Making the business case for identity and access management

Executive summary

Your organisation's Identity and Access Management (IAM) solution is one of the cornerstones of its digital architecture. Nonetheless, significant expenditure on your IAM solution will require consent from the business. This whitepaper discusses the themes that will be common to most organisations considering the business for investment. These are: reduce the cost of your identity administration; improve your users' productivity and satisfaction levels; monitor and enhance the impact of your services subscriptions; and ensure information security and compliance.

Document Date: September 2020

Author: Josh Howlett

Introduction

An organisation's Identity and Access Management (IAM) solution is one of the cornerstones of its digital architecture. As the gateway – and gatekeeper – to your users' services, from the CEO downwards, it is essential to your digital estate.

Improvements to your IAM solution can sometimes be delivered through incremental change. But more significant expenditure on transformational change will require consent from the business, which will consider this investment based on the business case.

The specifics of the business case will be different for every business. But, as a general-purpose capability needed by almost all organisations, there are common themes. This whitepaper discusses these themes as an aide to understanding and developing the business case for investment in IAM.

Reduce the cost of your identity administration

Almost all digital systems require some concept of their users' identities and their permissions. Rather than have each system manage these separately, an IAM solution enables the organisation to centralise their management. This is sometimes called the "single source of truth for identity". It is important because it is much less costly to maintain a single source of data than multiple sources.

The extent of this saving depends on the solution's ability to model the business' IAM landscape: the organisational structure, its users, their services, their permissions; and, most importantly, the processes surrounding these. The more faithfully it can reflect these, the more able it is to replace costly manual systems.

For example, an IAM solution will allow users to be organised into groups. Users can then inherit access permissions that have been assigned once to the group, rather than assigned to each user individually, reducing the administrative burden. These objects can be organised hierarchically, reflecting the organisation's structure; and responsibility for their management delegated to the appropriate organisational units. At the same time, transparency, accountability, and consistency can be maintained through centrally managed policies, reporting, and auditing.

The most effective IAM solutions allow these objects to be created, updated, and removed "just in time". These processes can be triggered by data and events from upstream sources, such as human resources, finance, and customer relationship management systems. The goal is that the IAM solution can orchestrate the end-to-end management of the lifecycle of every identity based on business events (such as a new client; a departing employee; or an acquisition), with the minimum level of human intervention.

Improve your users' productivity and satisfaction levels

Increasingly, businesses are sourcing their services from third party providers. Most of these services will require the user to authenticate. But this creates a barrier to access if the user is required to provide authentication credentials; and this is barrier is elevated further if each of those services require different authentication credentials. Not only must the user manage these credentials, but the business also needs systems to issue and revoke them; for example, if a user forgets a password or leaves the organisation.

This creates new layers of administration that frustrate users and those tasked to support them. And while the helpdesk is processing the user's request, the business is paying for a service that isn't being used, and the user can't use the tool they need to be productive.

An IAM solution solves these problems with single sign-on (SSO). This means a user only needs to authenticate once, using a single credential provided by the organisation, to access all their services. Fortunately, most services now support SSO; but this support is not ubiquitous, particularly for legacy applications. The most effective IAM solutions will provide features that mimic SSO for these cases by, for example, synchronising passwords between the IAM solution and the legacy applications.

By empowering your users with effective IAM, you can improve their productivity and enhance their experience of your digital estate.

Monitor and enhance the impact of your service subscriptions

As the diversity and number of services and providers expands an increasing proportion of IT expenditure is spent on subscriptions. This expenditure usually falls within highly scrutinised OPEX budgets, and so it is important that the business can monitor and assess its impact.

Service providers will usually provide usage data, but the metrics and presentation will be different between providers, making comparison difficult. The reports may also change over time, making historical analysis harder; and for compliance reasons, it may be impossible to attribute usage to specific users (this can be useful, for example, for recharging costs internally). Finally, these reports are often predefined, precluding customisation that might yield organisation-specific insights.

The IAM solution, on the other hand, is controlled fully by the subscriber. Reports can be customised d generated when needed, enabling like-for-like comparison of usage between service providers. Changing patterns of usage can be identified and attributed to individuals or groups of users: licensing requirements adjusted to reduce costs; heavy users identified and charged. Finally, future procurements can be designed around data rather than conjecture.

