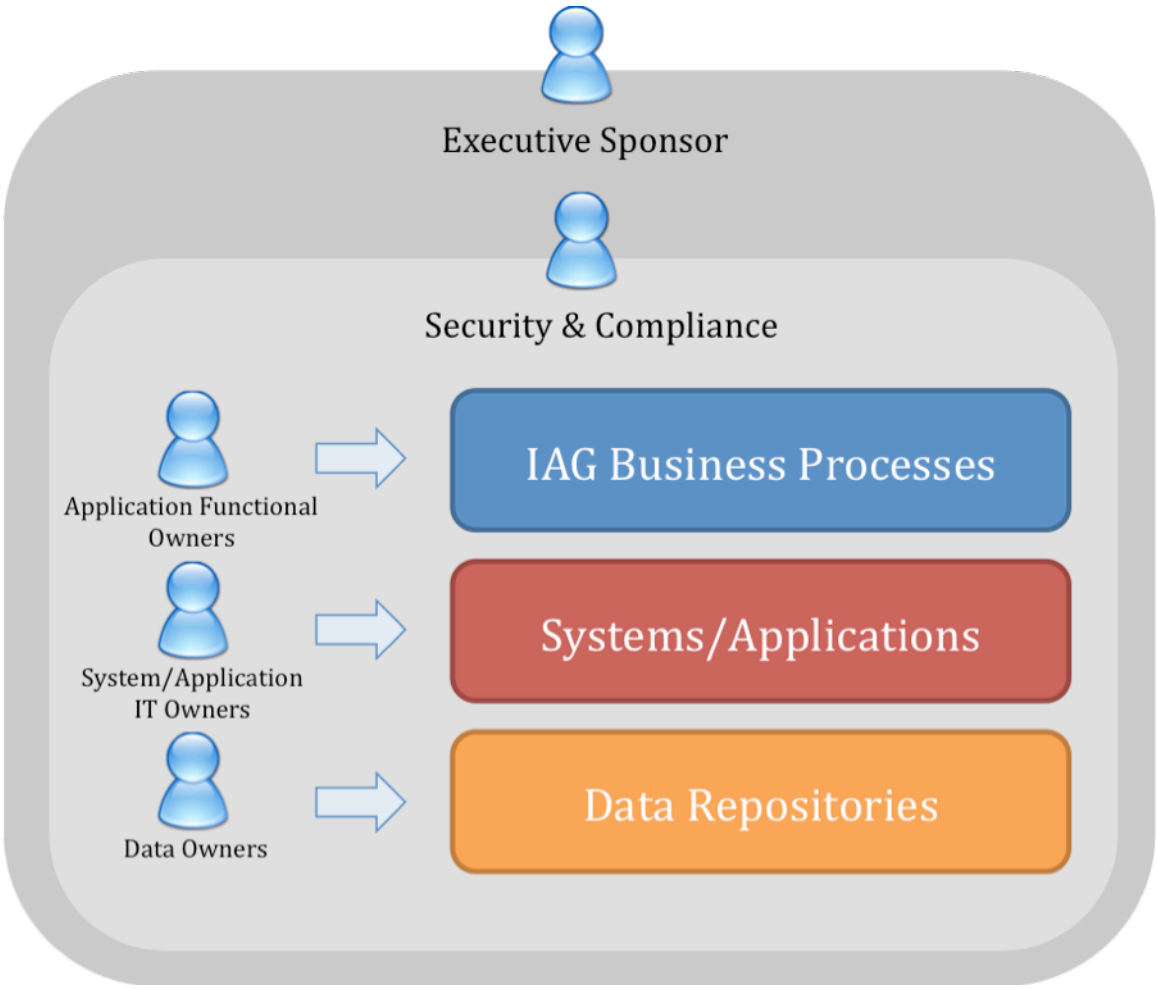
Identity Initiative
Workshop Stakeholders

The success of Identropy's Identity Workshop relies heavily on the attendees having the right combination of knowledge of the existing processes and infrastructure on the one hand, and executive decision making authority on the other. The workshop is designed to engage the client in a roundtable discussion with key stakeholders in order to foster discussion around the client's identity management requirements, in order to identify the appropriate solutions as well as the foundations for an Identity & Access Governance roadmap.

Stakeholders Overview

The five types of stakeholders are Process Owners, System/Application Owners, Data Owners, Security & Compliance and Executive Sponsors. Each category has subdivisions, and an individual may fall into multiple classifications.



Executive Sponsor

An executive sponsor is an individual who authorizes the Identity & Access Governance (IAG) Program and funds it. While it isn't the Executive

Sponsor's responsibility to directly manage the project, he or she must be involved enough to provide the necessary leadership and authorization to the overall Program in order to ensure the necessary cooperation from the various stakeholders for the success of the program.

Examples: CIO, CFO, Director of IT, etc.

