Cyber security

Identity and access management services

Contents

An effective IAM strategy combines people and processes with technology to drive efficiency, competitive advantage and risk reduction.

Cyber security is part of everything we do

And Identity and Access Management (IAM) is a key enabler.

We have over 1,700 cyber security experts globally and one of the largest cyber security practices in the UK helping clients manage complex security challenges with a business-focused approach, protecting what is most valuable to them.

We work with leading organisations across the commercial and government sectors in the UK, Canada, USA, Australia and Europe.

One of the most important challenges facing senior management right now is making sure their organisation is resilient to cyber attacks and that their data is protected accordingly. As a result, managing identities and access must be a key component of their cyber security strategy.

We understand that IAM is not just about technology. An effective IAM strategy combines people and processes with technology to drive efficiency, competitive advantage and risk reduction. Our IAM solution offerings focus on the three key problem domains – Enterprise Identity Governance and Administration, Risk Based Conditional Access and Privileged Access Management.

Our specialist consulting services help organisations deliver their strategic and tactical requirements across these three critical cyber security domains:

Assess the risk:

Helping you to assess the risks associated with identity and access so you can prioritise implementation of your security controls.

Protect the business:

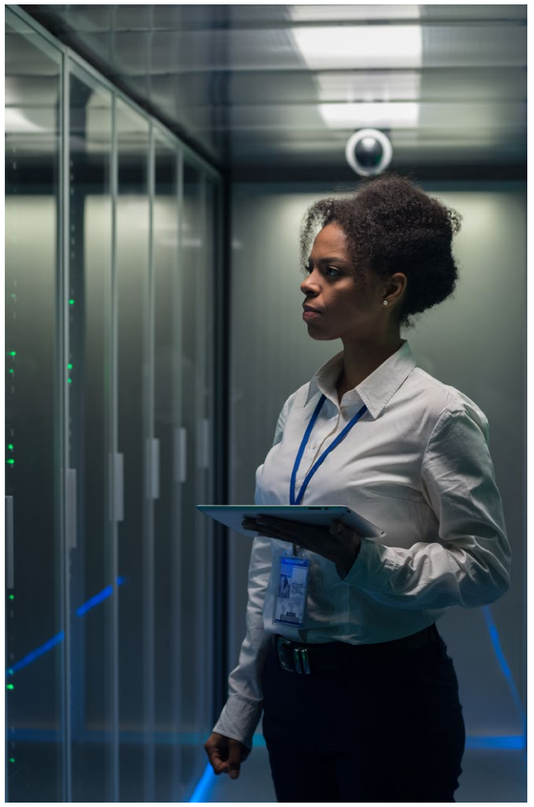
Helping you to build your IAM controls to ensure that only authorised users have access to your information assets and customer data.

Operate with confidence:

Helping you to monitor critical user access control events to prevent and respond to security attacks in a reliable and cost-effective way.

Enterprise identity governance and administration

IAM is critically important for every enterprise. Supply chain integration, cloud services, and bring your own device (BYOD) policies are eroding organisational boundaries, making it increasingly difficult to protect access to critical resources, while meeting rigorous compliance requirements. There is pressure on IAM programmes to be aligned closely to the business' needs, cost effective and, more importantly, agile in supporting new business initiatives.



The challenge

Enterprise IT departments face the following challenges in controlling access to the organisation's critical information assets:

Accountability and risk of data breach

- **The IT infrastructure is vulnerable to insiders who have approved access to the trusted environment.** According to research by the Ponemon Institute, negligent employees or contractors cost companies an average of £307K, and the cost triples to £871K if the negligence involves credential theft[1].
- **It is difficult to balance access with security.** Organisations must make it easy to do business by meeting information-sharing requirements, but at the same time, must protect critical business-sensitive assets from compromise by third parties. This is made more complicated by a distributed workforce and an extensive supply chain network.
- **A complex environment increases the security challenge.** Managing users and their entitlements across a complex distributed application landscape is made more complicated by the adoption of SaaS and other cloud models.
- **There are competing data use cases.** Balancing consumer privacy and consent with the use of consumer data for business intelligence and marketing.

