Application Onboarding Overview

September 06, 2023

Michael Klug
Principal Architect, Architecture Services
SailPoint Technologies, Inc.
mike.klug@sailpoint.com

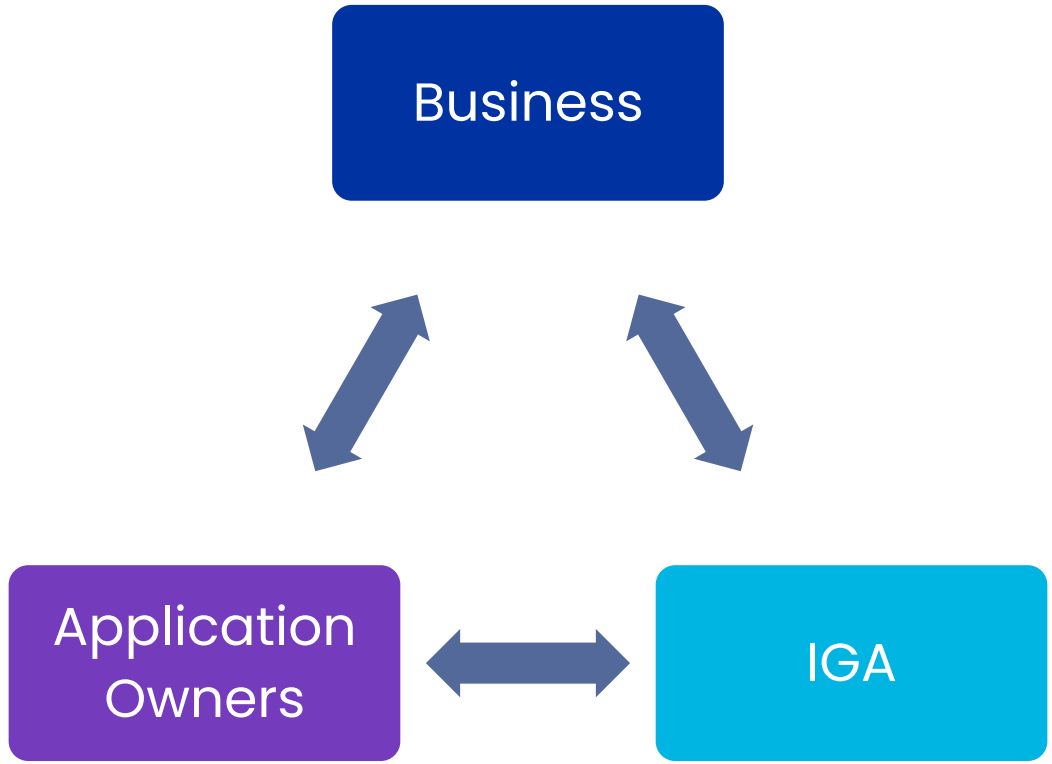
Application Onboarding Overview

Application onboarding is a process that brings data related to account access into the IdentityIQ system.

Once onboarded, use cases can be implemented to determine who should have access to that application, what access they should have, and regularly verifies that access is appropriate.

This requires active collaboration between business owners, application owners, and IGA team (Identity Governance & Administration), each doing their part for successful and secure management of an application.

The process is important to ensure that only the right people have the appropriate access to applications and information.



Handling Application Onboarding (AOB)

Two Major Workstreams

Workstream 1 – Overall Process Management of AOB

- Executing and enforcing the overall process and goals of the AOB
- Performing the prioritization information gathering
- Determining the application sets per phase
- Revisiting and revising the metrics and scoring of applications as needed
- Providing ad hoc reviews for unique situations

Workstream 2 – Application Discovery

- Tactical team that meets with and gathers information from the candidate application teams and introducing those teams to the IdentityIQ system
- Uses the application onboarding questionnaire to gather business/technical information
- Executes on integration, testing and deployment with the development team

