MP180884

November 16, 2018

Response of The MITRE Corporation to the Request for Comments on the Cross-Agency Priority Goal: Leveraging Data as a Strategic Asset: Phase 2

For additional information about this response, please contact:
Duane Blackburn, S&T Policy Analyst
The MITRE Corporation
7596 Colshire Drive
McLean, VA 22102-7539

dblackburn@mitre.org
(434) 964-5023

This page intentionally left blank.

Introduction

The MITRE Corporation is a not-for-profit company that works across government to tackle difficult problems that challenge the safety, stability, security, and well-being of our nation through its operation of multiple federally funded research and development centers (FFRDCs) as well as public-private partnerships. With a unique vantage point working across federal, state, and local governments, as well as industry and academia, MITRE works in the public interest to discover new possibilities, create unexpected opportunities, and lead by pioneering together for public good to bring innovative ideas into existence in areas such as artificial intelligence, intuitive data science, quantum information science, health informatics, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience.

MITRE has direct experience assisting federal agencies leverage government and private-sector data to meet critical mission needs. Per the Federal Acquisition Regulation, FFRDCs can have unique access to both sensitive government data and proprietary private sector data – and both the government and the public sector have regularly trusted MITRE to access and leverage their data. Thus, we have combined and leveraged a variety of data sources in support of research, analysis, and the development of new operational capabilities on important national issues. MITRE's access to, and use of, disparate data sources has given us insight into data's untapped potential, as well as the challenges associated with greater use of government data (alone and in combination with private-sector data). Our experiences show that high-quality data combined with best practices will increase the effectiveness of the federal government, enhance accountability, and promote transparency.

MITRE agrees with the concept of basing the *Federal Data Strategy* on a collection of practices and action steps, and welcomes the opportunity provided by this Request for Comments to provide our thoughts on the draft practices.[1] The final practices will have the greatest impact when they are easily understood and it is readily apparent which apply[2] to each impacted actor within the federal data ecosystem. The currently-drafted framework, however, attempts to organize forty-seven practices around (a) five objectives, (b) ten principles, and (c) six lifecycle steps. The result is a three-dimensional matrix that requires an excessive amount of effort to fully comprehend.

As requested in the Request for Comments, MITRE has reviewed the current framework and considered how to restate and organize the practices so that they would have greater impact.[3] In so doing, we strove to reach a final product that fit on a single page, thus allowing federal agencies to orient around a set of easy-to-reference data strategy practices. This required combining[4] multiple current practices

[1] Note that this Request for Comments required an extensive amount of analysis and deliberation before a response could begin to be crafted, reviewed and finalized. Expecting all of this to be done in a complete and quality manner within 30 days is highly optimistic. We request more time to be allocated on future requests for public input, especially for these more-complex requests.

[2] The current strategy doesn't yet address this aspect, which would likely fall under phase three of the strategy development.

[3] This is the combined request of questions 1-4 in the Request for Comments. Questions 5 & 6 asked for examples and practice steps on the practices. We added these for the consolidated practices.

[4] Note that we also deleted practices 16, 35, and 36 from the draft strategy, as these were considered either self-explanatory or are already common practices.

into single, higher-level practices, which also necessitates follow-on discussion on each practice to ensure that important items and nuances aren't lost. Given that the Request for Comments stated an intention to do this already (via to-be-developed action steps), we determined this would be acceptable.

Objective	Practice #	Data Practice
Govern and Manage Data as a Strategic Asset	A	Establish an overarching Data Governance Council that spans all agencies. Establish, and connect a network of offices responsible for data management
	B	Standardize, Coordinate, and Inventory Key Data Assets. Manage them as authoritative data sources across federal government
	C	Periodically review data collection procedures to promote public trust
	D	Make data management requirements a fundamental component of contracts and agreements
Protect and Secure Data	E	Define roles and responsibilities for protecting confidentiality
	F	Make data-centric security fundamental to system design
Promote Efficient Use of Data Assets	G	Publish, maintain, and protect comprehensive data and documentation for agencies, partners, and citizens. Allow for multiple access tiers
	H	Preserve federal data by standardizing and applying metadata
	I	Promote data sharing within and across agencies and partners. Work towards a shared services platform
Build a Culture that Values Data as an Asset	J	Conduct and publish periodic assessments of federal data management maturity
	K	Educate and empower staff to increase capacity for data management and analytics
	L	Routinely assess the value of data assets and recover allowable costs
	M	Connect federal spending to the value of specific data assets
	N	Standardize and explicitly depict data investments in annual capital planning processes
Honor Stakeholder Input and Leverage Partners	O	Leverage and optimize use of private-sector data assets and services
	P	Engage end users and stakeholders directly in verifying data quality
	Q	Establish a process for members of the public to access and amend federal data about themselves
	R	Leverage public-private partnerships and collaboration

Table 1 - Consolidated Federal Data Practices

1.0 Consolidated Practices Discussion

1.A Establish an overarching Data Governance Council that spans all agencies. Establish, and connect a network of offices responsible for data management[5]

Practice Discussion:

Wholesale cultural changes in data use and management within and across federal agencies requires sustained leadership, oversight, and collaboration encouragement. While establishing the *Federal Data Strategy* is a critical step, it is also only the first step for meeting the President's Management Agenda (PMA) objectives.

The CIO Council should establish a limited-duration Data Governance Council to help it facilitate the implementation of the *Federal Data Strategy*. This Council likely cannot be prescriptive in dictating actions that individual agencies can take, but it can set objectives and timelines, assess agencies' progress and provide status updates to the CIO Council (and other elements within the Executive Office of the President[6]), foster collaboration and mutual mentoring across agencies, promote federal data assets, and highlight the government's new data use and/or sharing successes. Large Departments with multiple data assets and needs should consider creating a similar structure at the Departmental level.

Recommended Action Steps:

1. Finalize the *Federal Data Strategy*, which will clearly state overall objectives and intended outcomes.
2. Formally establish, via Executive Order or a similarly-influential means, the Data Governance Council. Specifically state its authorities, tasks, and limitations, as well as the administration's expectations for federal Departments' and Agencies' membership, participation and support of Council activities.
3. The Data Governance Council supports the finalization of the *Federal Data Strategy's* "Year 1 Action Plan", and then sets quarterly targets for individual (and groups of) federal Departments and Agencies to meet.
4. The Data Governance Council works to support and advise agencies as they work towards meeting their quarterly targets. The Council also leads public-private discussions[7] that will enable federal employees to leverage the knowledge and experiences of private sector entities.

