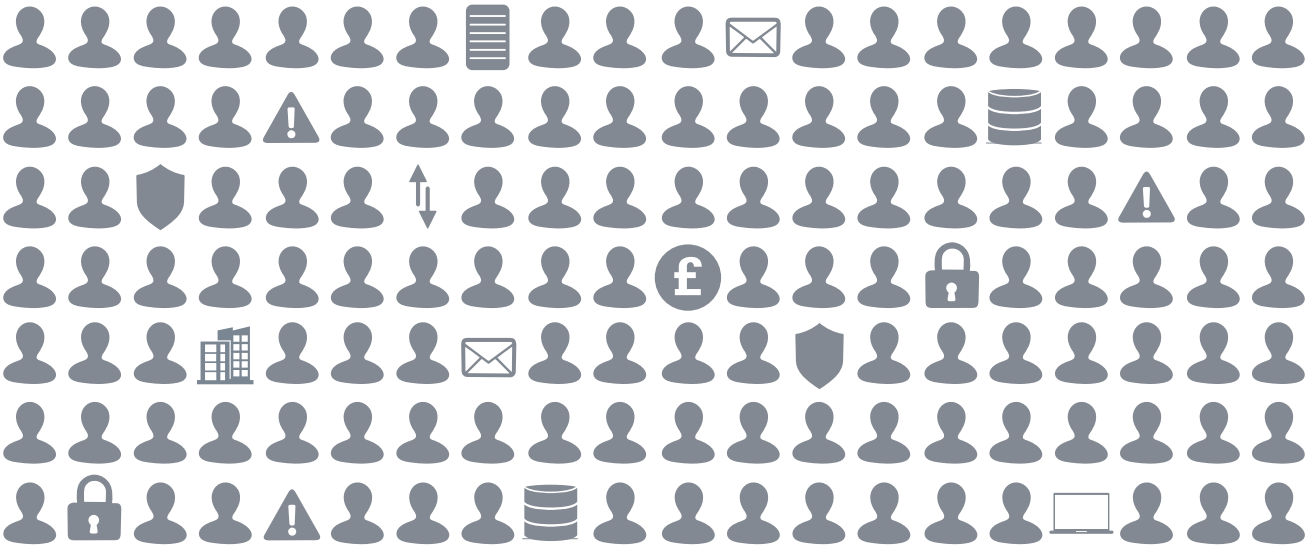
How to establish your functional requirements for an Identity and Access Management system

ilex International



INTRODUCTION

In order for organisations to determine the effectiveness and efficiency of their identity and access management (IAM) systems, they first need to assess the extent to which their deployed systems fulfil their functional requirements. Simply put, do these IAM systems do what is needed by the organisation and its intended users? It is therefore necessary and logical to establish the functional requirements before assessing the features and functions of candidate IAM systems.

Organisations face significant challenges securing access to their assets as customers, employees and agents seek to utilise mobile devices to carry out their business processes. Similarly, the utilisation of cloud services is predicated upon effective and efficient identity and access management systems. An organisation's business case to exploit the many advantages of permitting access to their assets by mobiles, BYOD or COPE devices, and/or the utilisation of cloud services must include an identity-based risk assessment. This assessment must determine the relevant controls to protect the organisation's assets and the users' privacy in the application context. The identified security controls form the basis of the organisation's functional requirements for the organisation's identity and access management system.

Functional requirements for an IAM system depend upon an understanding of several factors relevant to the organisation, stakeholders (including users) and application context(s). This and an analysis of the acquired data then allows for the production of functional performance and assurance requirements for an IAM system.

We categorise these interrelated factors into ten themes:

1) BUSINESS CASE

An understanding of the business problems and the rationale for organisations to introduce or revise an IAM system is fundamental. The need for an IAM system may be driven by a risk management and compliance initiative, an operational effectiveness or efficiency initiative, a business enablement initiative or possibly a combination of all three considerations.

An organisation may decide to minimise the risks to assets by instigating a change programme with an associated budget. Usually, a feasibility study estimates the stakeholders' costs and benefits to implement these business strategies and to sustain the controls over a predicted lifetime.

The decision processes for revising an IAM system should be articulated in the Programme Governance Framework between the direct users. This describes the participant roles, particularly the entity empowered by the programme sponsor, to make changes to consultation or decision processes or representative body membership.

The intended user community will not derive direct benefits for using the IAM system and an unacceptable user authentication method will have an undesirable impact on the users' objectives to introduce or revise an IAM system. Organisations need to consider the use of financial incentives or penalties, as well as educational material, to persuade users to manage their credentials as designed.