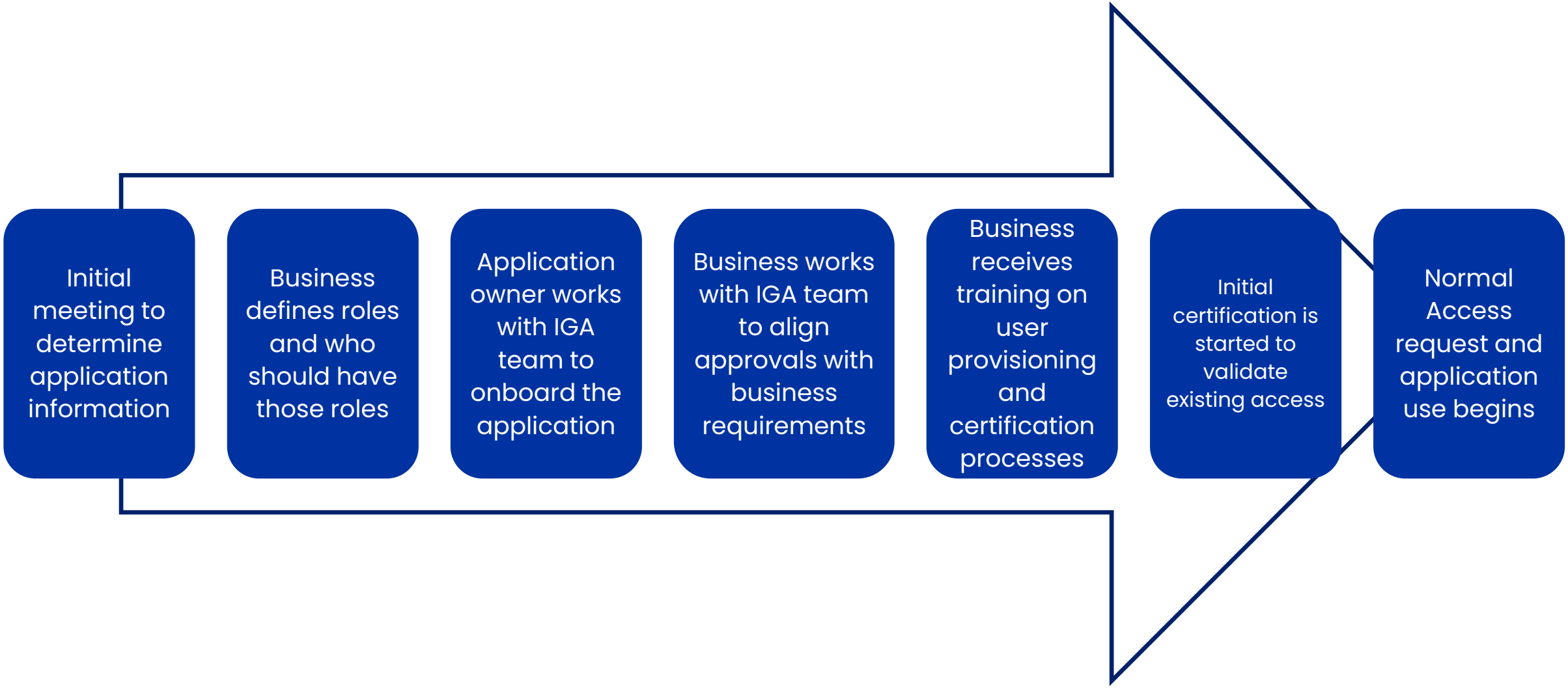
Interacting with the AOB Team

What application teams should expect during onboarding

We use the following methodology for gathering information and connecting the IdentityIQ solution to your system(s):

- Initial introductions and overview of the IdentityIQ solution
- Identification/verification of business and technical leads for your system(s)
- In person and offline follow up of information gathering via our application onboarding questionnaire
- Development environment setup and connectivity
- Data analysis for user accounts and access permissions/entitlements
- Collaboration on solution use cases
- Training reviewed and shared for admin/system end users
- Implementation and ongoing updates for new features or capabilities to use down the road

Process in Action



Business Accountability

- The business plays a key role in the application onboarding process. It is necessary for the business to define the roles of the users within the application. A role defines what should a user be able to do when they use the application. A role is also important to help define segregation of duties and policy configuration. Requesting access may also occur through entitlement/permissions request in IdentityIQ via the Entitlement Catalog
- The business has the accountability for requesting user additions and deletions, assigning roles and necessary changes to the permissions of a user. As an example, if a user changes jobs, often times an adjustment of permissions may be required within the application.
- The business is also responsible to certify users access to the application in an ongoing process.

