

FFIEC Resources

elm.infotex.com

blog.infotex.com

Summaries Concerning the FFIEC **Architecture, Infrastructure and Operations IT Booklet As of 7/15/21.**

DISCLAIMER: *While we attempt to assert that this document includes all information available on the ffiec.gov website as of the date listed above, we offer this as an aid to audit and consulting Clients, and in no way warrant this as being all-inclusive, complete, or thorough. Please use at your own risk.*

What's New: In June 2021 the Architecture, Infrastructure and Operations IT booklet replaced the Operations booklet. Key changes to the guidance include:

- Additional coverage of emerging technologies, including cloud computing, AI, ZeroTrust, and IoT.
- An increased focus on cybersecurity throughout all sections of the booklet.
- A new section covering governance and common risk management elements of architecture, infrastructure and operations, as well as the risks specific to each.
- The architecture section has been expanded to include strategic planning of IT architecture to better support the business functions of the enterprise, and service delivery to customers.
- The infrastructure section has expanded sections on hardware, network and telecommunications, software, environmental controls and physical access controls.
- The operations section was updated to address key operational principles in IT environments, including operational controls, IT operational processes, service and support processes and ongoing monitoring and evaluation processes.
- Throughout the booklet, references to NIST and other authoritative sources are provided.

Resources:

FFIEC Architecture, Infrastructure and Operations IT Booklet

I: Architecture, Infrastructure and Operations

<https://ithandbook.ffiec.gov/it-booklets/architecture,-infrastructure,-and-operations/i-architecture,-infrastructure,-and-operations.aspx> (Accessed 7/15/21)

Architecture refers to the manner in which the strategic design of the hardware and software infrastructure components (e.g., devices, systems, and networks) are organized and integrated to achieve and support the entity's business objectives. Planning and designing an effective IT architecture facilitate management's ability to implement infrastructure that aligns with the entity's strategic goals and business objectives.

Infrastructure refers to the physical elements, products, and services necessary to provide and maintain ongoing operations to support business activity and includes the maintenance of physical facilities. The focus of this booklet is on IT infrastructure, which is a subset of infrastructure and includes hardware, network and telecommunications, software, IT environmental controls (e.g., power, heating, ventilation, and air conditioning

FFIEC Resources

[HVAC]), and physical access. Once built and implemented, IT infrastructure can be managed internally or by a third-party service provider as part of the operations function.

Operations are the performance of activities comprising methods, principles, processes, procedures, and services that support business functions. Operations transform resource or data inputs into desired products, services, or results, and help in the creation and delivery of business value to internal and external customers. Operations include the ongoing maintenance, monitoring, and support for business systems, products, and services. This booklet addresses IT operations in the context of tactical management and daily delivery of services to support the overall business processes of the entity.

FFIEC Architecture, Infrastructure and Operations IT Booklet

II: Architecture, Infrastructure and Operations Governance

<https://ithandbook.ffiec.gov/it-booklets/architecture,-infrastructure,-and-operations/i-architecture,-infrastructure,-and-operations.aspx> (Accessed 7/15/21)

Management should implement a process, such as a life cycle approach, to continuously manage technology to support operational needs and mitigate AIO-related risks. Figure 1 identifies the actions associated with this process for changing the architecture design to address evolving strategic and technology needs, building infrastructure that accommodates architecture changes, and managing technology in day-to-day operations.

To address risks, management should employ effective governance that includes the following:

- Delineation of board and senior management responsibilities.
- Strategic planning.
- Enterprise risk management (ERM).
- Delineation of other roles and responsibilities.
- Policies, standards, and procedures.
- Internal audit, independent reviews, and certifications.
- Communications.
- Board and senior management reporting.

The board, or its designated committee, and senior management should consider the entity's business objectives when governing the functions of AIO, including functions performed by affiliates and third-party service providers. Management should identify and evaluate risks associated with AIO, set short- and long-term objectives, and create policies and procedures to mitigate those risks. Furthermore, management should consider security and resilience in the design of new products and services.

FFIEC Resources

elm.infotex.com

blog.infotex.com

FFIEC Architecture, Infrastructure and Operations IT Booklet

III: Common AIO Risk Management Topics

<https://ithandbook.ffiec.gov/it-booklets/architecture,-infrastructure,-and-operations/ii-architecture,-infrastructure,-and-operations-governance.aspx> (Accessed 7/15/21)

IT systems are designed, built, and implemented to achieve strategic goals and business objectives. While there are risks specific to each of the AIO functions, certain risks are common to all three. Common AIO risk management topics are discussed in the following sections:

- Data governance and data management.
- ITAM.
- Business and IT environment representation.
- Managing change in AIO and change management.
- Oversight of third-party service providers.
- Resilience.
- Remote access.
- Personally owned devices.
- File exchange.

Data governance and data management are fundamental to maintaining the confidentiality, integrity, and availability of information. Data governance is a set of processes for formally managing data assets throughout the entity. It establishes authority, management, and decision-making parameters related to the data that the entity produces or manages. Additionally, data governance involves the process for setting and enforcing the business and IT priorities for managing data.^[1] The data management process involves the development and execution of policies, standards, and procedures to acquire, validate, store, protect, and process data. Effective data management ensures that the required data are accessible, reliable, and timely to meet user needs. When data are no longer used, management should have a process for the data's removal or destruction and validate the effectiveness of that process.

