Security and the digital enterprise

Secure methods for implementing digital technologies that drive business transformation.

An Advisory Services PoV

The cyber threat

As a society that continues to grow and evolve its online presence, we are experiencing a larger, more sophisticated cyber security threat than ever before.

Cyber criminals exploit vulnerabilities in IT and our interaction with it, commercialising on the new emerging technologies that we embrace. Specifically, organisations are increasingly adopting all things "digital" to reap many benefits, including remaining competitive, cutting costs, improving performance and user satisfaction, supporting new business models and gaining new revenue sources.

One key trend in this digital transformation is a move to the cloud, with many organisations adopting a cloud-first strategy for new projects. This change may be necessary, but as we adopt the unfamiliar and adapt to the new, there are potential risks. Cloud adoption for example, brings new technologies, new ways of doing things, changing responsibilities, increasing reliance on others and an extended attack surface.

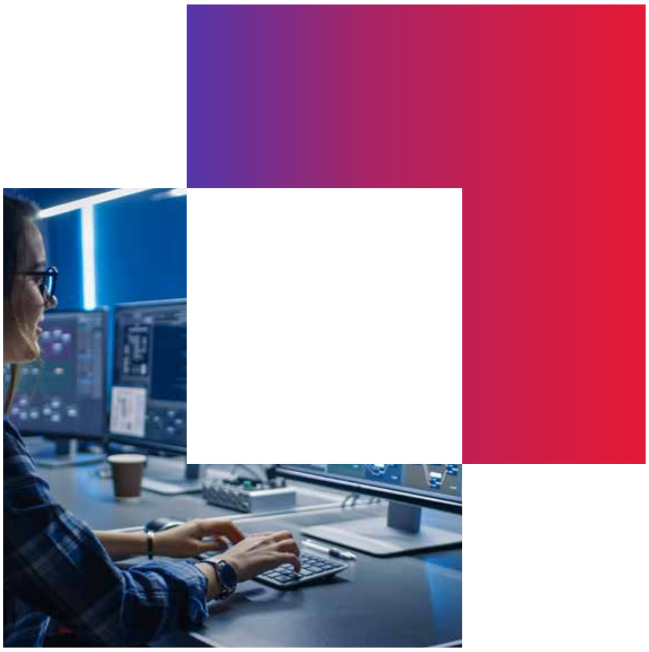
There is also a proliferation of services and data held within and transferred between organisations. This, combined with more users working from home than ever before, means that organisations now have more to defend as they become increasingly vulnerable to attacks. This is especially the case as cyber criminals continue to exploit users to facilitate attacks, using social engineering and other methods of manipulation or coercion.

Cyber security has therefore never been more challenging or important. It plays a central role in continued operations, ensuring regulatory compliance, protecting against intellectual property loss and the reputational damage associated with data breaches, and most critically it builds confidence and trust in those very new capabilities that empower businesses and society.

Assessing the risk

From security threats to business opportunities

CGI takes a risk-based approach to digital transformation. We ensure that your organisation's risk posture is not negatively impacted by change, with robust, digitally enabled and proportional controls that support secure operations, maintain critical service uptime and instil confidence in your new digital services.



Assess the risk

Risks, threats and vulnerabilities assessments, security training and awareness.

Protect the business

Cyber security and digital transformation, cloud security and identity management solutions, security consulting.

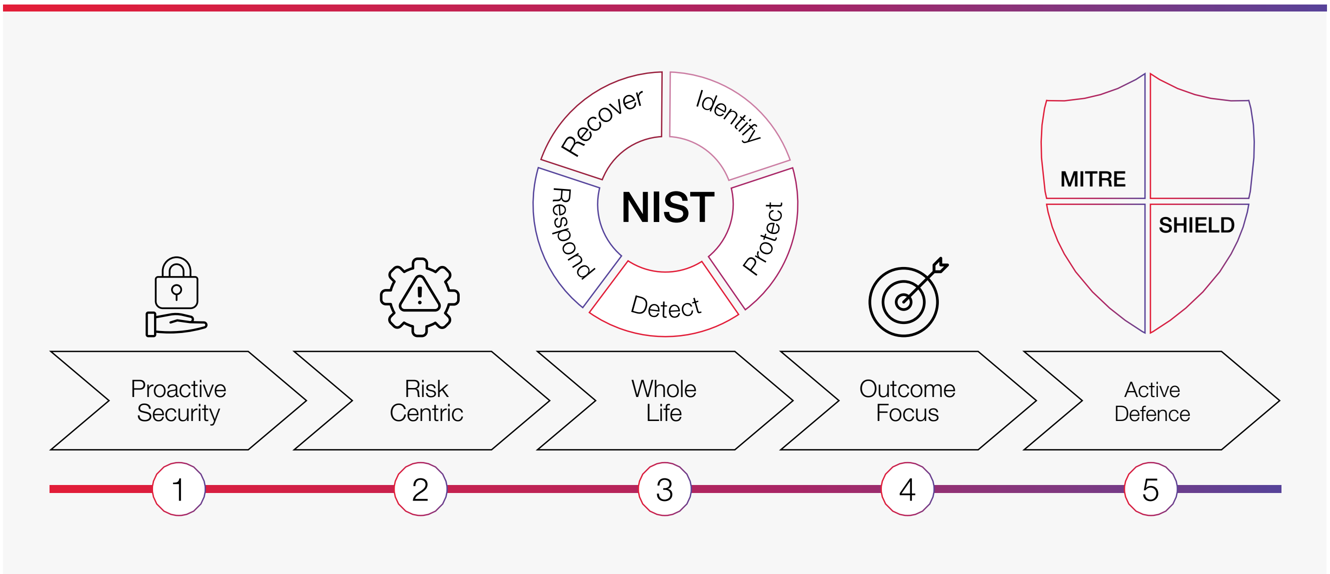
Operate with confidence

Ongoing threat monitoring and risk management, managed security services, incident detections and response.

