Federal Zero Trust Data Security Guide: Appendices

OCTOBER 2024

federal CDO council

CISO Council

CIO.GOV

TABLE OF CONTENTS

TABLES

RESOURCES

CISA PUBLICATIONS

- CISA Zero Trust Maturity Model, https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
- CISA BOD 18-02: Securing High Value Assets, https://www.cisa.gov/news-events/directives/bod-18-02-securing-high-value-assets

EXECUTIVE ORDERS

- EO 14028 on *Improving the Nation's Cybersecurity*, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- EO 13744 on *Making Open and Machine Readable the New Default for Government Information*, https://obamawhitehouse.archives.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government-

LAWS

- FISMA 2014, https://www.congress.gov/bill/113th-congress/senate-bill/2521
- HIPAA 1996, https://www.congress.gov/bill/104th-congress/house-bill/3103/text
- The E-Government Act of 2002, https://www.congress.gov/bill/107th-congress/house-bill/2458
- The Foundations for Evidence-Based Policy Making Act of 2018, https://www.congress.gov/bill/115th-congress/house-bill/4174
- The Paperwork Reduction Act of 1980, https://www.congress.gov/96/statute/STATUTE-94/STATUTE-94-Pg2812.pdf
- The Privacy Act of 1974, https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf

NIST PUBLICATIONS

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf
- NIST Cybersecurity Framework (CSF) 2.0, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

- NIST Privacy Framework, https://www.nist.gov/privacy-framework
- NIST Risk Management Framework (RMF), https://csrc.nist.gov/projects/risk-management/about-rmf
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, https://csrc.nist.gov/pubs/sp/800/39/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 800-60, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf
- NIST SP 800-63, *Digital Identity Guidelines*, https://pages.nist.gov/800-63-3/
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, https://csrc.nist.gov/pubs/sp/800/122/final

OMB CIRCULARS

- OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, https://obamawhitehouse.archives.gov/omb/circulars_a123_rev
- OMB Circular A-130, *Managing Information as a Strategic Resource*, https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource

OMB GUIDANCE

- OMB M-03-22: *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2003/m03_22.pdf
- OMB M-16-17: *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-17.pdf
- OMB M-17-12: *Preparing for and Responding to a Breach of Personally Identifiable Information*, https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf
- OMB M-18-16: *Appendix A to OMB Circular No. A-123, Management of Reporting and Data Integrity Risk*, https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-16.pdf
- OMB M-19-03: *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*, https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf
- OMB M-19-18: *Federal Data Strategy — A Framework for Consistency*, https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-18.pdf

- OMB M-21-27: *Evidence-Based Policymaking: Learning Agendas and Annual Evaluation Plans*, https://www.whitehouse.gov/wp-content/uploads/2021/06/M-21-27.pdf
- OMB M-22-09: *Moving the U.S. Government Towards Zero Trust Cybersecurity Principles*, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
- OMB M-23-04: *Establishment of Standard Application Process Requirements on Recognized Statistical Agencies and Units*, https://www.whitehouse.gov/wp-content/uploads/2022/12/M-23-04.pdf
- OMB M-24-14: *Administration Cybersecurity Priorities for the FY 2026 Budget*, https://www.whitehouse.gov/wp-content/uploads/2024/07/FY26-Cybersecurity-Priorities-Memo_Signed.pdf

OTHER

- A Framework for Data Quality, https://nces.ed.gov/FCSM/pdf/FCSM.20.04_A_Framework_for_Data_Quality.pdf
- Business Reference Model of Federal Enterprise Architecture, https://obamawhitehouse.archives.gov/omb/e-gov/FEA
- CDO Council Data Inventory Report, https://resources.data.gov/assets/documents/CDOC_Data_Inventory_Report_Final.pdf
- DATA Act Information Model Schema (DAIMS), https://resources.data.gov/standards/catalog/daims/
- DCAT-US v1.1, https://resources.data.gov/resources/dcat-us/
- DCAT-US v3.0 Schema, https://github.com/DOI-DO/dcat-us
- Desirable Characteristics of Data Repositories for Federally Funded Research, https://www.whitehouse.gov/wp-content/uploads/2022/05/05-2022-Desirable-Characteristics-of-Data-Repositories.pdf
- Digital Identity Risk Assessment (DIRA), U.S. Agency for International Development, https://www.usaid.gov/digitalstrategy/dira
- General Records Schedules, https://www.archives.gov/records-mgmt/grs
- Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions, CHCO Council, https://www.chcoc.gov/content/guidance-assigning-new-cybersecurity-codes-positions-information-technology-cybersecurity
- Guide for Mapping Types of Information and Systems to Security Categories, https://doi.org/10.6028/NIST.SP.800-60r2.iwd
- Joint Knowledge Online Login; Search for DoD course “US005” — DAU ZT for Executives, https://jkodirect.jten.mil/Atlas2/page/login/Login.jsf

- National Cyber-Informed Engineering Strategy, U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf

- National Cyber Workforce and Education Strategy, Office of the National Cyber Director, https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf

- National Cybersecurity Strategy, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

- NIEMOpen, https://www.niem.gov/

GLOSSARY

Data and security practitioners must understand each other's nomenclature to effectively safeguard their agencies' data and enable appropriate use. Table 1 outlines terms that can have slight variations in definition depending on their interpretation from a security or data management perspective.

