



CDO Core Competency Model

Federal Chief Data Officers Council's
Business of Data Working Group

September 21, 2026

Version History

Version	Date	Scope
1.0	September 2026	Final

Table of Contents

CDO Core Competency Model.....	1
Purpose.....	5
Scope.....	5
Introduction.....	7
Key Components.....	8
Core Competencies.....	13
Data Strategy.....	14
Data Governance.....	15
Data Management.....	16
Data Analytics and Insights.....	17
Data Security and Privacy.....	17
Leadership and Collaboration.....	18
Change Management.....	19
Innovation.....	19
Competency Levels.....	20
Knowledge, Skills, and Abilities.....	20
Assessment and Evaluation.....	23
Development and Training.....	23
Life Cycle of Data.....	25
Summation and Path Forward.....	27
References.....	29

Purpose

The purpose of this Chief Data Officer (CDO) Competency Model is to introduce and define the core competencies needed for the role, providing clear guidelines for the necessary expertise in areas such as data strategy, data management, data security, analytics, and regulatory compliance.¹ This model establishes a comprehensive framework for developing and assessing the skills, knowledge, and abilities essential for effective data governance within the government. It aims to support the professionalization of the CDO role by identifying standards for recruitment, training, and performance evaluation—ensuring CDOs are equipped to lead enterprise data governance and build the infrastructure required to support evidence-based decision-making. In particular, CDO responsibilities outlined in [OMB Memorandum M-25-05](#)², such as strengthening governance, improving data access, and enabling agency-wide interoperability, directly inform the competencies described in this model.

Scope

This CDO Competency Model applies to all individuals serving in or aspiring to the CDO role within the federal government. It promotes consistency in the qualifications and capabilities of CDOs across agencies to ensure a unified approach to data governance. In alignment with the [Foundations for Evidence-Based Policymaking Act of 2018 \(Evidence Act\)](#)³, this model outlines the essential responsibilities and qualifications required to effectively manage data within an organization. Per 44 U.S.C. § 3520, the Evidence Act establishes the statutory responsibilities of agency Chief Data Officers, including: (1) Life Cycle of Data Management; (2) data governance; (3) promoting data use in decision-making; (4) ensuring data interoperability and standardization; (5) coordinating with statistical and evaluation officials; and (6) supporting open data requirements. These statutory functions form the baseline qualifications and responsibilities that inform this Competency Model.⁴

¹ The Competency Model is a product of the Federal Chief Data Officers (CDO) Council's Business of Data Working Group. *About CDOC - Councils.gov / Federal Executive Councils*. (2018). <https://www.councils.gov/cdoc/>

² OMB Memorandum M-25-05, Phase 2 Implementation of the Evidence Act: Open Government Data Access and Management Guidance (2025).

³ Public Law 115-435 (2019).

⁴ The Federal CDO Council, established by statute under the Evidence Act and further extended in M-25-06 Re-establishing the Chief Data Officer Council, serves to establish best practices for government-wide data management, support the adoption of new technologies, and improve user access to government data.

The model emphasizes the importance of collaboration with other officials, promoting data literacy, continuous improvement, and innovation, and integrating data-driven practices across departments.⁵ It aims to equip CDOs with the necessary capabilities to support evidence-based policymaking and improve government operations through informed decision-making and strategic data use. This competency model serves as a comprehensive guideline for the recruitment, development, and evaluation of Chief Data Officers, ensuring that they are well-equipped to manage data as a strategic asset for the government. It is designed primarily for federal Chief Data Officers as a self-assessment, development, and role-alignment guide. A secondary audience includes agency leadership, HR specialists, and governing bodies responsible for supporting and overseeing CDO functions.

⁵ Other federal officials include Chief Information Officers (CIOs), Senior Agency Officials for Privacy (SAOPs), Chief Information Security Officers (CISOs), Chief AI Officers (CAIOs), among others , and more.

Introduction

Public sector organizations are under increasing pressure to improve services while ensuring transparency, accountability, and efficiency. Data plays a crucial role in helping them meet these challenges, and CDOs have become key leaders in using data to support informed decision-making. Their role has shifted from technical execution to enterprise strategy and decision support. The CDO Core Competency Model provides a practical framework for data leadership.

At the heart of the model are key components and core competencies that define a successful CDO. The model also introduces competency levels necessary for mastering data leadership. It outlines the essential skills and knowledge CDOs need, including technical expertise, strategic thinking, and governance. These foundational competencies include data strategy, data governance, analytics, and data security. Additionally, it addresses the full data lifecycle: capturing, storing, managing, analyzing, and applying data effectively. By understanding these elements, CDOs and their teams can build strong data capabilities tailored to needs across the federal enterprise, as well as the evolving needs of public- and private-sector stakeholders. Both public- and private-sector stakeholders rely on the availability, usability, and quality of federal data, reinforcing the importance of the CDO role in supporting external transparency and internal mission delivery.

Applying the CDO Competency Model

This Competency Model is intended for direct use by Federal Chief Data Officers to assess their capabilities, align development with agency priorities, and guide Evidence Act implementation activities. Agencies may apply the model by mapping each competency to statutory CDO functions, M-25-05 requirements, and mission-specific data responsibilities. Using the model in this way strengthens enterprise data governance, supports agency evaluation and statistical activities, and promotes consistent application of federal data policy across programs.⁶

⁶ Agencies may also draw on other CDO Council resources, including the [CDO Playbook Advancing the Federal Data Strategy](https://resources.data.gov/assets/documents/CDO_Playbook_2021.pdf) (https://resources.data.gov/assets/documents/CDO_Playbook_2021.pdf), which details best practices for data management. Additional resources include the [Data Catalog Vocabulary \(DCAT\)-US Schema v3.0](https://resources.data.gov/resources/dcat-us3/) (<https://resources.data.gov/resources/dcat-us3/>), reference documentation for the DCAT-US v3.0's federal metadata standards for documenting datasets, APIs, and data services; as well as the [Zero Trust Data Security Guide](https://resources.data.gov/assets/documents/Zero-Trust-DataSecurityGuide_RevisedMay2025_CIO.govVersion.pdf) (https://resources.data.gov/assets/documents/Zero-Trust-DataSecurityGuide_RevisedMay2025_CIO.govVersion.pdf) outlining best practices for strengthening data security.

