CHIEF INFORMATION OFFICERS COUNCIL

SMALL AGENCY CIO AND IT EXECUTIVE HANDBOOK

AN INITIATIVE OF IT MODERNIZATION

Table of Contents

Executive Summary

Document Objectives

This handbook was developed by the Small Agency Chief Information Officer Council (SACC) to meet a variety of needs expressed by Chief Information Officers (CIOs) and IT Executives of small agencies. According to the Office of Personnel Management (OPM), there are around 100 small agencies and about 50 of these agencies have fewer than 100 employees.[1] Compared to the 24 agencies named in the Chief Financial Officers (CFO) Act that comprise the CIO Council, these medium, small, and micro agencies have fewer personnel and financial resources to devote to information technology (IT).

This document is meant to provide agency IT Executives with a foundational understanding of responsibilities related to IT. It is designed to support agencies that do not have a full suite of IT leadership roles, such as agencies that don't have a designated CIO, individuals fulfilling multiple roles in IT management, and executives with more limited technical and organizational experience. This document is also intended to serve as a resource to small agency executives who may not have subject-matter expertise across all technical or organizational components but play a leadership role in IT strategy, operations, security, and compliance.

This handbook expands on the Federal CIO Handbook. We also have included responsibilities related to cybersecurity, data management, and privacy, highlighting and referencing handbooks for other IT Executives, including the Chief Information Security Officer (CISO) and Chief Data Officer (CDO). In addition, this document contains general information for executives who may be new to the Federal Government, including topics such as federal procurement and the budget cycle. Overall, this handbook is designed to be useful both to an executive with no Federal Government experience and to a seasoned federal employee.

This handbook benefitted from substantial contributions and feedback from the federal community and small agency representatives and leaders.

[1] U.S. Office of Personnel Management. Federal Agencies List. *Open Government.* OPM.gov. https://www.opm.gov/about-us/open-government/Data/Apps/Agencies/

Handbook Overview

Audience

The Federal Small Agency Chief Information Officers and IT Executives Handbook is intended for executives responsible for IT in small agencies. In this handbook's context, "small agency" refers to any Federal Civilian Executive Branch (FCEB) agency not included in the CIO Council.[2,3] Instead, these agencies are members of the Small Agency Chief Information Officer Council (SACC). These agencies are not included in the Chief Financial Officers (CFO) Act of 1990 and are often referred to as non-CFO Act agencies. At times, certain oversight, regulations, or guidance may only apply to CFO Act agencies. Therefore, small, non-CFO Act agencies share some of the policy implications of their non-CFO Act status. However, this categorization of "small agency" includes around 100 agencies with a wide range of total agency staff, budget, and IT staff, and thus a wide range of resources are available for agency IT Executives. The Office of Personnel Management's (OPM) Open Government Data Federal Agencies List categorizes agencies into three groups based on number of employees: more than 1,000 employees; 100-999 employees; less than 100 employees. There are around 50 agencies with less than 100 employees.[4]

This handbook was developed by the Small Agency Chief Information Officer Council (SACC) specifically to meet the needs expressed by IT executives of small agencies with limited staff and budget resources (typically fewer than 500 employees), but it may be used by any agency regardless of size. These types of small and micro agencies often have specific challenges and unique organizational structures that do not always follow the traditional staffing model for IT administration. In these agencies, there may not be a dedicated CIO role, the individual fulfilling CIO responsibilities may not have broad technical knowledge or federal experience, other IT staff may have multiple roles, and there may be a limited number of Subject Matter Experts (SME). Small agency executives responsible for an IT organization are constantly making decisions about how to allocate staff time. They must find creative ways to ensure all responsibilities are covered and decide whether or not to undertake tasks and activities based on staffing constraints. In addition to staffing, IT budgets for operations and innovation are much smaller than the CFO Act agencies, which often makes the scale of the agencies' procurements and IT implementations quite different. Certain practices and approaches for both procurement and service delivery do not easily translate to small agencies, and small agencies may have a different amount of FAR-compliant funds (appropriated funds). In addition, federal requirements

[2] All federal agencies not designated by EO13011 to be members of the "large" CIO Council are eligible for membership in the Small Agency CIO Council.
https://www.sac.gov/committees/cio/

[3] Exec. Order No. 13011. (July 16, 1996) *Federal Information Technology.* Office of the Chief Information Officer.
https://nodis3.gsfc.nasa.gov/displayEO.cfm?id=EO_13011

[4] U.S. Office of Personnel Management. Federal Agencies List. *Open Government.* OPM.gov.
https://www.opm.gov/about-us/open-government/Data/Apps/Agencies/

and guidance regarding IT for agencies are often broad, complex, and designed with a focus on implementation by CFO Act agencies. Small agencies often do not have the staff resources to monitor the policy landscape, review and digest new policies and regulations, and implement policies that were not designed with their scale and resources in mind.

Due to the varied nature of executive staffing in small agencies, we primarily use the term **IT Executive**, instead of CIO, in this handbook to refer to the highest-ranking individual with responsibility for IT operations and strategy. As a result, the IT Executive may have more responsibilities than a typical CIO. For example, the IT Executive may also be responsible for cybersecurity or data management.

This resource would be targeted for Small Agency CIOs, CISOs, Deputy CIOs, Deputy CISOs, CDOs, agency heads, and other senior leaders within the organization. While the handbook has been written with small agencies in mind, large agencies (i.e., CFO Act agencies) may still find relevant content since overlap exists between small and large agency needs, considerations, and practices.

Purpose

The handbook is intended to supplement existing resources, including the foundational, role-specific guidance contained in the CIO Handbook, CISO Handbook, and CDO Playbook.

To address the small agency challenges noted above, the Federal Small Agency Chief Information Officers and IT Executives Handbook aims to:

- Give small agency IT Executives foundational information about their areas of responsibility in managing their IT portfolio.
- Highlight laws, policies, tools, and initiatives related to federal IT to improve compliance and implementation.
- Provide decision-making guidance and recommendations for challenges specific to small agencies.
- Serve as a consolidated knowledge base and a quick reference to access information and resources from GSA and other organizations.

Content

The Federal Small Agency Chief Information Officers and IT Executives Handbook has a modular design with three main sections that can stand alone. They are:

- Leadership and Management Considerations: Provides leadership and management considerations and practices for small agency CIOs and IT Executives with a focus on executive leadership, portfolio assessment, and planning.

- Technical Components: Reviews IT components and associated IT capabilities needed for small agencies to meet business needs and statutory and regulatory requirements.
- Organizational Components: Reviews the organizational components, from procurement to customer service, that overlay the technical components to help small agencies establish, maintain, and control their IT environments.

The content of any section can be read in any order or be used as a reference for relevant technical or organizational information. Those with less federal or IT experience may prefer to proceed through the handbook sequentially for an overview of major areas of responsibility and resources for support.

Within each section, information about a specific topic includes:

- Overview and key details about the topic's technical and organizational areas of responsibility.
- Management and leadership considerations.
- Unique challenges and benefits of small agencies.
- Resources, including tools, publications, training, and government and professional organizations.
    - There are countless (fee and non-fee) resources across the Federal Government that can be utilized by small agencies to maximize their efficiency and effectiveness. The information in this handbook may be used as a starting point for small agencies to research and find these resources.

Introduction

Federal IT Management

IT is deeply embedded in all federal agency missions and business processes. IT resources "enable the Federal Government to provide quality services to citizens, generate and disseminate knowledge, and facilitate greater productivity and advancement as a Nation."[5] IT intersects with aspects of the Presidential Management Agenda (PMA), including customer experience, workforce, and making the government more efficient and effective.[6] There also are governmentwide IT initiatives communicated in the Federal CIO Operating Plan, the Federal Data Strategy, and other strategic policy documents. Governmentwide priorities include:

- Cybersecurity
    - Zero Trust
- IT modernization
    - IPv6
    - Cloud Smart
- Digitization
    - Customer experience
- Data as strategic asset

At an agency level, IT has broad impacts on employee productivity, customer experience, data management, and information security. In addition, IT infrastructure and security are critical to an agency's foundation and success. As the impact of IT on agency mission objectives increases, so does the scope of IT management. The IT Executive's three broad areas of responsibility are:

- IT infrastructure and operations
- Mission-delivery and business solutions
- IT practices and management[7]

---

[5] U.S. Office of Management and Budget. (2016). *Managing Information as a Strategic Resource* (Circular A-130). Executive Office of the President, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

[6] Miller, J. (2022, December 27). *Federal CIO Martorana on her plans for 2023.* Federalist News Network. https://federalnewsnetwork.com/technology-main/2022/12/federal-cio-martorana-on-her-plans-for-2023/

[7] U.S. Department of Justice. (August 2020). *Information Technology Governance Guide*. U.S. Department of Justice. https://www.justice.gov/jmd/file/705831/download

CIO Role

In each agency, there is one or more individuals responsible for leading IT strategy and implementation for the agency. In the CFO Act agencies, there is a dedicated Chief Information Officer (CIO) role responsible for ensuring "IT is acquired and information resources are managed in a manner that supports the agency's mission, goals, and objectives."[8]

The foundational responsibilities identified for the CIO position in the CFO Act agencies are summarized in the CIO Handbook as follows:[9]

1. IT leadership and accountability – CIOs are responsible and accountable for the effective implementation of IT management responsibilities.
2. IT strategic planning – CIOs are responsible for strategic planning for all IT management functions.
3. IT workforce – CIOs are responsible for assessing agency IT workforce needs and developing strategies and plans for meeting those needs.
4. IT budgeting – CIOs are responsible for the processes for all annual and multiyear IT planning, programming, and budgeting decisions.
5. IT investment management – CIOs are responsible for the processes for managing, evaluating, and assessing how well the agency is managing its IT resources.
6. Information security and privacy – CIOs are responsible for establishing, implementing, and ensuring compliance with an agencywide information security program. (GAO-18-93. Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities. August 2018.)
7. Architecture.
8. Information resources and data.

Small Agency IT Administration

Small agencies shoulder the same responsibilities as large agencies with respect to IT responsibilities and implementation. Small agencies often have unique organizational structures that do not follow the traditional staffing model for IT administration. In a small agency, there may not be a designated CIO position. Instead, small agency staffing may result in one executive serving two or more roles. For example, an executive may have more responsibilities than the standard federal CIO role. In some cases, the agency director may also serve as the CIO. At many small agencies, executives face specific challenges, such as limited agency

[8] U.S. Chief Information Officers Council. *CIO Handbook.* CIO.gov https://www.cio.gov/handbook/cio-role-at-glance/
[9] U.S. Chief Information Officers Council. *CIO Handbook.* CIO.gov https://www.cio.gov/handbook/cio-role-at-glance/

resources, access to timely information, and awareness of federal resources, services and organizations. In addition, federal requirements and guidance regarding IT for agencies is often broad, complex, and designed with a focus on implementation by CFO Act agencies.

For these reasons, this handbook provides a general approach to comprehensive management of an agency's IT portfolio, including an overview of foundational elements and principles to establish and maintain reliable, secure, and effective IT operations and services. It also includes information about managing data and information security – two areas that are led by chief-level executives (Chief Data Officer [CDO] and Chief Information Security Officer [CISO]) in most CFO Act agencies. Due to the diverse nature of small agency staffing, this handbook uses the term **IT Executive** to mean the individual at the agency with the primary responsibility for IT management and the standard duties of a federal Chief Information Officer (CIO). The ultimate responsibility for managing IT, data, and information security is with the agency head.

A high-level overview of the following roles is included for reference and to provide context for the related information included in this handbook.

Chief Data Officer (CDO): The role of the Chief Data Officer is described in 44 U.S. Code § 3520 - Chief Data Officers and responsibilities are summarized in the CIO Handbook as follows:[10]

- Responsible for lifecycle data management.
- Coordinate with any official in the agency responsible for using, protecting, disseminating, and generating data to ensure the data needs of the agency are met.
- Manage data assets of the agency, including the standardization of data format, sharing of data assets, and publication of data assets in accordance with applicable law.
- Ensure that, to the extent possible, agency data conforms with data management best practices.
- Engage agency employees, the public, and contractors in using public data assets and encourage collaborative approaches on improving data use.
- Support the Performance Improvement Officer of the agency in identifying and using data to carry out the functions described in section 1124(a)(2) of title 31 (31 U.S.C. § 1124(a)(2). Performance Improvement Officers).
- Support the Evaluation Officer of the agency in obtaining data to carry out the functions described in section 313(d) of title 5 (5 U.S.C. § 313(d). Evaluation Officers).
- Review the impact of the infrastructure of the agency on data asset accessibility and coordinate with the CIO of the agency to improve such infrastructure to reduce barriers that inhibit data asset accessibility.

[10] U.S. Chief Information Officers Council. Chief Data Officer (CDO). *CIO Handbook*. CIO.gov. https://www.cio.gov/handbook/key-stakeholders/cdo/

- Ensure that, to the extent possible, the agency maximizes the use of data in the agency, including for the production of evidence (as defined in section 3561 (44 U.S.C. § 3561. Definitions)), cybersecurity, and the improvement of agency operations.
- Identify points of contact for roles and responsibilities related to open data use and implementation.
- Serve as the agency liaison to other agencies and [OMB] on the best way to use existing agency data for statistical purposes (as defined in section 3561 ([Ibid]).

Chief Information Security Officer (CISO): As described in the Chief Information Security Officer Handbook, below are some of the key information security responsibilities assigned to agencies as a whole.[11] Depending on the agency, these tasks may or may not fall entirely or exclusively to the CISO.

- Comply with Executive Orders and Presidential Memoranda, minimum security requirements and standards promulgated by the NIST, and binding operational directives (BODs) developed by the Department of Homeland Security (DHS).
- Assess risk and determine the appropriate level of protections for assets.
- Develop and maintain information security policies, procedures, and control techniques to address all applicable governmentwide requirements.
- Comply with federal reporting requirements.
- Develop plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.
- Train information security staff and ensure all agency personnel are held accountable for complying with the agencywide information security program.
- Report breaches and major incidents to DHS's Computer Emergency Readiness Team (US-CERT) within mandatory timelines.

Leading and Managing Small Agency IT

Executive Leadership

In your role as IT Executive, you are both a leader of the IT department and an executive leader of the agency. As an executive, you contribute to the management of the agency, including human resources, budget, operations, and information. As an agency leader, you contribute to

[11] Chief Information Security Officer Council. *Chief Information Security Officer Handbook*. Chief Information Officer Council. https://www.cio.gov/assets/resources/CISO_Handbook.pdf

its strategic direction.[12] For some, the CIO role represents a transition from department to agency and enterprise leadership. As you consider your role and plan for success, it is helpful to understand: (1) the responsibilities and capabilities of a successful executive leader and (2) the context of the CIO role in your agency.

Responsibilities

As the lead IT Executive within your agency, your foundational responsibilities are to ensure basic IT operates reliably and meets or exceeds your customers' expectations. This means the IT department provides basic operations support to all parts of the agency. Your agency's network should be operational, the computers should work without issue, and the applications should be accessible without service degradation. Also, procedures should be in place to monitor and maintain the confidentiality, integrity, and availability of your systems and data. In addition, the IT organization must understand the business requirements and provide solutions to support the business. The department should focus on relevant IT projects and programs that benefit your agency and mission outcomes within reasonable parameters of budget, cost, and quality. Finally, oversight and governance are also key to success for the agency IT leader. Ensure that policies and procedures are in place to receive minimal findings and favorable results from third party oversight, audits, and reviews.

Establishing high quality IT operations and services are essential for an IT Executive to establish and maintain credibility and confidence with agency leaders. Without the demonstrated ability to manage the core IT functions, the IT Executive will have difficulty contributing as a member of the agency's executive leadership team.

In addition to running the IT organization and providing mission support services, the IT Executive's leadership responsibilities include the following:

- Strategic thinking
- Leading change, promoting innovation
- Achieving results, executing strategic priorities
- Managing risk
- Cultivating productive working relationships and partnerships
- Exemplifying personal drive and integrity
- Communicating with influence

[12] Tropman, J., & Wooten, L. (2010, September 23). Executive leadership: a 7C approach. *Problems and Perspectives in Management, .8(4)*. Business Perspectives. https://www.businessperspectives.org/index.php/journals?controller=pdfview&task=download&item_id=3469

Skills and Capabilities

As described in the article, "A Nonpartisan Model for Developing Public-Service Leaders," the Partnership for Public Service Public Service Leadership Model identifies four core competencies for federal leaders:[13]

- Becoming self-aware
- Achieving results
- Engaging others
- Leading change

The article also identifies five skills or capabilities that support the development of these competencies:

- Emotional intelligence
- Evidence-based decision making
- Equitably engaging a diverse workforce
- Understanding the importance of technology
- Encouraging innovation and creativity

The article notes that federal leaders share two core values that guide their decisions – "stewardship of public trust and commitment to public good."[14]

Keys to Success

- Establish technical credibility via a high-functioning IT organization.
    - Fix Problems. If the core IT functions are not meeting high standards, focus on immediate, high visibility issues as your first priority (before working on IT strategy).
    - Get a team. Bring together (or assemble) your IT team. Identify key roles and skills, and identify gaps. Identify individuals who can lead and manage teams or workstreams.
    - Are there any actions that can deliver a quick win?
- Establish performance metrics for IT.

---

[13] McDonald, R., Conant, D., & Marshall, A. (2020, April 20). *A Nonpartisan Model for Developing Public-Service Leaders.* Harvard Business Review. https://hbr.org/2020/04/a-nonpartisan-model-for-developing-public-service-leadership

[14] McDonald, R., Conant, D., & Marshall, A. (2020, April 20). *A Nonpartisan Model for Developing Public-Service Leaders.* Harvard Business Review. https://hbr.org/2020/04/a-nonpartisan-model-for-developing-public-service-leadership

- Establish a vision for the IT organization.
    - Communicate why you are here and what you are trying to accomplish.
- Understand agency mission objectives and strategic initiatives.
    - Consider establishing a cadence (e.g., quarterly) for engaging with executives to discuss their initiatives and potential integration with technology.
    - Consider engaging leaders of mission work streams in portfolio workshops to review their current IT portfolio and identify changes and future needs.
- Contribute to technical innovation to support mission and agency operations.
- Structure the IT department to support your responsibilities as an executive.
    - Build a capable leadership team and delegate daily management responsibilities.
- A big part of your role is communicating, inspiring, and leading.
- Consider federal executive training or leadership training.
- Be honest and open about existing or identified issues.
- Highlight and celebrate your organization's successes.
- Have confidence in your abilities and have confidence to admit if you don't know something.
- Think back to your previous experiences with leadership (both as a leader and as a team member). You won't have all the answers, but you have a depth of work experiences to help guide you.
    - What worked?
    - What didn't?
    - What were key lessons learned about leading and managing?
- Make time for reflection on your leadership.
- Leverage external partners and internal resources.
- Consider establishing a formal or informal relationship with a mentor.
- Ask for help. Someone in the government has had this issue, situation, or question before. Someone also likely has a resource, template, example, or solution.
- If you are dealing with resolving multiple issues in the IT organization, remember your leadership and colleagues want you to succeed, while being compliant and "doing things the right way."

Context of Small Agency

- Resource challenged
    - Many staff, including executives, have multiple roles

    - Regularly analyzing tradeoffs to manage time
    - Lack of technical expertise
- Constant change
- Diversity of work area responsibilities and tasks
    - Ability to be hands on across a wide range of activities, from developing agency strategy to developing contract requirements
- Ambiguity, as role definition may be less clear
- Increased visibility and access to agency executive
- Potential for increased impact on agency direction and mission

Context of Your Agency

- Why were you brought into the role?
- How is the performance of the IT organization?
- Is there an agencywide strategy or vision defined for IT? Is it well communicated?

Support and Resources

- Colleagues and Peers
- Small Agency Chief Information Officer Council (SACC)
- Federal executive and leadership training opportunities
    - Partnership for Public Service Leadership model

Executive Partners

Depending on the structure of the small agency, there may be additional executives and functions that impact IT administration and operations, in areas of overall agency administration, finance, contracting, human resources, and mission partners. Agency management functions, such as acquisition, finance, human capital, data, information security, operations, and performance, may each be led by an individual in a "chief" role, or an individual executive may fill multiple roles. In some agencies, IT Executives themselves are responsible for one of more of these functions.

Regardless of organizational structure, the group of agency executives work to "ensure that mission support resources are effectively and efficiently aligned and deployed to achieve the agency mission."[15] This includes setting goals, analyzing and communicating results, and making changes as needed to ensure the agency's management functions are effective in supporting the agency's goals and objectives. The responsibility for IT management includes

[15] U.S. Chief Information Officers Council. Overview of Key Stakeholders. *CIO Handbook.* CIO.gov. https://www.cio.gov/handbook/key-stakeholders/overview-key-stakeholders/?clickEvt

the establishment of relationships and processes with executive partners in order to drive change in technology-related procurement, workforce development, and budget allocation. The success of the IT Executive often involves partnership and consideration of individuals responsible for agency administration and operations. By establishing relationships with executive partners, a CIO can help drive change in "technology-related procurement, workforce development, budget allocation," and other areas.[16] Below are high-level overviews of various executive roles that contribute to IT administration and operations, as well as collaborators and executive partners for IT Executives.

Administrative Partners

The IT Executive must work closely with the agency's administrative and operations executives. These roles vary throughout small agencies and may include Chief Administrative Officer (CAO), Chief Operations Officer (COO), Director, and other related titles and roles. Agencies may also have executives dedicated to customer experience, strategic planning, learning and development, and performance improvement.

Finance Partners

The IT Executive must partner with the agency's financial executive(s) responsible for the agency's budget, contracts, and procurement. Common roles for these executive partners include the Chief Financial Officer (CFO), Chief Acquisition Officer (CAO), and Contracting Officer (CO). As non-CFO Act agencies, a small agency may not have these positions specifically designated, or roles may be held by a single individual. Regardless of the small agency structure, the IT Executive must work closely with the finance executives to determine funding resources, contracting opportunities, and procurement of IT equipment.

Human Resource (HR) Partners

HR executives, such as the Chief Human Capital Officer (CHCO), also work closely with the IT Executive as an agency customer and as a partner in execution, training, and change management.

Agency Customers

The work of an IT Executive is not only based on federal requirements and funding resources, but it must be specifically targeted to meet the needs of agency customers responsible for carrying out the mission of the agency. Working with agency customers to determine their technology needs and requirements presents specific challenges depending on the work of the agency, the current state of the agency's IT infrastructure, and the available funding to modernize systems and technology.

---

[16] U.S. Federal CIO Council. (2017, January). *State of Federal Information Technology.* GSA's Office of Government-wide Policy. https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2017/05/CIO-Council-State-of-Federal-IT-Report-January-2017-1.pdf

IT Management Approach

Overview

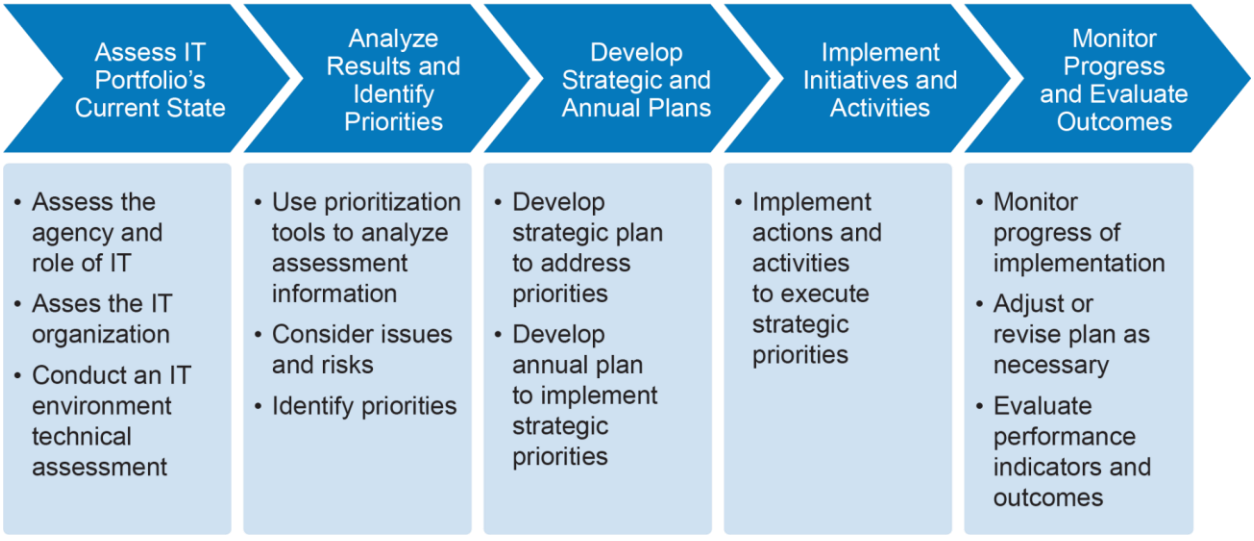
This handbook contains a significant amount of information and resources related to small agency IT operations. The following information provides a high-level framework for IT Executives to develop a baseline understanding of the agency's IT functional and supporting areas. Following the high-level overview in the section, the document provides detailed information for various Technical and Organizational topics.

The approach has five components:

1. Assess IT portfolio's current state
2. Analyze results and identify priorities
3. Develop strategic and annual plans
4. Implement initiatives and activities
5. Monitor progress and evaluate outcomes

Monitoring progress is often done in parallel with implementation, as an iterative process, so that monitoring results may be used to impact the implementation.

Figure 1. *General IT Management Approach*



How to Get Started

In a small agency, executives have unique visibility and influence across the agency. Whether you are new to the IT Executive role or re-evaluating a current role, it is essential to identify each component that makes up the agency's IT portfolio and to identify the IT Executive's responsibilities. In parallel, identify any information or technology areas that are not in the scope of responsibility, but are related. For example, does the Chief Information Security Officer (CISO) or Chief Data Officer (CDO) report to a different executive (e.g., the Chief Operating Officer [COO])?

Step 1: Assess Current State of IT Portfolio

An important first step in managing an IT portfolio is to assess the current state of IT in the agency. A comprehensive IT Portfolio Assessment should include an evaluation of the following three areas:

- The agency and the role of IT
- The IT organization
- The IT environment

The assessment should be a holistic review of the IT portfolio, gathering information about what is known and unknown, in order to identify priorities (both strategic initiatives and areas with risks and issues) that can form the basis of both strategic (over 3 to 5 years) and annual plans. The assessment includes research and reviews to determine capabilities, funding, current technology, requirements, and resources unique to your agency.

Below, sample questions are grouped into the three major areas to guide a comprehensive IT portfolio assessment. This will help small agency IT Executives better understand the agency's IT landscape, define the "must do's" at this agency, identify key partners, highlight issues and risks, and identify opportunities for strategic initiatives.

Step 1.1: Assess the Agency and the Role of IT[17,18,19]

Table 1. *Assessment Questions: Agency and Role of IT*

Questions	Answers
What are the agency's mission functions?	
What are the agency chief executive's priorities? ● Improve business processes ● Increase use of information; support reporting ● Digitize and modernize services ● Support compliance ● Consolidate business operations ● Reduce costs ● Create new services; reach new customers	
How is data, information, and technology used to enable mission functions?	
What is the organizational structure of the agency? ● Who are the executive peers (e.g., CFO, COO, CHRO)?	
Are any other executive positions responsible for any part of IT? ● Which executive positions are responsible for organizational support for IT (e.g., HR, procurement, budget)?	
How are executive-level decisions made?	