TABLE 1: Glossary

Term	Definition from Security Perspective	Definition from Data Perspective
Data discovery	Identifying where sensitive data is located, such as endpoint and cloud applications.	Finding and cataloging data sources, such as databases, data warehouses, and data lakes. You may see this referred to as data ingestion.
Data categorization	This is sometimes used interchangeably with data classification. It may be used to describe data type, such as "invoice," "memo," or "intake form."	Identifying the categories of the data assets.
Data classification	Identifying what data is sensitive and tagging/labeling that data, then determining the risk to the organization if the data is exposed by sensitivity level. The purpose is to inform the appropriate data controls (including automation), handling practices, and third-party requirements.	Identifying data type.
Data tagging or labeling	This may be used in reference to data classification, with tags/labels, such as "public" vs. "internal" vs. "highly restricted." It could reference tags/labels such as "PII" vs. "Finance data" vs. "HR data." The purpose is to inform the appropriate data controls (including automation) and handling practices.	Tagging/labeling for informing business use purposes, such as use of tags in a data catalog. *See Appendix A for more details.*
Data inventory	Discovery, categorization, classification, and mapping of data flows. You'll often see this term used in the context of privacy compliance.	Making a list of all data assets and gathering the technical metadata. *See Appendix A for more details.*

Data governance	This can be viewed as security and privacy controls and processes, though this is only one aspect of data governance.	An umbrella term and theme covering multiple competencies, including master data management, data quality, data retention, data integrity, data democratization, data literacy, and data compliance and risk. It may also include capabilities like data definitions, policies, quality, stewardship, literacy, regulatory requirements, ethical considerations, risk management, privacy and security, and end-to-end lifecycle management.
Data integrity	Preventing data tampering or manipulation.	Related to data accuracy and quality.
Data protection	Often viewed as data security controls, in addition to related data handling processes/ practices meeting privacy compliance requirements. Focus is primarily on ensuring data confidentiality.	This could be viewed as synonymous with data security.

APPENDIX A: DATA INVENTORY

A.1: A DATA INVENTORY AND DATA CATALOG ARE COMPLEMENTARY YET DISTINCT

While “data inventory” and “data catalog” are often used interchangeably, it’s important to understand that they are not the same. In April 2022, the CDO Council released the Enterprise Data Inventories Report[1] which highlights the distinction between these two artifacts:

> “Although the terms ‘data catalog’ and ‘data inventory’ are often used synonymously, they mean very different things. A data catalog is the mechanism that helps users discover the data assets that are found in the data inventory. The data catalog contains such information as the organizational ownership of data assets, its meaning to the organization (business metadata), and where and how to access it. However, a data inventory can contain more technical and granular metadata such as the definitions of specific data elements, their format, valid values, and their completeness. While the concepts are distinct, they are complementary.”

The report notes that agencies should plan on maintaining *both* a data inventory and a data catalog.

Table 2 provides a summary of the differences between a data inventory and data catalog.

TABLE 2: Data Inventory vs. Data Catalog: Definitions

Aspect	Data Inventory	Data Catalog
Definition	Details the type and location of each data point in an organization	References an organization’s datasets in various categories for search and discovery
Scope	Helps map an organization’s data, primarily for compliance with regulations	Enables data search and discovery of data assets, with the right context. It also ensure data quality, integrity, and reliability
Users	IT teams use it to find and map all essential data assets	Technical and business users use it to access the right data and extract insights
Key difference	Includes the technical metadata associated with each data asset	Includes all metadata types — technical, business, operational, and social

[1] CDO Council Data Inventory Report, https://resources.data.gov/assets/documents/CDOC_Data_Inventory_Report_Final.pdf

Top benefits	**Transparency and awareness** IT teams know what data their organizations collect, store, and use, including dark data	**A single source of truth** Serves as a central repository for everyone within an organization to find and access the data they need
	Trustworthy data IT teams can trace data origins and verify its authenticity and credibility	**High-quality, timely, and trustworthy data** Automates lineage and propagates policies through lineage; creates automatic data profiles and runs automated quality checks frequently to spot anomalies or inconsistencies in data
	Legal compliance for sensitive data Helps with legal and regulatory compliance by finding and mapping sensitive data	**End-to-end governance and data democratization** Helps with compliance by enabling granular (column-level) access controls, lineage mapping, tag-based access policies, and automated PII data classification
Relationship	A data inventory involves identifying all the data of an organization. It is the first step toward creating a data catalog	Inventorying data is an essential aspect of data catalogs. They're created after identifying the data within an organization's warehouses and lakes

A.2: FEDERAL REQUIREMENTS TO CREATE AN ENTERPRISE DATA INVENTORY

The need to maintain an accurate data inventory and catalog is emphasized in multiple Federal documents and communities. The CDO Council's report, "Enterprise Data Inventories: Agencies face challenges and opportunities to increase the value of data assets when implementing data inventories," provides a comprehensive list of statutory requirements for creating an enterprise data inventory.

*The **Foundations for Evidence-Based Policymaking Act of 2018 (Evidence Act)** calls for a systematic rethinking of how the Federal government manages and uses the information it collects, emphasizing strong agency coordination for the strategic use of data. Specifically, Title II of the Evidence Act is the **Open, Public, Electronic and Necessary (OPEN)** Government Data Act (an Act within an Act), which lays out certain agency responsibilities, including the requirement for a comprehensive data inventory.*

A.3: THE FOUNDATION OF AN ENTERPRISE DATA INVENTORY AND ENTERPRISE DATA CATALOG

Oversight/governance authority. Creating an accurate data inventory requires the support and accountability of all stakeholders. A multi-disciplinary, cross-functional agency group that manages the enterprise data inventory to ensure uniform processes increases the likelihood of successful agency adoption.

