



# NIST CSF 2.0

## Policies and Procedures



**CONFIDENTIALITY NOTE:** The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for: Client Company

Prepared by: YourIT Company

# Table of Contents

<b>01</b>	Purpose
<b>02</b>	Scope
<b>03</b>	Sanctions/Compliance
<b>04</b>	NIST CSF 2.0 DE.AE-02 - Potentially Adverse Event Analysis
<b>05</b>	NIST CSF 2.0 DE.AE-03 - Event Information Correlation
<b>06</b>	NIST CSF 2.0 DE.AE-04 - Impact & Scope Determination
<b>07</b>	NIST CSF 2.0 DE.AE-06 - Event Information Sharing
<b>08</b>	NIST CSF 2.0 DE.AE-07 - Contextual Analysis
<b>09</b>	NIST CSF 2.0 DE.AE-08 - Incident Declaration
<b>10</b>	NIST CSF 2.0 DE.CM-01 - Network Monitoring
<b>11</b>	NIST CSF 2.0 DE.CM-02 - Physical Environment Monitoring
<b>12</b>	NIST CSF 2.0 DE.CM-03 - Personnel Activity Monitoring
<b>13</b>	NIST CSF 2.0 DE.CM-06 - Service Provider Monitoring
<b>14</b>	NIST CSF 2.0 DE.CM-09 - Hardware, Software, & Data Monitoring
<b>15</b>	NIST CSF 2.0 GV.OC-01 - Organizational Mission
<b>16</b>	NIST CSF 2.0 GV.OC-02 - Stakeholder Risk Management Expectations
<b>17</b>	NIST CSF 2.0 GV.OC-03 - Legal, Regulatory, & Contractual Requirements
<b>18</b>	NIST CSF 2.0 GV.OC-04 - Stakeholder Service Expectations
<b>19</b>	NIST CSF 2.0 GV.OC-05 - Organizational Service Dependencies
<b>20</b>	NIST CSF 2.0 GV.OV-01 - Risk Management Strategy Outcomes Review
<b>21</b>	NIST CSF 2.0 GV.OV-02 - Risk Management Strategy Review & Adjustment
<b>22</b>	NIST CSF 2.0 GV.OV-03 - Risk Management Performance Measurement
<b>23</b>	NIST CSF 2.0 GV.PO-01 - Establishment of Policies & Procedures
<b>24</b>	NIST CSF 2.0 GV.PO-02 - Policy & Procedure Review & Update
<b>25</b>	NIST CSF 2.0 GV.RM-01 - Risk Management Objectives Agreement
<b>26</b>	NIST CSF 2.0 GV.RM-02 - Risk Appetite & Risk Tolerance Statements
<b>27</b>	NIST CSF 2.0 GV.RM-03 - Enterprise Risk Integration



28	NIST CSF 2.0 GV.RM-04 - Risk Response Strategic Direction
29	NIST CSF 2.0 GV.RM-05 - Lines of Communication
30	NIST CSF 2.0 GV.RM-06 - Standardized Risk Management Method
31	NIST CSF 2.0 GV.RM-07 - Strategic Opportunities
32	NIST CSF 2.0 GV.RR-01 - Organizational Leadership Responsibility
33	NIST CSF 2.0 GV.RR-02 - Risk Management Roles & Responsibilities
34	NIST CSF 2.0 GV.RR-03 - Resource Adequacy
35	NIST CSF 2.0 GV.RR-04 - Human Resource Practices
36	NIST CSF 2.0 GV.SC-01 - Supply Chain Risk Management Program
37	NIST CSF 2.0 GV.SC-02 - Third Party Roles & Responsibilities
38	NIST CSF 2.0 GV.SC-03 - Supply Chain Risk Management Integration
39	NIST CSF 2.0 GV.SC-04 - Supplier Identification & Prioritization
40	NIST CSF 2.0 GV.SC-05 - Cybersecurity Risks & Supply Chain Contracts
41	NIST CSF 2.0 GV.SC-06 - Supplier Due Diligence
42	NIST CSF 2.0 GV.SC-07 - Supplier Risk Assessment and Risk Management
43	NIST CSF 2.0 GV.SC-08 - Third Party Incident Management Integration
44	NIST CSF 2.0 GV.SC-09 - Supply Chain Security Practice Integration
45	NIST CSF 2.0 GV.SC-10 - Third Party Post Relationship Risk Management
46	NIST CSF 2.0 ID.AM-01 - Hardware Inventory
47	NIST CSF 2.0 ID.AM-02 - Software, Services, & Systems Inventory
48	NIST CSF 2.0 ID.AM-03 - Network Communications & Data Flows
49	NIST CSF 2.0 ID.AM-04 - Supplier Services Inventory
50	NIST CSF 2.0 ID.AM-05 - Asset Protection Prioritization
51	NIST CSF 2.0 ID.AM-07 - Data & Metadata Inventory
52	NIST CSF 2.0 ID.AM-08 - Asset Life Cycle Management
53	NIST CSF 2.0 ID.IM-01 - Continuous Improvements Evaluation
54	NIST CSF 2.0 ID.IM-02 - Tests & Exercises
55	NIST CSF 2.0 ID.IM-03 - Improvements from Lessons Learned
56	NIST CSF 2.0 ID.IM-04 - Plans Affecting Operations
57	NIST CSF 2.0 ID.RA-01 - Asset Vulnerability Identification



