Developing your business case for investment in identity and access management

ilex International

INTRODUCTION

Identity and access management (IAM) offers many business enhancement opportunities. This management discipline should not be regarded simply as a tool to repair technological problems.

Chief Information Security Officers (CISOs) often encounter a lack of organisational understanding and experience difficulties in communicating the business value proposed by an IAM project. Historically, much emphasis has been placed on technical enhancements which did not appear to directly address business objectives or align with IT strategies. Organisational stakeholders are, justifiably, very cautious in prioritising IAM initiatives and committing scarce funds into IAM projects which do not demonstrate clear business benefits from the outset.

Commonly, narrow IAM solutions with limited capabilities have been deployed by organisations to fix a specific access control issue, e.g. introducing Two-Factor Authentication (2FA), to enhance existing user authentication methods. These technology-focused deployments, however, engender organisational mistrust in IAM projects to deliver capabilities that fulfil business needs. Such efforts also bring obstacles, such as redundancy costs, to organisations attempting to develop a coherent IAM strategy for managing identities and access privileges for employees, contractors, agents and partners in an evolving business world.

CHALLENGES

The challenges of developing a viable and robust business case for IAM investment are exacerbated by the complexity of system ownership and responsibility for IAM initiatives in an organisation. Organisational structures also hamper efforts to define an IAM governance framework or obtain multi-stakeholder agreement to allocate budget for an IAM project. Executive sponsorship, i.e. an IAM champion, appears to offer a viable alternative to a robust business case.

Ilex International recommends that organisations pursue a business-centric approach to managing digital identities for the authorised users' access control to information assets and resources. IAM projects must, therefore, focus on fulfilling stakeholders' business objectives. A business case for investment in IAM must also involve consultations with all relevant stakeholders, internal departments and where relevant, external entities, to enable the identification of business needs, business constraints, risks and most importantly, business benefits.

Before we present our business-centric approach to IAM, it's important to examine some of the difficulties associated with certain types of IAM business cases. The drivers for instigating an initiative to develop a business case for an IAM project originate from four main business challenges:

1) RISKS REDUCTION DRIVER

Increasing fraud and associated losses or changes in risks profile, from a discovery of vulnerabilities, threat intelligence and possibly attitudes towards risk appetites, could result in initiatives to revise access controls to an organisation's information assets.

An internal audit report may reveal security flaws, e.g. active user accounts of ex-employees, which require attention by the IT operation department. This discovery often results in the organisation's IT operation department absorbing the costs to resolve the identified audit discrepancies, or revert to the executive for additional funding to repair what is perceived as a technical problem. Such funding requests for technological repairs are viewed by many executives and other departments as a "cost" to the business which must be reduced to its lowest possible level.

An IAM project funded to repair discovered security problems, for example the recertification (or reconfirmation) of the privileges assigned to all employees, is an ongoing management challenge and should not be viewed as a single one-off isolated technical activity.

The organisational perception of IAM projects, based solely on addressing risks, therefore, is that IAM is a cost to be controlled rather than a business capability in which to invest. The management of business risks however, is a business activity. Knowledge of who has access to which organisational assets to perform various business activities informs risk management processes, e.g. periodic risks assessments.

2) REGULATORY COMPLIANCE DRIVER

Regulatory authorities, particularly in the finance and health care industries, have increased their regulatory requirements to ensure that organisations closely manage and control user access, particularly to ensure segregation of duties. Also, the threat of sanctions and/or fines and the possibility of exposure in media for failure to comply with privacy legislation by authorities such as the Information Commissioner's Office, necessitates that an organisation's executive committee issues a mandate and provides investment, not only to comply with the regulatory requirements but also to generate relevant evidence to support claims of compliance.

Again, organisations view these regulatory compliance projects as a cost to business to be reduced rather than a strategic IAM initiative to demonstrate significant benefits of regulatory compliance through:

- Quality improvements by preventing errors or failures before they occur
- Improvements in efficiency by embedding efficient compliance processes into business operations as opposed to delegating such activities to a separate department
- Facilitating trust and brand loyalty which demonstrates the importance of compliance to an enterprise's customers and business partners
- Competitive differentiation by consistently demonstrating active compliance initiatives in comparison to unconvincing efforts by an organisation's competitors

Nevertheless, an organisation's executive committee is unlikely to initiate long-term IAM initiatives based solely on the need to comply with regulations while minimising costs. Therefore, strategic IAM initiatives based solely upon risks reduction and compliance drivers need to be complemented by other tangible business benefits.

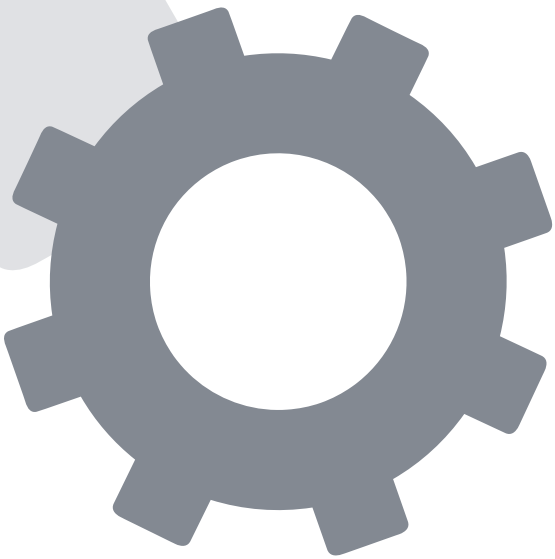
3) PRODUCTIVITY IMPROVEMENTS DRIVER

Searching for costs savings is unlikely to reveal costs savings in managing IAM activities because any meaningful costs reduction, as a prime objective for an IAM project, has to identify inefficient processes. Additionally, organisations are not going to introduce new processes if they are not already carrying out these activities prior to the project and are deemed, therefore, to be of little business benefit.