Risk mitigation and best practices

Risk management has evolved from an initial focus on the identification and deployment of preventative controls, to a lifecycle model with increasing emphasis on attack detection and response. This is because effective risk management considers threats throughout the lifecycle, providing overlaid, in-depth controls across all functions to mitigate risk and provide defence. A good example of this is the NIST Cyber Security Framework's (CSF) identify, protect, detect, respond and recover functions. These form the basis of the CGI "cyber wheel", which we use to define our services and capabilities.

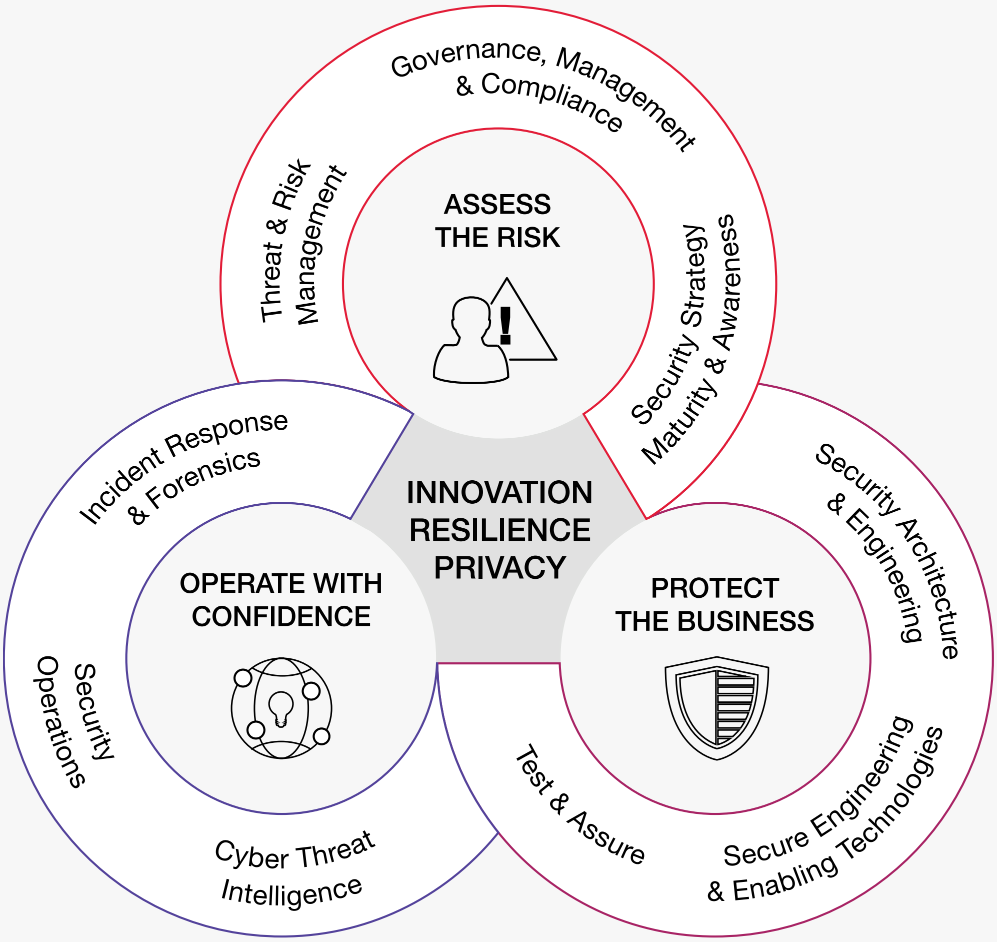
The MITRE (Shield) and NIST (Tier 4 Adaptive) frameworks also adopt active defence postures. This approach extends military concepts of sowing doubt and confusion in the enemy (in this case, cyber criminals) to disrupt, distract and contain their actions whilst learning about their capabilities and motivations. The aim is to change the dynamics of cyber security, forcing attackers to become defensive whilst increasing their cost of operations and minimising their ability to achieve value. By learning about attacker capabilities and motivations, we can thereby change the cost benefit of conducting an attack, whether it be financial (organised crime), reputational (script kiddies) or indirect damage.



Empowering digital transformation

To enable digitalisation, trust and confidence is essential. This comes from demonstrating robust cyber security best practices that are subject to independent scrutiny and oversight throughout delivery.