---

[5] This practice consolidates the draft strategy's practices 1 & 24.

[6] For example:

- OSTP, on new technical standards or capability gaps
- OMB, on budgetary needs or regulation & rulemaking issues

[7] This could potentially be performed in collaboration with the to-be-developed GEAR Center.

5. The Data Governance Council provides quarterly progress reports back to the CIO Council, and updates future quarterly goals as needed.

Example(s) of Successful Implementation:

1. In the mid-2000s, federal agencies were struggling with biometric data on known and suspected terrorists (KST). Multiple federal Departments collected and used biometric data within their screening programs, but they did so using different standards and protocols. There was also no way for this critically-important data to be exchanged across the Departments. The National Science & Technology Council (NSTC)'s Subcommittee on Biometrics and Identity Management first began tackling this issue by developing a coordinated plan to foster necessary research and standards development to overcome the technical hurdles. As these efforts were underway, the NSTC collaborated with the National Security Council so that operational policies would be changed and oversight mechanisms were created to manage a new interagency KST biometrics paradigm. The President later issued National Security Presidential Memorandum 59 to solidify this new paradigm, and a unit at the Terrorist Screening Center was created to help manage real-time data exchanges between federal agencies. The EOP's sustained leadership, oversight, and collaboration encouragement on this topic, over a period of years, turned a critical gap in our national security posture into a strength – and created an interagency data governance success story.
2. An example of assigned stewardship responsibilities for ensuring data is discoverable, coordinated, interoperable, and shared is with OMB Circular No. A-16 Revised "Coordination of Geographic Information and Related Spatial Data Activities" dated August 2002. Addressing the confidentiality and integrity of spatial data is included in this Circular. The Circular affirms and describes the National Spatial Data Infrastructure (NSDI) as the technology, policies, standards, human resources, and related activities necessary to acquire, process, distribute, use, maintain, and preserve spatial data. The NSDI assures that spatial data from multiple sources (federal, state, local, and tribal governments, academia, and the private sector) are available and easily integrated to enhance the understanding of our physical and cultural world. Federal agencies and the Federal Geographic Data Committee (FGDC) carry out the activities required to implement their responsibilities as described the Circular. Certain federal agencies have lead responsibilities for coordinating the national coverage and stewardship of specific spatial data themes. The data themes in the NSDI, their description, and the responsible lead for each theme are listed in the Circular.

1.B Standardize, Coordinate, and Inventory Key Data Assets. Manage them as authoritative data sources across federal government[8]

Practice Discussion:

Agencies need to understand the data that is most critical to their missions and identify the authoritative source(s) for that data. Understanding and maintaining these sources and information

[8] This practice consolidates the draft strategy's practices 2, 5, 9, 17 & 31.

flows is the first step towards preserving data integrity and conveying data such that its veracity is consistent.[9]

Needed data often resides in multiple data stores and is leveraged by multiple federal agencies. Interagency coordination is thus required to establish data and exchange standards, business rules, and procedures for joint maintenance.

Recommended Action Steps:

1. Inventory and track key data assets across the federal government. Determine and log which of those data assets are authoritative under a specific circumstance
2. Improve data standardization and sharing capabilities
    a. Implement data standards and common vocabularies and participate in cross-agency data standards collaboration efforts
    b. Establish a process framework for:
        i. Conducting data standards identification[10]
        ii. Initiating data standards development and implementation projects
        iii. identifying opportunities for collaboration on data standards and sharing with external stakeholders
    c. Utilize common data management tools across the Agencies to facilitate interoperability and seamless exchange of data and relevant information; enhancing communication capabilities and improving the exchange, indexing and retrieval of information needed to solve problems across the federal government
    d. Develop a comprehensive standardized catalog of data assets and common vocabularies
    e. Issue guidance on the use of a new data standards and common vocabularies via Federal Register Notice (FRN)

Example(s) of Successful Implementation:

1. The FDA Data Standards Advisory Board (FDA DSAB) is charged with coordinating, planning and developing sound information management capabilities and policies within the Agency, through standardization and improved utilization of health and regulatory information. They publish and maintain an agency-wide FDA Data Standards Strategy (FDA DSS), instructing their various Centers to develop their own DSSs in alignment with the agency DSS. Cross-agency activities of the FDA DSS have included Health Level 7 involvement, implementing controlled terminology for the U.S. National Cancer Institute, and harmonizing an FDA vocabulary for use by partner agencies, among other examples.

[9] On July 13, 2018, the DoD CIO issued the "DCIO IE A&E Data-to-Decision (D2D) Initiative Volume 1: Strategy & Policy Analysis". It points to the DoD's challenges to coordinate data and information management across DoD and explicitly states that such coordination is key to unlocking "the information potential and synergies we need to gain and maintain the competitive edge over our Nation's adversaries."

[10] Implementation of existing standards should be the initial focus; changes to an existing standard may be necessary. Development of new standards should be a secondary priority.

2. The DHS Cyber Division has established a Chief Data office empowered to move its mission to becoming a data-centric, evidence-based organization. This office has assessed its data environment and established a data strategy that matures it data capabilities with appropriate considerations of its organizational context. The agency has established a data inventory to enable asset discovery and access. The agency is working to institutionalize a common lexicon and promote interoperability standards beginning with a cyber conceptual data model.
3. As part of the Federal Aviation Administration's (FAA's) mission to provide the safest, most efficient aerospace system in the world, the FAA captures, creates and shares data and information internally and with external organizations for all of its mission areas. This encompasses classes of information and data, including air traffic flight and flow, aeronautical, meteorological, and safety. Effective management of information has become critical to the FAA, as it has with any large commercial or government enterprise. In response to this situation, the FAA has introduced and is evolving practices for Enterprise Information Management (EIM). The primary components of FAA EIM are an executive level EIM Steering Committee and a set of Communities of Interest (COI) and Stewardship Communities of Practice (SCoP). COIs are focused on an information service domain and are responsible for information requirements. They work with and across FAA organizations to provide effective management of information services throughout their lifecycle. SCoPs are focused on data subject areas and translate information service requirements into a data architecture for solutions development and implementation. They work with and across FAA organizations to provide effective management of data throughout its lifecycle. The FAA has several COIs and SCoPs established and in various phases of maturity, with plans to establish additional groups.