Operational overhead and user experience

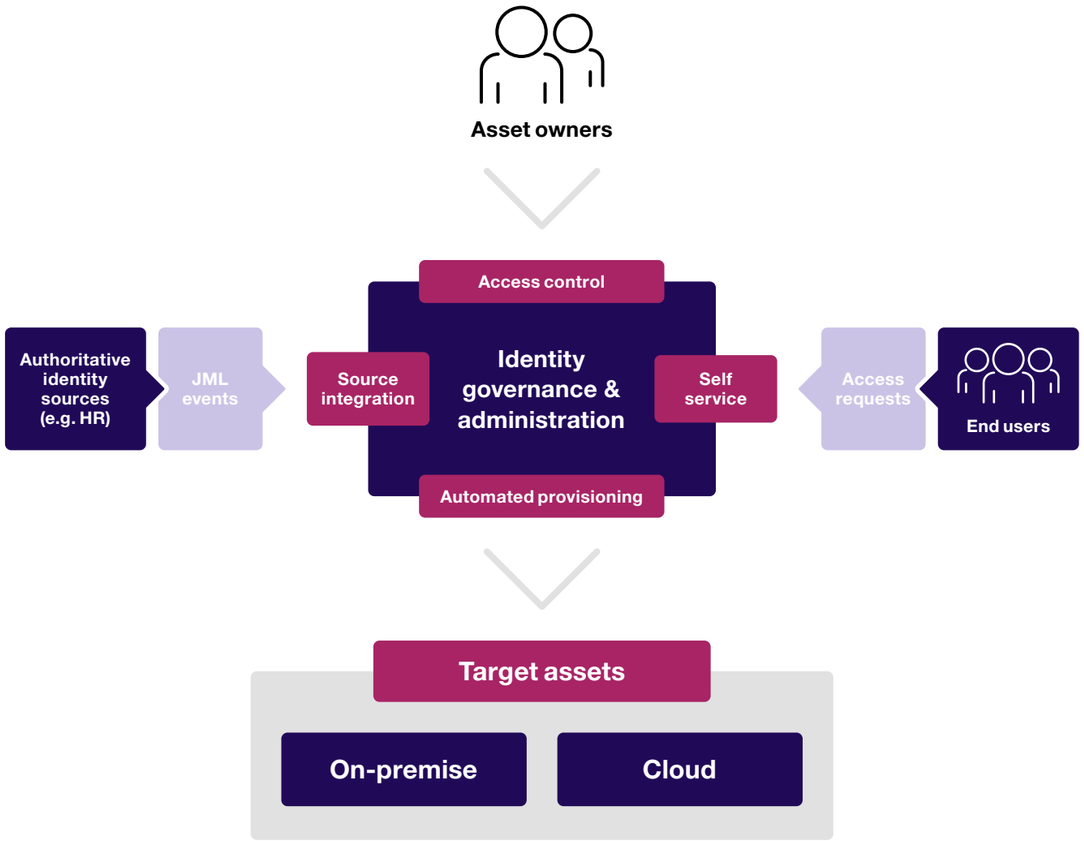
- **Inefficiencies hold the business back.** Inefficient identity management and access management pushes up operational costs and causes disruptions and delay.
- **Good collaboration with partners and supply chains can grow revenue.** Gartner estimates that greater customer experience during identity corroboration will earn 20% more revenue by 2022[2].

Ability to meet multiple audit and compliance requirements

- Privacy regulations, e.g. GDPR, HIPAA.
- Identity best practice/guidance, e.g. NIST, NCSC, CPNI identity guidelines.
- Other standards/regulation, e.g. ISO/IEC 27001, IEC 62443-2-1:2011, PCI-DSS, SOX.

