WHITE PAPER

Delivering Business Value Through a Well-Governed Digital Identity Program

GUIDEPOINT
SECURITY

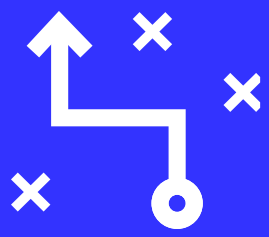
A strong governance process enables your identity program to be agile in adopting new approaches to Cyber Security, such as zero trust, in the support of your business.

- ✔ When instituting an IAM program, IAM practitioners should identify the key stakeholders early and define program level “attributes” to ensure full support from all business groups.
- ✔ The “attributes” can be derived from business requirements and can help in many aspects of the program which will be discussed in this paper.
- ✔ A well-defined governance framework that uses an attribute-based approach supports the creation of IAM capabilities, helps prioritize implementation and roll out of additional capabilities, and helps to keep all stakeholders continually informed.

Identity and Access Management as a Key Business Enabler

Security solutions are generally designed with the focus on Confidentiality, Integrity and Availability (CIA). However, just focusing on CIA limits the ability to fully communicate the value of IAM to the business. Although IAM is often considered a security and compliance function, a mature IAM program can also deliver many additional business benefits, including reduced operational costs through process automation, improved user experience through single sign-on, improved user productivity through self-service and birth-right provisioning, and reduced risk through automation of lifecycle process and access certification.

This white paper explores how IAM programs can deliver value and help meet business objectives through an attribute-based approach. This paper also discusses the necessary framework for identity governance programs and how to create a governance structure for delivering expected outcomes to the business.



Digital identity is central to conducting business in today's digital world, and a sound digital Identity and Access Management (IAM) capability is critical to securely operating in an increasingly online environment. An effective and successful IAM program requires both agility and strong governance to not only ensure that current business needs are met, but also flexible enough to meet future business needs while reducing time to value.

Identity and Access Management (IAM) gives businesses the tools and processes necessary to manage the digital identity lifecycle processes and govern user access to key information assets, making IAM central to the way an organization conducts business in a digital environment. Yet, as the pace of digital transformation has increased, the definition of 'identity' has evolved, making the classification and ongoing management of digital identities more complex. No longer limited to human staff, identity has expanded to include "things" or non-human identities. Coupled with digital transformation are increased cloud adoption and remote work, which further blur the boundaries of the traditional network perimeter, creating a greater need for cybersecurity around identity and access.

New IAM approaches such as "zero trust" require a solid foundation built around the three pillars of IAM: identity governance and administration (IGA), privileged access management (PAM), and access management (AM). A successful IAM program needs to fully support all aspects of business operations, as well as key business drivers and objectives. A well-defined governance framework is essential to achieving these objectives.

Understanding Identity Governance Attributes

When organizations roll-out a formal identity program, three of the most common missteps are failing to define the stakeholder groups, failing to take time to understand the business needs of each stakeholder groups early enough in the process, and failing to document these stakeholder requirements. By identifying key stakeholders early and the defining program 'attributes' (keywords derived from stakeholder requirements), IAM practitioners can maximize commitment and buy-in from all business groups, which is critical in the journey of creating a mature IAM program. The approach of defining program "attributes", based on work by Sherwood Applied Business Security Architecture (SABSA), can be used to facilitate the following:

- Selection of an appropriate technology solution.
- Alignment of identity program objectives to key business drivers.
- Reporting on identity program performance on an ongoing basis.

Mapping Identity Governance Attributes for each Stakeholder Group

IAM programs have many stakeholders and each stakeholder has different program requirements based on the business process they manage or support. The figure below lists key stakeholders and a set of attributes that are typically most important to each stakeholder group.

