GoodDogLabs.
A SPYGLASS COMPANY.

IGA – A Foundational Approach

New, modern IAM solutions have emerged to meet the demand for next-generation IAM capabilities. Legacy solutions have failed to keep up and have even fell short of their original promise. Organizations must avoid these aging solutions and embrace the future – platforms with modern architectures and sophisticated features necessary to manage the increasing complexity and risk profile of today's digital identity and access management landscape.

GoodDogLabs.
A SPYGLASS COMPANY.

IGA – A Foundational Approach

IGA is a dynamic ecosystem

Identity Governance and Administration (IGA) isn't accomplished with a single solution which has clear boundaries and that, once implemented, leaves you with the feeling of 'one and done'. As revealed in the journey through an organization's IGA program, IGA entails a broad and diverse ecosystem of interdependent systems with a reach throughout the enterprise. And the ecosystem never reaches stasis. It changes, as they say, "at the speed of business" and at the speed of technological change, both of which wait for no one.

Not only does change not wait, it happens fast. From the last few years alone, examples include major areas like the cloud, mobile, shadow IT, digital commerce (B2C), the expansion of hosted applications (B2B), and IoT. When you consider that IoT is only just unfolding, and the current rapid adoption of modern paradigms such as DevOps, it's easy to see that change isn't slowing down. All these dramatically broaden the challenges and scope of what IT organizations must successfully manage.

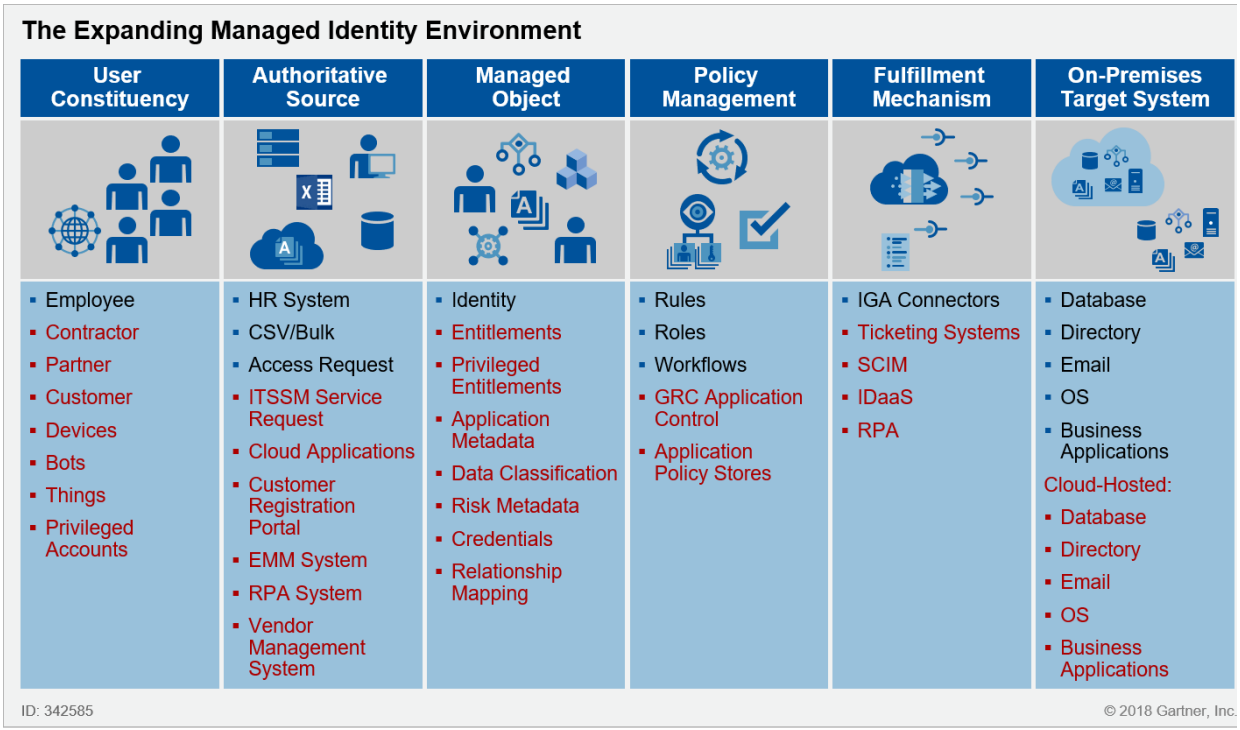
But the change goes beyond the technologies or systems and platforms. These in turn drive much more complexity into the data and its relationships, as well as the decisions which an IGA program must manage. The parallel discipline of Cybersecurity must also be considered. Consequently, IGA solutions are under pressure to quickly meet new demands for advanced features. These include support for complex data models, advanced analytics and AI, orchestrated integration with Cybersecurity systems, and centralized governance of distributed digital identity events.