[17] Reina, D.S. (2021). *The New CIO: How to make an impact on the first year on the job*. Gartner. https://emtemp.gcom.cloud/ngw/globalassets/en/information-technology/documents/insights/gartner-new-to-role-cio-ebook2.pdf

[18] Gartner. *The CIO's First 100 Days: A Toolkit*. Gartner. https://www.gartner.com/imagesrv/pdf/1st100Days_SummaryBro2012.pdf?_ga=2.208104407.410470118.1673388306-1395972700.1662739392&_gac=1.52916570.1669591126.Cj0KCQiAsoycBhC6ARIsAPPbeLsiCsZVgqcj_8vpwHwa9Wxa_kLBFwL-eqX1npBQ0XayzObY2O79l_QaAlJpEALw_wcB

[19] Reina, D.S. (2021). *The New CIO: How to make an impact on the first year on the job*. Gartner. https://emtemp.gcom.cloud/ngw/globalassets/en/information-technology/documents/insights/gartner-new-to-role-cio-ebook2.pdf

Table 1.1. *Assessment Questions: Agency and Role of IT*

Questions	Answers
What are the expectations for the role of the CIO? ● Is there a current IT strategy? ○ What is it? ● Is your role to run, grow, or transform agency IT?	
What are the key systems that are critical to the mission? ● Are there issues or risks with any of these systems?	
What are the expectations and perceived quality of IT by executives? ● What's working well? ● What are the major initiatives? ● What are challenges, risks, and pain points? ● How does the IT operating model help agency operations and support innovation and advancement? ● How does IT hinder operations and limit change and innovation?	
What are the expectations and perceived quality of IT by business leaders?	
What is the level of engagement between business programs and the IT organization?	
Who are the agency's IT stakeholders and is the IT portfolio meeting expectations?	

Keys to success for small agency CIOs

As technology becomes increasingly tied to business outcomes and more common for technology executives not to have a technical background, it is important for IT Executives to position themselves as business leaders with technical knowledge.[20]

[20] Reina, D.S. (2021). *The New CIO: How to make an impact on the first year on the job*. Gartner. https://emtemp.gcom.cloud/ngw/globalassets/en/information-technology/documents/insights/gartner-new-to-role-cio-ebook2.pdf

- Identify operational issues that need urgent attention; focus on the critical issues until they are resolved
- Look for opportunities to solve business problems using technology; demonstrate link between technology to business value
- Examples of business priorities include:[21]
    - Improve business processes
    - Increase use of information; support reporting
    - Digitize and modernize services
    - Support compliance
    - Consolidate business operations
    - Reduce costs
    - Create new services; reach new customers
- Establish relationships and partnerships with executives and program (business) leaders
- Develop trust of peers, customers, and staff by building credibility and commitment to results and delivery
- Validate job description and key performance indicators with agency executive

Step 1.2: Assess the IT Organization[22,23]

The structure and capabilities of the IT team should be reviewed to determine whether gaps in knowledge or skills exist, how contractors are incorporated into operations, and whether the agency utilizes any Federal shared services for IT. Part of the assessment process includes gathering information about past and current IT spending with respect to the cost of personnel, contractors, applications, systems, and licenses. Knowing what IT costs are incurred is a first step. Next, information should be gathered working with executive partners to determine the budget for future IT expenses.

---

[21] Reina, D.S. (2021). *The New CIO: How to make an impact on the first year on the job*. Gartner. https://emtemp.gcom.cloud/ngw/globalassets/en/information-technology/documents/insights/gartner-new-to-role-cio-ebook2.pdf

[22] Gartner. *Toolkit: The Application Leader's First 100 Days* (G00390073). Gartner.

[23] Gartner. Executive Summary. *The CIO's First 100 Days: A Toolkit*. Gartner. https://www.gartner.com/imagesrv/pdf/1st100Days_SummaryBro2012.pdf?_ga=2.208104407.410470118.1673388306-1395972700.1662739392&_gac=1.52916570.1669591126.Cj0KCQiAsoycBhC6ARIsAPPbeLsiCsZVgqcj_8vpwHwa9Wxa_kLBFwL-eqX1npBQ0XayzObY2O79l_QaAlJpEALw_wcB

Table 2. *Assessment Questions: IT Organization*

Questions	Answers
Who are responsible for key IT functions: Data (CDO), security (CISO), privacy (CPO), and accessibility?	
What is the IT organization structure? ● Do the positions cover the scope of what you are responsible for? ● What functions are covered by contractors? ● Is the structure designed for effectiveness? ○ How many direct reports do you and your managers have?	
What are the capabilities of the IT staff? ● Are there any shortfalls in skills, people, and resources? ● Who are the key staff members to keep systems operational?	
What is the state of IT governance?	
What is the state of IT compliance? ● Are there any current compliance issues or risks?	
What is the IT budget? ● What is the balance of operations vs new projects? ● Is the budget in line with peers?	
What are the major current IT projects?	

Table 2.1. *Assessment Questions: IT Organization*

Questions	Answers
What are the current contracts and vendors?	
Are there any contracts that can be re-evaluated for service or cost?	

Keys to success

- Understanding roles and governance regarding agency IT
- Awareness of current initiatives, status, and budgetary considerations
- Identify leaders who can manage day-to-day operations
- Develop scorecard to measure key areas of performance (operational performance, business value, and customer service)

Step 1.3: Conduct IT Environment Technical Assessment[24]

Assessing the current state of the IT technical environment requires information about the agency's hardware, software, network, telecommunications, data center, devices, and cybersecurity.

Table 3. *Assessment: IT Environment (Technical)*

Hardware

Questions	Answers
Is there an inventory?	
How well is the inventory managed?	
Does the hardware meet customer and system needs?	

[24] General Services Administration Cloud Information Center. *Technical Implementations.* GSA.gov. https://cic.gsa.gov/planning/technical-implementations

Network

Questions	Answers
Is there a network diagram?	
How are the quality, reliability, cost, and security?	

Systems

Questions	Answers
Who are the system owners?	
What is in place for patching?	
What is in place for end-point protection?	
Is there a system security plan?	

Enterprise Architecture

Questions	Answers
Is the agency's enterprise architecture documented?	
Is the architecture up to date?	
How are changes to the architecture managed?	
Are there defined change management procedures?	
Do you have staff assigned to the enterprise architecture function?	

Software Applications

Questions	Answers
Is there an inventory?	
Does the inventory identify key applications?	
Does the inventory identify legacy systems? ● Are any unmanaged?	
Has there been any type of application rationalization? ● If so, what are the most recent results?	
Is there a business case for each application?	
Are systems and software serving their original purpose?	

Cloud Adoption and Modernization

Questions	Answers
Who is responsible for leading efforts in cloud adoption?	
What current Service Level Agreements (SLAs) exist for cloud services?	

Digitization

Questions	Answers
Who is responsible?	
What plans are in place?	

Security

Questions	Answers
Who is responsible?	
When was the most recent security assessment?	
What policies are in place? ● What is the level of compliance?	
What processes are in place for: ● Patching ● Scanning ● Log Reviews	

Data: Collection, Storage, Access

Questions	Answers
What are the workflows for data collection? ● Are they optimized for efficiency?	
Does the storage capacity meet current and future needs?	
Is data optimized for access by: ● Agency staff ● Public	

Data: Security and Privacy

Questions	Answers
Who is responsible? ● Is protected data identified and marked? ● Is encryption available?	
What are processes for handling and storing and accessing?	

Data: Records Management

Questions	Answers
Who is responsible? ● Is there a Records Management Policy?	

Enterprise Help Desk

Questions	Answers
Who is responsible?	
Who does the help desk support? ● When is it available?	
How is the function organized? ● What are the workflows? ● Is there a ticketing system? ● What skillsets are required?	
Have you defined SLAs or Service Level Objectives for your help desk?	
Has a service catalog been developed? ● Is the service catalog automated?	
Has the service catalog and SLAs/SLOs been communicated to your stakeholders?	

Step 2: Analyze Results and Identify Priorities

Step 2.2: Analyze Assessment Information

There are various approaches and tools that can be used to analyze the information gained through the assessments. A general approach is to identify the functional area or category of the organization that is being assessed. For example, items from the list above may be categorized according to:

- **Areas of responsibility**[25,26]
    - **Eight areas identified for Federal CIOs by CIO Council**
        - IT Leadership and Accountability
        - IT Strategic Planning

[25] U.S. Chief Information Officers Council. *CIO Handbook.* CIO.gov. https://www.cio.gov/handbook/cio-role-at-glance/
[26] Government Accountability Office. (2022, September). *Chief Information Officers: Private Sector Practices Can Inform Government Roles*. GAO.gov. https://www.gao.gov/products/gao-22-104603

        - IT Workforce
        - IT Budgeting
        - IT Investment Management
        - Information Security and Privacy
        - Architecture
        - Information Resources and Data
    - **Additional areas**
        - IT Infrastructure Management and Performance
        - Application and System Development
        - Application and System Performance and Management
        - Governance
        - Compliance
        - Customer Service and Satisfaction
        - Modernization, Digitization
- **Functional Objectives**[27]
    - Engage Business and Stakeholders
    - Lead Strategy
    - Lead Technology Implementation and Innovation
    - Manage Governance
    - Manage IT Finance
    - Lead Workforce
    - Manage IT Performance

Alternatively, individual initiatives, projects, activities, and any other category that would benefit may be evaluated. Examples include:

- Agency and business strategic objectives (e.g., finance, mission, process, and workforce)
- IT guiding principles (e.g., simplicity, usability, business value, innovation, data management, compliance, and customer focus)
- IT strategic initiatives (e.g., digitization, cloud, cost reduction, innovative and flexible sourcing, business capabilities, and operational performance)

[27] Gartner. *IT Score for CIOs.* Gartner. https://www.gartner.com/en/information-technology/trends/it-score-cios

Then, identify and define the criteria to rate each item being assessed. The following are common criteria used for evaluation:[28]

- Strategic importance to agency or business
- Strategic alignment with agency or IT plans
- Impact (e.g., number of users, customers, business lines, and agency objectives)
- Urgency (i.e., level of risk associated with delaying implementation)
- Level of maturity
- Cost and return on investment
- Opportunity for cost reduction
- Opportunity for business process improvement
- Complexity
- Impact on compliance
- Longevity
- Sustainability
- Feasibility
- Resistance

For each criterion identified, use a rating scale with definitions of each value. The following table shows three different types of scales that could be used to define a value:

[28] Data Modernization Initiative. *Project Prioritization Matrix*. PHII.org/DMIToolkit https://phii.org/wp-content/uploads/2021/07/DMPlanningTemplate_S7_Prioritization-Matrix.pdf

Table 4. *Examples of Rating Scale Values*

Example 1	Example 2	Example 3
High	Good	Excellent
Medium	Fair	Very Good
Low	Poor	Fair
		Poor
		Very Poor

The table below from the United States Copyright Office (USCO) *Provisional IT Modernization Plan and Cost Analysis* provides criteria definitions for three factors (criticality, cost, complexity) that were used to analyze program initiatives for an IT roadmap analysis.[29]

Table 5. *Rating Scale with Values Defined for Criticality, Cost & Complexity*

Value	Criticality	Cost	Complexity
High	Project that is critical to achieving successful and timely separation from LoC systems	Project estimated to cost $1.5M+	Project with substantial amount of development and/or integration
Medium	Project that delivers capabilities that USCO currently has but are not critical to a successful Day 1	Project estimated to cost $500,000 - $1.5M	Project with moderate amount of development and/or integration
Low	Project that delivers capabilities that build on current USCO IT capabilities	Project estimated to cost <$500,000	Project with minimal amount of development and/or integration

[29] United States Copyright Office. (2016, February 29). *Provisional Information Technology Modernization Plan and Cost Analysis.* Copyright.gov https://www.copyright.gov/reports/itplan/technology-report.pdf.

The table below provides sample definitions for five levels of a metric to evaluate program or implementation maturity.[30,31] A maturity model can be used to assess the current state of operation or implementation for a range of activities. For example, the maturity assessment criteria can be used to analyze the state of software development practices, project management practices, agency cybersecurity practices, etc. A maturity model may be used to identify current weaknesses and create an improvement plan to reach the criteria of a higher level of maturity.

[30] Cybersecurity & Infrastructure Security Agency. (2021, May 12). *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1*. CISA.gov https://www.cisa.gov/sites/default/files/publications/FY%202021%20IG%20FISMA%20Metrics%20Final%20v1.1%202020-05-12.pdf

[31] Cybersecurity & Infrastructure Security Agency Cybersecurity Division. (2021, June). *CISA Zero Trust Maturity Model.* CISA.gov https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

Table 6. *Sample Maturity Model*

Level	Sample Definition	Simplified Scale
Level 5	Optimized Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.	Optimal
Level 4	Managed and Measurable Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.	Advanced
Level 3	Consistently Implemented Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.	Advanced
Level 2	Defined Policies, procedures, and strategies are formalized and documented but not consistently implemented.	Initial
Level 1	Ad-hoc Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.	Initial

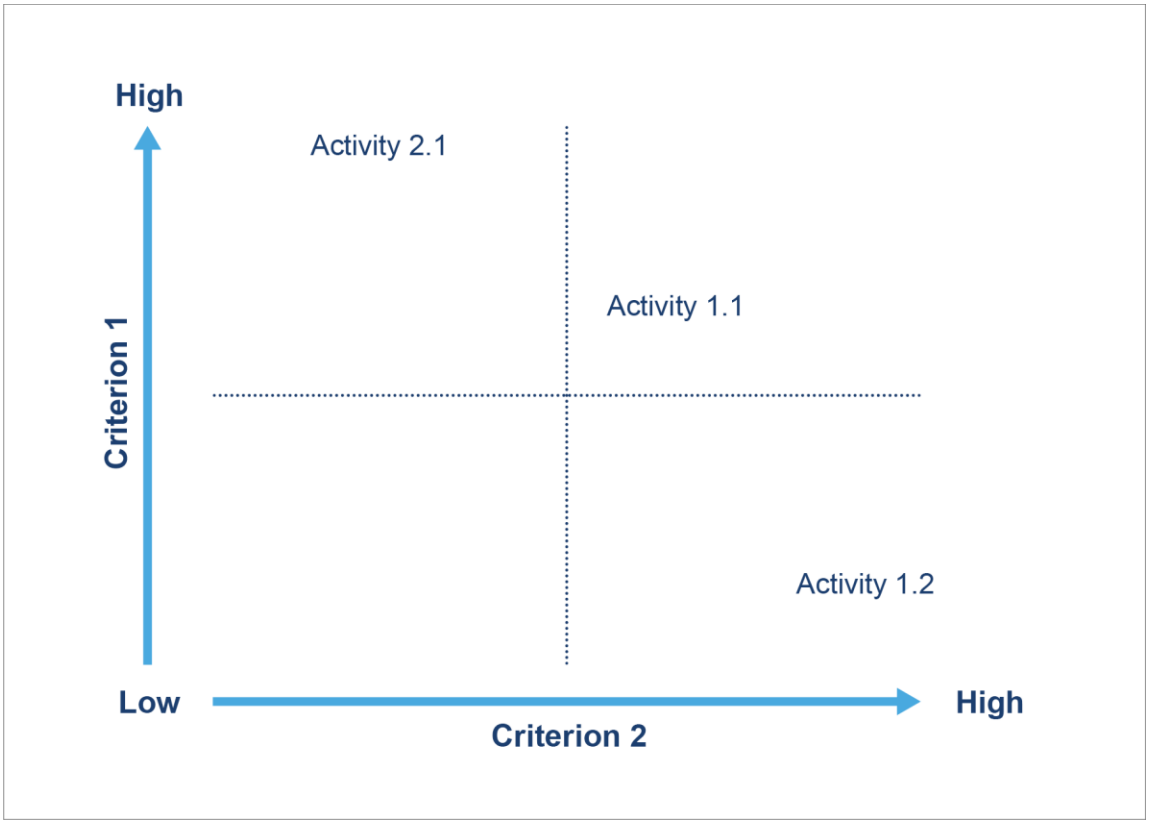
Step 2.2: Prioritization

Tables and matrices (decision matrix) are two common tools that can be used to analyze assessment results. Analyses may be used to identify issues and risks and prioritize areas, activities, and projects for action to develop short-term action plans and longer term strategic plans.

Table 7. *Sample Table for Analysis*

Area of Responsibility	Activity	Criterion 1	Criterion 2	Criterion N
IT Leadership	Activity 1.1			
IT Leadership	Activity 1.2			
IT Leadership	Activity 1.3			
IT Leadership	Activity 1.4			
IT Budget	Activity 2.1			

Figure 2. *Sample Matrix for Analysis*



To consider more than two criteria for prioritization, create a matrix with the least important criteria for decision making. Take the items identified as High and High and analyze this group using a second matrix with different analysis criteria.

The following are a few examples of how the assessment results may be analyzed to identify priority areas and actions:

- Compare current state results to a desired state and identify gaps to prioritize. Consider the root causes of the gaps to identify strategies and initiatives to improve performance.

Table 8. *Analysis of Current vs Target Level*

Area of Responsibility	Activity	Current Level	Target Level
IT Leadership	Activity 1.1		
IT Leadership	Activity 1.2		
IT Leadership	Activity 1.3		
IT Leadership	Activity 1.4		
IT Budget	Activity 2.1		

- Evaluate assessment results in the context of the agency's strategic and annual plan and prioritize activities with high alignment and impact.
- Evaluate assessment results in the context of the IT organization's strategic or operational plan.

Table 9. *Analysis of Impact on Strategic and Annual Plan*

Area of Responsibility	Activity	Current State Performance	Strategic Plan Impact	Annual Plan Impact
IT Leadership	Activity 1.1			

- Evaluate area's maturity versus impact on agency's business objectives to identify both strengths and opportunities for improvement.[32]
- Are there initiatives that have budgetary time constraints?
- Rate the initiative's level of urgency versus importance to the IT organization and agency.
- Assign an estimated "time for implementation" to initiatives and group initiatives into similar "time horizons" to assess impact and resource availability.

[32] Gartner. *IT Scores for CIOs*. Gartner. https://www.gartner.com/en/information-technology/trends/it-score-cios

- Are there projects that could generate quick wins?
- Compare impact versus complexity (i.e., effort, cost, and level of risk)

Step 3: Develop Strategic and Annual Plans

After conducting the assessment and identifying areas of work to prioritize, develop an IT strategy composed of strategic and annual plans. Strategic and annual planning models are discussed in the next section.

Step 4: Implement and Establish Initiatives and Activities

After developing the IT strategy, the next step is to execute the plan by implementing activities to produce results and objectives defined by the strategic plans. Such activities may involve acquiring additional personnel, contract support, IT shared services or changes to hardware, software, or IT services. To optimize successful implementation, communicate the IT strategy objectives and related priority activities to stakeholders involved with implementation, ensure that job duties align to the objectives and activities, and encourage your staff to maintain their focus and alignment with the IT strategy goals. Consider if any change management principles could benefit your staff, partners, or customers.

Step 5: Evaluate and Monitor Progress Toward Objectives

Plan implementation should include a process to regularly (e.g., monthly, quarterly) monitor progress against timelines, milestones, and goals to identify issues, roadblocks, internal or external changes, and other variables. Progress monitoring may also include measuring outcomes and indicators to determine if the implementation is having any impact or the desired effect. Progress monitoring data enables the organization to adjust course and update the plan in response to changing circumstances and new developments and opportunities.[33]

At the end of the plan's implementation period, there should be a focused evaluation of the plan's level of success at implementation and the impact on identified outcomes.[34] Were the goals met? A retrospective meeting to reflect on the implementation process can provide insight and learning about what contributed to and detracted from the success. Consider the questions below from the article, "A Manager's Guide to Successful Strategy Implementation."[35]

---

[33] National Center for Educational Statistics. *Forum Unified Education Technology Suite*. Institute of Education Sciences.
https://nces.ed.gov/pubs2005/tech_suite/part_1.asp

[34] Miller, K. (2020, February 25). *A Manager's Guide to Successful Strategy Implementation.* Harvard Business School Online.
https://online.hbs.edu/blog/post/strategy-implementation-for-managers

[35] Miller, K. (2020, February 25). *A Manager's Guide to Successful Strategy Implementation.* Harvard Business School Online.
https://online.hbs.edu/blog/post/strategy-implementation-for-managers

- Did we achieve our goals?
- If not, why? What steps are required to get us to those goals?
- What roadblocks or challenges emerged over the course of the project that could have been anticipated? How can we avoid these challenges in the future?
- In general, what lessons can we learn from the process?
    - An unsuccessful or flawed strategy implementation can prove a valuable learning experience for an organization, so long as time is taken to understand what went wrong and why.

Planning

Overview

Strategic planning includes developing the following:[36]

- Strategy
- Strategic plan
- Operational or annual plans

The assessment and prioritization activities described in the previous section can contribute to the agency's IT strategy, which includes the agency's major long-term goals and desired future state within the next three to five years. A strategic plan provides a roadmap to execute the strategy and achieve the objectives over a planning period of typically two to four years. The plan identifies key outcomes to achieve and the initiatives that will lead to those outcomes. Operational plans are annual plans that identify activities and resources required to achieve a strategic plan's objectives; they also may include key operational tasks for the year. Operational plans are usually closely related to the agency's budget process.

Strategic Planning

At least every four years, most agencies are required to provide a strategic plan concurrent with the President's Budget in the second year of a presidential term. The plan should cover a minimum of 4 years. Because IT is integral to many agency mission objectives, an agency's strategic plan will likely include some technology initiatives. In addition, it is a best practice for an IT organization to create a strategic plan that maps to the overall agency's strategic plan. The functions and activities related to strategic planning are considered inherently governmental functions, only to be performed by federal employees.

[36] Nielsen, T. (2022, May 23). *Quick Answer: What's the Difference Between Strategy, Strategic Plans and Operational Plans?* (ID G00768586). Gartner.

The following steps and guidance are from the GSA web publication, "How to Strategic Plan in 7 Steps."[37] The first three steps are similar to the assessment and prioritization efforts described above.

Step 1: Environmental Scan

The first step of any strategic planning process starts with research to identify factors that may impact the long-term direction of the agency. Review the incoming administration's priorities (e.g., customer experience and equity) and potential new regulations to incorporate into the future vision.

Step 2: Internal Analysis

Complete an internal analysis, including a strengths, weaknesses, opportunities, and threats (SWOT) analysis, of the IT operations, human capital, products and services, and security. Information from annual review processes can be used to evaluate performance across the agency, as well as feedback from IT staff and agency and business leaders.

Step 3: Strategic Direction

Based on the findings from the environmental scan and internal analysis, create a strategic direction. Use input from staff and stakeholders to build a vision that is idealistic and high impact. Identify initiatives that align to the agencies' management priorities for the IT organization (e.g., customer service, business productivity, cost reduction, system [infrastructure and application] performance, and innovation). Aim to align IT initiatives with Administration and agency priorities and initiatives. Determine what is actually achievable and what the agency should strive for.

Step 4: Develop Goals and Objectives

With strategic direction and vision in mind, engage with stakeholders, IT leadership, and agency leaders to create goals and objectives. Initiative or subject matter experts should come up with strategies, indicators, and desired outcomes for each goal. Outcomes should be measurable and there should be a plan to produce a status report of actual results at the end of the plan. Use existing processes if possible, such as staff engagement, communities of practice, and quarterly reviews, to get buy-in from across the agency. If these processes do not exist, strategic planning is an excellent time to establish them.

[37] Collins, A. (2022, April 26). *How to Strategic Plan in 7 Steps*. Performance.gov https://www.performance.gov/blog/strategic-plan-7-steps/

Step 5: Define Metrics, Set Timelines, and Track Progress

After the goals and objectives are set, add details to the plan. Determine the responsible offices and teams for each goal. The responsible leaders should identify the necessary resource allocations, create actionable timeframes, and define metrics that measure success.

Step 6: Write and Publish a Strategic Plan

Create an informed strategic plan that captures the agency's vision and purpose for IT. Consistent engagement with staff and stakeholders in steps 2 through 5 contributes to support for the strategic plan and reduces the likelihood that the plan ends up as a standalone document.

Step 7: Plan for Implementation and the Future

Plan for execution of the strategic goals. Identify performance measures that track progress and create a system to review the plan and update goals and objectives annually at a minimum. As a best practice, create an annual plan to support implementation of the strategic plan.

Considerations

- Ensure broad, appropriate participation in the strategic planning process.
- Identify clear accountability for each strategic objective to avoid confusion.
- Make sure every goal has a Key Performance Indicator (KPI) measurement to define and identify success.
- Use the strategic plan as a framework when determining annual goals.

Resources

- www.performance.gov
- www.evaluation.gov
- www.gao.gov

Annual Operational Plan

An operational plan provides short-term (i.e., annual) execution guidance for the strategic plan initiatives. Annual plans provide structure to the strategic plan's implementation by identifying how budget, staff, and other resources will be used to achieve outcomes and objectives. In addition to activities related to the strategic plan, an annual plan may include key operational activities or activities to address urgent issues. The plan's projects and activities should have measurable outcomes that will be assessed annually, or more frequently according to the

activity. Schedules, timelines, or deliverable milestones may also be included based on the activity or workstream.

The development of the IT department's annual plan often is part of the enterprise portfolio management process. Decisions about projects, activities, workstreams, and initiatives to include in an annual plan may be made by the department's governance body. The development and approval of annual plan activities often are closely tied to the agency's annual budget process. Many agencies develop annual Agency Performance Plans as part of their budget request.

IT Portfolio Essentials

Technical Components

Hardware

Overview

Hardware comprises the physical components of IT infrastructure. Hardware includes:

- Network hardware: router, hub or switch, modem, and server
- Storage devices
- Mainframe
- User access and computing equipment: computers, monitors, tablets, phones, mobile devices, printers, copiers, and audio visual equipment

Details

Lifecycle

- Each type of hardware has an expected useful lifespan.
- Actively manage (inventory, track, and correct) hardware assets in your IT infrastructure.
    - Track value, ownership, physical location, age, condition, and status throughout the lifecycle from acquisition through disposal. (See Figure 3.)
    - Incorporate lifecycle information into budget forecasts by comparing business needs and asset inventory and condition.
    - Software assets are managed through a similar process. (See Software Application Portfolio Management section.)
- Account for hardware maintenance and support in your infrastructure spend plan.
- Ensure IT hardware is appropriately decommissioned and disposed of per agency's policies.

Security

- Certain types of hardware can be attacked. “Specifically, any hardware asset that is addressable (i.e., has an IP address) and is connected to your organization’s network(s) and infrastructure physically, virtually, remotely, and those within cloud environments. These devices and their peripherals are remotely attackable.”[38]
    - Machines vulnerable to attack include new and unprotected systems as well as “forgotten” and unmanaged machines.
    - Ensuring each device has an owner is key to managing security risk.

Budget and Purchasing

- As part of managing IT spending, the Office of Management and Budget (OMB) directs agencies to identify IT operations and maintenance (O&M) expenditures, known as non-provisioned services, that do not use solutions often viewed as more efficient such as cloud computing and shared services.

Small Agency Considerations

- Age and obsolescence are two risks for federal IT.
    - Work with program and business units to identify drivers of technology use over the next five years to plan spending and minimize risk.
    - Consider annual evaluation of O&M investments to evaluate if agency needs are being met.
        - Determine if newer versions of hardware can better meet your agency’s needs.[39]
- Consider using Governmentwide Acquisition Contracts (GWACs), especially for common hardware items. See the IT Procurement Section for more information.
- Using cloud infrastructure services and leasing equipment may be alternatives to purchasing hardware.
    - Existing hardware can be used for a hybrid cloud environment. (See Cloud Operations and Optimization Management section.)
- Support and services from CISA for monitoring hardware: Continuous Diagnostics and Mitigation (CDM) Program.