1.C Periodically review data collection procedures to promote public trust[11]

Practice Discussion:

Data analytics are increasingly integral to solving our nation's most crucial problems. Effective military mission execution, targeted healthcare, and emergency response are examples where high-quality data analytics can save human lives. However, if the underlying data is poor – or worse, incorrect – analytics has the potential to cause harm, rather than mitigate it. As our dependence on data increases, we need to ensure that data collected is of the right quality for its intended use.

In addition, we need to be mindful of collecting the right amount of data. The bigger data sets get, the higher the risk of over-collection and including data out of context. Aggregation and automation without review can also lead to privacy and other concerns that reduce public trust and engagement.[12]

[11] This practice consolidates the draft strategy's practices 3, 4, 33 & 34.

[12] For example, the 2006 release by AOL of search keywords used by 20 million de-identified users, was sufficiently large to allow analysts to reconstruct data and identify specific individuals. https://www.nytimes.com/2006/08/09/technology/09aol.html

Recommended Action Steps:

Routinely identify agencies and key programs where the government requests (collects) and holds Personally Identifiable Information (PII) on citizens. Have an independent third party publish a report on the veracity of the data collection procedures.

Example(s) of Successful Implementation:

The General Data Protection Regulation (GDPR), as implemented in the European Union, is new and its success and impact have not been tested by time or law. However, the concept of an at-scale, international program to protect citizens' privacy, which requires more scrutiny by industry of their data holdings and the explicit consent required by the citizen, is a good example of data collection review.

1.D Make data management requirements a fundamental component of contracts and agreements[13]

Practice Discussion:

The federal government has a robust process in place for the governance of contracts – for example acquisition contracts. However, the inclusion of data management principles as part of these governance processes is often lacking. Including data management language in contracts and agreements provides a concrete understanding of how the data may be used, as well as required constraints.[14]

Recommended Action Steps:

1. Infuse data practices into federal processes for evaluating proposals and awarding contracts, as well as other official agreements.
2. Include data management requirements in relevant contracts and key agreements

1.E Define roles and responsibilities for protecting confidentiality[15]

Practice Discussion:

A common approach to privacy, or individual control over personal information, has been organized in the form of Fair Information Practice Principles (FIPPs). FIPPs have evolved over time, and they allow organizations and agencies to customize to meet their specific needs. Several federal

[13] This practice restates the draft strategy's practice 18.
[14] Example: "As this data set contains PII, it must be stored in a secure environment and encrypted while in transit and at rest."
[15] This practice restates the draft strategy's practice 11.

departments, agencies, and programs have articulated their own versions of FIPPs.[16] For example, DHS' FIPPs focus includes transparency, authority to collect and use PII, accountability, and security.[17] The focus on security is primarily to address confidentiality.

For greatest success, data confidentiality requires formalized practices and processes to ensure data is not being accessed by unauthorized individuals or parties. Data stewardship as an organizational approach formalizes roles and responsibilities to address both the confidentiality and integrity of data. Business and IT roles often already perform informal data stewardship in an organization. Formal data steward responsibilities begin with operational data stewards responsible for a given data domain. It's important for stewards to also have management support and an escalation path. This requires defining roles and responsibilities at both the management and executive levels.[18]

Recommended Action Steps:

1. Leverage FIPPs to align confidentiality specification roles and responsibilities across and within federal agencies
2. Determine and align relevant policies and business rules for access and use of various types of data
3. Assign data stewards who will coordinate data confidentiality policies and access rules; provide an escalation framework for data stewards

Example(s) of Successful Implementation:

Every executive branch agency is required to have a Senior Agency Official for Privacy (SAOP) that is a senior official at the Deputy Assistant Secretary or equivalent.[19] The SAOP's role aims to be primarily focused on risk management, accountability, and compliance with applicable data privacy laws, regulations, and policies.[20] Responsibilities of this role include policy-making around data privacy, overseeing compliance, and privacy risk reviews.[21]

---

[16] U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum**,** Memorandum 2008-01, 2008. The OMB sets forth a U.S. governmentwide version of the FIPPs in its July 2016 updates to OMB Circular A-130. The OMB version includes the same notions as the DHS FIPPs and draws out other common notions, such as Authority and Access and Amendment.

[17] See https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf

[18] For details of a common data governance framework, see Fleckenstein, M., Fellows, L. "Modern Data Strategy", Chapter 8, Springer, 2018

[19] See U.S. Office of Management and Budget (OMB), Role and Designation of Senior Agency Officials for Privacy, Memorandum M-16-24, 2016.

[20] See OMB M-16-24

[21] The 2016 revisions to OMB A-130 reiterate the SAOP role as discussed in other OMB policy and include additional privacy program responsibilities, which implies a more explicit set of responsibilities for SAOPs.

1.F Make data-centric security fundamental to system design [22]

Practice Discussion:

Traditionally, security's focus has been on limiting access to networks and systems. However, organizations are realizing that the data itself – rather than just systems – need to be secured. As a result, security is focusing on data-centric security, including encryption, data loss prevention, making data consistent and self-explanatory, and consistent data management policies across technology platforms. Other data-centric security aspects include defining up-front how data will be used, who can see it, and when they can see it. For the federal government, this focus is becoming particularly acute as data moves to cloud environments.

Recommended Action Steps:

1. Incorporate data-centric security into the organization's overall security framework
2. Include specific data-centric security metrics as part of security audits
3. Explicitly outline data-centric security in contracts and key agreements
4. Encourage the use shared service platforms that utilize consistent data-centric security, thus promoting a systems engineering view

1.G Publish, maintain, and protect comprehensive data and documentation for agencies, partners, and citizens. Allow for multiple access tiers[23]

Practice Discussion:

Multiple federal guidelines and memoranda require the federal government to share and make data transparent among and across agencies, with citizens, and with partners, understanding that multiple tiers are often required as there is no one-size-fits-all solution. For example:

- Open Data Policy—Managing Information as an Asset. This White House Memorandum from 2013, mandates that federal agencies information resources be accessible, discoverable, and usable.[24]
- White House Digital Service Playbook. This guide by the Federal CIO outlines the government's approach to digital services best practices. making information accessible, seamless, comprehensive for the public. [25]
- President's Memorandum on Transparency and Open Government. This memorandum aims to openly disclose information for citizens about what government is doing and refers to information maintained by the federal government a national asset. It calls on Executive departments and agencies to harness new technologies, to put information about their