Concentration on examining existing processes to identify those activities which are not being implemented in an acceptable manner may facilitate better use of administrative resources. The aim should be to set objectives to ensure that administrative resources become more productive, which in turn could improve the efficiency of IAM activities. For example, building automated IAM workflow processes to create an employee digital identifier, allowing access to resources such as corporate-owned, personally enabled (COPE) mobile phones, or the setting of specific access privileges for organisation roles/applications can be delivered to organisation entrants more efficiently than through manual processes.

The complexity of processes involved in setting up entrants to work in an organisation together with other digital identity life-cycle management activities appear to correlate to the size of organisations. These enrolment processes often involve many individuals with specific functions/roles in different departments, which range from personnel departments, to IT systems administration.

While potential productivity gains may be realised over a protracted period, e.g. 5 years, it is difficult to construct a viable business case based upon return on investment (ROI) calculations because costs savings and, particularly reducing employee numbers, are rarely realised. It is also difficult to justify potential productivity gains when the costs of the IAM project itself need to be accommodated.



4) BUSINESS ENABLEMENT DRIVER

The introduction of new business capabilities is a compelling driver to many executives for establishing a business case to enhance IAM capabilities. The articulation of introducing new business capabilities are easier to explain to executives than potential productivity gains, minimising of risks and/or reduction of operating costs.

For example, enabling peripatetic sales staff to have access to specific organisational data from mobile devices should align with strategic business objectives to increase sales. Similarly, by introducing this type of IAM capability it may create competitive advantages or enable your sales employees or agents to cross-sell other products or services to existing customers.

In most circumstances, for every business development strategy, there will be a corresponding need to improve employee, agent, contractor, and partner and customer access to data and/or resources. Visibility of who is accessing which information systems and whether these users possess the appropriate level of authentication and authorisation is essential for effective business management.

Therefore, Ilex International believes that organisations should pursue a business-centric approach, because the business values are articulated in business terms and the success of the IAM project is related to the fulfilment of stakeholders' business objectives. The business' requirements for an IAM system may then be expressed in terms which reconcile directly with the stakeholders' objectives, i.e. requirements are not technology driven but business driven. The effectiveness and efficiency of candidate IAM systems may then be evaluated against business objectives rather than technological assessment criteria.

A BUSINESS-CENTRIC APPROACH TO DEVELOPING AN IAM BUSINESS CASE

The prime aim of an IAM business case is to demonstrate to executive decision-makers that investment in an IAM programme, containing a high-level IAM roadmap linked to business capabilities, is a valuable business investment.

Below we have outlined our business-centric approach to acquire the relevant data in order to construct an efficacious IAM business case. The Ilex International approach consists of the following major activities to:

- Acquire an understanding of the organisation's business processes in terms of their purposes, values and benefits sought
- Identify, consult and engage with stakeholders to ascertain their functional role in the organisation's business processes and their specific business objectives
- Gain an appreciation of the characteristics of organisation's target user communities (including customers). This appreciation includes knowledge of their liabilities and responsibilities, their operating environments, their ubiquitous devices and their attitudes towards the use of technology to fulfil their operational tasks
- Acquire an understanding of the organisation's policies (not just security policies) which are derived from regulatory or other external directives
- Acquire an understanding of the constraints in terms of budgetary, social norms and practices and technological limitations (e.g. legacy systems) of the business operating environments
- Acquire an understanding of the status of existing IAM capabilities and identify vulnerabilities, issues and costs
- Determine and define the scope, high-level requirements as part of a constructing a strategic IAM roadmap
- Assess the operational feasibility, estimated costs and most importantly business benefits for an IAM project
- Determine how to utilise the organisation's decision-making processes to ensure that the business case is articulated using the appropriate terminology and that the methodologies practised by the organisation to implement business change are incorporated into the business case

While it may be desirable to approach to produce a comprehensive business case for strategic investment in IAM, there are situations where expediency is paramount and selection of IAM capabilities do not allow for such analytical rigour. An integrated collection of foundational IAM components offers a migration path to match an IAM strategy under development.

In conclusion, organisations should seek solutions from suppliers which have a demonstrable track record of deploying an integrated set of foundational IAM technological components. This strategy enables an organisation to manage the identity and access of all types of user communities (e.g. customers, employees, contractors, agents, partners etc.) as its business needs evolve and also to respond quickly to an organisation's business needs.

ABOUT THE AUTHOR

Dr. Anthony Palmer, UK Principle Consultant, Ilex International

Dr. Anthony Palmer has a Ph.D. in Information Security, awarded in December 2015, on Methodologies to select systems for Automated Personal Identification from Royal Holloway University of London. He is also a member of the British Standards Institute's IST/33 WG5 Security Techniques-Identity Management and Privacy Techniques Committee and has been a Full Member of the Institute of Information Security Professionals since 2007.

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/