altIAM®

Let the Right One In

Identity Access Management

"Let the Right One In"

altIAM
Let the Right One In

What is Identity Access Management?

Gartner defines IAM as:

"Identity and Access Management is a fundamental and critical cybersecurity capability, to ensure the ***right*** identities, have the ***right*** access to the ***right*** resources at the ***right*** time for the ***right*** reasons."

Business and public sector organisations are expected to offer frictionless and transparent access to their digital estate for:

employees – to enable hybrid working

customers – can place orders, track orders, obtain customer support

suppliers – monitor stock levels, check payments

government agencies – monitor compliance, collect taxes

devices – IoT can input data, as part of the day-to-day business operations and transactions. This access then gives cybercriminals, cyberwar and other malicious bad actors, the access vectors into your digital estate which must be secure.

Digital Access Problem Space

Identities
People, systems, things

- Employees
- Contactors
- Customer
- Members
- Suppliers
- Public
- Devices (IoT)
- Systems

Systems
On prem, hybrid, hosting

- On premise
- Corporate Cloud
- Public Cloud
- As service (Saas) or platform (PaaS)

Channels
System devices and end points

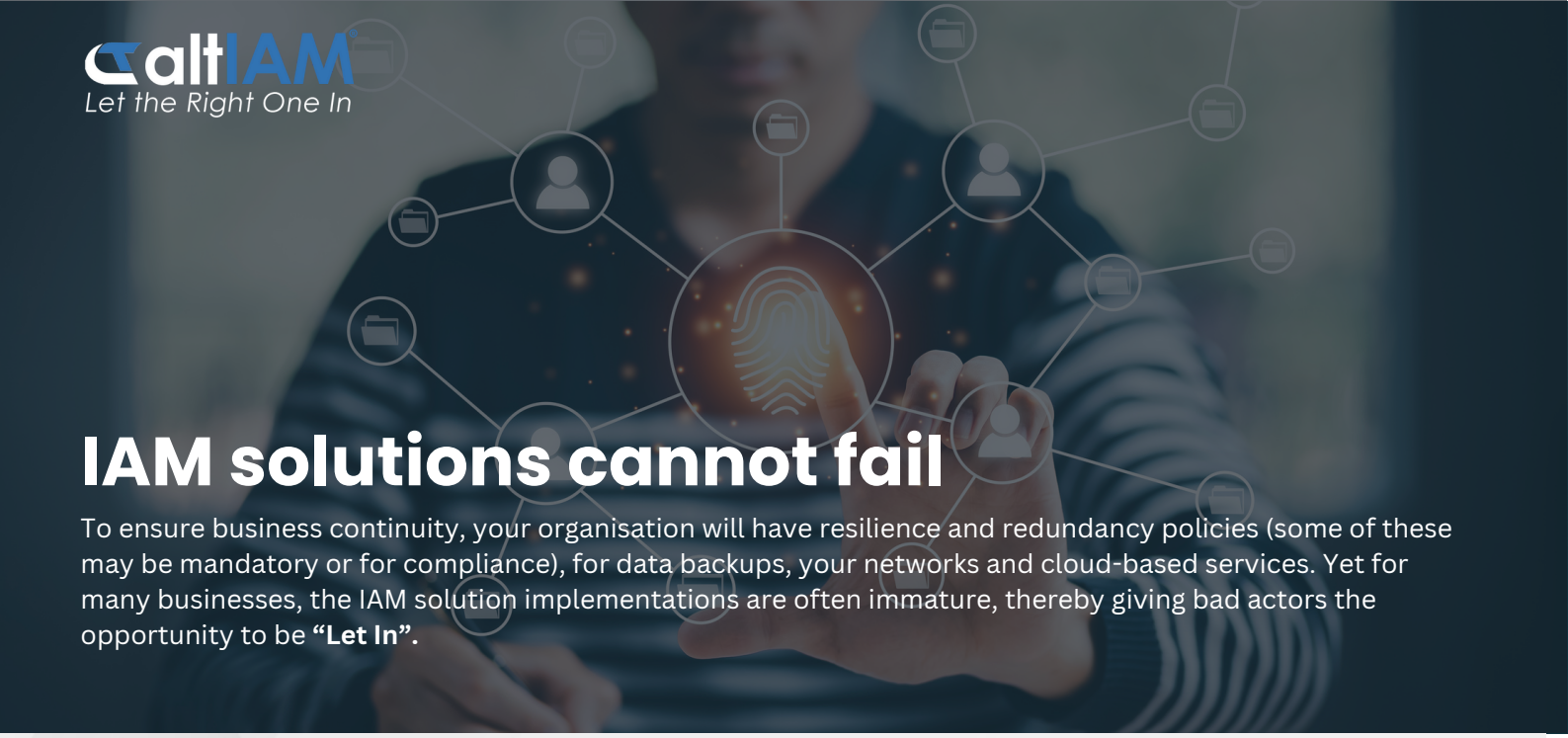
- Business computers - servers, personal
- Personal computers and BOYD
- Suppliers
- Operational partners

