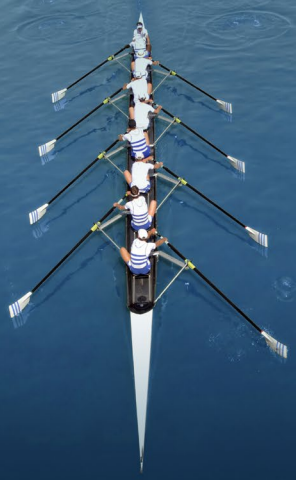

Secure and streamlined

Identity and Access Management for a Big 4 bank

Customer success story:

> Overview

When reviewing its security operations, a Big 4 bank pinpointed Identity and Access Management (IAM) as a major focus area for improvement – viewing it as vital for keeping the bank and its customer information safe, maintaining an acceptable risk posture, meeting regulatory compliance requirements in regard to privacy and security, reducing audit items, and uplifting its staff user experience.

> Challenge

The organisation needed a technology tool to deliver this vision – one that would govern the levels of access provided for each staff identity, without making its employees go to any additional effort in their daily activities. The bank's internal identity landscape was maintained by discrete teams spread throughout the business, rather than having a holistic identity governance and administration system that seamlessly gave the right people access to the right information at the right time, without any unnecessary delays.

> Solution

The bank selected SailPoint IdentityIQ, and engaged KPMG as their implementation partner, due to the team's experience in executing IdentityIQ deployments at a large scale. The bank now has an integrated and streamlined IAM system, which has delivered a significant uplift in security and productivity, as well as being simple for staff use.

Having well-managed controls around employee access to systems is vital for financial institutions. In this technology implementation, KPMG worked with a major Australian bank to ensure every change was an opportunity to make life simpler for staff, not more complex, and as a result efficiency and productivity are up.

When one of the four largest financial institutions in Australia with billions of dollars in deposits and mortgages needed to step up its Identity and Access Management strategy for its 50,000-plus staff, it sought out the right technology solution, and the right implementation partner, to make sure it was deployed efficiently and effectively.

The bank pinpointed its Identity and Access Management (IAM) as a major focus area, viewing it as vital for keeping the bank safe, maintaining an acceptable risk posture, meeting regulatory compliance requirements, reducing audit items and uplifting its staff user experience.

It needed the right IAM technology tool to automatically govern the levels of access provided for each staff identity, without making its staff go to any additional effort. Employees in the main organisation, and also the bank's subsidiaries, require access to different systems, such as finance, payment and training systems. Manually controlling this is arduous.

Dispersed security management

The bank's internal identity landscape was largely maintained by discrete teams spread throughout the enterprise. This had resulted in disparate, manual and often immature processes being relied on to manage the identity lifecycle (consisting of provision, de-provision, updating and revalidating) of internal staff members and external vendors.

© 2018 KPMG, an Australian partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. Liability limited by a scheme approved under Professional Standards Legislation.

The organisation outsources a large part of its IT management, which means that if employees want to be granted access to a server, they have to create a 'job ticket' and wait for assistance. This disparate approach impacts the ability of everyone to be productive, however when the SailPoint IdentityIQ access request capability is enabled, this process will increase user efficiency via automation.

A holistic approach was needed

The bank needed an integrated, overarching identity governance and administration system that seamlessly gave the right people access to the right information at the right time, without any unnecessary delays.

Of paramount importance was a technology platform that had an intuitive user interface and easy navigation. The solution had to be understood quickly by a general 'business user'. Factors such as the User Interface, Workflow, Lifecycle and Bulk Load capabilities were vital.

Evaluation and decisions

The bank undertook a formal vendor evaluation process to identify the most appropriate solution for these needs. It was looking to:

- simplify reviews of user access
- improve the efficiency of requesting and removing of access to assets
- implement a role based access request, review and control tool
- satisfy regulatory and compliance control requirements.

The bank determined that SailPoint IdentityIQ would meet its demands, and engaged KPMG to work closely with them to implement and tailor the solution to fit their complex requirements.

The organisation benefited from KPMG's extensive experience with large scale deployments, the ability to have onshore resourcing, and immediate access to expertise. They also gained the benefits of customised training in SailPoint IdentityIQ.

The engagement began in mid-2015 and is set to continue throughout 2018 as more uses are identified.

Connecting the dots

The organisation needed to connect countless systems to the SailPoint IdentityIQ technology – for example its Microsoft Active directory. This directory stores a number of specific identity attributes, all correlated with their technology user name, password and email address information.