Identity Governance Stakeholder Attribute Map

Attribute-contributing Stakeholders

Executives & Sponsors	End-user Computing	Managers	Operations	Risk Management	Compliance	Enterprise Architecture
C-level Executives, Program Sponsors	Staff, Customers, Contractors, non-human identities	Access or Authorization-granting Managers	HR, IT Operations, Service Desk	Operational and Information risk	Legal, Compliance	Enterprise Architecture team (IT)

Attributes: Keyword associated with the stakeholders based on requirements, values, objectives, or priorities

Reduction in Operational Cost	Accessible	Automated	Available	Assurable	Admissible	Extendable
Support for Business Growth	Accurate	Cost Effective	Interoperable	Auditable	Compliant	Flexible
Speed and Agility	Consistent	Maintainable	Standardized Processes	Certifiable	Enforceable	Scalable
Innovation	Current	Access Governed	Performance-measured	Automated Remediation	Reporting & Analytics	Standards Compliant
Return on Investment	Ease of Use		Optimized TCO	Duty Segregated		Out-of-the-box Integrations
Improved Productivity	Self-service					
Time to Value						

Executives and Program Sponsor Stakeholders and Attributes

Executives and program sponsors include “C-suite” employees (e.g., CEO, CIO, CISO) and the program sponsor (e.g., C-level executives or another member of senior management). Executive and program sponsor attributes serve as the starting point for most programs within an organization and help create the framework for both current and future business needs. Typically, these attributes include:

REDUCTION IN OPERATIONAL COST

Automation of key business processes such as joiner, leaver, and mover results in the reduction of operational cost as manual steps are removed.

SUPPORT FOR BUSINESS GROWTH

Continually aligning the identity management program with business objectives can effectively support business growth and expansion—for example, integration with cloud infrastructure and visibility and ability to govern cloud access.

SPEED AND AGILITY

The identity management program needs to keep pace with business transformation initiatives and be agile enough to reduce time to market for new capabilities.

INNOVATION

The identity management team should question the status quo and work with technology vendors to continually evaluate how new vendor innovations can be used to improve business operations and support business growth.

RETURN ON INVESTMENT

As more applications and systems are integrated with the IGA platform for automated provisioning, operational costs are reduced, which helps to improve the return on investment. Ongoing integration of new business applications is critical to deliver ROI.

IMPROVED PRODUCTIVITY

Productivity improvement includes automation of repeatable business processes such as joiner, leaver, mover as well as access certification to reduce resource requirements and operational cycles.

TIME TO VALUE

IAM teams need to deliver incremental capabilities that are most critical for the business through an agile delivery approach, for example, delivering foundational digital identity lifecycle management capability and user self-service followed by cloud access management. Attempting to roll out many capabilities together results in increased time to value.

End User Computing Stakeholders and Attributes

End-user computing stakeholders are composed of individual users. This stakeholder group is usually the biggest IAM customer. The most important user attributes include:

ACCESSIBLE

Users require uninterrupted access to the IAM system based on service level agreements (SLAs), as such the design should address availability and accessibility requirements.

ACCURATE

End-user and entitlement data in the system needs to be accurate and reflect changes affected by lifecycle events as well as reviewer decisions during access certifications.

CONSISTENT

The individual systems in a clustered environment needs to have consistent configurations and data.

CURRENT

End-user and entitlement data need to be kept current in the system through ongoing aggregations.

EASE OF USE

The system's user interface (UI) should be easy to navigate while conducting various daily tasks, such as requesting and approving access and performing self-service.

SELF-SERVICE

Users should be able to perform tasks without requiring assistance from the service desk.

Manager Stakeholders and Attributes

This stakeholder group is comprised of the management team that are responsible for reviewing and approving or rejecting user access. The most important and relevant attributes include:

AUTOMATED

Repeatable processes such as joiner, leaver, mover, and access certification need to be automated. In addition, key development items such as software build and deployment as well as test execution should be automated.

COST EFFECTIVE

The solution should be cost-effective to support efforts on an ongoing basis. As such, it is important to minimize customization to lower the total cost of ownership.

MAINTAINABLE

The IGA system should be easy to maintain and staff to support the selected solution should be easily acquirable in the marketplace.

ACCESS GOVERNED

Access reviewers have other responsibilities as defined by their primary job duties. Access certification, when performed manually, tends to be cumbersome and time-consuming, which may result in the exercise being relegated to a 'rubber-stamp' practice. Automating this process not only reduces operational cycles but also improves user experience and overall efficiency.