Identify metadata (i.e., data about data assets). Agencies should use a business-oriented metadata collection approach when conducting data inventory and catalog. The metadata should include data processes, sources, purposes, storage locations, subjects, types, and why, where, and how the data is entering the agency's system. This metadata allows the agency to craft policies, ensure compliance with applicable laws, and understand the risk to, from, and in the data. *See Chapter 3.1 in the Federal Zero Trust Data Security Guide for more details about data risks.*

Periodically review workflows and practices. To prevent the inventory and catalog metadata from becoming stale and losing value, it is essential to conduct regular reviews of workflows and practices. This maintenance is also crucial for ensuring that data security policies are up to date, align with current use cases, and meet changing requirements and needs. A data inventory and catalog are snapshots in time and — since data is constantly moving through its lifecycle – the inventory and catalog metadata will likely change.

A.4: PRIORITIZING THE MANUAL POPULATION OF AN ENTERPRISE DATA INVENTORY OR ENTERPRISE DATA CATALOG

Practitioners should begin with what may already exist inside their agency. If there is no automation tool to create the inventory and catalog, practitioners will need to manually create the data inventory and then move to the data catalog. The agency's privacy team may already have a **Governance, Risk, and Compliance (GRC)** tool populated with a starter set of data catalog information. At a minimum, the GRC tool should identify all agency **high value assets (HVAs)**. Agency HVAs and their associated data assets, typically structured and semi-structured data, should be the first entries in the data inventory and data catalog. Practitioners may also prioritize manually populating the data inventory and data catalog with the FISMA risk level data.

A.5: STEPS TO MANUALLY CREATE AN INITIAL ENTERPRISE DATA INVENTORY OR ENTERPRISE DATA CATALOG WHEN THE AGENCY HAS A GOVERNANCE, RISK, AND COMPLIANCE TOOL

1. Consult the privacy team and a technical data steward with access to the agency's GRC tool to obtain a report of the agency HVAs and the contact information of responsible technical data stewards and technical **subject matter experts (SMEs)**.

2. Collaborate with the technical data stewards and SME(s) to obtain the data inventory for the system and gather metadata.

3. Complete data gathering for all HVAs and put the information in a common tool (e.g., Word, Excel, or CSV file).

4. Repeat the above steps for all FISMA High Impact systems, then Moderate Impact systems, and lastly Low Impact systems.

5. Establish a process for periodic review of the data inventory to ensure that it stays accurate.

If a practitioner's agency doesn't have the budget to purchase a new catalog software, there are other ways to get the process started at low cost by investing processing time to collect the information. These steps are essential so that the agency can categorize and label its data assets and then subsequently apply the appropriate security controls to protect the data assets.

The shortcoming of this manual approach is that the inventory will be limited to known data (typically structured and semi-structured) as identified in the agency's GRC tool. This may leave the inventory incomplete. It also does not provide any coverage for structured and unstructured data that are stored on on-premises agency mass storage devices, cloud locations, etc.

A.6: STEPS TO MANUALLY CREATE AN INITIAL ENTERPRISE DATA INVENTORY OR ENTERPRISE DATA CATALOG WHEN THE AGENCY DOES NOT HAVE A GOVERNANCE, RISK, AND COMPLIANCE TOOL

1. Consult the agency's technical data steward(s) to create a technical metadata[2] inventory. Enter the technical metadata inventory into a common tool (e.g., Word, Excel, or CSV document).

2. Consult the agency's business data steward(s) to create an operational metadata[3] inventory. Enter the operational metadata inventory into a common tool (e.g., Word, Excel, or CSV document).

3. Consult the agency's business data steward(s) to create a business metadata[4] inventory. Enter the business metadata inventory into a common tool (e.g., Word, Excel, or CSV document).

4. Merge the technical, operational, and business metadata inventory files into a single standard file.

5. Establish a process for periodic review of the data inventory to ensure its accuracy.

[2] IT stewards or technical users capture technical metadata. It includes descriptions of existing data assets (e.g., database, data lake, other storage layer or system), data structures (e.g., models, schemas), and data locations (e.g., virtual private cloud [VPC], on-premises). Technical metadata is extracted through data or schema exports from database management systems or other data management platforms like data integration, data quality, or Master Data Management (MDM) tools. Data & Analytics leaders and their teams use existing metadata export functions or manually capture metadata visually from user interfaces or queries to APIs. It includes file formats, media specifications, and source information, shedding light on the inner workings of the data. It also includes identifying systems, applications, databases, sources, targets, security controls, etc.

[3] Operational metadata is extracted from log files from transactional systems or data management tools and differs from technical metadata in that it is created whenever actions are taken on data. For example, if data is moved, copied, transformed, or otherwise updated, this creates operational metadata. Operational metadata is captured in a similar manner to technical data (i.e., via exports, UIs, and APIs) by Data & Analytics leaders and their teams. Log files are a common source, as data movement generates logged transactions and events. Operational metadata commonly references technical metadata as sources and targets of data actions.

[4] Business metadata is captured by business users, analysts, line-of-business owners, and enterprise architects. It starts with business glossaries, where business teams capture standard business terms, processes, and other definitions to be shared and standardized. Business metadata defines not only the business terms but also describes processes in a business context. It refers to the information that provides context and insights into how the data is used within the organization and represents the data's characteristics, origins, and relationships, enabling users to understand and interpret it accurately. Business metadata encompasses various aspects, including data definitions, lineage, classification, and governance policies.