Key Components

Understanding the scope and expectations of the CDO role within government agencies provides a foundation for identifying the essential competencies required for effective performance. To ensure that CDOs can fulfill their responsibilities and drive strategic data initiatives, it is crucial to focus on five key components of competency: skills, knowledge, abilities, behaviors, and attributes.⁷ These components collectively enable CDOs to manage data as a strategic asset, support evidence-based policymaking, and enhance government operations. The following sections describe each of these components to outline what makes an effective and successful CDO.

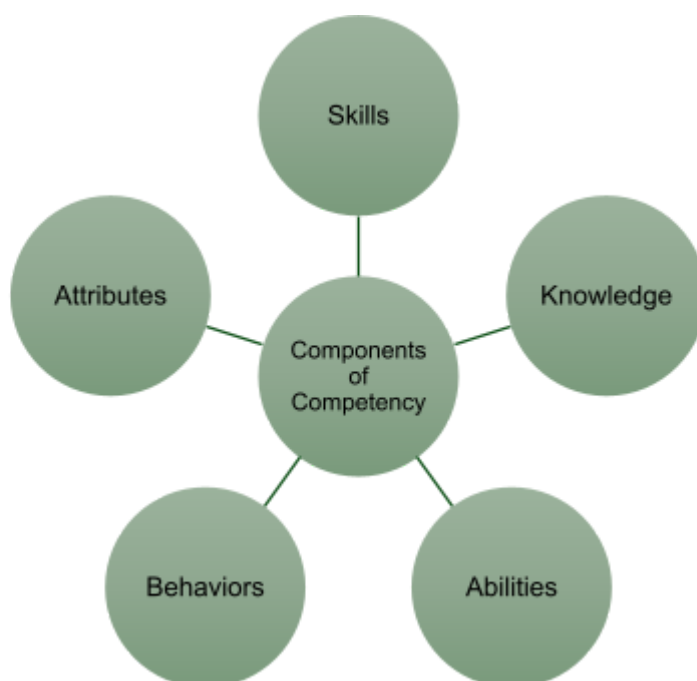


Figure 1. Five key components of competency. The five key components of competency are skills, knowledge, abilities, behaviors, and attributes.

Skills

Skills represent the practical abilities that individuals acquire through repeated practice and experience. They are crucial for performing specific tasks and roles effectively. Skills can be broadly classified into two categories: technical skills and soft skills.

⁷ These competency domains are adapted from the Federal Data Strategy (<https://strategy.data.gov/>), the [Evidence Act](#) (44 U.S.C. § 3520), and various CDO Council working group products.

Technical Skills: These are specialized abilities that require specific knowledge and expertise. In the context of a CDO, technical skills might include data analysis, coding, database management, and proficiency in data visualization tools. Technical skills enable a CDO to handle complex data systems, perform detailed analysis, and create meaningful reports and visualizations that inform decision-making.

Soft Skills: These are interpersonal and relational abilities that facilitate effective communication and collaboration. For a CDO, essential soft skills might include leadership, teamwork, communication, problem-solving, and adaptability. Soft skills are vital for leading cross-functional teams, fostering a collaborative work environment, and effectively communicating data-driven insights to stakeholders at all levels of government.

Together, technical and soft skills equip a CDO with the capabilities needed to navigate the technical complexities of data management while also leading and inspiring their team to achieve organizational goals.

Knowledge

Knowledge refers to the theoretical and practical understanding of a subject. It includes facts, information, principles, and context relevant to a specific area of expertise.. Knowledge is typically acquired through formal education, training programs, reading, research, and practical experience.

Theoretical Knowledge: This involves understanding the fundamental concepts and principles that form the foundation of a particular field. For a CDO, this might include knowledge of data governance frameworks, data lifecycle management, statistical methods, and data privacy laws.

Domain-Specific Knowledge: This is specialized knowledge pertinent to a specific government sector. For example, a CDO responsible for data governance must be knowledgeable about regulations and guidelines set by the Office of Management and Budget (OMB) and the Federal Data Strategy, ensuring compliance with federal data policies and best practices.

Practical Knowledge: This involves applying theoretical knowledge to real-world situations. It includes understanding how to implement data management tools, best practices for data security, and techniques for data analysis and visualization. Practical knowledge is often gained through hands-on experience and problem-solving in professional settings.

Continuous Learning: The field of data is constantly evolving, with new technologies, methodologies, and regulations emerging regularly. Therefore,

continuous learning is crucial for a CDO to stay updated with the latest advancements and maintain their expertise. This can involve attending workshops, participating in webinars, obtaining certifications, and engaging with professional communities.

Together, these facets of knowledge enable a CDO to make informed decisions, develop effective data strategies, and ensure compliance with relevant regulations, ultimately enhancing the organization's ability to leverage data as a strategic asset.

Abilities

Abilities refer to the natural or developed capacities that individuals possess, enabling them to perform various tasks effectively. These capacities can be categorized into cognitive, physical, and emotional abilities, each playing a crucial role in different aspects of job performance.