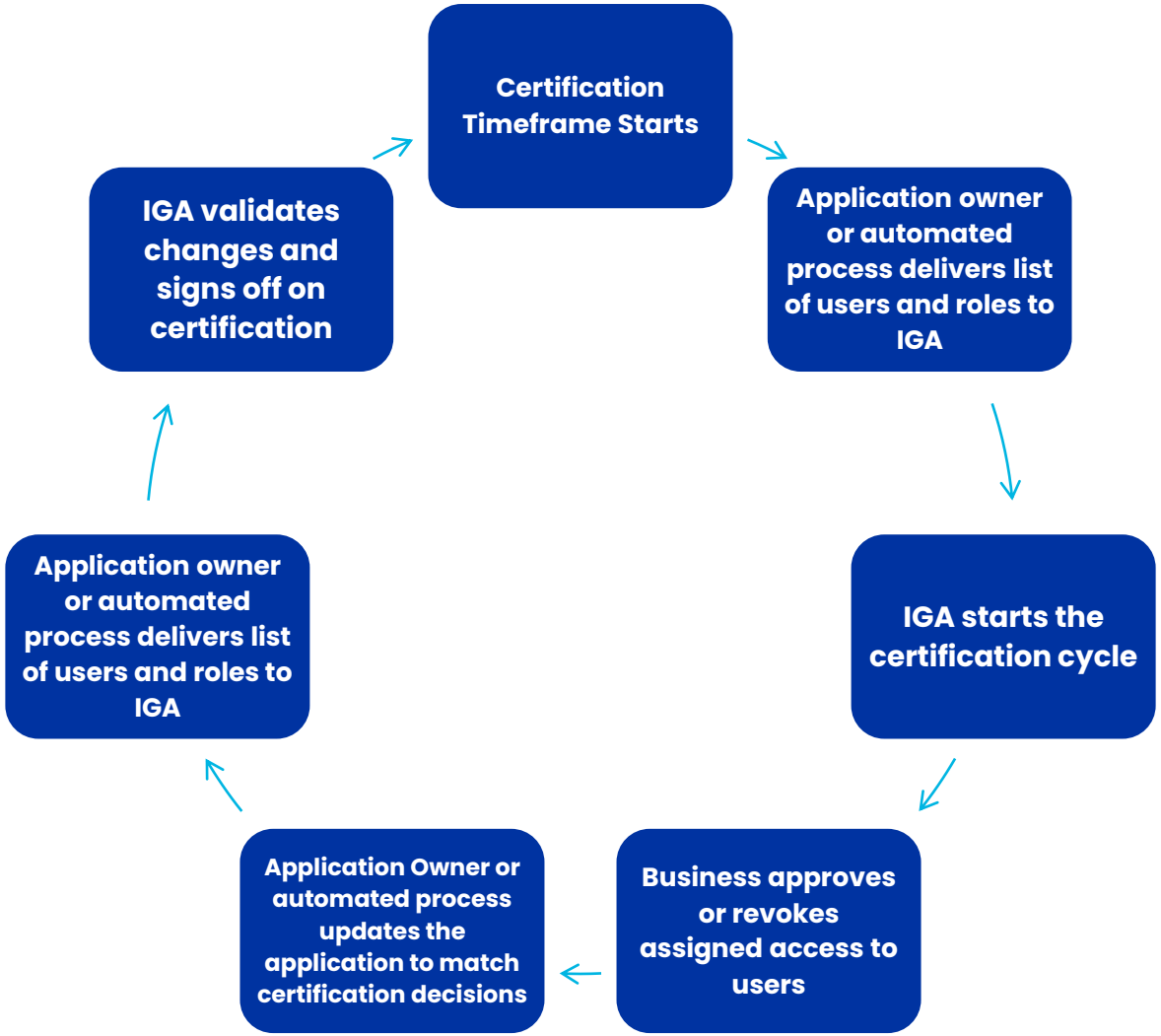
Application Owner Accountability

- The application owner works with the business to establish roles within the application. The application owner works with IGA team to define how user management activities take place, whether through automated integration with the user management system, or by a manual process such as ITSM (IT Service Management) ticketing system or email interactions.
- During this process, the application owner defines how the user management system will connect to the application to perform user adds, changes, deletes, and user certifications. If automated actions are not possible, the application owner collaborates with IGA team to determine how use cases will be handled.