1. https://www.observeit.com/wp-content/uploads/2020/04/2020-Global-Cost-of-Insider-Threats-Ponemon-Report_UTD.pdf
2. Gartner IAM Summit 2019 – Keynote: The future of Identity and Access Management.

Our solution and business benefits



To help organisations address these challenges, our solution puts in place the policy, processes and automations to address the following key areas:

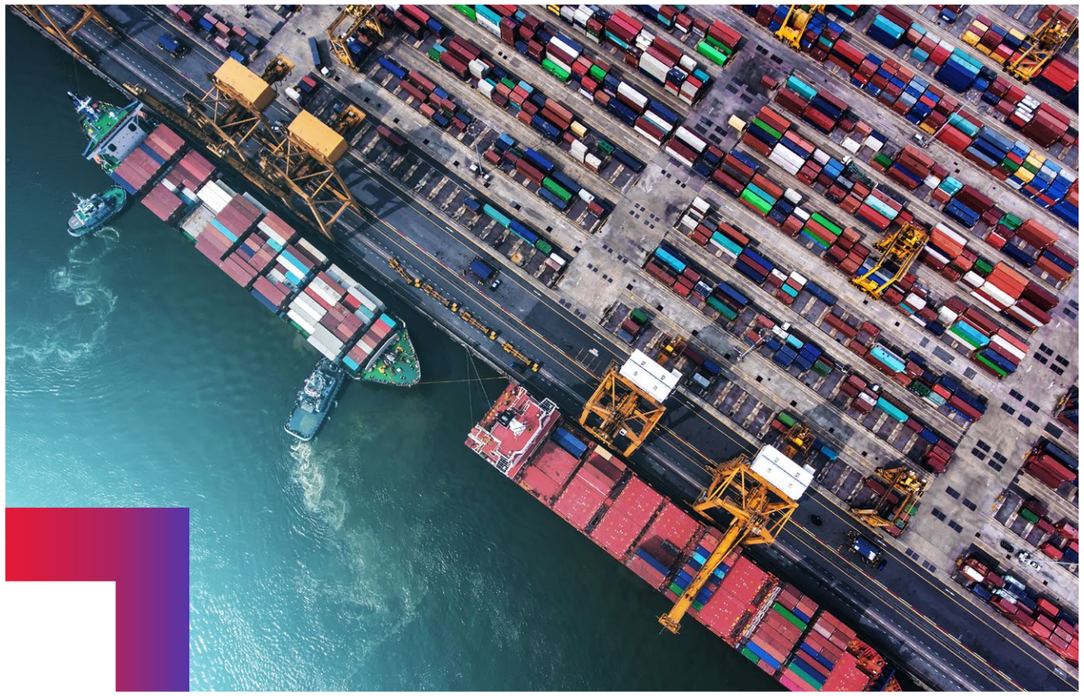
- Tracking access permissions by integrating identity sources with the latest information on joiners, movers and leavers within your organisation. As well as reducing inefficient manual processes, this will fix lapses in the leaver process, reduce the risk of dormant accounts and cut down on unnecessary privileges.
- Control over who has access to what through establishing who owns what information assets, enforcing protection policies at both design-time and request-time, implementing approval workflows, and ongoing spot check reviews of permission to access followed by confirmation of justified permissions.
- Flexibility and user experience, driven through self-service while, at the same time, minimising risk through automating account creation with just-in-time provisioning.
- Establishing policy-driven automated provisioning and de-provisioning of entitlements to reduce operational latency and to swiftly remove toxic and redundant permissions.

Together, these measures will help you minimise the risk of data breach and reduce your operational overheads, at the same time as making sure you meet regulatory requirements and improve your users' experience. Our solution will also help you to respond swiftly to the changing security and operational needs of your business.

Risk-based conditional access

Today's enterprises have a complex user base with multiple devices that need to access many different applications and datasets, across on-premise and cloud environments. With so many access points, this hybrid environment is highly vulnerable and managing access control risk should be one of the top concerns of any enterprise.