Cognitive Abilities: These are mental capabilities that influence how individuals think, learn, and solve problems. Examples include critical thinking, analytical reasoning, problem-solving, and decision-making. For a CDO, cognitive abilities are essential for analyzing complex datasets, developing data strategies, and making informed decisions that drive organizational success.

Physical Abilities: These involve the physical capacity to perform tasks that require bodily movement and coordination. Although physical abilities are generally less central to the CDO role, they may be relevant in limited operational contexts, such as oversight of physical data storage facilities or hardware environments. However, in most cases, the emphasis for a CDO is more on mental rather than physical prowess.

Emotional Abilities: These encompass the capacity to understand, manage, and express emotions effectively. Emotional abilities include empathy, emotional intelligence, and interpersonal skills. For a CDO, emotional abilities are crucial for leading and motivating teams, managing stakeholder relationships, and fostering a positive organizational culture. Being able to empathize with team members and stakeholders helps build trust and cooperation, which are vital for successful data governance and management.

Developed Abilities: While some abilities may be inherent, many can be developed and enhanced through training, practice, and experience. Continuous learning and professional development are essential for honing abilities and staying competitive in a rapidly evolving field like data management.

By leveraging a combination of cognitive, physical, and emotional abilities, a CDO can effectively navigate the complexities of data governance, lead their teams with confidence, and drive meaningful organizational change.

Behaviors

Behaviors refer to the observable actions or responses of an individual in various situations. They demonstrate how skills and knowledge are applied in real-world scenarios, influencing job performance and interactions with others. Understanding and cultivating positive behaviors are crucial for success in any role, including that of a CDO.

Teamwork: This behavior involves working collaboratively with others to achieve common goals. It includes effective communication, cooperation, and the ability to share responsibilities and successes. For a CDO, teamwork is essential for leading data initiatives and fostering a collaborative culture across departments.

Adaptability: The ability to adjust to new conditions and changing environments is a key behavior. Adaptability allows individuals to handle unforeseen challenges and embrace new technologies or processes. A CDO must be adaptable to stay ahead in the rapidly evolving field of data management.

Resilience: This behavior reflects an individual's capacity to recover from setbacks and remain focused on objectives. Resilience is critical for navigating the complexities and pressures associated with managing large-scale data projects and ensuring data integrity.

Problem-Solving: Effective problem-solving behaviors include identifying issues, generating solutions, and implementing them efficiently. A CDO must exhibit strong problem-solving skills to address data-related challenges and optimize data strategies.

Leadership: Demonstrating leadership behaviors means guiding and inspiring others toward achieving organizational goals. It involves setting a vision, motivating team members, and taking decisive action. A CDO must lead by example and drive data-driven decision-making within the organization.

Ethical Conduct: Upholding ethical standards and integrity is fundamental. This behavior ensures that data is managed responsibly and ethically, respecting privacy and compliance regulations. A CDO must model ethical conduct and instill a culture of trust and accountability.

Communication: Effective communication requires clear messaging, active listening, and open dialogue. A CDO needs to communicate complex data insights in a way that is understandable and actionable for various stakeholders.

These behaviors collectively enhance the ability of a CDO to perform their role effectively, ensuring that their skills and knowledge translate into tangible, positive outcomes for the organization.

Attributes

Attributes are the personal characteristics or traits that influence how an individual approaches their work and interacts with others. These innate or developed qualities play a crucial role in shaping behaviors, driving performance, and underpinning how competencies are demonstrated in practice. Key attributes for a CDO might include:

Motivation: This attribute reflects an individual's drive to achieve goals and pursue excellence. A highly motivated CDO is proactive, takes initiative, and strives for continuous improvement in data governance and management.

Integrity: Integrity involves being honest, ethical, and trustworthy. For a CDO, maintaining integrity is vital for building trust with stakeholders, ensuring compliance with regulations, and upholding data privacy and security standards.

Attention to Detail: This attribute signifies the ability to notice and address small details that can impact the quality and accuracy of data. A CDO with strong attention to detail ensures data integrity, reduces errors, and enhances the reliability of data-driven decisions.

Adaptability: Adaptability refers to the capacity to adjust to changing conditions and new challenges. A CDO must be adaptable to stay current with evolving data technologies, methodologies, and regulatory landscapes.

Leadership: Leadership as an attribute entails the ability to inspire, guide, and influence others. A CDO with strong leadership qualities can effectively lead cross-functional teams, drive strategic initiatives, and foster a collaborative work environment.

Visionary Thinking: This attribute involves the ability to foresee future trends and opportunities. A visionary CDO can anticipate changes in the data landscape, innovate solutions, and align data strategies with long-term organizational goals.

Resilience: Resilience is the capacity to recover from setbacks and persist in the face of challenges. A resilient CDO can navigate the complexities and pressures of data management, maintaining focus and determination.

Comprehension: Comprehension is the ability to understand and interpret the concerns of others. A CDO with strong comprehension can build meaningful relationships, navigate conflicts with insight, and foster a collaborative and supportive work culture.

These attributes collectively contribute to the overall effectiveness of a CDO, influencing how CDOs apply their skills and knowledge, interact with teams and stakeholders, and drive successful data initiatives.

Core Competencies

It is essential to translate these broad key components into categories of specific core competencies that define the role of a CDO. These core competencies form the foundation for effective performance, ensuring that CDOs can manage data strategically, drive evidence-based policymaking, and enhance government operations. The following section delves into the core competencies that are critical for a successful CDO.