A.7: PRIORITIZING THE INITIAL AUTOMATED DISCOVERY OF AGENCY DATA IN A DATA INVENTORY OR DATA CATALOG

If a practitioner's agency has the budget to purchase a Data & Analytics Governance tool, document the business and technical requirements to ensure alignment with mission-oriented goals and strategic objectives and compatibility with the technology landscape, such as data management tools, GRC tools, and network security boundaries. The requirements should include use cases encompassing critical data management needs, such as research and data analysis, data issue identification, and compliance management. In addition to requirements gathering, practitioners should establish standards, definitions, policies, and processes for entering data assets into the data inventory or catalog tool.

An automated tool allows for additional capabilities that enable the classification of the data against an agency's data taxonomy or data classification schema. This data taxonomy should be entered or built into the data inventory or catalog, and data stewards should be assigned by those defined data subject areas or data concepts. Once those foundational steps are complete, the agency's HVAs and their associated data assets should be entered into the automated data inventory or catalog in alignment with priorities set forth by the agency's requirements and use cases. Similar to the manual process, prioritize the population of the data inventory or catalog by information or data type with the FISMA risk level.

A.8: STEPS TO AUTOMATICALLY CREATE AN ENTERPRISE DATA INVENTORY OR ENTERPRISE DATA CATALOG

1. Run a report with the assistance of the agency's privacy team and technical data steward(s) who have access to the agency's GRC tool or a system inventory tool that includes risk information. This report will identify the agency's HVAs, the associated data stewards and technical SMEs, and the access information for each data source.

2. Establishing a robust technical architecture that depicts the data inventory or catalog components is crucial. This architecture should be designed to address the agency's data sources and outline the methods for moving the inventory from these sources into the catalog tool.

3. When planning and implementing the data inventory or catalog tool, selecting the appropriate development framework is essential. This includes building the front-end application with critical features and capabilities. These features, such as repository, search, data asset linkages, workflows, and metadata extractions, should strongly focus on data security, privacy, integrity, and compliance. This can be achieved through appropriate encryption, masking, and authorization mechanisms.

4. Establish the enterprise business glossary or the agency's data taxonomy (i.e., a collection of business terms organized into a hierarchical structure, typically parent-child relationships, used to classify the types of data and information collected by the agency).

5. Enter any relevant data standards, policies, rules, and other classification assets and information into the data inventory or catalog to establish a relationship between these items and the data inventory from source systems.

6. Working with each system’s technical data stewards and SMEs, confirm the existence of the system’s data inventory and plan the approach to accessing and obtaining it.

7. Consult the technical data stewards and technical SMEs to determine the appropriate method to extract the metadata for the data inventory. Assess the metadata volume, the storage location format, compatibility with the data inventory or catalog tool and its environment, and other import/export requirements — leverage tool capabilities to auto-discover and auto-populate metadata from sources. While the data gathering may still need curation, this can help reduce the workload upfront. Catalogs must be able to connect to and capture metadata directly from the sources.

8. Export the metadata from the source system to the data inventory or catalog platform in order of HVA systems, FISMA High Impact, FISMA Medium Impact, FISMA Low Impact systems, and other low priority systems per agency requirements and use cases.

9. Ensure the data inventory or catalog platform enables data stewards to review all their metadata periodically to ensure accuracy and timeliness. Determine an appropriate frequency for refreshes or automated updates.

10. Business/technical data stewards and SMEs should create or validate relationships between their data inventory and the agency data taxonomy, data standards, data policies, and other related data-related assets that are entered into the data inventory or catalog. They should also manage automated data classification, tagging, documentation, and lineage mapping.

The automated data inventory or catalog platform should align with the agency’s overall data governance and compliance needs and its data management goals and objectives. It is essential to have a well-established enterprise data governance framework with policies, processes, data stewardship roles, and responsibilities in place to govern the usage of the data inventory or catalog platform and ensure data security, privacy, integrity, compliance, and accountability.

APPENDIX B: DATA STEWARDSHIP

B.1: ESTABLISHING AND MATURING DATA STEWARDSHIP

Data stewardship is the role of individuals or teams across an agency to oversee the management, quality, and security of their agency's data assets. Developing and maturing an enterprise-wide data stewardship program is critical to the success of data categorization and ZT data security. Data stewardship involves the careful management and governance of data throughout its lifecycle, ensuring that data is accurate, accessible, and secure. By establishing clear roles and responsibilities for data stewards, agencies can ensure that data is consistently categorized, maintained, and protected according to defined standards.

Data governance bodies (DGBs) are essential to establishing and overseeing data stewardship programs within their respective agencies as they are required by OMB M-19-23 to set agency data policy and coordinate and support implementation of data management responsibilities with data-management actors within their respective agencies. DGBs guide the establishment of the agency's overarching strategy and framework for data governance, which includes the role of stewardship. By setting clear policies and standards, DGBs facilitate a structured approach to managing data, which is crucial for maintaining data quality, enhancing transparency, and ensuring compliance with regulatory requirements. This strategic oversight ensures that data is leveraged effectively to support decision-making and operational needs while safeguarding privacy and security.

In addition to strategy development, DGBs should provide critical oversight to ensure the data stewardship program is effectively implemented across the organization. They establish accountability by defining roles and responsibilities for data stewards who manage and categorize data assets. DGBs should also monitor the progress and effectiveness of data stewardship activities, adjusting as necessary to address emerging challenges or opportunities. By fostering a culture of data literacy and collaboration, DGBs empower data stewards to uphold best practices in data management and drive continuous improvement in how data is utilized across the agency. This comprehensive approach helps agencies maximize the value of their data assets while minimizing risks associated with data mismanagement.