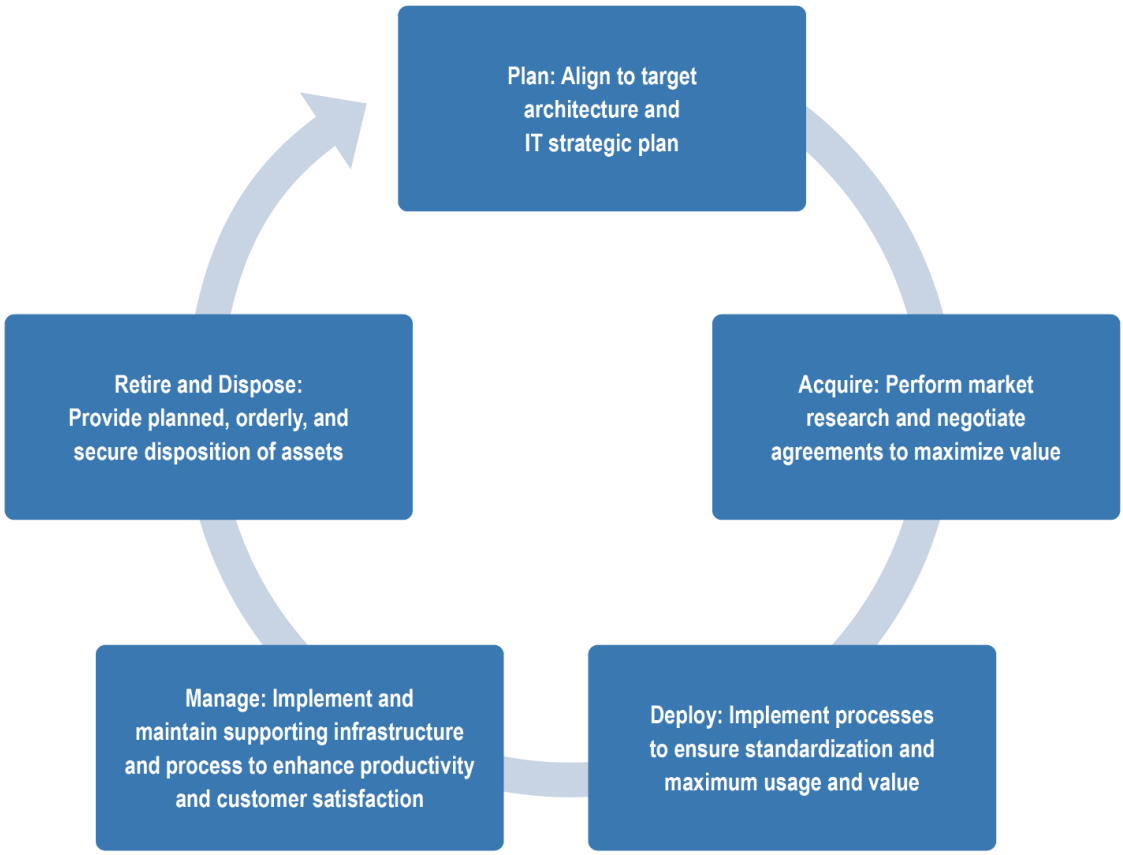
[38] Office of Cybersecurity and Communications Federal Network Resilience. *CDM Hardware Asset Management (HWAW) Capability.* U.S. Department of Homeland Security. https://www.cisa.gov/uscert/sites/default/files/cdm_files/Intro_to_HWAM.pdf

[39] GAO-16-468 (2016, May 25). *Information Technology: Federal Agencies Need to Address Aging Legacy Systems*. GAO.gov. https://www.gao.gov/products/gao-16-468

Resources for Executives

- IT Asset Management Policy (NRC)

***Figure 3**. IT Asset Lifecycle Management Process*[40]



[40] U.S. Nuclear Regulatory Commission. (2016, December). *IT Asset Management Policy.* Office of the Chief Information Officer. https://www.nrc.gov/docs/ML1630/ML16309A561.pdf

Network Configuration and Management

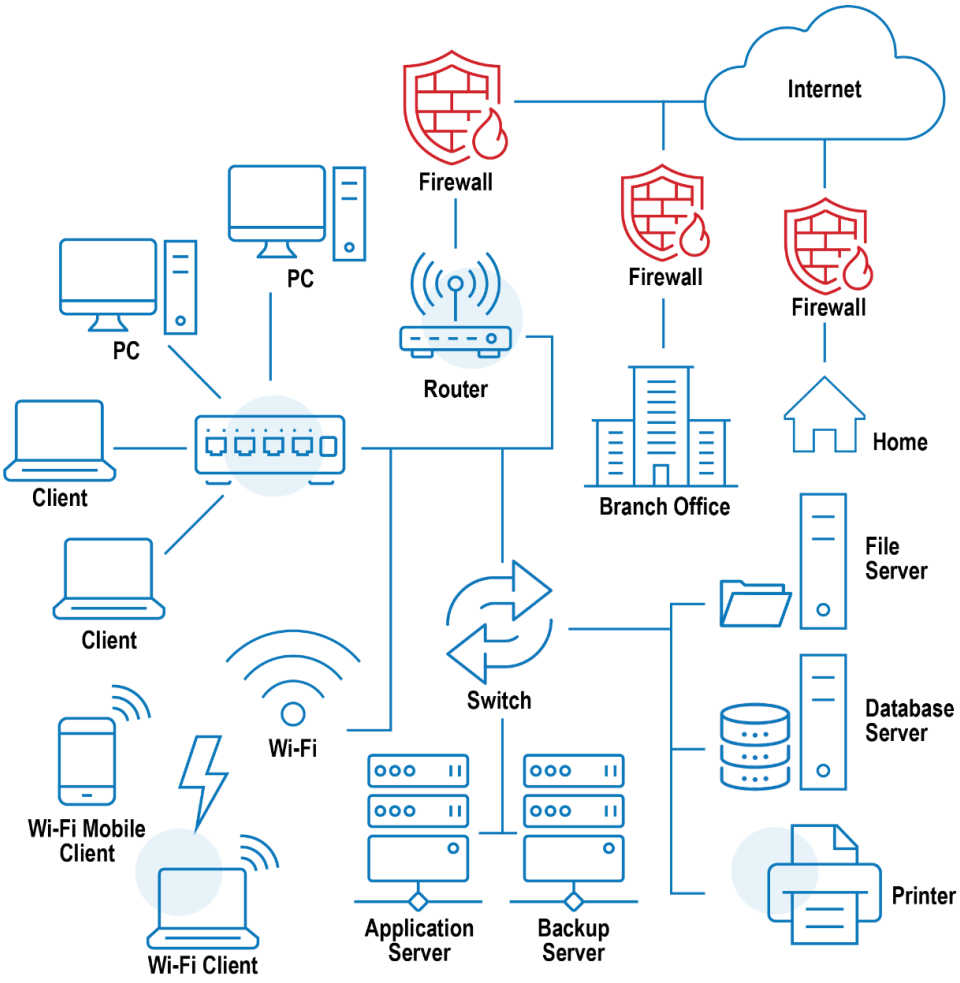
Overview

The primary function of a network is to provide connectivity between devices. In today's networks, Transmission Control Protocol/Internet Protocol (TCP/IP) is utilized with IPv4 and IPv6. Internet protocol is a standardized way of packaging, addressing, routing, and transmitting data between devices via the Internet. Each device has at least one unique IP number (IP address).

The following networks can be on premise, in the cloud, or in the hybrid cloud.

- A Local Area Network (LAN) is focused on network connectivity to a single physical location.
- A Metro Area Network (MAN) interconnects multiple LAN locations together in a metro area.
- A Wide Area Network (WAN) connects multiple locations together regardless of physical location.

Figure 4. *Example of a Network*



In OMB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," networks are identified as a core feature of zero trust architecture and no network is implicitly trusted. This means networks are no longer "trusted" entities for authentication to applications. In other words, a user doesn't automatically get access to network resources by authenticating to the network. Instead, agencies should decouple network access from the user's ability to gain authorization to data resources (i.e., applications, share drives, folders, etc.).

A best practice is to build security into the network design to ensure protection of the network infrastructure from attacks.

- Maturing Software Defined Networking (SDN) technologies help build some of the required security into the environment inherently.

- Another key capability that can increase network security is to enable data-in-transit encryption at every hop within the network infrastructure.
- By moving to a modern identity provider (IdP), the ability to authenticate users directly to the application and add context-based authentication (i.e., checking the user's device for configuration compliance) enhances the security of both the data and the network and better supports a highly remote workforce.

One key policy to be aware of is OMB Memorandum M-21-07, "Completing the Transition to Internet Protocol Version 6 (IPv6)." This memorandum requires federal agencies to adopt IPv6 with a target date of 2025 to complete the transition. IPv6 uses a 128-bit format and can support 2 to the 128th power of unique addresses, which provides significantly more IP address space than the current IPv4 protocol. IPv6 provides some additional updates to IPv4, including security and privacy improvements, and should be used for the internal network to help get to zero trust with its security measures. As IT continues to evolve toward mobile platforms, Internet of Things (IoT), and wireless networks, IPv6 growth will continue to accelerate.

Details

Gather Network Requirements

The network is part of the foundation that enables mission requirements. Therefore, CIOs need to meet with business units and mission owners to understand network requirements for their mission objectives and applications. Capacity and latency are two key requirements for making decisions about network operations. Capacity determines the amount of data that can be transmitted in a specific amount of time. Latency is a delay in network communication, so it determines response time and the time it takes for data to travel across the network. Reliability is another factor to consider. Network decisions will require stakeholders to consider the impact of their needs for reliability, capacity, and speed on the total cost of network services. If your agency lacks the resources to develop a requirements list and document capacity and latency needs, you may contract with a firm through GSA schedules to accomplish this task.

The following questions can help identify capacity and latency needs, in addition to other requirements for enterprise network planning:

- What systems and applications do you need to support on the network?
    - Is there a requirement for Unified Communication as a Service or Call Center as a Service that requires real-time transmission protocols?
    - Can applications that are currently on-premise be hosted in the cloud and do you have a strategic intent to put applications in the cloud?
- How many users will the application or network support? Where are your users located?
- What is the current capacity of the network?
- What type of networking technology do you have?

- Do you have a network traffic baseline of all the sites (i.e., branch offices), the data centers, and Internet access? (Typically, network management tools can provide these data points.)
- Have you identified any bottlenecks in the network connectivity that may cause poor performance?
- What are the requirements from business stakeholders?
    - Is there a need to scale with high capacity for certain periods of time?
    - Is there a time period where uptime with a very low failure rate is critical?
    - What are the "must-haves" for reliability, capacity, and speed? What is the priority of cost efficiency compared to these factors? Is there a priority of cost efficiency over reliability or speed?
- Is there application documentation that provides bandwidth requirements for the application access?
- Consider how the agency will support a hybrid work environment.
    - Identify the applications and services remote users need.
    - Determine the amount of traffic that needs to go to data center applications versus cloud applications.
    - Ensure the agency has enough network capability to allow external home connections to their enterprise network.
- Do we have the resources to design, implement, and manage a network to support our business needs?

As you think through your network strategy, it is important to include internal and external design elements, such as access to Cloud solutions that include SaaS, PaaS, and IaaS. Your agency will need to develop an overarching architecture to support routing between all services. Some cloud-based applications have large capacity needs (i.e., bandwidth intensive) that you will need to factor into your network requirements. A greater reliance on cloud services leads to a greater need to design a network to support the cloud service delivery model.

CIOs should work with their network engineering staff or managed network service provider to include security elements in the network design, including elements for zero trust adoption. Network segmentation (i.e., breaking the network into different zones with controlled access) will be required to meet zero trust security principles. Microsegmentation places individual devices or applications in separate zones to allow for individualized access monitoring control.

Networks are dynamic and they will change with time based on user needs and use patterns. Since demand for WAN resources (especially at compute hubs such as data centers and colocation facilities) grows by as much as 30 percent a year, plans must reflect the need to accommodate increasing demand. At the same time, demand for LAN resources may slow down now that more people are working remotely. A network should be scalable and reliable,

with the ability to adapt to changing requirements. If your agency does not have a workforce that can monitor and support changes to your network, consider using managed LAN and WAN services through GSA schedules such as the EIS contract.

Future Technology Considerations

Agencies should develop plans to mature their network environments as the market evolves to support new technologies. Agencies should consider software defined network solutions, such as Software Defined Networking (SDN), Software Defined WAN (SD-WAN), Network Function Virtualization (NFV), and Software Defined LAN (SD-LAN). These technologies allow a significant amount of automation and efficiency in management and scalability, which will increase capabilities and potentially lower costs through efficiency. These technologies are software based and less reliant on physical infrastructure. Agencies can get more in depth information about these modern technologies through the GSA Enterprise Infrastructure Solutions (EIS) modernization guides found here.

Workforce Considerations

Current networking technology is complex and agencies need to evaluate their existing workforces' abilities to support the advanced networking technologies (i.e., cloud and software-based networking solutions) replacing the legacy hardware-based network delivery model. As technology evolves, engineers need the ability to grow professionally to support these services and ensure maximum uptime and security. If your agency does not have existing resources and are unable to hire capable staff, you should hire managed services providers where possible.

Network Governance

It is vital for agencies to understand exactly what network capabilities they have. Network mapping tools can be used to analyze existing ports, protocols, traffic flows, bandwidth utilization, and other detailed information that should be documented.

Ensure your agency has created an Enterprise Network Architecture Document. This document should:

- Include WAN and LAN connectivity along with connectivity to data centers and cloud environments.
- Document methods and data access routes for internal users, external users, and partners.
- Document all network-related data points, such as Cloud Security Groups, HTTP(s) traffic, ingress and egress traffic, port traffic, firewall traffic and privileges, etc.

If your agency does not have a workforce capable of doing this in detail, many small businesses run automated tools to provide this information for a nominal fee.

Ensure your agency has real-time network monitoring capability in place to manage your environment. This function can be done internally or acquired as part of a managed network service.

Evaluate your terms and conditions for existing contracts and ensure refresh periods, along with your budget cycle, and plan accordingly. Also, standardize on service provider tiers and performance. Ensure your locations have the appropriate network access services with appropriate performance required to meet mission requirements.

Federal Requirements

- Internet Protocol Version 6 (IPv6) GSA Resources
- OMB Memorandum M-21-07 Completing the Transition to Internet Protocol Version 6 (IPv6)
- OMB Memorandum M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

Telecommunications

Overview

Telecommunication (telecom) services enable the transmission of information for agency facilities, data centers, and employees. Telecom services are critical to an agency's mission since communications would come to a standstill without them. These services include fixed-network services such as data, internet, voice, and mobile services. Telecom also includes non-traditional, IP-based services, such as unified communications services, that allow an employee's telephone number to move with them as part of a hybrid work environment and allow for the use of software-based phones instead of the traditional hardware telephone device.

Fixed-data services are connections between a service provider and an end user or customer. Types of fixed data services include dedicated and private lines that provide dedicated, unshared bandwidth to a customer. Other examples include packet and circuit-switched access services, such as Integrated Services Digital Network (ISDN), ethernet, broadband, and satellite. These transport mechanisms do not treat specific traffic differently when transmitted over the medium. All types of transmissions, such as voice, video, images, and video conferences, can be transmitted over these mediums regardless of whether it's in analog or digital format. Federal agencies and industry in general are moving towards digital access. Agencies should seek modern solutions, such as ethernet transport services, for the majority of their bandwidth needs but can also seek dark fiber and optical wavelength services for high transmission needs if required. Agencies can work with the GSA EIS team to assess their services and develop a modernization plan accordingly.

Fixed voice services are local and long-distance phone services using a landline. Traditionally, voice services were provisioned using the circuit-switched Public Switched Telephone Network

(PSTN). Today, many agencies leverage Voice over IP (VoIP) services that provide voice communication over the data network via data services.

Mobile Telecommunication Services (Wireless Mobility Service) include both voice and data capability through the mobile networks. Information on mobility service capabilities available through the GSA Mobility SIN are located here and through EIS in GSA's publicly available service guides.

Details

Agencies have been focused on the modernization of telecommunication infrastructure since the release of the GSA EIS contract several years ago. In the past, many agencies leveraged the Networx contract along with Local Service Agreements to acquire voice and data services. Many small agencies are in the midst of their IT modernization efforts. The best practices and guiding principles below are provided by the EIS program office to assist agencies in their efforts. These best practices are lessons learned from many interactions with agencies as they transition from Networx to the EIS contract.

- Before transition or modernization, complete an inventory and analysis that includes current state versus future state.
- Understand current and future agency mission needs and plan accordingly.
- Determine if the organization has the staff to support the current and future state. If not, do other agencies offer any type of support?
- Where possible, utilize "As a Service" models to control risk and expenditures.
- During an acquisition process, mandate site surveys from offerors to mitigate implementation delays and cost overruns.
- As a response to any service solicitation, a deliverable should be required from offerors that includes an Implementation Plan. Recommend using the number of days post award for each milestone. For instance: Arrive at site 3 days post award.
- Significant problems with transition and modernization have been associated with the lack of a detailed implementation plan and schedule.

Outside of modernization and new service acquisition, if your agency has a significant amount of telecommunication services, consider using a Telecommunications Expense Management (TEM) service. These vendors manage communications-related IT and cloud-based services. They can provide full lifecycle management of mobile assets along with fixed voice and data lines. If your agency does not have staff available to manage these services, consider contracting with a firm that provides this capability. Using a TEM provider results in more effective cost control, cost management, and visibility into your spend.

Small Agency Considerations

Focus on modernization as you transition from legacy telecom services to modern services. For example, agencies may want to consider a Unified Communication solution that provides collaboration and voice capability rather than using traditional landlines for communication in a hybrid work environment.

Consider using the data network for voice communication (VoIP) or mobile devices. Unused voice circuits can be discontinued for voice savings.

Create solutions that include a combination of dedicated and guaranteed bandwidth, such as MPLS circuits and broadband solutions, to reduce overall telecom expenditure.

Focus on managed services for commodity telecom, such as voice, voicemail, mobile devices, etc.

Explore the use of TEM companies to streamline your telecom spending and identify opportunities for savings. This can be a one-time endeavor or an ongoing partnership.

When soliciting for telecom and IT services, EIS should be the course of action if soliciting for an all-inclusive enterprise solution. The more difficult decision is when you are soliciting for a single service, such as Mobility, or a group of services that do not require complete integration, such as COMSATCOM and Earth Observation. When ordering through EIS or using one of the Multiple Award Schedule (MAS) Telecommunications Management Service options, your agency may not need to purchase, deploy, and maintain the backend systems needed to provide the ordering, billing, inventory, and reporting tools provided automatically through Conexus and the National Hosting Center (NHC) or that would be provided when using one of the vendor-provided Telecommunications Management Service options. Conexus and the NHC provide EIS customers with an integrated Telecommunications Services Management solution featuring a customizable dashboard using the administrative tool. You can find an in-depth look at the Conexus Tools on the Conexus website.

Other considerations include the available vendors, your agency's geographic diversity, and staff familiarity with EIS versus the MAS options.

Resources for Executives

The following resources are available to support telecommunications requirements:

- Telecommunications Acquisition Support Services - Contact your service broker for assistance.
- Telecommunications and Network Services
- GSA Multiple Award Schedule
- GSA eLibrary contains the latest GSA contract award information:

Agencies can search on a particular topic (i.e., telecommunications) or use the Category Guide to select a particular field (i.e., information technology) then further select the area of need.

Visit the GSA EIS Public Pricer website, which is open to the public and requires no login, to access the below tasks and resources:

- Convert street addresses to the closest Network and Sharing Center (NSC).
- Check service availability by street address or NSC.
- Map awarded CBSAs by rank, service, and vendor.
- Download awarded services by CBSA, country or jurisdiction, and vendor.
- Price Contract Line Item Numbers (CLINs) across vendors.
- Access service guides and white papers.

For additional resources on EIS NSCs, awarded CBSAs, CLINs, access to our Solicitation Review Tools, and contract mod and catalog submissions, visit the GSA EIS Agency Pricer website. To obtain access, contact the EOS Help Desk at eos.help@eos.gsa.gov.

GSA Solution Brokers: GSA Solution Brokers (SB) can assist agencies with defining business requirements, developing solicitations, acquisition planning, and task order execution efforts. SBs also coordinate with other organizations to support life-cycle project management and implementation, service ordering, and delivery of vendor services.

For more information on the telecom services offered through EIS, please review the EIS Service Guides and White Papers. For additional information on the service offerings through EIS and how to acquire them, please review the EIS Resource Page.

Data Center Operations and Optimization Management

Overview

A data center is a location that contains IT infrastructure, such as servers, databases, and mainframes. On-premise, agency-run data centers still remain a part of many agencies' operations, and they present challenges to providing effective mission support and achieving federal energy and sustainability goals. Modernization of an agency's IT infrastructure is a constant process requiring evolving management of hybrid cloud scenarios and active energy management of the physical infrastructure. Small agency CIOs must do both on limited budgets. With more people working remotely, continuing to operate our data centers is critical, even as we modernize our IT infrastructure and portfolios.

Details

Understand current and future agency mission needs and plan accordingly. Needs can include storage requirements, compute requirements, and space requirements. Data center planning

includes consideration of IT hardware mounting infrastructure and layout, network layout, physical security, active energy management and acquisition, equipment cooling management, continuity of operations (COOP) and disaster recovery (DR), and facilities maintenance operations and requirements.

Data storage takes up the most space, consumes the most energy, and needs the most cooling in a data center. Robust data storage management, including data security, is key going forward. You must constantly assess your retention policies, deduplications efforts, and data sovereignty.

Agencies should try to align to overall federal energy and sustainability goals where it makes sense.

- Do as much as possible to reduce your footprint and energy consumption.
- Outcomes can show cost savings, energy reduction, and operational improvement.
- Follow the links below to learn what you can do immediately in your data center to get started.

Many small agencies lack physical facilities that can provide the capabilities of colocation providers. Mission critical services require facilities that have proper cooling, redundancy, and availability. Seek out colocation opportunities from other agencies and commercially.

- Colocation facilities offer industry leading capabilities for managing IT hardware infrastructure and provide high-speed access to cloud services.
- Colocation facilities offer advantages, such as redundancy, high uptime, and stability.
- Evaluate facilities' alignment with Uptime Institute's Data Center Tier Standards for facilities. They are defined as the following:
    - Tier 1: Single path for power and cooling, and no backup components. This facility has an uptime of 99.671 percent per year or less than 22.8 hours of downtime per year.
    - Tier 2: Single path for power and cooling, and some redundant and backup components. This facility has an uptime of 99.741 percent per year or less than 22 hours of downtime per year.
    - Tier 3: This facility has multiple paths for power and cooling, and redundant systems. The physical systems can be worked on while online without downtime. The facility has an uptime of 99.982 percent per year or less than 1.6 hours per year.
    - Tier 4: All components have redundancy and the facility is completely fault-tolerant. The facility has an uptime of 99.995 percent per year or less than 26.3 minutes per year.

- Determine what is required to carry out your agency's mission when deciding which colocation facility to use. Cost is usually commensurate with Tier. Consider asking data center providers the following questions when evaluating facilities:
    - Where is your data center located?
    - What is your Tier rating?
    - What happens during a power outage? How do you refuel generators? Do you have a local contract for refueling?
    - Describe your uptime testing practices? How often do you test generators and power supplies?
    - What is your plan to recover from a major disaster?
    - What are your access control policies? Who can access the data center?
    - What hours can your staff access the data center? Are you open 24/7?
    - Describe your security. Make sure the provider has comprehensive security features. This will include physical aspects of the buildings in their location. Ensure the following are monitored: air conditioning, power, physical intrusion, uninterruptible power supply (UPS) backup, fire, generator, etc.
    - Does your data center have any industry certifications?
    - What type of network access does your data center have? Do you have high-speed connections to cloud service providers? Do you have redundant network connections and what is your capacity? Ensure the provider has network connectivity from multiple top tier telecom providers.
    - What type of support do you provide your customers? They should offer support 24/7, if possible. Additional questions can include:
        - How are incidents managed and what is the escalation process? What is the response time?
        - Do you provide services to reboot systems? What additional troubleshooting services do you offer?
        - What is your after-hours staffing plan? Do you have security guards and engineers?
        - Do you have an automated answering service for issues or does your staff answer the phone?
    - Do you provide any managed services? Examples include installation and management of hardware.

Be proactive with enterprise portfolio management and continually strategize using the Application Rationalization process to determine if what you have fits the purpose best based on cost, service delivery, and business resiliency. This process will help the agency decide what to

keep, what to combine, and where to put the application, system, or environment. This could be to the cloud, commercial colocation, or federal colocation.

Federal Requirements

- Most of the federal mandates for data centers are focused on the 24 CFO Act agencies.
    - OMB Memorandum M-19-9 Update to Data Center Optimization Initiative (DCOI)
    - Federal Cloud Computing Strategy
- Non-CFO Act agencies may consider the purpose and priorities of Data Center Optimization and Cloud Strategy guidance as recommended practices.

Small Agency Considerations

Know your enterprise portfolio inventory of hardware and software and their order of mission operational importance. This information can be used to plan for data center tiering requirements and redundancy requirements. Consider conducting a Business Impact Analysis.

Understand your production pain points and actively solve these issues. Pain points can include not having the ability to keep up with new technology, IT not being a core capability, reliability of data centers, and lack of high speed access to cloud services.

In addition to continuity of operations (COOP) and disaster recovery (DR) testing, you should include a data center operations manual that describes all operational functions and responsibilities and can be understood across all components (i.e., IT operations, facilities, and physical security) so that the data center can still operate in an emergency situation.

Strongly consider using colocation facilities to house your systems. Commercial colocation facilities offer significant capability, resilience, and reliability, while also offering high-speed network access to cloud computing services.

Resources for Executives

- Consider participating in the Data Center and Cloud Optimization Initiative (DCCOI) Community of Practice to share ideas and seek out assistance from other federal agencies.
- Federal data center policies and guidelines
- Energy efficiency in small data centers
- Solutions, programs, partners, events, and more
- Data center design guidelines
- Data Center and Cloud Optimization Initiative

Additional Resources

- Data Center and Cloud Optimization Initiative Project Management Office (PMO) Email: DCCOI@GSA.gov.
- The Application Rationalization Playbook: An Agency Guide to Portfolio Management
- Application Rationalization Data Dictionary (GSA)

Cloud Operations and Optimization Management

Overview

At its most basic, cloud computing represents a specific way of delivering computing services. Since 2010, the National Institute of Standards and Technology (NIST) has provided a widely accepted definition of cloud computing. NIST Special Publication 800-145, The NIST Definition of Cloud Computing, identifies the following "five characteristics that must be available in a computing capability to qualify as a 'cloud service.'"[41]

- On-demand self service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Cloud computing enables convenient access – most often via the Internet – to a shared pool of configurable computing resources (i.e., servers, networks, storage, applications). Users can provision cloud services on demand with minimal human intervention.[42,43]

NIST Special Publication 500-322 provides definitions and clarifications for cloud computing. Cloud services can be categorized by the type of computing capability that is provided. In general, "the term 'as a [cloud] Service' is a suffix describing a computing capability that

[41] Simmon, E. (2018, February). *Evaluation of Cloud Computing Services Based on National Institute of Standards and Technology SP 800-145*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf

[42] U.S. General Services Administration. (2010, July 21). *Cloud Computing: Statement of Dr. David McClure, Associate Administrator, Office of Citizen Services and Innovative Technologies, General Services Administration, Before the House Committee on Oversight and Government Reform Subcommittee on Government Management, Organization, and Procurement*. Gsa.gov. https://oversight.house.gov/wp-content/uploads/2012/01/20100701McClure.pdf

[43] Mell, P., & Grance, T. (2022, September 1). *SP 800-145 The NIST Definition of Cloud Computing*. Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-145/final

supports all five essential characteristics of cloud computing."[44] There are three general cloud services categories:

- **Software as a Service (SaaS):** Cloud-enabled applications (e.g., web or mobile) accessible via broad network access (not desktop applications installed on a virtual machine). SaaS provider is responsible for deploying, configuring, maintaining, and updating the software, along with any PaaS or IaaS dependencies.
    - Primary users: end users
- **Platform as a Service (PaaS):** Capability to develop and deploy applications created using programming languages, libraries, services, and tools supported by the cloud service provider, without the complexities of managing underlying infrastructure services.
    - Primary users: developers
- **Infrastructure as a Service (IaaS):** Networking, storage, and compute resources (e.g., servers and operating systems). In IaaS context, "software" and "application" refer to VM/desktop software and applications rather than cloud-enabled SaaS or web applications.
    - Primary users: IT operations

NIST SP 800-145 defines four cloud infrastructure deployment models:[45]

- Public: for use by the general public.
- Private: for use by a single organization.
- Community: for use by a community of users with shared concerns.
- Hybrid: composed of two or more distinct cloud infrastructures that are bound together by standardized or proprietary technology that enables data and application portability.