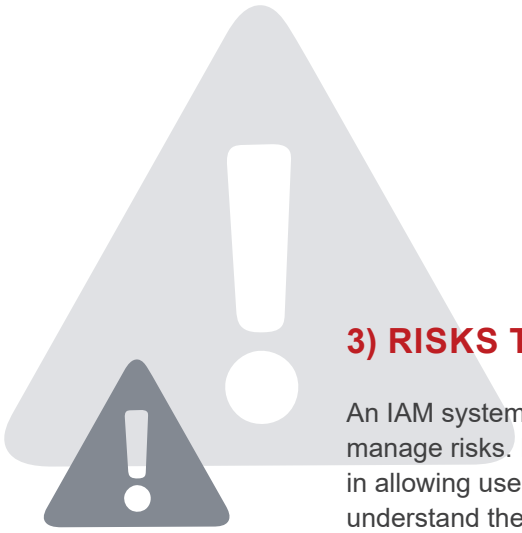
2) APPLICATIONS AND RESOURCES

Knowledge of the operations and technology platforms that underpin business processes, including mainframe systems, service-oriented architectures and the cloud, are essential as organisations migrate towards heterogeneous IT environments and distributed processing.

The locality of the information assets and the types of access, e.g. enterprise client or web, to the applications also need to be understood. Data and/or resources are available on the organisation's infrastructure, in the cloud or managed by a technology supplier. The types of access to these data/resources may include a specific client technology or the use of a web based application.

Organisations authorise employees, agents and contractors to create, modify and delete data according the established business operating rules. For example, dual control for payments and business processes when creating a bank account for a new customer.

These applications may include systems containing users' biographical data.



3) RISKS TO ASSETS/RESOURCES

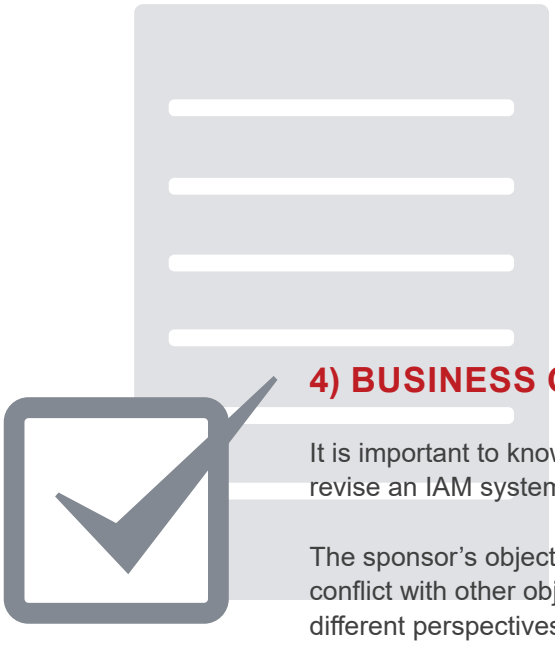
An IAM system is one of many controls introduced by organisations to manage risks. It is necessary to gain an understanding of the users' risks in allowing user access to an organisation's assets. There is a need to understand the range of risks on the business transactions in the intended usage environments.

Risks are normally identified by a risks assessment or audit review; however, use cases also offer the means to identify risks. In order to determine appropriate risk controls, a risk assessment should specify the assets to be protected, their value and vulnerabilities, acquire threat intelligence, ascertain incident probabilities and predict the likely impact on those assets in the event of a successful attack.

The introduction of new services (and different risks) to an existing operating environment are often overlooked by stakeholders. Invariably, operating environments may contain several applications/resources which may be accessed by users including systems administration personnel who do not have the relevant authorisation. Access to all assets and resources, including privileged accounts, should be assigned a risk grading (possibly in risk matrices) to ensure that authorisation policies are configured with the proportionate conditions.

The risk or risks' matrices should contain information on attack likelihood or compromise probability on a resource, the threat motivation, the vulnerabilities in the organisation's current operations, and information on compromises and their impact. Users may, however, possess different risk appetites and management strategies which should be agreed to manage identified risks and residual risks.

As a control measure, an IAM system forms part of the security architecture to minimise risks to assets. The impact of an IAM system failure needs to be determined for all stakeholders, including users who may be denied their entitled access to resources. Information is needed on the types of IAM system user deception attacks. Social engineering attacks on the user community and technology-based attacks need to be understood.



4) BUSINESS OBJECTIVES

It is important to know the sponsor's prime business objective to introduce or revise an IAM system.

The sponsor's objective to introduce or revise an IAM system could align or conflict with other objectives. Users in the same organisation may possess different perspectives on the risks to the assets or resources and may consequently want to pursue different risks management strategies to achieve their business aims.

For example, the marketing department may have a completely different view on the impact of an IAM system compromise on business operations to that of the Chief Information Security Officer. Nevertheless, it is essential to reach a balanced consensus on the controls needed to ensure the business operations are not interrupted or degraded, whilst simultaneously protecting the organisation's assets.