[22] This practice restates the draft strategy's practice 15.
[23] This practice consolidates the draft strategy's practices 6, 12, 13, 14, 27, 28, 30, 32 & 37.
[24] See Presidential Memorandum "Open Data Policy – Managing Data as an Asset," May 9, 2013, https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf
[25] See "U.S. Digital Service Playbook," https://playbook.cio.gov/

operations and decisions online and readily available to the public, and solicit public feedback to identify information of greatest use to the public.[26]

To accomplish this, the government should:

- Regularly conduct and publish reviews of federal data released to ensure accuracy and completeness and to minimize the risk of re-identification for de-identified data
- Promote fair and equitable public access to federal data, including machine-readable data[27]
- Prevent monopolization; ensure public data is as accessible and usable to as many members of the public as practicable
- Either link data for qualified researchers or allowing researchers themselves to link data in support of national priorities and agency learning agendas.
- Effectively transmit insights from data to a broad set of consumers, both internal and external to the government

Recommended Action Steps:

1. Integrate the numerous federal publishing portals[28]
2. Define a unified set of access tiers; classify key data to align with this set of access tiers
3. Develop a research environment to share aggregated, anonymized data for the purposes of study and the promotion of solving problems with data
4. Establish a process for members of the public to access and amend federal data about themselves

1.H Preserve federal data by standardizing and applying metadata[29]

Practice Discussion:

It is vital for the government to be able to locate and preserve mission-critical information. This not only applies to data in systems, but increasingly to digitized content. Creating one or more standard taxonomies, such as the agency's retention schedule among others, and leveraging that taxonomy to apply metadata to information, makes information discoverable (eDiscovery) and preserves records. Applying metadata in this type of consistent manner also allows agencies to disposition outdated information that poses a potential legal liability.

---

[26] See "President's Memorandum on Transparency and Open Government—Interagency Collaboration," https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_fy2009/m09-12.pdf

[27] Making machine-readable data open and interoperable is mandated in the "Executive Order—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

[28] For example data.gov, usa.gov/statistics, healthdata.gov, and others

[29] This practice restates the draft strategy's practice 10.

Guidance and requirements for preserving data in accordance with applicable law, regulation, policy, approved records retention or disposition schedules, and operational guidance are in place. In addition to facilitating eDiscovery and retention, metadata is used to describe things such information provenance and its relationship with other information. Metadata allows users to locate data and understand its context. To be most effective, metadata needs to be standardized.

Recommended Action Steps:

1. Develop / leverage one or more enterprise taxonomies, such as the agency's retention schedule, as a basis for standard metadata
2. Work with business stakeholders, such as Legal Counsel and the FOIA team, to understand eDiscovery and information retention requirements
3. Understand the legal mandates pertaining to federal data. For example, identify which information is considered a record by NARA definition, which information is considered personally identifiable data per Privacy Act, etc.). Build this into the enterprise metadata construct
4. Leverage relevant, existing metadata and data exchange frameworks, such as Dublin Core, HL7, NIEM, or the Bureau of Fiscal Services Data Registry[30] as input for metadata standard definitions

Example(s) of Successful Implementation:

The Nuclear Regulatory Commission (NRC) uses ADAMS (Agency-wide Document Access and Management System) for records management, a state-of-the-art records management application with one central repository. NRC policy dictates that all records be maintained in ADAMS.[31]

NRC's taxonomy reflects their lines of business. They will use this for document classification and metadata. NRC emphasizes the importance of adopting a taxonomy early and attaching all records retention schedules to this taxonomy. Some records are ingested by ADAMS automatically, using the Electric Information Exchange (EIE). The record and its metadata are captured and stored according to NRC specifications.

An integral part of ADAMS is the Legacy Library which includes header or profile information that points to microfiche for non-digitized records. Microfiche film contains legacy profile information in its library and this information along with any new profile information is migrated and captured in the ADAMS Legacy Library.

ADAMS' user interface is web-based and a public version is available externally to support the FOIA process.[32] NRC employees and contractors can search for data in ADAMS with the web portal.

[30] See https://www.transparency.treasury.gov/dataset/data-registry/registry#meta-data (Accessed November 12, 2018)

[31] Some records may not be kept in ADAMS due to sensitivity. For example, records on an employee investigation will be kept in a secure human resources repository.

[32] See https://adams.nrc.gov/wba/ (Accessed November 12, 2018)

Search access is role-based and access rights are required. Search can be done on content with full text search or on metadata or a combination of both.

1.I Promote data sharing within and across agencies and partners. Work towards a shared services platform[33]

Practice Discussion:

Federal programs rarely operate in complete isolation, and data from other agencies and external parties (particularly state and local governments) are often required for federal programs to function. Obtaining access to these external datasets and merging with in-house data is often an intensive process specifically developed for each external partner. Agencies should work to identify their datasets that would be useful to others, as well as external datasets that they need, and invest in creating collaborative platforms that can make the exchanges as simplistic and long-lasting as possible.

Recommended Action Steps:

1. The Data Governance Council should identify priority domains that require focused interagency and/or public-private efforts to better facilitate the exchange of data.
2. Agencies work to identify data assets and needs for each domain
3. Develop shared services platforms for each domain
4. Platforms are then used as starting points or exemplars for additional data exchange needs by individual agencies.

Example(s) of Successful Implementation:

Federal agencies understand the importance of sharing data and are increasingly doing so internally as well as externally. One example that points to this increase is the National Information Exchange Model (NIEM).34 The NIEM model allows agencies to store their information in proprietary fashion, but promotes a common exchange standard. Exchange standards have been developed form multiple domains, including agriculture, emergency management, immigration, intelligence, trade, military operations, and others.

Perhaps even more significant, a substantial number of agencies are leveraging shared services for payroll, human resources, and financial management.35 In fact shared services have shown so much promise that the federal government has established the Unified Shared Services Management

[33] This practice consolidates the draft strategy's practices 19, 20, 21 & 29
[34] See https://www.niem.gov/ (Accessed November 12, 2018)
[35] See Federal Shared Services, https://www.cio.gov/assets/files/sofit/02.04.shared.services.pdf , Figure D2: Shared Service Providers

(USSM) group to "drive agencies to share investments in people, business processes and technology".36 Transitioning to shared services across the federal government promotes multiple useful data management practices, including the use of standard data across federal agencies and assigning value to shared data assets by charging for services based on the cost to provide these services.

