



## **NIST CSF Implementation Guide Version 1**



[www.kncss.com](http://www.kncss.com)

(833) 562-7700

**Developed By**

# NIST CSF Implementation Guide Version 1

## Table of Contents

Version History .....	1
Foreword.....	2
NIST Cybersecurity Framework (CSF) Overview .....	3
Executive Summary.....	4
Implementing NIST CSF.....	5
Identify .....	7
Protect .....	44
Detect.....	103
Respond .....	130
Recover.....	156
Appendices.....	166
Appendix A Information Technology Agency Resources.....	167
Appendix B. Control Crosswalks .....	168
Appendix C. Informative References .....	169
Appendix D. Acronyms.....	170
Appendix E. Glossary .....	171
Appendix F. Journey To NIST CSF 2.0 .....	173
Appendix G. Templates.....	174

# Version History

Version #	Date Revised	Summary Of Changes
Version 1		N/A

## Foreword

The Internet has been the greatest technology enabler of our lifetime. Through the interconnectivity of computers, systems, and digital services, the world has been transformed many times over. However, the Internet has a dark side. Interconnected City systems and services can become a target of cyber criminals or vandals who seek to steal sensitive resident data, disrupt City services, encrypt City data for ransom, or hurt the City's reputation from a distance. Not always malicious, the same effects can occur from a misguided employee who simply discloses sensitive information unknowingly to the online public.

This rapidly changing world reinforces the importance of good cybersecurity controls, employee education, and ongoing training/testing for both malicious and misguided actors. Our audience is more than just IT professionals; this is a shared responsibility across the City workforce, with critical roles played by every City employee, City managers, and our IT professionals. More than just a listing of guidelines, the NIST Cyber Security Framework is designed for City departments to reap the maximum benefit that the Internet has to offer, while protecting us from a rapidly growing cyberthreat landscape.

## NIST Cybersecurity Framework (CSF) Overview



The NIST Cybersecurity Framework (CSF) was created as a cybersecurity risk management framework for voluntary use by critical infrastructure organizations. CSF was released in February 2014 and updated to CSF 1.1 in April 2018. The CSF was designed as a technology-neutral framework that has the flexibility and scalability to meet the needs of small to large organizations in many sectors. The CSF has been found to be very useful and effective for helping organizations understand and manage their cybersecurity risk.

The NIST CSF is arranged into five functions: **Identify**, **Protect**, **Detect**, **Respond**, and **Recover**. These five functions follow the lifecycle for managing cybersecurity risk over time. There are three parts to the framework: the **Framework Core**, the **Implementation Tiers**, and the **Framework Profiles**:

- **The core** consists of the activities, outcomes, and references that are common across sectors and critical infrastructure.
- **The implementation tiers** are the mechanisms for viewing and understanding an organization's approach to cybersecurity risk.
- **The Framework profiles** are derived from the framework core and are based on business needs from the selections made from the framework categories and subcategories. They are used to compare the current state to a future state to identify where improvements are needed.

☐ This guide is based on the NIST CSF version 1.1, as well as elements of the upcoming version 2.0 which improves upon the development of an organization's security profile by providing a standard approach to align with industry, privacy regulations, and alignment with other frameworks. Organizations are able to improve efficiency and reduce overlap by utilizing control mapping to international frameworks for example ISO 27001/27002. Once v2.0 is released any difference not included within this guide will be added to the continuous update process.

NIST, the National Institute of Science and Technology, is in the process of developing the NIST Cyber Security Framework Version 2.0 update. NIST CSF was originally created for Critical Infrastructure, but it has become a standard framework in many industries, public and private. NIST expects to release a final version in early 2024. The update to 2.0 is set to expand on the existing version, adding a new function of "Govern", as well as adding examples of implementation for each subcategory. All efforts to implement NIST CSF in an organization will only be enhanced by the eventual release of CSF 2.0.

***Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.***

## Executive Summary



The (City Name) is implementing the **NIST Cybersecurity Framework (National Institute of Standards & Technology)** throughout the (City or Department), to support compliance with the City's Information Security Policy. This document serves as a guide and a workbook for implementing the NIST Cybersecurity Framework.