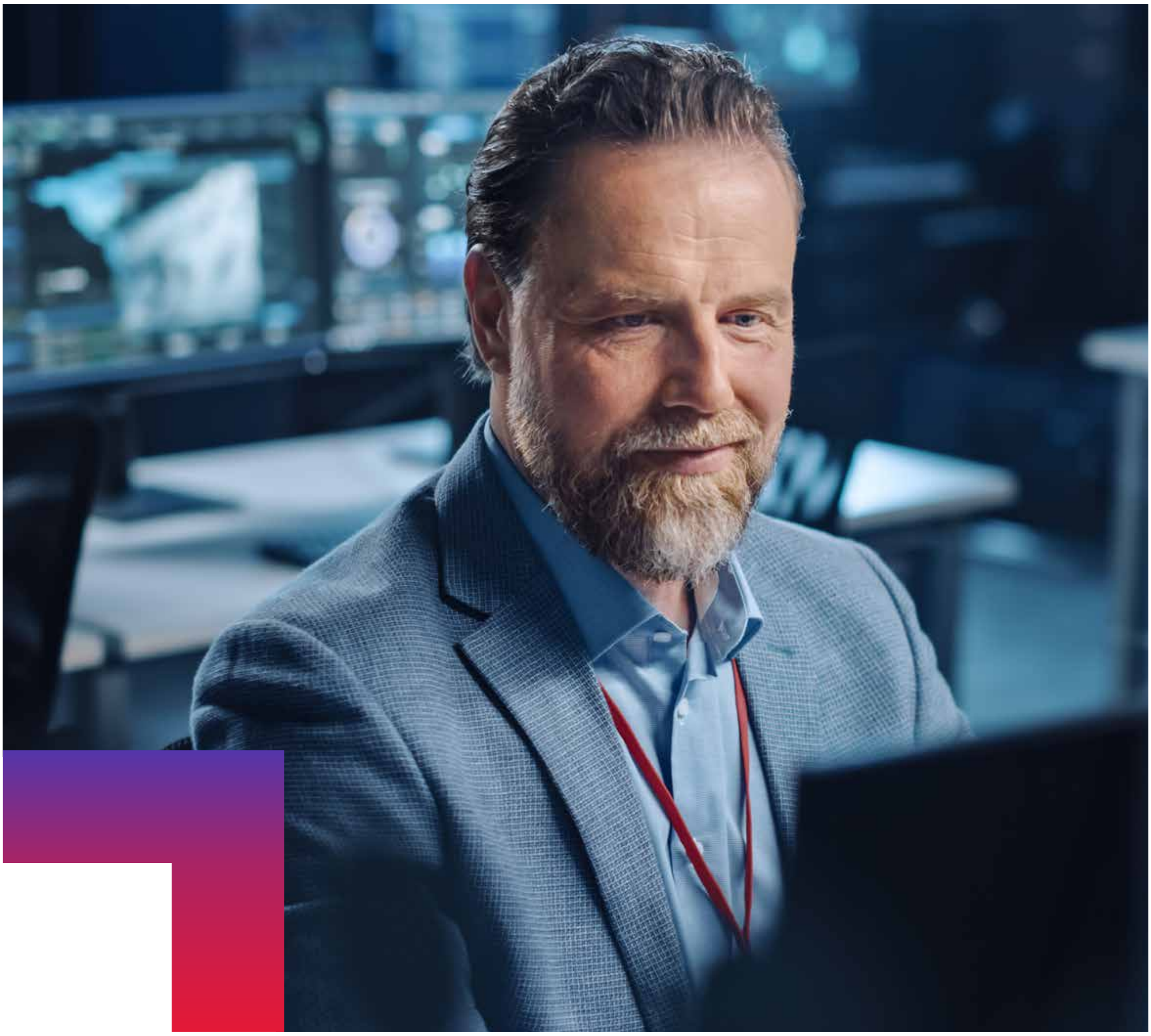
Security must be embedded throughout the lifecycle, with ongoing consideration of possible negative outcomes and use cases. To do this, we draw on our cross-sector experience and try to change the cyber security dynamic to allow good to prevail. This involves continuous adoption of new technologies and approaches in order to put any malicious actors on the backfoot.


Governance, Management & Compliance
Threat & Risk Management
ASSESS THE RISK
Security Strategy Maturity & Awareness
Incident Response & Forensics
INNOVATION RESILIENCE PRIVACY
Security Architecture & Engineering
OPERATE WITH CONFIDENCE
PROTECT THE BUSINESS
Security Operations
Test & Assure
Secure Engineering & Enabling Technologies
Cyber Threat Intelligence

Securing the IP - not just the perimeter

Conventional “castle-and-moat” cyber security models are no match for evolving cyber threats. They rely on secure network perimeters and constrained access via virtual private network-based employees and third-party remote access; however, business models and workforce dynamics have transformed.

The current trend sees organisations moving to cloud-based systems and hybrid IT environments to accommodate connected devices and remote working, which is dissolving the network perimeter. Furthermore, the growth of smart devices, 5G, edge computing and artificial intelligence creates even more data and connected nodes that further expand attack surfaces.