Data stewards are typically selected from program offices who possess critical domain-specific or business knowledge about their data, making them uniquely qualified to oversee its management. Their deep understanding of the data's context, usage, and relevance allows them to catalog and classify it within data governance tools accurately. By leveraging their expertise, these stewards can ensure that data is properly documented, enhancing its discoverability and usability across the organization. This localized management, supported by an overarching enterprise-wide data governance policy, not only improves data quality and integrity but also aligns data governance practices with the specific operational needs of each program office, fostering a more cohesive and effective data governance framework.

B.2: TYPES OF DATA STEWARDS

When establishing a data steward program, it is beneficial to consider the creation of three distinct roles: technical, business, and information data stewards.

Technical data stewards are responsible for the more technical aspects of data management. Their primary focus is the data infrastructure, including data integration, quality, security, and governance. They ensure data is accurately and efficiently stored, processed, and maintained within the IT systems. Technical data stewards are typically well-versed in database management, data architecture, and IT policies, including a deep understanding of the FISMA risk levels associated with their systems. They work closely with IT departments to implement and uphold data standards and best practices.

On the other hand, **business data stewards** are responsible for the practical application and interpretation of data within the context of business operations. They ensure that the data meets the business needs, is accessible and usable for decision-making, and aligns with business goals. Business data stewards work closely with agency program offices and are typically experts in the specific business domain they support, understanding the data requirements, definitions, and usage within that area.

Meanwhile, **information data stewards** oversee unstructured data — data without a predefined model or organization, such as emails, documents, and multimedia files — ensuring they are categorized by data sensitivity and efficiently managed and disposed of according to established records management policies. By collaborating closely with the Senior Agency Official for Records Management, SAOP, and the Agency Records Officer, information data stewards ensure their program offices adhere to relevant records management statutes, regulations, and policies issued by NARA and OMB.

Identifying these three types of data stewards for their respective data assets is critical for advancing ZT. This data stewardship model ensures comprehensive data management, where both security and business requirements are met, enhancing the overall integrity and trustworthiness of the organization's data environment.

B.3: BUSINESS AND INFORMATION DATA STEWARDS' ROLES IN DATA CATEGORIZATION AND METADATA COMPLETION

Business and information data stewards are essential for effectively categorizing structured and unstructured data, a critical component in maturing ZT. Their expertise and in-depth knowledge of the data they manage enables precise categorization based on sensitivity, criticality, and usage. This precise categorization is vital for ZT environments, where stringent access controls are enforced, and trust is continuously verified. Accurate data categorization by stewards ensures that appropriate security measures are implemented, allowing only authorized individuals to access specific data, enhancing overall data security, and reducing risk.

It is critical that business data stewards categorize their data within data governance tools. Their intimate understanding of the data's context and relevance within the organization ensures that the categorization is both accurate and meaningful. By directly engaging in the categorization process, data stewards help maintain strict oversight and control over data access and usage, fostering trust and accountability within the organization. Equally important, information data stewards collaborate closely with program office personnel to ensure that all sensitive unstructured data generated by their program office is appropriately labeled, categorized, and protected under their agency-wide CUI and records management policies.

These data stewards play a pivotal role in completing and maintaining metadata, which is essential for effective data governance and implementing ZT. They ensure that metadata accurately describes data assets, such as defining data types, formats, sources, usage contexts, and access permissions. By meticulously cataloging this information using data governance tools, data stewards enhance data's discoverability, usability, and management across the organization. Their domain-specific knowledge allows them to provide precise and relevant metadata that aligns with their respective departments' operational needs and compliance requirements, thereby fostering a comprehensive and reliable data ecosystem.

When considering metadata completion in the context of ZT for a data steward program, several key considerations come into play:

1. Data stewards must ensure that metadata includes detailed access control information, which may include information on who can access the data, under what conditions, and for what purposes.
2. Metadata should capture the data's sensitivity and categorization levels to inform encryption and other security measures.
3. Data stewards must regularly update and audit metadata to reflect changes in data usage or regulatory requirements, ensuring that security policies remain robust and adaptive to emerging threats.
4. The NARA baseline metadata requirements, found in CFR 1236.54, should be considered a baseline for metadata. Other metadata may be captured as needed.

By addressing these considerations, data stewards help create a secure, transparent, and resilient data environment that aligns with ZT principles. Furthermore, as data stewardship matures, it facilitates the integration of advanced technologies and methodologies that bolster ZT security measures. For instance, through data stewardship, organizations can leverage automated tools for data categorization and encryption, ensuring that sensitive data is always protected. By continuously refining data management practices and incorporating feedback from data stewards, organizations can adapt to emerging threats and evolving regulatory requirements. This iterative process strengthens the security posture and ensures that data assets remain resilient against potential threats.

APPENDIX C: SECURITY MONITORING AND CONTROLS

C.1: EXAMPLE IMPLEMENTATION PLAN

Step 1: Initial Setup

- Working alongside the agency data and privacy practitioners, start by choosing a handful of sensitive data asset categories for monitoring.
- Configure system logs to record external data movement to identify if critical data is being used in a risky or unapproved manner, such as being exfiltrated.
- Review logs for accuracy and necessary follow-up actions.

Step 2: Enhanced Actions

- Set up notifications, alerts, quarantines, and blocking for the chosen data asset categories.