1.J Conduct and publish periodic assessments of federal data management maturity[37]

Practice Discussion:

The government needs a consistent (agency and domain agnostic) means of assessing the maturity of federal efforts in implementing the *Federal Data Strategy*'s practices. Doing so will not only help identify gaps that require focused attention, but also uncover new innovations or best practices that could potentially be ported to other agencies or domains.

Numerous frameworks for data management exist, including the Federal Data Management Maturity Model published by the National Technical Information Service (NTIS).[38] This framework leverages several other industry frameworks. At least one of the referenced maturity frameworks, the CMMI Data Management Maturity Model, provides detailed steps for assessing maturity in multiple data management domains, including data quality, data governance, and others.

Recommended Action Steps:

1. Develop a Maturity Model based on one or more existing frameworks; identify specific metrics
2. Task the Data Governance Council to assess & report on the maturity of federal data activities on a regular & recurring basis.

1.K Educate and empower staff to increase capacity for data management and analytics[39]

Practice Discussion:

Educating federal employees on data management and analytics should be a key plank within the government's workforce realignment efforts[40], as numerous priority efforts ultimately rely on the use of data. It already has proven experience with a variety of leading educational tracks, including the Army War College and Senior Executive Service Candidate Development Program. The

[36] See https://www.ussm.gov/ (Accessed November 12, 2018)
[37] This practice restates the draft strategy's practice 7
[38] See https://www.ntis.gov/TheDataCabinet/assets/FDMM.pdf
[39] This practice restates the draft strategy's practice 15
[40] See https://www.performance.gov/CAP/CAP_goal_3.html (Accessed November 12, 2018)

government can create similar educational learning paths in the area of data management and analytics, either on its own, or by partnering with select institutions and influencing course material.

Educating and empowering staff to increase capacity for data management and analytics is an on-going process. Data management and analytics encompasses a variety of topics from data modeling and database design to data governance and strategies to data quality improvement to data visualization. Given the diversity of the data management and analytics world, focusing on a select set of learning paths and certifications serves as a foundation for good data management. Many institutes provide customized in-house options when training an entire unit or group at the same time is more feasible to meet an immediate knowledge need.

Recommended Action Steps:

1. Establish foundational learning paths and certifications centered on data management that go beyond data analytics
2. Identify options for education and training, such as creating a state-of-the-art federal training institution for data management, or partnering with industry (e.g. CMMI Institute, MIT Data Quality Symposium, University of Arkansas Chief Data Officer program, etc.)
3. Schedule selected options

1.L Routinely assess the value of key data assets and recover allowable costs[41]

Practice Discussion:

The federal government holds a significant amount of data – far too much to expect to work on all of it simultaneously. It must therefore be prioritized so that federal efforts are focused towards activities that will yield the greatest returns. This in turn requires that we understand the potential value of existing data, as well as the potential benefits of doing more with that data and the costs of creating those new opportunities.

A series of guiding questions can help determine the value of data assets:

- What is the risk associated with faulty or incomplete data regarding a given federal mission? For example, are lives at stake?
- If data is shared with other agencies or external partners, what is the cost of compiling and maintaining value-added data?
- Is the data idle (i.e., not being used)? By implication data that is not accessed and used has little or no value, or there are barriers preventing its discovery
- How flawed is the data? The cost of using data with low quality may be high and its value low
- What is the cost if data is lost? This cost may reveal high or low value
- How much value does a given set of archived data have?

[41] This practice consolidates the draft strategy's practices 3, 4, 33 & 34

Recommended Action Steps:

Once the questions pertaining to value are defined, they can be used to plan routine assessments as a method of monitoring data sets.

1. Define guiding questions to determine value of data assets and assign value; assign value to data assets based on risk, cost, usefulness, applicable law, regulation, policy, and operational guidance
2. Align resources in ratio to the determined value of key data assets
3. Conduct routine assessments to monitor high value data assets ensuring discovery, access, and interoperability
4. Periodically review federal data operations costs and user demand to identify cost recovery, for supporting the marginal costs of dissemination, the provision of federal labor expertise, and/or enhancement of data services

Example(s) of Successful Implementation:

Federal shared services provide a related example for determining the value of key data assets and recovering allowable costs. Shared services functions, such as payroll processing (number of employees, number of checks), budgeting (labor hours, size of budget), office space/rent (square feet of space occupied), and others have developed specific metrics on which they base their cost.[42]

1.M Connect federal spending to the value of specific data assets[43]

Practice Discussion:

Agency budgets aren't unlimited; prioritization always occurs to determine what activities should receive funding. Agencies and OMB should begin to use the value assessments of 1.L as an important element within this prioritization.

Recommended Action Steps:

The Data Governance Council, as part of its ongoing duties, should help develop, evolve, and ensure agencies are using a supported approach to data valuation as part of their budget planning process, thus ensuring that priority agency and interagency data efforts are properly funded.

[42] See http://www.gfoa.org/pricing-internal-services (accessed November 12, 2018)
[43] This practice restates the draft strategy's practice 38

Example(s) of Successful Implementation:

The NSTC coordinates the development of interagency R&D plans on priority topics. The NSTC's identified research tasks for each agency are supposed to receive priority within their annual research budget requests. OMB and OSTP staff review these budget requests, comparing them to the NSTC's priorities, to ensure necessary alignment.[44] OMB and the Data Governance Council could take on similar duties by reviewing agency's budget requests to ensure that value of data is properly taken into account.

1.N Standardize and explicitly depict data investments in annual capital planning processes[45]

Practice Discussion:

A key step to treating datasets as an asset is to denote them as one in the capital planning process. Agencies could go even further, by keeping an internal balance sheet for their key data assets.[46]

OMB's Capital Programming Guide[47] "provide(s) professionals in the Federal Government guidance for a disciplined capital programming process, as well as techniques for planning and budgeting, acquisition, and management and disposition of capital assets", including data. We suggest a similar approach for agencies' key data assets as an underpinning for the *Federal Data Strategy*.