There is a lot of innovation happening in this area, and the technology involved remains volatile. Our flexible and cohesive approach to managing these risks takes into account the fact that technology is developing fast and protects your organisation as you adopt new technology. Our model supports your cloud services and your legacy estate simultaneously, including any iterative evolution while your organisation is moving to a cloud-first model.



The challenge

A typical enterprise transitioning to a cloud-first infrastructure model faces several challenges in controlling access to their critical information assets.

Hybrid environment and workforce

- **Existing control layers are not adequate.** The thin or non-existent organisation network boundaries of traditional, decoupled access control layers cannot adequately support today's workforce and security requirements.
- **It is a drawn-out process.** The journey towards a cloud native and multi-cloud infrastructure places organisations in an extended state of flux, with long periods of transition without a unified access control model.
- **Using third parties increases vulnerabilities.** Increasingly, organisations rely on third parties to carry out their business-critical functions, leading to a meshed employee-contractor-service provider workforce that increases the risk of data breaches.

Password problem

- Passwords are vulnerable. 80% of data breaches are estimated to be related to weak, default and stolen passwords[3]. Yet the vast majority of organisations only use password authentication to protect access to their information assets.
- Password reset is expensive. According to Forrester, the cost of single password reset averages £70[4].
- Password difficulties lose business. Up to 18% of online retail business is lost with password related shopping cart abandonment[5].

Operational efficiency and business agility

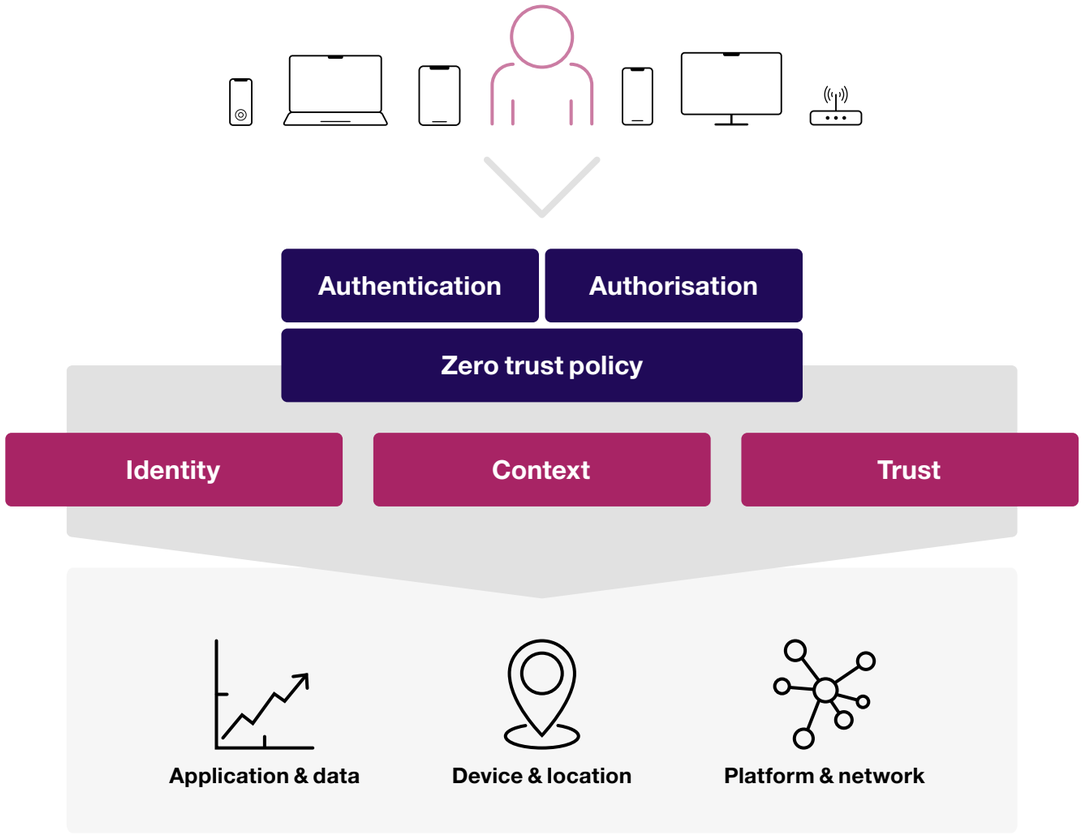
- Collaborating with partners and your supply chain needs to be seamless. Gartner estimates that greater customer experience during identity corroboration will earn 20% more revenue by 2022[6].
- Third party involvement complicates security. There are challenges around peer-to-peer trust and access token management when working with multiple third parties.