Cloud services offer several benefits including scalability, innovative technology, outsourcing operational responsibility, and improved disaster recovery capabilities. Typically, cost savings are not considered a benefit as cloud costs can be similar or higher.

The Federal Government has developed the Federal Cloud Computing Strategy called Cloud Smart to provide overarching strategic guidance for agency cloud adoption. The three pillars of the strategy are security, procurement, and the workforce. GSA developed multiple guidance

[44] Simmon, E. (2018, February). *Evaluation of Cloud Computing Services Based on National Institute of Standards and Technology SP 800-145*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf
[45] Mell, P., & Grance, T. (2011, September 1). *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology (SP 800-145)*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

documents and tools to assist agencies with migrating services to the cloud. (See Additional Resources in this section.)

Details

Enterprise Cloud Adoption Strategy

Before moving to enterprise cloud adoption, it is critical to develop a cloud strategy for your agency. Cloud strategies should fit the agency-specific mission, business, technology, and security needs, and policy limitations.[46] The Federal Cloud Strategy Guide: Agency Best Practices for Cloud Migration provides detailed guidance about major topics to consider in your cloud strategy. Key points are included in this section. If your agency is unable to use existing guidance available through CIO.gov, you can hire contract partners to conduct thorough assessments and develop a cloud strategy for your agency. A predefined Statement of Objectives Templates for such work can be accessed at the Cloud Information Center (CIC).

To start, agencies should do a thorough current state assessment of applications, services, network infrastructure, security posture, and workforce capabilities. Use the assessment to identify business needs and drivers of cloud adoption and to formulate a business case.

Identify agency goals, objectives, actions, and success criteria for the next two to five years. The cloud adoption strategy should align to your agency's strategic plans and answer the following questions:

- Why move to the cloud?
- What are we moving or acquiring from the cloud?
- What's the value proposition?
- Are we developing a workforce to support the new capabilities and service delivery model?
- Who are the stakeholders involved and how do they make decisions about the cloud?

As a general guiding principle, small agencies should leverage SaaS solutions to the greatest extent possible. Moving to SaaS solutions provides significant value since heavy technical skill sets are not required to maintain and operate the system. The responsibility is on the vendor to ensure the system is operational, secure, and updated. Many SaaS solutions are delivered via the web, which simplifies deployment and use of the system. Although the operational burden of maintaining and running the system is with a vendor, it is important to recognize that agency staff will need to focus on service and vendor management. They will need to be familiar with

[46] MAX Federal Community. *Federal Cloud Strategy Guide: Agency Best Practices for Cloud Migration*. MAX.gov. https://community.max.gov/download/attachments/2184717903/Cloud%20Strategy%20Guide%20v1.1.pdf?api=v2

the terms and conditions of the contract with the vendor and ensure governance policies are instituted to manage the relationship with the vendor.

PaaS solutions should be considered when organizations need to develop or customize software, provide analytics and business intelligence capabilities, and other services that require customization but without the focus on maintaining infrastructure. Consider PaaS solutions over IaaS when possible.

IaaS solutions should be used when your agency has a legitimate need to maintain their own infrastructure. This will require the greatest technical expertise and the majority of the responsibility to maintain and secure the environment will be with the agency.

Agency cloud strategies should focus on systems and individual applications and identify goals for each application. Use the Application Rationalization Playbook framework to evaluate your existing application environment. Conduct a thorough discovery process to understand what applications you have, your network infrastructure, where your data is located, traffic patterns, and requirements. These are just a few of the data points that should be documented. Your agency will also have to assess each application's readiness for cloud migration and identify the approach to use. There are five industry standard approaches for application migration: Rehosting, Refactoring, Rearchitecting, Rebuilding and Replacing applications. For each application, document which of the five approaches will be used.

It is also important to consider the budget implications of adopting cloud services when formulating your strategy. Cloud service costs are measured using an operating expense (OPEX) model instead of the capital expense (CAPEX) model used for many IT investments. Furthermore, consider more regularly occurring cloud operational expenditures (OpEx) in place of uneven on-premise IT capital expenditures to improve the flexibility and efficiency of your agency IT budget.

Cloud Acquisitions

Agencies have faced challenges with acquisition of cloud services because cloud services do not easily fit legacy procurement methods. GSA's Cloud Ordering Guide addresses common challenges and provides ordering guide details. The GSA Cloud Team is also available to consult with agencies on these topics at no charge and can be reached at cloudinfo@gsa.gov. They offer a quarterly "How to Buy Cloud for Government" webinar; view the schedule on the GSA events webpage.

Ensure your agency leverages the Federal Risk and Authorization Management Program (FedRAMP®) for your cloud services when applicable. FedRamp authorizes cloud products and services using a standardized security framework that ensures compliance with current FISMA security requirements.

Work with an acquisition specialist to address the following common challenges:

- Type of Contract: Which type of contact is best for cloud services, which are often billed on a time-metered basis like electricity or labor hours.
- Financing: 1- to 3-year cloud instances may be billed in 1- to 3-year increments using funds that must be expended within one fiscal year.
- Budgeting: The exact projected annual spend may not be known.
- FedRAMP Requirements: How to include FedRAMP in solicitation requirements.
- Small Business Goals: Difficulty defending a small business set aside for cloud services (even when using a small reseller) because the Small Business Administration (SBA) considers cloud a service so the nonmanufacturer rule does not apply.
- Procurement strategy: How a Blanket Purchase Agreement (BPA) may help solve some of these issues.

Cloud Workforce Considerations

Having a workforce that's capable of supporting cloud technologies should be a key part of your overall cloud strategy. The CIO organization should work with human resources and other senior agency officials to identify skill gaps and develop hiring or retraining strategies. One approach is to map the new skills required to manage, broker, and operate cloud services to legacy job series and categories. CIOs should plan for continuous and progressive skills training (i.e., upskilling) and education. All IT disciplines are impacted by cloud adoption regardless of title and will need some foundational training.

Recruitment may be challenging with a large pay disparity between General Schedule (GS) employees and the private sector. Emphasize benefits, such as remote work, mission and work-life balance, in addition to pay. Also, consider hiring contract staff to fill skills gaps, but ensure you understand the types of skill sets needed to carry out management activities in complex environments. Agencies can use GSA contract vehicles to acquire complete solutions that include cloud services along with the requisite contract workforce to support them.

Cloud Financial Management

It's important to manage the costs associated with your cloud services. SaaS solutions are fairly easy to understand and manage since they are subscription based and the vendor handles the infrastructure. However, PaaS and IaaS solutions can be more complex as usage is variable. Agencies can leverage spend tools built in the cloud service to get an overview of their expenditures, but it's recommended to take a structured approach to govern cloud service spending.

FinOps (Finance Operations) is an evolving financial management framework based on collaboration of business, finance, technology, and engineering teams to make data-driven spending decisions.[47] Cloud FinOps is a term for the practice of cloud financial and cost management. The FinOps Foundation describes FinOps as a model "for teams to manage their cloud costs, where everyone takes ownership of their cloud usage supported by a central best-practices group."[48] Unmanaged and ungoverned cloud services (especially IaaS) can lead to significant cost overruns. It's important to implement guardrails to ensure costs are accounted for, managed, and allocated to the consumers of these resources.

To accurately calculate the total cost of ownership for technology like applications and systems across the enterprise, it can be helpful to allocate shared costs to specific functions or business units. It is also important to separate, identify, and assign client-specific services. Shared cost allocation especially applies to cloud services, but the principle can be applied to any type of shared service, such as administrative, operational, and overhead costs. An allocation mechanism should proportionalize costs from shared services to sub-accounts or business units based on spend or consumption.

Compute and storage are typically the primary cost drivers for IaaS spend. Compute services can be billed on demand, which is typically billed per hour of use. Once there is an understanding of your compute workload, saving plans or reserved instances should be purchased. Both plans are discount billing constructs that are applied to compute resources. They require a certain level of spend commitment and can save, on average, up to 20 to 30 percent for a one-year commitment and up to 40 to 70 percent for a three-year commitment.

It is important to note there is not a 1-1 relationship for on-premise resources being migrated to the cloud. This means you must pay close attention post migration to compute utilization and performance needs so you can fine tune to the right instance, size, and type. Savings plans are the recommended approach unless there is a specific need for reserved instances. Either way, commitments should be purchased at approximately 80 percent of standard demand, ensuring you maximize savings and you are not overcommitting.

Storage tends to be configured and forgotten. In the cloud, storage costs can spiral out of control. Snapshots, commonly used for backup, need to be managed on a daily or weekly basis so older snapshots can be deleted. In many instances, this process can be scripted and automated. Also, storage is often over provisioned, unattached, or underutilized, incurring unnecessary costs.

Depending on your environment, these cloud cost management practices will need to be incorporated into the existing processes of the cloud or engineering teams, and management of

[47] FinOps Foundation. (2021, November). *What is FinOps?* FinOps.org https://www.finops.org/introduction/what-is-finops/

[48] FinOps Foundation. (2021, November). *What is FinOps?* FinOps.org https://www.finops.org/introduction/what-is-finops/

cloud resources will need to be done at a regular cadence. Establishing metrics and monthly reporting will provide insight to the Technology Business Management (TBM) team and leadership. Anomaly detection, cost allocation, and trending over time are common reports that help provide insight and data-based decision making. From a forecasting perspective, having this data will help predict future budgeting activities and planning for additional or renewed savings plans. Chargeback or showback will provide transparency of costs directly to the business consumers.

FinOps methods (and third party solutions to support implementation) can help your agency rightsize resource consumption by more accurately estimating compute and storage. Other considerations include decommissioning unused services and making better informed decisions on scheduling services and platform configuration.

Cloud Operations and Technical Management

Establish and maintain agency enterprise cloud design documents and guides. This can be a single document or a series of documents that define the physical implementation of the cloud environment for the agency as well as the processes and procedures related to managing the cloud environment. Use agency cloud readiness assessments and agency cloud strategy documents as inputs. Some agencies hire vendors to create these artifacts. The agency enterprise cloud design documents should contain some of the following:

- Account management
- Network design
- Cloud Service Provider user security, identity, and access management design
- Cloud security management
- Cloud Service Provider compute management
- Cloud Service Provider monitoring, logging, alerting, and resource analytics
- Disaster and failure recovery
- Cloud application architecture and management
- Cloud service delivery
- Cloud governance, risk, and compliance
- Foundational cloud implementation plan

It is also important to understand Cloud Network Administration. Document a design that includes the following:

- Routes
- Subnets

- Access control lists (ACLs)
- Security groups

Also, account for a design that is resilient to failure by leveraging availability zones, load balancing (ELB), multiregional capabilities, and a virtual firewall designed for resiliency and integration with internal network services, such as domain name system (DNS), dynamic host configuration protocol (DHCP), and IP address management.

Develop a cloud data management and storage design document to identify the processes, procedures, and best practices around managing and utilizing storage in the cloud. This includes but is not limited to file storage, object storage, buckets, and containers. Additionally, develop a database usage design to identify database options and best practices around using the different cloud database technologies.

Security is also a core consideration for your agency's IaaS solutions. Ensure your teams implement solutions and designs to support monitoring, logging, alerting, and resource analytics.

Federal Requirements

- Federal Cloud Computing Strategy

  https://cloud.cio.gov/

Small Agency Considerations

- Leverage SaaS solutions where available to overcome human resource limitations (i.e., workload and expertise.)
- Recruit and manage cloud workforce. Government employees will still need to have a core role.

Resources for Executives

- Data Center and Cloud Infrastructure Community of Practice
- Cloud Service Models Overview (DOI)

Additional Resources

GSA publishes the online Cloud Information Center (CIC), which contains cloud requirements templates and many other valuable resources.

Cloud Strategy

GSA Office of Government-wide Policy (OGP)

- Federal Cloud Strategy Guide
- Small Agency Cloud Strategy Toolkit
- Application Rationalization Guide

Acquisition

The Cloud Ordering Guide is found on the CIC site and details each of the topics in the cloud section of the Small Agency CIO Handbook.

https://cic.gsa.gov/acquisitions/acquisition-challenges

FinOps

- Use the resources available from the FinOps Foundation to manage your cloud costs and optimize your services. Other resources available are the FinOps Playbook and Cloud Tagging Strategy Guide.

IaaS Tagging Guide

- Multi-Cloud and Hybrid Cloud Guide and several other publications about cloud adoption can be found on CIO.gov.

Data Management

Overview

Data is defined as "recorded information, regardless of form or the media on which the data is recorded."[49] This includes information resources in any medium, including paper and electronic information, that is managed by your agency or vendors.[50] As increasing attention is given to federal data as both a strategic asset and a valuable national resource, agencies are required to establish comprehensive approaches for the acquisition, management, and use of their information resources. In general, policies that focus on improving the use of data also highlight security and privacy.

[49] 44 U.S.C. § 3502 (16) (2019). Coordination of Federal Information Policy. *Public Printing and Documents*. Uscode.house.gov. https://uscode.house.gov/view.xhtml?path=/prelim@title44/chapter35&edition=prelim

[50] U.S. Office of Management and Budget. (2016, July 28). *Managing Information as a Strategic Resource (Circular A-130)*. Executive Office of the President. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

Each agency is required to designate a Chief Data Officer (CDO).[51] Agency responsibilities related to managing "information resources (defined as "information and related resources, such as personnel, equipment, funds, and information technology")," including CDO responsibilities, are enumerated in 44 U.S.C., Chapter 35 ("Coordination of Federal Information Policy"), Subchapter I ("Federal Information Policy").[52] In addition, agencies can expect continued prioritization of governmentwide initiatives related to data, such as the examples below:

- In 2019, OMB Memorandum M-19-18 Federal Data Strategy: A Framework for Consistency presented a "10-year vision for how the Federal Government will accelerate the use of data to deliver on mission, serve the public, and steward resources while protecting security, privacy, and confidentiality."[53] The framework identifies 10 operating principles and a set of 40 best practices to "guide agencies in leveraging the value of federal and federally-sponsored data."[54]
    - **Agencies are directed by** annual governmentwide action plans that prioritize practice-related steps to support the Strategy's implementation.
- OMB Circular A-130–Managing Information as a Strategic Resource recognizes federal information as a strategic asset and national resource.
    - **Agencies are directed to** establish a comprehensive approach to improve the acquisition and management of information resources by implementing policy directives across a wide range of areas including IT planning, budgeting, governance, acquisition, enterprise architecture, information management, privacy, security, and records management.
        - An Information Resource Management (IRM) Strategic Plan should be developed and reviewed annually to identify agency's technology and information resources goals and demonstrate how they align with the agency's mission and organizational priorities.[55]

[51] 115th Congress. (2019, January 14). Foundations for Evidence-Based Policymaking Act of 2018. Pub.L. 115–435 § 202, 132 Stat. 5541. https://uscode.house.gov/view.xhtml?path=/prelim@title44/chapter35&edition=prelim

[52] 44 U.S.C. § 3502 (16) (2019). Coordination of Federal Information Policy. *Public Printing and Documents*. Uscode.house.gov. https://uscode.house.gov/view.xhtml?path=/prelim@title44/chapter35&edition=prelim

[53] Federal Data Strategy. FDS Framework: Mission, Principles, Practices, and Actions. *President's Management Agenda.* Strategy.data.gov. https://strategy.data.gov/assets/docs/2020-federal-data-strategy-framework.pdf

[54] Federal Data Strategy. FDS Framework: Mission, Principles, Practices, and Actions. *President's Management Agenda.* Strategy.data.gov. https://strategy.data.gov/assets/docs/2020-federal-data-strategy-framework.pdf

[55] U.S. Office of Management and Budget. (2016, July 28). *Managing Information as a Strategic Resource* (Circular A-130). Executive Office of the President. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

    - Data as a Strategic Asset is one of four priorities for a recent Annual Federal IT Operating Plan (2022).[56]
- The Foundations for Evidence-Based Policymaking Act of 2018 contains four titles that include "Federal Evidence-Building Activities" and "Open Government Data Act."[57]
    - **Agencies are directed to:**
        - Include in the agency strategic plan a list of different types of data used to support policymaking.
        - In conjunction with the agency performance plan, develop an evaluation plan that identifies key questions for evaluation and information to collect in the upcoming fiscal year.
        - Improve public access to data by making government data available in an open format that is easily accessed and used, thereby improving the "timeliness, completeness, consistency, accuracy, usefulness, and availability of open Government data assets and " prioritizing "data asset[s] for which disclosure would be in the public interest."
        - Establish a Chief Data Officer in each agency.

[56] U.S. Office of Management and Budget. (2022). *Federal Information Technology Operating Plan*. CIO.gov https://www.cio.gov/assets/files/Federal-IT-Operating-Plan-June-2022.pdf; Federal Data Strategy. FDS Framework: Mission, Principles, Practices, and Actions. *President's Management Agenda.* Strategy.data.gov. https://strategy.data.gov/assets/docs/2020-federal-data-strategy-framework.pdf

[57] 115th Congress. (2019, January 14). *Foundations for Evidence-Based Policymaking Act of 2018*. Pub.L. 115–435 § 202, 132 Stat. 5541 https://www.congress.gov/115/plaws/publ435/PLAW-115publ435.pdf

Table 10. *Data Capabilities and Recommended Tools and Technologies*

Capability	Recommended Tools and Technologies
Storage	● SQL ● Data lakes ● Data warehouses
Preparation and ETL	● Data integration and ETL tools ● Automated data flow mapping
Governance	● Metadata catalog tool with data asset discovery ● Governance tool that integrates metadata catalog, governance, and integrity ● Governance tool to implement and automate management, organization, and stewardship of data assets
Modeling	● Modeling tool that provides enterprise-grade semantic modeling
Analytics	● Statistical software to conduct scheduled and ad-hoc analysis of big and complex data
Visualizations	● Data visualization tool that integrates with analytics, with foci on business intelligence and geospatial data, as appropriate for agency mission
Collaboration and Access Control	● Directory and identity management service with conditional access controls for data ● Interactive tool that allows users to share and compile data

A variety of tools and technologies are needed to enable modern data capabilities, as shown above in Table 10. The capabilities of a modern data program should include:

- Storage,* which refers to the physical and digital record of data.
- Preparation* and Extract, Transform and Load (ETL),* often grouped together because they both help convert data from different sources to a single structure.
    - Preparation refers to the cleaning and consolidating raw data.
    - ETL refers to the three-step process by which data is moved from a data source (e.g., a database) to a single data repository (e.g., a data lake or data warehouse).

- Governance,* which refers to the internal standards and controls that establish priorities over how data is managed.
- Modeling, which refers to the conceptualization of how and which data will be stored and used.
- Analytics,* which refers to the systematic examination of data in order to gain insights and inform decision making.
- Visualizations, which refers to graphical representations of data to better convey insights gained from analytics.
- Collaboration and Access Control,* which refer to processes by which an organization shares its data with authorized users and protects its data from unauthorized users.

* Essential capabilities should be prioritized over the others when influenced by time, personnel, and funding constraints. (Table 10)

Details

A key role for the CDO is to be a data champion and leader at the executive level. The CDO should demonstrate the power of data and encourage its use across the agency by telling compelling stories with data. CDOs typically manage the data lifecycle, drive the data strategy to serve the agency mission, and focus on data-related risk, compliance, and policy. The CDO role, along with 14 foundational responsibilities, was introduced in the Foundations to Evidence-Based Policymaking Act and codified in 44 U.S.C. Chapter 35, Subchapter I.[58] New policies and guidance continue to provide details about the full scope of agency responsibilities related to information management, including data security, privacy, and records management.

While many Chief Data Officers (CDOs) report to the CIO or IT Executive, in some agencies the CDO and CIO report to different executives. In some small agencies, one person may act as both CIO and CDO. Regardless of organizational structure, agency leadership must ensure all information resources management responsibilities and requirements have clear owners. Special attention should be made to policies that may overlap roles or reporting structures, such as:

- IT investment budgeting and approval
- Records retention regulations
- FOIA responsiveness

The CDO should lead the agency data strategy. A data strategy is informed by an enterprisewide survey and analysis of current and future use cases related to the collection, analysis, use, storage, and disposal of data. The CDO should work with program offices and

[58] 115th Congress. (2019, January 14). *Foundations for Evidence-Based Policymaking Act of 2018*. Pub.L. 115–435 § 202, 132 Stat. 5541. https://www.govinfo.gov/content/pkg/PLAW-115publ435/pdf/PLAW-115publ435.pdf

stakeholder groups to develop current data flows and identify use cases that answer questions such as:

- Who is using data? Determine user behavioral patterns around data by identifying informational use cases and understanding from a user perspective what is usual and unusual activity pertaining to data (e.g., time, file sizes, data usage).
- What data are being collected? How useful are the data? Consider the availability and usefulness of data collected from external sources and the technical and managerial burdens it may impose. For example, is the data machine readable? Is it in an open format? Is anyone using the data after it comes in?
- How are data being categorized? Categorization of data (e.g., using metadata tags) is an indispensable aspect of data management because they allow CDOs and IT Executives to identify, track, organize, and analyze their agencies' data.
- How are data being protected? Establish robust identity and access management so data are not only secure (i.e., restricts unauthorized users), but users also are easily assigned and granted the correct level of access to the appropriate data.

Data flow diagrams can be used to identify duplicative, inefficient processes and security risks. By analyzing data flows and identifying areas of overlap, the CDO can design a data architecture that supports the agency's data strategy.

The CIO or IT Executive is positioned to support designing and implementing technical architecture and acquiring and integrating additional tools and technologies to support the data architecture and strategy. The CIO or IT Executive focuses more broadly on the management of the agency IT portfolio, spanning across eight areas: IT leadership and accountability, IT strategic planning, IT workforce, IT budgeting, IT investment management, cybersecurity and privacy, architecture, and information resources and data.[59] The CDO and CIO should work together to develop a data management strategy to prioritize investments and allocations across the infrastructure.

Data management is multidisciplinary. CDOs must consider the role of data in both the presentation layer (i.e., the front end) and the data access layer (i.e., the back end). A CDO should have training and experience in at least one of the following disciplines: "data management, governance (including creation, application, and maintenance of data standards), collection, analysis, protection, use, and dissemination."[60,61] Equally important is the ability to

[59] U.S. Chief Information Officers Council. *CIO Handbook.* CIO.gov https://www.cio.gov/handbook/cio-role-at-glance/

[60] 115th Congress. (2019, January 14). *Foundations for Evidence-Based Policymaking Act of 2018*. Pub.L. 115–435 § 202, 132 Stat. 5541. https://www.govinfo.gov/content/pkg/PLAW-115publ435/pdf/PLAW-115publ435.pdf

[61] Data Management Body of Knowledge is a valuable and comprehensive resource on data management.

negotiate and partner with professionals across disciplines to effectively use data to impact mission and performance.

The CDO, IT Executive, and Agency Director must be aware of federal requirements related to privacy and records management.

- Each agency must designate a Senior Agency Official for Privacy (SAOP) who is responsible for "implementation of privacy protections; compliance with federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals."[62]
- Each agency also must designate a Senior Agency Official for Records Management (SAORM). As described in the CIO Handbook, the SAORM ensures the agency "efficiently and appropriately complies with all applicable records management statutes, regulations, National Archives and Records Administration (NARA) policy, and OMB policy."[63]
    - As defined by 36 CFR § 1222.22,

      "To meet their obligation for adequate and proper documentation, agencies must prescribe the creation and maintenance of records that:

      (a) Document the persons, places, things, or matters dealt with by the agency.

      (b) Facilitate action by agency officials and their successors in office.

      (c) Make possible a proper scrutiny by the Congress or other duly authorized agencies of the Government.

      (d) Protect the financial, legal, and other rights of the Government and of persons directly affected by the Government's actions.

      (e) Document the formulation and execution of basic policies and decisions and the taking of necessary actions, including all substantive decisions and commitments reached orally (person-to-person, by telecommunications, or in conference) or electronically.

      (f) Document important board, committee, or staff meetings."[64]

[62] U.S. Chief Information Officers Council. Senior Agency Official for Privacy (SAOP). *Federal Chief Information Officers Handbook.* CIO.gov. https://www.cio.gov/handbook/key-stakeholders/saop/?clickEvt

[63] U.S. Chief Information Officers Council. Senior Agency Official for Records Management (SAORM). *Federal Chief Information Officers Handbook.* CIO.gov. *https://www.cio.gov/handbook/key-stakeholders/saorm/?clickEvt*

[64] 36 CFR § 1222.22

- In addition, the CIO Handbook identifies these additional responsibilities for the SAORM:[65]
  - Setting the vision and strategic direction for the agency records management program, including incorporating these goals into the agency's Strategic Information Resources Management (IRM) Plan.
  - Formally designating the Agency Records Officer and informing NARA in writing of this decision.
  - Ensuring the agency protects records against unauthorized removal or loss and ensures all agency staff are informed of their records management responsibilities as defined in NARA regulations and guidance.
  - Ensuring agency staff are informed of and receive training on their records management responsibilities as defined in NARA regulations and guidance.
  - Ensuring compliance with NARA requirements for electronic records including:
    - Managing all permanent electronic records electronically to the fullest extent possible for eventual transfer and accessioning by NARA in an electronic format.
    - Managing all email records electronically and retaining them in an appropriate electronic system that supports records management and litigation requirements, including the capability to identify, retrieve, and retain the records consistent with NARA-approved disposition authorities and regulatory exceptions.

Federal Requirements

In addition to the data-specific policies below, there are requirements around cybersecurity, budgeting, and other topics throughout this handbook that have implications for data management.

Foundations for Evidence-Based Policymaking Act of 2018:

- https://www.govinfo.gov/content/pkg/PLAW-115publ435/pdf/PLAW-115publ435.pdf

M-19-23 Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance:

[65] U.S. Chief Information Officers Council. Senior Agency Official for Records Management (SAORM). *Federal Chief Information Officers Handbook*. CIO.gov. https://www.cio.gov/handbook/key-stakeholders/saorm/?clickEvt

- https://www.whitehouse.gov/wp-content/uploads/2019/07/M-19-23.pdf

M-20-12 Phase 4 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Program Evaluation Standards and Practices (March 2020):

- https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-12.pdf

M-21-27 Evidence-Based Policymaking: Learning Agendas and Annual Evaluation Plans (June 30, 2021):

- https://www.whitehouse.gov/wp-content/uploads/2021/06/M-21-27.pdf

For additional mandates and requirements, please refer to Appendix A in the CDO Playbook:

- https://resources.data.gov/assets/documents/CDO_Playbook_2021.pdf

Information related to Federal records management

https://www.archives.gov/records-mgmt/policy

Small Agency Considerations

The first few months in the CIO and CDO role are critical for developing high-level agency priorities related to the data strategy.