### Overview of NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) can help an organization begin or improve its cybersecurity program. Built off of practices that are known to be effective, it can help organizations improve their cybersecurity posture. It fosters communication among both internal and external stakeholders about cybersecurity, and for larger organizations, helps to better integrate and align cybersecurity risk management with broader enterprise risk management processes as described in the [NISTIR 8286 series](#) (Integrating Cybersecurity and Enterprise Risk Management (ERM)).

### The NIST Cybersecurity Framework Functions

The Framework is organized by five key Functions – Identify, Protect, Detect, Respond, Recover. These five widely understood terms, when considered together, provide a comprehensive view of the lifecycle for managing cybersecurity risk over time.

- **Identify** - What processes and assets need protection?
- **Protect** - What safeguards are available?
- **Detect** - What techniques can identify incidents?
- **Respond** - What techniques can contain impacts of incidents?
- **Recover** - What techniques can restore capabilities?

**Source:** NIST Special Publication 1271, August 2021

### Organization Leadership during Implementation Process

Whether you are the sponsor, the advocate, or the project leader, your involvement from the executive level is critical to the successful implementation of the NIST CSF. During implementation, your oversight, support, and decision-making authority are key components to helping your organization implement the requirements properly, quickly, efficiently, and cost-effectively.

## Implementing NIST CSF



The **NIST CSF Framework Core** provides a set of desired cybersecurity activities and outcomes using common language that is easy to understand. The Core guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization’s existing cybersecurity and risk management processes.

### The CSF core is broken down into five functions:

1. **Identify** - Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
  
2. **Protect** - Develop and implement appropriate safeguards to ensure the delivery of critical services.
  
3. **Detect** - Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
  
4. **Respond** - Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
  
5. **Recover** - Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Below is a grid that shows the NIST CSF Functions, Categories, and the ID numbers.

Function	Category	ID
<b>Identify</b>	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
<b>Protect</b>	Identity Management & Access Control	PR.AC

	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
<b>Detect</b>	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
<b>Respond</b>	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
<b>Recover</b>	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

***Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.***



# Identify (Function)

Organizations should start their implementation of the NIST CSF by understanding what assets they have, how these assets are connected and the roles and responsibilities employees have surrounding each asset. This important business context helps organizations identify their cyber risks and will enable them to follow a risk management strategy.

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management

**Six key categories of the identify function:**

1. **Asset management** - Asset management covers what assets are in use, where they are located, and who is using them. Technology asset management also includes processes for renewing or retiring assets and for disposing of them when they are no longer needed.
2. **Business Environment** - Understanding the business context by reviewing the organization's goals, mission and operations.
3. **Governance** - Policies, procedures and processes involved in monitoring and managing the businesses legal, risk, regulatory and environmental duties.
4. **Risk Assessment** - Evaluating the risks that can affect the organization's personnel, operations and assets.
5. **Risk Management Strategy** - The risk management strategy provides a breakdown of how the organization wants to handle risk priorities, tolerances and constraints.
6. **Supply Chain Risk Management** - Understanding and managing the risks associated with the supply chain based on priorities, constraints, risk tolerances, and assumptions.

# Asset Management - ID.AM (Category)

Function	Category (ID Number)	Subcategory
<b>IDENTIFY (ID)</b>	<b>Asset Management (ID.AM):</b> The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.	<b>ID.AM-1:</b> Physical devices and systems within the organization are inventoried
		<b>ID.AM-2:</b> Software platforms and applications within the organization are inventoried
		<b>ID.AM-3:</b> Organizational communication and data flows are mapped
		<b>ID.AM-4:</b> External information systems are catalogued
		<b>ID.AM-5:</b> Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
		<b>ID.AM-6:</b> Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

**Control Owner Summary (what you are doing)**  
 The data, personnel, devices, systems, and facilities that help the organization achieve its business goals are identified and managed according to their relative importance to organizational objectives and the organization’s risk posture.

**Dependencies**

- These subcategories are unlikely to have dependencies.

**Implementation Time-frame**

- The implementation time frame for these controls will vary based on the size, complexity, and overall security posture of the organization. Larger, more complex organizations with poorer security postures will take longer to implement these controls than smaller, less complex organizations with better security postures. Organizations in higher-risk industries will also generally take longer to implement these controls than organizations in lower-risk industries.

**★ Pro Tip Note - How to do it well**

Inventories are dynamic and may not be perfect. Aim for continuous improvement and as much information as possible.

## **Asset Management - ID.AM (Category)**

### **ID.AM-1 (Subcategory): Physical devices and systems within the organization are inventoried**

Create an inventory of physical devices and systems within the agency. This can be done either automatically or manually.