Ability to meet multiple audit and compliance requirements

- Privacy regulations, e.g. GDPR, HIPAA.
- Open standards and competition, e.g. Open API, CMA, PSD2 RTS for SCA/CSC.
- Secure and consented exploitation of customer data.
- Identity guidance/standards, e.g. NIST SP.800-63B/C, SP.800-207.

3. https://enterprise.verizon.com/resources/reports/dbir/
4. https://www.forrester.com/report/Best+Practices+Selecting+Deploying+And+Managing+ Enterprise+Password+Managers/-/E-RES139333
5. https://baymard.com/blog/password-requirements-and-password-reset
6. Gartner IAM Summit 2019 – Keynote: The future of Identity and Access Management.

Our solution and business benefits



Our solution uses a centralised, identity-based architecture framework that takes a zero-trust approach, so it is structured to verify anything and everything trying to connect to its systems before granting access. It includes:

- The centralised management of access policies. This uses key factors such as identity, context and trust to monitor access to target applications, data, platforms and networks.
- A standardised policy decision service(s) that uses context-aware access, controlling what a user can access based on attributes such as identity, location, device security status and IP address. This service can work across all layers, including infrastructure, network, application and data. It will support both modern and legacy deployments, with appropriate mitigations.
- Support for password-less authentication. This uses something the user has such as a mobile phone, a one-time-password token, smart card or a hardware token to verify access and monitors usage patterns to agreed assurance levels.
- Using Hybrid Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC) models for efficiency, while maintaining high security standards. These restrict access based on the individual's role within your organisation (RBAC) or use a combination of factors such as role and project to determine access permissions (ABAC).
- A framework that can adapt easily to new offerings from different vendors (reducing vendor lock-in) and can enable innovation.
- A system which works for humans as well as for things.

These capabilities will help you minimise the risk of a data breach, reduce third-party access risks, meet regulatory requirements, improve user experience and reduce the cost of security assurance of modern applications and microservices.

Privileged access management

Privileged Access Management (PAM) is a collection of tools and practices that helps an organisation mitigate the risk of accidental and deliberate misuse of high impact accounts and permissions. PAM is one of the foundational security building blocks that help organisations defend themselves from cyber attacks in today's ever-changing cyber threat landscape. We believe PAM is an integral part of your overall Identity and Access Management strategy.

The challenge

A typical medium-sized organisation will have up to 500 virtual/physical servers, making keeping an eye on who has high privileges to these assets a big challenge. This challenge increases when you factor in numerous deployments using containers, and the use of software as a service (SaaS). In this context, organisations need a strong, cohesive strategy to avoid data breaches that considers the following issues.

Highly privileged accounts

- **Third-party involvement increases risk.** By relying more on third parties to carry out their business-critical operational functions, organisations are forced to delegate high privileges. Third-party high-privilege misuse is one of the top 10 risks faced by today's enterprises[7].
- **Threats from within the business are significant.** Insiders with high privileges are responsible for 34% of all data breaches[8].
- **Non-human access is also a threat vector.** Un-secure non-human and shared accounts such as root accounts, service accounts, database accounts and API keys are easy targets for privilege escalations.