Recommended Action Steps:

1. Routinely assess the value of key data assets, as described above
2. Explicitly denote key data assets in each agency's capital budget

1.O Leverage and optimize use of private-sector data assets and services[48]

Practice Discussion:

The private sector also maintains a significant amount of data, which agencies often have to access and use within their federal programs. Examples include safety data within the aviation space as

[44] https://www.mitre.org/sites/default/files/publications/pr-16-0916-interagency-s-and-t-leadership.pdf
[45] This practice restates the draft strategy's practice 8
[46] This concept has been suggested as an alternative to explicitly listing data assets in an organization's balance sheet. See Laney, D., "Introducing Infonomics: Valuing Information as a Corporate Asset," Gartner Research, March 21, 2012.
[47] https://www.whitehouse.gov/wp-content/uploads/2018/06/capital_programming_guide.pdf
[48] This practice consolidates the draft strategy's practices 22, 23 & 47

well as personal data that must be used to determine eligibility for federal benefits programs. In many domains, sharing of data and data-related services across federal-private sector lines remains in its infancy. Narrowing this gap would help the government provide better services to its citizens, as well as create new economic opportunities. Individual agencies, as well as interagency teams, need to continually look for opportunities to better leverage private-sector data and related services.

Recommended Action Steps:

1. Collect a library of exiting federal-private sector data sharing/service agreements that can serve as exemplars for enabling data sharing, while protecting privacy and ensuring proper oversight and controls.
2. Host regular challenge and prize competitions to encourage private sector entities to look for ways for their data to be used within federal contexts

Example(s) of Successful Implementation:

Improvements to Space Traffic Management (STM) and Space Situational Awareness (SSA) as described in Space Policy Directive 3[49] requires engagement and data sharing between industry, government and academia. Websites such as www.space-track.org are being used by the government to provide both data governance and access to shared data for improved safety across the globe.

1.P Engage end users and stakeholders directly in verifying data quality[50]

Practice Discussion:

Data quality is often misunderstood to mean that the accuracy and completeness of data needs to close to perfect, and that the timeliness of data needs to be sub-second. However, data quality needs vary and can range from raw data to highly refined and integrated data depending on the business need. For example, fraud analytics relies much more on very timely but raw data, while financial reporting relies more on highly accurate and cleansed data which may take some time to compile.

In addition, there are numerous other data quality dimensions besides accuracy, completeness, and timeliness. For example, the Massachusetts Institute of Technology (MIT), which has pioneered research in data quality over time, includes materials on Information Quality in Context and Information Quality Measurement. These include dimensions such as believability, value-added, relevancy, traceability, interpretability, and others.[51]

---

[49] https://www.whitehouse.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/ (Accessed November 12, 2018)

[50] This practice consolidates the draft strategy's practices 39, 40, 41 & 43

[51] Wang, R. Y., and Strong, D. M., "Beyond Accuracy: What Data Quality Means to Data Consumers," M. E. Sharpe, Spring 1996, http://mitiq.mit.edu/Documents/Publications/TDQMpub/14_Beyond_Accuracy.pdf

A data quality program that engages end users and other stakeholders can assist agencies to make informed choices of "quality fit for use". The ultimate outcome of ongoing data quality stakeholder input is the ability to certify the quality level of data provided. This will assure the government agencies' internal and external data consumers of the credibility of information upon which they base their decisions.

Recommended Action Steps:

1. Routinely engage internal and external stakeholders throughout the data lifecycle to assess their data quality "fit for use" needs
2. Review stakeholder feedback as part of the process for making annual and multiyear planning, programming, budgeting, and execution decisions related to data stewardship and data management
3. Monitor public perceptions including, monitoring views of the value, accuracy, and objectivity of federal data to make strategic improvements and ensure transparency about information policies and practices
4. Create a secure mechanism for citizens and corporations to contribute and verify their data. One use case might be to allow people with a disease or condition, that is not widely researched due to lack of aggregated data, to voluntarily submit and maintain their health history data for research purposes.

1.Q Establish a process for members of the public to access and amend federal data about themselves[52]

Practice Discussion:

The federal government's data about individual citizens is not always accurate, and this fact is not often known until after decisions are made that have a negative impact on the citizens. In addition, citizens often have to navigate a myriad of non-integrated platforms in which to enter and maintain data about themselves. This leads to ineffective data management and poor data quality. The Federal Data Strategy should create a central platform to enable citizens to review the data about themselves and provide a single means for those citizens to submit information to fix erroneous data.[53]

[52] This practice restates the draft strategy's practice 42

[53] Citizen-submitted change requests may need to be verified – both that the individual providing such information is authorized to do so, and – depending on the data provided – that the information itself is correct.

Recommended Action Steps:

- Choose a specific federal dataset as a pilot case for identifying and working through the process of citizens submitting change requests via a central portal on federally-held data.
- Create an inter-agency team that can provide guidance and offer support (such as verification using their data sets) throughout the pilot

Example(s) of Successful Implementation:

- The government of Sweden started, in 2012, to provide its citizens all county-funded health data through its national patient portal. Access to this portal is being rolled out country-wide with a very high satisfaction rate. The system uses a national health information exchange platform allowing each data provider to store data in proprietary form but mandating conversion to the national standard for the portal.[54]
- Credit monitoring services such as Experian, Equifax and TransUnion provide a means for people to update and correct their credit history.

1.R Leverage public-private partnerships and collaboration[55]

Practice Discussion:

The federal government increasingly leverages public-private partnerships (e.g. NASA's use of private rockets). Public-private partnerships (P3) in technology domains are particularly useful. These allows the government to remain more agile as technology changes. With regard to data for example, the mandate for federal agencies to move to cloud platforms for data storage, removes the government from having to upgrade and maintain data storage technologies.

The government should also continue exploring data exchange and integration opportunities with its commercial partners. For example, sandbox environments that allow industry researchers to combine their data with de-identified federal data have proven useful in the healthcare space. The government can also benefit from bi-directional data exchanges. For example, combining federal weather data with commercial data of big storm chasers and with social media[56] likely increases our ability overall to respond to potential weather-related emergencies. Data exchanges between the federal government and the private sector will require sustained activity and commitment. Lessons-learned, both positive and negative, on data practices should also regularly be shared across the public/private divide, as well as across different contexts. Both would benefit from long-term P3s, which agencies should regularly leverage.

---

[54] See https://www.futurehealthindex.com/2017/10/30/access-electronic-health-records/ (Accessed November 12, 2018)

[55] This practice consolidates the draft strategy's practices 44, 45 & 46

[56] The use of social media to improve emergency management has been documented. For example, see https://www.dhs.gov/sites/default/files/publications/Social-Media-EM_0913-508_0.pdf

Recommended Action Steps:

- Identify opportunities for new, as well as existing P3s, that can be amended and then leveraged to support federal data efforts
- Identify priority topics that would most benefit from P3s, and work to create them.

