FFIEC AIO Summary and Guide

August 30, 2022

DATALOGIQ 360

Executive Summary: Architecture, Infrastructure, and Operations booklet (AIO)

The AIO booklet does not impose requirements on entities. Instead, this booklet describes principles and practices that examiners review to assess an entity's AIO functions.

With the publication of this booklet, the FFIEC member agencies replace the "Operations" booklet issued in July 2004. The title change reflects the overall importance of an entity's architecture, infrastructure, and operations (AIO). For IT Handbook purposes, the term "entities" includes depository financial institutions nonbank financial institutions, bank holding companies, and third-party service providers.

- Explains how architecture, infrastructure, and operations are separate, but related, functions that, together, assist management in overseeing an entity's activities related to designing, building, and managing the entity's technology.
- Discusses how appropriate governance of the architecture, infrastructure, and operations functions and related activities can
  - promote risk identification across banks, as well as nonbank financial institutions, bank holding companies, and third-party service providers.
  - support implementation of effective risk management.
  - assist management through the regular assessment of the entity's strategies and plans.
  - promote alignment and integration between the functions.

Management needs to implement a process, such as a life cycle approach, to continuously manage information & technology to support operational needs and mitigate AIO-related risks

AIO Roles and Responsibilities:

The booklet carves out responsibilities for different roles within an organization, from board and senior manager responsibilities, to chief architect and operations management responsibilities. Some of these roles include:

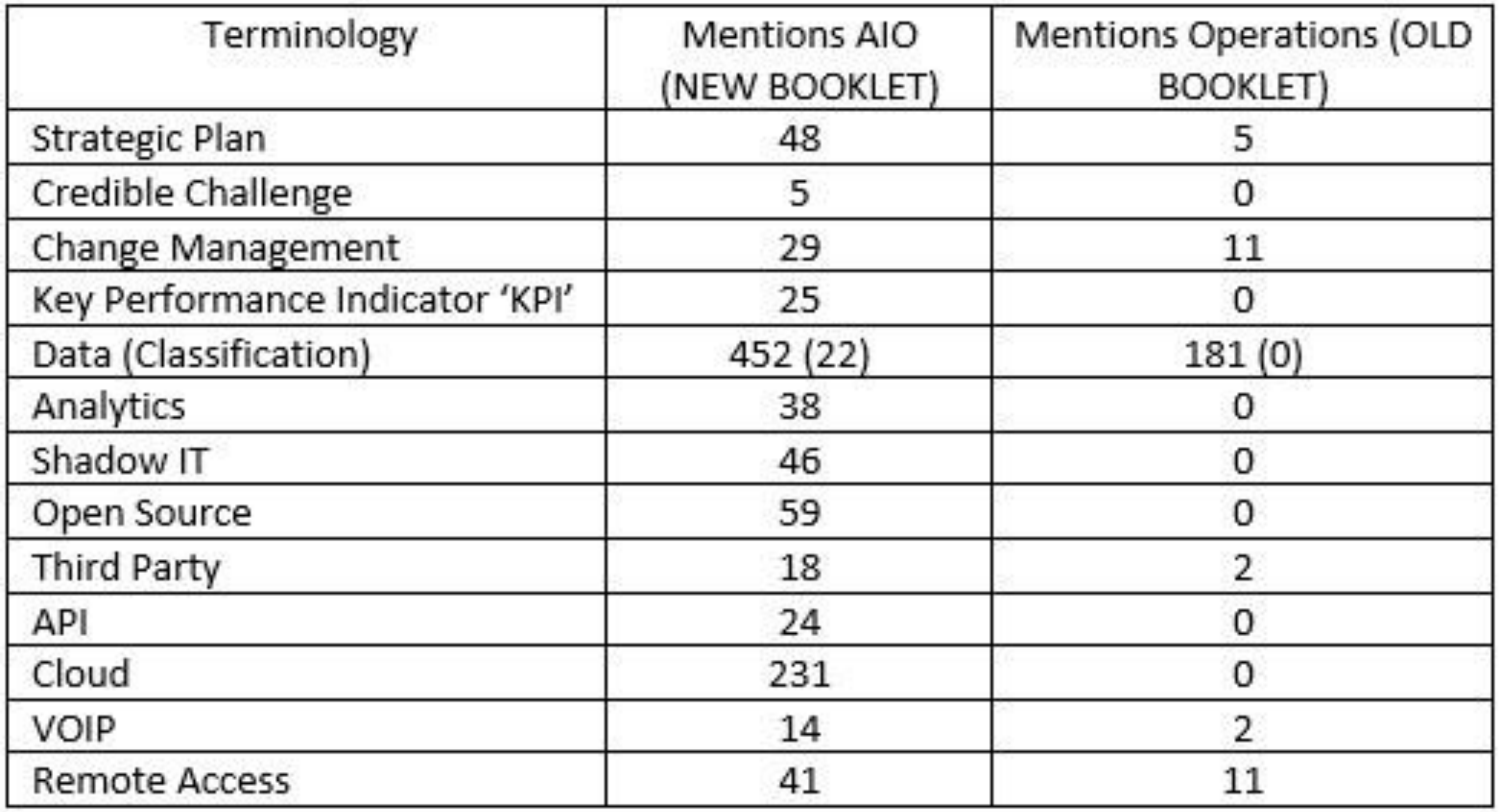
1. Board and Senior Management – responsibilities include strategic planning, and enterprise risk management. Using an enterprise risk management framework, and providing the framework for architecture, asset management, ongoing monitoring, roles, responsibilities, and procedures for all AIO activities.