- Determine the current and target state of the data operating model and conduct a gap analysis to identify roles and competencies related to data and IT that are needed to move toward the target state.[66]
    - Determine whether functions should be centralized or distributed, outsourced or insourced, and the agency's capacity for change.
- Communicate the value proposition to stakeholders whose work and outcomes will benefit from the changes, and those that will help drive your strategy. Establish partnerships with cybersecurity and technology teams.
- Establish or refine, socialize, and implement data governance controls, including governance structure, roles, policies, and procedures.
    - All federal agencies are expected to name members and charter a data governance body, which the CDO must chair.[67]

[66] A requirement of the Federal Data Strategy is a Data Maturity Assessment. Note the Federal Data Strategy 2020 Action Plan and 2021 Action Plan.
[67] Federal Data Strategy. (2020). *2020 Action Plan*. Strategy.data.gov https://strategy.data.gov/2020/action-plan/

- Develop metrics that emphasize the value of data to key agency stakeholders and begin tracking the execution of data strategy, according to these metrics.

Resources for Executives

- Federal Data Strategy: https://strategy.data.gov/overview/
- Federal Data Strategy: 2021 Action Plan: https://strategy.data.gov/assets/docs/2021-Federal-Data-Strategy-Action-Plan.pdf

Additional Resources

- Federal CDO Council: https://www.cdo.gov/
- CDO Playbook: https://resources.data.gov/assets/documents/CDO_Playbook_2021.pdf
- CDO Council on OMB MAX: https://community.max.gov/display/DATA/CDO+Council+Home+Page
- Data.gov: https://data.gov/

Cybersecurity

Overview

Cybersecurity involves preventing, detecting, and responding to cyberattacks, which are malicious attempts to access or damage a computer or network system.[68] Cyberattacks can prevent access to and disrupt the functioning of internal and public networks, systems, and applications. Attacks can also be specifically targeted at misusing, destroying, or preventing access to data and information. In addition to operational and privacy risks, cyberattacks can damage the public's trust in technology systems and data. Agencies are required to report on specific cybersecurity metrics annually as part of the Federal Information Security Modernization Act (FISMA). The Federal CIO Handbook provides detailed information for this requirement and can be found here. Additionally, the Cybersecurity and Infrastructure Security Agency provides annual FISMA-related reporting documentation here.

Details

The Cybersecurity and Infrastructure Security Agency (CISA) leads the Federal Government's approach to cybersecurity. The National Institute of Standards and Technology (NIST) developed and maintains a cybersecurity framework. As cyberattacks constantly evolve, CISA recommends leaders: (1) develop a culture of cyber readiness and (2) implement a cybersecurity risk management approach to identify risk, reduce vulnerabilities, and plan for

[68] Ready. *Cybersecurity.* Ready.gov https://www.ready.gov/cybersecurity

contingencies.[69] CISA's Cyber Essentials website contains concise, actionable resources for leaders of small agencies to develop and implement organizational cybersecurity practices.

A key goal of cybersecurity is to prevent malicious actors from gaining access to systems and information. The following are common ways attackers try to gain access:

- Scam emails
- Infected websites, online ads
- Unauthorized use of passwords (e.g., stolen passwords, insider misuse of privileges)
- Password attacks through brute force (i.e., trial and error), key logging
- Security flaws in software (i.e., a zero-day attack) where vulnerabilities are "exploited by threat actors before a patch is developed and applied"[70]
- Server vulnerabilities
- Internet of Things (IoT) vulnerabilities. The Internet of Things describes physical objects (e.g., cameras, thermostats, door locks, cars, parking meters, and medical devices) that connect to the Internet. Such objects contain sensors and computing power to collect and transmit data and execute code
- Infecting physical elements of the supply chain
- Removable media, such as flash drives (e.g., given away at conferences)
- Loss or theft of devices containing confidential information[71,72]

After gaining unauthorized access to systems or information, the following types of cyberattacks can occur:

- Malware (i.e., malicious software) installation, which are applications that can perform malicious actions for the purpose of theft, extortion, disruption; includes spyware, ransomware, viruses

---

[69] Cybersecurity & Infrastructure Security Agency. (2021, Spring). The Basics for Building a Culture of Cyber Readiness. *CISA Cyber Essentials Starter Kit*. CISA.gov https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf

[70] U.S. Department of Health & Human Services (HHS) Cybersecurity Program. (2021, November 18). *Zero-Day Attacks*. U.S. Department of Health & Human Services. https://www.hhs.gov/sites/default/files/zero-day-attacks-tlpwhite.pdf

[71] Division of Banks. Know the Types of Cyber Threats. *Executive Office of Housing and Economic Development*. Mass.gov https://www.mass.gov/service-details/know-the-types-of-cyber-threats

[72] Federal Trade Commission. Cybersecurity Basics. *Cybersecurity for Small Businesses*. FTC.gov https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf

- Phishing, which collects sensitive information like login credentials and credit card information
- Distributed Denial of Service (DDoS), which involves multiple compromised devices targeting and overwhelming a server with traffic

The Federal Government is moving to a security model known as zero trust architecture (ZTA). A zero trust model eliminates implicit trust in any "actor, system, network, or service operating outside or within the organization's security perimeter."[73] Instead, anything and everything attempting to establish access must be verified. In addition, a zero trust approach only allows users access to the bare minimum they need to perform their jobs. It is a paradigm shift from a single, one-time verification at the network or system perimeter to the continual verification of each user, device, application, and transaction.[74,75]

CISA's Cyber Essentials Starter Kit is written for organization leaders and identifies the following essential elements and associated objectives for *Building a Culture of Cyber Readiness:*[76]

- **The Leader:** Drives cybersecurity strategy, investment, and culture.
- **Staff:** Develops security awareness and vigilance.
- **Systems:** Protect critical assets and applications.
- **Digital Workplace:** Ensures only those who belong on the digital workplace have access.
- **Data:** Make backups and avoid loss of critical information.
- **Crisis Response:** Limit damage and quicken restoration of normal operations.

[73] Young, S. (2022, January 26). *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*. Department of Defense.
https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
Defense Information Systems Agency & National Security Agency Zero Trust Engineering Team. (2022, July). *Zero Trust Reference Architecture*. Department of Defense.
https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[74] Young, S. (2022, January 26). *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*. Department of Defense.
https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[75] Biden, J. (2021, May 12) *Executive Order on Improving the Nation's Cybersecurity.* The White House.
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[76] Cybersecurity & Infrastructure Security Agency. (2021, Spring). The Basics for Building a Culture of Cyber Readiness. *CISA Cyber Essentials Starter Kit*. CISA.gov
https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf

CISA Insights publication, “Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats,” provides the following foundational steps for an organization to improve security:[77,78]

Prevent

- Train all staff about cybersecurity.
- Implement multi-factor authentication (MFA) for all users; prioritize privileged, administrative, and remote access users.
- Keep all software up to date by enabling automatic updates, replacing unsupported operating systems, applications, and hardware, and testing and deploying patches quickly.
- Secure, protect, and back up sensitive data by employing a backup solution that automatically and continuously backs up critical data and system configurations. Encrypt sensitive data, at rest and in transit.

Detect

- Confirm the organization's entire network is protected by antivirus and antimalware software.
- Establish the capacity to identify unexpected or unusual network behavior.

Be Prepared to Respond

- Designate a crisis response team with main points of contact for a suspected cybersecurity incident and assign roles and responsibilities within the organization, including technology, communications, legal, and business continuity.
- Ensure key personnel are available to provide surge support for an incident. Maximize the organization's resilience to a destructive cyber incident.
- Test backup procedures to ensure critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure backups are isolated from network connections.

---

[77] Cybersecurity & Infrastructure Security Agency. (2022, January 18). Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats. *CISA Insights*. CISA.gov https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf

[78] U.S. Small Business Administration. *Strengthen Your Cybersecurity*. SBA.gov https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity#section-header-4

Federal Requirements

Executive Order on Improving the Nation's Cybersecurity

M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

Annual FISMA requirements

Resources

- Federal Chief Information Security Officer (CISO) Council
    - Small / Micro-Agency Chief Information Security Officers Council (SMAC)

CISA

- CISA runs a number of programs for small agencies, including the Continuous Diagnostics and Mitigation (CDM) Program, Homeland Security Information Network (HSIN), information sharing, assessments, and many others.
    - Small agencies should interact with CISA and its many sources of information and support to harden and secure the Federal Government's assets.
    - Please refer to the CISA Programs and Resources section in this document.

NIST

- Small Business [Agency] Risks and Threats
- Cybersecurity Basics Glossary
- Small Business [Agency] Cybersecurity Corner

CISA Programs and Resources

Overview

The Cybersecurity and Infrastructure Security Agency (CISA) offers a range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust and resilient cyber framework.

Details

CISA provides the following professional, no-cost assessments to help agencies manage risk and strengthen cybersecurity. For the latest content about each, use the CISA Cyber Hub page.

- Assessment Evaluation and Standardization (AES) program
- Vulnerability Scanning: a persistent "internet scanning-as-a-service" to continuously assess the health of internet-accessible assets by checking for known vulnerabilities,

weak configurations (or configuration errors) and suboptimal security practices. The service also recommends ways to enhance security through modern web and email standards.

- Cyber Resilience Review (CRR): evaluates the maturity of an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities across 10 domains.
- External Dependencies Management Assessment (EDM): evaluates an agency's reliance on external entities to provide services; assesses vendor-related issues and the organization's risk management related to external dependencies and service protection and sustainment.
- Cyber Infrastructure Survey: evaluates the effectiveness of 80 cybersecurity controls, preparedness, and overall resilience of an organization's cybersecurity ecosystem across five domains.
- Cyber Security Evaluation Tool (CSET®): a self-assessment to help organizations evaluate how well they are equipped to defend and recover from cyber incidents.
- CISA has compiled a list of free public and private sector cybersecurity services and tools to help organizations improve their security capabilities.

In addition, CISA offers small agencies support and guidance in the following areas:

- Information Sharing - The CyberLiaison team is CISA's centralized hub for facilitating information sharing and technical exchanges across the government. Through CyberLiaison, CISA regularly shares threat and vulnerability information. The CyberLiaison team primarily shares this information through two mailboxes: CyberLiaison@cisa.dhs.gov and federal@us-cert.gov. The sensitivity of the information shared determines which mailbox will send the email. Providing the CyberLiaison team with the best points of contact for various messaging and technical exchanges enables CISA to provide its federal partners with the most timely, relevant, and actionable information available. To add or update contacts, please reach out to CyberLiaison@cisa.dhs.gov.
- Homeland Security Information Network (HSIN) - HSIN is the Department of Homeland Security's (DHS) secure platform used to connect CISA with its federal partners. Among the many features HSIN offers, federal agencies use it to access Homeland Security-related datasets, send requests to DHS, and securely share information in support of fulfilling their cybersecurity mission. To obtain access to HSIN, prospective users may submit a request to cyberliaison@cisa.dhs.gov and include their full name, agency, and official .gov or .mil email address.
- Cyber Technical Exchanges - CISA fosters information sharing among agencies through recurring exchanges, calls, and events. By convening the appropriate stakeholders in the proper contexts, CISA amplifies best practices, brings attention to emerging threats

and vulnerabilities, and provides roadmaps to overcoming shared obstacles. Examples include:

  - Security Operations Center (SOC) calls
  - Small and Micro Agency CISO Council (SMAC) meetings
  - Joint Agency Cyber Knowledge Exchange (JACKE) meetings

- Federal Network Authorization (FNA) - A FNA legal agreement defines the terms by which DHS incident response personnel are authorized to assist in searching for evidence and mitigating a potential or confirmed intrusion into a network.
- Continuous Diagnostics and Mitigation (CDM) Program - CDM provides a dynamic approach to fortifying the cybersecurity of government networks and systems. The CDM Program delivers cybersecurity tools, integration services, and dashboards that help participating agencies improve their security posture.
- Protective Domain Name System (DNS) Resolver Service - This service is an evolution of EINSTEIN 3 Accelerated (E3A), which allows CISA to detect and prevent cyberattacks targeting agency networks. The service also offers a broad range of capabilities to safeguard cloud, mobile, and nomadic devices.
- Cyber Defense Education and Training (CDET) - The CDET team addresses today's cyber workforce challenges through innovative education and training opportunities. Their goal is to lead and influence national cyber training and education to promote and enable the cyber-ready workforce of tomorrow through various educational training and engagements. Contact Education@cisa.dhs.gov for more information.
- CyberStat Workshops - CyberStat Workshops use a cohort model to address common problems across the government and provide agencies with additional skills, knowledge, and toolsets to improve cybersecurity hygiene. Participating agencies engage in an activity-oriented workshop that provides cybersecurity resources. Agency POCs can join the CyberStat workshop distribution list by emailing CyberStat@cisa.dhs.gov.
- CISA Cybersecurity Shared Services Marketplace and Cybersecurity Shared Services Office (CSSO) - The marketplace will be a one-stop shop for all CISA shared services. Users will be able to learn about, explore, and pursue procurement options through a single web portal. For more information on the current version of the marketplace, please visit: Cyber QSMO Marketplace | CISA.

Federal Requirements

- Directives | CISA
- Binding Operational Directive 19-02
- FY2020 annual Federal Information Security Modernization Act memorandum (OMB M-20-04)
- OMB M-21-31 and M-22-09

Small Agency Considerations

- CISA has the unique authority to direct certain agencies to deploy information security protections or mitigations in response to a threat, incident, or vulnerability. CISA directives fall into two categories: Binding Operational Directives (BODs) and Emergency Directives (EDs).
    - A BOD is a compulsory direction to Federal Civilian Executive Branch (FCEB) agencies to safeguard federal data and information systems from a known (or reasonably suspected) threat, vulnerability, or risk. Compared to EDs, BODs generally fulfill more strategic objectives and operate across longer time periods.
    - EDs are issued in response to a specific threat or vulnerability and require agencies to take specific action to protect their data or information systems. EDs seek to help federal agencies "prioritize their remediation efforts, focus on those assets that carry the highest risk, and provide guidance for mitigations where updates are still not available."[79]
- Most CISA directives only apply to federal agencies included in this list: Agencies | CISA. Not all small agencies are on the list, however the directives are still considered best practices for these agencies.

Resources for Executives

- To access free services or schedule an assessment, contact cyberadvisor@cisa.dhs.gov
- https://www.cisa.gov/sites/default/files/publications/FINAL-CSSO-Protective_DNS-Fact_Sheet.pdf
- Continuous Diagnostics and Mitigation Program | CISA
- US-CERT Federal Incident Notification Guidelines | CISA
- Cyber Hygiene Services | CISA
- Homeland Security Information Network (HSIN) | Homeland Security (dhs.gov)
- For more information on the CISA CSSO (formerly Cyber QSMO), visit: Cyber QSMO | CISA
- CISA Services Catalog | CISA.
- CISA CyberStat Program - Dept of Homeland Security - MAX Federal Community

[79] Cybersecurity Infrastructure & Security Agency. (2022, April 8). *Emergency Directive 22-02 Mitigate Apache Log4J Vulnerability.* CISA.gov. https://www.cisa.gov/emergency-directive-22-02

Software Application Development and Delivery

Overview

This section introduces some overarching terms and concepts that apply to software application development and delivery. It also introduces terms specific to two contrasting methodologies or approaches to software development and delivery: Agile and Waterfall.

Software is a collection of instructions that enable computers to operate and execute specific tasks.

- The term “application” is generally used when referring to a component of software executed by a user; applications are designed to help users complete tasks.
    - Types of applications include workplace productivity (e.g., email, word processing, video, and media players), business, data management and analysis, and security.
- “Software application” and “application” are often used synonymously.[80,81]

In the context of software development, a product refers to an application that is developed and maintained to provide value for end users (stakeholders, customers, business users).

A platform is a software environment on which systems, applications, and websites are built and run.

Application types may be categorized by how the user accesses the application:

- Desktop application
    - Runs locally and uses local data
- Web application (accessed via web browser)
    - Requires internet connection
    - Can use online data and databases
    - May be dynamic or static (without server processing)
        - A website provides content but is not interactive
- Mobile application

[80] Computer Security Resource Center. *Application*. National Institute of Standards and Technology. https://csrc.nist.gov/glossary/term/application

[81] Exec. Order No. 14028. (2022, February 4). *Software Supply Chain Guidance.* NIST.gov. https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf

- Native: developed (coded) and designed to be used only on a specific mobile platform[82]
- Web: developed for use by mobile web browser
- Hybrid: core functionality is a web application packaged in a native app so it can be installed and accessed like native apps

Software applications can be hosted and delivered on cloud servers using the following delivery types (where the provider provides access to the software or platform in accordance with defined security, availability, and performance standards):

- Software as a Service (SaaS) products, which are ready-to-use software products.
- Platform as a Service (PaaS), which provides the platform for customized applications.

Your agency can host its own applications in a cloud IaaS environment.

In a non-technical context, the term "software development" often refers to the overall discipline or practice of designing and implementing applications to meet specific business needs. In a more technical context, software "delivery" is the broad term that refers to the entire process of implementing a software application, from concept through design and development to acceptance by the end user. Speaking technically, development is a more narrow term, as it is part of the delivery process. Development activities are primarily technical, and include design, coding and configuration, unit testing, integration testing, building, and releasing software.[83] Development can also include configuration of software products and modernizing or improving existing products or applications to improve capabilities or performance. In any context, when discussing "software development," it is important to understand: (1) the distinction between the processes of development and delivery and (2) which process is being referenced (regardless of which term is being used) by the individual, group, or resource (i.e., document, website, etc.) that you are engaged with.

In the discipline of software development, a product refers to an application that is developed and maintained to provide value for end users (i.e., stakeholders, customers, business users). Products are designed to meet business needs and solve business problems. Differences in the terms "product" and "application" or "software" may seem subtle. However, focusing on "product development" as a practice instead of "software development" can result in a substantial shift in the delivery approach and results because the business context and business value are centered and prioritized in product development. The goal of product development is to deliver products users want to use to complete tasks. Product development integrates business and user research, user experience design, and software development. The product development

[82] Gartner. Mobile Web Applications. *Gartner Glossary.* Gartner. https://www.gartner.com/en/information-technology/glossary/mobile-web-applications
[83] Technical Reference Architecture. *Concepts and Terminology*. Centers for Medicare & Medicaid Services. https://www.cms.gov/tra/Content/Application_Development/AD_0020_Application_Concepts_Terminology.htm

approach is recommended over the more traditional project management approach to software development that prioritizes delivering a rigid scope of work on-time and on-budget.

Details

Application projects fall into two main types that are generally funded using different types of funds:

- Development/Modernization/Enhancement (DME)
    - New development
    - Major enhancements
    - Minor enhancements and defects corrections
    - Infrastructure changes[84]
- Operations & Maintenance (O&M)
    - After an application is in use and in production, maintenance occurs in the O&M phase. Maintaining an application includes tracking and fixing defects and producing software patches.

The software delivery process may be described using a conceptual framework that identifies different activities that occur.[85] In general, software delivery includes the following activities:

- Identify need; concept or idea generation
- Analysis of requirements
- Design
- Build
- Test
- Deployment

Software delivery *methodologies* integrate project management and the software delivery process. In general, a methodology defines practices, procedures, activities, deliverables, and governance controls. Software delivery projects benefit from structure and organization from concept to completion to manage expected outcomes, timeframes, and budgets. Defining and implementing a delivery methodology is a way to standardize practices, manage projects, and minimize risks.

[84] GSA IT. (2018, June). *Solutions Life Cycle Handbook*. General Services Administration. https://docs.google.com/document/d/1nWx5hPQNF9j31t_vI8yNHGcths_Q-Gs2UkRfZGBdwCM/edit#
[85] U.S. Office of Administration. *Glossary*. OA.PA.gov https://www.oa.pa.gov/Policies/Pages/Glossary.aspx#S

Two primary delivery methodologies are Agile and Waterfall.[86] The Agile delivery framework was conceptualized after the 2001 publication of the Agile Manifesto. As described by 18F, a digital services agency within GSA's Technology Transformation Services department, the "Agile approach feature[s] outreach to potential users of software, decomposition of large software projects into much smaller projects that were much less difficult and risky, and empowerment of development teams to respond to evolving requirements."[87] Although the Agile methodology has existed for more than 20 years, it is still considered to be a "newer" methodology than the more traditional Waterfall methodology.

In a Waterfall methodology, once a project is initiated, a complete list of requirements and features and a detailed plan and schedule for the project are developed and documented before development starts. A comprehensive list of features are identified, defined, scoped, and planned for delivery at the end of the project, which can be months or years long. The project then moves through delivery activities and phases linearly. Exit criteria and milestone or gate reviews are generally required for the project to move to the next phase. Changes to the development plan (scope and schedule) are not encouraged.[88]

A key difference between the two methodologies is the approach to deliverables. An Agile approach is incremental and iterative, using short development cycles for frequent and regular delivery of functional features to users for testing and feedback. In a typical Agile approach, the goal is to quickly deliver a basic usable product that meets the minimum number of product objectives, and then to engage in continuous improvement of the product, adding or changing functionality in future iterations to meet product objectives and in response to user feedback . The initial delivery of an Agile product is sometimes called a "minimum viable product." In Agile, the version of the product used in production changes much more frequently than in Waterfall, as the team works on features and releases them in frequent iterations.

For a typical product in an Agile delivery framework, a product roadmap document provides the overall vision and plan for the product's functionality. It articulates the business case and value, identifies user groups, and clearly states user goals and product objectives. The product roadmap is used to align expectations between customers and agile teams and to support funding requests.[89] The high level functional capabilities and objectives in the product roadmap are typically organized into units of work called "epics." The work of an epic is broken down into multiple "user stories." In an Agile framework, a "user story" is the smallest unit of work and describes one distinct requirement for a product feature. User stories "are written as small,

---

[86] 18F Agile Principles. *Modern Software Product Development*. General Services Administration's Technology Transformation Services.
https://agile.18f.gov/modern-software-product-development/
[87] 18F Agile Principles. *Introduction.* GSA's Technology Transformation Services.
https://agile.18f.gov/
[88] GSA IT. (2018, June). *Solutions Life Cycle Handbook*. General Services Administration.
https://docs.google.com/document/d/1nWx5hPQNF9j31t_vI8yNHGcths_Q-Gs2UkRfZGBdwCM/edit#
[89] Tech at GSA. *3 Steps to Develop an Agile Product Roadmap*. General Services Administration.
https://tech.gsa.gov/guides/develop_an_agile_product_roadmap/

independently testable increments of the business need."[90] In Agile, a team member works with the business owner of the product (or product owner) to prioritize user stories for development. The development team works on the selected number of stories for a relatively short amount of time (usually one to four weeks) called an iteration or "sprint." At the end of the sprint, the stories are presented to the end user for testing, feedback, and acceptance. The process of user story prioritization, development sprints with functionality delivered to production, and user story creation continues in an iterative process. Note that both Waterfall and Agile methodologies include the same general activities of software delivery mentioned previously in this section. In Waterfall, the activities proceed linearly. In Agile, the activities progress in an iterative cycle.

In a typical Agile methodology, the goal is to deliver new product functionality and a new working version of the product in production at the end of each sprint. Key features of the approach are that (1) changes to the product do not impact its usability (i.e., the product is always functioning) and (2) incremental and frequent changes are made to the production version. The frequent delivery of features and functionality results in frequent feedback from users. Changes in response to new information and customer feedback are expected and welcomed, and they can be incorporated and accommodated. Product change requests are captured as user stories and stored in a product "backlog." 18F recommends establishing a cadence for stakeholders to review the product roadmap, prioritize future functionality, change product objectives as needed, and update the roadmap "to reflect the most up-to-date state for the product. The frequency of review can be set monthly, quarterly or tagged to the performance of a specific release, depending on the maturity of the product and the pace of change in the industry or market."[91] The product roadmap also may be revisited and updated. It is widely accepted that the Agile approach's regular user feedback and the frequent delivery of changes to production both reduce risk of overall "project" failure compared to the Waterfall methodology.

Agile is the recommended delivery method for software delivery and product management. 18F recommends using the following frameworks to deliver low-risk, successful technology projects in government:[92]

- Agile delivery: iteratively develop functional software, deploying and testing continuously.
- User-centered design: design with, not for, the users of a system or government service.
- Build and communicate in the open: build trust through transparency.

[90] Tech at GSA. *Writing Effective User Stories*. General Services Administration. https://tech.gsa.gov/guides/effective_user_stories/
[91] Tech at GSA. *3 Steps to Develop an Agile Product Roadmap*. General Services Administration. https://tech.gsa.gov/guides/develop_an_agile_product_roadmap/
[92] General Services Administration's Technology Transformation Services. *The 18F Product Guide*. General Services Administration. https://product-guide.18f.gov/

- Low-risk technology acquisition: ensure software services or off-the-shelf products are low-risk purchases and contracts are structured modularly.

In addition, a DevSecOps approach enhances "delivery efficiency through Continuous Integration and Continuous Delivery activities that encourage and support frequent code check-in, version control, sensible test automation, continuous low-risk releases, and feedback."[93]

To effectively plan and manage application development, it is essential to establish and maintain relationships with business stakeholders through communication about topics such as:

- What is the status of the stakeholder's IT projects?
- What are their plans and top requirements for their applications during the next one, three, and five years?
    - Are the projects strategic or non-strategic?
    - Do they want to participate in efforts to align IT people, technologies, and processes with their business direction?
- How involved is the stakeholder with the application organization? Do they participate in the governance and strategy processes? Do they have joint accountability for the results of application work?
- What is the overall perception of the application software quality and agility?
    - What is the quality of the vendors?
    - What is the quality of the support provided by the application team?[94]

Common business needs driving application development:

- Digital transformation of business processes
- Modernization of legacy applications
- Database management
- Productivity applications
- Accounting, billing payroll management, asset management
- Enterprise Resource Planning (ERP)

In general, federal guidance recommends considering the following types of development solutions, listed in order of descending priority:

1. Use existing agency or federal systems and contribute to the shared resources.

[93] Tech at GSA. *Building at DevSecOps Culture – from a Technical Perspective*. General Services Administration.
https://tech.gsa.gov/guides/building_devsecops_culture/
[94] Gartner. *Toolkit: The Application Leader's First 100 Days* (G00390073). Gartner.

2. Buy off-the-shelf (or open-source) and change business processes to align with functionality.
3. Build on a development platform, such as Platform as a Service (PaaS).
4. Build custom applications.[95]

In deciding on a solution, it is important to analyze business requirements and determine which are necessary and which are "nice to have." Especially when analyzing whether an existing or off-the-shelf application can meet requirements, consider if business processes and requirements can be modified to align with the application's functionality.