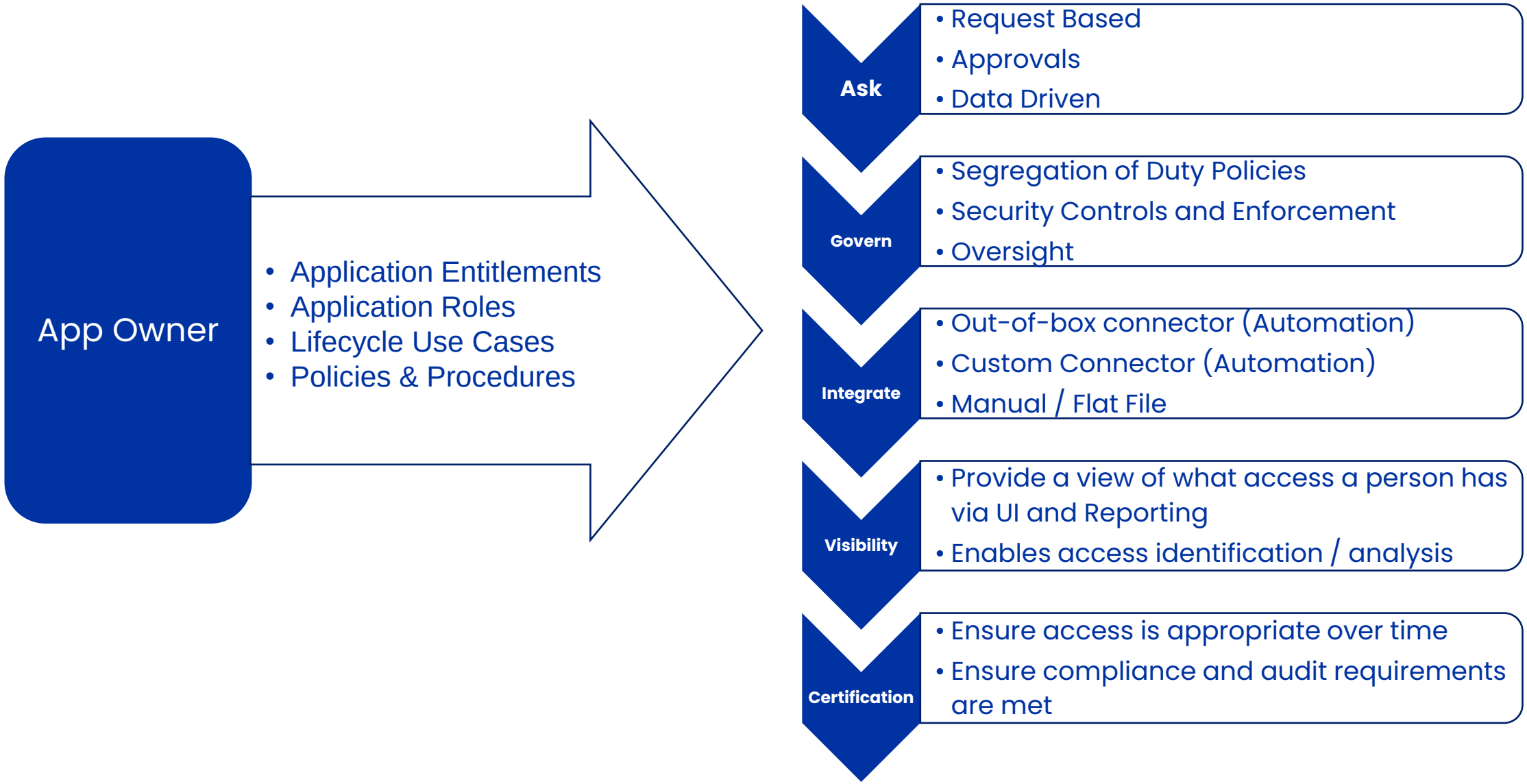
IGA Accountability

- IGA team will work in conjunction with the application owner to define the method to be used for user access management and user certification.
- If an automated integration is possible, IGA team will focus efforts with the application owner to configure connectivity between IdentityIQ and the application. IGA team will also work with the business to define how user changes are requested, what approvals are required, the schedule for access certifications, and provide training for the process to end users.
- If a manual process is necessary, IGA team will work with the business and application owners to define how user changes are requested, what approvals are required, the schedule for user certifications, and provide training for the process. In addition, IGA team will provide monitoring of this process to make sure that access certifications are being completed.