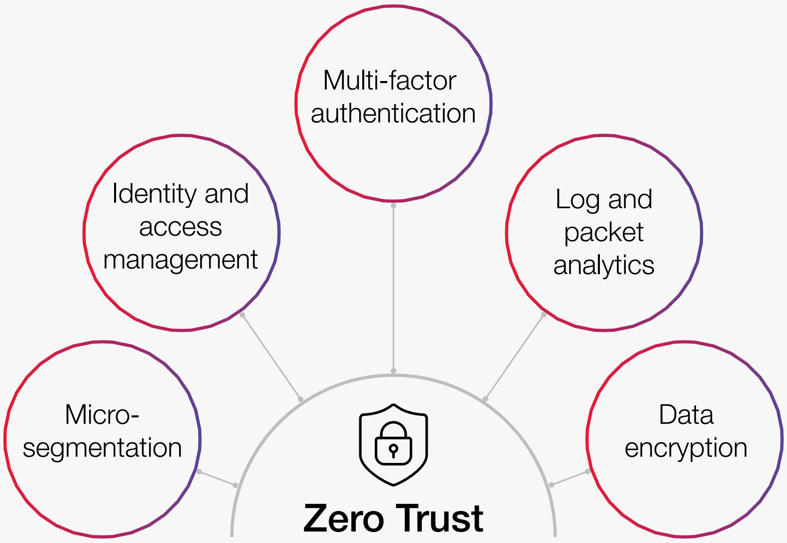
Zero trust approach

A zero trust approach is underpinned by effective identification and authentication that limits access based on the principle of least privilege, where a minimum set of users, applications, services and devices can access data and applications.

The proper design and engineering of zero trust architectures can result in simple, modular environments and straight forward user access that streamlines the security stack. This can eliminate considerable management headaches by significantly reducing operational overheads and risks of misconfiguration, whilst enabling scale to tens of thousands of users. Onboarding employees, contractors, cloud service providers and other vendors also becomes more efficient, flexible, responsive and secure.

Carefully designed zero trust architectures also embed automation and orchestration capabilities that amplify and work with other automated IT practices, such as DevSecOps and NoOps. This use of APIs across the technology ecosystem facilitates system management in a zero trust manner to provide a consistent control layer. Furthermore, leveraging cloud-based services also empowers organisations with the substantial security investments of cloud vendors.

Another key feature of a zero trust approach is the microsegmentation of networks, data, applications, workloads and other resources into individual, manageable units with clear ownership. This contains breaches and wraps security controls at the lowest level possible.



Proactive security - alerts and threat management

In contrast to a reactive approach to remediating cyber incidents, proactive security focuses on preventing incidents from happening in the first place, taking actions before any vulnerabilities are exploited or malware accesses server resources.

As organisations around the world have increasingly turned digital, cyber criminals have sought to maximise their profits by exploiting the vulnerabilities that come with rapidly expanding ecosystems. Ransomware therefore remains a significant security threat, and proactive security has become an essential approach to stop attacks.

Organisations achieve massive benefits from proactive security, including:

- Reduced risk to revenue
- Reduced risk to brand reputation, improving loyalty and trust from customers
- Reduced risk to productivity
- Reduced investigation and incident response costs
- Reduced likelihood of breaches and data loss.

Proactive security often requires additional applications and appliances built specifically for detecting attacks before they turn into critical incidents. This can require additional resources, and with the current skills shortage in cyber security, is increasingly costly. However, CGI has extensive experience with a proactive approach to protecting our clients' assets. Our cyber security experts are adept at adjusting the security posture based upon threat intelligence, actively tuning detection mechanisms based upon threats and using techniques such as MITRE to identify early signs of attack and ingress.

We also use techniques (i.e. Honeypot systems) to engage an attacker for a sufficiently long period to obtain high-level indicators of compromise (IoC), such as attack tools and tactics, techniques and procedures (TTPs). We can then take the appropriate action to ensure our customers are protected from malware, spammers and ransomware.

Data privacy and classification

Jurisdictions around the world are enacting strict new privacy laws (such as GDPR, CCPA, LGPD and CPPA) to better regulate and respond to modern privacy and data protection challenges. These laws drive an enormous amount of investment, business transformation, remediation and compliance effort across all economic sectors.

We often find that clients are not fully compliant with existing applicable privacy laws and are unprepared for major upcoming changes to those laws. As a result, our clients are increasingly identifying non-compliance with data protection laws as a top corporate concern in terms of legal, financial and reputational risk.

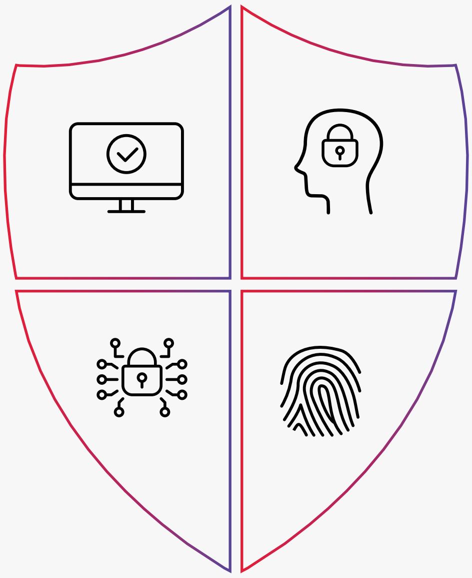
CGI UK was one of the first companies in the UK to achieve a UKAS accredited ISO 27701 certificate (the recently introduced data privacy standard), so is ideally placed to assist you with this challenge.