Additional factors to consider when selecting a development solution:

- Speed to solution
- Expected lifetime cost of ownership (licenses, enhancements, support, and maintenance)
- Risk of development failure
- Flexibility and customizability
- Interoperability and integration

The application design and development principles below reflect current best practices, reduce risk, and promote the production of high-quality, secure software that is compatible with the IT environment, inexpensive to maintain, and cost effective to enhance.[96,97]

- Comply with enterprise architecture.
- Integrate security into each phase.
- Incorporate 508 standards into design and development.
- Implement modular software delivery consistent with an Agile approach, "which calls for producing software in small, short increments" and seeking regular and ongoing feedback from end users.[98,99]

---

[95] U.S. Environmental Protection Agency. (2022, April 12). *Guiding Principles for Application Development.* EPA.gov https://www.epa.gov/developers/guiding-principles-application-development

[96] Technical Reference Architecture. *Introduction to Application Development*. Centers for Medicare & Medicaid Services. https://www.cms.gov/tra/Content/Application_Development/AD_0010_Application_Introduction.htm

[97] 18F. (2020, September). De-risking Government Technology. *Federal Agency Field Guide*. General Services Administration. https://derisking-guide.18f.gov/assets/federal-field-guide-4dccc06e01cd56773eb140ff6e6b2805cc517a460d6bff6689e7edd0ef349598.pdf

[98] GAO-12-681. (2012, July). *Software Development: Effective Practices and Federal Challenges in Applying Agile Methods*. GAO.gov https://www.gao.gov/assets/gao-12-681.pdf

[99] U.S. Office of Management and Budget. (2012, June 14). Contracting Guidance to Support Modular Development. Obamawhitehouse.archives.gov

Federal Requirements

- US Web Design System (Standards for Federal Websites)

Small Agency Considerations

- Have a senior leader responsible for managing application development to bring experience and perspective to complex decision making.
- Consider implementing a product management approach.
- Adopt Agile delivery practices and migrate away from Waterfall approaches.
    - Communicate frameworks and related expectations, policies, and applicability for development projects throughout the agency, especially to senior leaders so it becomes part of the culture.
- Centralize development and maintenance in the IT organization; maintain oversight of all agency applications.
    - In some organizations, "shadow IT" (software developed without the knowledge or control of the IT organization) exists because of perceived limitations of the central IT organization.[100]
        - "Shadow IT" applications represent risks for security, compliance, integration, quality, and cost.
    - Application development managed solely by a business unit (without knowledge of the CIO) should be the exception not the norm.
- Encourage, empower, and enable IT project managers to tailor the delivery activities based on the project type, size, and nature.[101,102]
    - Strive for lightweight documentation.
    - Identify and prioritize critical checkpoints and governance challenges.
- Review functional processes and identify opportunities to streamline and improve processes before investing in IT solutions.
- When making decisions about development solutions, prioritize:
    - Cloud solutions

https://obamawhitehouse.archives.gov/sites/default/files/omb/procurement/guidance/modular-approaches-for-information-technology.pdf

[100] Gartner. *Information Technology Glossary.* Gartner. https://www.gartner.com/en/information-technology/glossary/shadow

[101] Cybersecurity & Infrastructure Security Agency. (2013, July). Definitions. *Secure Software Development Life Cycle Processes*. CISA.gov https://www.cisa.gov/uscert/bsi/articles/knowledge/sdlc-process/secure-software-development-life-cycle-processes#definitions

[102] GSA IT. (2018, June) *Solutions Life Cycle Handbook*. General Services Administration. https://docs.google.com/document/d/1nWx5hPQNF9j31t_vI8yNHGcths_Q-Gs2UkRfZGBdwCM/edit#

- Externally sourced solutions
- Minimizing custom development[103]

Resources for Executives

- Introduction to Application Development (Centers for Medicare & Medicaid Services)
- List of common Federal IT Budget – Capital Planning definitions [including DME and O&M]
- Development Guidance (EPA)
- Systems Development Lifecycle (NIST)
- Systems Development Lifecycle (DOJ)
- Example of Small Agency Cloud Adoption Projects (NRC)
- Effective Practices and Federal Challenges in Applying Agile Methods
- Agile project management: 12 key principles, 4 big hurdles

Additional Resources

- GSA 18F Guides
  - Product Development
  - Agile Principles
  - Prerequisites for Modular Contracting
  - An Agile Software Development Solicitation Guide
- GSA Tech Guides
  - DevOps (GSA)
- Resources on Agile (digital.gov)
- Guidance for delivering successful custom technology projects in government (GSA 18F)
- Content Management System of Government Agencies
- Example of Small Agency Cloud Adoption Projects (NRC), pages 15-16
- Solution Lifecycle Handbook (GSA IT)
- Build vs Buy Considerations
- Agile Resources
  - GSA Tech Guides–Agile (many resources on aspects of Agile Methodology)
  - Agile - Digital.gov

[103] Jaquith, W., Hart, R., Hopson, M., & McFadden, V. (2019, August 20). *An Agile Software Development Solicitation Guide*. General Services Administration. https://18f.gsa.gov/2019/08/20/an-agile-software-development-solicitation-guide/

- Agile Alliance: What is Agile? | Agile 101
- Manifesto for Agile Software Development

Software Application Portfolio Management

Overview

Application portfolio management is the discipline of managing enterprise software applications. It establishes policies, procedures, and best practices to ensure appropriate maintenance and security of all software assets. It does not include activities specifically related to software or application development.

Individual applications and the enterprise suite of software applications require active management to maximize application effectiveness and minimize risk and cost.

Application lifecycle management identifies activities involved in managing an individual application from initiation through delivery to decommissioning.

Details

Application portfolio management includes the following activities:

- Obtaining and maintaining licenses
- Diagnosing and resolving technical problems; defect management
- Change management
- Implementing patches, fixes, version upgrades
- Other operations and maintenance functions[104]

Software can be a security risk because it can allow attackers access to an agency's hardware, network, and data. Devices can become compromised due to unsafe configurations, outdated security patches, and installation and use of compromised, vulnerable, or targeted software.[105]

To maximize security, ensure software is kept up to date. Enable automatic software updates whenever possible to ensure software updates are installed as quickly as possible.[106]

It is a best practice to centralize software purchasing and management at both agency and governmentwide levels.

---

[104] Office of Administration. *Glossary*. OA.PA.gov
https://www.oa.pa.gov/Policies/Pages/Glossary.aspx#S
[105] Cybersecurity & Infrastructure Security Agency. *Software Asset Management FAQ*. CISA.gov
https://www.cisa.gov/uscert/cdm/capabilities/swam
[106] Cybersecurity & Infrastructure Security Agency. (2009, July 14). *Security Tip: Understanding Patches and Software Updates*. CISA.gov
https://www.cisa.gov/uscert/ncas/tips/ST04-006

- Centralized acquisition strategies define common software license and maintenance requirements, can reduce the duplication of acquisition efforts, license agreements, and maintenance contracts, and result in cost savings from consolidated purchasing.[107]
- Centralized management of software acquisition and delivery supports cost efficiency, mission effectiveness, and the customer experience.[108]

Centralized software management can reduce security risks, underutilization, and redundant applications.[109]

Agencywide software asset management is similar to hardware asset management in both the purpose and the process.[110] Actively manage (inventory, track, and update) software assets in your organization by doing the following:

- For each application, track:
    - Program and business ownership, business capabilities supported, date acquired, vendor and platform, service provider, Terms of Service, number of licenses, activation codes, period of performance, purchase order number and cost, individual ownership (if applicable), license usage, version, and installed endpoints.[111]
- Automated tools can be used to capture the software applications and their attributes installed in your environment.
- With the relative ease and speed of development of web-based applications on low- or no-code platforms, it can be difficult to maintain a complete, current, and centralized inventory. Therefore, you should:
    - Design policies and processes to balance standardization and innovation.
    - Determine the criteria of applications that must be included in the central inventory.
    - Implement application onboarding and decommissioning processes to keep inventory up to date.

---

[107] Rung, A.E. & Scott, T. (2016, June 2). *Improving the Acquisition and Management of Common Information Technology: Software Licensing.* Executive Office of the President. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-12_1.pdf

[108] U.S. Agency for International Development. (2016, November 17). *Acquisition of Federal Information Technology (IT) Resources*. U.S. Agency for International Development. https://2012-2017.usaid.gov/sites/default/files/documents/1868/546.pdf

[109] Scott, R. & Rung, A. (2016, June 3). *Applying Category Management Principles to Software Management Practices*. The White House. https://www.cio.gov/2016/06/03/category-management-priciples.html

[110] Office of the Chief Information Officer. (2016, December). *IT Asset Management Policy.* U.S. Nuclear Regulatory Commission. https://www.nrc.gov/docs/ML1630/ML16309A561.pdf

[111] U.S. Agency for International Development. (2016, November 17). *Acquisition of Federal Information Technology (IT) Resources*. U.S. Agency for International Development. https://2012-2017.usaid.gov/sites/default/files/documents/1868/546.pdf

Application rationalization is a process to strategically review a subset of business applications and make the following determinations:

- Maintain and enhance
- Invest and modernize
- Divest and replace or retire
- Consolidate[112, 113]
- Analyze and make decisions about applications included in the rationalization process considering the following variables:
    - Business value
    - Technical quality
    - Architectural fit
    - Total cost of ownership
    - Application age, technology, and roadmap or future plans
- Optimize the scope of the rationalization effort by reviewing a subset of applications including:
    - Those that support a business capability or process.
    - All applications within a business domain.
    - IT infrastructure applications.
    - Data lifecycle applications.
    - Applications based on location (on premise, cloud)[114]

Federal Requirements

M-16-12: Improving the Acquisition and Management of Common Information Technology: Software Licensing

Resources for Executives

- IT Asset Management Policy (NRC)
- Application Rationalization Playbook
    - Detailed questions for business and technical fit assessments
    - Including Department of Justice (DOJ) Case Study, page 13

---

[112] CIO Council & Cloud & Infrastructure Community of Practice. *The Application Rationalization Playbook*. CIO.gov. https://www.cio.gov/assets/files/Application-Rationalization-Playbook.pdf

[113] Gartner Research. (2015, February). *Toolkit: The CIO's First 100 Days*. Gartner. Gartner cio_100_days_toolkit.pdf

[114] Dia, H., Hunter, R. & Clifford, M. (2010, May). *Application Portfolio Rationalization: How IT Standardization Fuels Growth.* Oracle Corporation. https://www.oracle.com/technetwork/topics/entarch/articles/oracle-ea-app-portfolio-167297.pdf

Shared Services

Overview

Shared services refers to the practice of centralizing solutions to address common business and technical needs across federal agencies. Such solutions are typically offered by a central federal agency to the governmentwide marketplace and specialize in mission support functions such as financial management, HR management, grants management, or IT solutions.

Several federal agencies offer shared services that small agencies can leverage to improve their IT infrastructure and operations. These services reduce duplication of effort, enhance customer experience, improve service delivery, and save agency and taxpayer money. Implementing a new IT capability within an agency requires capital investments and often a long lead time to be fully operational. OMB M-19-16 designated several agencies as Quality Service Management Offices (QSMOs) for select mission support functions to be offered as federal shared services.[115] Additionally, GSA offers many shared services used across the Federal Government, such as cloud.gov and login.gov.

The handbook does not include an exhaustive list of shared services offered by federal agencies. Therefore, your agency is encouraged to explore and pursue shared services beyond those described here. Many exist informally or unofficially and may only be identified through direct engagement with a specific agency.

Details

CISA, Treasury, HHS, and OPM are shared service providers through the QSMO program.[116] Agency CIOs can contact QSMOs to determine if their agency can benefit from services offered. Importantly, formally designated QSMOs receive formal oversight from OMB upon approval by OMB of a five-year Marketplace Implementation plan. Pre-designated QSMOs are those that have not yet completed this Marketplace Implementation plan and received OMB approval.

[115] Office of Management and Budget. (2019, April 26). *Centralized Mission Support Capabilities for the Federal Government* (M-19-16). https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-16.pdf

[116] Office of Government-wide Policy & Office of Shared Solutions and Performance Improvement. *Quality Service Management Offices (QSMOs)*. General Services Administration. https://ussm.gsa.gov/qsmo/#subject=*&role=*&status=*

Table 11. *Formally Designated QSMO Agencies*

Agency	Service Type	Service Offerings
CISA	Cybersecurity	• Security Operations Center Standardization • Vulnerability Management Standardization • DNS Resolver service
Treasury	Core Financial Management	• Accounts Payable • Accounts Receivable • General Ledger • Reporting
HHS	Grants Management	• Grant Program Administration and Oversight • Management of Grant Pre-award, Award, Post-award, and Closeout • Grant Recipient Oversight (initial focus may be a Single Audit Solution)

Table 12. *Pre-designated QSMO Agencies*

Agency	Service Type	Service Offerings
CISA	Cybersecurity	• Network Defense • Incident Management • Threat Intelligence • Enterprise Intrusion Detection and Prevention • Cyber Supply Chain Risk Management • Hardware and Software Asset Management • Digital Identity and Access Management • Data Protection • Mobile Security Services
OPM	Civilian Human Resources Transaction Services	• Talent Acquisition • Talent Development • Employee Performance Management • Benefits Management • Compensation Management • Work Schedule • Leave Management

In addition to its QSMO noted above, the Department of Treasury offers G-Invoicing, a governmentwide invoicing solution for intergovernmental transactions (IGT), such as interagency agreements and transfer of funds. All federal agencies are required to use it to meet federal financial management responsibilities.[117]

Furthermore, GSA offers many shared services across the government, including the following:[118]

[117] 31 U.S.C. § 3512 (b) (1995, January 4). *Executive agency accounting and other financial management and plans*. Uscode.house.gov.
31 U.S.C. § 3513 (1995, January 4). *Financial reporting and accounting system*. Uscode.house.gov.
[118] General Services Administration. *Shared Services*. GSA.gov
https://www.gsa.gov/buy-through-us/shared-services

- The Assisted Acquisition Services (AAS) helps agencies navigate the full acquisition lifecycle with trained acquisition specialists.
- Enterprise Infrastructure Solutions refers to a Best-in-Class (BIC) contract vehicle to help agencies to modernize their telecommunications and IT infrastructure.
- Federalist is a cloud-based content management system (CMS) that agencies can use to manage and publish their web content.
- The GSA Fleet provides agencies with vehicle purchasing, leasing, rental, and electrification services.
- GSA SmartPay is a centralized payment program that provides agencies with purchase, travel, and fleet cards.
- Payroll Shared Services refers to centralized payroll processing services that can manage the entirety of an employee's federal service.
- The Travel Category Schedule allows agencies to use the existing GSA master contract to access qualified, travel-related contractors.

GSA offers other technology shared services such as cloud.gov, which allows agencies to host web pages and run applications in a cloud environment, and login.gov, which provides identity management services. You can find a comprehensive list of technology-related services from GSA here. GSA OGP also offers Folio, a web-based service to help agencies manage their own IT services and solutions in compliance with FITARA and FedRAMP.

Federal Requirements

- OMB M-19-16: Centralized Mission Support Capabilities for the Federal Government
    - https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-16.pdf

Resources for Executives

Table 13. *Summary of Shared Service Providers with Websites and Points of Contact*

Shared Service Provider	Website	Point of Contact
GSA Quality Service Management Office PMO	https://ussm.gsa.gov/	ussmteam@gsa.gov
CISA Cyber QSMO	https://www.cisa.gov/cyber-gsmo	QSMO@cisa.dhs.gov
Treasury Financial Management QSMO	https://fiscal.treasury.gov/fmqsmo/	FMQSMO@Fiscal.Treasury.Gov
HHS Grants Management QSMO	https://www.hhs.gov/about/agencies/asfr/grants-quality-service-management-office/index.html	GrantsQSMO@hhs.gov
GSA Shared Services	https://www.gsa.gov/buy-through-us/shared-services	Numerous, depending on shared service
GSA Folio	https://digital.gov/services/folio	folio.pmo@gsa.gov
GSA Technology Transfer Services (TTS)	https://www.gsa.gov/about-us/organization/federal-acquisition-service/technology-transformation-services/tts-solutions	tts-info@gsa.gov
GSA Support Services for Presidential or Congressional Commissions and Boards	https://www.gsa.gov/buy-through-us/shared-services/support-services-for-presidential-or-congressional-commissions-and-boards	cabs@gsa.gov

Organizational Components

IT Budgeting

Overview

While many statutory requirements, regulations, and guidances do not formally apply to the 24 non-CFO Act agencies, they should inform statutorily required submission budget requests to OMB as well as spending of Congressionally appropriated funds. The Government Accountability Office (GAO) expects small agencies to manage their IT budget processes and be good stewards of public money, even if they are not required to submit those budgets to OMB.

The key federal budgeting guidance document is OMB Circular A-11 Preparation, Submission, and Execution of the Budget, which provides guidance and standards for the preparation of the president's annual budget.[119] With only a few exceptions, federal agencies, including small agencies, are required to follow its guidance and standards when developing and submitting their budgets.[120] Of particular importance to IT budgeting is Section 55, which provides guidance on reporting on IT investments and IT budget and spending analysis.[121] More broadly, the circular:

- Establishes the overall budget process, including the timeline and key deadlines for agencies to follow.
- Provides guidance on the format and content of budget submissions, including the types of information that should be included and the level of detail required.
- Outlines the principles and policies that should guide budget development, including considerations of cost-effectiveness, efficiency, and program performance.
- Establishes requirements for the submission of performance plans and reports, including the use of performance measures and targets.
- Provides guidance on the development of multiyear budget plans and the use of budget scenarios.
- Sets forth rules for the preparation and submission of Congressional budget justifications and other budget-related documents.

---

[119] Office of Management and Budget. (2022, August). *Preparation, Submission, and Execution of the Budget*. (Circular A-11). Executive Office of the President. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

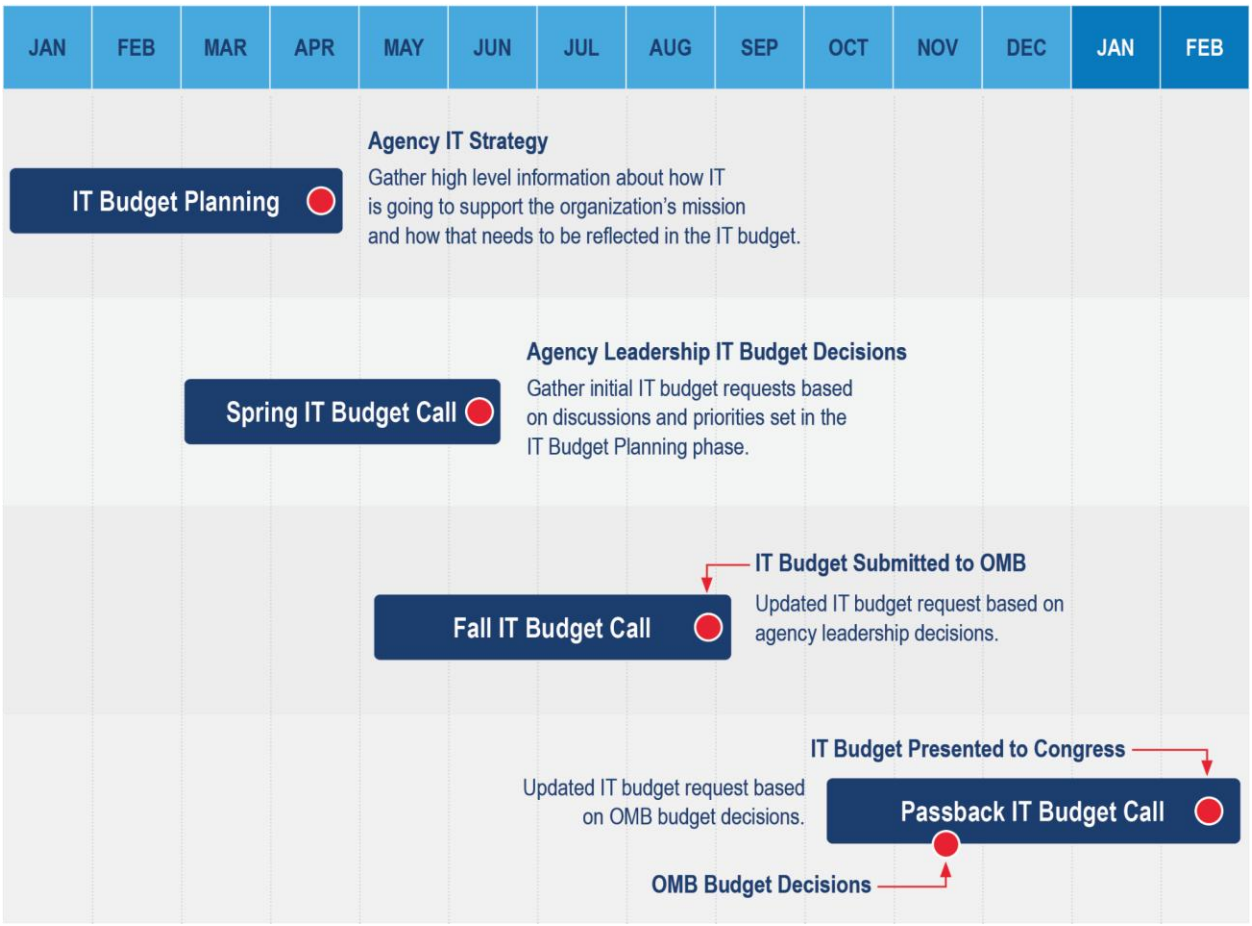
[120] Office of Management and Budget. Budget. *Circulars*. The White House. https://www.whitehouse.gov/omb/information-for-agencies/circulars/#budget

[121] Office of Management and Budget. (2022, August). Section 55—Information Technology Investments. *Preparation, Submission, and Execution of the Budget*. (Circular A-11). Executive Office of the President. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

While CFOs typically have the final authority on how funds are spent at small agencies, federal IT Executives must understand and actively participate in the agency budget process that spans well beyond the fiscal year of October 1 to September 30 of the following year. This process consists of two key, sequential components: budget formulation and budget execution.

Budget formulation begins with IT budget planning in the January two years before the corresponding IT budget execution (which would begin in the October of the following year). IT budget planning aims to determine how the IT budget will support your agency's mission and be incorporated into your agency's IT strategy (Figure X). Overlapping the latter half of IT budget planning should be an agencywide IT budget call starting in early March during which initial IT budget requests are gathered and prioritized in accordance with the aforementioned planning. Ideally, the spring budget call should culminate with budget decisions by agency leadership in late June, followed by an updated IT budget request over the summer to reflect these decisions. In September, your agency should submit the budget request to OMB for review of budget rationale and alignment to the Administration's goals, objectives, and implementation strategies for the Federal Government. OMB will then modify and finalize your agency's budget for inclusion in the president's consolidated budget submission to Congress between January 1 and February 1 of the following year (i.e., the January and February before the upcoming fiscal year).

***Figure 5**. Timeline of Budget Formulation*[122]



The specific documents your agency needs to submit to OMB, as well as the timing and format of those submissions, depends on your role and responsibilities within your agency and the type of budget request you are submitting. Typically, OMB Circular A-11 requires the following budget-related documents from agencies:

- A budget request, which is submitted in September and outlines the agency's proposed spending for the upcoming fiscal year.
- A Congressional budget justification, which is submitted in January of the following fiscal year, provides detailed information on the agency's budget request and how it aligns with the agency's mission and goals. The budget justification may be consolidated with an Annual Performance Plan (APP) and an Annual Performance Report (APR).
- Other budget-related documents, such as reprogramming requests and budget execution reports.

[122] Fiorentino, D. (2021, August 17). *Federal Information Technology (IT) Budgeting Process in the Executive Branch: An Overview.* Congressional Research Service. https://sgp.fas.org/crs/misc/R46877.pdf

Though highly variable from agency to agency, budget execution can be understood across the following four domains described by the Congressional Research Service (CRS):[123]

1. **Apportionment of funds:** OMB receives appropriations from Congress and distributes them to agencies through legally-binding, OMB-approved budgetary plans called apportionments.[124]
2. **Contractual obligations:** Agencies enter into contractual obligations and incur payments for a variety of IT goods and services, such as hardware, software, and IT personnel.
3. **Reporting of appropriations and obligations:** Congress requires agencies to provide account-level reporting on all appropriations and obligations.
4. **Outlay of funds:** Agencies outlay funds in order to pay for obligations incurred within the same or previous fiscal year.

Details

Leverage IT funding mechanisms provided by Congress in addition to appropriations, including:[125]

- **Non-recurring expense funds (NEFs):** If Congress permits your agency to have unobligated discretionary funds from previous fiscal years, or NEFs, consider using them to purchase IT goods and services.
- **Technology Modernization Fund (TMF):** Consider submitting a proposal to the TMF to fund agency IT modernization efforts.[126] Agencies submit an Initial Project Proposal (IPP) to the TMF board and, if accepted, submits a Full Project Proposal that includes a detailed project and financial plan. The agency then may repay the TMF through cost savings generated by the IT modernization effort in accordance with a written agreement between the TMF and the agency.
- **18F:** An office within GSA, 18F provides direct technical support to other agencies. Because 18F does not receive appropriations from Congress, it charges agencies for services rendered.

Plan and integrate IT service delivery with your agency's strategic planning and financial planning cycles. Such planning and integration is encouraged because of the long lead times

---

[123] Fiorentino, D. (2021, August 17). *Federal Information Technology (IT) Budgeting Process in the Executive Branch: An Overview.* Congressional Research Service. https://sgp.fas.org/crs/misc/R46877.pdf

[124] Small Agency Apportionments can be found in the "Other Independent Agencies" folder https://apportionment-public.max.gov/

[125] Fiorentino, D. (2021, August 17). *Federal Information Technology (IT) Budgeting Process in the Executive Branch: An Overview.* Congressional Research Service. https://sgp.fas.org/crs/misc/R46877.pdf

[126] The Technology Modernization Fund. CIO.gov. https://tmf.cio.gov/

and administrative burden associated with delivering IT services to employees, contractors, and the public. This planning should also encompass human capital planning, procurement planning, and related integrations. A lack of integration of IT into agency strategic and financial plans may lead to IT project failures, even with the best technologists involved. Furthermore, while not required by statute for small agencies, they are recommended, to the extent practicable, to follow the annual Capital Planning and Investment Control (CPIC) process and a strong internal IT governance process to systematically manage IT investments.[127]

Organize your IT environment into one or more IT portfolios (e.g., projects, services, investments) and consider reviewing them annually through the following steps:

1. Define and refine goals, objectives, and metrics for each IT portfolio. This practice should be informed by conducting a strengths, weaknesses, opportunities, and threats (SWOT) analysis to holistically evaluate the portfolios.
2. Create a three- to five-year roadmap for each IT portfolio to align with agency goals and objectives and stakeholders' plans. Identify big end-of-life and major procurements (end of complex contracts that must be renewed) to ensure sufficient lead time.
3. Decompose roadmaps into financial projections that delineate between "must-haves" and "nice-to-haves," and account for projected head counts, the inflation rate, and full life-cycle costs, not just implementation costs.
4. Develop a human capital strategy to ensure each IT portfolio is appropriately staffed. Conduct a gap analysis between the current and future organizational structure to identify skill gaps that might hinder progress toward the future state of the IT portfolio.

Ensure solid IT project management and budgeting for the full lifecycle for federal IT projects. Consider the Federal Acquisition Certification for Program and Project Managers (FAC-P/PM) program to learn how to integrate project management with federal budget, compliance, and procurement.[128]

Leverage Technology Business Management (TBM) framework to gain visibility into your agency's IT costs, consumption, and performance.[129] As outlined by Figure 6, the costs of IT solutions can be translated through each layer of the TBM Taxonomy, from the cost pool layer to the business layer. TBM can offer your agency a standard approach to communicate the business and mission value of IT spending to IT leaders governmentwide.