One approach to inventorying physical devices and systems within an organization is to use a tool such as Microsoft System Center Configuration Manager (SCCM). SCCM can create an inventory of devices and systems, as well as their various attributes, such as operating system version, device type, and so on. Another approach is to create an inventory of physical devices and systems manually. You can do this by creating a list of all devices and systems and then gathering information about each one, such as its operating system version, device type, and other attributes.

#### **Implementation Steps:**

1. Start with using an inventory management tool if available (there are many available that can scan a network and create an inventory of assets), or a spreadsheet to create a hardware inventory of all physical devices (computers, printers, monitors, routers, firewalls, switches, etc.).
2. Capture all information about each asset including serial #, brand, model, type of assets, when acquired, when the end of life is, if known, and firmware version. See the Hardware Inventory Form template below for reference.
3. Managing this process manually can be very time-consuming, depending on the number of assets, and amount of personnel able to work on this. Using an inventory management tools is highly recommended. Enter or input all of the captured information in to an inventory management tool.

**Implementation Resources:**

- An organization’s Information Security Policy, Standards, and Procedures
- An organization’s available Asset Management applications, Asset Management databases/spreadsheets, and any available network scanning tools for inventorying assets
- An organization’s Information Technology department, personnel, or external service providers that have the tools available for scanning and inventorying assets
- An organization’s procurement department or personnel with records of asset purchases and details on the assets
- Template: Hardware Inventory Form (See Appendix)

**Notes**

|  
|  
|  
|

**ID.AM-2 (Subcategory): Software platforms and applications within the organization are inventoried**

After creating the hardware inventory, create an inventory of software platforms and applications that are installed and in use within the agency.

The inventory should identify the application name, version, publisher, and primary function. Where possible, include the number of devices the application is installed on, how many users have the application, and how many licenses have been procured. This inventory can be created either manually or by using third-party products. Software developed internally should be inventoried as well, and should include an SBOM (Software Bill of Materials).

**Implementation Steps:**

1. Start with using an inventory management tool if available (there are many available that can scan a systems and create an inventory of the software installed), or a spreadsheet to create an inventory of all software installed.
2. Capture all information about each application including vendor, version, type, and licenses.
3. Managing this process manually can be very time-consuming, depending on the number of systems and applications installed, and amount of personnel able to work on this. Use of inventory management tools is highly recommended.

**Implementation Resources:**

- An organization’s Information Security Policy, Standards, and Procedures

## Appendix B. Control Crosswalks

### ISO 27001

The current version of NIST CSF aligns with the ISO/IEC 27001:2013 standard. As the new version of NIST CSF 2.0 comes out it will be aligned to the new ISO/IEC 27001:2023 standard.

Download the NIST CSF to ISO/IEC 27001:2013 Mapping in Excel or PDF below.

### NIST CSF to ISO/IEC 27001:2013 Control Mapping (PDF)

[NIST CSF to ISO-IEC 27001-2013 Mapping.pdf](#)

