Federal Trade Commission

Information Resource Management (IRM) Strategic Plan

FY 2022 to FY 2026

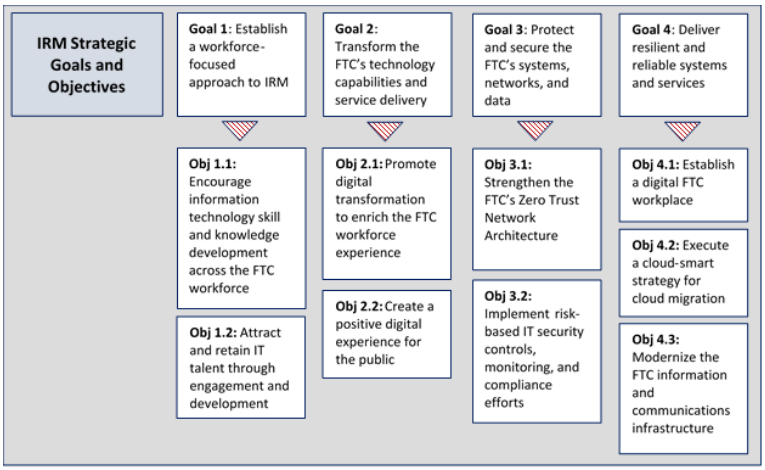
Mission Success Across All Bureaus and Offices

Message from the Chief Information and Chief Data Officer

The Federal Trade Commission's Information Resources Management (IRM) Strategic Plan for Fiscal Years 2022 – 2026 seeks digital transformations of mission processes to advance the FTC's Strategic Plan. The IRM plan builds on the foundation guided by prior plans that led to modernized IT operations through cloud services and continuous improvements in reliability, security, and mobility of IT services.

To pursue digital transformations, the IRM plan anticipates that future mission impact depends on empowering the FTC workforce to adopt transformational technology built on a strong foundation of cybersecurity, risk management, and core IT services. By treating technologies for data analytics, artificial intelligence, machine learning, robotic process automation, and virtual collaboration as general-purpose technology, the IRM goals will advance mission impact from every FTC Bureau and Office.

- Train and empower its existing workforce, who possess deep knowledge of the agency's mission, to update mission processes using transformational technologies, and
- Welcome and motivate additions to its workforce, who possess skills with transformational technologies, to learn and advance the agency's mission.



This plan, written with insight from stakeholders from every Bureau and Office, covers investments in IT across the agency. Accordingly, the plan requires their continued support for the agency to cohesively capitalize on those investments to the benefit of the American public.

Mark Gray

Acting Chief Information and Chief Data Officer

Federal Trade Commission

Summary of Changes

Version	Description of Changes	Date Approved
1.0	Final approval of IRM Strategic Plan by FTC's Senior Management Council	2/28/2023

Contents

Information Resource Management at the FTC

The Federal Trade Commission (FTC) is an independent federal agency with a unique joint mission to protect the public from fraud and deceptive practices and promote an open and competitive marketplace. The FTC executes this mission by identifying, investigating, and stopping deceptive and anticompetitive practices and educating the public on how to protect and defend themselves and others against deceptive and fraudulent practices.

Information technology (IT) services to are critical to achieving this mission, from specialized applications and services that support investigations and litigation to websites and public-facing applications, to basic productivity and communications services. Law enforcement activities require that nearly all elements of the workforce rapidly assess and understand technologies across every industry. The FTC's mission and its need for high-quality IT drive ongoing development and maintenance of an Information Resources Management (IRM) Strategic Plan that aligns IT with the FTC's priorities.

The IRM Strategic Plan is designed to support the FTC's mission and strategic direction. The IRM is a tool for guiding the direction, mission alignment, investment planning, workforce management, and accountability of the FTC's IT community. Over the next five years, the outcome of this plan will maximize the value of IT to the FTC's mission, workforce, and the public.

IRM Approach

A new IRM Strategic Plan is developed every four years in alignment with the FTC Strategic Plan as required by the Government Performance and Results Modernization Act (GPRA-MA) and the Office of Management and Budget's (OMB) Circulars A-11 and A-130. The IRM Strategic Plan is reviewed annually to ensure continuous alignment with the FTC's mission as well as consideration for technology trends and new government-wide mandates and regulations.