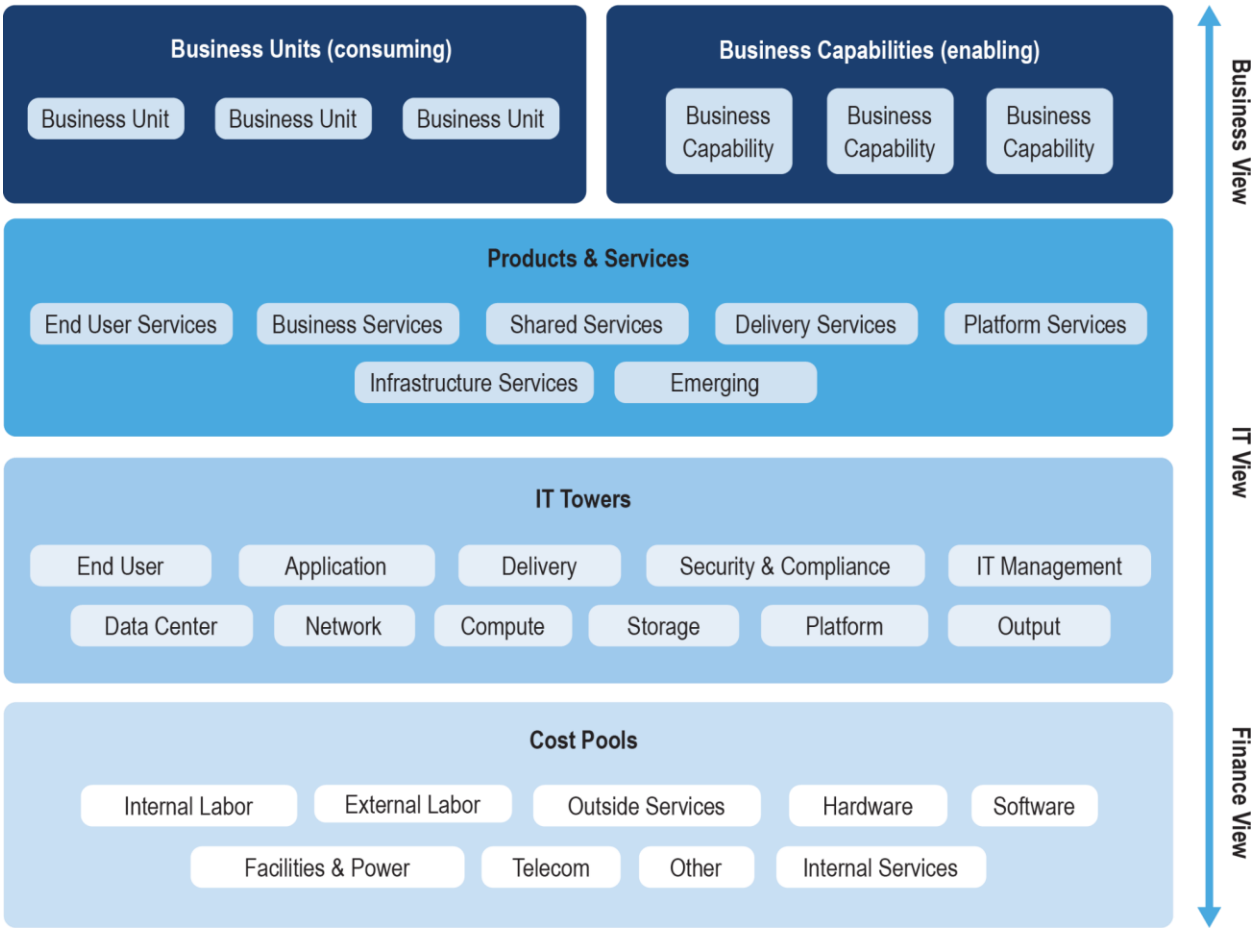
---

[127] CIO Council. Capital Planning and Investment Control (CPIC). *Policies & Priorities*. CIO.gov https://www.cio.gov/policies-and-priorities/cpic/

[128] Federal Acquisition Institute. *Program and Project Managers (FAC-P/PM)*. FAI.gov https://www.fai.gov/certification/fac-ppm

[129] CIO Council. Technology Business Management. *Policies & Priorities*. CIO.gov https://www.cio.gov/policies-and-priorities/tbm/

***Figure 6**. Diagram of the TBM Taxonomy*[130]



Federal Requirements

With the exception of A-11, few other budgetary federal mandates apply to small agencies since small agencies are non-CFO Act agencies and typically do not meet the budget size that requires inclusion of Major IT Investment Business Case in the agency's budget justification (formerly Exhibit 300). Agencies may use guidance in the following documents for best practices and reference:

- OMB Circulars on budgeting, most importantly including A-11: https://www.whitehouse.gov/omb/information-for-agencies/circulars/#budget
- OMB Circular No. A-130: Managing Information as a Strategic Resource: https://www.cio.gov/policies-and-priorities/circular-a-130/

[130] TBM Council. (2018, November 2). *TBM Taxonomy Version 3.0.2*. TBM Council. https://higherlogicdownload.s3.amazonaws.com/TBMCOUNCIL/c15d372f-9951-46c8-9c3f-213c696401b6/UploadedImages/TBM_Taxonomy_V4_0.pdf

- The Government Performance and Results Act of 1993: https://www.govinfo.gov/content/pkg/STATUTE-107/pdf/STATUTE-107-Pg285.pdf
- The Government Performance and Results Modernization Act of 2010: https://www.congress.gov/111/plaws/publ352/PLAW-111publ352.pdf
- Resources related to CPIC (though not required for non-CFO Act Agencies):
    - Federal CIO Council Summary of CPIC: https://www.cio.gov/handbook/policies-initiatives/cpic/
    - Clinger-Cohen Act of 1996, which mandates CPIC: https://dodcio.defense.gov/Portals/0/Documents/ciodesrefvolone.pdf

Small Agency Considerations

Strive to reduce the level of effort required for the annual budgeting process through the use of budget and finance templates. The examples provided below were designed and used in a small agency CIO organization. The preparers noted, however, that templates and processes for preparing budgets and tracking implementation are not unique to IT. They recommended reaching out to peers in other business units and in accounting and finance to discuss best practices and resources that work for your agency.

- **Attachment 1. Budget Tracking Spreadsheet:** Tracks spending by line item throughout the fiscal year.
- **Attachment 2. Spend Plan Spreadsheet:** Describes planned spending by fiscal year quarter.
- **Attachment 3. IT Portfolio Spreadsheet:** Calculates the budget exhibits and includes spending across the agency with projections through FY2026.

Though not required for non-CFO Act Agencies, consider the Capital Planning and Investment Control (CPIC) process to systematically manage IT investments.[131]

The primary leadership interaction regarding IT budgeting occurs between the agency IT Executive and CFO or Finance Executive. Use that engagement as an opportunity to seek support for the IT budget from the rest of agency leadership.

Resources for Executives

- Guidance Page for IT Exhibits for Small Agencies on OMB MAX: https://community.max.gov/display/Egov/Guidance+Page+for+IT+Exhibits+for+Small+Agencies
- Federal Information Technology (IT) Budgeting Process in the Executive Branch: An Overview: https://sgp.fas.org/crs/misc/R46877.pdf

[131] Chief Information Officers Council. Capital Planning and Investment Control. *CIO Handbook*. CIO.gov https://www.cio.gov/handbook/policies-initiatives/cpic/

Additional Resources

- The Executive Budget Process: An Overview: https://sgp.fas.org/crs/misc/R47019.pdf
- The Role of Executive Agencies in Budget Development: In Brief: https://crsreports.congress.gov/product/pdf/R/R47091

Procurement & Contracting

General Procurement

Overview

Acquisition is the process an agency uses to enter into a contract to obtain goods or services by purchase or lease.[132] The terms "acquisition" and "procurement" may be used interchangeably. Purchasing or buying is a subset of the broader procurement function.

Acquisition begins when agencies' needs are established and includes:

- Requirements definition
- Market research and planning
- Solicitation development
- Selection and contract award
- Contract financing
- Contract administration
- Evaluating contract performance
- Contract closeout[133]

Federal procurement is governed by the United States Code (USC) and the Federal Acquisition Regulations (FAR). Agencies may supplement the FAR to establish additional regulatory requirements.

Key Roles

Contracting Officer (CO)

> As defined by the Federal Acquisition Institute (FAI), "a Contracting Officer (CO)
>
> is a person who can bind the Federal Government of the United States to a contract. Contracting Officers hold a warrant [or Certificate of Appointment] that allows them to

[132] Federal Acquisition Regulation. (2023, January 31). *Definitions of Words and Terms*. Acquisition.gov. https://www.acquisition.gov/far/part-2#FAR_Subpart_2_1
[133] General Services Administration. *Buy.GSA.gov*. GSA.gov. https://buy.gsa.gov/

negotiate on behalf of the United States Government. As the Government's agent, only COs may execute, modify, or terminate a contract. There is a need for Contracting Officers both domestically and overseas depending on the agency."[134,135]

Only a warranted Contracting Officer is authorized to obligate the government.

Contract Specialists

"Contract Specialists are trained in acquisition and in related business skills such as market research, source selection, cost and price analysis, negotiation, and contract administration."[136]

Your agency's contracting staff are responsible for leading the acquisition process. Having some basic knowledge of the process and requirements will help you plan and manage procurement timelines and expectations.

Details

The following information is intended to provide a generalized overview of how to initiate a procurement. Based on your agency's experience and the level of complexity, the process may be more or less complex.

- The first step in any procurement is to identify the need (e.g., IT maintenance support, monitors for video conferences). For certain requirements, it can be helpful to do some initial research of what exists in the market.
- Next, contact a primary contracting officer. Contracting officers discuss and evaluate requirements. They use their knowledge of the market and acquisition tools to identify the best method to fulfill the requirements with both quality and efficiency.
- Often, the contract officer will recommend market research to refine and focus the procurement. Pre-solicitation communication with industry can provide the following benefits:
    - Industry questions about the requirements and program responses can shape and clarify the scope of the final requirements and solicitation.
    - Industry can articulate existing capabilities.
    - Interested and capable businesses can be identified and targeted, including small businesses and businesses aligned with governmentwide socioeconomic goals (veteran-owned small business; service-disabled, veteran-owned small

[134] Federal Acquisition Institute. *Frequently Asked Questions (FAQ) About Government Contracting Careers.* Federal Acquisition Institute. https://www.fai.gov/sites/default/files/Questions%20for%20new%20contacting%20professionals.pdf
[135] Federal Acquisition Institute. *Frequently Asked Questions (FAQs).* Federal Acquisition Institute. https://www.fai.gov/training/frequently-asked-questions-faqs
[136] Federal Acquisition Institute. *Frequently Asked Questions (FAQ) About Government Contracting Careers.* Federal Acquisition Institute. .https://www.fai.gov/sites/default/files/Questions%20for%20new%20contacting%20professionals.pdf

business; HUBZone small business; small disadvantaged business; and women-owned small business), in accordance with FAR part 19 (Small Business Programs).

- GSA provides no-cost support for the pre-solicitation and solicitation phase as part of their Market Research as a Service (MRAS) offering. Assistance includes:
    - Developing a customized Request for Information (RFI) and summary of market responses.
    - Developing or reviewing Performance Work Statement (PWS) or Statement of Work (SOW), Understanding (SOU), or Objectives (SOO) that defines the required results with measurable outcomes.
    - Identification of procurement strategies and solutions.
    - Product Market Research.

GSA has a number of resources available to provide individualized support for any type of acquisition, including Tier 1 Customer Support, GSA Customer Service Directors, and National Account Directors for Small Agencies.

Buy.GSA.gov provides centralized information for government buyers and links to the following:

- GSA Buyer's Resource for pre-solicitation lifecycle stages:
    - Plan
    - Develop Documents
    - Research Products, Services, and Pricing
- Document Library
    - GSA Buyers guides, ordering guides, and acquisition templates, and tips
- Market Research as a Service

GSA's Acquisition Package Planning site provides guidance and resources in the pre-award phases for various types of IT and office management products and services. Navigate to the type of purchase (Hardware, Security, Services, Software (including Cloud), Telecommunications) and expand the menu sections for the following information:

- **Discovery**
    - Buyer's Guides, Ordering Guides
- **Requirements Definition:** Document your needs and estimate associated costs.
    - SOO, PWS, SOW, IGCE, and Buying Tips and Tools

- **Market Research and Planning:** Review information on the supply base, available contract vehicles, and key regulations.
    - RFI, Sources Sought Notice, Market Research Report, MRAS Report, and Policy and Guidance
- **Solicitation Development:** Develop solicitation documents to express your business requirements and invite private sector contractors to compete for your work.
    - RFQ, RFP, and Other Solicitation Resources and Templates

For purchases under the micro-purchase threshold (i.e., $10,000 or an agency-defined higher amount), the governmentwide commercial purchase card is the preferred purchasing method.

- The FAR states agency heads are encouraged to delegate micro-purchase authority to employees of an agency who will be using the supplies or services being purchased. Individuals delegated this authority are appointed in writing in accordance with agency procedures.

Purchases between the micro-purchase threshold and the simplified acquisition threshold ($250,000 or an agency-defined higher amount) may use simplified acquisition procedures.

- Only a warranted contracting officer may use the governmentwide commercial purchase card for purchases between $10,000 and $250,000

For purchases larger than the simplified acquisition threshold, or for purchases with highly customized requirements, agency contracting officers will lead the acquisition process and be responsible for ensuring compliance with FAR through all phases of the acquisition process.

Publicizing Contract Opportunities (FAR)

As a general principle, for purchases over $25,000, the government is required to provide notice of contract opportunities (for supplies and services) at the governmentwide point of entry. The System for Award Management (SAM.gov) is the governmentwide point of entry for the public to access contract opportunity notices, such as:

- Pre-solicitation notices
- Solicitation notices
- Award notices
- Sole source notices[137]

[137] SAM.gov. *Contract Opportunities*. SAM.gov https://sam.gov/content/opportunities

As stated in FAR Part 5, contract actions are publicized to:

- Increase competition.
- Broaden industry participation in meeting government requirements.
- Assist small business concerns; veteran-owned small business concerns; service-disabled, veteran-owned small business concerns; HUBZone small business concerns; small disadvantaged business concerns; and women-owned small business concerns in obtaining contracts and subcontracts.[138]

Sourcing Policy (FAR)

The following mandatory government sources must be considered, in order of descending priority, for supplies and services:

- Inventories of the requiring agency
- Excess from other agencies
- Wholesale supply sources, such as GSA stock programs

Agencies are then encouraged to consider the following non-mandatory sources before accessing commercial sources on the open market:

- Federal Supply Schedules
- Governmentwide acquisition contracts
- Multiagency contracts
- Procurement instruments intended for use by multiple agencies, including blanket purchase agreements (BPAs)[139]
    - Blanket purchase orders (BPAs) are procurement tools used to support purchases expected to repeat.
        - Once the BPA is established, subsequent needs can be addressed through the valid BPA at reduced timeframes, leveraging the time spent on the initial BPA.

[138] Federal Acquisition Regulation. (2023, January 31). *Publicizing Contract Action*. Acquisition.gov. https://www.acquisition.gov/far/part-5
[139] Federal Acquisition Regulation. (2023, January 31). *Priorities for use of mandatory Government sources*. Acquisition.gov. https://www.acquisition.gov/far/part-8#FAR_8_002

The Federal Supply Schedule program is also known as the GSA Schedules Program or the Multiple Award Schedule Program.

- Simplified process for obtaining commercial supplies and commercial services at prices associated with volume buying[140]
- Access via: GSA Advantage!

Category Management

- A governmentwide initiative to coordinate and leverage spending on commonly purchased goods and services
- Ten categories of goods and services (including IT and Office Management) are managed by an interagency team of experts within their respective market areas.
- The goal is to drive federal customers to buy the goods and services available using the category's acquisition tools. To accomplish this, the Category Management Teams engage in market research, prospective user research, and business intelligence (including agency spend data) to develop market expertise, leverage best practices, and align quality and availability of products and services to customer needs. Ideally, government customers have access to the best quality, streamlined purchasing, and increased savings for commonly purchased items.[141,142]

Federal Requirements

- Federal Acquisition Regulations (FAR)
- Category management

Small Agency Considerations

- For many small agencies, contracts are critical to IT operations. It is essential that the IT organization has an effective (and compliant) process to initiate and maintain contracts.
- Partner with contract officers at your organization, GSA, or other applicable agencies to discuss procurement and budget needs and identify innovative, customized procurement solutions that provide both quality service and purchasing flexibility.
- It is helpful to have one or more employees with advanced acquisition knowledge. The Federal Acquisition Institute offers certifications for project managers and a

[140] Federal Acquisition Regulation. (2023, January 31). *General*. Acquisition.gov. https://www.acquisition.gov/far/8.402
[141] Acquisition Gateway. (2018, February). *Category Management & Best-in-Class*. GSA.gov. https://hallways.cap.gsa.gov/app/#/gateway/professional-services/23372/category-management-best-class
[142] Defense Acquisition University. *Category Management*. DAU.gov. https://aaf.dau.edu/aaf/services/category-management/

specialization for IT project managers. Information is available at https://www.fai.gov/ and GSA's Acquisition Portal at https://insite.gsa.gov/acquisitionportal.

    - The Federal Acquisition Certification for Program and Project Managers (FAC-P/PM) core certification program certifies program and project managers at three levels: entry, mid and senior.
    - Federal Acquisition Certification for Program and Project Managers-IT Specialization (FAC-P/PM-IT Specialization)

- Leverage GSA's free MRAS service offerings for all your RFI needs.
- Include pre-solicitation research and market research into acquisition lead time.
- General decision-making questions to consider:
    - Are you purchasing goods or services?
    - Are the requirements standard or customized?
    - Will this be a recurring purchase?
    - Do you need advice from a contracting officer?
    - Is it a micro-purchase?
        - Who is authorized to spend?
    - Has the contracting officer identified multiple procurement methods?
        - What is the method most commonly used for?
        - What are the restrictions?
        - What are the pros and cons?

Resources for Executives

GSA's Acquisition Support

- GSA | FAS | Customer Service Director
- National Account Director for Small Agencies

An Acquisition Guide for Agency Executives (DOE 2017) NOTE: This guide from 2017 has not been updated. It is included because it provides a unique, high-level overview for executives. Use this as a general reference, but not for specific threshold dollar amounts.

Additional Resources

- Federal Acquisition Regulations (FAR)
- Overview of GSA Buying Tools
- GSA Advantage

    - The government's central online shopping superstore, GSA Advantage, provides online access to millions of products and services from thousands of federal contractors.
- GSA eBuy! is an online Request for Quotation (RFQ) tool. It provides access to the following acquisition resources:
    - Federal Supply Schedules
    - Technology Contracts
        - GWAC
        - Network Service and telecommunications
    - Blanket Purchase Agreements
- System for Award Management (SAM.gov) is the governmentwide point of entry for the public to access contract opportunity notices.
- Federal Procurement Data System (fpds.gov) contains information on every contract where the estimated value is more than the micro-purchase threshold of $10,000.
- General Services Acquisition Manual / Regulation (GSAM/R)
- GSA-Helping Agencies Meet Socioeconomic Goals

IT Procurement

Overview

Information Technology is one of the governmentwide acquisition categories designed to ensure best pricing and eliminate duplicative contracts for IT products and services. The IT Category is led by the assistant commissioner of the FAS Office of Information Technology Category (ITC).

The governmentwide IT Category Management effort is supported by the IT Vendor Management Office (ITVMO). The ITVMO outlines its mission as a trusted independent advisor and advocate to help agencies buy common IT goods and services in compliance with procurement laws.

- The ITVMO leverages governmentwide IT procurement data, conducts market research, and develops shared agency acquisition knowledge to support agencies in procurement decisions.

The ITC provides consolidated federal acquisition paths to ensure a breadth and variety of high-quality, cost-effective technology solutions (products and services) are available to meet a wide range of agency mission needs and budgets.[143]

- ITC subject matter experts (SMEs) manage vendors and acquisition channels to encourage and support centralized IT spending in the federal marketplace and to optimize price and quality.

In the Multiple Award Schedule (MAS), the IT Category (formerly known as Schedule 70) includes subcategories and Special Item Numbers (SIN), such as:[144]

- Hardware Leasing, Purchasing, and Maintenance
- Software Licenses and Maintenance Agreements
- IT Solutions: Cloud services; identity, credential, access management, and other specialized solutions
- IT Services: Database planning and design, systems analysis and design, network services, programming, conversion and implementation support, network services project management, and data and records management
- Electronic Commerce: Email services, internet access services, electronic subscription services, data transmission services, and emerging electronic commerce technologies
- Cybersecurity
    - Zero trust architecture
- Enterprise Technology Solutions

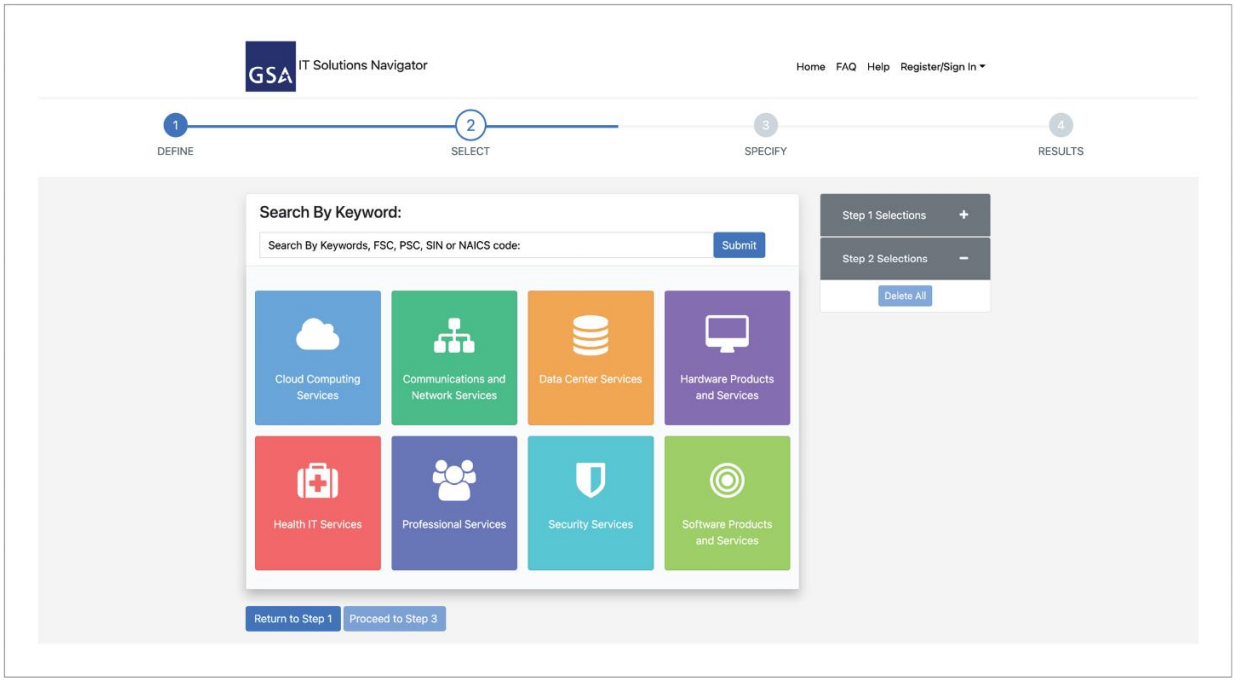
[143] Stanton, L. (2022, December 16). GSA Plans to grant DOJ, DHS extended period to complete EIS transition. *Great Government Through Technology*. GSA.gov. https://gsablogs.gsa.gov/technology/

[144] General Services Administration. *SINs and Solutions We Offer*. GSA.gov. https://www.gsa.gov/technology/technology-purchasing-programs/mas-information-technology/sins-and-solutions-we-offer

Access the IT MAS at GSA Advantage!

GSA's IT Solution Navigator tool below provides a starting place for any IT procurement. A decision tree of questions provides contract matches for the identified IT need.

Figure 7. *Screenshot of GSA's IT Solution Navigator*



Details

This section contains content from GSA IT Category service publications.

The IT Multiple Award Schedule (MAS) offers a full suite of IT and telecommunications products, services, and solutions from highly qualified industry partners and more than 4,600 pre-vetted vendors. ITC technology SMEs constantly monitor the market to add new products and services, as well as new, innovative companies.

The IT MAS is recognized as a best-in-class (BIC) acquisition solution – acquisition solutions that can be used by multiple agencies and satisfy key criteria defined by the White House Office of Management and Budget.

The IT Category and ITVMO provide information and support for other IT Best-in-Class (BIC) Contracting Vehicles, also referred to as BIC vehicles. These contracts are pre-competed, multiple-award, indefinite-delivery, indefinite-quantity (MA-IDIQ) Governmentwide Acquisition Contracts (GWACs) and Blanket Purchase Agreements (BPAs).

- All contract awardees have the required facility clearances and can provide the best value IT solutions to federal agencies while helping agencies meet socioeconomic goals.
- The highly qualified companies on BIC GWACs can complete almost any IT service requirement including:[145]
    - Agile software development
    - Systems design
    - Artificial intelligence (AI),
    - Cloud computing
    - Other emerging technologies

As an example, the MAS IT includes the BIC GSA AdvantageSelect Government-wide Strategic Solutions (GSS) for laptop and desktop products because:

- GSS BPAs are FAR compliant, pre-competed, short-term, brand-name (or equal), single-award BPAs for all Dell™, HP®, and Lenovo® laptop and desktop products that meet GSS standard configurations and options for configuring to agency needs.[146, 147]
- They allow all government agencies to simply "click and buy" pre-configured laptops, desktops, tablets, and monitors.
- The GSS BPAs are recompeted annually to incorporate customer feedback and new products. This ensures:
    - The latest technology is available.
    - Technology configurations align with agency needs.
    - More consistent and competitive pricing.
    - Better terms and conditions.

In general, IT MAS contracts and other BIC contracts enable:

- Faster acquisition.
- Federal Acquisition Regulation (FAR) compliance.
- Lower prices.

---

[145] Stanton, L. (2022, November 29). Category: IT Services. *Great Government Through Technology*. GSA.gov. https://gsablogs.gsa.gov/technology/category/it-services/

[146] Stanton, L. (2022, December 16). Latest Posts. *Great Government Through Technology*. GSA.gov. https://gsablogs.gsa.gov/technology/

[147] General Services Administration. *GSA's Government-wide Strategic Solutions (GSS) for Desktops and Laptops Program*. GSAAdvantage.gov. https://www.gsaadvantage.gov/advdata/gss/GSS-Desktop-Laptop-Guide.pdf

In addition, purchasing from the IT MAS results in:

- Less administrative time and contract documentation since the master contract is managed by GSA.
- A single contracting vehicle to fulfill complex or ongoing needs and reduce overall contract awards and administration.
- Socioeconomic credit for orders awarded to small businesses and other socioeconomic categories.

The GSA Acquisition Gateway details a maturity model for Category Management. In general, the model classifies category-related spend under management (SUM) according to the following acquisition tools:

- Tier 1: Agency-wide Mandatory Solutions
- Tier 2: Multiagency Solutions
- Tier 3: Best-in-Class (BIC) Solutions

Federal Requirements

- Summary of IT Acquisition Policies

Small Agency Considerations

- In smaller organizations, third-party managed services are often used to fulfill the following functions:
    - Cloud management
    - IT service and help desk
    - Security
    - Web hosting
    - Network management
    - Data and analytics
    - Data center management and operations
    - Backup and recovery[148]
- Consider using TechFar Hub resources (resources to help government acquisition and program professionals buy, build, and deliver modern digital services while staying on the correct side of compliance)

[148] Gartner. (2021, December 13). *Leadership Vision for 2022: Midsize Enterprise CIO*. Gartner. https://www.gartner.com/en/documents/4009401

- Consider using Governmentwide Acquisition Contracts (GWACs), especially for common IT items. These contracts are pre-competed, which reduces your agency's administrative burden. Also, the IT contracts have both high-quality specifications and vendors, so they are designed to provide reputable quality at the best available price.
    - In addition to GSA's GWACs, NASA, Army, and NIH have IT GWACs that may be useful for small agencies. Reach out to the GWAC's customer support for assistance in using the contract. It can also be helpful to speak with a colleague or peer that has used a GWAC to understand the benefits and challenges of this procurement method.
- Consider that small businesses may have special experience and more flexibility to meet the needs of a small agency. Larger contractors may be accustomed to working with large agencies and less familiar with the staffing structures and constraints of small agencies.
- Source mission-support services from organizations that do it at scale (e.g., shared services, larger agencies, external providers). See the Shared Services section in this document.