Questions to Ask: What are the current strategic IT initiatives for your organization? What is the relationship, if any, of your identity initiative and your current strategic initiatives? What are the drivers for an Identity & Access Governance project in your organization? Does your organization have a corporate governance structure in place? IT governance?

Security & Compliance

Security & Compliance are the individuals who define acceptable/unacceptable risks within your organization as well the corporate security and compliance policies. In many organizations, these stakeholders can be divided into 2 categories: the IT Security & Compliance stakeholders and the Financial Compliance stakeholders.

Examples: CFO, Compliance Officer, CISO, etc.

Questions to Ask: Does your organization currently have a security & compliance policy? Please describe. How is risk defined in relation to access to systems within your organization? Does your organization have security model in place that matches your risk definition? Does your organization have an attestation model in place? authorization model? role model?

Application Functional Owners

Process Owners are responsible for interacting with corporate systems or applications (or other individuals who interact with the systems or applications) in order to manage identities from a functional perspective. These individuals do not interact with the systems or applications from a technical maintenance perspective, and are typically limited to performing identity & access governance related tasks on the system or

application through a graphical interface that is not intended for technical administrators.

Examples: HR Functional Administrators, Deployment Managers (for applications, networks), LOB Managers, Help Desk Administrators, Portal Content Managers, Change Order Approvals Manager, Physical Security Administrator, etc.

Questions to Ask: How are user accounts created/disabled/modified for end users within your organization? How are passwords changed? How is access granted to various aspects of a system/application? Is access managed by group memberships or roles? Are approvals required? If so, for what actions? Are there multiple administrators for the system or application? If so, how are responsibilities divided? Is there a delegated model? Are you involved with user access reviews? If so, describe the process and your involvement in it. Are there any future changes expected to the existing processes and why? Are there any upcoming needs that may require changes to the existing processes?

System/Application IT Owners

System/Application Owners are responsible for maintaining various systems or applications from a technical perspective. These individuals tend to not only manage identities within the system, but also manage the overall maintenance of the system. These individuals may also leverage a graphical interface to maintain user identities, although the interface is intended for use by technical administrators.

Examples: Active Directory Administrators, Content Management System Administrator, Unix Administrators, Vendor Portal Administrator, etc.

Questions to Ask: What are the different user types within the system you manage? Are there multiple ways for users to be created/deleted/disabled? What is the security model for the application you own? Who contacts you if there is a problem with a user's identity? How is user profile data updated in the system? How do you manage access within the system or application? Are there any non-human users in your system? Does your application function as a "user" for any other applications or systems? Are any new critical systems/applications

expected to be deployed in the near future? How is the identity data related to the new systems/applications going to be managed?

Data Owners

Data Owners are responsible for managing data in the environment. They are usually database administrators and directory infrastructure administrators with an in-depth understanding of the size and flow of data in the infrastructure. Data owners should be knowledge of any online or offline synchronization activities that occur between repositories, as well as data transfer methods that are employed.

Examples: Directory Infrastructure Architect, Database Administrator, etc.

Questions to Ask: How is data entered into the various repositories? Are there synchronization activities of identity data? What tools are utilized to pull/push data? How is identity data classified? How is access to the data managed? Are access control lists or other access management mechanisms utilized?

Suggestion Points

Note: The examples of roles/titles provided above for Identity & Access Governance Stakeholders are typically not one-to-one relationships with individuals in a corporation, as overlap of job functions is common. For example, one individual may function as a system owner as well as a data owner. Another example is a Systems Administrator may utilize a graphical interface to create/delete users, thereby functioning as a process owner as well.

Note: The two critical ingredients for a successful workshop are knowledge of the existing identity & access governance related processes (from both a technical and business perspective) that exist within the corporation, and the decision making authority regarding making changes to the existing processes. Knowledge of the process without the ability to make changes may result in a plan that cannot be executed, while authority without the knowledge of what exists results in aspirations without a plan of execution. It is critical for both aspects to be present at different phases of the workshop.

Note: A common misconception regarding the Identity & Access Governance workshop is that there exists a direct relationship between the number of parties present at the workshop and its efficacy. In fact, the opposite holds to be true in most cases. The best result is to minimize the number of parties present without sacrificing the two critical ingredients for a successful workshop mentioned above. An excellent approach is to seek out individuals that can accurately represent multiple systems, applications, processes and data repositories. Often times, an individual can accurately represent both the technical and process aspects of system or systems – or an individual may be able to represent data flow within the entire organization. Such individuals are typically extremely useful in the workshop.

Note: Another common misconception is that decisions regarding scope definition for identity & access governance projects should be deferred to after the completion of the workshop. For larger organizations, a preliminary scope check regarding the expected identity management deployment is critical in order to ensure the practicality of the workshop. Rather than initially seeking for a comprehensive map of every detail regarding an identity & access governance infrastructure, it is better to focus on gathering stakeholders from the business critical applications, systems and repositories first.