Figure 2. Federal Chief Data Officer Core Competencies. Key competencies of successful Federal Chief Data Officers include Leadership and Collaboration, Innovation, Data Strategy, Data

Governance, Data Management, Change Management, Data Security and Privacy, and Data Analytics and Insights.

Data Strategy

Developing and implementing a comprehensive data strategy that aligns with the agency's mission is essential. Under M-25-05, federal CDOs are responsible for leading Evidence Act Phase 2 data governance and open data access activities, which serve as core anchors for agency data strategies. A robust data strategy ensures that data-related activities support the broader objectives of the agency. It involves establishing a clear vision that articulates how data will contribute to the agency's mission and strategic priorities. By setting Specific, Measurable, Achievable, Realistic, and Time-bound (SMART) goals, the strategy provides a framework for tracking progress and achieving success. Engaging key stakeholders from different departments is critical to ensure that the strategy addresses different needs and garners broad support. This collaborative approach makes data initiatives relevant and impactful. Additionally, creating a structured framework and policies for data governance, management, and usage is crucial. This framework should include data quality standards, data stewardship responsibilities, and compliance with regulatory requirements.

Ensuring that data initiatives support business objectives and add value is crucial. To achieve this, the strategy should focus on empowering the organization to make informed decisions based on accurate, timely, and relevant data by implementing analytics and business intelligence tools that provide actionable insights. It involves prioritizing data projects that align with strategic goals and allocating resources accordingly to ensure that the most critical initiatives receive the necessary support and investment. Additionally, defining key performance indicators (KPIs) to measure the impact of data initiatives on business outcomes and regularly reviewing these metrics helps adjust strategies and tactics for improved performance.

Fostering a culture of continuous improvement and innovation by leveraging new technologies and methodologies is essential. Encouraging experimentation and learning from both successes and failures enhances the organization's data capabilities. Demonstrating the tangible benefits of data initiatives, such as increased efficiency, cost savings, or enhanced customer satisfaction, is crucial. Clear communication of these benefits helps in securing ongoing support and investment for data activities. By developing a comprehensive data strategy and ensuring that data initiatives are aligned with business objectives, CDOs can maximize the value derived from data, driving organizational success and competitive advantage.

Data Governance

Data governance is a critical function that involves establishing policies, standards, and practices for effective data management. This comprehensive approach ensures that data is handled consistently and responsibly across the organization. By setting clear guidelines and protocols, data governance helps maintain data quality, security, and privacy, which are essential for building trust and compliance with regulatory requirements. Federal data governance should align with key standards and frameworks, including NIST SP 800-53, NIST SP 800-60 for information categorization, ISO/IEC 11179 for metadata registries, and the Dublin Core Metadata Initiative, as well as DCAT-US requirements.

One of the key aspects of data governance is the establishment of robust policies and standards. These policies define how data should be collected, stored, processed, and shared, ensuring consistency and accuracy. Standards are developed to maintain data quality, which includes data accuracy, completeness, reliability, and relevance. Effective data management practices are essential for achieving these standards and ensuring that data can be trusted and used effectively.

Overseeing data quality involves continuous monitoring and improvement efforts. Data stewards, data owners, and other personnel play a vital role in managing data quality by identifying and addressing issues such as data duplication, inconsistencies, and errors. Ensuring high data quality is crucial for making accurate, informed decisions and for maximizing the value of data as a strategic asset.

Data security is another critical component of data governance. This involves implementing measures to protect data from unauthorized access, breaches, and other security threats. Ensuring data security requires a combination of technical solutions, such as encryption and access controls, and organizational practices, such as regular security audits and training for employees on data protection protocols.

Privacy is also a fundamental aspect of data governance. Organizations must comply with data privacy regulations, such as GDPR, HIPAA, and CCPA, which govern how personal data is collected, processed, and stored. This includes obtaining proper consent from individuals, ensuring data is used transparently and ethically, and protecting data from unauthorized disclosure.

In summary, data governance encompasses a range of activities aimed at managing data effectively and responsibly. By establishing clear policies, standards, and

practices, and by overseeing data quality, security, and privacy, organizations can ensure compliance with regulations, build trust with stakeholders, and harness the full potential of their data assets.

Data Management

Data management involves overseeing the entire lifecycle of data, from acquisition to disposal. It ensures that data is handled efficiently and effectively at every stage. This process begins with the acquisition of data, which involves collecting data from various sources, whether internal or external. Once acquired, the data must be cleaned and validated to ensure its accuracy and reliability.

Managing the lifecycle of data also includes storage and organization. Data must be stored in a way that is both secure and accessible, allowing for easy retrieval and use. This often involves setting up databases and data warehouses, implementing backup and recovery procedures, and ensuring that data is properly indexed and categorized.

Ensuring data accuracy, consistency, and accessibility is a core aspect of data management. Accurate data is free from errors and reliably reflects the real-world conditions it represents.. Consistent data maintains uniformity across different datasets and systems, avoiding discrepancies that can lead to incorrect analyses and decisions. Accessibility ensures that data is available to authorized users whenever they need it, enabling timely and informed decision-making.

Effective data management also involves maintaining data quality through regular monitoring and validation processes. This includes identifying and correcting data errors, updating data to keep it current, and ensuring that data is consistently formatted and standardized. Data quality management tools and practices are essential for maintaining high standards of data integrity.

Finally, data disposal is an important aspect of the data management lifecycle. It involves securely deleting data that is no longer needed, in compliance with legal and regulatory requirements. Proper data disposal practices help protect sensitive information and ensure that the organization does not retain unnecessary data that could pose security risks.