DevSecOps and automation

- **Old security standards are inadequate or inappropriate.** In the DevSecOps, continuous integration, continuous deployment (CI/CD) world, the credentials used in automation usually have very high privilege and any leakage could lead to catastrophic failures.

The security of a hybrid, interconnected environment

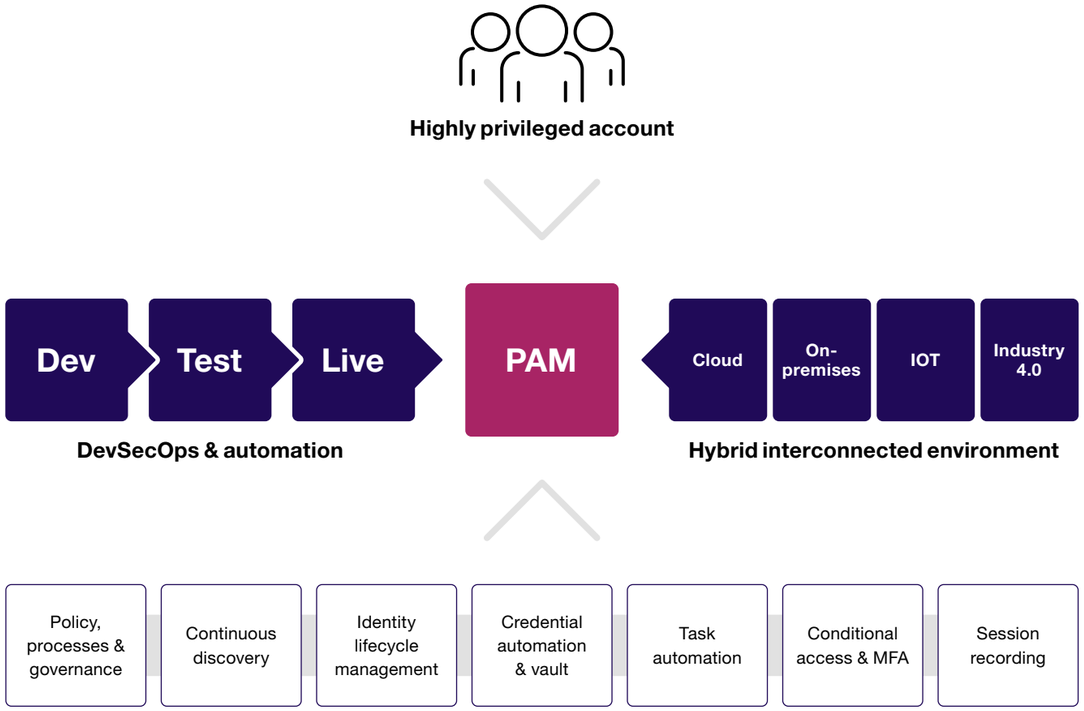
- **Low visibility of highly privileged accounts.** With a constantly changing infrastructure, it is difficult to achieve comprehensive discovery.
- **At-a-glance visibility is difficult.** There is no single view available across on-premise and cloud environments.
- **A distributed environment complicates access management.** This arises from Low visibility and the need to control dynamic, distributed compute and serverless infrastructure.
- **Policy enforcement is difficult.** Decentralised access control leads to inconsistent policy enforcement.

Ability to meet multiple audit and compliance requirements

- Privacy regulations, e.g. GDPR, HIPAA.
- Identity guidance and standards, e.g. NIST SP 1800-18.
- Other standards and regulations, e.g. ISO/IEC 27001, IEC 62443-2-1:2011, PCI-DSS, SOX.