Step 3: Expand Coverage

- Include additional data asset categories in the monitoring system.
- Begin with logging and review before implementing further actions.

Step 4: Comprehensive Controls

- Apply the full range of security actions to the new data asset categories.

Step 5: Internal Data Flow Management

- Identify and control internal data transfers within the agency.
- Start with logging and analysis then proceed to more proactive measures.

Step 6: Continuous Improvement

- Implement controls at various points within the network and endpoints.
- Adjust actions as needed to align with mission objectives.
- Assess effectiveness of controls.

Step 7: Iterate and Expand

- Iterate with new criteria and scope.
- Expand to add new sensitive data asset categories for monitoring.

APPENDIX D: ROLES IN DATA SECURITY RISK MANAGEMENT

Table 3 provides examples of roles, responsibilities, and guidance for data security risk management.

As noted in NIST SP-800-37 Appendix D (Roles and Responsibilities), organizations have varying missions, business functions, and organizational structures. Therefore, there may be subtle differences in naming conventions for risk management roles and how risk management responsibilities are allocated among organizational personnel (e.g., multiple individuals filling a single role or one individual filling multiple roles). However, the basic functions should remain the same.

TABLE 3: Roles in Data Security Risk Management

	Who		**Does What**
	Role	**Data Role**	**Representative Responsibilities and Guidance**
Level 1: Organization	Chief Information Officer (CIO)	Data Owner	The CIO is the organizational officer responsible for establishing information security programs, allocating resources, and ensuring that risk management policies are integrated with organizational goals. The CIO is responsible for the overarching data governance strategy, ensuring that data security and privacy policies are enforced across all levels and throughout the organization.
	Chief Data Officer (CDO)	Data Owner	The CDO enables data search and discovery of data assets with the right context. The CDO also ensures data quality, integrity, and reliability.
	Agency Records Officer (ARO)	Data Custodian	AROs are operationally responsible for their agency's records management program. Federal Records Officers manage and direct records management activities for their agencies to ensure compliance with the Federal Records Act.
	Senior Agency Information Security Officers (SAISO)	Data Custodian	The SAISO develops and maintains the organization's risk management strategy while ensuring alignment with Federal and organizational policies and standards. They guide security control implementation and report risk levels to the executive leadership teams. The SAISOs ensure that data-centric risks are addressed through comprehensive security controls and that all data handling processes comply with relevant laws and policies.

Level 1: Organization	Chief Risk Officer (CRO)	Data Owner	The CRO ensures that risks are consistently identified, assessed, and mitigated across the organization and that there is clear communication between the various levels of the organization regarding risk management efforts. The CRO oversees the identification and management of data-related risks, ensuring that any potential threats to data's confidentiality, integrity, and availability are continuously monitored and mitigated across the organization.
	Executive Leadership (e.g., CEO, Agency Head, other C-suite, etc.)	Data Steward	Executive leadership ensures that the overall organizational risks are managed effectively and efficiently. This is achieved by fostering a culture of security awareness and training — a crucial step in the current data security landscape — to ensure risk and data resources are properly allocated and making informed decisions about risk tolerance and acceptance. Executive leadership sets the tone for data security and privacy within the organization, ensuring that data protection is a priority.
Level 2: Mission/Business Process	Mission or Business Owners	Data Steward	Mission and business owners are responsible for ensuring that secure systems support their operations and data that is critical to their mission is protected. They work closely across various organizational levels to ensure that risk and data management practices are in place and mission-critical functions are protected from threats. They are responsible for overseeing the enforcement of data security measures while maintaining data privacy within their operational areas. For example, this may be represented by a vertical mission capability such as a **Mission Essential Function (MEF)** or crosscutting through various operations areas, such as financial and cyber.
	Bureau/Division Leaders	Data Steward	Bureau and division leaders ensure that security and privacy measures align with mission goals. They are responsible for ensuring that risks within their domain are appropriately identified, mitigated, and communicated to higher organizational levels.
	Security/Privacy Managers	Data Processor, Data Custodian	ZT requires a consolidated view of mission and business data and metadata about the infrastructure (e.g., log data, endpoint data, and privacy). Security and privacy managers are the backbone of an organization's security and privacy. They ensure security and privacy policies and practices are implemented within the bureau's mission or business area. They are responsible for translating organization-level policies into controls.

Level 3: Information System	System Administrators	Data Processor, Data Custodian	This role involves implementing and maintaining controls on systems. System administrators ensure systems are protected with appropriate controls and identified vulnerabilities are addressed.
	Control Assessors	Data Processor, Data Custodian (Support)	Control assessors conduct assessments to verify that controls are correctly implemented and function as intended. Assessment findings are reported to system owners and authorizing officials for risk review, risk response, and system authorization to operate.
	System Owners	Data Controller, Data Owner	System owners are responsible for the overall security and risk management of systems throughout the system development lifecycle, supporting the organization's mission. The system owners ensure that controls are implemented and remain effective for systems under their control. They manage risks, monitor system performance, and report risk information to the organization. System owners play a crucial role in the creation and maintenance of system plans following organizational policies. They are also responsible for ensuring risk assessments are conducted and for responding to risk findings.
	Security and Privacy Officials	Data Processor, Data Custodian	Security and privacy officials are responsible for ensuring that daily operations follow security and privacy policies and procedures while maintaining the security and privacy posture of the system. They conduct regular system monitoring, support incident response, and report risks.