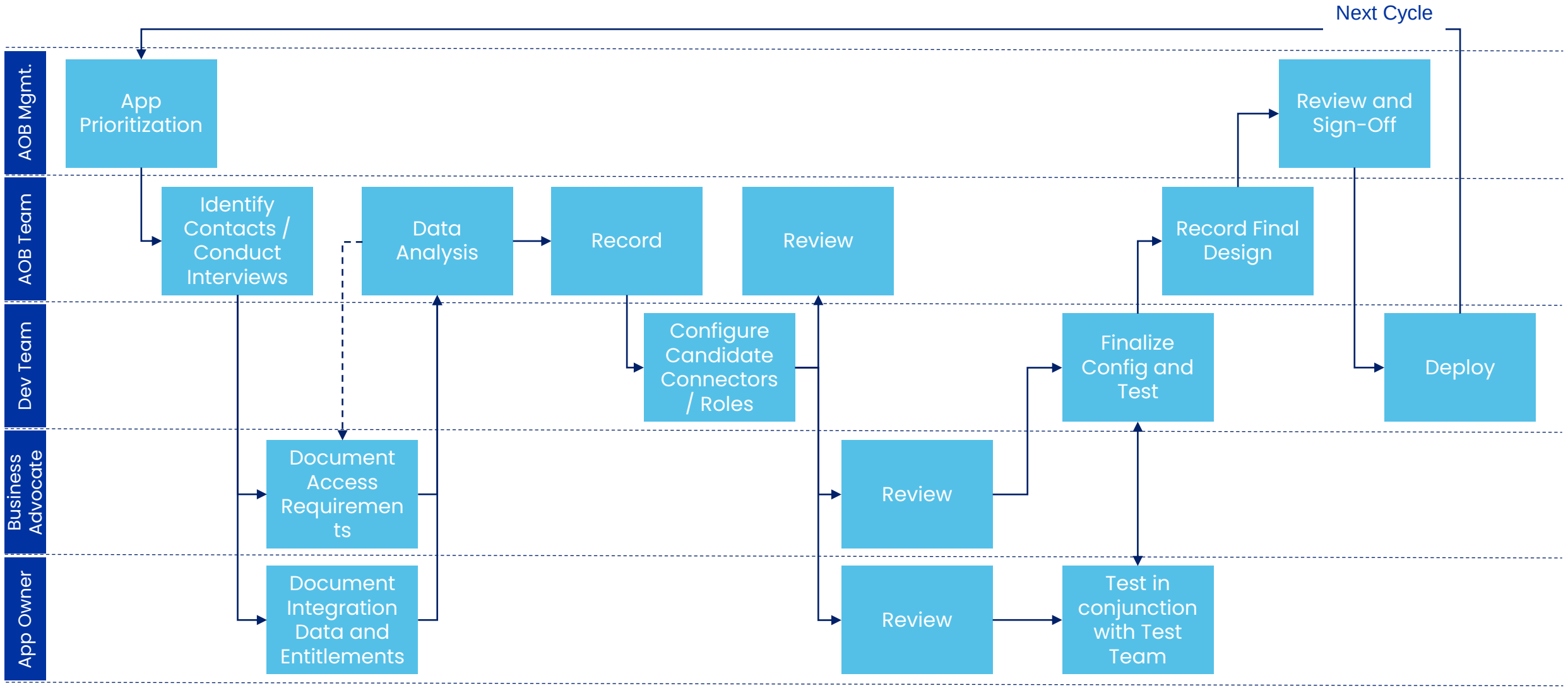
Certification Cycle



Application to Logical Access Process



Onboarding Process



Standard Steps for Application Onboarding

Process of onboarding an application

1. Data collection and analysis via Onboarding Questionnaire
2. Connector details - schema, entitlements
3. Create connector
4. Connector configuration
5. Connector rules (load, entitlements, correlation)
6. Connector data load
7. Uncorrelated accounts report review
8. Entitlement descriptions
9. Finalize mappings and process design
10. Review
11. Test
12. Deploy