With SailPoint IdentityIQ, that identifying information can be automatically provisioned or de-provisioned to access different areas of the business, according to needs and authorisation. For example, offering one employee access to finance, trading or invoices, but not to other areas.

Providing for the employee lifecycle

A key requirement was a system that was capable of providing for the employee lifecycle. With SailPoint IdentityIQ, the bank now has seamless employee lifecycle management – starting from when a new starter signs on with the organisation, throughout their tenure, to when they leave the company.

For example, new employees will be allocated with an email address, a network account, and access to the appropriate parts of the server. Through SailPoint IdentityIQ, all access can be managed provisionally, quickly granted or removed as required.

If an organisation isn't set up for this level of accuracy, the ramifications can be serious. In one example at a European bank, an employee in settlements, responsible for reconciling trades, was promoted to be a trader, but their access to settlements was not removed. This is known as a 'segregation of duties violation'. In that scenario, the employee took the opportunity to engage in rogue trading, costing the bank significantly.

© 2018 KPMG, an Australian partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. Liability limited by a scheme approved under Professional Standards Legislation.

With SailPoint IdentityIQ, as soon as an employee changes roles or leaves the organisation, non-authorised access is immediately and automatically blocked.

A streamlined system

The bank's intent was to implement an enterprise class IAM system that provided the right security, while also making it easier for employees to get the right access to the right systems, at the right time.

With SailPoint IdentityIQ, this has been achieved by consolidating and centralising technology, processes and identity service ownership.

Since implementation, the bank has experienced an enhancement in its ability to manage IAM and security, and has also had a significant uplift in day-one productivity for new staff. Other key advantages include:

- automation of cumbersome processes
- preventative and detective controls applied
- visibility into user access entitlements and privileges
- requests can now be submitted and tracked via a central interface (not across disparate platforms/locations)
- the ability to identify and correct separation of duty violations as part of the user access reviews process
- time for new user account creations (network login) has reduced by 95 percent. For example, it used to take 3 days for a new starter to be set up online, now it takes half a day. It previously took 2 days to gain access to a system, it now takes 2 hours.
- leavers' access is now disabled automatically (as per their end date within the linked HR system)

Experience counts

Experience with large scale deployments and a strong on-shore presence is really important when implementing a technology change of this scale. The bank needed a partner that had the strategy and experience to do this, but could also be agile and adaptable throughout the process.

The KPMG team had already assisted two major banks and a smaller bank with this process, so was able to bring the deep experience and insight needed for success.

The bank's team delivered a strong change management strategy, working with agility and adaptability to implement new ideas along the way, and were also able to bring people along the journey to enhance engagement and success.

Lessons for the future

By working so closely with the bank, KPMG saw that it had an impeccable approach to the change management process that added to the success of the project.

While the transformation had security at the core, KPMG, along with the bank, concentrated on the positive benefits to their employees, and the efficiency gains. The bank implemented great internal marketing to ensure all employees knew about the change, how to adopt it, and the benefits, which meant staff were ready and willing to take it on.

The KPMG team also saw the benefit when different performance units across the bank understood what the new technology could do, then were forthcoming with suggestions for even more ways to use it and to improve it. This is where the team's agility and adaptability came into play along the way, as they tested and implemented new uses of the technology.

© 2018 KPMG, an Australian partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. Liability limited by a scheme approved under Professional Standards Legislation.

Contact us

To find out more about SailPoint IdentityIQ and how KPMG could work with you to improve your Identity Access Management, contact:

Gordon Archibald
Partner
T: +61 2 9346 5530
E: garchibald@kpmg.com.au

Jeremy Knight
Director
T: +61 3 9838 4050
E: jjaknight@kpmg.com.au

Danny Flint
Director
T: +61 7 3434 9191
E: dflint@kpmg.com.au

About SailPoint IdentityIQ

Identity Access Management system SailPoint IdentityIQ is designed to help large organisations to mitigate risk, increase efficiency, streamline costs and ensure compliance. It quickly delivers tangible results with risk-aware compliance management, closed loop user lifecycle management, flexible provisioning, an integrated governance model, and identity intelligence.

KPMG.com.au

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

© 2018 KPMG, an Australian partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo and are registered trademarks or trademarks of KPMG International.

Liability limited by a scheme approved under Professional Standards Legislation.

April 2018. QLDN16541MC.