Equally, a reconciliation of objectives is needed when the operating environment involves many different organisational entities. Knowledge of the relationships between the users and the wider community together with an appreciation of any implicit sensitivity can support attempts to promote collaboration.

An understanding of organisational interests and benefits sought together with knowledge of their current issues is needed to determine the functional requirements for an IAM system or changes to access control protection.

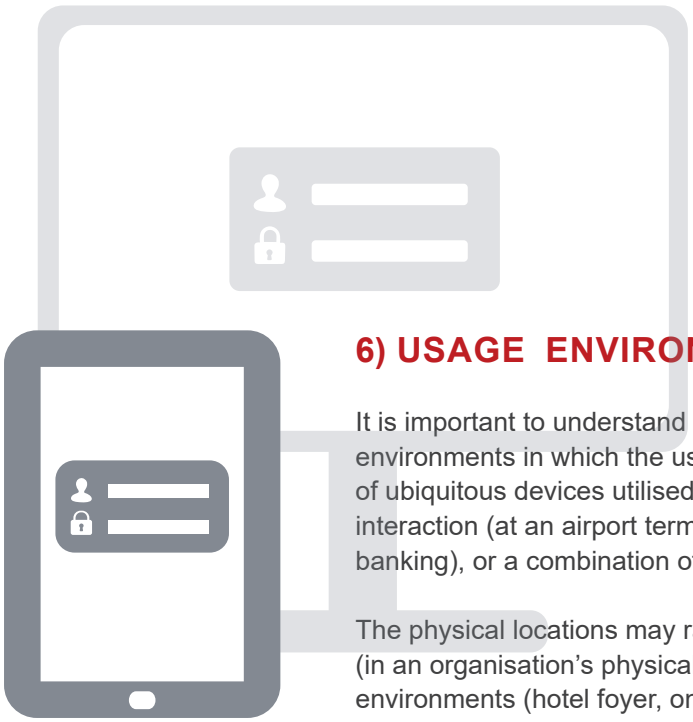
5) USER COMMUNITY'S CHARACTERISTICS

An understanding of the characteristics of the user community, such as customers, agents, employees etc., is essential in order to minimise usability issues.
The degree of reliance and acceptability of the IAM system may be based on existing relationships and perceptions of trust of organisations. The degree of trust between organisations and their customers, particularly where an affiliation has not been established, influences the social acceptability of some security mechanisms.

These issues may also reveal social attitudes towards using specific types of user authentication methods and costs (if any) to use the IAM system. Without trust between the interacting parties, some users may not use the IAM system as designed. Trust is further established from a contractual agreement or consumer protection legislation.

While security codes of conduct are an integral part of an employee's employment contract, an organisation's customers and agents may be subject to unacceptable liabilities in the terms and conditions for using the IAM system. These potentially outweigh any potential benefit or service proposition to the user.

An understanding of the varied characteristics of the user community may create advantages (and limitations) for utilising certain types of user authentication methods, particularly biometrics. It is important that the user authentication method does not exclude members of the user community. For example, it is not always possible to acquire fingerprint data, for authentication purposes, from all individuals.



6) USAGE ENVIRONMENTS

It is important to understand the physical and logical characteristics of the environments in which the user communities operate, including the types of ubiquitous devices utilised. User authentication may include face-to-face interaction (at an airport terminal kiosk), or a remote interaction (online banking), or a combination of both.

The physical locations may range from a secured physical environment (in an organisation's physically secured data centre premises), or to open environments (hotel foyer, on public transport etc.).

The physical location may impact the user's ability to operate the user authentication method, whether the device is ubiquitous, such as a mobile phone, or dedicated mechanism (specific type of One Time PIN generating pad). The environment may impact the ergonomic operation of these devices, cause usability problems or inhibit authentication data-capture for example, when a voice recording is done in a noisy office or café.

The extent to which a user population is able or willing to use a new device or process may impact the types of input devices and the nature of the IAM system's user authentication interaction. The regular usage of an IAM system may reinforce users' habits. Irregular usage of the mechanism is enforced by bad habits, and should be minimised.

The user authentication interaction may appear at the start of the user's task, during and/or at the completion of the transaction. The logic of where to place user authentication system interaction is dictated by how the user would habitually complete the task.

The similarity of user authentication methods, such as too many passwords, leads to confusion, errors or undesired behaviour which could include writing down identifiers and associated passwords on sticky notes and placing them on their desks. User inability to recall several complex passwords upon demand may result in frequent requests for resetting user credentials.

