Digital Identity and Access Management Advisory

Ensuring trusted identities in a connected and open world

CGI

Today's organizations require agility and innovation to deliver seamless digital experiences—anytime, anywhere. In response, customer, employee and supplier ecosystems have become more complex, connected and open. At the same time, cyber threats and risks are growing in velocity and complexity.

With more digital and connected ecosystems, along with the rise of remote working and the gig economy, the volume, velocity and variety of digital identities (both human and non-human) to manage is rising exponentially.

How can you continue to drive agility and innovate at pace while securing access by digital identities to critical information?

Securing today's digital realities

Enterprises are continuously evolving to deliver value to customers, citizens, employees and shareholders at pace in response to fast-changing needs.

New technologies, data sources and connections are enabling this evolution, including multi-cloud environments, edge computing, automation, artificial intelligence (AI), Internet of Things, 5G, micro-services, devices, and application programming interfaces (APIs). However, cyber threat actors are harnessing these same advances to create an increasingly sophisticated and dynamic risk landscape. The cybersecurity arms race is escalating.

Enterprises also are expanding their supplier ecosystems and customer bases. Many are involved in mergers, acquisitions, divestitures and reorganizations, and have increasingly hybrid workforces (human and non-human) operating from almost anywhere.

At the same time, greater volumes and types of data can be accessed more easily (e.g., via the cloud and edge computing). Enterprises are using this data to "train" AI solutions, automate decisions, control robots and co-bots, and optimize human experiences. Stricter data protection and privacy regulations are increasing across the globe. Non-compliance or a breach can have devastating reputational and financial effects.

As data and technologies become more widely distributed and connected, trusted physical security perimeters are disappearing, and enterprises are transitioning to a zero-trust security model. In addition, the "as a service" trend is forcing organizations to change how they purchase, operate, monitor, control and decommission IT.

79%
of organizations have experienced an identity-related security breach in the last two years, and …

99%
believe their identity-related breaches were preventable.
Source: IDSA

78%
say their organization uses some form of cloud; 65% say securing cloud platforms is a key cybersecurity priority for their organization.

20%
are currently implementing or have completed algorithmic automation implementations (driven by advanced analytics, including machine learning).

Source: 2021 CGI Voice of Our Clients

Achieving the right balance with an insights-led approach

By staying abreast of rapidly changing technologies, ecosystems and threats, our consultants are ready to help you achieve the right balance of connectivity, agility and risk measures, so you can be sure the right access is given to the right identity at the right time.

- **Enable innovation and collaboration at pace:** Secure and seamless access is imperative to improving agility, time to market and customer and employee experiences.

- **Reduce risk exposure:** An effective digital IAM approach minimizes exposure to new risks by considering the complex hybrid environment holistically, along with the human and non-human identities that require access to critical information

