# CYBERSECURITY FRAMEWORK 2.0 ASSESMENT REPORT FOR ACME CORPORATION

Eric D. Cataline

## Contents

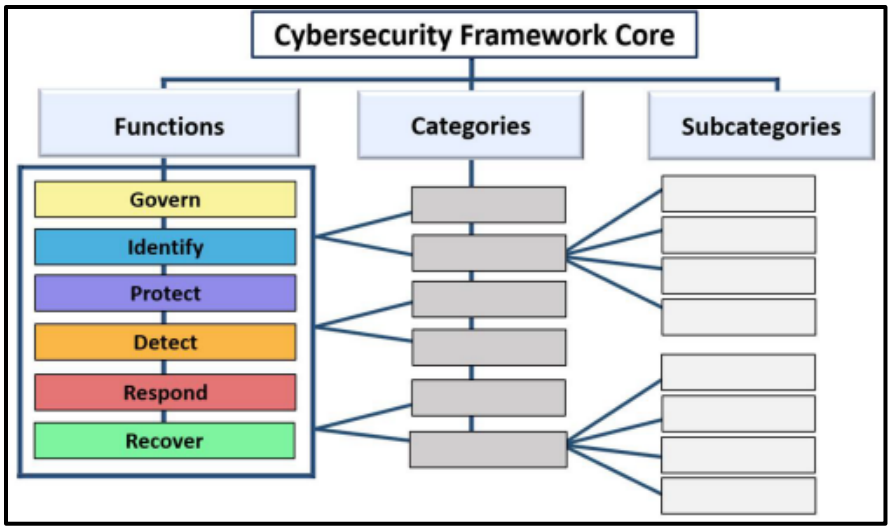


## Background and Purpose

Acme Corp. contacted Cadre Consulting Engineering Services to conduct an assessment of the Cybersecurity Framework 2.0. The assessment took place in August of 2025 and was conducted by Eric Cataline. The following is a report intended to convey the results of the assessment to the appropriate organization officials. This report was created based on the NIST CSF 2.0 and the NIST Special Publication (SP) 800-53Ar5 *Assessing Security and Privacy Controls in Information Systems and Organizations*.

## Assessment Methodology

The assessment was conducted using the CSF 2.0 core as the target profile for the organization. The CSF 2.0 Core is “a set of cybersecurity outcomes arranged by Function, then Category, and finally Subcategory,” as seen below.




There are approximately 110 controls or safeguards to assess in the Cybersecurity Framework 2.0 Core. All categories and subcategories were assessed using one or more of three methods: Examine, Interview, and/or Test.

| **Assessment Methods**<br>Source NIST SP 800-53Ar5 | | |
|---|---|---|
| **Examine** | **Interview** | **Test** |
| The examine method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities) to facilitate assessor understanding, achieve clarification, or obtain evidence. | The interview method is the process of holding discussions with individuals or groups of individuals within an organization to facilitate assessor understanding, achieve clarification, or obtain evidence. | The test method is the process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare the actual state of the object to the desired state or expected behavior of the object. |

The CSF 2.0 Assessment Tool was used to document detailed information for each security control or safeguard being assessed. The CSF 2.0 Assessment Tool is to facilitate the assessment of the CSF 2.0 for an organization. The tool is designed to conduct gap analysis of an organization's current profile against their target profile. The tool provides a

metric/rating out of 10 that aligns to the four CSF 2.0 Tiers and characteristics. A rating score for each control/safeguard is entered during the assessment, and an overall rating score is calculated by the tool. The rating value is used to express a level in which a desired outcome is achieved. Ultimately, numeric values are somewhat arbitrary; however, a rating of 9.9 is considered rarified air, and a rating of 10 is not considered to be achievable.

| CSF 2.0 Tier | Rating | Tier Characteristics<br>Source: CSF 2.0, Appendix B:<br>https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf |
|---|---|---|
| **Tier 4: Adaptive** | **8.0 - 9.9** | Organization-wide approach to managing cybersecurity<br><br>Uses risk-informed policies, processes, and procedures to address potential cybersecurity events.<br><br>Adaptive cybersecurity practices based on previous and current activities, including lessons learned and predictive indicators.<br><br>Cybersecurity information is constantly shared throughout the organization and with authorized third parties. |
| **Tier 3: Repeatable** | **6.0 - 7.9** | Risk management practices are formally approved and expressed as policy.<br><br>Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed.<br><br>Consistent methods are in place to respond effectively to changes in risk.<br><br>Risk strategy is informed by the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. Personnel formally act upon those risks through mechanisms such as written agreements to communicate baseline requirements, governance structures and policy implementation and monitoring. |