Value of certification

ISO27701 provides a valuable framework to support our efforts in legislative compliance and implementation of our data protection processes.

Legislative requirements

ISO27701 is an internationally recognised standard and is aligned with GDPR, demonstrating that data privacy is an integral part of the services that we deliver.



Expertise

Teams and members with the skills, knowledge and experience to support your projects that include handling personal data.

Partner of choice

Certification suports you in choosing CGI as a partner to process personal data.

What is data classification?

Data classification is the process of organising data by relevant categories in order to use and protect it more efficiently. Whilst on the surface this process makes data classification types easier to locate and retrieve, data classification is of particular importance when it comes to risk management, compliance and data security.

The three main types of data classification considered to be industry standards are:

1. **Content-based classification -** Inspects and interprets files, looking for sensitive information.
2. **Content-based classification -** Looks at application, location or creator (amongst other variables) as indirect indicators of sensitive information.
3. **User-based classification -** Depends on a manual, end-user selection of each document, relying on user knowledge and discretion at creation, edit, review or dissemination to flag sensitive documents.

With General Data Protection Regulation (GDPR) in effect, data classification is more imperative than ever for organisations that store, transfer or process data pertaining to EU citizens. It is crucial that these organisations classify data so that anything covered by GDPR is easily identifiable and the appropriate security precautions are taken.

Additionally, GDPR requires elevated protection for certain categories of personal data. For instance, GDPR explicitly prohibits basing decisions on data related to racial or ethnic origin, political opinions and religious or philosophical beliefs, i.e. sensitive data. Sensitive personal data is also subject to additional controls, including archiving. Classifying such data accordingly therefore significantly reduces the risk of compliance issues.

Whilst data classification is essential in enabling organisations to implement appropriate controls and policies based on the sensitivity of their data, we understand that it can be difficult to know where to start, especially where organisations process and store large volumes of unstructured data. CGI possesses in-depth experience of supporting clients on their journeys to facilitate more adequate data discovery and protection measures, and is here to help promote employee compliance with security policies.

Public

Data that may be freely disclosed to the public.

E.g. marketing materials, contact information, price lists, etc.

Internal only

Internal data not meant for pubic disclosure.

E.g. battlecards, sales playbooks, organisational charts, etc.

Confidential

Sensitive data that if compromised could negatively affect operations.

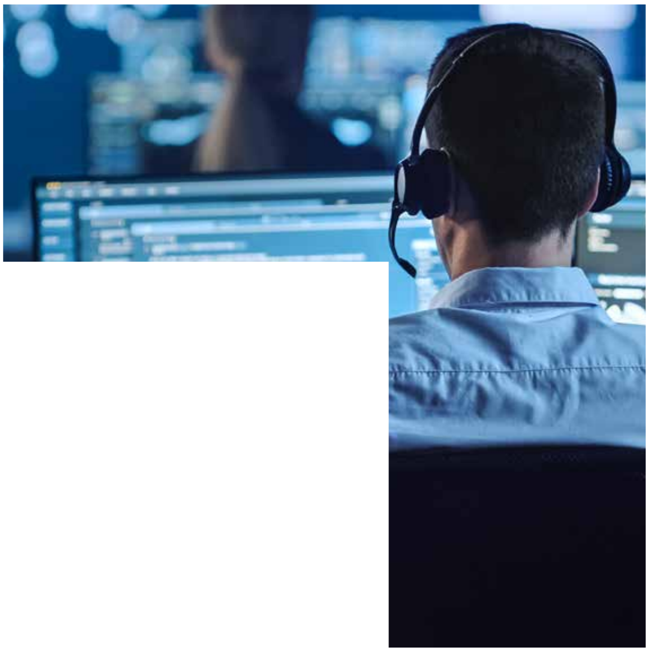
E.g. contracts with vendors, employee reviews, etc.

Restricted

Highly sensitive corporate data that if compromised could put the organisation in financial or legal risk.

E.g. IP, credit card information, social security numbers, PHI, etc.