Overall, there's a pressing need for new, modern IGA solutions that provide a broader, more sophisticated platform and a more flexible architecture than the classic IGA solutions to date.

> *IGA systems are aging poorly as deployments struggle to meet new digital business demands. Technical professionals responsible for IAM must rethink their IGA architecture and adopt next-generation technologies that support cloud, mobile, DevOps, AI, analytics and cybersecurity initiatives. (Gartner, Identity Next: Rethinking Identity Governance and Administration)*

Figure 1 is Gartner's sampling of the expanding demands facing an IGA program. The items in red have emerged in only recent years. We believe that this clearly demonstrates the changing nature of the IGA ecosystem and the need for an advanced IGA platform that can change with it.

Figure 1. The Expanding Identity Environment



CSV = comma-separated values; EMM = enterprise mobile management; GRC = governance, risk and compliance; IDaaS = identity and access management as a service; ITSSM = IT
service and support management; RPA = robotic process automation; SCIM = System for Cross-domain Identity Management

Source: (Gartner, Identity Next: Rethinking Identity Governance and Administration)

IGA Foundation – the interchange of digital identity data

Organizations must first respect that the essential aspect of today's IGA ecosystem is the interchange of digital identity data. This must occur between systems wherever they reside, and whether they source the data, consume the data, manage the data, or manage the digital identities themselves. The process and data must be adaptable to the diversity of systems, increasing complexity of the data, your business requirements, and inevitable change. It goes without saying that the data must be clean and reliable.

It can't be overstated how foundational this aspect of the IGA ecosystem is - and that therefore it must be the foundation of an IGA program.

Traditionally, user access provisioning has been the essential objective of an IGA program. But as shown in the 'Fullfillment Mechanism' column of Figure 1, we feel that other systems are playing a role in that function. For example, IDaaS systems can now be expected to provision to SaaS applications. ITSM systems are used for managing access requests and fulfillment. RPA may become widely used for automating manual provisioning tasks. As demands increase for IGA programs to meet other pressing needs, provisioning is giving way as the essential element.

Governance is now the primary objective of an IGA program. "As discussed in the document, "IGA Best Practices: Governance First, Automated Provisioning Later," you should prioritize governance-related capabilities over automated provisioning when planning for IGA deployment" (Gartner, Identity Next: Rethinking Identity Governance and Administration). Several capabilities already mentioned are centralized governance of distributed digital identity events, advanced analytics, orchestration with the Cybersecurity landscape, etc. The common, essential element enabling all these functions is the data – the digital identity data. It's not just reliable and effective communication that is necessary. The ability to manage the increasingly complex data models is also a necessity. Together, these are the foundational capabilities of today's modern IGA program..

The challenge for legacy IGA solutions

These important truths about the nature of IGA – that it's an evolving ecosystem reliant on the reliable interchange of clean and accurate digital identity data – hasn't been adequately appreciated in the past, at least not by IGA vendors or consultants. Or if it was, it wasn't addressed in their products, nor did they counsel their customers accordingly.

The discrete and monolithic IGA approaches of the past have only limited reach within and across computing environments. Their data integrations are static and solution-specific. Beyond provisioning user access, they are only an endpoint for the data. They'll never be the means to manage and distribute the data further. I could cite several reasons why, but above all, that's not the business they are in. Basically, regarding the interchange of digital identity data, legacy IGA solutions are just an endpoint, and for only a subset of data.

