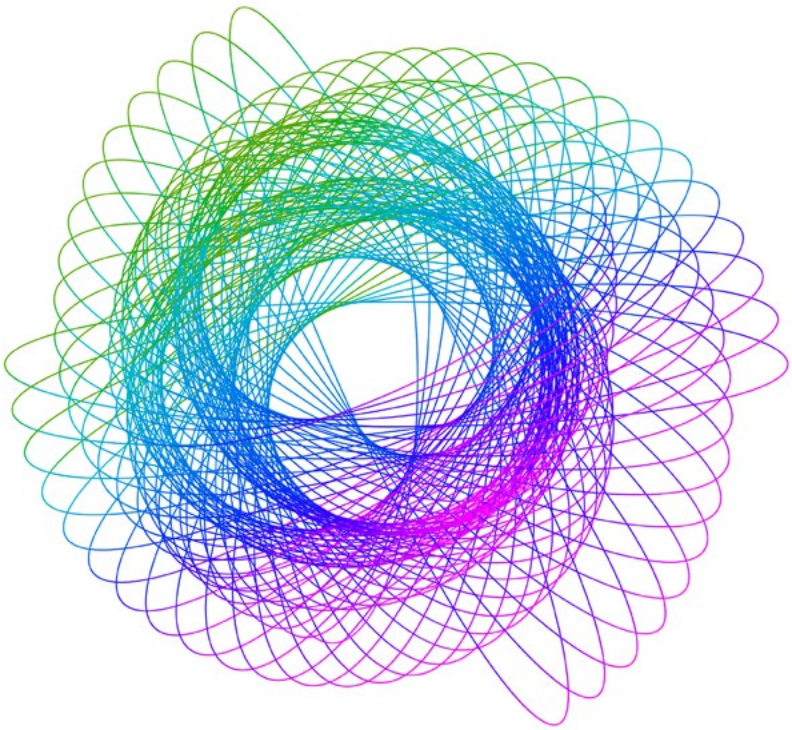
Deloitte.



FFIEC issues Architecture, Infrastructure and Operations booklet

July 18, 2021

On June 30, 2021, the Federal Financial Institution Examination Council (FFIEC) released the "Architecture, Infrastructure and Operations" booklet of the Information Technology Examination Handbook.[1] This new booklet replaces the "Operations" booklet that was originally issued in 2004. This booklet is a guide for examiners at its respective member regulatory agencies to determine the adequacy of an institution's information technology (IT) architecture, infrastructure, and operations (AIO).

In addition, this booklet provides guidance to financial institutions (including banks as well as bank service providers) on assessing and establishing governance of common AIO-related risks, enterprise-wide IT architectural planning and design, implementation of virtual and physical infrastructure, and assessment of an entity's related operational controls. This handbook remains the broadest collection of regulation expectations for IT controls and governance and how banking institutions are expected to mitigate IT risks and identify emerging risks.

The updates to the handbook come at a time when financial institutions are becoming increasingly reliant on technology infrastructure to drive digitization and automation of core business processes in order to meet expectations of both younger generations and customer behavior that moved increasingly remote work environments during COVID-19. Digital transformation brings its own set of security challenges and risks. An increase in cyber-attacks, outages, and data breaches have steered the focus of both bank management and regulators toward managing operational and cyber risks. A report by the International Criminal Police Organization (INTERPOL) showed an alarming rate of cyberattacks during the pandemic with a significant target shift from individuals and small businesses to major corporations, governments, and critical infrastructure.[2] According to Federal Reserve Chairman Jerome Powell, cyberattacks are now the foremost risk to the global financial system, even more than the lending and liquidity risks that led to the 2008 financial crisis.[3]

Key Highlights

The AIO booklet focuses on enterprise-wide, process-oriented approaches that relate to the design of technology within the overall business structure, implementation of IT infrastructure components, and delivery of services and value for customers. The key highlights compared to the previous Operations booklet are provided below:

- The new AIO booklet introduces three new functions: Infrastructure; Architecture; and, Operations. The functions comprise a variety of activities that support the business and provides a more broad view of management's activities related to designing, building, and managing the entity's technology.
- The previous booklet's focus was on risk management processes and expected controls that promote safe and sound operation of technology environments. It also addressed IT operations in the context of tactical management and daily delivery of technology to capture, transmit, process, and store the information assets and support the business processes of the institution. The new booklet incorporates all this information while organizing them under different sections such as AIO governance & common AIO risk management topics to provide a dynamic and interconnected view of IT risk management.
- The booklet emphasizes Governance with the addition of subsections such as communication, and board and senior management reporting.
- The booklet defines the responsibilities of key IT executive roles (Chief Architect, Chief Data Officer and IT Operations Management). The section on the responsibilities of IT operations personnel has been broadened to delineate the functions of IT personnel in three categories: network infrastructure management; server and device management; and, IT environment management.
- The Operations section has been reorganized with primary focus on following areas – operational controls, IT operational processes, service and support processes, and ongoing monitoring and evaluation.
- The new AIO booklet emphasizes on the need for data governance and data management defining the responsibilities and controls required in the process to maintaining the confidentiality, integrity, and availability of information (i.e., data quality and data integrity). Data management has been broadened to include data identification and data classification to encompass structured and unstructured data.
- Oversight of third-party service providers is newly introduced in this booklet considering many entities are outsourcing AIO activities to one or more third-party service providers.
- In order to align with rapidly changing and evolving technologies in the financial market, the booklet also incorporates a new section on 'Evolving Technologies' with general information on emerging technologies like cloud computing, zero trust architecture (ZTA), microservices, and artificial intelligence and machine learning (AI/ML).

Next steps

The updates to the FFIEC's Information Technology Examination Handbook reflect the changing technological environment and the enterprise-wide need for IT controls, governance and security. It reflects the overall view that financial institutions are both responsible and need to demonstrate a level of capability to effectively address IT risks that affect their business models. To be prepared for when examiners utilize using this booklet, firms should catalogue what new or enhanced controls are required and applicable to their institution and what steps were taken to achieve compliance. For example, firms could tier their data to determine which data should be tightly governed (more critical data) versus data that can be less governed (less critical data). This upfront work is invaluable, especially as regulators enhance their IT supervisory expectations to deal with changes in the IT landscape.

End notes:

1. Office of the Comptroller of the Currency, "FFIEC Information Technology Handbook: New Architecture, Infrastructure, and Operations Booklet," accessed July 8, 2021.
2. International Criminal Police Organization (INTERPOL), "INTERPOL report shows alarming rate of cyberattacks during COVID-19," accessed July 8, 2021.
3. CNN Business, "Cyberattacks are the number-one threat to the global financial system, Fed chair says," accessed July 8, 2021.

Contacts

Kiran Nagaraj
Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Nitin Pandey
Managing Director | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Sameer Ansari
Managing Director | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Richard Rosenthal
Business & Entity Transformation Lead
Senior Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Prateek Saha
Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche Assurance &
Enterprise Risk Services India Private Limited

Neeraj A S
Senior Consultant | Deloitte Risk & Financial Advisory
Deloitte & Touche Assurance & Enterprise
Risk Services India Private Limited
Deloitte Center for Regulatory Strategy

Irena Gecas-McCarthy
FSI Director, Deloitte Center for
Regulatory Strategy, Americas
Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Austin Tuell
Manager| Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Kyle Cooke
Senior Consultant | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Deloitte.