7. https://www.cyberark.com/resources/blog/third-party-access-is-a-top-10-organizational-risk
8. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Our solution and business benefits



Our approach is based on the experience we have gained working for numerous customers across the globe. We take a holistic, identity-driven approach to mitigate the risks of giving special access beyond that of a standard user (privileged access). This approach covers the following areas:

- Standardised privileged access management policy and processes which integrate with a robust enterprise identity and access governance solution.
- Continuous and incremental risk-based discovery, assisted by best-of-breed analytics tools. This identifies potential failure points meaning you can fast-track fixes and ensure continual compliance.
- Pattern-based cloud integration and account mapping to enforce standardisation in a multi-cloud ecosystem.
- Integrating identity management into your organisation's automation, orchestration and service desk processes to shrink your attack surface.
- Risk-based conditional access with multifactor authentication (MFA) minimising third-party access risks.
- Password vaults, automated password recycling and session recording (where appropriate) to enable legacy integration.
- Standardised, risk-based audit collection patterns designed to capture the optimal levels of audit records and enable efficient integration with security monitoring technology.

CGI IAM consulting services

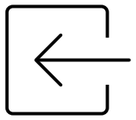
We are one of the leading cyber security specialists in the UK. Our practice includes a large number of consultants specialising in IAM. We offer a broad range of IAM business and technology services, which are tailored to meet the needs of modern enterprises across all industries.

IAM Strategy

To be successful in today's hyper-digitalised market, a robust identity strategy is essential. We find that engaging with all stakeholders and improving the employee and customer experiences is key to the success of any IAM project. This is because IAM is more than implementing technology; it involves integrating both people and business processes. We take a risk-based, agile approach to setting your strategy and roadmap. We carefully align our approach with your business and operational needs, so that we achieve the best possible risk mitigation outcomes and a cost-effective solution.

Enterprise IAM Architecture

Businesses are changing the way they operate, often demanding more collaboration and flexible working. This means, to be effective, systems need to demonstrate a fine balance between security, usability and cost. Plus, now that you can deploy supporting digital services over a plethora of cloud and on-premise infrastructures, IAM is a constantly evolving area. IAM implementations need to be flexible and adaptable, supporting this hybrid setup with standardised policies, processes and technology. We will help you realise your tactical and strategic IAM requirements with a pragmatic risk-based approach.



IAM Essentials

Managing users and their access to information assets is a critical undertaking for any enterprise. Although requirements may vary based on how a business interacts with its partners, customers and third parties, most businesses will face similar risks. Not all organisations will need to invest heavily in IAM, but every organisation will need to establish the most important and cost-effective IAM controls for them. Our IAM Essentials will help you meet those baseline requirements.

CGI IAM Essentials is a packaged consultancy engagement, which lets you quickly discover and remediate your most critical IAM vulnerabilities to establish your baseline governance. We use a hybrid top-down and bottom-up method to identify prioritised remediation to speed up your risk mitigation activities.

CGI IAM consulting services

Zero-Trust Identity and Access Architecture

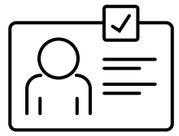
Because of the erosion of more traditional security perimeters, where everything inside the perimeter was trusted, the new security architectural concepts such as Zero-Trust Architecture (ZTA) are becoming popular. ZTA assumes a breach and verifies each access request as if it originated on an open network. Each access request is authenticated and authorised. Granularity of control and the ability to make access changes quickly are key advantages of this architecture. This requires a strong IAM strategy and implementation approach to underpin it. We have relationships with a wide variety of platform and product vendors and provide comprehensive out-of-the-box or tailored solutions for our clients.

Password-less Access

Stolen or compromised passwords contribute to 80% of data breaches. It is one of the major vulnerabilities, and it is also expensive to support, with many helpdesk calls relating to forgotten passwords. In practice, reducing these costs is held back by the use of legacy systems, hybrid environments and cost of maintaining additional credentials. Fortunately, with the new FIDO2.0 and WebAuthN standards there are options available for implementing cost-effective authentication that does not need passwords. We have broad experience of delivering strong authentication including Multi Factor Authentication (MFA) to some of the most highly secure environments. We can help you mitigate your risks associated with passwords and improve your user authentication experience at the same time.