FFIEC Architecture, Infrastructure and Operations IT Booklet

IV: Architecture

<https://ithandbook.ffiec.gov/it-booklets/architecture,-infrastructure,-and-operations/iv-architecture.aspx> (Accessed 7/15/21)

Management should implement architecture principles that can be applied enterprise wide. When designing an entity's architecture, management should balance the mitigation of risks to various stakeholders, considering both the enterprise's needs as well as the needs of individual business units. Regardless of how management designs the entity's architecture, it should align the architecture with IT and business objectives, for example,

FFIEC Resources

elm.infotex.com

blog.infotex.com

providing maximum benefits with lowest risks and acceptable costs. The architecture's design should meet the entity's needs for confidentiality, integrity, and availability and adhere to the entity's policies, standards, and procedures. In addition, management should consider the entity's architecture requirements for its existing technology and any planned changes.

Management should clearly define its mission and any strategic initiatives for architecture. Business units should understand their portion of the design, which should align with management's mission and strategic initiatives. In determining its future architecture, management should first identify the entity's IT assets and external constraints, as well as industry IT architecture trends. Once management understands the entity's current state of architecture, management should perform a gap analysis to determine the requirements to reach its future state.

Management should have a documented and approved architecture plan that identifies the entity's current state. The architecture plan should align with the entity's strategic plan to support the business and strategic objectives of the entity. Management should have policies, standards, and procedures that govern architecture initiatives and changes to the architecture plan. There should be processes including obtaining approvals for initiatives, making changes to the plan, and reporting to management or the board as appropriate.

FFIEC Architecture, Infrastructure and Operations IT Booklet

V: Infrastructure

<https://ithandbook.ffiec.gov/it-booklets/architecture,-infrastructure,-and-operations/v-infrastructure.aspx>
(Accessed 7/15/21)

As previously stated, infrastructure refers to the physical elements, products, and services necessary to provide and maintain ongoing operations to support business activity and includes the maintenance of physical facilities. IT infrastructure includes hardware, network and telecommunications, software, IT environmental controls (e.g., power and HVAC), and physical access that allow for an enterprise IT environment's operation and management. IT infrastructure implementation should include considerations for server and data redundancy and resilience of telecommunications lines. Planning and designing an effective IT architecture facilitates management's ability to implement an IT infrastructure that achieves and promotes the objectives of confidentiality, integrity, and availability and supports the entity's business operations. IT infrastructure may be managed internally or externally by a third-party service provider, including a cloud service provider.

Management should identify unauthorized technology assets and determine their disposition (e.g., remove, isolate (quarantine), or add them to the inventory). If an asset is determined to be unauthorized, management should evaluate how the device gained access and what, if any, compromise may have occurred. Management should determine whether the policy or procedures should be updated or whether additional training is necessary. Automated tools can assist management in maintaining the accuracy and availability of hardware components. Network discovery tools identify assets connected to the network and compare them to an inventory of authorized hardware assets. Advanced asset discovery tools (e.g., using dynamic host configuration

FFIEC Resources

elm.infotex.com

blog.infotex.com

protocol [DHCP] on servers or asset management tools using IP addresses) may be used to provide oversight of the entity's technology asset inventory.

FFIEC Architecture, Infrastructure and Operations IT Booklet

VI: Operations

<https://ithandbook.ffiec.gov/it-booklets/architecture,-infrastructure,-and-operations/vi-operations.aspx>
(Accessed 7/15/21)

Operations are the performance of activities comprising methods, principles, processes, procedures, and services that support business functions. For the purposes of this booklet, IT operations include the tactical management of technology assets and daily delivery of services to capture, transmit, process, and store transactions and information that support the entity's overall business processes.

The operational environment includes the systems and facilities that the entity uses to run its business processes and operations. Operations functions are sometimes referred to as "back-office" functions because they are traditionally carried out in locations away from customer-facing functions. Operations functions are the "nerve center" of an entity and encompass the day-to-day processing and support functions, service delivery and service management, and control processes to support both the operations and overall mission of the entity. The operational environment is addressed in the following subsections:

- Operational controls.
- IT operational processes.
- Service and support processes.
- Ongoing monitoring and evaluation processes.

Operational controls are the day-to-day procedures and mechanisms used to protect operational systems and software. Operational controls affect the system and software environment. Because the system and software environment(s) are the foundation for the entity's business processes, management should define processes and implement controls to protect the entity's operational environment(s). This includes the use of operating centers, authorization boundaries, IAM controls, personnel controls, and controls for the use of personally owned devices.

FFIEC Architecture, Infrastructure and Operations IT Booklet

VIII: Evolving Technologies

<https://ithandbook.ffiec.gov/it-booklets/architecture,-infrastructure,-and-operations/vii-evolving-technologies.aspx> (Accessed 7/15/21)

Entities use a variety of evolving technologies (e.g., cloud, zero trust architecture [ZTA], AI and ML, and IoT) that may impact architecture, infrastructure, and operations functions. This section provides general information

FFIEC Resources

elm.infotex.com

blog.infotex.com

relating to these evolving technologies and, when appropriate, certain risks and control principles discussed in prior sections of this booklet.

Cloud computing environments are enabled by virtualization technologies, which allow cloud service providers to segregate and isolate multiple clients on a common set of physical or virtual hardware. NIST defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or third-party service provider interaction.”^[1] Cloud systems provide several benefits, including scalability of resources and consistency in deployment of controls across systems and software.

For the purposes of this section of the booklet, when the term “cloud service provider” is used, it refers to the provider offering cloud computing services. When the term “entity” is used, it refers to the client receiving cloud computing services.