### NIST CSF to ISO/IEC 27001:2013 Control Mapping (Excel)

NIST CSF to ISO/IEC 27001:2013

Practice	Category	Subcategory	ISO Reference
IDENTIFY (CS)	Asset Management (CA.M)	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	15.10-5 Physical devices and systems within the organization are inventoried
IDENTIFY (CS)	Asset Management (CA.M)	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	15.10-5 Software platforms and applications within the organization are inventoried
IDENTIFY (CS)	Asset Management (CA.M)	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	15.10-5 Organizational personnel and data flows are mapped
IDENTIFY (CS)	Asset Management (CA.M)	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	15.10-6 External information resources are managed
IDENTIFY (CS)	Asset Management (CA.M)	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	15.10-6 Supplier (e.g., service, device, data, and software) are prioritized based on their classifications, criticality, and business value
IDENTIFY (CS)	Asset Management (CA.M)	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	15.10-6 Cybersecurity risks and vulnerabilities for the entire ecosystem (e.g., suppliers, partners, partners) are established
IDENTIFY (CS)	Business Requirement (CB.M)	The organization's mission, objectives, stakeholders, and activities are understood and prioritized. This information is used to inform cybersecurity risk, responsibility, and risk management decisions.	15.10-1 The organization's role in the supply chain is identified and documented
IDENTIFY (CS)	Business Requirement (CB.M)	The organization's mission, objectives, stakeholders, and activities are understood and prioritized. This information is used to inform cybersecurity risk, responsibility, and risk management decisions.	15.10-4 Dependence and critical functions for delivery of critical services are established
IDENTIFY (CS)	Business Requirement (CB.M)	The organization's mission, objectives, stakeholders, and activities are understood and prioritized. This information is used to inform cybersecurity risk, responsibility, and risk management decisions.	15.10-5 Resilience requirements to support delivery of critical services are established
IDENTIFY (CS)	Governance (CA.G)	The policies, procedures, and programs to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	15.07-1 Organizational information security policy is established
IDENTIFY (CS)	Governance (CA.G)	The policies, procedures, and programs to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	15.07-2 Information security rules & response (rules) are established and aligned with internal rules and external partners
IDENTIFY (CS)	Governance (CA.G)	The policies, procedures, and programs to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	15.07-3 Incident response requirements regarding cybersecurity, including primary and civil (law) obligations, are understood and managed
IDENTIFY (CS)	Risk Management (CA.R)	The organization's operational risks (including mission, functions, image, or reputation, organizational assets, and capabilities)	15.10-1 Asset vulnerabilities are identified and documented
IDENTIFY (CS)	Risk Management (CA.R)	The organization's operational risks (including mission, functions, image, or reputation, organizational assets, and capabilities)	15.10-2 Asset vulnerability information is provided from information sharing forums and events
IDENTIFY (CS)	Risk Management (CA.R)	The organization's operational risks (including mission, functions, image, or reputation, organizational assets, and capabilities)	15.10-6 Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
DETECT (CM)	Anomaly and Events (CA.E)	Unauthorized activity is detected in a timely manner and the potential impact of events is understood.	15.08-5 Detect events are monitored to understand attack tactics and methods
DETECT (CM)	Anomaly and Events (CA.E)	Unauthorized activity is detected in a timely manner and the potential impact of events is understood.	15.08-5 Anomaly detection activities are monitored to detect potential cybersecurity events

### Zero Trust Architecture

Download the Zero Trust Architecture to NIST CSF Categories Mapping in PDF below.

### Zero Trust Architecture to NIST CSF Categories Mapping

[ZTA to CSF Map.pdf](#)



## Appendix D. Acronyms

<b>Acronym</b>	<b>Meaning</b>
ANSI	American National Standards Institute
CEA	Cybersecurity Enhancement Act of 2014
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technology
CPS	Cyber-Physical Systems
CSC	Critical Security Control
DHS	Department of Homeland Security
EO	Executive Order
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IoT	Internet of Things
IR	Interagency Report
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
OT	Operational Technology
PII	Personally Identifiable Information
RFI	Request for Information
RMP	Risk Management Process
SCRM	Supply Chain Risk Management
SP	Special Publication

## Appendix E. Glossary

<b>Term</b>	<b>Definition</b>
Buyer	The people or organizations that consume a given product or service.
Category	The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Identity Management and Access Control,” and “Detection Processes.”
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.
Control	Controls are the means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature. Reference: NIST SP 800-160 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach
Control Owner	The person(s) that are responsible to implementing the Functions, Categories, and Sub-Categories
Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks.
Cybersecurity Event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
Cybersecurity Incident	A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the “Cybersecurity Framework.”
Framework Core	A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.
Framework Implementation Tier	A lens through which to view the characteristics of an organization’s approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.
Framework Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.



<b>Term</b>	<b>Definition</b>
Function	One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify, Protect, Detect, Respond, and Recover.
Identify (function)	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Informative Reference	A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory. An example of an Informative Reference is ISO/IEC 27001 Control A.10.8.3, which supports the “Data-in-transit is protected” Subcategory of the “Data Security” Category in the “Protect” function.
Mobile Code	A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.
Protect (function)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Privileged User	A user that is authorized (and, therefore, trusted) to perform security- relevant functions that ordinary users are not authorized to perform.
Recover (function)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
Respond (function)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Management	The process of identifying, assessing, and responding to risk.
Subcategory	The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”
Supplier	Product and service providers used for an organization’s internal purposes (e.g., IT infrastructure) or integrated into the products of services provided to that organization’s Buyers.
Taxonomy	A scheme of classification.