2. Executives responsible for day-to-day oversight and execution
    1. Chief Information Officer - Responsibilities include overseeing and maintaining the functions of architecture, infrastructure, and operations in the IT environment, as well as delegation (and separation) of duties for these functions
    2. Chief Architect – role includes developing the enterprise model and establishing common blueprints and architectures. Ensuring consistency across lines of business and matching business results to the enterprise architecture.
    3. Chief Data Officer – role includes defining data strategies that are able to meet the organizations needs consistently while being able to meet compliance and security objectives
    4. IT Operations Management – ensures safety and soundness of the mission critical infrastructure required to enable business functions

3. IT & Data Operations personnel – cover the breadth of day to day actions supporting the digital and information requirements of a business

What’s Changed from the previous booklet?

Notice the number of mentions on data related topics



Terminology	Mentions AIO (NEW BOOKLET)	Mentions Operations (OLD BOOKLET)
Strategic Plan	48	5
Credible Challenge	5	0
Change Management	29	11
Key Performance Indicator ‘KPI’	25	0
Data (Classification)	452 (22)	181 (0)
Analytics	38	0
Shadow IT	46	0
Open Source	59	0
Third Party	18	2
API	24	0
Cloud	231	0
VOIP	14	2
Remote Access	41	11

Internal Audit, Independent Reviews, and Certification Processes Action Summary (p 12)

The board and senior management should engage internal audit or other independent personnel or third parties to review AIO functions and activities and validate effectiveness of controls. Effective AIO auditing assists the board and senior management with oversight, helps verify compliance with applicable laws and regulations, and helps ensure adherence to contractual agreements and entity policies, standards, and procedures to mitigate risks.

Banks should assess for the following:		
Independence of AIO-related audits or other reviews.	Appropriate scope and detail of AIO-related audits or other reviews	Applicable reporting of the AIO-related audit results to the board
Evaluation of third-party service providers' AIO-related audit or review reports	Qualifications of auditors reviewing AIO functions and activities	

Data Governance and Data Management Action Summary (p 15)

Management should promote a culture that takes a data-centric approach for AIO functions and define responsibility and controls as part of data governance and data management processes.

Banks should assess for the following:		
Data identification and classification processes	Data management controls for safeguarding data in physical and digital form	Effectiveness of processes for monitoring new and existing databases, noncompliant or misconfigured databases, and changes to the databases
Effectiveness of processes for securing databases, analytics tools, and reports	Processes for controlling non-masked data in non-production environments	Processes for patching databases and monitoring whether the patch level of the production database is up to date

ARCHITECTURE Action Summary (p 43)

Management should design, apply, and align its IT architecture to meet the strategic and business objectives of the enterprise. The architecture plan should meet the entity's needs for confidentiality, integrity, and availability to minimize operational and reputational risks resulting from poorly designed systems.

Banks should assess for the following:		
Identification of the entity's information and technology assets	Assessment of future enterprise IT needs	Documentation of the architecture plan, including policies, standards, and procedures
Development of appropriate design objectives, including changes, EOL, and identification of shadow IT	Design of IT architecture (e.g., in-house, virtualization and cloud, or hybrid)	Documentation of EA elements

DATALOGIQ 360

Operational Controls Action Summary (p 74)

Management should develop and implement operational controls to safeguard the entity’s operational environment. These controls should be designed to protect the overall environment, including the physical facilities, infrastructure supporting the entity’s operations, systems and software, and personnel.

Banks should assess for the following:

Effective controls over the entity’s operating centers, including physical and logical controls	Defined and appropriately administered authorization boundaries containing the entity’s systems, software, and information	IAM methods used to appropriately identify and authenticate authorized users
Personnel controls (e.g., hiring and retention practices, maintaining appropriate skillsets and knowledge, and activity monitoring processes) to maintain an effective workforce	Controls allowing for the use of personally owned devices	

DATALOGIQ 360

IT Operational Processes Action Summary (p 76)

Management should implement effective IT operational processes to reduce the number of potential operational failures and minimize the impact of issues that occur. Management should evaluate the effectiveness of those IT operational processes and adjust them as needed.

Banks should assess for the following:			
Appropriate preventive maintenance or operational restoration processes for equipment within the facilities that support the entity's business objectives	Configuration management processes	Effective vulnerability and patch management processes	Backup and replication processes that facilitate recovery
• Scheduling processes to manage and effectively use IT resources (e.g., hardware and processing time).	Capacity management processes that support the entity's current and future strategic objectives	Log management processes that allow management to capture system, software, and physical access activities	Processes for the appropriate disposal of data and media

DATALOGIQ 360

Service and Support Processes Action Summary (p 84)

Management should develop and implement service and support processes. These processes should be designed to support an entity's strategic goals and objectives by preventing issues, ensuring continuous reliability and resilience, and supporting users (e.g., business lines, personnel, and customers).

Banks should assess for the following:

Effective planning processes for service management that consider services offered, SLAs and contractual provisions, known limitations, and metrics and measurements	Communication processes with business line management	Operational support processes, controls, and mechanisms to report transmission and processing errors
Processes to document and track issues through resolution	Documented event, incident, and problem management processes	

Ongoing Monitoring and Evaluation Processes Action Summary (p 88)

Management should develop processes to oversee operations functions, evaluate the effectiveness of controls, and identify opportunities for improvement.

Banks should Assess for the following			
Implementation of processes to monitor and report on control effectiveness	Stakeholder input into the types of reports and metrics produced	Defined objectives for IT, operations, and key performance indicators (KPI	KPIs that align with the entity’s ERM processes
Processes for reporting KPIs to the board	Implementation of corrective action plans when KPIs do not meet established targets	Processes to recommend changes in operations processes and controls	Strategies for service and process improvement and methods to measure the results of those improvement efforts

DATALOGIQ 360

In a data-dominated era, DATALOGIQ 360 is transforming the companies of today into data-driven companies of the future