Operations Stakeholders and Attributes

Business teams that support IT operations, organizational change management (OCM), service desk, or human resources (HR) have a vested interest in IGA and expect that IGA will deliver certain values from an operational standpoint. Typical attributes for this stakeholder group includes:

AVAILABLE

The most critical aspect of any solution from an operational standpoint is system availability, and the IAM solutions should be designed based on availability requirements.

INTEROPERABLE

Organizations typically have various technology solutions addressing key business requirements, and these solutions need to interoperate. For example, IGA should be able to integrate with the PAM solution to manage the lifecycle of privileged accounts. Likewise, the SSO solution should be able to integrate with IGA for seamless user login.

STANDARDIZED PROCESSES

It is important to standardize processes across the organization, as automating disparate processes to deliver the same outcome can increases the TCO.

PERFORMANCE-MEASURED

The solution should be designed to deliver an expected level of performance at peak loads, such as when performing large access certifications.

OPTIMIZED TCO

IAM solutions, in particular IGA, should support most of the requirements out of the box, so that custom solutions are minimized. Customized solutions increase the total cost of ownership and makes upgrades expensive.

Risk Management Stakeholders and Attributes

Risk management stakeholders include business and IT risk departments. These groups often work closely together to identify, manage, and respond to risk factors associated with both business operations and IT functions. The following attributes are important from a risk management standpoint:

ASSURABLE

IGA solutions, in particular, need to provide a 360-degree view of identity and associated access and produce reports of such access when required. This provides assurance of ongoing access-related activities, such as access removal as part of a termination lifecycle event.

AUDITABLE

Risk management stakeholders will want to audit and report on various identity lifecycle events, as well as actions from access certification.

CERTIFIABLE

User access can be easily certified through an automated process.

AUTOMATED REMEDIATION

When reviewers make access decisions, any access flagged for removal can be automatically removed from critical applications and systems.

DUTY SEGREGATED

The IGA system supports implementation of segregation of duties controls that are designed in collaboration with functional teams.

Compliance Stakeholders and Attributes

Almost every industry has some degree of regulation and compliance. Compliance stakeholders may include members of the legal or compliance teams. Examples of compliance attributes include:

ADMISSIBLE

Any updates to user access should be admissible in a compliance or regulatory environment to support claims of policy adherence.

COMPLIANT

The IGA solution is particularly useful in helping an organization comply with the regulatory requirements applicable to their industry. For example, the IGA solution can suspend network access if certain training is not completed on time, as required by North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards, which are applicable to the energy and utilities industry.

ENFORCEABLE

Various identity and access policies can be enforced proactively by the IGA solution, such as requiring two-level approval when requesting certain entitlements or flagging access requests as violations of a separation of duties (SOD) policy.

REPORTING & ANALYTICS

The IGA solution supports various reports out of the box required to collect evidence of action performed as a result of a life cycle event or access certification.

Enterprise Architecture Stakeholders and Attributes

Because enterprise architecture works closely with business teams to define future solutions to support new business requirements, identity management should be an integrated part of the enterprise architecture process. As such, enterprise architecture becomes a key stakeholder for identity governance. Some of the key attributes from architectural standpoint are:

EXTENDABLE

The IGA solution should be extendable to provide visibility into various on-premise and cloud applications and infrastructure as hybrid environments are becoming more commonplace within organizations.

FLEXIBLE

The IGA solution should allow flexibility to update key out-of-the-box functionality such as workflows and various templates to meet certain business needs.

SCALABLE

The solution must support vertical and horizontal scalability to allow for future business growth and expansion.

STANDARDS COMPLIANT

The solution should support various industry standards, such as System for Cross-domain Identity Management (SCIM) for provisioning, especially since many of cloud applications support SCIM-based integrations for provisioning across domains. Likewise, the system should be able to integrate through application program interfaces (APIs) that are common for performing user access operations in many applications.

OUT-OF-THE-BOX INTEGRATIONS

IGA systems should provide a framework that allows connecting to a large number of applications and systems through purpose-built or generic connectors.