Past iterations of the IRM Strategic Plan emphasized modernization of core IT services and applications through a new foundation built on cloud services. The FTC has successfully modernized several IT services, such as email and office productivity, identity and access management, and IT service management, through cloud migration. These modernization efforts have improved overall reliability, security, and mobility of IT services. However, these efforts did little to reduce the manual burden for data entry or review that have consumed significant levels of effort throughout the agency or replace legacy workflows still reliant on email and paper documents. The latest version of the IRM Strategic Plan shifts the focus from simply modernizing existing IT services to transforming FTC business processes through modern digital technologies.

IRM Vision and Mission

FTC Vision

A vibrant economy fueled by fair competition, open markets, and an empowered, informed public.

FTC Mission

Protecting the public from deceptive, and unfair business practices and policing unfair competition through law enforcement, advocacy, research, and education

IRM Vision

Mission-centric information resources readily adopted by a knowledgeable and confident workforce.

IRM Mission

Deliver secure, resilient, and mobile information resources that facilitate mission success

IRM Guiding Principles

During the IRM Strategic Planning process, several cross-cutting principles emerged. They are universal to the way the FTC achieves its IRM mission and vision.

- **Mission Alignment**: Consider information technology a strategic resource and prioritize IT investments that directly support the FTC's mission
- **Risk Management**: Proactively identify and effectively mitigate risk while optimizing information security and privacy
- **Transparency**: Monitor IT investments to promote transparency and proper stewardship of Federal resources, while also ensuring integration of records management, privacy, and information security requirements
- **Collaboration**: Build coalitions and consensus across the agency, find common ground, and achieve shared goals through information sharing and communication
- **User Experience**: Focus on the user experience, leveraging user-centric design practices to better understand needs and eliminate pain points, invest in change management and training to promote technology adoption
- **Data Driven Decision Making**: Measure success through quantitative methods to the maximum extent possible. Work to optimize organizational performance through data analysis and continual feedback

IRM Strategic Goals and Objectives

The FTC has established four IRM strategic goals, each aligned with a key focus area within the IRM function. These four focus areas are: Workforce, Transformational Technologies, Cybersecurity and Risk Management, and Core IT Services.

Goal 1: Workforce

IRM Goal 1: Establish a workforce-focused approach to information resource management

The FTC's IT workforce includes employees and contractors across the agency who serve in positions such as IT specialist, data analyst, litigation support specialist, paralegal specialist, program support specialist, digital forensic examiner, and technology and information manager. In an increasingly technology-driven world, every employee interacts with IT. The FTC recognizes the importance and value of all employees in the success of any IT modernization and transformation initiative.

Objective 1.1: Encourage information technology skill and knowledge development across the FTC workforce

Employees require the appropriate skills to use technology in a meaningful and productive manner. Understanding the capabilities of available technologies is critical to the successful adoption and continued use of modernized technologies and a positive user experience. Most FTC employees are already well-versed in technology products, such as office productivity tools, electronic discovery (eDiscovery) tools, legal and business research platforms, business intelligence and reporting, and basic database and workflow development. Continued development and refinement of these skills will allow employees to continue to feel comfortable with using technology in their daily tasks and help them recognize areas of improvements and gaps that can be addressed with new features or functionality.

Employees will be provided with opportunities for advancing their skills and knowledge in newly deployed technologies, to include applications and tools currently in use. Upon deployment of any new application or product, users will receive training on its use and interface. Users will also be provided resources for ongoing support and guidance, such as tip-sheets, recorded training videos, and access to knowledge bases to support self-service and self-sufficiency in learning new tools. Additionally, the FTC will encourage its workforce to seek training in technology areas that impact their daily tasks, such as legal technology, informatics, data science, and data visualization and analytics. Annual cybersecurity and privacy awareness training, which also incorporates records and information management components, will continue to educate all employees on their role in securing and managing agency technology, information, and data. Finally, the FTC will continue to promote continuous learning opportunities in areas such as office productivity, data and statistical analysis, and eDiscovery tools, allowing employees to further strengthen their skills and learn new ways of using existing tools.

Objective 1.2: Attract and retain IT talent through engagement and development

The FTC recognizes the importance of a work environment that offers opportunities for career development and fosters an inclusive environment where all staff feel engaged, productive, and valued. This environment is especially important in attracting and retaining an IT workforce with the critical skillsets needed to transform the organization. Strong emphasis will be placed on recruiting and retaining employees with skill sets that align with transformational technologies, as well as

complementary skills such as project management, business process reengineering, and contract management.