Example(s) of Successful Implementation:

1. The Aviation Safety Information Analysis and Sharing (ASIAS) platform serves as a central conduit for the exchange of safety information among its P3 stakeholders, which includes many commercial airlines, industry bodies, and the federal government.[57] By combining public data (like weather and air traffic management data) with digital flight data, ASIAS provides a valuable resource, both for the aviation community as well as for travelers. In combination this data allows ASIAS to be effectively leveraged for risk monitoring and vulnerability assessments.

2. In October, 2018 the National Technical Information Service (NTIS), through the NTIS Joint Venture Partnerships (JVP) program, agreed to fund an approach to better connect entrepreneurs, industry and investors with inventions created as a result of federally funded research and development.[58] Commercial partners, including Berico, Dun & Bradstreet Federal, Amazon Web Services and the Virginia Tech University Pamplin College of Business, will create a cloud-based solution that consolidates access to commercially relevant information on federal technologies and intellectual assets.

2.0 Alignment of Practices with Existing Industry Frameworks

While Section 1 of our response answers the questions posed within the RFC by presenting an approach for easily grasping data strategy practices as well as building out their foundation, we also felt it important to discuss how current data management industry frameworks align to these practices. The following presents an overview of how these industry frameworks align to data practices. We feel that having this alignment will help the government develop and implement the *Federal Data Strategy*.

2.1 Existing Data Management Frameworks

There are numerous existing data management frameworks that the government can leverage as they work to implement the final data practices. MITRE highlights some[59] of these, from both government

[57] See https://portal.asias.aero/web/guest/home (Accessed November 12, 2018)
[58] See https://www.ntis.gov/newsroom/2018/10/24/nist-awards-funds-for-cloud-based-tool-connecting-private-sector-investment-an/ (Accessed November 12, 2018)
[59] This is not a full list of existing frameworks. Many others exist to serve specialized needs.

and industry, that are routinely used to solve data issues the underlie specific operational problems. The actual selection of any particular framework depends on the specific operational problem an agency wishes to solve.

Data Management Framework Domain(s)	Relevant Data Management Framework Examples[60]
Data & Information Management Maturity	CMMI DMM, EDMC DCAM, NARA RIM, MITRE DMDF (Data Management Maturity)
Data Architecture & Modeling	TOGAF, DODAF, Zachman, MITRE Data Architecture
Data Management (Overarching)	DMBOK, MITRE DMDF, Mike 2.0, MITRE MDS
Data Quality	ISO/TS 8000-150
Data Security & Privacy	FICAM, ISO/IEC 27001:2013, ISO/IEC 27002:2013, NIST SP 800-37; NIST SP 800-53, Rev. 4
Data Standardization, Interoperability & Sharing	NIEM, DDF, Blockchain-Based Framework
Semantic Data & Information Frameworks	Dublin Core, MODS, METS, EDMC FIBO, FEA DRM

The following table describes the top existing data management frameworks that are aligned with each of the consolidated practices. Practitioners would likely leverage these frameworks while executing a given practice. Note that not every consolidated practice has an existing framework that could be leveraged, however. In these cases, the federal government has the opportunity to lead and define a baseline industry/federal framework. For example, the practice of "Make data management requirements a fundamental component of contracts and agreements", is of key importance to the overall acquisition governance process, and a framework to include data management requirements in contracts as a matter of routine is of high value to the federal government.

Practice #	Data Practice	Applicable Framework Examples
A	Establish an overarching Data Governance Council that spans all agencies. Establish, and connect a network of offices responsible for data management	MITRE MDS (Data Governance), DMBOK (Data Governance), CMMI DMM (Data Quality)
B	Standardize, Coordinate, and Inventory Key Data Assets. Manage them as authoritative data sources across federal government	MITRE MDS (Data Architecture), NIEM, FEA DRM, Mike 2.0
C	Periodically review data collection procedures to promote public trust	MITRE DMS (Data Architecture), CMMI DMM (Platform and Architecture), MITRE DMDF (Data Architecture)

[60] See Appendix for a more detailed description of these frameworks

D	Make data management requirements a fundamental component of contracts and agreements	*None, New Framework Required*
E	Define roles and responsibilities for protecting confidentiality	NIST SP 800-53, Rev. 4, MITRE DMS
F	Make data-centric security fundamental to system design	FICAM, NIST SP 800-37, ISO/IEC 27001:2013, ISO/IEC 27002:2013,
G	Publish, maintain, and protect comprehensive data and documentation for agencies, partners, and citizens. Allow for multiple access tiers	TOGAF, NIEM, FEA DRM, Dublin Core
H	Preserve federal data by standardizing and applying metadata	Dublin Core, METS, MODS
I	Promote data sharing within and across agencies and partners. Work towards a shared services platform	NIEM, HL7, DDF, Blockchain-Based Framework
J	Conduct and publish periodic assessments of federal data management maturity	CMMI DMM, EDMC DCAM, NARA RIM
K	Educate and empower staff to increase capacity for data management and analytics	*None, New Framework Required*
L	Routinely assess the value of data assets and recover allowable costs	*None, New Framework Required*[61]
M	Connect federal spending to the value of specific data assets	EDMC FIBO
N	Standardize and explicitly depict data investments in annual capital planning processes	EDMC FIBO
O	Leverage and optimize use of private-sector data assets and services	*None, New Framework Required*
P	Engage end users and stakeholders directly in verifying data quality	*None, New Framework Required*[62]
Q	Establish a process for members of the public to access and amend federal data about themselves	*None, New Framework Required*
R	Leverage public-private partnerships and collaboration	*None, New Framework Required*

[61] Information to support the development of this framework can be found in Fleckenstein, M., Fellows L., "Modern Data Strategy", Springer, 2018 Chapter 3 "Valuing Data as an Asset"

[62] Information to support the development of this framework can be found in publication ISO/TS 8000-150