D.1: DATA ROLES AND RISK MANAGEMENT FRAMEWORK ROLES

Table 4 provides a mapping between risk management roles as defined in the NIST RMF and roles required to manage data security risks. Understanding data roles is important for data security, privacy, and risk management practitioners because it ensures that they can collectively and correctly identify responsibilities and accountability for data protection within their organization.

TABLE 4: Mapping Between Data Roles and Risk Management Roles

Data Role	Definition	NIST RMF Role(s)	NIST Reference
Data Subject	The person or entity that information is about.	While not explicitly defined in the NIST RMF, this may align with the conception references to "individuals" or "persons" whose data is collected.	N/A
Data Owner	The entity that collects or creates the data and is responsible and accountable for protecting it.	Chief Information Officer (CIO), Chief Data Officer (CDO), Chief Risk Officer (CRO), Information Owner/Steward, System Owner	NIST RMF, Appendix D
Data Controller	The entity that determines the purpose and meaning of the processing data, as well as ensuring its protection and privacy.	Information Owner/Steward, System Owner	NIST RMF, Appendix D
Data Processor	An entity that works under the direction of the owner/controller, such as an IT department, and processes data in accordance with the instructions of the data controllers and security standards.	Security/Privacy Managers, System Administrator, Security and Privacy Officers, Control Assessors	NIST RMF, Appendix D
Data Custodian	The person or entity responsible for the maintenance and care of data or data sources. For example, implementing technical controls, procedures, and systems.	Senior Agency Information Security Officers (SAISO), Security/Privacy Managers, System Administrator, Security and Privacy Officers, Control Assessors	NIST RMF, Appendix D
Data Steward	Users of the data for mission or business purposes, ensuring data quality and policy adherence.	Executive Leadership (e.g., CEO, Agency Head, other C-suite, etc.), Mission/ Business Owner, Bureau/Division Leaders	NIST RMF, Appendix D

APPENDIX E: IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT PRINCIPLES

For each of the core elements of **Identity, Credential, and Access Management (ICAM)**, data owners and operators should be aware of the essential practices and understand the underlying reason for those practices. Where applicable, each practice references important external sources of information to which the data owner or operator can consider for further information.

Identity Validation and Verification

Protection of data requires that all entities that are authorized to access data are properly identified and verified. Data owners and operators must ensure that the process of identifying users is performed in such a manner that the level of identity assurance and the level of authentication assurance are reliable and that the access granted to the user is appropriated to risk associated with the strength of the **identity assurance level (IAL)** and **authenticator assurance level (AAL)**. For public-facing users, agencies should use Digital Identity Risk Assessments, as described in NIST Special Publication 800-63,[5] to assess risk and select controls that balance security with access and usability. To understand the level of identity proofing for a given application, refer to the FICAM Digital Identity Risk Assessment Playbook.[6]

Principle of Least Privilege

Data owners and operators should conduct regular access reviews to ensure that users have only the necessary access privileges for their roles. It is the responsibility of the data owner to ensure that there is separation of duties between those that operate systems and those that back them up. This ensures that a compromise of operational accounts does not also compromise backup accounts and that they are available for recovery efforts.

For critical systems deployed in cloud services, data owners should utilize entitlement analytics, such as **cloud infrastructure entitlement management (CIEM)** tools, to provide a holistic view of permissions (entitlements) in cloud environments. Data owners have a responsibility to understand who has entitlement to systems under their control. Cloud services that operate through **application programming interfaces (APIs)** make it difficult to see the totality of permissions and it is an essential practice for critical data systems to be able to view entitlements across the cloud infrastructure to prevent unexpected lateral movement of adversaries who compromise an account.

[5] NIST SP 800-63, *Digital Identity Guidelines*, https://pages.nist.gov/800-63-3/sp800-63b.html

[6] Digital Identity Risk Assessment (DIRA), U.S. Agency for International Development, https://www.usaid.gov/digitalstrategy/dira

Data owners should assess job roles and responsibilities to determine the minimum access privileges required for each role and implement RBAC to assign access privileges to those predefined roles with appropriate responsibilities. This can be a complex and resource-intensive process and should utilize modern machine learning-assisted role analysis tools where available.

User Provisioning and Lifecycle Management

Data owners and operators should separate administrator accounts from user accounts to ensure only designated admin accounts are used for admin purposes.[7] If an individual user needs administrative rights over their workstation, use a separate account that does not have administrative access to other hosts, such as servers. Data owners and operators should use ICAM provisioning services with provisioning accounts or keys to enforce separation of duties based upon criticality of the control. Care should be given as this strategy introduces additional management overhead and is not appropriate in all environments.

Continuous Monitoring

Data owners and operators should utilize **user behavior analytics (UBA)** using either SIEM-integrated modules or through standalone capabilities when these are implemented as part of the Agency ICAM service. UBA can identify patterns and anomalies that may indicate unauthorized access or suspicious activity. Conditional access policies require users who want to access a resource to complete an action. Conditional access policies also account for common signals, such as user or group memberships, IP location information, device, application, and risky sign-in behavior identified through integration using UBA. Refer to the CISA Joint Cybersecurity Advisory *Threat Actor Leverages Compromised Account of Former Employee to Access State Government Organization*, which describes a common attack utilizing a compromised account.[8]

When implementing logging and monitoring mechanisms, data owners and operators should consider how to monitor access in such a manner as to detect potential security events. Refer to the joint CISA and NSA publication *Recommended Best Practices for Administrators*[9] section on Preparation for Implementing Best Practice, which describes key considerations for assessing an organization's logging and monitoring capability to determine which improvements are necessary to counter top threats.

