



# Connecting, protecting, and perfecting the digital business

## Executive summary

Identity and Access Management (IAM) is a highly transformative digital capability. But making the business case to invest in something that is not well understood by the business can be a real challenge. In these circumstances, it can be helpful to have a strategic framework that sets out the main issues for the decision-makers. This paper introduces the IAM Transformation Triangle and explains how it can be used to develop the strategy and case for investment in IAM. Subsequent papers in this series explain how Able+ can help the organisation implement this.

# Introduction

The digital business is formed from two types of digital capability.

Digital capabilities that have an equivalent in the non-digital context. For example, a retailer having an e-commerce presence and bricks-and-mortar outlets. The familiar non-digital equivalent (the outlet) makes it easy to understand the digital capability (the e-commerce presence) and so value it.

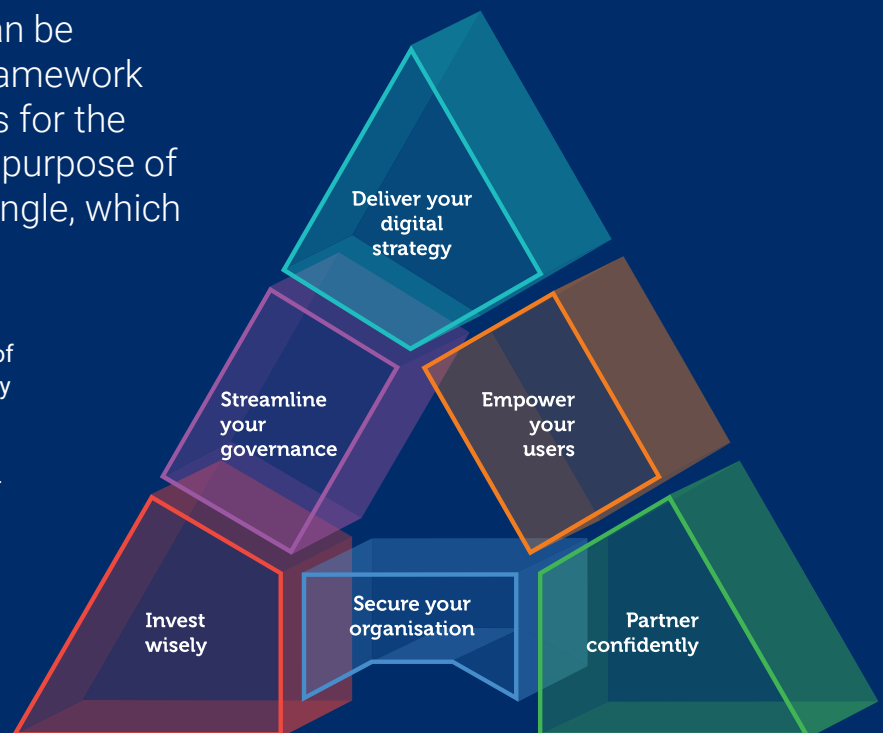
Digital capabilities that lack an equivalent in the non-digital context. This is because they address needs that are uniquely digital. This can make them harder to understand and therefore value, until they become ubiquitous. For example, 22 years ago the capabilities, impact and usage of Google was a tiny fraction to what it is now.

Those capabilities in the second category often offer the greatest value. They enable the transformative change that the business needs to flourish, freed from the constraints of the analogue era.

Identity and Access Management (IAM) is an example of one of these highly transformative capabilities. But making the business case to invest in something that is not well understood by the business can be a real challenge.

In these circumstances, it can be helpful to have a strategic framework that sets out the main issues for the decision-makers. This is the purpose of our IAM Transformation Triangle, which covers six key benefit areas.

The goal of this paper is to describe some of these benefit areas, without reference to any product, to facilitate the development and implementation of an IAM strategy. In subsequent papers we'll discuss how Able+ can help within each of these areas.





## Deliver your digital strategy

No business can afford to be without a digital strategy. It explains how it plans to acquire and use different digital capabilities to support the business' objectives. As we'll see in this and subsequent papers, an effective digital strategy requires an IAM solution that is deeply embedded within the business. As a result, the IAM solution will have many touchpoints across the organisation.