58	NIST CSF 2.0 ID.RA-02 - Information Sharing Forums
59	NIST CSF 2.0 ID.RA-03 - Threat Identification
60	NIST CSF 2.0 ID.RA-04 - Impact & Likelihood Analysis
61	NIST CSF 2.0 ID.RA-05 - Risk Exposure Determination & Prioritization
62	NIST CSF 2.0 ID.RA-06 - Risk Response Determination
63	NIST CSF 2.0 ID.RA-07 - Change & Exception Management
64	NIST CSF 2.0 ID.RA-08 - Vulnerability Disclosure Response
65	NIST CSF 2.0 ID.RA-09 - Pre-acquisition Integrity Assessment
66	NIST CSF 2.0 ID.RA-10 - Supplier Pre-Acquisition Assessments
67	NIST CSF 2.0 PR.AA-01 - Identity & Credential Management
68	NIST CSF 2.0 PR.AA-02 - Identity Binding to Credentials
69	NIST CSF 2.0 PR.AA-03 - Authentication
70	NIST CSF 2.0 PR.AA-04 - Identity Assertions
71	NIST CSF 2.0 PR.AA-05 - Access Authorizations
72	NIST CSF 2.0 PR.AA-06 - Physical Access
73	NIST CSF 2.0 PR.AT-01 - User Awareness & Training
74	NIST CSF 2.0 PR.AT-02 - Specialized Role Awareness & Training
75	NIST CSF 2.0 PR.DS-01 - Protection of Data at Rest
76	NIST CSF 2.0 PR.DS-02 - Protection of Data in Transit
77	NIST CSF 2.0 PR.DS-10 - Protection of Data in Use
78	NIST CSF 2.0 PR.DS-11 - Data Backup
79	NIST CSF 2.0 PR.IR-01 - Logical Access Protections
80	NIST CSF 2.0 PR.IR-02 - Environmental Threat Protections
81	NIST CSF 2.0 PR.IR-03 - Resilience Measures
82	NIST CSF 2.0 PR.IR-04 - Capacity Management
83	NIST CSF 2.0 PR.PS-01 - Configuration Management
84	NIST CSF 2.0 PR.PS-02 - Software Maintenance & Replacement
85	NIST CSF 2.0 PR.PS-03 - Hardware Maintenance
86	NIST CSF 2.0 PR.PS-04 - Log Record Generation
87	NIST CSF 2.0 PR.PS-05 - Unauthorized Software Installation & Execution
88	NIST CSF 2.0 PR.PS-06 - Secure Systems Development Practices



89	NIST CSF 2.0 RC.CO-03 - Recovery Activity Communication
90	NIST CSF 2.0 RC.CO-04 - Public Information Sharing
91	NIST CSF 2.0 RC.RP-01 - Recovery Plan Execution
92	NIST CSF 2.0 RC.RP-02 - Recovery Action Performance
93	NIST CSF 2.0 RC.RP-03 - Backup & Restoration Asset Integrity
94	NIST CSF 2.0 RC.RP-04 - Post-Incident Operational Norms
95	NIST CSF 2.0 RC.RP-05 - Asset Integrity Restoration
96	NIST CSF 2.0 RC.RP-06 - End-of-Incident Determination
97	NIST CSF 2.0 RS.AN-03 - Incident Analysis & Root Cause Determination
98	NIST CSF 2.0 RS.AN-06 - Investigation Documentation
99	NIST CSF 2.0 RS.AN-07 - Incident Data Collection & Preservation
100	NIST CSF 2.0 RS.AN-08 - Incident Magnitude Determination
101	NIST CSF 2.0 RS.CO-02 - Stakeholder Incident Notification
102	NIST CSF 2.0 RS.CO-03 - Stakeholder Incident Information Sharing
103	NIST CSF 2.0 RS.MA-01 - Response Plan Execution
104	NIST CSF 2.0 RS.MA-02 - Incident Triage & Validation
105	NIST CSF 2.0 RS.MA-03 - Incident Categorization & Prioritization
106	NIST CSF 2.0 RS.MA-04 - Incident Escalation
107	NIST CSF 2.0 RS.MA-05 - Recovery Initiation
108	NIST CSF 2.0 RS.MI-01 - Incident Containment
109	NIST CSF 2.0 RS.MI-02 - Incident Eradication



