protiviti®
Global Business Consulting

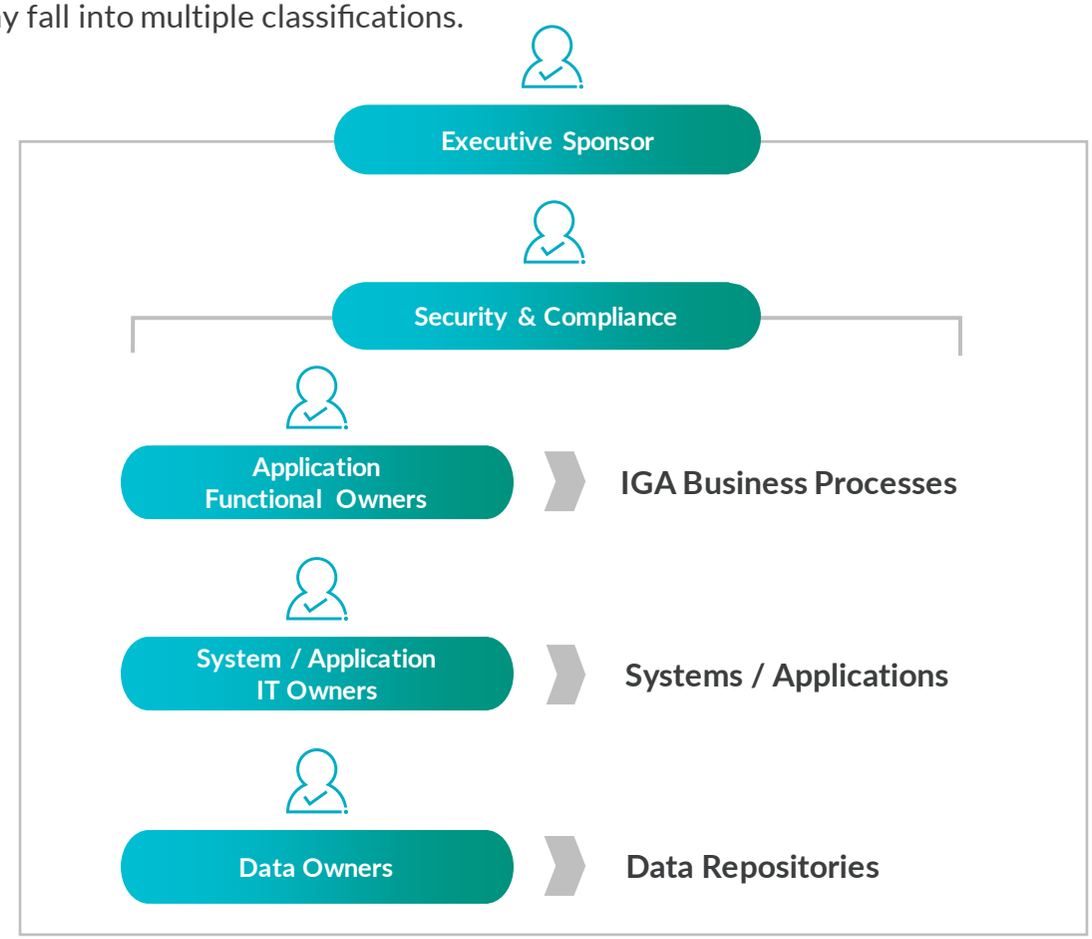
Identity Governance and Administration Workshop Stakeholders

Achieve success with the right people in the right roles

The success of Protiviti's Identity Governance and Administration (IGA) workshop relies heavily on the attendees having the right combination of knowledge of both existing processes and infrastructure and executive decision-making authority. The workshop is designed to engage key stakeholders in a roundtable discussion to foster discussion around your identity management requirements, identify appropriate solutions and begin building the foundation for an Identity Governance and Administration (IGA) roadmap.

Stakeholders Overview

The five types of stakeholders are executive sponsors, security and compliance, appliance functional owners, system/application IT owners and data owners. Each category has subdivisions, and an individual may fall into multiple classifications.



IGA Stakeholders

Executive Sponsor

An executive sponsor is an individual who authorizes and funds the Identity Governance and Administration (IGA) program. While it is not 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 to ensure 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 IGA and your current strategic initiatives?
- What are the drivers for an Identity Governance and Administration project in your organization?
- Does your organization have a corporate governance structure in place? IT governance?

Security and Compliance

Security and compliance are the individuals who define both acceptable/unacceptable risks and corporate security and compliance policies within your organization. In many organizations, these stakeholders can be divided into two categories: the IT security and compliance stakeholders and the financial compliance stakeholders.

Examples: CFO, Compliance Officer, CISO, etc.

Questions to Ask:

- Does your organization currently have a security and 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?

protiviti®
Global Business Consulting

IGA Stakeholders

Application Functional Owners

Application Functional Owners and 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 Governance and Administration 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 or 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 system maintenance. 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 or 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 a 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?

protiviti®
Global Business Consulting

IGA Stakeholders

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 have knowledge of any online or offline synchronization activities that occur between repositories and 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 Governance and Administration (IGA) 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 who may use a graphical interface to create/delete users, thereby also functioning as a process owner.

Note: A common misconception regarding the Identity Governance and Administration 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. It is best to minimize the number of IGA workshop attendees to ensure maximum results. We recommend including individuals that can accurately represent multiple systems, applications, processes and data repositories. Often, 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: The two critical ingredients for a successful workshop are knowledge of the existing Identity Governance and Administration related processes (from both a technical and business perspective) that exist within the corporation and having the decision-making authority to make 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: Another common misconception is that decisions regarding scope definition for Identity Governance and Administration projects should be deferred until after the workshop. For larger organizations, a preliminary scope check regarding the expected identity management deployment is critical to ensure the practicality of the workshop. Rather than initially defining every detail of an Identity Governance and Administration infrastructure, it is better to first focus on gathering stakeholders from the business-critical applications, systems and repositories.

protiviti®
Global Business Consulting