**Primary Source: NIST Glossary** <https://csrc.nist.gov/glossary>

## **Appendix F. Journey To NIST CSF 2.0**

### **NIST Cyber Security Framework (CSF) Version 2.0**

On August 8, 2023, The National Institute of Science and Technology (NIST) released the Initial Public Draft (IPD) of the NIST Cyber Security Framework 2.0. The last update was in 2018. The Initial Public Draft release allows for the public to submit comments on the proposed revisions, to which NIST will then review and consider making additional revisions and then release the official version. NIST CSF was created for Critical Infrastructure, but it has become a standard framework in many industries, public and private. NIST expects to release a final version in early 2024.

With the release of the IPD, NIST has shown that it is responding to the public comments asking for greater guidance on implementation, as well as bringing it up to date with the current technical and threat environment, and for threats that are emerging, such as supply chain risk. Of the proposed changes for version 2.0, the major changes are as follows:

1. Expanding the scope from critical infrastructure to broad applicability from small to large organizations, in the public sector and private.
2. Expansion from the original five functions of identify, protect, detect, respond, and recover, to now include a govern function. Govern focus on cybersecurity strategy and enterprise risk management.
3. Expanding on the guidance for implementation through the creation of the profiles which determine what aspects of CSF need to be implemented. Implementation examples have been added to the subcategories.
4. Focus added on continuous improvement through the addition of an Improvement category within the Identify function.

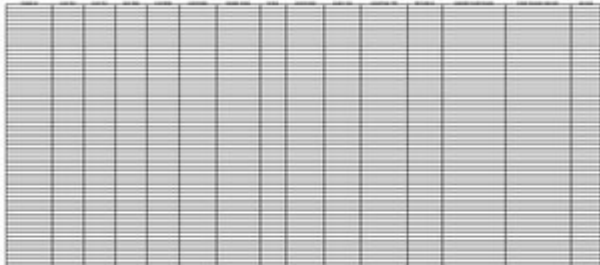
## Appendix G. Templates

Template links require viewing this document in Adobe Acrobat.

- ID.AM-1 Hardware Inventory Form
- ID.AM-2 Software Inventory Form
- ID.AM-3 Example Data Flow Diagrams
- ID.AM-4 External Information Systems Form
- ID.AM-5 Business Impact Analysis Form
- ID.AM-6 Roles and Responsibilities (RACI Matrix) Form
- ID.BE-1 Supplier Assessment Form
- ID.BE-2 Industry Sector Summary Form
- ID.BE-3 Company Mission, Objectives, and Activities Summary Form
- ID.BE-4 Critical Dependencies and Functions Form
- ID.BE-5 Resiliency and Disaster Recovery Summary Form
- ID.GV-1 Acceptable Use Policy User Agreement Form
- ID.GV-2 Roles and Responsibilities (RACI Matrix) Form
- ID.GV-3 Legal and Regulatory Requirements Form
- ID.GV-4 Governance, Risk, and Compliance Framework Form
- ID.RA-1 Vulnerability Management Process
- ID.RA-2 Threat Intelligence Program
- ID.RA-3 Risk Register Form
- ID.RA-4 Business Impact Assessment (BIA) Form
- ID.RA-5 Risk Assessment Form
- ID.RA-6 Residual Risk Assessment
- ID.RM-1 Risk Management Stakeholder Communications
- ID.RM-2 Organizational Risk Tolerance
- ID.RM-3 Critical Infrastructure and Sector Risk Assessment
- ID.SC-1 Cyber Supply Chain Stakeholders
- ID.SC-2 Cyber Supply Chain Risk Assessment
- ID.SC-3 Cyber Supply Chain Contractual Requirements
- ID.SC-4 Cyber Supply Chain Compliance Assessment
- ID.SC-5 Supply Chain Tabletop Exercise

**ID.AM-1 Hardware Inventory Form**

Capture the key details about all organizational hardware assets.

A large, empty grid representing a hardware inventory table. The grid consists of approximately 15 columns and 25 rows, with a light gray border around each cell.

[ID.AM-1 Hardware Inventory Form.xlsx](#)

**ID.AM-2 Software Inventory Form**

Capture the key details about all organizational software assets.

Department	Software Type (OS, System, Application)	Software Name	Software Vendor	Software Version	Licenses / Copies
------------	--	---------------	-----------------	------------------	-------------------

[ID.AM-2 Software Inventory Form.xlsx](#)