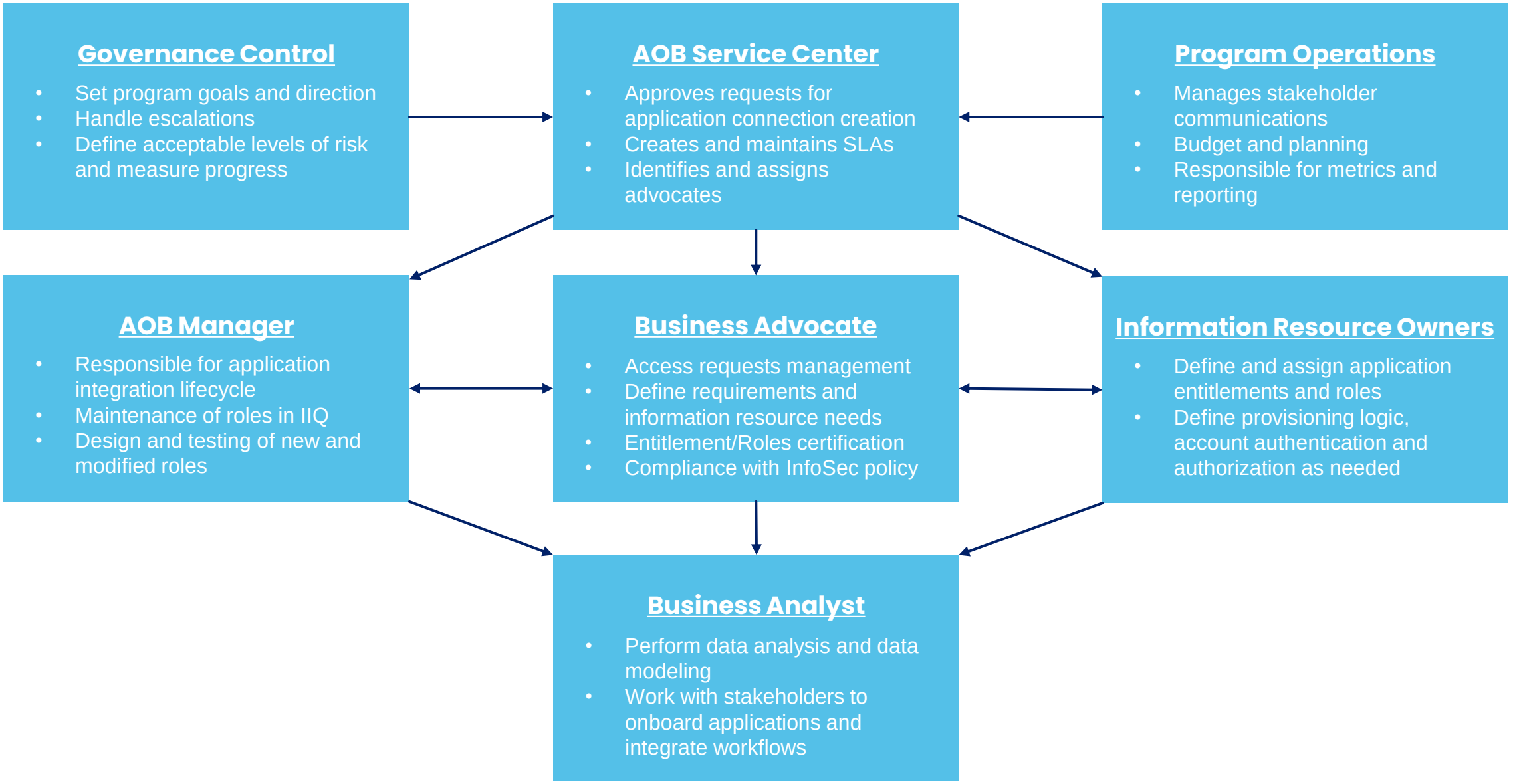
Capabilities provided post-onboarding

- Provisioning Rules (Account Management)
- Access Request
- Account Request
- Automatic Request (Joiner / Mover / Leaver)
- Workflows
- Certification
- Password Management

Application Lifecycle

- A key consideration for access governance projects is that they are not finished once deployed. Applications require constant maintenance to keep pace with constantly evolving business and technology needs. Ongoing planning and maintenance will be driven by external triggers, such as:
  - Need for business systems
  - Changes in IT systems
  - Introduction of new applications and systems
- Data collection, analysis and design should be facilitated by managers, and performed by business analysts, using mining and analytics tools. Once design has been completed, the AOB Manager will be responsible for developing and unit testing
- Following the creation of and sign-off by the owner, the AOB team is required to review and approve implementation, ensuring that new applications or modifications to existing applications are consistent with policies and standards.

Staffing Application Onboarding



Actors and Responsibilities

- **Application Onboarding Service Center**
  - Approves requests for application connection creation / mods
  - Creates and maintains service definitions and SLAs
  - Identifies and assigns Advocates
- **Program Operations**
  - Managers stakeholder communications
  - Budget and planning
  - Responsibility for metrics and reporting
- **AOB Manager**
  - The AOB Manager has functional responsibility for the application integration lifecycle
  - They perform maintenance of applications in IdentityIQ, in accordance with changes approved by AOB service center and Advocate
  - AOB Manager will perform design and testing of new connections and use cases

Actors and Responsibilities

- **Governance Control**
  - Access governance incorporates the definition and enforcement of standards and standard operating procedures surrounding user access, ensuring full compliance with appropriate regulatory mandates
  - An effective governance framework, comprised of robust and enforceable standards, is essential to the success and sustainability of an enterprise Application Onboarding Service
  - Because the CISO organization is ultimately responsible for access governance, it should act as the primary source of requirements for Application Onboarding Service adoption, enablement, strategy and prioritization of deliverables
  - The CISO is responsible for devising and enforcing governance policies that provide an operational framework for the Onboarding Service
  - The CISO will also be responsible for monitoring and ensuring timely remediation of policy violations

Actors and Responsibilities

- **Business Advocate**
  - Initiates creation / change requests according to business or technology need
  - Defines specifications and requirements
  - Defines the information resources required for business application
  - Certifies composition and membership
  - Ensures compliance with corporate and regulatory policies
  - Approves access requests as appropriate
- **Information Resource Owner (Application Owner)**
  - Technology manager responsible for the functionality, stability and security of the resource
  - Defines the rights and permissions for system-level functionality, and is accountable for controlling the production, maintenance, use, storage and access of resources
  - Approves changes to any workflows that provide access to the information resource