It is not possible to solve the IAM problem space by adding more software or hiring more staff. To implement an effective and sustainable IAM solution, specifically tailored to your company's needs, requires a solution to be designed, implemented and supported by IAM subject matter experts.

At altIAM, we have the skills, to assess your requirements and implement robust IAM solutions that will make your IAM problem cybersecure.

Identity Access Management
"Let the Right One In"

altIAM
Let the Right One In



IAM solutions cannot fail

To ensure business continuity, your organisation will have resilience and redundancy policies (some of these may be mandatory or for compliance), for data backups, your networks and cloud-based services. Yet for many businesses, the IAM solution implementations are often immature, thereby giving bad actors the opportunity to be **“Let In”.**

If the bad actors are allowed “in”, the impact can be significant, such as:

- **Operational** – manufacturing capacity reduced or closed, power cuts, logistics delays, reduction in availability of healthcare services
- **Financial** – theft, fines, customer churn due to loss of personal data
- **Reputational** – customer confidence, brand trustworthiness

If your organisation is experiencing one or more of the following challenges with the implementation of your IAM solution, altIAM can help with:

- **IAM solution Implementation**. It can require a compelling business case, which shows both the Return on Investment (ROI), and Total Cost of Ownership (TCO) that addresses the cybersecurity risks and aligns the IAM solution with the company’s objectives. AltIAM’s DART solution model can provide the input to help support the IAM solution business case for senior management
- **Resources in-house**. Your organisation may have limited or no IAM expertise to design, deploy and manage your in-life IAM Solution as well as maintain and develop your digital estate to meet business needs
- **Governance.** IAM solution does not have the “buy-in” or comprehensive strategy, or roadmap from executive management. In addition, departmental arguing over the ownership and control of data and applications can prevent IAM solution deployment

- **Change management**. “It’s how we’ve always done it,” has been institutionalised, therefore, hindering change management and organisational transformation procedures
- **Identity Authority**. Do you know who can access your digital estate? How is this access managed? How do you prevent privilege creep? How do you stop unverified identities and privileges from being transferred between systems in your digital estate?

Identity Access Management
"Let the Right One In"

IAM solutions cannot fail (Continued)

- **Program Failure.** IAM solution deployment has a high Delivery Complexity, as it requires the implementation of processes and systems across all the operational divisions of an organisation. A combination of optimistic delivery timetables and resource scarcity can lead to project overrun and delayed IAM solution deployment

Compliance Regulations and Legislation

- **Federal Financial Institutions Examinations Council (FFIEC)**. USA compliance standards for financial institutions.
- **Sarbanes-Oxley Act.** USA legislation financial institutions to protect the confidentiality of non-public customer data.
- **Gramm-Leach-Bliley-Act.** USA legislation for financial institutions to protect the confidentiality of non-public customer data.
- **HIPAA.** USA legislation that controls for preparing financial reports and integrity report data.
- **Family Educational Rights and Privacy Act.** USA legislation educational institutions to protect student records and associated data.
- **ISO 27000 series** of IAM standards are widely used as an audit benchmark.
- **PCI DSS.** This global security payment card distributors standards, including IAM requirements.
- **GDPR.** European standard security and protection issues, including IAM requirements. EU GDPR has been replaced by UK GDPR 2021
- **FCA Compliance**
- **The Data Protection Act 1998 (DPA).** The common law duty of confidentiality.
- **The Social Care Record Guarantee for England.** The international information security standard: ISO/IEC 27002:2005
- **The Code of Practice for the Management of Confidential Information** Confidential information concerning or connected with the provision of health services or adult social care.
- **Government Connect Secure Extranet (GCSX).** A managed network service and a secure Wide Area Network (WAN) that allows officials at local public-sector organisations to interact and share data privately and securely with central government departments.