Managers and leadership will promote employee development through challenging job assignments and increased autonomy, allowing the employee to feel empowered and respected. An important tool in employee development will be the use of competency models, which are frameworks for defining the skill and knowledge requirements of a job. Over time, the Federal Government has developed several competency models for members of the IT workforce, such as the National Initiative for Cybersecurity Information (NICE) Framework. Those employees serving in IT roles across the FTC will be evaluated and assessed for development opportunities based on these competency models, providing a consistent and thorough approach to employee development.

The FTC recognizes the important role IT service providers and contractors play in the success of IT initiatives. Their knowledge of current IT trends and best practices will be invaluable to the FTC in planning and development of IT systems and services. Contract management and performance will be critical to the success of all IT modernization and transformation efforts. Contract requirements will allow flexibility for the service provider to restructure resources when technology changes require new skill sets. Contracts will include key performance indicators (KPIs) and/or service level agreements (SLAs) where appropriate to quantitatively evaluate performance. Contracting Officer Representatives (CORs) for IT contracts will be provided the training and resources they need to monitor performance of individual contracts and work with contract program managers and the contracting officer to address any areas of performance concern.

Goal 2: Transformational Technologies

IRM Goal 2: Transform the FTC's technology capabilities and service delivery

As a small independent agency with a broad mission to promote competition in the marketplace and protect the public from deceptive practices, the FTC is uniquely positioned to take an agile, inventive, and innovative approach to technology investments. Major technology programs, such as the Sentinel Network Services (SNS) program (which includes the Do-Not-Call Registry, Consumer Sentinel Network, IdentityTheft.gov, eConsumer.gov, and ReportFraud.gov), have allowed the FTC to meet its mandate through innovation and continuous technology improvements. The FTC must continue to embrace innovative technologies, further transforming mission work and meet the everchanging needs of the public.

New technologies will be deployed using the cloud-smart strategy (detailed in Objective 4.2) and industry best practices, such as agile software development [1] and DevSecOps [2]. Transformation projects will feature close collaboration between the business units, the project manager, and software developers. This ensures development remains on track and progressive releases add value to the solution implementation aiming to achieve desired business outcomes.

[1] Agile software development is an approach to software development that delivers software in increments of functionality, allowing developers and users to test and make changes throughout the development cycle rather than waiting on a "big bang" launch.

[2] DevSecOps is an approach to software and system development based on Agile methodology that integrates information security requirements throughout the incremental releases of the agile software process.

Objective 2.1: Promote digital transformation to enrich the FTC workforce experience

Digital transformation uses technology to create new – or modify existing – business processes, culture, and customer experiences to meet changing requirements, increase efficiency, improve user experience, and streamline business operations. Digital transformation is greater than simply upgrading existing applications and technology platforms to the latest version. It requires the use of emerging technologies, such as artificial intelligence [3], data analytics, and virtual collaboration, to change the way an organization does business.

Currently, several FTC business processes rely on paper, or a portfolio of custom-built or heavily customized commercial applications. These applications require manual data entry from paper-based forms or the manual moving of data from one stovepipe application to another. To increase efficiency and improve service delivery, the FTC will focus on transforming critical agency business processes. As processes are automated, users can spend more time on high value, knowledge-based activities rather than routing and repetitive tasks. Increased digitization also increases the amount of data available for analysis and reporting, contributing to improved data-driven decision making throughout the FTC. The FTC seeks to focus investment on those technologies necessary to digitally transform business processes in a continuous and methodical fashion.

The FTC will deploy digital technologies in a manner that prioritizes alignment with the mission. Technology services will be designed to embrace the skills of the attorneys, economists, and technologists entering the workforce in the next five years to attract and retain top talent accustomed to modern IT tools. A major challenge in seeking digital transformation is acquiring the requisite resources to deploy new digital technologies. The FTC will mitigate this challenge by leveraging the transformational technologies currently embedded as features in cloud services already in use. This strategy positions transformational technologies as new features in familiar tools rather than intimidating or costly new systems. Digital technologies will be tested through proofs-of-concept, prototyping, and pilot projects to allow users to become more comfortable with new capabilities and features in the context of their requirements. Evaluation will be focused on those tools needed to support legal teams and economics/data analysts with processing and analyzing the anticipated surges in data collected during discovery, investigation, and other mission activities.

Simultaneously, the FTC will focus on reengineering and automating critical agency business processes and workflows. The FTC will utilize automated workflows to digitize manual processes while also modernizing, re-platforming and replacing current digital processes. An important component to the automation of business processes is the digitization of the FTC's records and information. The digitization of agency records will transform the FTC's business processes, allowing the agency to automate business processes that create records and content, from creation through automated workflows for approval and review to the disposition of those records according to their established schedules. The FTC will work to migrate to electronic records, in line with NARA requirements, to facilitate process automation and streamline records and content management practices.