| | | |
|---|---|---|
| **Tier 2: Risk-Informed** | **3.0 - 5.9** | Risk management practices are approved by management but may not be established as organization wide policy.<br><br>Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization.<br><br>Cybersecurity information is shared within the organization on an informal basis.<br><br>Aware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses, but it does not act consistently or formally in response to those risks. |
| **Tier 1: Partial** | **0.0 - 2.9** | Application of the organizational cybersecurity risk strategy is managed in an ad hoc manner.<br><br>Prioritization is ad hoc and not formally based on objectives or threat environment.<br><br>There is limited awareness of cybersecurity risks at the organizational level.<br><br>Generally unaware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. |

## Assessment Summary

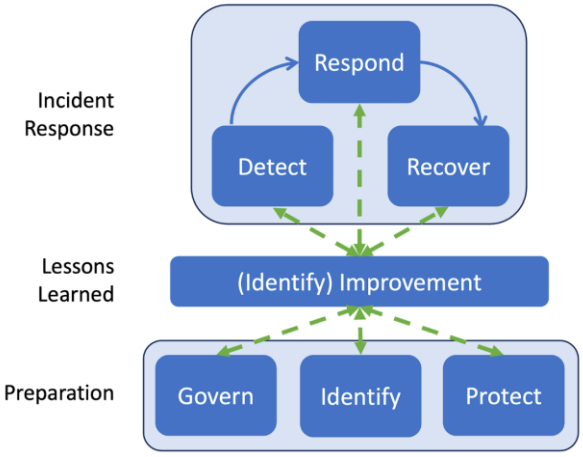
Acme Corp.'s overall rating for this assessment was 9.2, which equates to the Adaptive Tier in the CSF 2.0 and an excellent Cybersecurity posture. All individual CSF functions were rated in the adaptive tier except the Recover function, which is rated as Repeatable, still a commendable rating. Detailed assessment results can be found in the CSF 2.0 Assessment Tool.

| Overall Rating: | | | 9.2 | | ADAPTIVE |
|---|---|---|---|---|---|
| **Function** | **Rating** | **Previous** | **Target** | **Delta** | **Current Rating** |
| GOVERN (GV) | 9.1 | N/A | 9.5 | N/A | ADAPTIVE |
| IDENTIFY (ID) | 9.5 | N/A | 9.5 | N/A | ADAPTIVE |
| PROTECT (PR) | 9.5 | N/A | 9.5 | N/A | ADAPTIVE |
| DETECT (DE) | 9.5 | N/A | 9.5 | N/A | ADAPTIVE |
| RESPOND (RS) | 9.5 | N/A | 9.5 | N/A | ADAPTIVE |
| RECOVER (RC) | 7.9 | N/A | 9.5 | N/A | REPEATABLE |

## Assessor Comments and Recommendations

### Incident Recovery | RC.CO-3,RC.CO-04,RC.RP-1,RC.RP-02,RC.RP-03,RC.RP-04,RC.RP-05,RC.RP-06

During the assessment it was noted that a robust Incident Response plan is needed if Acme Corp. intends to progress towards its target profile. See the CSF 2.0 controls in the Assessment Tool. Additionally, in April of 2025, the NIST released the Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. The profile can "*help organizations prepare for incident responses, reduce the number and impact of incidents that occur, and improve the efficiency and effectiveness of their incident detection, response, and recovery activities*."




## Vulnerability scans | DE.CM-09

There is already some scanning and monitoring being done on the network; however, it is recommended to add the function of a vulnerability scanning tool that can facilitate flaw remediation by scanning endpoints and infrastructure components to verify that the current and recommended software and firmware versions are installed as well as scanning for open CVEs. There are multiple tools on the market that can perform network discovery and credentialed endpoint scanning and Cadre recommends that Acme Corp. examine some of these tools. Additionally, in April of 2022, the NIST released the SP 800-40 rev 4: Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology.

## References and Links

- **NIST Cybersecurity Framwork 2.0:** https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- **NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile:** https://csrc.nist.gov/pubs/sp/800/61/r3/final
- **NIST Special Publication 800-40 Rev. 4: Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology:** https://csrc.nist.gov/pubs/sp/800/40/r4/final

- **NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations:** https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
- **NIST SP 800-53A Rev. 5: Assessing Security and Privacy Controls in Information Systems and Organizations:** https://csrc.nist.gov/pubs/sp/800/53/a/r5/final