# Purpose

---

The purpose is to ensure the security of data aligned with a federal standard, to meet regulatory, contractual, or insurance requirements, or to ensure a high level of data protection.



# Scope

---

This policy applies to the workforce members and vendors of organization that come in contact with sensitive, confidential, and/or protected data.



# Sanctions/Compliance

---

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.





# NIST CSF 2.0 DE.AE-02 - Potentially Adverse Event Analysis

<b>NIST CSF 2.0</b>  <b>DE.AE-02</b>  <b>Potentially Adverse Event Analysis</b>	<b>Other Requirements</b> N/A
---	----------------------------------

## Policy

The organization will implement internal controls to satisfy the following requirement:

DE.AE-02: Potentially adverse events are analyzed to better understand associated activities.

## Guidance

Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Use security information and event management (SIEM) or other tools to continuously monitor log events for known malicious and suspicious activity

Ex2: Utilize up-to-date cyber threat intelligence in log analysis tools to improve detection accuracy and characterize threat actors, their methods, and indicators of compromise

Ex3: Regularly conduct manual reviews of log events for technologies that cannot be sufficiently monitored through automation

Ex4: Use log analysis tools to generate reports on their findings

NIST CSF 2.0 - Informative References:

CIS Controls v8.0: 8.11  
CRI Profile v2.0: DE.AE-02  
CRI Profile v2.0: DE.AE-02.01  
CRI Profile v2.0: DE.AE-02.02  
CSF v1.1: DE.AE-2  
SP 800-53 Rev 5.1.1: AU-06  
SP 800-53 Rev 5.1.1: CA-07  
SP 800-53 Rev 5.1.1: IR-04  
SP 800-53 Rev 5.1.1: SI-04

## Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.



#### **Related Internal Controls**

- CIS8.11 - Conduct Audit Log Reviews: Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.

#### **References**

- NIST Cybersecurity Framework - <https://www.nist.gov/cyberframework>
- CIS Critical Security Controls - <https://www.cisecurity.org/controls>
- CRI Profile v2.0 - <https://cyberriskinstitute.org/the-profile/>
- NIST CSF 1.1 Archive - <https://www.nist.gov/cyberframework/csf-11-archive>

# NIST CSF 2.0 DE.AE-03 - Event Information Correlation

<b>NIST CSF 2.0</b>  <b>DE.AE-03</b>  <b>Event Information Correlation</b>	<b>Other Requirements</b> N/A
--	----------------------------------

## Policy

The organization will implement internal controls to satisfy the following requirement:

DE.AE-03: Information is correlated from multiple sources.

## Guidance

Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Constantly transfer log data generated by other sources to a relatively small number of log servers

Ex2: Use event correlation technology (e.g., SIEM) to collect information captured by multiple sources

Ex3: Utilize cyber threat intelligence to help correlate events among log sources

NIST CSF 2.0 - Informative References:

CRI Profile v2.0: DE.AE-03  
CRI Profile v2.0: DE.AE-03.01  
CRI Profile v2.0: DE.AE-03.02  
CSF v1.1: DE.AE-3  
SP 800-53 Rev 5.1.1: AU-06  
SP 800-53 Rev 5.1.1: CA-07  
SP 800-53 Rev 5.1.1: PM-16  
SP 800-53 Rev 5.1.1: IR-04  
SP 800-53 Rev 5.1.1: IR-05  
SP 800-53 Rev 5.1.1: IR-08  
SP 800-53 Rev 5.1.1: SI-04

## Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

## Related Internal Controls

- CRI.DE.AE-03.01 - Event Information Correlation.01:  
NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-03.01:



The organization implements systematic and real-time logging, collection, monitoring, detection, and alerting measures across multiple layers of the organization's infrastructure, including physical perimeters, network, operating systems, applications, data, and external (cloud and outsourced) environments, sufficient to protect the organization's information assets.