[3] Artificial intelligence (AI) is technology that leverages computers and machines to mimic the problem solving and decision-making capabilities of the human mind. Well-known uses for AI technology include robotic process automation, speech and voice recognition, online virtual agents, automated stock trading, self-driving cars, and facial recognition.

Once a new technology is deployed, user feedback and performance will be continually assessed to assist in building a pipeline of continuous improvements to implement in a manner consistent with agile development principles. It will also determine if the technology requires reengineering or replacement. Finally, legacy products will be quickly decommissioned when no longer in use or needed to prevent unnecessary resource expenditure.

Objective 2.2: Create a positive digital experience for the public

The FTC is dedicated to providing consumers and businesses access to the information and data they need to protect themselves and make sound decisions. The FTC is equally dedicated to communicating the agency's work and mission, informing the public on the important actions taken every day to protect the public from deception and fraud and promote open markets, and how those actions provide value to the public. Digital public services, such as websites, social media, and web-based content, reach the intended audiences with this important messaging.

The FTC's digital service portfolio includes externally facing informational websites, social media, and other digital technologies used to communicate to and engage with the public and other stakeholders. The FTC will continue to prioritize investment in rich content (e.g., posters and brochures, videos, blogs, data visualizations, audio files and podcasts, infographics), social media, search engine optimization, campaign and marketing management, content syndication, and press release distribution to distribute information and content to customers in a targeted manner. All web-based services will be compliant with accessibility regulations to ensure all people are able to access information and content. In alignment with the 21st Century Integrated Digital Experience Act (IDEAct), the FTC will ensure public service processes, such as submission of forms and information from the public, are digitized and automated to the maximum extent possible, and available on all computing platforms (as feasible). The FTC will utilize data-driven decision-making using various data sources that provide insight into reach, engagement, awareness, and impact. An agile approach to continuous improvements on digital public services will ensure the user experience is optimal, deploying enhancements for new functionality and features based on customer demand or changing design elements to increase usability.

Data and information will continue to be a key component of the digital public service portfolio. Section 202 of the Foundations of Evidence Based Policymaking Act, known as the OPEN Government Data Act, requires Federal agencies to make agency data available to the maximum extent possible. Even before the OPEN Government Data Act was enacted, the FTC provided critical data sets on subject areas such as merger activity, Do-Not-Call violations, and consumer complaints providing the public with critical data points for research, advocacy, and outreach. These data sets will remain available (where data is appropriate for public release) through high-quality data visualizations embedded in our informational websites, as well as publishing to Data.gov, the Federal Government's central source for data. As more data becomes available through automation and digitization, the FTC's Data Governance Board will evaluate the feasibility and risk of public release of new data sets. Finally, live streaming and webinar capabilities for events such as Commission meetings, workshops, and conferences will allow an expanded audience visibility and participation in FTC events, regardless of location.

Goal 3: Cybersecurity and Risk Management

IRM Goal 3: Protect and secure the FTC's systems, networks, and data

The FTC's mission involves the collection of sensitive information from the public, such as consumer information and proprietary business information, as well as personal information about the FTC's employees. As the executive agency in charge of enforcing data privacy laws, the FTC would suffer irreparable damage to its reputation and credibility if data was exfiltrated because of a preventable attack. Therefore, the FTC must ensure its cybersecurity posture provides adequate protection against cyber threats, while also complying with Federal mandates and maintaining a positive user experience.

The activities conducted under Goal 4 will underpin compliance with Executive Order 14028 on Improving the Nation's Cybersecurity.

Objective 3.1: Strengthen the FTC's Zero Trust Network Architecture

The core of the FTC's cybersecurity strategy will be the implementation and maintenance of a Zero Trust architecture. Zero Trust (ZT) is a security model in which an organization assumes no implicit trust in any user or device, even those within the security perimeter. Benefits of ZT include greater visibility into network traffic and activity and access to IT resources reducing the risk and impact of data breaches. ZT can also simplify and streamline network infrastructure and improve user experience. The FTC's strategy for ZT implementation will align with the principles detailed in OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, including identity, credential, and access management (ICAM), endpoint security, network microsegmentation[4], data encryption, application testing, vulnerability management, and data classification and categorization.

