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 cybersecurity, 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.

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)
Reduction in operational cost	Accessible	Automated	Available	Assurable	Admissible	Extendable
Support for business growth	Accurate	Cost-effective	Inter-operable	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						

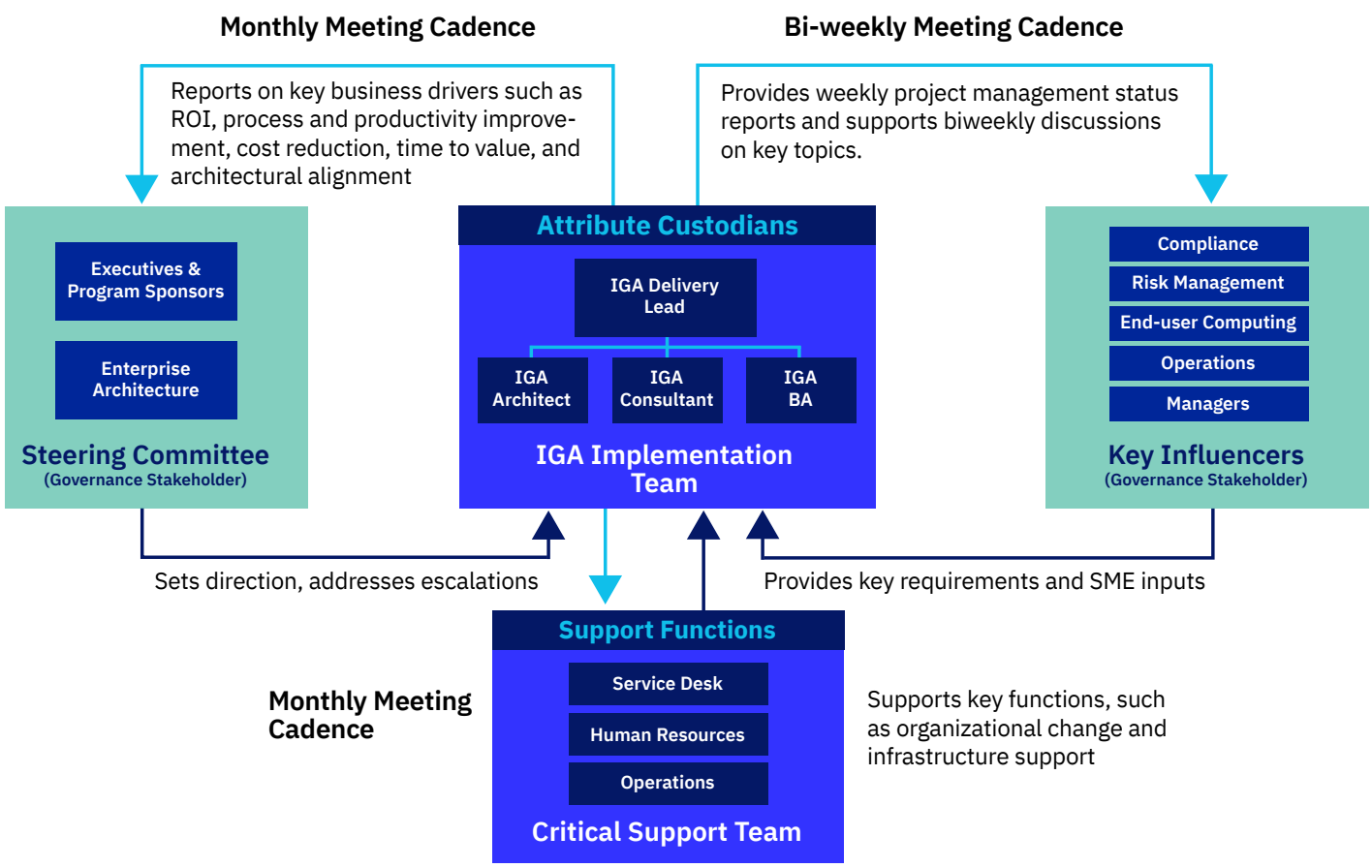
Using Attributes to Manage and Govern an IGA Program

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

This committee, composed of attribute contributing stakeholders (Executive & Program Sponsor, Enterprise Architecture), 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. Additionally, the committee can allocate 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.

IGA IMPLEMENTATION TEAM

This team, comprised of the delivery lead, IGA architect, IGA consultant(s) and the IGA business analyst (BA), 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.

KEY INFLUENCERS

Compliance, Risk Management, End-user Computing, Operations, and Managers 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 owns the authoritative sources that seed identity data to the IGA system. OCM communicates across the organization on the progress of a new program and works with various user groups to support training needs. OCM also guides the IGA team in creating training material for groups such as the service desk to equip them to handle user questions. The infrastructure teams must support infrastructure on which IGA software runs. The recommended meeting cadence with these critical support functions is biweekly or as needed. Key attributes to focus on include communication and training, availability, interoperability, and process standardization.

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.

GUIDEPOINT®

SECURITY

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