- CRI.DE.AE-03.02 - Event Information Correlation.02 :  
NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-03.02:

The organization performs real-time central analysis, aggregation, and correlation of anomalous activities, network and system alerts, and relevant event and cyber threat intelligence, including both internal and external (cloud and outsourced) environments, to better detect and prevent multifaceted cyber attacks.

#### References

- NIST Cybersecurity Framework - <https://www.nist.gov/cyberframework>
- CRI Profile v2.0 - <https://cyberriskinstitute.org/the-profile/>
- NIST CSF 1.1 Archive - <https://www.nist.gov/cyberframework/csf-11-archive>

# NIST CSF 2.0 DE.AE-04 - Impact & Scope Determination

<b>NIST CSF 2.0</b>  <b>DE.AE-04</b>  <b>Impact &amp; Scope Determination</b>	<b>Other Requirements</b> N/A
---	----------------------------------

## Policy

The organization will implement internal controls to satisfy the following requirement:

DE.AE-04: The estimated impact and scope of adverse events are understood.

## Guidance

Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Use SIEMs or other tools to estimate impact and scope, and review and refine the estimates

Ex2: A person creates their own estimates of impact and scope

NIST CSF 2.0 - Informative References:

CRI Profile v2.0: DE.AE-04  
CRI Profile v2.0: DE.AE-04.01  
CSF v1.1: DE.AE-4  
SP 800-53 Rev 5.1.1: PM-09  
SP 800-53 Rev 5.1.1: PM-11  
SP 800-53 Rev 5.1.1: PM-18  
SP 800-53 Rev 5.1.1: PM-28  
SP 800-53 Rev 5.1.1: PM-30

## Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

## Related Internal Controls

- CRI.DE.AE-04.01 - Impact & Scope Determination:  
NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-04.01:

The organization has a documented process to analyze and triage incidents to assess root cause, technical impact, mitigation priority, and business impact on the organization, as well as across the financial sector and other third party stakeholders.



## References

- NIST Cybersecurity Framework - <https://www.nist.gov/cyberframework>
- CRI Profile v2.0 - <https://cyberriskinstitute.org/the-profile/>
- NIST CSF 1.1 Archive - <https://www.nist.gov/cyberframework/csf-11-archive>

# NIST CSF 2.0 DE.AE-06 - Event Information Sharing

<b>NIST CSF 2.0</b>  <b>DE.AE-06</b>  <b>Event Information Sharing</b>	<b>Other Requirements</b> N/A
--	----------------------------------

## Policy

The organization will implement internal controls to satisfy the following requirement:

DE.AE-06: Information on adverse events is provided to authorized staff and tools.

## Guidance

Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Use cybersecurity software to generate alerts and provide them to the security operations center (SOC), incident responders, and incident response tools

Ex2: Incident responders and other authorized personnel can access log analysis findings at all times

Ex3: Automatically create and assign tickets in the organization's ticketing system when certain types of alerts occur

Ex4: Manually create and assign tickets in the organization's ticketing system when technical staff discover indicators of compromise

NIST CSF 2.0 - Informative References:

CRI Profile v2.0: DE.AE-06  
CRI Profile v2.0: DE.AE-06.01  
CSF v1.1: DE.DP-4  
SP 800-53 Rev 5.1.1: IR-04  
SP 800-53 Rev 5.1.1: PM-15  
SP 800-53 Rev 5.1.1: PM-16  
SP 800-53 Rev 5.1.1: RA-04  
SP 800-53 Rev 5.1.1: RA-10

## Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

## Related Internal Controls



- CRI.DE.AE-06.01 - Event Information Sharing:  
NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-06.01:

The organization has established processes and protocols to communicate, alert, and regularly report potential cyber attacks and incident information, including its corresponding analysis and cyber threat intelligence, to authorized internal and external stakeholders.

#### References

- NIST Cybersecurity Framework - <https://www.nist.gov/cyberframework>
- CRI Profile v2.0 - <https://cyberriskinstitute.org/the-profile/>
- NIST CSF 1.1 Archive - <https://www.nist.gov/cyberframework/csf-11-archive>



# NIST CSF 2.0 DE.AE-07 - Contextual Analysis

<b>NIST CSF 2.0</b>  <b>DE.AE-07</b>  <b>Contextual Analysis</b>	<b>Other Requirements</b> N/A
--	----------------------------------

## Policy

The organization will implement internal controls to satisfy the following requirement:

DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis.