Recent modernization initiatives have established a strong foundation for future ZT initiatives. The FTC's external network modernization project incorporated the deployment of ZT network tools that support greater security for remote access used by FTC staff for remote work and telework. Similarly, the FTC's migration to a cloud-based office productivity and email suite has provided access to numerous cybersecurity tools that support ZT. The FTC's strategy for ZT will focus on evaluating and expanding the use of tools currently in use at FTC. This involves a review of FTC's existing portfolio of cybersecurity tools and the available features and functions and aligning those products with ZT principles. In areas where gaps in features and functionality exist, the FTC will procure new tools that provide ZT support without inhibiting user performance. This includes working with our partners at the Cybersecurity and Infrastructure Security Agency (CISA) to leverage tools in the DHS Continuous Diagnostics and Mitigation (CDM) program.

One area of ZT that the FTC focuses heavily on is identity, credential, and access management (ICAM). ICAM is a discipline focused on the structures and processes within any organization that administers and manages its users' access to resources. The FTC has prioritized ICAM as a critical part of any IT modernization and transformation initiative. The FTC uses a centralized, cloud-based ICAM platform which provides single-sign-on (SSO) capabilities, with the FTC-issued PIV card for multifactor authentication, for both on-premise and cloud-based resources. This approach to authentication, will

[4] Network microsegmentation is a method of creating zones in data centers and cloud environments to isolate workloads from one another and secure them individually. With microsegmentation, systems administrators can create policies that limit network traffic between workloads based on a Zero Trust approach.

support maturation of ICAM practices. Embedded functionality within the ICAM platform and service management tools will automate user account processes, integrating user account creation and deletion and changes in user permissions and access needs within the onboarding/changes/offboarding processes. Additionally, the FTC will continue to expand the use of multi-factor authentication and single sign on throughout both internal-use and external-use systems and applications.

Objective 3.2: Implement risk-based IT security and privacy controls, monitoring, and compliance efforts

Operating and maintaining a hybrid cloud architecture[5] requires an agile approach to information security and privacy monitoring, compliance, and risk management. For each workflow and data set the FTC moves to externally hosted cloud environments, a new compliance effort is required, increasing costs, tying up resources, and creating project backlogs and delays if not properly planned. Digital transformation requires a streamlined approach to security and privacy that provides adequate controls for sensitive data without hindering functionality for the end user.

The FTC will practice a risk-based compliance standard that allows the agency to quickly and successfully adopt new technologies with highly valued features, in a secure environment, without degradation of performance. As new threats emerge and the Federal government responds with new mandates and guidance, the FTC will review and evaluate these requirements to determine the impact to agency systems and the level of risk the agency is willing to accept. The FTC has worked to establish an information security continuous monitoring (ISCM) program that provides agency leadership with insight into key cybersecurity metrics and status of compliance and remediation efforts for systems with high and moderate risk of vulnerability. The agency will continue to strengthen this program through increased automation, leveraging new security management tools and embedded reporting capabilities to provide real-time data with less human intervention. To respond to emerging cyber threats, the FTC will expand its security operations and monitoring capabilities by acquiring highly skilled, dedicated resources and new security monitoring and response tools to monitor the FTC's network and user traffic across the enterprise to detect suspicious activity and address security incidents. Data will drive further security compliance, determining which systems are at highest risk, and using metrics to drive priority of investments in system security. Security and privacy controls will be regularly reviewed and audited as part of a continuous information system authorization process, which assesses and certifies compliance for each system through a cyclical annual review of security controls rather than an intensive, costly effort conducted every three years.

Security and privacy requirements and baselines will be considered throughout the lifecycle of a system, starting with procurement, through the system development lifecycle and throughout the operations and maintenance of that system. Supply chain risk management (SCRM) principles will be built into the IT acquisition process using established government-wide acquisition vehicles with stringent supply chain transparency requirements. The agency has leveraged the Federal Risk Authorization and Management Program (FedRAMP) for selecting and authorizing cloud systems and will continue to do so in the future where FedRAMP services are appropriate to meet agency needs.

[5] Hybrid cloud architecture – the deliberate integration of public cloud, private cloud, and on-premise infrastructure. In a hybrid cloud architecture, the organization hosts applications and data across a portfolio of cloud services and on-premise infrastructure.