Resources for Executives

IT TIER 1 Customer Support:

Call: 855-482-4348
Hours for live chat and calls:
Sun 8 p.m. - Fri 8:30 p.m. CST
Email: ITCSC@gsa.gov

- FAS Small Agency "National Account Manager" (NAM)
- Director, National Marketing Communications Division (Has access to a master contract and team members dedicated to all things "IT," with familiarity on existing collateral "in the warehouse" and a line of sight on any possible "small agency" marketing work in play.)
- ITVMO Support: itvmo@gsa.gov
- IT Category Support: ITCSC@gsa.gov
- IT Solution Navigator
- Digital Services Playbook
- Acquisition Principles for Digital Services

Additional Resources

- GSA Technology Purchasing Programs Home Page
- GSA IT Category Home Page
- GSA IT Acquisition Help Resources
- GSA IT BIC Solutions
- Governmentwide IT Acquisition Contracts Overview
- Search for Buyer's Guides and Ordering Guides on BUY.GSA.GOV
- Governmentwide Acquisition Contracts (GWACs)
- MAS Information Technology
- Telecommunications and Network Services
- Software Purchase Agreements
- USAccess: Identity, Credentials, and Access Management
- GSA Technology Home Page
- Sample Statements of Objectives for Software Development
- Sample Technology Statements of Work
- Cybersecurity Sub-Category SME: ITSecurityCM@gsa.gov
- Digital IT Acquisition Professional (DITAP) Training
- TechFar Handbook

  (Guidance on Agile Software Development procurement)

IT Workforce

Overview

The IT Workforce is one of the most important factors and considerations in the implementation of both operational and strategic IT initiatives. Historically, many small agencies have struggled to justify and maintain adequate IT workforces, resulting in small agency CIOs and IT staff serving multiple roles. This creates a need for small agencies to be lean, efficient, and effective with their IT teams. Significant governmentwide resources are available to small agency IT teams, but require time to research and find. This section is intended to provide agencies with resources and recommendations on how to build, retain, and train a lean IT workforce.

Details

- Utilize NIST's NICE Framework for Position Classification and Planning - The NICE Framework is a comprehensive IT and cybersecurity-focused framework for planning, hiring, and training a robust IT workforce. The NICE Framework provides significant information about various classification and hiring needs, and can help small agencies quickly build out job descriptions and hiring requisitions.
- Small Agency CIOs should review the OPM Hiring Authorities. Many agencies may be eligible, in particular for direct hire authority, and should take advantage of these special authorities.

- Ideal IT Team Composition - Define the necessary minimum required roles and functions for an IT team:
    - CIO
    - CDO
    - CISO
    - Privacy Officer and Team
    - Strategy and Policy
    - Enterprise Architect
    - Application Manager
    - Procurement
    - Help Desk
    - Contractors

Federal Requirements

- Complete List of Workforce-related OPM Memos and Updates
- OPM Hiring Authorities
- Federal Cybersecurity Workforce Strategy

Small Agency Considerations

- Do not make sacrifices in the budget on high-level workforce planning. Every agency requires a series of dedicated staff related to IT policy, strategy, governance, architecture, and planning. At the very least, small agencies need to have FTE IT staff assigned to support these functions at the highest levels.
- Consider the composition of your IT workforce before hiring or contracting IT work. Typically, large agency budgets can support the need for highly specialized IT contractors who can build or implement custom or COTs products, often in multiple environments. However, small agencies should consider the value of building, maintaining, and retaining an internal IT workforce. Facilitating cohesion among small teams of FTEs and contractors can prove difficult and staff augmentation may feel less expensive up front, but may cost more long term.

Resources for Executives

- Future of the Federal IT Workforce
- NICE Framework
- GS-2210 OPM Guidance on Position Classification
- USAJOBS GS-2210 References and Open Positions

Additional Resources

- Federal Chief Human Capital Officers (CHCO) Council - May be useful for engagement and representation for alignment with agency CHCO.

Policies & Reporting Requirements

It is important to understand and monitor the entities responsible for direction and oversight of federal agency operations. A number of IT components are subject to focused requirements and oversight, including:

- Data management (including record retention)
- Access to information (FOIA, privacy, section 508)
- Cybersecurity
- IT investments and procurement

NOTE: Even if laws or regulations do not require implementation or reporting by small agencies, oversight bodies such as Congress and the Government Accountability Office (GAO), and the public, expect small agencies to follow best practices in IT governance, management, budgeting, and procurement. While the compliance and reporting requirements may not exist for small agencies, it does not mean they are not obligated to be good stewards of public trust and resources.

Requirements and prohibitions for agencies are delivered by the following entities, listed according to the hierarchy of the documents issued.

- Congress:
    - Laws:
        - United States Code:

          Applicability: Most laws apply to all agencies, not just the 24 CFO Act agencies.

          Best practice: Using the links below, set up email alerts from Congress.gov to monitor legislative developments in relevant IT topic areas. As a starting point, consider using as key words some of the technical and organizational components in this handbook, including hardware, network, telecommunications, data management, data centers, cloud computing, software development, software management, IT budgeting, IT procurement, IT workforce, IT governance, IT accessibility, and customer service. Beyond searching for specific words or phrases, legislation may also be more specifically tracked according to bill sponsor, House and Senate committee, legislative action, among other options.
        - To register for an account, visit: https://www.congress.gov/account/register
        - To sign into an account, visit: https://www.congress.gov/account/signin
        - To set up email alerts, visit: https://www.congress.gov/alerts

- Executive Office of the President (Office of Management and Budget):

  The Office of Management and Budget (OMB) oversees the performance of federal agencies and administers the federal budget. The following are used to manage operations of the Federal Government, including routine administrative matters and the internal operations of federal agencies:[149]

  - Executive Orders
  - Presidential Directives
  - Memoranda
  - Circulars

    Applicability: All civilian agencies or only required for CFO Act Agencies.

- Federal Agencies
  - Rules and Regulations: Congress may grant rulemaking authority to federal agencies. The regulations issued pursuant to this authority carry the force and effect of law.[150] These are published in the Federal Register and the Code of Federal Regulations (CFR).
  - Conditions of an agreement, such as funding agreements, may also include operational requirements.
  - Emergency Directives & Binding Operational Directives:
    - CISA/DHS

      Applicability: These civilian Executive Branch agencies fall under CISA's authorities.
  - Standards and guidelines produced by non-regulatory agencies may be incorporated into requirements from OMB or other agency regulations.
    - NIST

[149] USA.gov. *Office of Management and Budget*. USA.gov. https://www.usa.gov/federal-agencies/office-of-management-and-budget

[150] Congressional Research Service. (2021, March 19). *An Overview of Federal Regulations and the Rulemaking Process*. Congressional Research Service. https://sgp.fas.org/crs/misc/IF10003.pdf

Oversight

- Congressional:

  Congressional oversight "refers to the review, monitoring, and supervision of federal agencies, programs, and policy implementation."[151]

  - Committee hearings and requests
  - Government Accountability Office (GAO) investigations and reports

    Best practice: Set up email alerts from GAO to monitor Congressional audit developments in relevant IT topic areas. As a starting point, consider selecting the following subscription topics: Information Management, Information Security, and Information Technology.

    - To set up email alerts, visit: https://public.govdelivery.com/accounts/USGAO/subscribers/new

- OMB:

  Reporting and data submissions are required in response to OMB's management and oversight of the following:

  - Budget development and execution
  - Agency performance, procurement, financial management, and IT (including annual performance plans)
  - Coordination and review of all significant federal regulations from executive agencies, privacy policy, and information policy

- Offices of Inspectors General (OIGs)
  - Audit
  - Evaluation
  - Investigation

    Applicability: In addition to oversight, OIG publishes informational reports, including annual Top Management Challenges from various federal agencies.

Guidance, Strategies, Priorities, and Initiatives

- Executive Office of the President
  - President's Management Agenda
    - CAP Goals and Strategies

[151] Congressional Research Service. (2022, December 22). *Congressional Oversight Manual*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/RL/RL30240#:~:text=Oversight%20is%20an%20activity%20that,activities%2C%20and%20policy%20implementation.4

        - Office of the Chief Technology Officer
            - Federal CIO Work Plan
            - Federal Cloud Computing Strategy
- Federal Agencies
    - Guidance and Guidelines are also frequently adopted by organizations as best practices, even if they are not required to do so.

Additional Resources

Resources for Federal Information Technology Requirements

- Federal Digital Services Requirements

Resources for Federal Information Technology Reporting Requirements

- OFCIO Reporting (Integrated Data Collection–IDC)
- CISO Reporting

The CIO Handbook has summary information and links to IT Laws and other authorities including Executive Orders, OMB Circulars, OMB Memoranda, and DHS Binding Operational Directives (BOD).

IT Governance

Overview

IT Governance (ITG) is a formal method consisting of frameworks and policies that align organizational IT plans, operations, and services with organizational objectives and strategy. IT Governance spans multiple facets of IT, such as IT investment decisions, implementation oversight, and operational oversight, and helps an agency run in an efficient, effective, and compliant fashion. Determining the appropriate level of governance processes and policies for an agency can be a challenge. CIOs must determine the right amount of oversight. Too many guardrails and controls hurt operational efficiency and too few expose the enterprise to unnecessary risks.

Details

Small agency CIOs should implement an effective IT governance policy framework for the appropriate and compliant use of IT assets within an enterprise.

Policies that comprise an agency's governance framework should be written in plain language. IT policies directed at the user community should not include technical nomenclature and be user-focused.

Policies should be centrally stored, easily accessed, and communicated to the user base. Policies should be evaluated in a predefined timeframe, at least annually, for applicability, changes, updates, and validity.

Ensure buy-in from agency leadership, including the Executive Officer, CFO, Procurement, Human Resources, and others. Establish an agency IT Management policy that outlines the authorities, responsibilities, and policies for managing agency IT solutions. Articulate the why and how of the requirements. This can be as simple as articulating the need to meet federal requirements, reduce risk, increase efficiency, etc. Overarching policy should officially state the agency's position on the role of CIO in IT decision making and IT investment process.

Once agency buy-in for IT Governance is acquired, implement a streamlined governance body composed of stakeholders, such as the CFO and others, to manage IT investments and decisions.

Small Agency CIOs should be familiar with GAO's Information Technology Investment Management (ITIM), which is a framework for assessing and improving process maturity. The ITIM is used by GAO to assess an agency's IT Governance model. The ITIM framework consists of 13 processes required for successful investment. These processes are presented in several stages of maturity. Even if your agency does not get audited by GAO, the framework can be a useful reference to build your agency's IT Governance model. It can be found here.

In addition to the GAO ITIM, agency CIOs should be familiar with OMB Circular A-130. CIO.gov defines the circular as "general policy for information governance, acquisitions, records management, open data, workforce, security, and privacy." CIOs should be familiar with the governance requirements on pages 8 and 9 of the document. The comprehensive list of governance-related actions ranges from establishing IT Governance processes to conducting assessments of new investment decisions.

The following examples are examples of operational-level policies:

IT Policies:

- Service Management Policies, Change Management Policies, and Release and Deployment Policies

IT Security and Privacy Policies:

- Acceptable Usage Policy, Social Media Policy, Rules of Behavior, Account Management Policy, Logging, and Remote Access

Standard Operating Procedures:

- System maintenance, Backup procedures, Database Maintenance, and Patching procedures

Federal Requirements

Federal Information Technology Acquisition Reform ACT (FITARA)

Federal Information Security Act (FISMA)

Small Agency Considerations

Small agency CIOs should be selective when determining the appropriate amount of governance required for their agency. They should select the minimum amount of policies and procedures to effectively carry out their mission without compromising the enterprise with unnecessary risk.

Agency CIOs tasked with implementing IT Governance need to address the following points:

1) Understand the current governance framework and policies within the agency and establish a baseline.
2) Identify the need for governance and the problems we are trying to solve. For example, IT operations don't have a standard means to inform end users of system outages or downtimes. An SOP can be created to formalize this process that will reduce errors and increase user confidence in the IT department.
3) Socialize policy with all relevant stakeholders.
4) Finalize with stakeholder input and publish through appropriate channels, such as newsletters, emails, and collaboration sites.

Resources for Executives

- Industry Frameworks for Governance
    - COBIT 2019 Framework - Control Objectives for Information and Related Technology (COBIT) is an IT Governance framework used in multiple industries and was developed by the ISACA.
    - ITIL - IT Infrastructure Library (ITIL) was developed by the UK's Cabinet Office and consists of best practices for IT Service Management.
    - ISO 20000 - International Organization for Standardization (ISO) for IT Service Management
    - ISO 27001 - ISO Standards on Managing Information Security
    - NIST 800-53 - Security Governance and Requirements for Federal Agencies

IT Accessibility (Section 508)

Overview

Under Section 508 of the Rehabilitation Act (29 USC §794d), agencies must provide equivalent access to information and communications technology (ICT) for employees and members of the public with disabilities.

Section 508 of the Rehabilitation Act (29 USC §794d) begins as follows:[152]

"(a) Requirements for Federal departments and agencies

(1) Accessibility

(A) Development, procurement, maintenance, or use of electronic and information technology

When developing, procuring, maintaining, or using electronic and information technology, each Federal department or agency, including the United States Postal Service, shall ensure, unless an undue burden would be imposed on the department or agency, that the electronic and information technology allows, regardless of the type of medium of the technology—

(i) individuals with disabilities who are federal employees to have access to and use of information and data that is comparable to the access to and use of the information and data by Federal employees who are not individuals with disabilities; and

(ii) individuals with disabilities who are members of the public seeking information or services from a Federal department or agency to have access to and use of information and data that is comparable to the access to and use of the information and data by such members of the public who are not individuals with disabilities."

Details

Agencies should evaluate overall maturity of their IT Accessibility (Section 508 Programs) and make definitive plans to achieve full maturity in implementing the requirements of Section 508 of the Rehabilitation Act (see Technology Accessibility Playbook on Section508.gov). Successful implementation of Section 508 requires integration of accessibility considerations throughout IT development and acquisition lifecycles. Section 508 law requires agencies to report to the DOJ their overall compliance with the Section 508 law.

In addition to overall Section 508 compliance, agencies must incorporate accessibility into both culture and practices. This means:

- All systems engineers, designers, developers, testers, IT project managers, product owners, and content creators should complete training for awareness and understanding of Section 508 requirements.
- Procurement officials, business analysts, designers, developers, and testers should also complete specific training and should have the skills necessary to build and implement IT solutions that provide equal access to information and technology.
- Web content managers must implement policies and practices to ensure that any content posted to internal and external websites is accessible to people with disabilities.

[152] 29 U.S.C § 794 (d) (1998). *Rehabilitation Act of 1973*. Uscode.house.gov. https://www.govinfo.gov/content/pkg/USCODE-2011-title29/html/USCODE-2011-title29-chap16-subchapV-sec794d.htm

- Content authors, including any federal employee or contractor who may create agency official communications or electronic documents that may be widely distributed, must complete training and understand how to create accessible electronic content (e.g., documents, presentations, multimedia, social media posts, etc.).
- IT Acquisition professionals should complete training for awareness and understanding of Section 508 requirements and ensure IT accessibility requirements are included in solicitation documents and contract requirements. (See the Accessibility Requirements Tool.)

Federal Requirements

- Section 508 of the Rehabilitation Act of 1973, as amended
- Revised Section 508 Standards
- 21st Century Integrated Digital Experience Act (IDEA)
- Executive Order 14035, on Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce
- Strategic Plan for Improving Management of Section 508 of the Rehabilitation Act
- FAR Part 39 - Acquisition of Information Technology

Small Agency Considerations

Agencies cannot excuse non-conformance due to lack of adequate funding because Section 508 implementation is exempt from the Unfunded Mandates Reform Act. Therefore, the Section 508 requirements to provide accessible ICT are no different for small agencies than they are for large agencies. However, small agencies may need to share resources and distribute responsibilities differently than larger agencies. To achieve this balance, small agencies are advised to:

- Designate a well-qualified Section 508 program manager to manage a resourced Section 508 Program on your behalf that includes developing and maintaining agency policies, guidance, and best practices.
- Ensure Section 508 accessibility considerations are incorporated in the planning, operation, and management of any IT the agency buys, develops, uses, or maintains.
- Invest in the workforce by integrating accessibility from the beginning of a project so quality products are the default output. Remediation is rework and rework is waste.

Resources for Executives

- Section508.gov
- Executive Guide to IT Accessibility
- Play 1: Establish a Section 508 Program Manager to lead compliance efforts

Additional Resources

- Buy Accessible Products and Services
- Play 4: Establish a Section 508 Policy
- Integrating Accessibility into Agency Diversity, Equity, Inclusion and Accessibility (DEIA) Implementation Plans
- Play 12: Educate the workforce (Establish accessibility awareness training for general staff.)
- Include standard Section 508 language in all IT solicitations. (Also see the Accessibility Requirements Tool [ART].)

Project and Product Management

Project management is the process of leading a team to deliver project goals within the constraints of time and budget. Projects are temporary, planned sets of activities that have defined scopes, costs, and completion dates.[153,154] IT projects are undertaken to develop, modify, or enhance a product, service, or system and deliver business outcomes and values that meet customer needs.

Project management operates within and supports the organization's governance framework. A project manager focuses on executing, monitoring, and controlling daily activities throughout the project lifespan to ensure requirements are met and business value is delivered through a product or service.

There are many approaches and tools used for project management. Standardization and flexibility are key to consistent and effective implementation. Helpful practices include:

- Providing clear expectations and guidance.
- Providing standard tools, templates, examples, and other resources.
- Tailoring of the project management approach identifies the essential project management requirements for the individual project and excludes processes and deliverables that are not essential or applicable.
    - The following documents and artifacts are often used in managing a project:
        - Project Charter

[153] Office of Management and Budget. (2022). *Program and Project Management. (Circular No. A-11))*. Executive Office of the President. ttps://www.whitehouse.gov/wp-content/uploads/2018/06/s270.pdf
[154] U.S. Department of Health & Human Services. (2021). *HHS Policy for Information Technology Portfolio Management (PfM)*. HHS.gov. https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/hhs-policy-information-technology-portfolio-management.html

        - Project Schedule
        - Project Requirements
        - Risk Management Log
        - Solution Design Document
    - Allowing for flexibility in the process and maintaining a “light” and streamlined approach encourages adoption of project management practices and maintains core baseline standards for project management.

The agency’s IT governance body members should define the criteria of IT projects that are required to follow the agency’s IT Project Management process; such projects are generally assigned and managed by an IT project manager. Benefits of being managed under this process include:[155]

- Visibility into application development and functionality across the enterprise
    - Inventory of applications to monitor for security risks and protection
    - Integration of systems and enterprise architecture
    - Minimization of duplicate effort and resources
- Standard practices to manage project cost, quality, business impact and value
- Standard approach to risk management

The agency also must define and communicate a clear process for how a program office or business unit submits a request for a project, and how a project is initiated. Having clear criteria and processes for project initiation supports enterprisewide adoption of IT project management.

IT projects represent significant investments of resources. Due to their complexity, IT projects also have significant risks of budget and schedule overrun, delivering less business value than expected, and failure of implementation. For this reason, risk management is essential to project management throughout the lifecycle.

In software development projects, the following activities occur later in the project, after the development phase, but they are important components and helpful to include in the initial project plan:

- Testing approach
- Customer acceptance and certification
- Authorization to Operate (ATO) requirements and approval process and timeline

[155] *Management and Oversight of IT*. State of Federal IT Report. https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2017/05/SOFIT-Policy-Papers_A_ManagementandOversightofIT_PR_v2.pdf

- User documentation and User guide
- Training
- O&M

In comparison to projects, products are implemented for a longer term. They are not intended to be temporary endeavors. As defined by GSA's 18F, "product" is shorthand for whatever is being created (i.e., a website, an iOS app, an intranet application, etc).[156] IT products are created to respond to ongoing business needs and must adapt to meet future business requirements. Throughout its lifespan, a product may have multiple projects associated with it. Many organizations have adopted a strategic product management approach, in addition to implementing more tactical project management. With product management, a product team composed of business and IT are engaged for the lifecycle of a product. The product manager focuses the team on the customer and end user to ensure the product continuously delivers value and supports mission outcomes.

The goal of a product manager is to deliver a product people want to use.[157] The product manager knows the customers and end users, the business context, the purpose of the product, and the problems the product intends to solve. Each member of an effective product team should be able to explain the following:

- The users and customers
- The problems being solved
- Why this is a priority and which mission function or strategic initiative it supports

Product managers identify opportunities for continuous product improvement; can help to prioritize ideas for new products, features, and functionality that will bring the most value to the agency; and they can identify ineffective products that need to be improved or ended. The following artifacts are common in product management:

- Business case and market need
- Product description
- Product roadmap

By centering the focus on optimizing business value and outcomes for customers and end users, organizations have found product management reduces a major area of risk of project

[156] Jaquith, W., Rowland, P., Myers, M., McFadden, V., & Hopson, M. *Assign dedicated and empowered product owners to lead development efforts*. General Services Administration. https://derisking-guide.18f.gov/federal-field-guide/planning/
[157] Jaquith, W., Rowland, P., Myers, M., McFadden, V., & Hopson, M. *Assign dedicated and empowered product owners to lead development efforts*. General Services Administration. https://derisking-guide.18f.gov/federal-field-guide/planning/

failure where projects don't work as well as expected. The products have better design, quality, performance, and usability than those delivered by the traditional IT project management approach.[158]

A comprehensive framework for managing IT investments often includes program and portfolio management. Program management focuses on planning, prioritizing, funding, and managing a group of products and projects that impact a key strategic objective.[159] IT portfolio management is the application of systematic management practices applied to the agency's enterprise IT investments, projects, and activities. IT portfolio management allows the department to provide continuous oversight and decision-making support about which initiatives to undertake, which to continue, and which to discontinue or not approve. To implement portfolio management, the CIO may delegate authority, create entities with specific functions, develop policies and practices, define roles and responsibilities, and identify decision-making rules and powers.[160] At both the program and portfolio levels, governance focuses on product and project alignment to agency strategic initiatives, high-level decision making and controls, risk management, and performance measurement. Taking a program management view can facilitate project prioritization to ensure limited resources are allocated to the highest priority projects.

Resources

Program and Project Management Toolkit: a knowledge base, developed and maintained by a partnership between FAI and the Federal Program and Project Management Community of Practice (FedPM CoP)

Product Guide (GSA 18F)

IT Governance Guide (DOJ)

[158] Atlassian. *What is Product Management?* Atlassian. https://www.atlassian.com/agile/product-management

[159] Office of the Chief Information Officer. (2019, April 30). *Information Technology (IT) Governance and Investment Management Guidance*. U.S. Department of Education. https://www2.ed.gov/digitalstrategy/policyarchive/it-governance-and-investment-management-guidance_20190430.pdf

[160] U.S. Department of Justice. (2020, August). *Information Technology Governance Guide*. U.S. Department of Justice. https://www.justice.gov/jmd/file/705831/download

Customer Service

Overview

A key component of Information Technology Service Management (ITSM) is the service desk. The service desk, also referred to as the "help desk," is the centralized means by which user requests are received and incidents are reported, prioritized, and resolved by IT staff. It offers many benefits, including:

- Single point of contact (SPOC) between users and providers of agency IT via phone or support portal.
- Ticketing system to manage requests and incidents.
- Development, sharing, and maintenance of agency IT knowledge via publication of knowledge articles.
- Live chat support.
- Self service models, which can encompass self service portals, service catalogs, knowledge articles, request forms, and chatbots.

The service desk is traditionally organized into three levels of increasing priority depending on the impact (e.g., number of users impacted, mission importance) and urgency of requests and incidents (based on service level agreements [SLAs]).

- Level 1 (L1): For basic issues that do not negatively impact the agency, such as password resets and troubleshooting for simple issues. Aim to resolve as many requests and incidents as possible through L1.
- Level 2 (L2): For more complex issues that require more skill to solve and may require a faster resolution.
- Level 3 (L3): For major incidents that comprise an agency's IT infrastructure and require an immediate "all hands on deck" response.

Details

Use an eliminate, automate, or leverage (EAL) model to optimize IT service interactions.[161] The EAL model describes the relationship between business consumer sentiment (ranging from irritated to valued) and business value (ranging from high to low) to classify approaches to handling customer support interactions. The three approaches are described below:

- **Eliminate** low-value interactions that irritate the business consumer.
    - Assess holistically how IT and business processes impact end users to eliminate underlying causes of low-value, avoidable issues. For example, incident reporting

[161] Matchett, C. (2018, March 5). *3 Simple Ways IT Service Desks Should Handle Incidents and Requests* (ID G00349556). Gartner. https://www.gartner.com/en/documents/3865567

allows your agency to sort and classify incidents, and to in turn identify and eliminate the root causes of low business consumer sentiment (i.e., those that irritate users). If possible, use a Configuration Management Database (CMDB) to identify the cause of the majority of technical issues.

- **Automate** responses to simple, standard, and repeatable requests.
    - Leverage automation to reduce the total number of contacts to the desk and to resolve low-value (i.e., L1) requests and issues that cannot be eliminated. Automation benefits both the IT support staff, who would otherwise spend time addressing the requests, and the requesters, who are able to resume their job duties more readily.
        - A common approach to service desk automation is Artificial Information Technology Service Management (AITSM), which refers to the automation of IT service-related tasks using AI tools. Examples of such tasks include automated password resets and automated request processing and fulfillment.
- **Leverage** high-value incidents to address underlying IT problems and improve IT operations.
    - Focus service desk efforts on high-value issues that add business value and improve business consumer engagement. Should never be automated.
        - Allows the service desk to demonstrate its value to the agency because they often address issues that impact its mission (of which some are mission critical).
    - Service desk interactions examples to leverage include but are not limited to:
        - Major incidents
        - Incidents of which the root cause is not known
        - Rare incidents on commonly-used applications
        - User needs for new IT services

When selecting and implementing a service desk tool, consider:[162]

- How well does it meet the needs of different end users (inter-agency, intra-agency, public)?
- How well does it serve the agency mission needs?

[162] Matchett, C. (2018, March 5). *3 Simple Ways IT Service Desks Should Handle Incidents and Requests* (ID G00349556). Gartner. https://www.gartner.com/en/documents/3865567

- How knowledgeable is the service desk staff about the tool? Could they easily implement and use it, or would they require outside help to optimize workflows? Would third-party experts need to assist with configuration and implementation?

Federal Requirements

- Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government:
    - https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/13/executive-order-on-transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government/

Small Agency Considerations

Use collaborative hubs in place of traditional service desks:[163]

- Restructure IT service desks into collaborative hubs where business consumers and users can post requests and receive answers from a combination of service desk staff, process business engineers, product teams, and other IT staff. Your agency may wish to moderate these exchanges of information to ensure accuracy and utility.
- Can be especially useful for small agencies, which often face staffing and funding challenges.
    - May be particularly appealing for service desk staff who work across different IT functions (i.e., dual and triple hatted) and may find the traditional service desk approach burdensome and slow.

Consider outsourcing service desk functions. A contractor can offer benefits including:

- Partially or entirely relieve agency staff of service desk duties
- Shorter response times, in accordance with SLAs
- Ability to scale up according to customer demand and bring in additional contractor staff
- Freeing up IT staff to focus on core IT functions and better serve agency mission

Additionally, should your agency pursue outsourcing service desk functions, consider the level of technical support required by the agency to maximize business value and business consumer sentiment. To that end, it is vital to have in place sound metrics, SLAs, well-documented roles and responsibilities, and rules of engagement.

[163] Matchett, C., Doheny, R., Shetty, S., Cleary, M. (2021, October 26). *2022 Strategic Roadmap for IT Service Management* (ID G00739529). Gartner. https://www.gartner.com/en/documents/4007545

Resources for Executives

- ITIL - IT Infrastructure Library (ITIL) was developed by the UK's Cabinet Office and consists of best-practices for IT Service Management.
- ISO 20000 - International Organization for Standardization (ISO) for IT Service Management