- **User Experience.** To “Let The Right One In” for your employees, your customers and others who need to access your digital estate, this needs to be a compelling experience which supports your digital transformation, without compromising your cybersecurity
- **Right technology**. Selecting and deploying the right combination of technology is complex and requires selection, based on an organisation’s vision and business needs
- **Disruptive digital technologies.** The norm is digital change such as hybrid and migration to the cloud, growth of IoT, mobile working practices, virtualization of “everything” which means, many organisations lack the internal expertise and capacity to support effective IAM solutions in the constantly changing digital landscape
- **Regulatory compliance.** Regulatory authorities who set cybersecurity policies for industry sectors, mandate that IAM solutions are essential for organisations to secure regulatory authority compliance. Without this compliance, organisations will not be allowed to engage business operations. Regulatory authorities undertake audits to confirm organisations are compliant and to verify they are continuously maintaining an effective IAM cybersecurity solution.

AltIAM will be able to help with both the issues and challenges of implementing an IAM solution.

Identity Access Management
"Let the Right One In"

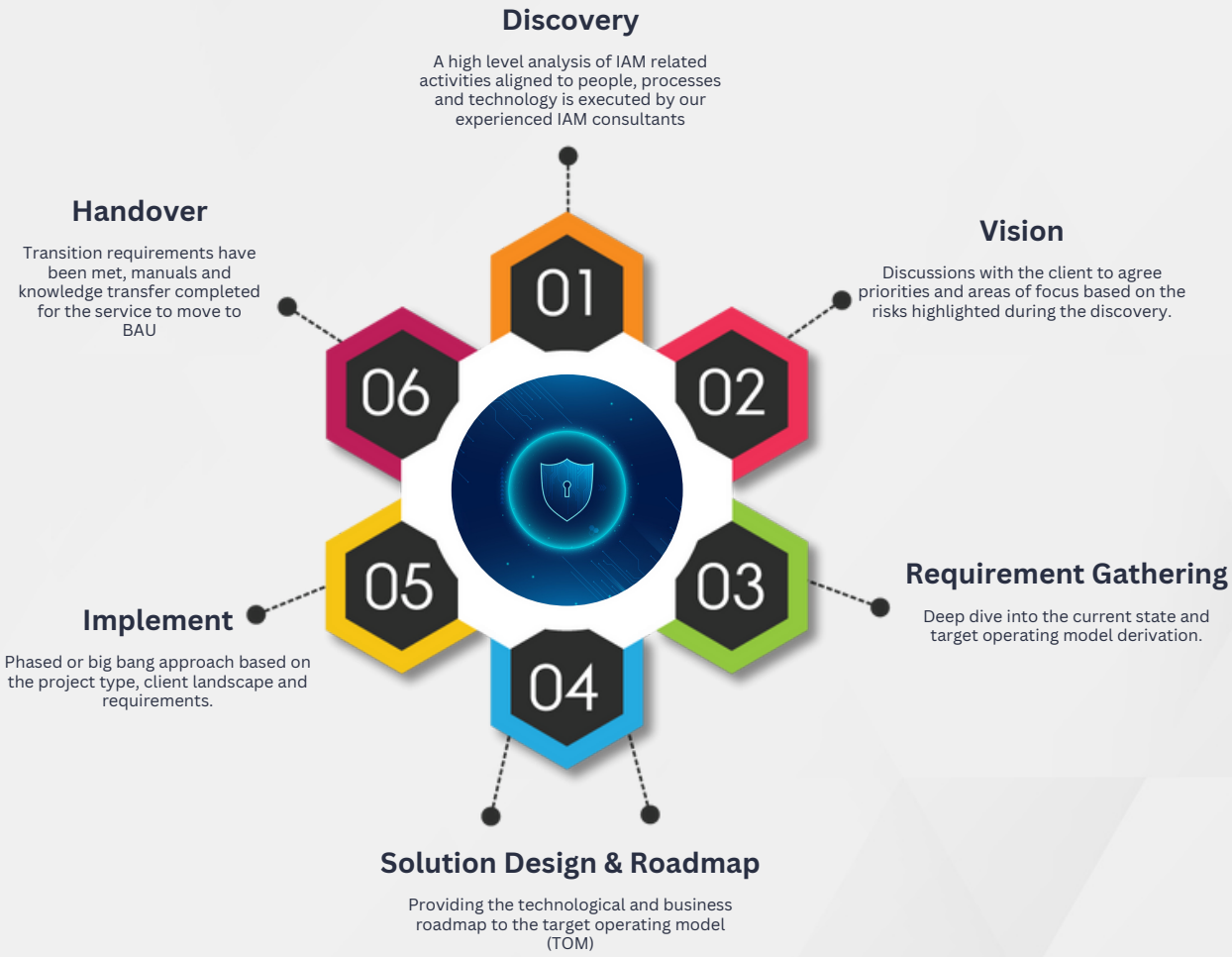
AltIAM
Let the Right One In

AltIAM – Why Implement an IAM Solution

Ensure Success - fit for purpose
The challenge for most organisations to implement and maintain an effective IAM Solution, requires the integration of the IAM Service Components and the business values, objectives and governance.