Actors and Responsibilities

- **Business Analyst / Data Analyst**
  - The business analyst works with business/technical stakeholders and information resource owners to define application metadata, descriptive verbiage and attributes.
  - Additionally, the business analyst models IGA business processes and workflows in accordance with documented business requirements, and facilitates communication between technical and business stakeholders throughout the onboarding process.
  - Once candidate connections, entitlements and workflows have been identified, modeled and defined by the business analyst, they are handed off to the AOB manager for configuration within IGA.

App Onboarding Best Practices

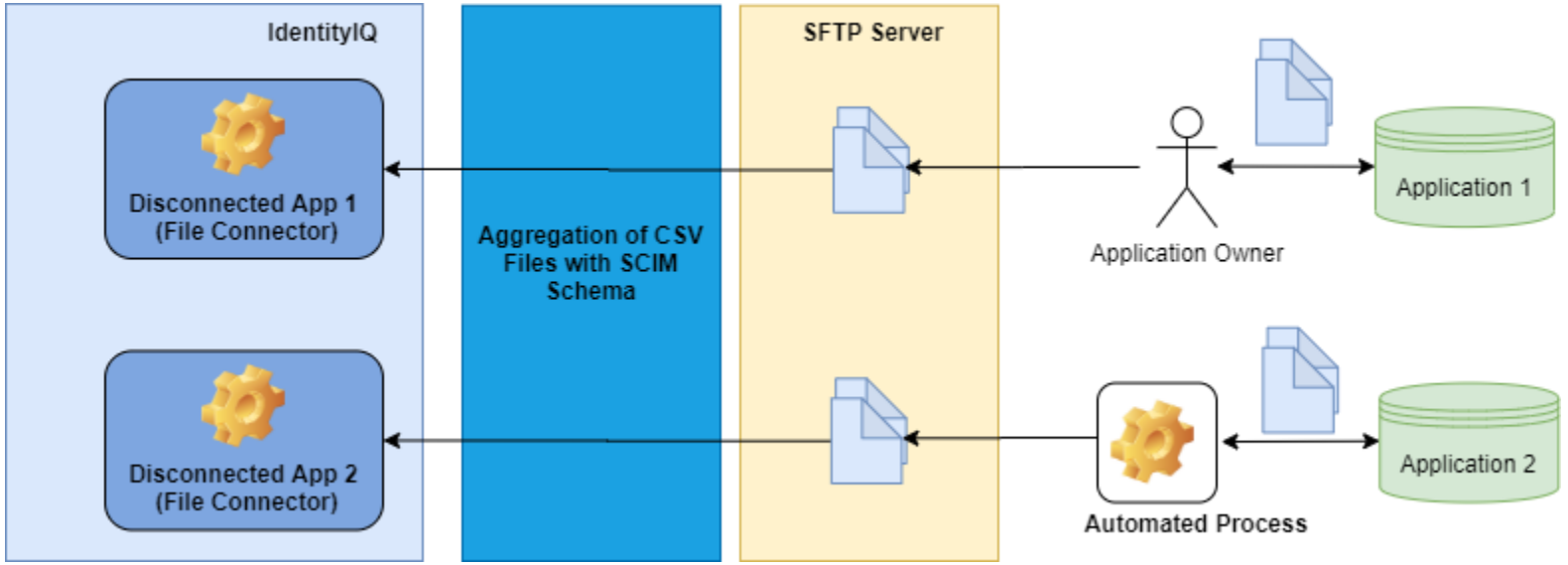
- Executive Sponsorship is Key.
- Get the Correct App Team Members Involved (needs to know technical details and process)
- Provide Clear Timelines to App Teams (your portion starts on __ date and will go through ___)
- Set expectations with App Owners on Time Needed (daily, weekly, etc.)

Prioritizing Applications for Onboarding

- Connection type = Effort Estimate
  - Small – 1day-2 weeks (flat file, AD, LDAP, ootb connector)
  - Medium – 3-4 weeks (Web Services, JDBC, Mainframe, connector)
  - Large – 6-8 weeks (Custom connector)
- Compliance Requirements (SOX, GDPR, HIPAA, etc.)
- Company Usage (i.e. – high volume of provisioning, large certification volumes, etc.)
- Number of Identities
- App Owner Team Readiness
  - Have app details been provided to the IAM team?
  - Can be accomplished via creating a form, via phone call, or a combination.

