

AIO – 18 Gray Areas

The AIO guidance does address where “smaller and less complex entities” can be less stringent in their compliance with the guidance. However, it does not define “smaller and less complex entities,” it still requires those entities to meet certain responsibilities, and it does not define “less stringent.” Good luck, auditors!

1. Responsibilities for architecture and data management may fall to a chief architect or a data officer; however, in smaller or less complex entities, these responsibilities may be rolled into one or more other roles.
2. In smaller or less complex entities, a formal chief architect may not be named, but the responsibilities should be addressed according to the entity’s size and complexity
3. [Regarding a Chief Data Architect] This individual may be a C-level or senior executive who also reports to and works with other C-level personnel to manage risk. In smaller or less complex entities, this role may not be separate. Regardless, the responsibilities should be addressed. [Then it goes on to list a slew of duties not previously part of anybody’s job description.]
4. Smaller or less complex entities may have one policy and related procedures that encompass AIO, while larger or more complex entities may have multiple policies, standards, and procedures covering various aspects of AIO or various divisions or departments. Regardless of the entity’s size and complexity, management should implement policies, standards, and procedures that address scope, responsibilities, accountability, authority, and guidance to develop and maintain effective processes related to AIO
5. Larger or more complex entities may have multiple audits covering various departments or aspects of AIO functions and activities. Smaller or less complex entities may include a review of AIO within an IT general controls audit.
6. In larger or more complex entities, data governance and data management are formally managed with defined responsibilities and functions. In smaller or less complex entities, these functions may be included in the responsibilities of a business line manager. Regardless of the entity’s size or complexity, business line management, which generally is the most knowledgeable about the entity’s data usage, should be consulted to assist in data classification, the development of recovery standards, and control validation by personnel responsible for these activities.
7. Responsibilities for database management controls typically are managed by a DBA; however, in smaller or less complex entities, these responsibilities may be assigned to other personnel.
8. As part of ITAM, management should use appropriate inventory mechanisms to track and validate the entity’s information and technology assets. Smaller or less complex entities may use informal methods (e.g., spreadsheets) to track IT assets.
9. Management also should consider IT assets that do not fall into traditional hardware or software inventories, such as internet assets (e.g., website addresses owned, certificates employed, domains used, or rights to audio or video files). Smaller or less complex entities may have one comprehensive inventory that contains all of its technology assets.
10. Smaller or less complex entities may use manual asset inventory processes; these processes, however, should allow management to effectively document, track, and oversee the entity’s technology assets.
11. In smaller or less complex IT environments, data flow diagrams and network diagrams may be combined. In larger or more complex IT environments, the entity generally has multiple data flow diagrams and network diagrams broken out in a variety of ways (e.g., lines of business, geographic locations, network segments, and business functions).
12. Smaller or less complex entities may have a less structured architecture plan and generally have fewer initiatives or changes to the plan. Larger or more complex entities often have complex architecture plans, architecture review processes, and architecture boards or planning groups to ensure that initiatives are carried out according to architectural principles.

AIO – 18 Gray Areas

13. Smaller or less complex entities may not have EA, but those entities still should manage their existing architecture needs and planned changes. As an entity becomes larger or more complex and different systems are needed to support that growth, management should consider the implementation of EA to align its architecture with the entity's strategic plans and business functions.
14. In smaller or less complex entities, there may not be separate operating centers. For example, the entity may have only a server room or closet.
15. Adequate segregation of duties is a challenge in smaller or less complex entities. In such circumstances, appropriately implemented rotation of duties can be an effective compensating control. Management should closely review and monitor activities to provide effective supervision, facilitate training, and validate control effectiveness.
16. SLAs, referred to as OLAs when used for internal service delivery, often outline business line expectations for service management and support functions (e.g., uptime requirements and response times). Documented OLAs are less common in smaller or less complex entities; business line management, however, should still communicate and coordinate its business requirements to personnel responsible for the execution of service management functions.
17. Larger or more complex entities often use documented service requests within a system to track their activities and the actions taken. Smaller or less complex entities often track and fulfill business requests through less formal processes.
18. [regarding Change Management, from the examination work program] Depending on the complexity of the change, determine the adequacy of the processes to manage the change. Verify that changes to any IT system or service are supported by an orderly, adaptable, documented, and measurable process.
 - a. If the entity implements more complex types of changes (e.g., core conversions, migrations to cloud-based environments, or implementing a system to support a new product), assess whether formal planning and management oversight processes are in place and adequate.
 - b. If the entity implements less complex, but planned changes (e.g., implementation of patches), assess the appropriateness of the change process.