By managing the lifecycle of data and ensuring its accuracy, consistency, and accessibility, organizations can maximize the value of their data assets, support informed decision-making, and maintain compliance with relevant regulations and standards.

Data Analytics and Insights

Data analytics and insights play a pivotal role in driving informed business decision-making and uncovering valuable insights. Leveraging data analytics involves using various techniques and tools to analyze data, identify patterns, and draw meaningful conclusions. This process helps organizations transform raw data into actionable insights that can inform strategic decisions, optimize operations, and uncover opportunities for innovation and growth.

By promoting the use of data-driven insights, organizations can enhance their business operations and strategies. Data-driven insights provide a factual basis for decision-making, reducing reliance on intuition and guesswork. This leads to more accurate and effective decisions that can improve efficiency, increase profitability, and drive competitive advantage. Additionally, data-driven insights enable organizations to identify trends, monitor performance, and predict future outcomes, allowing them to proactively address challenges and seize opportunities.

Encouraging a culture of data-driven decision-making involves ensuring that data analytics tools and techniques are accessible to employees at all levels of the organization. This includes providing training and resources to develop data literacy and analytical skills. By fostering an environment where data is valued and utilized effectively, organizations can maximize the potential of their data assets and achieve their strategic objectives.

Data Security and Privacy

Data security and privacy are critical components of effective data management, particularly for a CDO. Ensuring robust data protection measures is essential to safeguard sensitive information from unauthorized access, breaches, and other security threats. This involves implementing a variety of technical solutions, such as encryption, firewalls, access controls, and intrusion detection systems. Additionally, organizations must regularly conduct security audits and vulnerability assessments to identify and address potential risks. Agencies should also incorporate the [Federal Zero Trust Strategy](#) and [Zero Trust Data Security Guide](#), which outline required controls for identity, access, data segmentation, and continuous monitoring across the data lifecycle.⁸

Maintaining compliance with data privacy laws and regulations is equally important. These laws, such as the General Data Protection Regulation (GDPR), the Health

⁸ [The Federal Zero Trust Data Security Guide](#) was developed under the Office of Management and Budget (OMB) [Memorandum M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles](#) and was published jointly by the Federal CDO and the Federal Chief Information Security Officer (CISO) Councils.

Insurance Portability and Accountability Act (HIPAA), and the California Consumer Privacy Act (CCPA), establish guidelines for how personal data should be collected, processed, stored, and shared. Compliance with these regulations not only helps protect individuals' privacy rights but also helps organizations avoid legal penalties and maintain their reputation.

The Confidential Information Protection and Statistical Efficiency Act (CIPSEA), as codified under Title III of the Evidence Act, reinforces the protection of data collected for statistical purposes. It mandates strict safeguards to ensure that confidential information is used solely for authorized statistical activities and is never disclosed in identifiable form. Adhering to CIPSEA requirements helps federal agencies and their partners maintain public trust, uphold privacy commitments, and ensure that data is managed with integrity and accountability throughout its lifecycle.

Furthermore, fostering a culture of data security and privacy within the organization is crucial. This involves training employees on best practices for data protection, raising awareness about potential security threats, and establishing clear policies and procedures for handling sensitive information. By prioritizing data security and privacy, organizations can build trust with stakeholders, mitigate risks, and ensure the integrity and confidentiality of their data assets.

Leadership and Collaboration

Leadership and collaboration are critical aspects of a Chief Data Officer's (CDO) role. Leading cross-functional teams to implement data initiatives involves guiding and motivating different groups of employees from across departments. Effective leadership requires setting a clear vision, establishing goals, and ensuring that team members have the resources and support they need to achieve these objectives. It also involves fostering a collaborative culture where team members feel valued and are encouraged to share their ideas and expertise. Under OMB M-19-23, the CDO plays a central leadership role in the agency Data Governance Body, coordinating enterprise data priorities, governance standards, and interdepartmental alignment.

Collaboration with senior-level officials and directors is essential for integrating data-driven practices across government agencies. The CDO must work closely with high-ranking members of the executive team, such as the Secretary, Deputy Secretary, Chief Information Officer (CIO), and department directors, to ensure that data initiatives are aligned with the broader strategic goals of the organization. This involves regular communication and coordination to ensure that data initiatives are effectively incorporated into business processes and decision-making frameworks.

By combining strong leadership with effective collaboration, the CDO can drive the successful implementation of data initiatives, enhance the organization's data capabilities, and ensure that data is used as a strategic asset to support overall business objectives.

Change Management

Change management is a crucial aspect of effectively implementing data initiatives within an organization. It involves promoting a culture of data literacy and data-driven decision-making, ensuring that all employees understand the importance of data and how to use it effectively in their roles. This includes providing training and resources to develop the necessary skills and knowledge, fostering an environment where data is valued and utilized to inform decisions.

Additionally, change management requires leading organizational change to embrace and adopt new data practices and technologies. This involves guiding the organization through the transition, addressing any resistance to change, and ensuring that new data practices are integrated smoothly into existing workflows. Effective change management helps create a culture of continuous improvement, where new technologies and methodologies are readily adopted, and innovation is encouraged.

By promoting data literacy and leading organizational change, Chief Data Officers (CDOs) can ensure that their organizations are well-equipped to leverage data as a strategic asset, driving business success and competitive advantage.

Innovation

Innovation in data management is vital for staying competitive in a rapidly evolving technological landscape. Staying abreast of emerging data technologies and trends is a fundamental aspect of this process. This involves continuously monitoring advancements in areas such as artificial intelligence, machine learning, big data analytics, and data storage solutions. By keeping up to date with these developments, organizations can leverage the latest tools and methodologies to enhance their data capabilities.

