Organizational Context Procedure (GV.OC)

PROCEDURE # CS-PROC-01	EFFECTIVE DATE January 1, 2026	APPROVED BY Insert Approver
VERSION # 2.0	LAST REVISED Insert Last Revised Date	REFERENCE NIST CSF: Organizational Context (GV.OC)

Purpose

This procedure establishes a framework for aligning cybersecurity strategies and practices with the organization's mission, objectives, and business environment. It is designed to ensure that cybersecurity initiatives support and enhance the organization's operational effectiveness, stakeholder requirements, and compliance with relevant legal and regulatory standards.

Procedure

Organizational Mission, Objectives and Activities

ORGANIZATION_NAME:

- Mission/ business process definitions and associated information protection requirements are documented by ORGANIZATION_NAME.
- Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy.
- Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes.

Critical Infrastructure Communication

Protection strategies are based on the prioritization of critical assets and resources.

The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance.

ORGANIZATION_NAME addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

External Partners Cybersecurity Roles and Responsibilities

ORGANIZATION_NAME establishes cybersecurity roles and responsibilities both internally and coordinate them with internal roles and external partners.

Cybersecurity Legal and Regulatory Requirements

The following process is followed to ensure ORGANIZATION_NAME workforce members. Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. Management is responsible for ensuring compliance with legal and regulatory compliance to cybersecurity.

Critical Services Delivery

ORGANIZATION_NAME establishes alternate telecommunications services including necessary agreements to permit the resumption of organization-defined information system operations for essential missions and business functions within organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

ORGANIZATION_NAME determines the types of protection necessary for power equipment and cabling employed at different locations both internal and external to ORGANIZATION_NAME facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings,

internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.

ORGANIZATION_NAME protects power equipment and power cabling for the information system from damage and destruction.

ORGANIZATION_NAME will outline procedures specific to their needs and infrastructure for the following:

- Redundant Cabling
- Automatic Voltage Controls

ORGANIZATION_NAME will outline procedures specific to their needs and infrastructure for the following:

- Long-Term Alternate Power Supply - Minimal Operational Capability
- Long-Term Alternate Power Supply - Self-Contained

Critical Services Delivery Support

Trustworthy systems are important to mission/business success. Two factors affecting the trustworthiness of information systems include:

- Security functionality (i.e., the security features, functions, and/or mechanisms employed within the system and its environment of operation).
- Security assurance (i.e., the grounds for confidence that the security functionality is effective in its application).

Assurance is also based on the assessment of evidence produced during the system development life cycle. Critical missions/business functions are supported by high-impact systems and the associated assurance requirements for such systems. ORGANIZATION_NAME selects assurance overlays that have been developed, validated, and approved for community adoption (e.g., cross-organization, government-wide), limiting the development of such overlays on an organization-by-organization basis.

ORGANIZATION_NAME can conduct criticality analyses to determine the information systems, system components, or information system services that require high-assurance solutions. Trustworthiness requirements and assurance overlays can be described in the security plans for ORGANIZATION_NAME information systems.

Supply Chain

ORGANIZATION_NAME's role in the supply chain is identified and communicated.

- ORGANIZATION_NAME identifies and protects against supply chain threats to the information system, system component, or information system service by employing safeguards as part of a comprehensive, defense-in-breadth information security strategy.
- Identify supply chain personnel in the supply chain with specific roles and responsibilities related to the secure development, delivery, maintenance, and disposal of a system or system component.

ORGANIZATION_NAME will bring together additional key information security elements of business continuity management, including:

- Implementing additional preventive detective controls for the critical assets identified to mitigate risks to the greatest extent possible.
- Identifying financial, organizational, technical, and environmental resources to address the identified information security requirements.
- Testing and updating, at a minimum, a section of the plans and processes put in place at least annually.
- Ensuring that the management of business continuity is incorporated in ORGANIZATION_NAME's processes and structure.
- Assigning responsibility for the business continuity management process at an appropriate level within ORGANIZATION_NAME.

ORGANIZATION_NAME protects against supply chain threats to the information system, system component, or information system service by employing organization-defined security safeguards as part of a comprehensive, defense-in-breadth information security strategy.

Commented [AR1]: This procedure is for reference only. Please insert process details for this procedure that is specific to your organization.

Responsibilities

In addition to the responsibilities identified on page four (4), the ISO is responsible for conducting at least an annual review of the Organizational Context Procedure, making any appropriate changes, and disseminating the updated procedure to workforce members.

Related Form(s) and Evidence

- None

References

- NIST Cybersecurity Framework v2.0: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Contact

Insert Contact Person
Insert Full Address

E: Insert Email ID P: Insert Phone No.

Procedure History

Initial effective date: January 1, 2026.