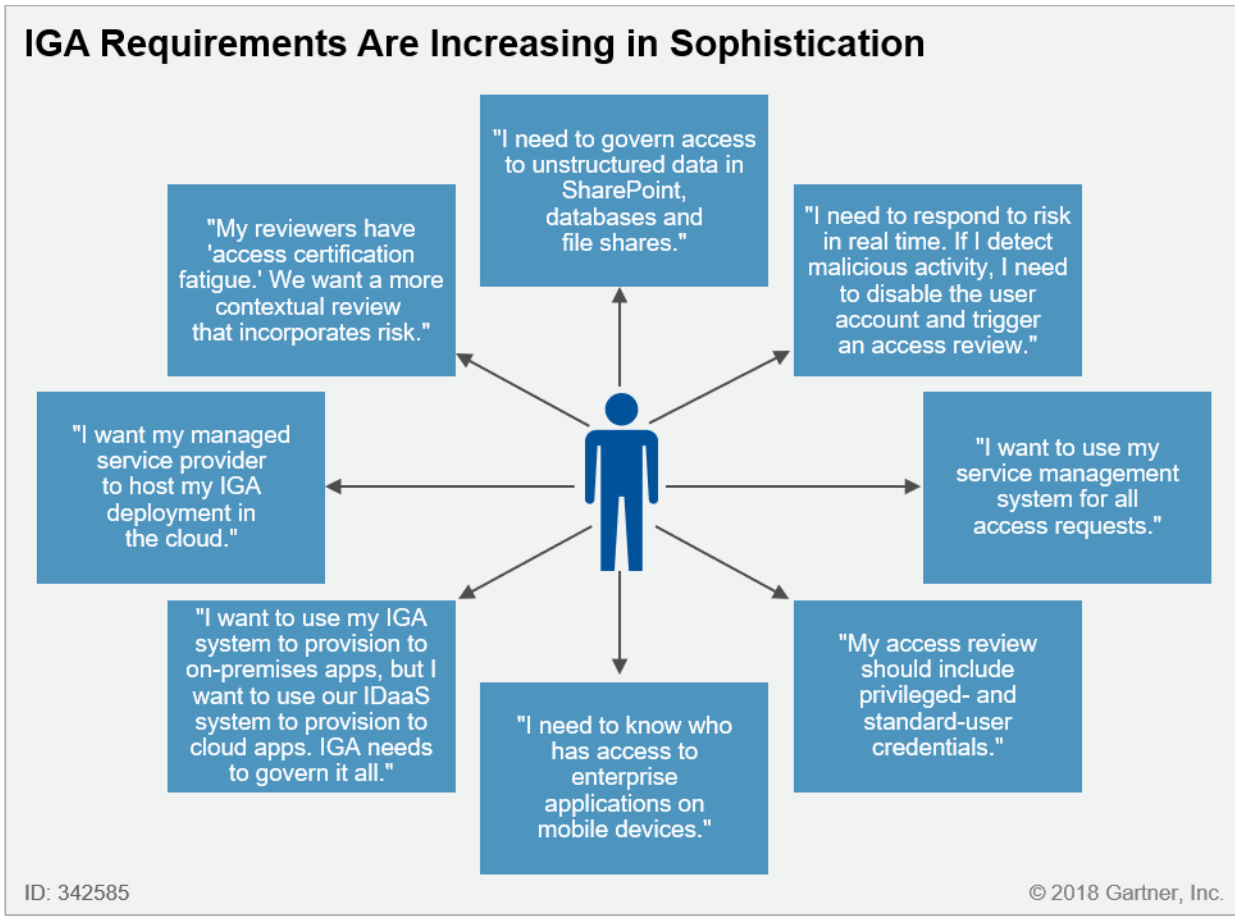
The consequences of their failings can't be more meaningfully demonstrated than by the fact that, as Gartner reports, they are observing an increase in re-implementations. "Today, most IAM implementations are re-implementations"…"63 percent of organizations surveyed plan to re-implement at least one IAM module in the next two years" (Gartner, Best Practices for IAM Reimplementations). "Sixty-three percent of organizations surveyed plan to reimplement at least one IAM module in the next two years." (Gartner, Best Practices for IAM Reimplementations, Figure 1. IAM Technologies Planned to be Repaced in the Next Two Years). What a stunning reversal, given that their IGA programs were likely very expensive and major undertakings. To pull the plug so soon speaks terribly of the industry's legacy solutions and their promise of ROI.

> *In a recent Gartner IAM survey, 63% of participants stated that their organizations plan to upgrade at least one IAM module in the next two years. The most common reason is that their existing IAM solution doesn't address their known requirements. (Gartner, Best Practices for IAM Reimplementations)*

> *Numerous IGA deployments underperform or have altogether failed. Gartner estimates that 50% of deployments are in distress. (Gartner, Identity Next: Rethinking Identity Governance and Administration)*

Figure 2 is Gartner's sampling of modern use-case requirements that Gartner hears from clients. in our view, legacy IGA solutions fail to adequately meet emerging needs.

Figure 2. IGA requirements are increasing in sophistication.



Source: (Gartner, Identity Next: Rethinking Identity Governance and Administration

> *Despite the addition of new features and functions, many first- and second-generation IGA systems (aka classic IGA systems) are cracking under the pressure of digital business use cases. Classic IGA systems are rigid, proprietary and built on a monolithic architecture that does not scale to meet digital business demands…*
> *(Gartner, Identity Next: Rethinking Identity Governance and Administration)*

Today's new microservice architectures

Sometimes things happen around us which disrupt the status quo but which we don't need to react to immediately. Nevertheless, change can't be held back, and we eventually change with it. I'm not going to suggest that the answers to today's IGA challenges lie in the cloud - that would be too simple, and by now, cliché. However, cloud computing has ushered in great new technologies and architectures which are applicable to all environments, on-premise included and where they're being rapidly adopted.