[7] CISA CPG Cross-Sector Cybersecurity Performance Goals, https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf

[8] CISA Threat Actor Leverages Compromised Account of Former Employee to Access State Government Organization, https://www.cisa.gov/sites/default/files/2024-02/aa24-046a-threat-actor-leverages-compromised%20account-of%20former-employee.pdf

[9] CISA Recommended Best Practices for Administrators: Identity and Access Management, https://www.cisa.gov/sites/default/files/2023-12/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.pdf

Authentication

Implement continuous authentication mechanisms, such as adaptive authentication or risk-based authentication, to verify user identities throughout their sessions. Do layered authentication policies based on what your access management tool supports or the features of your identity architecture. Integrate MFA mechanisms to match the risk level of access. Utilize identity management systems that automate the identity verification process and provide real-time validation of user identities.

Access Control Mechanisms

Access control mechanisms are essential to the ICAM capabilities in ZT, and they traditionally have various means of implementation. RBAC defines access privileges based on job roles and responsibilities, while ABAC is used for more granular and dynamic access control based on user attributes and contextual information.

Data owners and operators should understand who in their charge should has have elevated privileges, ensuring that they use the principle of least privilege to limit user account permissions to those that are necessary to perform their job. ICAM services often offer **privileged access management (PAM)** tools to control and monitor access to privileged accounts and ensure accountability. The Enduring Security Framework has provided extensive guidance regarding best practices for administrators who are the most common users to utilize privileged access management tools.[10]

For those data owners and operators who utilize RBAC systems that map roles to specific access privileges and dynamically adjust them based on changes in job roles or responsibilities, they can refer to an ISACA resource[11] that helps them understand how to establish appropriate **segregation of duties (SoD)**. Some products can help identify where SoD should be applied but is not applied by using “role mining” techniques. Data owners and operators should ask if their organization’s ICAM capabilities offer support for role mining if they are having difficulty understanding how to create appropriate roles.

For data owners and operators that utilize ABAC mechanisms, they can consider attributes like user location, time of access, and other factors to determine access privileges so long as the attributes are available at the time the decision is made. NSA and CISA together have published a guide for securing data in the cloud[12] in which they state, “Consider utilizing a data tagging system or solution, where data is conditionally accessed via granular ABAC policies to protect data. It is also important to separate accounts that grant access to resources from those that manage them daily.”

Data owners and operators should use the ICAM capabilities that best match the data that they are trying to protect. CISA has observed that access control decisions are best made using the context in which the access request is being made and refers to CBAC which

[10] CISA Recommended Best Practices for Administrators: Identity and Access Management, https://www.cisa.gov/sites/default/files/2023-12/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.pdf

[11] A Step-by-Step SoD Implementation Guide, ISACA, https://www.isaca.org/resources/isaca-journal/issues/2022/volume-5/a-step-by-step-sod-implementation-guide

[12] CISA Secure Data in the Cloud, https://media.defense.gov/2024/Mar/07/2003407862/-1/-1/0/CSI-CloudTop10-Secure-Data.PDF

combines features of RBAC and ABAC to apply dynamic access policies using device-level signals as cues. For more information about CBAC, refer to *Secure Cloud Business Applications: Hybrid Identity Solutions Guidance*.[13]

PAM

Data owners and operators must recognize that privileged accounts require additional monitoring and control over normal users. They should identify which administrators are granted elevated privileges and should be separately managed using a PAM solution with strong identity governance in order to properly manage those users.

Data owners and operators should continue to take advantage of the tools that have been provided by CISA's CDM program that provide PAM in the manner described in the NIST Cybersecurity White Paper. Refer to the CISA: Tool Secures Privileged Access Management report for more information on how to transition from disparate information systems into a cohesive enterprise-wide approach.[14]

Integration with ZT

Data owners and operators should look for opportunities to integrate ICAM control with other components of ZT, such as network segmentation and micro-segmentation, to enforce data protection at every layer. CISA has published guidance on *Layering Network Security Segmentation*[15] that emphasizes the importance of implementing network segmentation where each subnetwork acts on its own. Data owners and operators who operate within cloud services should pay particular attention to the joint NSA and CISA guidance *Use Secure Cloud Identity and Access Management Practices*,[16] which discusses a specific threat model and associated adversary tactics and techniques. Data owners and operators should regularly assess and update access policies and controls to align with evolving ZT requirements and emerging threats.

Governance

Data owners and operators should establish or work within an already established governance framework that includes regular audits, compliance monitoring, and incident response planning to maintain the effectiveness of ICAM control. Refer to *OMB M-19-17*[17] section on "Shifting the Operating Model beyond the Perimeter" when developing a governance structure within the agency. The structure outlined in this chapter identifies a broad group of executives that operate in support of enterprise risk management to effectively drive ICAM efforts.

[13] Secure Cloud Business Applications: Hybrid Identity Solutions Guidance, https://www.cisa.gov/resources-tools/resources/secure-cloud-business-applications-hybrid-identity-solutions-guidance

[14] CISA Tool Secures Privileged Access Management, https://www.cisa.gov/sites/default/files/publications/CDM%2520Success%2520Story-CISA%2520PAM%2520Tool%2520.pdf

[15] CISA Layering Network Security through Segmentation, https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf

[16] Use Secure Cloud Identity and Access Management Processes, https://media.defense.gov/2024/Mar/07/2003407866/-1/-1/0/CSI-CloudTop10-Identity-Access-Management.PDF

[17] OMB M-19-17: *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

federal CDO council

CISO Council

CIO.GOV