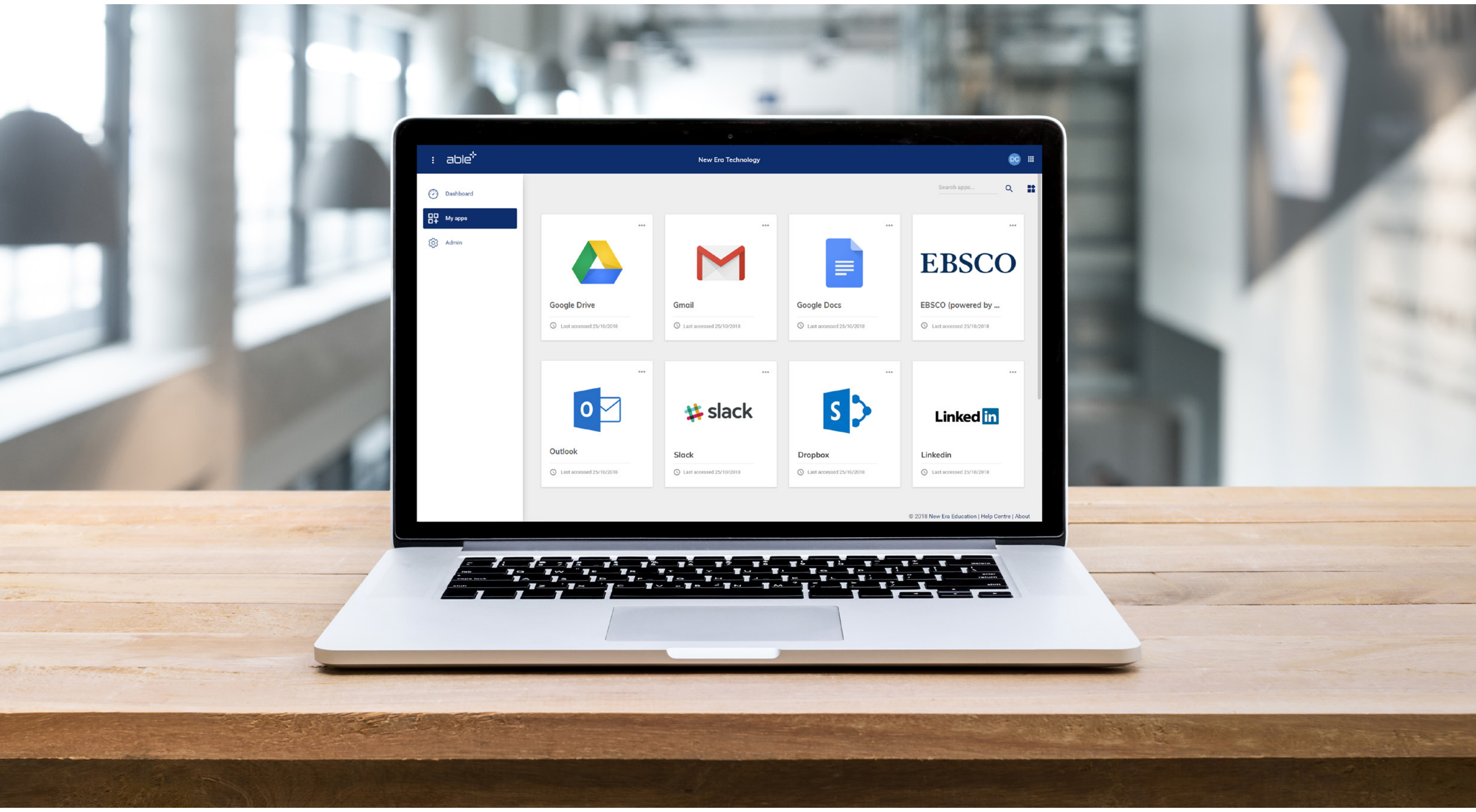
Ensure information security and compliance

Identity and access management is sometimes described as “providing the right access, to the right users, at the right time”. It sounds simple but, if the IAM solution is not performing correctly, it might give the wrong access to the wrong users. There’s never a right time for that. Consequently, IAM is considered a key information security control and, as such, is fundamental to any organisation’s security architecture and strategy.

In the best-case scenario, the impact of a poorly performing IAM solution on the business might be relatively benign. In fact, it may go unnoticed for a considerable length of time. For example, a benign and well-intentioned user is unlikely to notice that their permissions have been accidentally elevated, perhaps owing to a configuration error. In this scenario, the elevated privileges usually only reveal themselves when the user performs an operation that is normally reserved for more highly privileged users, potentially with highly damaging consequences, such as the accidental distribution of customers’ personal data.

The severity of information security incidents can be far more serious if malign actors are involved. Such actors will actively seek out weaknesses within the IAM solution, and then leverage these to acquire unauthorised access to the target systems. A compromise of the IAM solution itself can yield control of swathes of the business’ digital estate to the attackers, with potentially existential consequences for the organisation.

Managing and mitigating these risks is a core purpose of many compliance regimes, whether those are internal policies, third-party accreditation schemes, or regulatory or statutory obligations. The most effective IAM solutions, therefore, will not just provide the tools needed to implement access control; but also the capability to assess that these tools are being applied in ways that actually deliver compliance with these regimes. This greatly increases the likelihood that a weakness can be identified and remedied by the business before a security incident exposes it to a much wider audience.



03334 559424

info@neweratech.co.uk • neweratech.co.uk