## Guidance

Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Securely provide cyber threat intelligence feeds to detection technologies, processes, and personnel

Ex2: Securely provide information from asset inventories to detection technologies, processes, and personnel

Ex3: Rapidly acquire and analyze vulnerability disclosures for the organization's technologies from suppliers, vendors, and third-party security advisories

NIST CSF 2.0 - Informative References:

CRI Profile v2.0: DE.AE-07  
CRI Profile v2.0: DE.AE-07.01  
CRI Profile v2.0: DE.AE-07.02  
CSF v1.1: DE.AE-3  
SP 800-53 Rev 5.1.1: PM-16  
SP 800-53 Rev 5.1.1: RA-03  
SP 800-53 Rev 5.1.1: RA-10

## Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

## Related Internal Controls

- CRI.DE.AE-07.01 - Contextual Analysis.01:  
NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-07.01:



The organization implements measures for monitoring external sources (e.g., social media, the dark web, etc.) to integrate with other intelligence information to better detect and evaluate potential threats and compromises.

- CRI.DE.AE-07.02 - Contextual Analysis.02:  
NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-07.02:

Relevant event data is packaged for subsequent review and triage and events are categorized for efficient handling, assignment, and escalation.

#### References

- NIST Cybersecurity Framework - <https://www.nist.gov/cyberframework>
- CRI Profile v2.0 - <https://cyberriskinstitute.org/the-profile/>
- NIST CSF 1.1 Archive - <https://www.nist.gov/cyberframework/csf-11-archive>

# NIST CSF 2.0 DE.AE-08 - Incident Declaration

<b>NIST CSF 2.0</b>  <b>DE.AE-08</b>  <b>Incident Declaration</b>	<b>Other Requirements</b> N/A
---	----------------------------------

## Policy

The organization will implement internal controls to satisfy the following requirement:

DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria.

## Guidance

Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Apply incident criteria to known and assumed characteristics of activity in order to determine whether an incident should be declared

Ex2: Take known false positives into account when applying incident criteria

NIST CSF 2.0 - Informative References:

CRI Profile v2.0: DE.AE-08  
CRI Profile v2.0: DE.AE-08.01  
CSF v1.1: DE.AE-5  
SP 800-53 Rev 5.1.1: IR-04  
SP 800-53 Rev 5.1.1: IR-08

## Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

## Related Internal Controls

- CRI.DE.AE-08.01 - Incident Declaration:  
NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.AE-08.01:

Defined criteria and severity levels are in place to facilitate the declaration, escalation, organization, and alignment of response activities to response plans within the organization and across relevant third parties.

## References

- NIST Cybersecurity Framework - <https://www.nist.gov/cyberframework>



- CRI Profile v2.0 - <https://cyberriskinstitute.org/the-profile/>
- NIST CSF 1.1 Archive - <https://www.nist.gov/cyberframework/csf-11-archive>

# NIST CSF 2.0 DE.CM-01 - Network Monitoring

<b>NIST CSF 2.0</b>  <b>DE.CM-01</b>  <b>Network Monitoring</b>	<b>Other Requirements</b> N/A
---	----------------------------------

## Policy

The organization will implement internal controls to satisfy the following requirement:

DE.CM-01: Networks and network services are monitored to find potentially adverse events.

## Guidance

Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Monitor DNS, BGP, and other network services for adverse events

Ex2: Monitor wired and wireless networks for connections from unauthorized endpoints

Ex3: Monitor facilities for unauthorized or rogue wireless networks

Ex4: Compare actual network flows against baselines to detect deviations

Ex5: Monitor network communications to identify changes in security postures for zero trust purposes

NIST CSF 2.0 - Informative References:

CIS Controls v8.0: 13.1  
CRI Profile v2.0: DE.CM-01  
CRI Profile v2.0: DE.CM-01.01  
CRI Profile v2.0: DE.CM-01.02  
CRI Profile v2.0: DE.CM-01.03  
CRI Profile v2.0: DE.CM-01.04  
CRI Profile v2.0: DE.CM-01.05  
CRI Profile v2.0: DE.CM-01.06  
CSF v1.1: DE.CM-1  
CSF v1.1: DE.CM-4  
CSF v1.1: DE.CM-5  
CSF v1.1: DE.CM-7  
SP 800-53 Rev 5.1.1: AC-02  
SP 800-53 Rev 5.1.1: AU-12



SP 800-53 Rev 5.1.1: CA-07  
SP 800-53 Rev 5.1.1: CM-03  
SP 800-53 Rev 5.1.1: SC-05  
SP 800-53 Rev 5.1.1: SC-07  
SP 800-53 Rev 5.1.1: SI-04

### **Responsibilities**

The Security Officer is responsible for ensuring the implementation of this policy.