- **Improve regulatory compliance:** Data is everywhere and is fueling innovation, new revenue opportunities, better user experiences, and optimized operations. Ensuring the right access to this data is critical to complying with increasingly strict regulations.
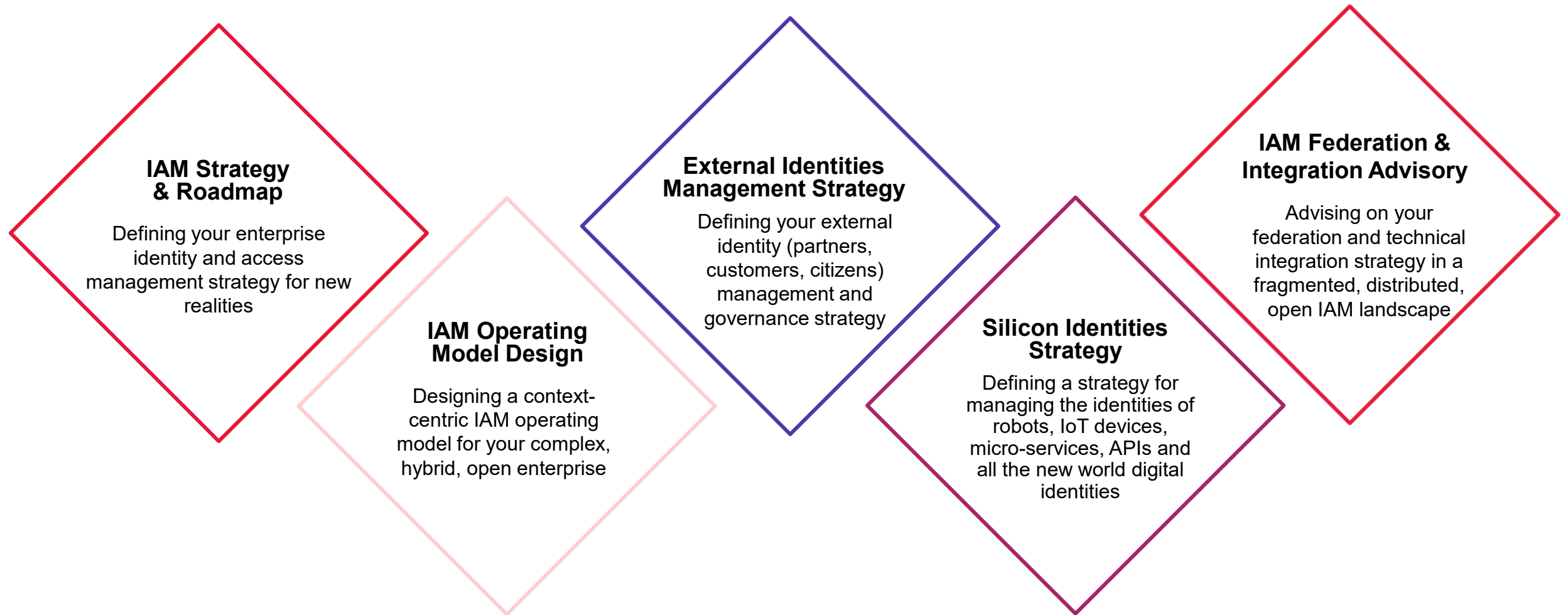

With CGI's Digital Identity and Access Management (IAM) Advisory Services, you can secure access for digital identities while driving the agility and innovation you need to optimize operations, improve the user experience, and speed up time to market.

What does an effective digital IAM deliver ?

- **Employees:** When an employee or contractor joins the organization, or when they work remotely, they quickly access the right information and systems at the right time and for the right reasons. When their context changes, their access is updated.

- **Customers:** Customers access services securely in a seamless experience.

- **Supplier ecosystem:** Enterprise systems are interoperable with partners in a secure fashion.

- **Non-human identities:** Software robots from automations, third-party APIs, microservices and IoT devices securely access the right data and systems at the right time, and for the right reasons.

- **Enterprise:** IAM in a hybrid environment is managed holistically, with a clear governance and operating model, in compliance with regulations, and truly enables the digital organization.

CGI Digital IAM Advisory Services

IAM Strategy & Roadmap

Defining your enterprise identity and access management strategy for new realities

IAM Operating Model Design

Designing a context-centric IAM operating model for your complex, hybrid, open enterprise

External Identities Management Strategy

Defining your external identity (partners, customers, citizens) management and governance strategy

Silicon Identities Strategy

Defining a strategy for managing the identities of robots, IoT devices, micro-services, APIs and all the new world digital identities

IAM Federation & Integration Advisory

Advising on your federation and technical integration strategy in a fragmented, distributed, open IAM landscape

5

01 IAM Strategy & Roadmap

We work with you to develop a tailored IAM strategy and roadmap of key initiatives tied to measurable business value. We use our unique maturity model, based on ISO 27001 / 27002, to assess your current IAM strategy in the following areas: governance, policies, processes, including lifecycle management, organizational entities and identity types, access control model service desk, information classifications, and IAM technologies and vendors.

In this service, we also cover all aspects of identity and governance administration (IGA), privileged access management, and access control. We examine your current environment and jointly formulate your ambition for a modern digital IAM approach that enables you to define and enforce IAM policy and connect IAM functions for compliance purposes.

02 IAM Operating Model Design

Successful IAM programs often require a new IAM Operating Model to operationalize governance with updated processes and tooling. By analyzing your current state of IAM-related processes, policies, roles, authorization, contexts, devices, microservices and tooling, we help you design a new IAM operating model using our blueprints to support your transition towards a zero trust model. This includes considering the digital identities of humans as well as robots, IoT devices, microservices and APIs—in a multi-cloud environment.