Goal 4: Core IT Services

IRM Goal 4: Deliver resilient and reliable core IT systems and services

The FTC's users require timely access to agency applications, data, and information, regardless of their location. In support of these needs, the FTC will provide highly available, resilient, and scalable core IT services, to include end user and IT infrastructure services. To ensure maximum availability for end users and address performance gaps, the FTC will continually evaluate the feasibility of moving mission-critical processes, documents, applications, and systems to cloud-based environments, while maintaining infrastructure to support on-premise systems and services.

Objective 4.1: Establish a digital workplace

The COVID-19 Pandemic provided lessons learned for many businesses and institutions on how to use technology to conduct normal business operations when employees cannot enter the physical workplace. Those same technologies deployed to support pandemic operations will continue to be critical to the employee experience as employees seek continued workplace flexibilities. Additionally, the FTC's mission requires both domestic and international travel, which requires employees to have resources to work from any location. A digital workplace is the modern evolution of the traditional employee workplace from a physical workspace to one that incorporates all technologies people use to work in today's workplace, regardless of location. Digital workplace applications and technologies include mobility, office productivity suites, content services platforms, unified communications and collaboration, endpoint device management, and remote access platforms.

To provide a true digital workplace for employees, the FTC will evaluate and deploy modern endpoint devices and end user technologies that emphasize mobility of the user and mobility of information and data. User endpoints, such as mobile devices and laptops, will be managed and monitored in a unified manner, with the objective of having a similar experience and performance across all devices. Mobile-friendly applications and technologies, such as mobile versions of office productivity and communications apps, will be deployed to FTC-issued mobile devices. Technologies will make communication and collaboration simple, whether between internal users, or between users and external partners and collaborators. Tools will enable employees to share ideas and accomplish tasks, whether they are at home, travelling, in a Regional Office, or at Headquarters.

The FTC will ensure users can successfully access the necessary documents, content, and information regardless of location. A critical step in increasing information access will be the digitization of agency records, in accordance with OMB and NARA requirements in OMB Memorandum M-19-21, *Transition to Electronic Records*. The agency is committed to migrating to electronic records to increase employee access to digital information, content, and records. Information, content, and documents will be readily available for remote users and relevant, up-to-date, searchable, and easy-to-find.

Objective 4.2: Execute a "cloud-smart" strategy for cloud migration

As the FTC moves toward cloud-based technologies that support rapid deployment, agile development, and shared technologies, the agency will encounter opportunities to improve service delivery and meet evolving mission needs. However, in the rapidly changing technology industry, it is no longer enough to just "move to the cloud". Organizations must strategically move systems and applications to cloud-based environments based on mission needs, costs, risks, and alignment with the overall strategy.

According to the Federal Chief Information Officers (CIO) Council[6], many organizations have shifted their cloud strategy from "cloud first", which prioritizes cloud adoption above other considerations, to "cloud smart" which balances cloud adoption with the organization's unique circumstances and business value (https://cloud.cio.gov/strategy). In accordance with the Federal Cloud Computing Strategy, and Executive Order 14028 (Improving the Nation's Cybersecurity, resources will be prioritized toward those investments involving cloud-based services.

To execute a "cloud-smart" strategy, the FTC will regularly evaluate and assess alternatives and strategies for moving individual agency workflows and data sets to cloud-based environments. Alternatives range from migrating existing applications to an infrastructure-as-a-service (IaaS)[7] environment that mirrors the FTC data center, complete re-engineering of applications in a platform as a service (PaaS)[8] or use of a commercial-off-the-shelf software-as-a-service product (SaaS)[9], or a Federal Shared Service[10] to completely replace existing applications. These alternatives will be evaluated based on multiple factors such as cost, security, risk, and program needs. An outcome-driven approach will be taken to cloud migration, aligning business capabilities and needs with functionalities of different cloud offerings to ensure new cloud services meet business requirements and contribute to the mission success. Chosen cloud services will integrate with existing tools such as monitoring and management tools, ICAM tools, and service management tools, as needed, to ensure a seamless experience for the user.

Approaches to individual application requirements will be based on the business capabilities and industry availability of commercial-off-the-shelf (COTS) software products, but new applications will be deployed in a cloud-based environment to ensure high availability, reduce the FTC's infrastructure footprint, integrate with ICAM platforms, and comply with relevant security regulations and mandates. Low-code or no-code development platforms will be used to the maximum extent possible to ensure faster and more accurate delivery of functionality based on user feedback and less complex custom coding.