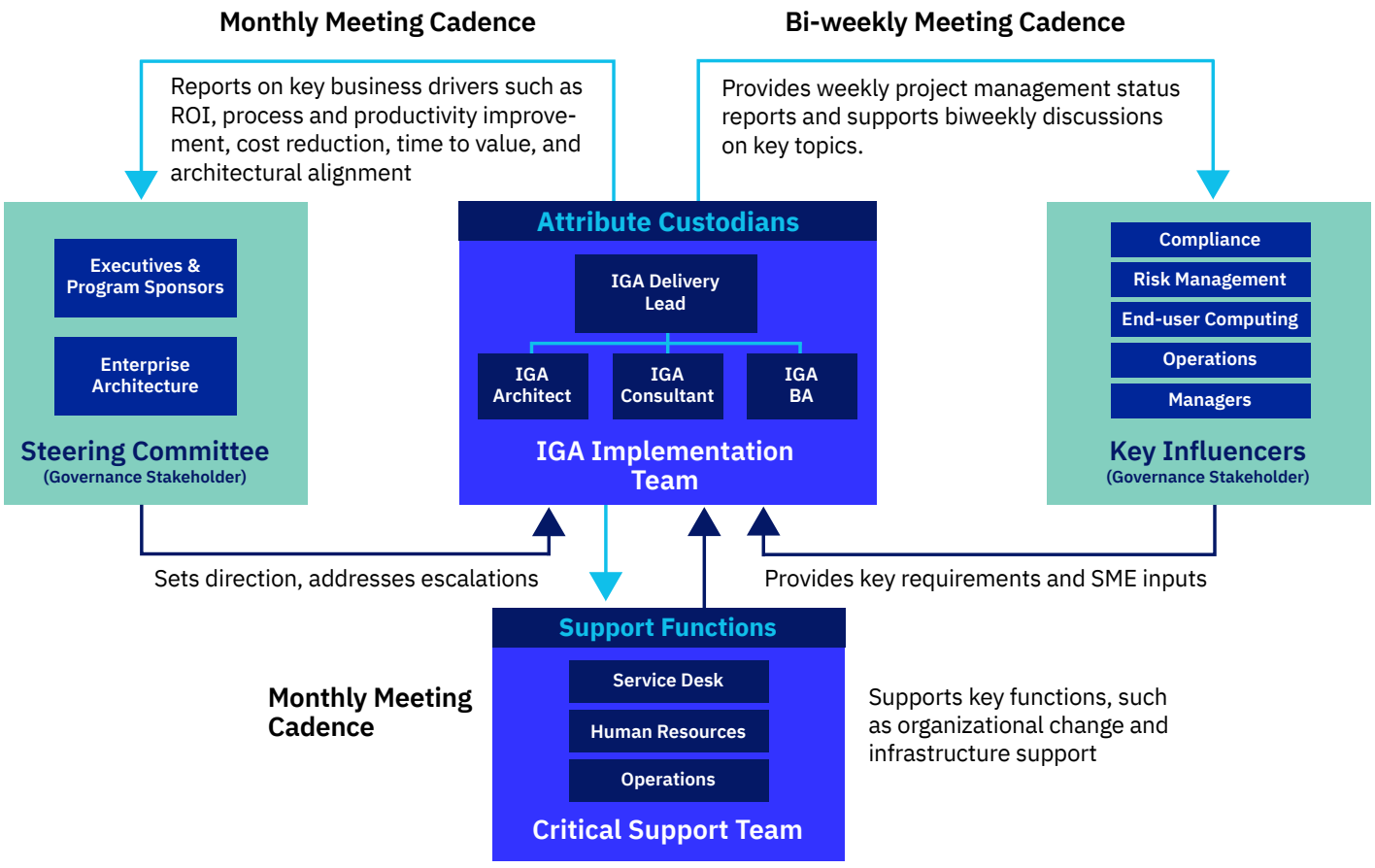
Using Attributes to Manage and Govern an IGA Program

Defining and operating within a structured governance framework is critical to running IGA. Once key attributes are defined based on input from each stakeholder, it is essential to put a governance framework in place. The governance framework:

- ✓ Supports the creation of an IGA capability across people, process, and technology to address each attribute.
- ✓ Helps creation of a prioritized plan for rolling out the functional capabilities to address each attribute.
- ✓ Identifies and defines the stakeholder categories.
- ✓ Puts processes in place for ongoing cadence with each stakeholder group, focusing on attributes of interest for various stakeholder groups during each cadence.