The starting aim is to ensure we have set the road to best practice to a security-first Zero Trust Policy.

Our IAM subject matter experts have created a methodological approach to ensure that the deployment of your IAM solution is the best fit option for your company. Our solution won't try to force your company into a one-size-fits-all mould, which some software solutions will try to do.



AltIAM - The DART Approach

Our IAM solution starts with our DART process.

Our IAM subject matter experts have created a methodological approach to ensure that the deployment of your IAM solution is the best fit option for your company. Our solution won't try to force your company into a one-size-fits-all mould, which some software solutions will try to do.

Discovery
A high-level analysis of IAM-related activities aligned to people, processes and technology, this phase will include understanding business vision, governance and additional requirements for an IAM solution will be captured.

Assessment
An assessment of your business' current identity process, practice and systems and provide a gap
analysis to a reference IAM solution maturity level.

Recommend
This covers solution designs and a roadmap for achieving the desired operating model from technological and business objectives

Transform
The implementation of an IAM solution, covering the deployment of Access Management, Governance, Provisioning and Privilege Access Management.

Identity Access Management
"Let the Right One In"

altIAM
Let the Right One In

AltIAM – Best Practice

The following diagram details the altIAM approach to the deployment and implementation of an IAM Best Practice Solution.

AltIAM Best Practice

Your organisational IAM solution will be shaped by your business needs and visions. The altIAM goal is to help your business be cybersecure, so you only “Let the Right One In” to your digital estate.

- **Perimeter Defence** — A defined first line of defence
- **Centralization** — Centralize identity management
- **SSO** — Enable single sign-on
- **Filter** — Enable conditional access
- **MFA** — Enforce multifactor authentication
- **Roles** — User role-based access control
- **Least Privilege** — Limit privileged accounts
- **Monitoring** — Active identity monitoring

Identity Access Management

"Let the Right One In"

altIAM
Let the Right One In

About Us

AltIAM is a division of Altiatech Ltd, a Managed Service Provider (MSP) offering a range of Information Technology and Communications (ITC) and cloud services with customers in the private, public and not for profit sectors. The company has Microsoft Gold Partner accreditation. Our customers reached out, to help them to implement solutions such as Single Sign-On (SSO) and Multi-factor Authentication (MFA). As we tried to implement these solutions, we found that these were being deployed in a siloed and piecemeal approach. As a result, we found that their IAM Solution maturity assessment gap was significant, thereby increasing the risk of a successful cyberattack. Therefore, with our IAM Solution subject matter experts, we developed a companywide IAM solution service.

Our services include as required, using tools such as SSO, MFA plus Privilege Access Management (PAM) to help our customers to implement an IAM solution deployment that achieves optimal IAM Solution maturity assessment, including vendor selection as required. In addition to implementing an IAM solution, we offer 24 x 7 technical support and for those organisations who require the operational and commercial flexibility, we can provide IAM-as-a-Solution (IAMaaS) service solution.

Contact Us

AltIAM – Assess Your IAM Solution Maturity

You may have already begun your IAM solution implementation or are now considering your next steps to enhance your cybersecurity. We offer the opportunity for an assessment consultancy, typically up to half a day of your time is required.

Please visit www.altIAM.co.uk and complete a form to book a 20-minute call, to discuss how we can help you with implementing a tailored cybersecurity solution to ensure that you are only “Letting the right one in.”

+44 (0)33 033 25842

www.altIAM.co.uk

letmein@altiam.co.uk

London Office
6 Portland Business Centre
Manor House Lane
Dachet
SL3 9EG

AltIAM consultancy is to “Let the Right One In”. This comes from folklore, that vampires cannot enter a house unless invited. The challenge of the IAM problem space for organisations, is to ensure you “Let the Right One In.”

Identity Access Management
"Let the Right One In"