As the FTC moves more applications and data to cloud environments, the risk of vendor lock in increases. Vendor lock-in is a situation where the cost of switching to a different cloud service vendor is prohibitive so that the customer is forced to continue using a cloud service that may no longer meet

[6] The Chief Information Officers (CIO) Council is the principal interagency forum for improving Federal agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of Federal information resources. Consists of the Federal CIO, Deputy Federal CIO, and CIOs from cabinet-level Federal agencies.

[7] Infrastructure-as-a-Service (IaaS) – on-demand access to cloud-hosted computing infrastructure – servers, storage capacity, and networking resources. The cloud server provider hosts, manages, and maintains the hardware in their own data centers while customers can provision, configure, and operate the resources over the internet.

[8] Platform-as-a-Service (PaaS) – a cloud-based platform for developing, running, and managing applications. The cloud service provider hosts, manages and maintains all the hardware and software included in the platform – including servers, operating systems, storage, networking, databases, middleware, frameworks, and development tools while the customer builds and manages the applications.

[9] Software-as-a-Service (SaaS) – cloud-hosted ready-to-use application software. The application and all infrastructure required to deliver it – servers, storage, networking, middleware, application software, and data storage – are hosted and managed by the SaaS vendor. Popular SaaS solutions include Microsoft Office365, Google's GSuite, and Dropbox.

[10] Federal Shared Service – an information technology function that is provided for consumption by multiple organizations within or between Federal agencies. Examples of Federal Shared Services include financial systems and accounting services for use by Federal agencies offered by organization such as Treasury's Administrative Resource Center or Interior's Interior Business Center, or Human Resource systems offered by OPM.

functional requirements or represent the best value. Vendor lock-in may occur when an organization uses a cloud service that requires the use of proprietary technologies that do not translate to other services or when vendors impose other technical, financial, or legal restrictions to discourage users from leaving. To mitigate the risk of vendor lock-in, the FTC will build a portfolio of cloud services that leverages existing relationships with cloud services already in use, while also evaluating the use of new cloud services and technologies to provide a wide array of options for cloud migration without becoming unmanageable.

Objective 4.3: Modernize the FTC's information and communications technology infrastructure

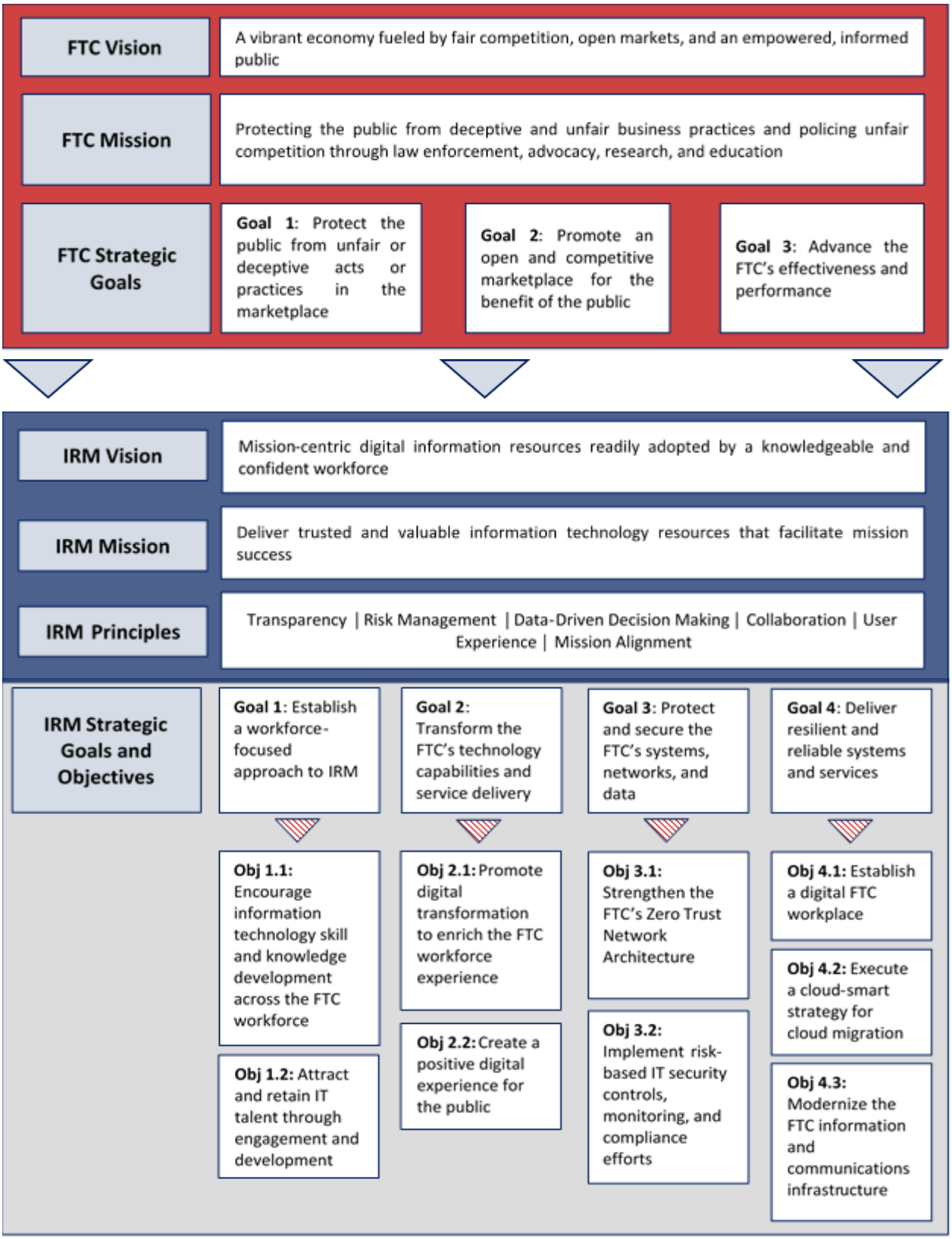
The FTC's on-premise information and communications technology (ICT) infrastructure plays an important role in agency operations. The FTC must balance the focus on cloud migration with the need to maintain a secure and reliable on-premise infrastructure to host those systems where cloud migration is not feasible, or where cloud migration is in process. Without proper maintenance, infrastructure software and hardware will lose reliability and support as it ages, putting the FTC at greater risk for system outages, performance issues, and increased security vulnerabilities (for unsupported software and firmware).

