts for known attack indicators

Questions to Ask:
- Do we have visibility into network and host behavior?
- Are alerts in place for common attacks (DDoS, brute force, malware)?
- Can we distinguish normal vs. abnormal activity?
- Are alerts being reviewed in real-time?

Example: Using Snort to detect an ICMP flood attack or suspicious port scanning.

4. RESPOND – Minimize the damage.

Purpose: Take action once an event is detected to contain the threat and minimize its impact.

Key Activities:
- Isolate affected systems
- Communicate with internal teams and legal/compliance
- Execute a documented response playbook
- Conduct forensic analysis and log collection

Questions to Ask:

- What steps must we take to contain the threat?
- Who needs to be informed?
- Are roles and responsibilities clear?
- How is the response effort being documented?

Example: Blocking a malicious IP and isolating a compromised endpoint within 10 minutes of detection.

5. RECOVER – Get back to business - stronger.

Purpose: Restore normal operations and reduce the likelihood of the same event recurring.

Key Activities:
- Reimage or restore affected systems
- Review and update security policies
- Communicate status updates
- Conduct post-incident review and share lessons learned

Questions to Ask:
- Are all critical services restored?
- What changes must be made to prevent a recurrence?
- Were users or clients notified?
- Has the incident response plan been updated?

Example: After a phishing attack, restoring mailboxes, resetting passwords, and running mandatory phishing training.

How to Use This Framework

You can:
- Use each function as a heading during real-time incident response
- Guide security audits and tabletop exercises
- Build your personal or team playbooks

Prepared by: Charles J. Wasson

Source: Adapted from “Applying the NIST CSF” internal documentation