The governance framework shown below consists of two "governance stakeholder" groups that are composed of attribute-contributing stakeholders: the steering committee and key influencers. The IGA Implementation Team also acts as attribute custodians in the team is responsible for delivering those attributes to stakeholders. Each of these groups holds important responsibilities and interacts with each other at regular intervals. The IGA team engages with each stakeholder group to keep them informed on progress of the program as well as consult with them on key decisions.

IGA Governance Framework



STEERING COMMITTEE

The Steering Committee is composed of attribute-contributing stakeholder groups including the Executive & Program Sponsor and Enterprise Architecture. This committee sets the direction of the IGA team by assigning priorities to the overall plan. The steering committee also addresses any escalations from the IGA team and helps clear any roadblocks that can cause potential program delays. The committee can also allocate additional resources as required to meet key program goals. It is recommended to meet with the steering committee on a monthly cadence. Key attributes to focus on when reporting to the steering committee are ROI, process improvement, operational cost reduction, time to value, innovation and architectural alignment.

KEY INFLUENCERS

Key influencers are the remaining attribute-contributing stakeholder groups (Compliance, Risk Management, End-user Computing, Operations, and Managers) that are heavy users of the IGA solution or owners of those systems that IGA connects with. These groups provide key IGA process requirements and are critical to the overall success of the program. They also participate in program-level decision making that can have organization-wide impact. The recommended meeting cadence with the key influencers is biweekly. Critical attributes to focus on when meeting with key influencers include automation, policy enforcement, process standardization, evidence collection, reporting and analytics, and compliance.

CRITICAL SUPPORT TEAM

This support group includes HR, the service desk, organizational change management (OCM), and infrastructure support. HR plays an important support role in the program since they own the authoritative sources that seed identity data to the IGA system. OCM plays a critical role in communicating across the organization on the progress of a new program and working with various user groups to support training needs. OCM also guides the IGA team in creating training material for various user groups as well as the service desk to equip them to handle any user questions. The infrastructure teams also play a crucial role, especially when deploying IGA solutions on-premise as they support infrastructure on which IGA software runs. The recommended meeting cadence with these critical support functions is biweekly or as needed. When meeting with this stakeholder group, some key attributes to focus on include communication and training, availability, interoperability, and process standardization.

IGA IMPLEMENTATION TEAM

The typical IGA implementation team comprises the delivery lead, IGA architect, IGA consultant(s) and the IGA business analyst (BA). This team is the custodian of all the attributes, and is accountable for addressing all the attributes derived from business requirements based on the priority assigned to them. This group reports to the steering committee on key business drivers, such as ROI, process improvement, cost reduction, productivity improvement, time to value, and architectural alignment. They engage with the key influencers to provide updates on key attributes, such as compliance, user adoption, evidence collection, application integration, automation, policy enforcement. Meeting cadences are monthly or biweekly, depending on the governance stakeholder group.

Conclusion

In order to align IGA programs with business objectives, organizations that are rolling out IGA capabilities to automate business processes need to identify all the key attribute-contributing stakeholders early in the initiative to avoid last minute surprises and ensure full commitment and support across the organization. Defining requirements and deriving key stakeholder attributes and then using those attributes to design the IGA solution and align the program goals to the organization's business objectives are the most critical success factors. In addition, these attributes should also be used on an ongoing basis to measure the program's continued relevance to the business and to make necessary improvements on an ongoing basis.

By understanding the critical factors associated with identity governance and putting a framework in place to continually govern the program, organizations can mature their identity governance program and position it to support business objectives and deliver value on an ongoing basis.

ABOUT THE AUTHOR

Abhi Sarmah

Practice Director for Identity and Access Management

Abhi Sarmah leads the Identity and Access Management practice at GuidePoint Security. As the practice director, he is responsible for working with clients and recommending solutions that are the best fit for our client's business objectives. Mr. Sarmah has been focused on IAM for the last decade and has delivered strategy engagements as well as led the delivery of several IAM solutions for clients across various industries, including financial services, energy and utilities, retail and education. Mr. Sarmah is a Sherwood Applied Business Security Architecture (SABSA) certified security architect.

GUIDEPOINT
SECURITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132
05.2021