To build on the success of recent modernization efforts and provide highly available systems and services, the FTC will maintain a hybrid IT environment featuring both cloud services and a scalable, efficient, and reliable data center environment. This approach will enable modernization initiatives and projects while reducing the likelihood of loss of service or performance degradation for current services. Those systems that cannot be quickly or easily migrated to a cloud environment without substantial cost or risk will remain in a data center with a robust and resilient IT infrastructure. Systems supporting mission-critical functions will be engineered and architected with maximum scalability and elasticity to accommodate anticipated voluminous increases in data collected during investigation, discovery, forensic capture, and data and economic analysis. Communications networks will be engineered to handle increased traffic necessary to support both cloud-related internet traffic and remote work. Solutions will eliminate single-points-of-failure for the end user, specifically those systems that would lose functionality or impact users in the event of a data center outage.

Technology components in the FTC data center will be upgraded as needed to ensure continued manufacturer support for patches and bug fixes. As aging components are replaced, they will be enabled with IPv6 in accordance with OMB Memorandum M-21-07, *Completing the Transition to Internet Protocol Version 6*. Through efforts to modernize the IT infrastructure, the FTC will meet the requirements of M-21-07 ensuring at least 80% of IP-enabled assets are operating in IPv6-only environments by the end of FY 2025.

The FTC will continue to mature configuration and change management processes to ensure technology component configurations, both on premise and external, are properly documented and analyzed. The FTC will also improve its operational monitoring activities by deploying new infrastructure and application monitoring tools that monitor the health and performance of applications and systems across the environment and support diagnosis of IT performance issues before users are negatively impacted.

Appendix A: IRM One-Page Summary



Appendix B: FTC Data Strategy

Key agency stakeholders contribute to both the IRM and Data Governance Board, and the IRM principles encompass the desired outcomes of improved agency data management ("Data Driven Decision Making"). The comprehensive approach in the IRM's goals and objectives will encourage adoption of digital experiences for the workforce and the public will require the adoption policies and procedures to manage data inventories sufficient to inform sharing within the agency, with other agency partners, and the public. Key sources of guidance on creation of those policies and procedures are:

OMB 22-09	Agency Chief Data Officers must work with key agency stakeholders to develop a set of initial categorizations for sensitive electronic documents within their enterprise, with the goal of automatically monitoring and potentially restricting how these documents are shared.
Federal Data Strategy	Publish an Open Data Plan that identifies specific priority data assets, including assets that support COVID-19 response and AI R&D Update comprehensive public data inventory on data.gov

In addition to sharing progress in future public updates to the IRM Strategic Plan, the FTC will update its progress at FTC.gov/open on items specific to Federal Data Strategy guidance.