Additionally, identifying opportunities to innovate and improve data processes is crucial for driving efficiency and effectiveness. This requires a proactive approach to evaluating current data practices and identifying areas for improvement. Whether it involves automating routine tasks, implementing more sophisticated analytics techniques, or adopting new data governance frameworks, innovation can lead to significant gains in productivity, accuracy, and insight generation.

By fostering a culture of innovation, organizations can encourage creativity and experimentation. This includes supporting initiatives that explore new ways to capture, manage, and analyze data, as well as embracing a mindset that values learning from both successes and failures. Ultimately, a focus on innovation enables organizations to stay ahead of the curve, continuously improve their data operations, and derive greater value from their data assets.

Competency Levels

The role of the CDO encompasses several key responsibilities. The CDO is tasked with developing and implementing data strategies that align with the agency's goals, ensuring robust data governance, security, and privacy, and managing the lifecycle of data from collection to dissemination. In alignment with Office of Management and Budget (OMB) [Memorandum M-19-23, "Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance"](#) and [Memorandum M-25-05 "Phase 2 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Open Government Data Access and Management Guidance"](#), the CDO plays a pivotal role in ensuring that data is effectively managed, protected, and utilized to support evidence-based policymaking and improve government operations. In the federal context, the CDO role includes responsibilities defined by statute, regulation, and OMB guidance.. The competency levels of a CDO are defined by three essential components: foundational knowledge, skills, and abilities; assessment and evaluation; and development and training. Combined, they form a dynamic framework that not only measures current performance but also identifies opportunities for continuous growth, ensuring that data leaders are well-equipped to meet current and emerging requirements.. These provide a detailed framework for understanding and advancing the essential dimensions of a CDO.

Knowledge, Skills, and Abilities

Building on the CDO core competencies, it's crucial to identify the specific Knowledge, Skills, and Abilities (KSAs) that candidates need to possess to obtain a job or succeed in a CDO role. These KSAs provide a detailed framework for the qualifications and capabilities required for effective performance, ensuring that CDOs can manage data strategically, support evidence-based policymaking, and enhance government operations. The following section will explore the KSAs essential for aspiring CDOs to demonstrate in their applications and during their tenure.

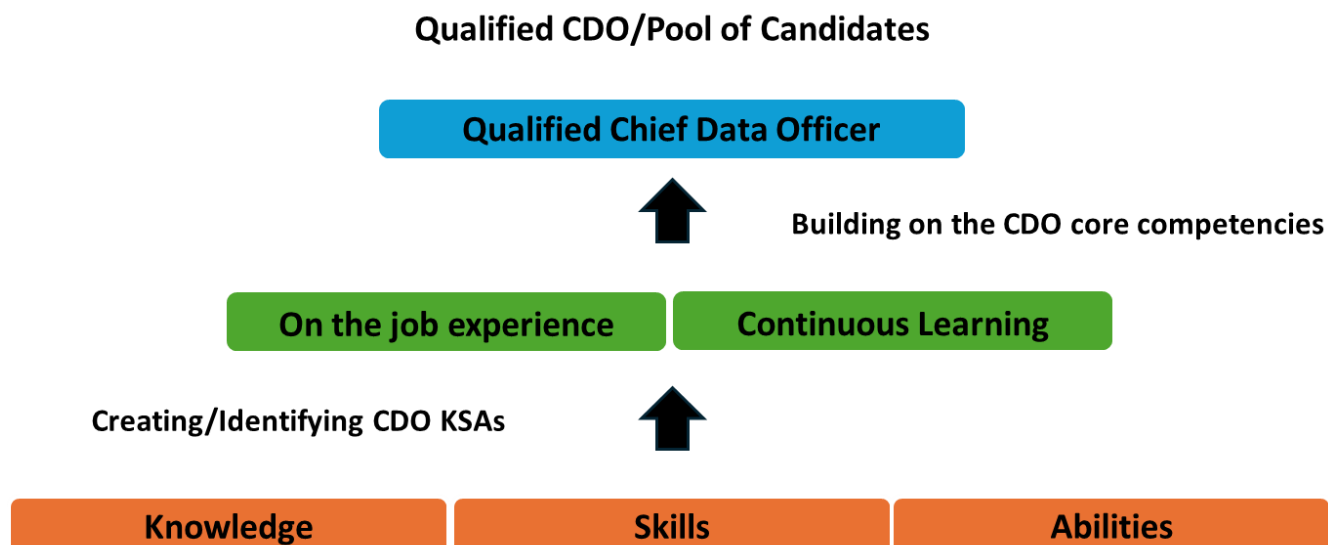


Figure 3. Federal Chief Data Officers’ Knowledge, Skills, and Abilities (KSAs).

Knowledge

Federal Chief Data Officers require enterprise-level mastery of the policies, frameworks, and strategic functions that define data leadership across the federal government. This includes:

Evidence Act Implementation Knowledge: Comprehensive understanding of the statutory responsibilities of CDOs under 44 U.S.C. § 3520, including lifecycle data management, governance, interoperability, and coordination with evaluation and statistical officials.

Federal Data Policy & OMB Guidance: Expert knowledge of OMB M-25-05 (Evidence Act Phase 2), M-19-23 (Data Governance Body requirements), Circular A-130, open data policy, and relevant Executive Orders that shape the government’s data ecosystem.

Data Governance & Compliance Frameworks: Advanced familiarity with NIST standards (SP 800-53, SP 800-60), privacy frameworks, Zero Trust data principles, metadata standards (e.g., DCAT-US), and federal security and privacy requirements.