Appendix – Descriptions of Existing Data Management Frameworks

Acronym	Description
Blockchain-Based Framework	Data Sharing with Fine-Grained Access Control in Decentralized Storage Systems. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8400511&tag=1
CMMI DMM	CMMI Data Management Maturity Model. CMMI Institute released the Data Management Maturity (DMM) model in 2014. This model breaks down data management into five high-level categories and one supporting category, including data management strategy, data governance, data quality, and others. https://cmmiinstitute.com/store/data-management-maturity-(dmm)-(1)
DDF	Distributed Data Framework. DDF is an interoperability platform that provides secure and scalable discovery and retrieval from a wide array of disparate sources. http://codice.org/ddf/Features.html
DMBOK	Data Management Body of Knowledge. An industry standard and overarching data management framework, published by the Data Management Association (DAMA), that segments data management into 11 knowledge areas, including data governance, data architecture, data quality, and others. https://dama.org/sites/default/files/download/DAMA-DMBOK2-Framework-V2-20140317-FINAL.pdf
DODAF	The DOD Architecture Framework (DODAF) developed by the U.S. Department of Defense is a publicly available enterprise architecture framework first developed in the 1990s. With Version 2.0, these architectural viewpoints were expanded, including the addition of a data and information view (DIV). The DIV focuses on a conceptual, logical, and physical data model, providing successive generic descriptions of these data models. http://dodcio.defense.gov/Library/DoD-Architecture-Framework/
Dublin Core	Dublin Core is a foundational standard used by other standards. It defines a small set of attributes that cover three categories: instantiation, content, and intellectual property rights. http://dublincore.org/documents/dcmi-terms/
EDMC DCAM	Data Management Capability Assessment Model. EDMC's Data Management Capability Assessment Model (DCAM) is a simple, self-assessment data management maturity model that covers maturity in component areas, including data strategy, data governance, data architecture, data quality, and technology architecture.

Acronym	Description
	https://edmcouncil.org/page/aboutdcamreview
EDMC FIBO	Financial Industry Business Ontology. FIBO is a business ontology standard that provides a business glossary (i.e., terms and relationships) for financial instruments, legal entities, market data and financial processes. https://edmcouncil.org/page/aboutfiboreview
FEA DRM	The Federal Enterprise Architecture Data Reference Model (FEA DRM) v3 classifies government data as part of the Federal Enterprise Architecture Framework. The DRM serves as a high-level common point of reference to support planning and alignment for new shared services and information sharing. The DRM was and still is meant to be a mechanism to facilitate harmonization of data across federal agencies and communities to support shared initiatives and goals. The DRM v3 resides in OMB Max.
FICAM	Federal Identity, Credential, and Access Management. Security disciplines that allows an organization to: enable the right individual to access the right resource at the right time for the right reason. https://arch.idmanagement.gov/
HL7	Health Level Seven International. HL7 is a standards body but the term HL7 is used generically to refer to the electronic health information exchange standards they create. http://www.hl7.org/
ISO/IEC 27001:2013	Information technology—Security techniques—Information security management systems — Requirements. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
ISO/IEC 27002:2013	Information technology -- Security techniques -- Code of practice for information security controls http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
ISO/TS 8000-150	specifies fundamental principles of master data quality management, and requirements for implementation, data exchange and provenance. https://www.iso.org/standard/54579.html
METS	Metadata Encoding and Transmission Standard. A standard for encoding descriptive, administrative, and structural metadata regarding objects within a digital library. http://www.loc.gov/standards/mets/METSOverview.v2.html#descMD

Acronym	Description
Mike 2.0	This is an open source information management best practices framework with core focus on business intelligence, enterprise data management, search, enterprise content management, information asset management, and information strategy/architecture/governance. Membership is free and provides access to a wide variety of industry contributions on data management. MIKE2.0 espouses the Scaled Agile Framework Architecture (SAFe), an evolutionary approach to business needs. http://mike2.openmethodology.org/wiki/What_is_MIKE2.0 A companion book, "Information Development Using MIKE2.0," is also available.
MITRE MDS	Modern Data Strategy. A reference guide with frameworks around multiple data management domains, including data governance, data architecture, records management, and others. https://www.springer.com/us/book/9783319689920 Digital version is freely available to sponsors upon request.
MITRE DMDF	MITRE's Data Management Domain Framework is an overarching data management framework that provides guidance on 26 domains, including data governance, data architecture, master data management, and others.
MODS	Metadata Object Description Schema. MODS was created by the Library of Congress and is similar in purpose to Dublin Core but it adds several attributes. http://www.loc.gov/standards/mods/
NARA RIM	NARA developed a spreadsheet-based maturity scoring model that assesses organizational maturity in management and organizational structure, policy/standards/governance, and program operations. Many areas parallel data management maturity. https://www.archives.gov/records-mgmt/prmd.html
N-Dex	National Data Exchange. N-DEx provides criminal justice agencies with an online tool for sharing, searching, linking, and analyzing information across jurisdictional boundaries. N-Dex is NIEM conformant. https://www.fbi.gov/services/cjis/ndex
NIEM	NIEM promotes enterprise-wide information exchange standards across disparate agencies and their partners. It is an XML-based framework used in the United States. Its contributors and users include federal, state, and local agencies, as well as private industry. NIEM maintains a core set of reference schemas and allows participants to publish compliant extensions and variations. Existing extensions include biometrics, emergency management, intelligence, immigration, international trade, and other areas. https://www.niem.gov

Acronym	Description
NIST SP 800-37	Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems, A Security Life Cycle Approach. The intent of the RMF is to improve data security, strengthen risk management processes, and encourage reciprocity among federal agencies. NIST SP 800-37, Rev1, Section 1.1
NIST SP 800-53, Rev. 4	Security and Privacy Controls for Federal Information Systems and Organizations. Organizes information security activities into security control families and provides over 850 controls as a resource for identifying appropriate security measures http://dx.doi.org/10.6028/NIST.SP.800-53r4
TOGAF	The Open Group Architecture Framework (TOGAF), Phase C, Chapter 10, focuses specifically on data architecture. This section, like the overall framework, contains a generic description of things needed, the steps to take, and sample outcome products, in this case, for data architecture. It also points to sample data principals, located in Section 23.6.2, Data Principles. https://www2.opengroup.org/ogsys/catalog/g116
Zachman	This two-dimensional enterprise architecture framework uses the y-axis to classify a product from contextual to detailed and the x-axis to segment products into process, data, event, organizational, geographical, and goal/rule quadrants. The data quadrants focus on products such as an entity relationship model and additional data details. https://www.zachman.com/about-the-zachman-framework