I'm specifically referring to the new *modern* application architecture consisting of lightweight and containerized, feature-specific microservices that communicate via REST APIs. This lightweight,

composable, and fully distributable architecture is eminently suited to the broader dynamic IGA ecosystems of today whether on-premise, hybrid-cloud, or multi-cloud.

These technologies are disrupting the status quo and IGA programs must embrace the change. Static, inflexible and monolithic approaches must be avoided.

> *Modernize the IGA architecture. Adopt a service-based architecture that modularizes identity services for flexibility, scale and elasticity; supports complex data models; and provides REST APIs for tight integration with external systems. (Gartner, Identity Next: Rethinking Identity Governance and Administration)*

Perseus IAM - The IAM Services Layer

By now it's clear – a successful IGA program must be modernized. This requires a data interchange layer to provide clean, adaptable, and managed digital identity data as a foundational component of your IGA ecosystem. It must reach all computing environments. It must support complex data models. The architecture must be modular and service-based, achieved through an agile and flexible microservices architecture.

That solution exists today. **Perseus IAM** from **Good Dog Labs, a Spyglass Company**, establishes secure, repeatable IAM data pipelines within an IAM Services Layer. The IAM Services Layer centrally manages the movement and form of all your digital identity data throughout the IGA ecosystem.

What follows are a few brief, high level descriptions of several of Perseus IAM's features. For a complete and detailed description of all its capabilities, technologies and architecture, please see the Perseus IAM Architectural Overview.

Perseus IAM – Complex Data Models

Earlier, we highlighted the modern application architecture of Perseus IAM that perfectly suits the challenges of the IGA ecosystem. Another very significant IGA challenge addressed by advancing technology is the ever-more complex and dynamic data representing a digital identity. The relationships and use cases are getting more complex and can change at any time as they change in the realm of IAM. And the scale is exploding due to the cloud and IoT, to cite two examples. Today's reality is that digital identity is everywhere.

Traditional approaches based on fixed schemas just won't work.

Perseus IAM utilizes advanced technology to solve the problems of data complexity, flexibility and scale. It has a highly flexible JSON-based data model suited for complex data. The model can change easily and scales across the IAM landscape. And it is format-neutral, allowing it to map data at runtime to any consumer such as an IGA or PIM/PAM system.

Perseus IAM - The IAM Identity Hub

Perseus IAM provides an enterprise-class Identity Hub. Each digital identity transiting the pipelines is loaded into the Identity Hub where the data is mastered. The Identity Hub is thus a global repository of

digital identities and their relationships including accounts, roles, entitlements, organizations, devices, and so on.

Perseus IAM - Managing the Data

Perseus IAM provides all the features needed for managing the data itself. It will correlate, transform, normalize and filter digital identity data in relation to any system, application, and device from which it is sourced to meet the data needs and business requirements of any system where it's consumed.

But, most critical of all, is that the data be clean and accurate. The ability of Perseus IAM to manage the data is greatly enhanced by its ability to filter the data and provide real-time alerts when the data is not of sufficient quality. It also provides real-time views into data quality and errors and ongoing data quality analytics.

Perseus IAM – The Data Pipelines

Perseus IAM gives you the ability to establish and centrally manage IAM data pipelines that are reliable, real-time, repeatable and reusable. And above all, they are secure. Any ingress, secure and fully configurable, can be leveraged for any egress, also secure and fully configurable.

Perseus IAM – Beyond IGA

Perseus IAM is a highly performant enterprise-class IAM platform. Beyond IGA, it's capable of integrating into all realms of IAM to manage digital identity data including IoT, Mobile, BYOD, IDaaS, SSO, AuthNZ, etc. Moreover, it can bridge the gap between IAM and real-time cybersecurity alerting from threat response systems (e.g., SIEM), providing a connected IGA-IAM-Cybersecurity Layer.

To learn more about Perseus IAM and the future of IGA, IAM and Cybersecurity, please see https://www.perseusiam.com.

Works Cited

Gartner, Identity Net: Rethinking Identity Governance and Administration, Lori Robinson, 26 March 2018.

Gartner, Best Practices for IAM Reimplementations, Mary Ruddy, Refreshed: 7 August 2018, Published on 17 April 2017.

Contact Good Dog Labs

Contact Good Dog Labs for more information on Perseus IAM.

Email: sales@gooddoglabs.com
Web Site: www.perseusiam.com

Good Dog Labs, LLC
6 Blackstone Valley Pl #205
Lincoln RI 02865

Good Dog Labs, LLC
801 Barton Springs Rd
Austin TX 78704

Authors:
Dino Pietropaolo, Chief Technical Officer & Co-Founder
dino@gooddoglabs.com

Aldo Pietropaolo, Chief Executive & Co-Founder
aldo@gooddoglabs.com

Good Dog Labs, LLC.