Data Strategy, Analytics, and Emerging Technologies: Deep understanding of data strategy formulation, advanced analytics, automation, machine learning/artificial intelligence, and the implications of emerging technologies for mission performance and public transparency.

Enterprise Operations & Mission Context: Knowledge of federal organizational structures, budget processes, risk management frameworks, and the mission needs of various stakeholders who depend on federal data.

Skills

Federal CDOs must demonstrate the ability to lead enterprise data transformation, influence cross-agency outcomes, and manage large-scale strategic initiatives. These include:

Strategic Vision & Execution: Ability to build government-wide data strategies aligned to agency missions, operational constraints, and long-term Evidence Act requirements and expectations.

Enterprise Leadership & Collaboration: Skill in leading cross-functional teams, chairing or co-chairing Data Governance Bodies, and driving cohesive data practices across programs, bureaus, and mission areas.

Change Leadership & Transformation Skills: Ability to plan, communicate, and guide organizational change needed for data modernization, culture shifts, and enterprise-wide adoption of data governance practices.

Analytical & Technical Decision-Making: Skill in evaluating data quality, assessing analytic maturity, prioritizing investments, and using evidence to guide decisions at strategic and policy levels.

Risk Management & Data Protection Skills: Ability to direct enterprise approaches to privacy, security, and data risk mitigation, including Zero Trust implementation and data classification.

Communication & Influence: Skill in framing data insights, policy impacts, and resource needs for senior leadership, OMB, Congress, and external oversight bodies in clear, compelling terms.

Abilities

Federal CDOs must demonstrate the core executive abilities required to lead federal data programs at scale.

Enterprise Integration: Ability to align data governance, technology, budget, and mission operations into a unified enterprise strategy that supports evidence-building and service delivery.

Ability to Lead Through Complexity: Capacity to navigate interagency coordination, conflicting priorities, political constraints, and statutory requirements while maintaining momentum on data initiatives.

Ability to Drive Innovation & Modernization: Demonstrated ability to identify emerging trends, introduce new analytical and technological capabilities, and modernize data infrastructure to improve mission performance.

Ability to Build and Sustain High-Performing Organizations: Ability to shape data organizations, develop workforce capability, identify skill gaps, and cultivate a culture of accountability, trust, and continuous improvement.

Ability to Ensure Compliance & Stewardship: Capacity to uphold federal standards for privacy, security, accessibility, and transparency across the entire data lifecycle.

Ability to Communicate at the Executive Level: Ability to brief senior leadership, articulate complex data issues in plain language, and represent the agency in government-wide councils, interagency bodies, and public forums.

Assessment and Evaluation

Effective assessment frameworks establish performance indicators that enable data leaders to track progress, uncover inefficiencies, and support continuous improvement. Examples include data quality scorecards, compliance reviews under the Evidence Act, maturity assessments aligned to M-25-05, periodic data inventory audits, and evaluations of data governance participation and performance. A well-structured evaluation process also strengthens compliance with governance policies and regulatory requirements. By implementing audit mechanisms and risk assessments, CDOs proactively mitigate vulnerabilities, safeguard data integrity, and uphold ethical standards.

Stakeholder feedback plays a crucial role in enhancing these frameworks. Regular reviews uncover areas for recalibration, helping leaders optimize efficiency and effectiveness across the organization. Assessment findings should directly shape development and training efforts, ensuring teams acquire the necessary skills to navigate evolving data landscapes. Identifying competency gaps enables organizations to design targeted learning programs that strengthen governance, technical expertise, and strategic data management capabilities.

Development and Training

To ensure the CDO is equipped with the skills and expertise required to drive data strategy, governance, and innovation, a structured training program should focus on core competencies that align with the organization's goals. These areas may include

federal data policy, data governance, privacy and security, analytics, change management, leadership, and emerging technologies.

Life Cycle of Data

With a clear understanding of the Knowledge, Skills, and Abilities (KSAs) required for the CDO role, it is essential to consider how these competencies are applied throughout the data lifecycle. The following section will explore the data lifecycle and its significance in effective data management.

The data lifecycle encompasses several critical stages that ensure data is managed effectively from creation to disposal. Data Creation/Acquisition involves generating or collecting data from various sources such as databases, APIs, surveys, sensors, or authorized web-based data collection. Ensuring the accuracy and integrity of data at this stage is crucial for its subsequent use. Data Storage follows, where once data is acquired, it must be securely stored in a manner that allows for easy retrieval and protection against unauthorized access. This involves the use of databases, data warehouses, and cloud storage solutions to keep data safe and accessible.

Data Maintenance comes next, involving regular updates and corrections to ensure data's accuracy, consistency, and completeness. This includes processes like data cleaning, validation, and integration to keep data reliable and up to date. Data Usage refers to the application of data for various purposes such as analysis, decision-making, and operational support, with analytics and business intelligence tools deriving actionable insights.

Data Sharing involves distributing data within the organization or with external stakeholders, following proper protocols and standards to maintain security and privacy. Throughout its lifecycle, data may be stored and replicated, or migrated across formats or locations, requiring continuous management to ensure it remains organized and accessible. Finally, Data Disposal is the stage where data is securely disposed of when no longer needed, in compliance with legal and regulatory requirements. Proper data disposal practices help protect sensitive information and reduce security risks.

By understanding and managing each stage of the data lifecycle, organizations can ensure that their data remains a valuable and secure asset throughout its entire existence.

Life Cycle of Data

Effective data management involves navigating through various stages to ensure the integrity, security, and usefulness of data throughout its entire lifecycle. Each stage plays a crucial role in maintaining the quality and reliability of data, from its creation to its eventual disposal.



