YourIT!
Your Logo Goes Here

NIST CSF Assessment

NIST CSF Identify Worksheet

Prepared for:
Your Client's Company
Prepared by:
YourIT Company

Table of Contents

Policies and Procedures

1.1 - Written Documentation

Does your organization have a written Policies and Procedures regarding cybersecurity? If yes, please attach.

No

1.2 - Security Officer

Who at your company is currently acting as the Security Officer? This will be the primary point of contact for information and events related to cybersecurity.

None

1.3 - Security Officer Contact

Enter the contact information for your Security Officer?

None

Asset Management (ID.AM)

2.1 - Physical devices and systems

An automated inventory of assets was performed as part of this assessment. The discovered assets can be seen in the Asset Inventory Worksheet. Are there additional assets that you wish to attach to this assessment? If yes, please attach files listing the additional assets.

No

2.2 - Software platforms and applications

An automated inventory of installed software was performed as part of this assessment. The discovered assets can be seen in the Application Inventory Worksheet. Are there additional software platform or application descriptions that you wish to attach to this assessment? If yes, please attach files listing the additional assets.

No

2.3 - Organizational communication and data flows

Are organizational communication and data flows mapped? Please attach supporting documentation.

No

2.4 - Cybersecurity roles and responsibilities

Are Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established in the organization's Policies and Procedures?

No

Business Environment (ID.BE)

3.1 - Role in Supply Chain

Has the organization's role in the supply chain is identified and communicated? If yes, please note when and who was notified.

No

3.2 - Role in Critical Infrastructure and Industry Sector

Has the organization's place in critical infrastructure and its industry sector is identified and communicated? If yes, please note when and who was notified.

No

3.3 - Priorities for Organizational Mission, Objectives, and Activities

Have the priorities for organizational mission, objectives, and activities are established and communicated? If yes, please note when and who was notified.

No

3.4 - Delivery of Critical Services

Have the dependencies and critical functions for delivery of critical services been established? Please attach relevant documentation.

No

3.5 - Resilience Requirements

Have the resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) been established? Please attach relevant documentation.

No

Governance (ID.GV)

4.1 - Organizational Cybersecurity Policy

Has the organizational cybersecurity policy been established and communicated? Attach copy of the cybersecurity policy.

No

4.2 - Cybersecurity Roles and Responsibilities

Are cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners? Attach copy of the cybersecurity policy and procedures.

No

4.3 - Legal and Regulatory Requirements Regarding Cybersecurity

Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed?

No

4.4 - Legal and Regulatory Requirements Regarding Cybersecurity

Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed?

No

Risk Assessment (ID.RA)

5.1 - Asset Vulnerabilities

As part of the Risk Assessment process, a scan for missing critical security patches on Windows assets was performed. On review of other systems, were any additional asset vulnerabilities identified and documented? If so, please attach documentation.

No

5.2 - Cyber Threat Intelligence

Please list any cyber threat intelligence source your organization receives information from (including NIST).

Source	URL
Mitre	www.mitre.org

Risk Management Strategy (ID.RM)

6.1 - Risk Management Strategy

A crucial part of the NIST Cyber Security framework is a clearly documented and access Risk Management Strategy. The strategy needs to be established, managed, and agreed to by organizational stakeholders. It also needs to have organizational risk tolerance determined and clearly expressed. Additionally, the organization's determination of risk tolerance should be informed by its role in critical infrastructure or sector specific risk analysis. \n Do the organizations Cybersecurity Policies and Procedures define a Risk Management Strategy that meets the above criteria ? Please attach a copy of the relevant Cybersecurity Policies and Procedures and other support documentation.

No

Supply Chain Risk Management (ID.RC)

7.1 - Supply Chain Risk Management

Does your organization have a cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders? Please attach a copy of the relevant Cybersecurity Policies and Procedures and other support documentation.

No

7.2 - Suppliers and third-party partners of information systems, components, and Services

Describe the cyber supply chain risk assessment process used to identify, prioritize, and assess suppliers and third-party partners of information systems, components, and services.

None

7.3 - Suppliers and Third-Party Partners

Are contracts with suppliers and third-party partners used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan?

No

7.4 - Assessment of Suppliers and Third-Party Partners

Are suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations? Please attach or retain records of the assessments.

No

7.5 - Response and recovery with Suppliers and Third-Party Partners

Are response and recovery planning and testing are conducted with suppliers and third-party providers? Attach any supporting documentation regarding the latest test.

No