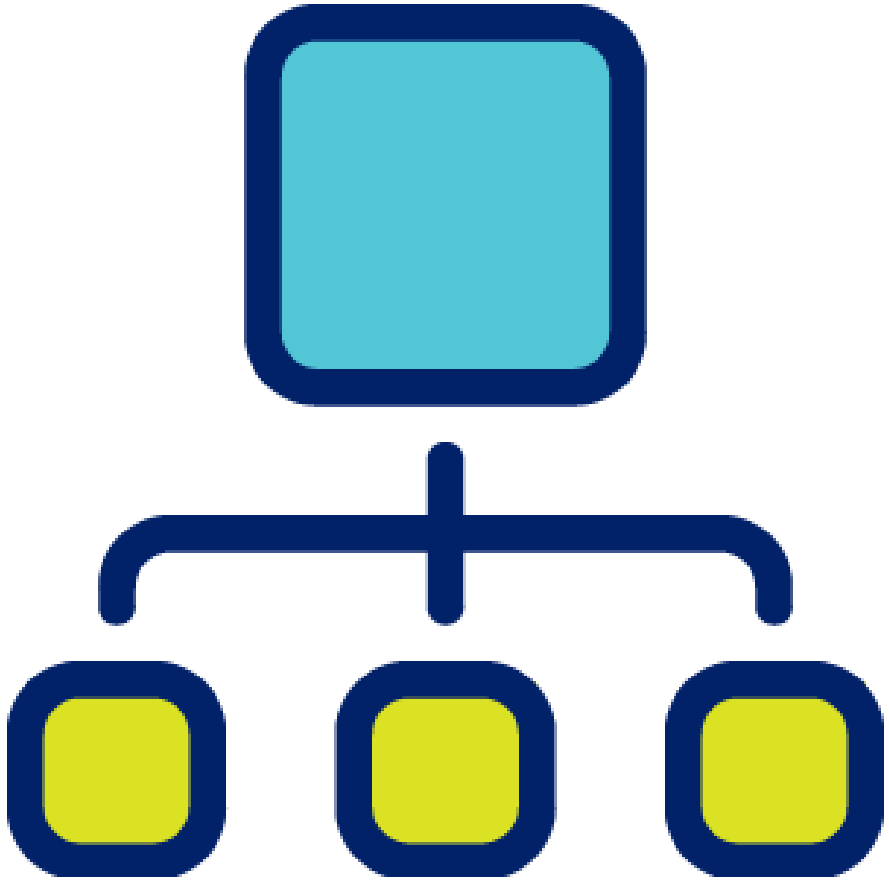
Onboarding Low Touch Apps via Flat File

Application owners push data in CSV file format to an SFTP server, either manually or through other process. IdentityIQ aggregates the data on a schedule via DelimitedFile Connectors. The CSV files have the same schema as the SCIM connector



Onboarding Low Touch Apps via Platform

- Onboard multiple applications to a platform (AD, LDAP, etc)
- Utilize schema attribute or entitlement to denote application



App Owner Hours Estimates

- 8 hours = Requirements/Design
- 8 hours = Onboard app to Sandbox and PROD
- 8 hours = Testing
- 8 hours = Verify data in PROD
- **TOTAL = 32-40 hours**
- (This will be more time for custom applications)

Role Onboarding Example

Bob (Business Owner) needs to use applications delivered by John to support his business objectives.

John (Application Owner) owns 3 applications with the following entitlements associated:

APP_A has entitlements A1, A2, A3
APP_B has entitlements B1 and B2
APP_C has entitlements C1, C2, C3, C4, C5

Role Onboarding Example (cont'd)

Bob knows what roles his team needs. Finance Administrator and Finance Monitoring are two roles within his team.

The Finance roles consist of different entitlements within three different applications.

Bob and John discuss and agree on which of the entitlements that John has defined within his applications make up the roles that Bob's people needs.

- Finance_Administrator consists of entitlement A1 in APP_A, B1 in App_B, and C1 in App_C.
- Finance_Monitoring consists of entitlement A2 in APP_A, B2 in App_B, and C1 in App_C.

Role Onboarding Example (cont'd)

IGA team works with John to integrate with his applications to enable the use of the entitlements and accounts in the applications.

IGA team works with Bob to construct the roles with the appropriate entitlements in each application for his team.

There may be a higher discussion with the business leader Jim. Jim discusses roles with Bob, but does not need to be involved with the Bob & John discussions.

The concept of the business may involve different levels of communication and levels of discussion. The same may hold true at the application level. John may discuss the higher level application entitlements and concepts, but have others at a lower level for further discussions.

Thank You!