Figure 4. Life Cycle of Data

Summation and Path Forward

The role of the government CDO is crucial. This competency model provides a comprehensive framework to guide the recruitment, development, and evaluation of CDOs, ensuring consistency and excellence across government agencies.

The model is built around five key components of competency: skills, knowledge, abilities, behaviors, and attributes. These components ensure that CDOs are well-equipped to develop and implement data strategies, manage data governance, security, and privacy, and oversee the entire Life Cycle of Data from creation to disposal.

Skills cover the practical capabilities required to perform data-related tasks, such as data collection, analysis, visualization, and protection. Knowledge encompasses the understanding of various data sources, collection methods, data governance frameworks, and relevant regulations. Abilities refer to the developed or inherent capacities that facilitate effective data management, such as critical thinking, problem-solving, and decision-making. Behaviors include the actions and conduct that promote a data-centric culture and collaborative environment, while attributes define the personal qualities that support the role, such as integrity, attention to detail, and a proactive mindset.

Integral to this model is the understanding of the Life Cycle of Data, which includes stages of data creation/acquisition, storage, maintenance, usage, sharing, and disposal. Managing each of these stages effectively ensures that data remains a valuable and secure asset throughout its entire existence.

In summary, by adhering to these competencies and managing the Life Cycle of Data efficiently, CDOs can significantly contribute to the advancement of evidence-based policymaking and the overall effectiveness of government operations.

Moreover, professionalizing the role of CDOs ensures that these leaders are recognized for their strategic importance within government agencies. As pivotal figures in the digital transformation landscape, CDOs play a critical role in shaping data governance frameworks, fostering a culture of data literacy, and driving innovation through data utilization. Their responsibilities extend beyond mere data management; they are entrusted with spearheading initiatives that enhance transparency, accountability, and decision-making processes.

Elevating the significance of the CDO role also involves providing continuous professional development opportunities, recognizing the need for specialized

certifications and training programs that keep CDOs at the forefront of emerging trends and technologies. This commitment to professional growth not only enhances the capabilities of individual CDOs but also strengthens the overall data governance and analytical capabilities of government agencies.

By professionalizing the CDO position and emphasizing its critical responsibilities, government organizations can ensure a robust approach to data management that supports policy development, operational efficiency, and public trust.⁹

This updated competency model incorporates statutory responsibilities under the Evidence Act, DCAT-US 3.0 schema implementation guidance in support of OMB [M-25-05](#), and governance requirements under [M-19-23](#) to ensure alignment with current federal data policy and the evolving role of the CDO.

⁹ The Federal Chief Data Officers Council serves as a central forum for Chief Data Officers and other data leaders by offering government-wide best practices, guidance, and tools to strengthen data governance, improve data quality, and advance the strategic use of data across agencies; for more information see *About CDOC - Councils.gov | Federal Executive Councils*. (2018). <https://www.councils.gov/cdoc/>.

References

- An Approach to Measuring Chief Data Officer Value and Impact. (2023). Published by the Federal Chief Data Officers Council.
https://resources.data.gov/assets/documents/Measuring_Value_Final_Report_GSA79CDO_21_508_Compliance.pdf
- Chief Data Officers Playbook. (2021). Published by the Federal Chief Data Officers Council. https://resources.data.gov/assets/documents/CDO_Playbook_2021.pdf
- Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115–435, 132 Stat. 5529. <https://www.congress.gov/115/plaws/publ435/PLAW-115publ435.pdf>
- National Institute of Standards and Technology. (2020). NIST SP 800-53 Rev. 5. <https://doi.org/10.6028/NIST.SP.800-53r5>
- National Institute of Standards and Technology. (2018). NIST SP 800-37 Rev. 2. <https://doi.org/10.6028/NIST.SP.800-37r2>
- National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework. <https://www.nist.gov/itl/ai-risk-management-framework>
- Office of Management and Budget. (2016). Circular A-130: Managing Information as a Strategic Resource. <https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf>
- Office of Management and Budget. (2019). Federal data strategy: A framework for consistency M-19-18. <https://trumpwhitehouse.archives.gov/wp-content/uploads/2019/06/M-19-18.pdf>
- Office of Management and Budget. (2019). OMB Memorandum M-19-23. <https://www.whitehouse.gov/wp-content/uploads/2019/07/m-19-23.pdf>
- Office of Management and Budget. (2025). OMB Memorandum M-25-05. <https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/M-25-05-Phase-2-Implementation-of-the-Foundations-for-Evidence-Based-Policymaking-Act-of-2018-Open-Government-Data-Access-and-Management-Guidance.pdf>
- OMB Memorandum M-25-21: Accelerating federal use of AI through innovation, governance, and public trust. <https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf>

Office of Management and Budget. (2019). Federal data strategy website.
<https://strategy.data.gov>

The Progress and Promise of Federal Enterprise Analytics. (2023). Published by the Federal Chief Data Officers Council.
<https://resources.data.gov/assets/documents/Enterprise-Analytics-Report-508-FINAL.pdf>

U.S. General Services Administration. (n.d.). Data.gov. <https://www.data.gov>

U.S. General Services Administration. (n.d.). Project Open Data metadata schema (DCAT-US). <https://resources.data.gov>

Federal Zero Trust (ZT) Security Guide. (2024).
https://resources.data.gov/assets/documents/Zero-Trust-DataSecurityGuide_RevisionMay2025_CIO.govVersion.pdf

Federal Zero Trust (ZT) Security Guide Appendices. (2024).
https://resources.data.gov/assets/documents/Zero-Trust-DataSecurityGuide_Oct24-Appendices.pdf