### **Related Internal Controls**

- CIS13.1 - Centralize Security Event Alerting: Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

### **References**

- NIST Cybersecurity Framework - <https://www.nist.gov/cyberframework>
- CIS Critical Security Controls - <https://www.cisecurity.org/controls>
- CRI Profile v2.0 - <https://cyberriskinstitute.org/the-profile/>
- NIST CSF 1.1 Archive - <https://www.nist.gov/cyberframework/csf-11-archive>

# NIST CSF 2.0 DE.CM-02 - Physical Environment Monitoring

<b>NIST CSF 2.0</b>  <b>DE.CM-02</b>  <b>Physical Environment Monitoring</b>	<b>Other Requirements</b> N/A
--	----------------------------------

## Policy

The organization will implement internal controls to satisfy the following requirement:

DE.CM-02: The physical environment is monitored to find potentially adverse events.

## Guidance

Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Monitor logs from physical access control systems (e.g., badge readers) to find unusual access patterns (e.g., deviations from the norm) and failed access attempts

Ex2: Review and monitor physical access records (e.g., from visitor registration, sign-in sheets)

Ex3: Monitor physical access controls (e.g., locks, latches, hinge pins, alarms) for signs of tampering

Ex4: Monitor the physical environment using alarm systems, cameras, and security guards

NIST CSF 2.0 - Informative References:

CRI Profile v2.0: DE.CM-02  
CRI Profile v2.0: DE.CM-02.01  
CSF v1.1: DE.CM-2  
SP 800-53 Rev 5.1.1: CA-07  
SP 800-53 Rev 5.1.1: PE-03  
SP 800-53 Rev 5.1.1: PE-06  
SP 800-53 Rev 5.1.1: PE-20

## Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

## Related Internal Controls

- CRI.DE.CM-02.01 - Physical Environment Monitoring:  
NIST CSF 2.0 Informative Reference - CRI Profile v2.0 - DE.CM-02.01:



The organization's controls include monitoring and detection of anomalous activities and potential intrusion events across the organization's physical environment and infrastructure, including the detection of environmental threats (fire, water, service outages, etc.) and unauthorized physical access to high-risk system components and locations.

#### References

- NIST Cybersecurity Framework - <https://www.nist.gov/cyberframework>
- CRI Profile v2.0 - <https://cyberriskinstitute.org/the-profile/>
- NIST CSF 1.1 Archive - <https://www.nist.gov/cyberframework/csf-11-archive>



# NIST CSF 2.0 DE.CM-03 - Personnel Activity Monitoring

## NIST CSF 2.0

## DE.CM-03

## Personnel Activity Monitoring

## Other Requirements

N/A

### Policy

The organization will implement internal controls to satisfy the following requirement:

DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events.

### Guidance

Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

NIST CSF 2.0 - Implementation Examples:

Ex1: Use behavior analytics software to detect anomalous user activity to mitigate insider threats

Ex2: Monitor logs from logical access control systems to find unusual access patterns and failed access attempts

Ex3: Continuously monitor deception technology, including user accounts, for any usage

NIST CSF 2.0 - Informative References:

CIS Controls v8.0: 10.7

CRI Profile v2.0: DE.CM-03

CRI Profile v2.0: DE.CM-03.01

CRI Profile v2.0: DE.CM-03.02

CRI Profile v2.0: DE.CM-03.03

CSF v1.1: DE.CM-3

CSF v1.1: DE.CM-7

SP 800-53 Rev 5.1.1: AC-02

SP 800-53 Rev 5.1.1: AU-12

SP 800-53 Rev 5.1.1: AU-13

SP 800-53 Rev 5.1.1: CA-07

SP 800-53 Rev 5.1.1: CM-10

SP 800-53 Rev 5.1.1: CM-11

### Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.



#### **Related Internal Controls**

- CIS10.7 - Use Behavior-Based Anti-Malware Software: Use behavior-based anti-malware software.

#### **References**

- NIST Cybersecurity Framework - <https://www.nist.gov/cyberframework>
- CIS Critical Security Controls - <https://www.cisecurity.org/controls>
- CRI Profile v2.0 - <https://cyberriskinstitute.org/the-profile/>
- NIST CSF 1.1 Archive - <https://www.nist.gov/cyberframework/csf-11-archive>

#### **Truncated Sample Document**