But no business will substantially change its ways of working to suit an IAM solution. It's therefore essential that the IAM solution can adapt to the organisation's prevailing policies, processes, and practices. Otherwise, the wider organisation will resort to less effective or less efficient ways of achieving their goals – or give up on them.

When selecting an IAM solution, therefore, resist a purely technical, feature-led approach. Instead, seek to understand the less malleable aspects of the organisation and consider how the IAM solution needs to adapt to those. Don't allow the IAM solution to dictate your organisation's strategy.



## Empower your users

In our own day-to-day digital experiences, we frequently deal with the consequences of inadequate IAM. For example, in the tiresome regularity with which we are required to authenticate; the time-consuming process of resetting a forgotten password; and, for the unfortunate, the sometimes-profound impact of identity theft.

These costs to user are usually obvious. But there are many other costs that weigh on the business. These are usually opportunity costs: missed opportunities to do something better that might save the business time, money or create new value. Examples include:

- the use of data from sources such as HR or customer databases to seamlessly create, update or revoke user accounts for employees, clients, and partners as their relationship with the business changes over time, so that these people can get what they need, when they need it
- the provision of single sign-on (SSO) to employees, allowing them to use a single password to access all their applications; or
- the central management of access permissions for customers to their service entitlements across a broad product portfolio, reducing the administrative effort needed to prevent unauthorised access

By empowering your users with effective IAM, you can improve their productivity and enhance their experience of your digital estate. In making the business case, understand and explain how an IAM solution will achieve this in the context of your business.



## Secure your organisation

IAM is a key requirement of information security. There are many facets to this, which will vary between organisations, but key drivers often include:

- the prevention of unauthorised access
- the facilitation of compliance with GDPR, by providing robust controls around access to personal data; or
- the need to meet audit requirements, including regulatory compliance within some sectors (which can stipulate IAM-related functionality)

Everyone would agree that having robust security is essential. But it can be difficult to agree which costly security capabilities are really needed to achieve this; and how these investments might offset potential losses to the business from theoretical security incidents that may never happen. This can make it challenging to derive the business case from a cost/benefit analysis.

As a result, security-led business cases often put the emphasis on compliance. That is important but it can be perceived as “box ticking” if it is not clear how that leads to business value. Conversely, it can often be straightforward to estimate the gains that come from empowering your users through greater efficiencies and so forth.

Therefore, when making the business case, try to link security features to functionality that also empowers users. For example, SSO is great for users because it makes their experience of the digital estate more seamless; and it also helps security by reducing the number of passwords. Remember that many security incidents result from poor user choices, such as writing down passwords. By making your digital estate more user friendly, you can encourage more secure user practices.

## Streamline your governance

It should be clear that, even from this brief list of examples, IAM will have touchpoints with almost every part of the business. An effective implementation will usually be embedded operationally within many if not all the key business systems.

Consequently, delivering a successful implementation is not a one-time deployment activity that can be delegated to a single business unit to take to fruition. It requires an on-going collaboration across the organisation to ensure the relevant business units are pulling in the same direction.

This is usually achieved through an internal IAM governance function, having representation from these stakeholders and oversight of the organisation's IAM-related policies and processes. Exactly what form this will take will be different for every organisation.

Therefore, in making the business case it is important to explain how the IAM governance will operate within the organisational context. Similarly, it is essential that the IAM solution has the technical features needed to align with the governance model. If neither of these are understood, it is likely that the IAM solution will fail to deliver against expectations.

## Enable your business

In this paper we have identified IAM as a strategic capability that is critical to effective digital delivery. We have discussed the key areas to consider when developing an IAM strategy and making the case to invest in an IAM solution. In the other papers in this series we will discuss how Able+ delivers against these areas. We hope that this will help you understand what you need in the context of your organisation.

01273 201 700

[info@neweratech.co.uk](mailto:info@neweratech.co.uk) • [neweratech.co.uk](http://neweratech.co.uk)