7) CONSTRAINTS

An understanding of constraints, ranging from technical limitations to social norms of the user community, is vital. An identity and access management system forms part of an organisation's security architecture, and the controls must be integrated to ensure that security controls remain effective.

Fundamentally, the funds and resources allocated by the organisation to introduce or revise an IAM system need to be proportionate to business incomes and risks. Laws and regulation may also place restrictions or additional tasks on stakeholder entities to demonstrate compliance.

The restrictions of the application contexts (including legacy systems), influences the proposition for an IAM system. The limitations and obligations specified in federated identity management schemes can constrain the configuration of an IAM system, ensuring interaction interoperability and reliability across the various security components.

An IAM system is limited by the ubiquitous technology available or utilised by the intended user community. Users may be unwilling to purchase specific devices, e.g. a smart card reader, not only from a cost/benefit perspective, but also from a lack of technical awareness.

Some user data, including personal identifiable information, needs to be exchanged between and credential issuing authorities and relying party service providers. The extent to which the customers in the user community believe that stakeholders will act reliably and securely with their private data, thereby safeguarding users' personal interests, needs to be realised.

8) ORGANISATIONAL POLICIES

Organisations create and maintain a range of policies, often derived from legislation.

Organisations' security policies are very relevant to the requirements for identity and access management systems. These security policies also define the processes and acceptable proof of identity evidence in the identification on new customers, employees and contractors. Organisational stakeholders must provide direction as to which entity determines the policies on the proof identity evidence, registration and enrolment processes.

Additionally, there may be other relevant policies which specify the general conditions for retaining and archiving data. These general conditions also apply to data relating the authentication of a user's access to resources. Knowledge of an organisation's policy for dealing with external miscreants or unauthorised access by employees or contractors is beneficial to aid understanding of the organisation's culture.

It is crucial to know how the different organisational policies influence decisions on the requirements for an IAM system and its deployment configuration.

9) PRIVACY PROTECTION LAWS

An understanding of the privacy laws of the relevant jurisdictions and their impact on data management, together with the necessary processes for an IAM system, need to be established.

The IAM system owner, as the data controller, needs evidence to demonstrate compliance with privacy, social accessibility and discrimination legislation. We acknowledge, however, that similar compliance factors could be relevant to other laws, regulations and corporate governance policies.

Some organisations perform their responsibilities to protect users' private data, by incorporating appropriate processes into their governance structure. Conversely, some heterogeneous implementations need the direction of a central or scheme body to set out the governance rules and security policies for using private data to identify individuals.

Organisations normally hold private data to link the identified person to a specific account or identifier maintained (normally in identity directories or databases), for carrying out human resource operations, such as salary payments. Biographical data may also be employed for user authentication purposes. All personal identifiable information may be considered as users' private data; however, the provisions of different privacy laws, together with their unique definitions and their specific impacts, require legal advice.

Organisations are encouraged by the authorities to perform privacy impact assessments. The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals, provide principles and guidelines on the protection of private data. Essentially, the principles assist determine the control processes necessary for the collection, use, maintenance, disclosure and protection of private data.

On 4 May 2016, the General Data Protection Regulation (GDPR) and the Directive was published in the EU Official Journal. While the Regulation enters into force on 24 May 2016, it shall apply from 25th May 2018. The Directive is in force from 5 May 2016 and EU Member States have to transpose it into their national law by 6th May 2018. While this regulation is regarded by some as overly complex and unnecessarily bureaucratic, an IAM system must generate audit data as evidence to enable an organisation to demonstrate compliance.

One of the most significant rules of GPDR relating to IAM systems is mandatory breach notification. The GDPR stipulates that organisations will have 72 hours to report security breaches to the regulators. The penalties for breaking this rule are significant, with potential fines set at up to four percent of an enterprise's annual global revenue.

10) MANAGEMENT DATA

Finally, it is necessary to understand the data required to perform periodic audit reviews, security investigations and compliance evidence for general operating purposes.

It may be necessary to establish those people utilising resources without appropriate authorisations. Management data is required in order to support a range of business purposes, ranging from resolving a customer user's access problems, to an online service, to the production of general statistics, such as user community churn rates.

An understanding of the retention period and measures for storing data which may be used for investigations or in court to meet legal or contractual requirements are also relevant here.

To find out more about the ten evaluation themes, download the full paper here.

ABOUT ILEX INTERNATIONAL

Ilex International is a European Identity & Access Management (I&AM) software vendor. Founded in 1989 Ilex offers a comprehensive solution including identity management (identity, rights and role management) and access management (authentication, access control, SSO, identity federation and card management). The organisation invests heavily in R&D, providing state of the art technology and services to a large international customer base across finance, defence, healthcare, government and retail sectors.

ILEX INTERNATIONAL

info@ilex-international.com
www.ilex-international.com/en/