Identity and access management

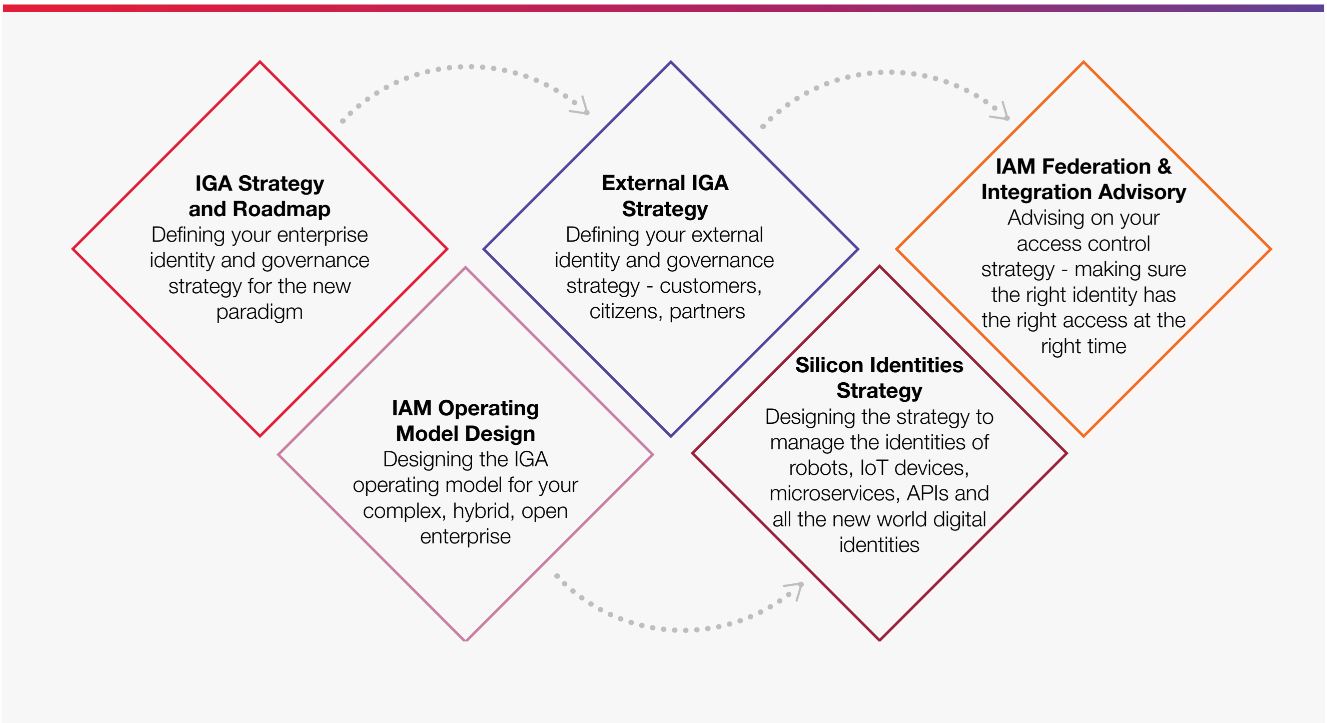


How can organisations maintain the digital speed and agility that they require, whilst simultaneously ensuring that internal and external digital identities remain secure, with the right level of privileged access given to the right identity at the right time?

Developed over 45 years of experience in providing cyber security managed services, CGI takes a holistic approach to designing and engineering digital identity and access management solutions. We stay abreast of the rapidly changing technology landscape and industry ecosystems, and factor in the connectivity, diversity and dynamism of needs to determine appropriate privacy, trust and security considerations for our clients.

We understand the complex environments our clients operate in, and the agile and seamless experiences required. Without the right digital identity and access management in place, your organisation will be exposed to new risks and threats that it will be unable to manage, and will be left behind, unable to innovate and collaborate. However, with the support from our deep industry and cyber security expertise, CGI clients can better navigate this new world of trusted, protected digital identities and context-based privileged access.

Our Advisory Services include:



IGA Strategy and Roadmap
Defining your enterprise identity and governance strategy for the new paradigm
External IGA Strategy
Defining your external identity and governance strategy - customers, citizens, partners
IAM Federation & Integration Advisory
Advising on your access control strategy - making sure the right identity has the right access at the right time
IAM Operating Model Design
Designing the IGA operating model for your complex, hybrid, open enterprise
Silicon Identities Strategy
Designing the strategy to manage the identities of robots, IoT devices, microservices, APIs and all the new world digital identities

IGA strategy and roadmap

In today's world, identity governance and administration (IGA) requires a reboot. We advise clients by examining the environmental currents they are facing and considering their needs and ambitions for a modern digital IGA approach. We develop a tailored identity and access management (IAM) strategy and roadmap of key initiatives to deliver measurable business value. We bring our unique maturity model (based upon ISO 27001 and ISO 27002) to assess our clients' current IGA in the areas of: governance, policies and processes, including lifecycle management, organisational entities and identity types, access control model, service desk, information classifications, and IAM technologies and vendors.

IAM operating model design

Beyond new IGA, organisations also need a new IAM operating model to operationalise governance with updated processes and tooling. We analyse clients' current state of IAM-related processes, policies, roles, authorisation, contexts, devices, microservices and tooling, and leverage our blueprints to design a new IAM operating model to support the transition towards an open zero trust model.

External IGA strategy

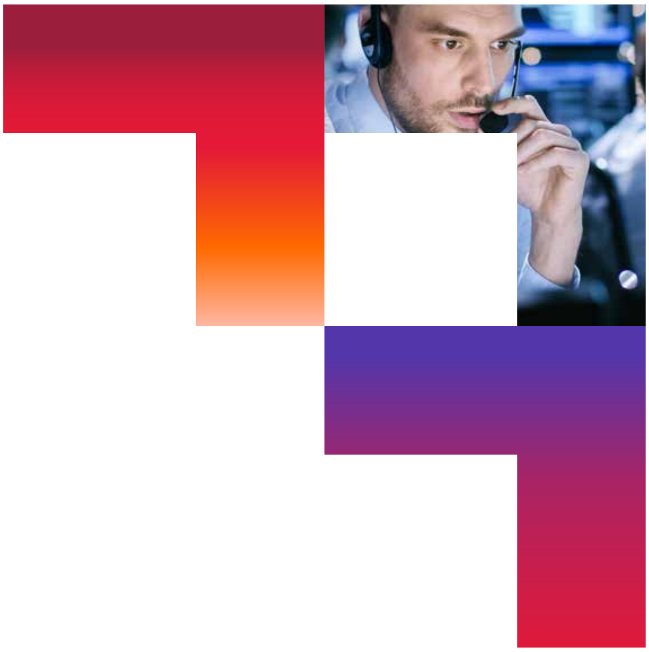
Traditionally, organisations are internally focused, seeking to secure the identity and access of employees. In today's open and connected ecosystems, organisations need to equally focus on identity governance and administration for external parties, including customers (B2B or B2C), citizens, suppliers and partners. We help our clients define their external IGA strategy using a proven methodology.