Hybrid Cloud IAM & DevSecOps

Hybrid cloud promises to optimise the digital supply chain, reduce single vendor lock-in and maximise time-to-value. Yet hybrid cloud invariably means distributed and numerous service providers along with new and varied risks of data breach. In reality, having multiple accounts across numerous environments and a need to log on to each separately may adversely affect the productivity of operational staff. Also, if DevSecOps and the use of containers is not managed properly, risk can increase because of floating highly privileged non-human accounts. A unified identity solution is key to reaping the benefits and full value of the hybrid cloud paradigm. We take a holistic view of IAM and bring together the disciplines of PAM, identity governance, federation and automation to reduce access control risks. We will help you improve productivity by implementing standardised policies, processes and technology across all your cloud platforms.



Bring your own identity (IAM Trust Management)

Interoperable identity is key to the success of modern digital business, whether it is used to collaborate with partners, the supply chain, service providers or to enable frictionless access for consumers and citizens. In this model, the organisation can rely on third parties to handle the privacy and liability of managing identities, using protocols such as SAML, OAuth, OIDC and zero-knowledge proof to achieve this integration. However, organisations will need to maintain appropriate levels of trust with those third parties, putting in place identity services and local controls that deliver the required level of security assurance. Our trust management capability will help you to manage the associated risks, and implement the required security controls, while maintaining a seamless user experience.

CGI UK IAM service catalogue

UK IAM consulting

- IAM strategy & roadmap
- IAM essentials (fast track remediation
- Enterprise IAM architecture
- Zero trust & access architecture
- Password-less access
- Hybrid cloud IAM & DevSecOps
- Identity trust management (BYOID)
- Identity data privacy & consent

IAM implementation services

- Enterprise identity governance & administration
- Risk based conditional access
- Privileged access management

UK cyber services

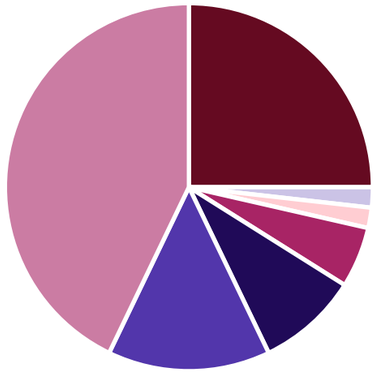
- Organisational security risk assessment
- Managed detection & response
- Penetration testing

On shore | **Blended delivery model** | Off shore

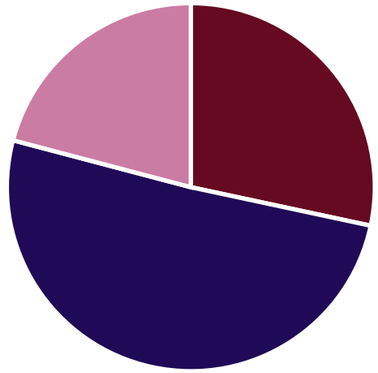
CGI IAM credentials

We have wide-ranging experience in delivering complex and large-scale IAM projects and services across a wide range of industries and sectors. We offer broad IAM business and technology expertise with significant breadth and depth of capability to support IAM requirements.

Over 50 IAM projects last 5 years



Broad experience



IAM is critically important for every enterprise. Supply chain integration, cloud services, and bring your own device (BYOD) policies are eroding organisational boundaries, making it increasingly difficult to protect access to critical resources, while meeting rigorous compliance requirements.

Make an enquiry

If you know who your contact point is within CGI, then simply reach out to discuss the options best suited to your requirement.

For general enquiries, please email: **cyber.enquiry.uk@cgi.com**

About CGI

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 industries 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.

Our commitment: Insights you can act on.

For more information, visit cgi.com/uk/cyber-security or email us at cyber.enquiry.uk@cgi.com