SAVIYNT FOR NTT DATA
Digital Trusted Identity Service – Identity Governance Administration (IGA)

NTT DATA's IGA services are designed to:

- Limit and guard access to sensitive data to reduce the risk of exposure
- Provide a seamless provisioning process with continuous automation
- Enable efficient on-boarding and off-boarding processes
- Streamline the joiner, mover, and leaver process
- Ensure adequate segregation of duties (SOD) across enterprise applications
- Decrease manager/certifier fatigue
- Prepare for cloud readiness (public, private, and hybrid)

NTT DATA
https://us.nttdata.com/en/digital/security-services/

security.sales@nttdata.com

Secure Your Business Against Cyberattacks

Today, all enterprise business and customer data are a target. Users and resources are no longer hidden securely within the perimeter or safely inside the data center. Employees work from home, field offices, client locations or anywhere there is an internet connection, and access internal resources while doing so.

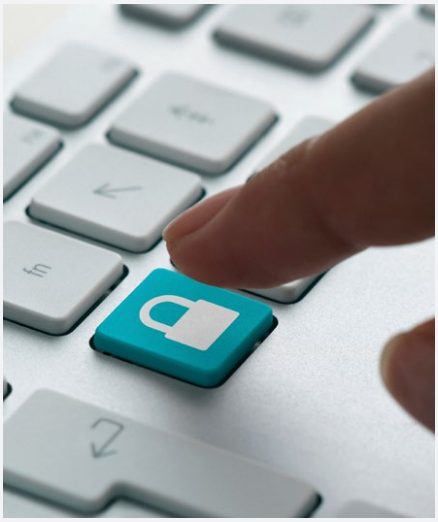
The key trends and critical considerations that go into assessing the need for a robust IGA strategy include:

- **Remote work:** Remote working has resulted in the demise of traditional security measures, accelerating the need for a Zero Trust approach
- **Complex infrastructure:** Managing complex infrastructure, including hybrid cloud, on-premises, and public cloud services platforms, is becoming the norm
- **Constantly changing user base:** Managing the security and privacy of those joining, moving within, and leaving the organization comes with its own set of challenges
- **Regulations and compliance:** Increasing regulations that impact identity governance can be daunting and financially devastating
- **Authentication:** Ineffective passwords and knowledge-based authentication need to be revisited

NTT DATA's Advisory, Implementation and Managed Services for IGA are designed to bring together users, applications, and technology and make it work for your business, yielding the following benefits:

- Continuous controls monitoring to avoid policy violation
- Intelligent access request and review to ensure permissions are secure and appropriate
- Application SOD management to prevent error and fraud, as well as meet compliance requirements
- Role, privilege, and policy design management for seamless access management

SAVIYNT MODERN IGA FOR DIGITAL TRANSFORMATION



Intelligent Identity. Smarter Security.

Saviynt starts with people and their access. Our cloud-native IGA solution enables full visibility into how and where users interact with data.

FedRAMP Authority-to-Operate (ATO) status ensures customers that we provide a secure vendor solution.

- **On Cloud**
- **Hybrid**
- **On-premise**

SAVIYNT, INC.
Headquarters
1301 E. El Segundo Bl, Suite D,
El Segundo, CA 90245
United States
310. 641. 1664 | info@saviynt.com

Four steps to ease IGA for Digital Business Models

Creating a modernized IT infrastructure that aligns with current and future business operations means merging cloud, hybrid, and on- premise infrastructures. While digital business models increase business agility and ease business operations, they often increase risk by amplifying the number of access points.

Managing digital, workforce and consumer identities across the modernized digital ecosystem requires modern identity governance and administration (IGA) solutions. To help ease your IGA transformation, consider these four steps.

IDENTIFY OBJECTIVES

Security and compliance starts with identification, and so must a solid IT modernization strategy. To identify risks and align them with business operation goals, organizations need to ask themselves:

- What are the corporate goals?
- What application tools can best meet these goals?
- Who are the users?

REVIEW THE RISKS

Maintaining data integrity requires controlling data access and use. The primary security barrier to IT modernization is the inability to mitigate risks for interconnected cloud-based apps using current legacy solutions. Complex apps create additional entry points requiring monitoring. Legacy solutions cannot manage interconnected apps, leading to individual identity solutions for each app and location. Isolated identity solutions often fail to maintain internal controls.

MITIGATE RISKS

Coarse grained definitions of identities and roles lead to security and compliance gaps. IGA links a user to the application, role and object needed and allows for more in-depth risk analysis, granular identification of SoD risks, and improved compliance.

AUTOMATE AND INFUSE INTELLIGENCE

New access requests for human or digital identities make the compliance requirement for continuous monitoring burdensome. An updated IT ecosystem requires intelligent analytics tools that provide real-time analysis and have the ability to automatically remediate or accept the requests.

About Saviynt

Our vision is to redefine IGA by converging traditional Identity Management with Cloud Security, PAM and Application GRC capabilities. In doing this, Saviynt enables enterprises to secure applications, data and infrastructure in a single platform for cloud and enterprise.

saviynt.com