Silicon identities strategy

Modern work and operating environments are hybrid, with humans, machines and software collaborating together. It is not just human identities that need managing, but also the software, robots, IoT devices, sensors, APIs, microservices and AI workloads. CGI Advisory Services helps clients take systematic control of all these digital identities to enable appropriate access.

IAM federation and integration advisory

Different identities are often managed by different systems or organisations, with asset access also distributed and sometimes controlled by third parties (partners, government agencies, cloud providers, etc.). This IAM fragmentation requires a careful federation and technical integration strategy, ensuring privileged access is secure and seamless, and helping to achieve agility and improved time to market. CGI helps clients define IAM federation and integration strategies and blueprints by analysing their wider ecosystem and connections, flow of services and information, levels of assurance, regulatory and security requirements, policies, controls, identity providers, and authentication and authorisation protocols and frameworks.



Security – our blueprint

Cyber security infiltrates everything we do, with a vast range of cyber security services available to secure your digital enterprise.

Threat & Risk Management

- Risk Methods
- Through-life Risk Modelling
- Business Resilience
- Threat Intelligence

Governance, Management & Compliance

- Regulations & Standards
- Third Party & Supply Chain Management
- Information Security Management Systems
- Compliance

Security Strategy Maturity & Awareness

- Information Risk (IRIS) Maturity Assessment
- Strategy
- Data Labelling & Information Classification
- Risk Register

Incident Response & Forensics

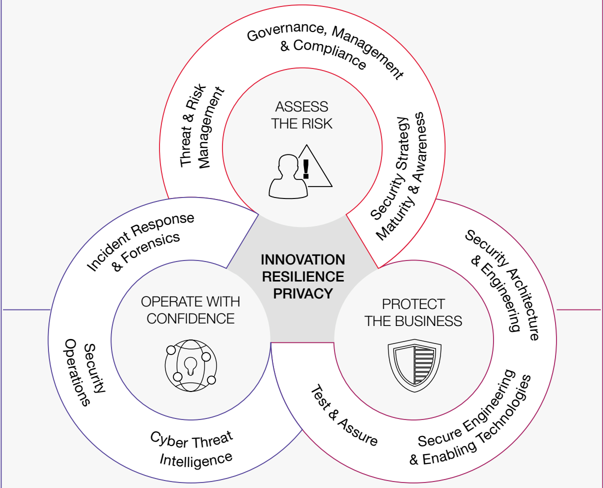
- Cyber Incident Management
- Cyber Incident Response
- Forensics Analysis
- Story Playbook

Security Operations

- 24x7 Protective Monitoring
- Managed Detections & Response
- Vulnerbaility Management
- Phishing Simulation & Triage

Cyber Threat Intelligence

- Client Focused Intelligence
- Personal Digital Footprints
- Corporate Digital Footprints
- Industry Intelligence Insights


Governance, Management & Compliance
Threat & Risk Management
Security Strategy Maturity & Awareness
ASSESS THE RISK
INNOVATION
RESILIENCE
PRIVACY
Incident Response & Forensics
OPERATE WITH CONFIDENCE
Security Operations
Cyber Threat Intelligence
Security Architecture & Engineering
PROTECT THE BUSINESS
Test & Assure
Secure Engineering & Enabling Technologies

Security Architecture & Engineering

- Assessing Security Impact
- Architecture
- Engineering Methods
- Secure System Design

Security Engineering & Enabling Technologies

- Safe Configuration & Deployment
- Enabling Adoption
- Subject Matter Expertise
- DevSecOps