03 External Identities Management Strategy

Organizations traditionally have focused internally, securing the identity and access (authentication and authorization) of employees. In today's open and connected ecosystems, an equal focus is needed for external parties, including customers (B2B or B2C), citizens, suppliers and partners. We use our proven methodology to help your organization define an external IAM strategy.

6

04 Silicon Identities Strategy

Today's hybrid work and operating environments reflect humans, machines and software coexisting and collaborating together. Non-human, silicon identities (e.g., software robots, IoT devices and sensors, APIs, microservices, and AI workloads) need managing. Through our advisory services, we help you take systematic control of all of your digital identities and their access.

05 IAM Federation & Integration Advisory

Different types of identities often are managed by different systems or even organizations. Assets to be accessed are distributed and sometimes controlled by third parties (e.g., partners, government agencies, cloud providers, etc.). This fragmentation requires a careful federation and technical integration strategy.
Our experts help you define your IAM Federation and Integration Strategy and Blueprint by analyzing your wider ecosystem, connections, and flow of services and information. This includes levels of assurance, regulatory and security requirements, policies, controls, identity providers, authentication and authorization protocols and frameworks.

Case in point

Serving as access control broker for 10+ million industrial IoT digital assets for an industry-wide service

For a large nationwide program involving the rollout of millions of industrial IoT digital assets, CGI designed, built, implemented, hosted, ran and supported the data services that lie at the heart of this program.

Our IAM advisory services, along with security services enable companies to access information to improve their services and customer experiences. These IAM services are crucial to the maintenance of consumer confidence which underpins the nationwide program and rollout.

Our solution provides a high-availability, high-resilience communication service in accordance with specifications and provides an access control function that cryptographically validates all access requests and verifies right of access against IoT registration data.

It also includes an industry-wide federated identity provider (IDP) service, enforcing federated two-factor authentication for employees of industry parties, roles and privilege assertion using SAML, and self-service management by industry party administrators. We also use this IDP service to control third-party access to industry service management systems.

In addition, the IDP service also includes effective management of privileged staff, management of risk in accordance with ISO 27005 and delivery of associated security services.

Case in point

Developing a long-term IAM strategy for a European energy company

Our clients' long-term strategic plan identified partnership and the integration of business processes among internal and external actors as a key component of their plan.

Tackling this initiative required an overall target view on how internal and external actors could get access to information, services and resources within the company.

To begin, CGI scoped an IAM assessment and strategy to focus on external actors – customers, employees (acting as customers), suppliers, and partnerships. We then identified requirements and produced a roadmap on how the client should move forward in its work with access and access rights.

We identified business requirements for access solutions, identified functional requirements on services providing access, the target architecture to strive for. We then provided a proposal of roadmap to reach defined targets for management of external access and access rights.

.

Based on 45 years of experience in building, integrating and managing cybersecurity solutions, our advisory services take a holistic view toward designing and engineering effective digital IAM solutions.

Proven IAM experience

Our proven methodology for advanced IAM concepts is designed to handle internal and external identities for complex organizations.

Our expertise includes:

- Securing entire digital societies

- Serving as access control broker for 10+ million Industrial IoT digital assets for an industry-wide service

- Co-designing, staffing (25+ cybersecurity and IAM experts), and operating a large organization's IAM competency center, supporting key projects and ongoing operations

- Providing certificate services and securing all connected cars for a major European luxury car manufacturer

- Being one of the very early adopters and providers of IAM "as a service"

CGI's Cybersecurity Advisory Services

CGI's Digital IAM Advisory Services are part of our suite of Cybersecurity Advisory Services designed to help you achieve your business goals through a holistic and balanced approach. In addition to improving IAM, we offer guidance for protecting the enterprise in a multi-cloud environment and safeguarding operations during AI-driven automation, as examples.

We stand ready to help secure your identities and your organization.

Contact us at info@cgi.com or learn more at cgi.com/cybersecurity

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world. We are insights-driven and outcomes-based to help accelerate returns on your investments. Across 21 industry sectors in 400 locations worldwide, our 77,000 professionals provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally. For more information

Visit cgi.com

Email us at info@cgi.com