Test & Assure

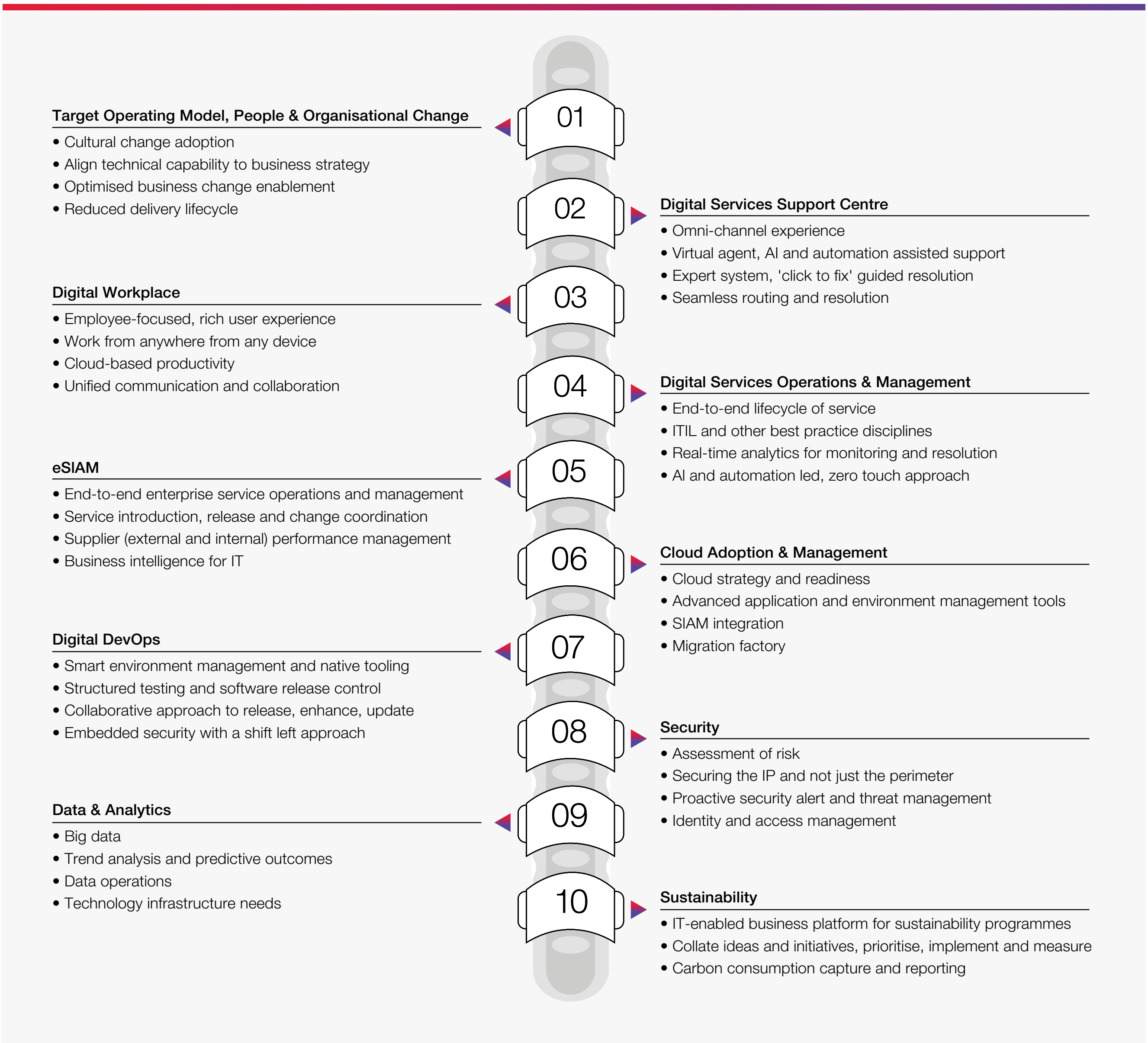
- ITHC, Pentesting, Red Team
- Design Assurance
- Implementation Assurance
- Code Assuarance

Advisory Services

Digital technologies can help organisations to unlock their full potential – but only when done right! The success of any digital transformation initiative relies upon embedding robust security throughout, and CGI Advisory Services is here to offer the support you need to securely transform the way your organisation works.

The Digital Backbone

The Digital Backbone is our methodology for encouraging digital transformation and enabling IT as an extension of our clients' organisations. With security a central component of any digital enterprise, we have therefore made it a key anchor of the Digital Backbone, incorporated throughout our portfolio of offerings.



01

Target Operating Model, People & Organisational Change

- Cultural change adoption
- Align technical capability to business strategy
- Optimised business change enablement
- Reduced delivery lifecycle

02

Digital Services Support Centre

- Omni-channel experience
- Virtual agent, AI and automation assisted support
- Expert system, 'click to fix' guided resolution
- Seamless routing and resolution

03

Digital Workplace

- Employee-focused, rich user experience
- Work from anywhere from any device
- Cloud-based productivity
- Unified communication and collaboration

04

Digital Services Operations & Management

- End-to-end lifecycle of service
- ITIL and other best practice disciplines
- Real-time analytics for monitoring and resolution
- AI and automation led, zero touch approach

05

eSIAM

- End-to-end enterprise service operations and management
- Service introduction, release and change coordination
- Supplier (external and internal) performance management
- Business intelligence for IT

06

Cloud Adoption & Management

- Cloud strategy and readiness
- Advanced application and environment management tools
- SIAM integration
- Migration factory

07

Digital DevOps

- Smart environment management and native tooling
- Structured testing and software release control
- Collaborative approach to release, enhance, update
- Embedded security with a shift left approach

08

Security

- Assessment of risk
- Securing the IP and not just the perimeter
- Proactive security alert and threat management
- Identity and access management

09

Data & Analytics

- Big data
- Trend analysis and predictive outcomes
- Data operations
- Technology infrastructure needs

10

Sustainability

- IT-enabled business platform for sustainability programmes
- Collate ideas and initiatives, prioritise, implement and measure
- Carbon consumption capture and reporting

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 88,500 professionals provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

Visit: Advisory Services

cgi.com/uk