

eBook

De-risking innovation in FinTech

How Australian firms can achieve
controlled growth and minimise
compliance-related costs



Data and analytics are fast becoming a crucial element of organisational success

Australia's FinTech sector is thriving. We rank sixth globally for FinTech¹, and have more than 800 FinTech firms, as well as one of the world's most sophisticated and fastest growing FinTech industries.²

800+

Australia ranks 6th globally — with over 800 FinTech firms.¹

Sophisticated, deep and liquid capital markets make Australia one of the major centres of financial markets activity in Asia.³ The strength of our financial services sector is supported by our mandated superannuation scheme, skilled and diverse workforce, and advanced business infrastructure.⁴

FinTech in Australia is also continuing to grow, with firms attracting both local and international capital. The number of Australian FinTechs doubled between 2017 and 2021.⁵

This growth does, however, bring risks — especially from a compliance perspective.

Australia's FinTech sector has ever-evolving compliance requirements which have scaled recently with updates to the Security of Critical Infrastructure Act (2018). New obligations have also been introduced for financial services organisations — making compliance both time consuming and potentially costly and complex. The costs associated with meeting compliance can also divert budgets and resources away from innovation.

Established FinTech organisations may also still be grappling with legacy infrastructure which is preventing effective compliance, and many organisations don't have the skills in-house to effectively meet compliance requirements.

The risk of cyberattack is also ever-present, and the financial and brand implications of an attack on a Fintech organisation are potentially devastating.

In this eBook we will explore some of these challenges in greater detail, and outline how Macquarie Cloud Services, and our partners Dell and VMWare, can help Australian FinTech organisations scale effectively — reducing the potentially vast risks and costs associated with compliance.

In this eBook

- Meeting compliance requirements: the challenges
- Achieving sustainable innovation: 5 ways to minimise your cloud costs as you grow
- About Macquarie Cloud Services
- Next steps

1, 2. Austrade, [Global Fintech Rankings 2021, Australia now ranks 6th in the world](#), 08/2021

3, 4. Global Australia, [Financial Services and FinTech](#) 5. KPMG, [Australian Fintech Survey Report](#), 06/2022

Meeting compliance requirements: the challenges

For FinTech organisations, meeting compliance requirements is a critical priority, and one which — when not managed optimally — threatens to consume profits and slow growth and innovation.



Key challenges for Australian FinTech firms in the current climate include:

Ever-evolving requirements

FinTech organisations are now required, by law, to provide extremely comprehensive information on their risk management and cyber-security preparedness and performance.

The Security of Critical Infrastructure Act (2018) (SOCIA) was recently strengthened via two tranches of legislative amendments, which passed in December 2021 and April 2022. These amendments expand the reach of the Act from 4 to 11 sectors, and create a framework which requires organisations to fulfil 'Positive Security Obligations'.⁶

51.1%

Risk and compliance expenditure consumed 51.1% of the Australia's financial sector's total investment spend in 2021.⁹

.....

This means organisations need to:

- Provide ownership and operational information to the Register of Critical Infrastructure Assets
- Report any security incidents within certain timeframes
- Develop a comprehensive Risk Management Program.

The updated Act also gives governments greater intervention and information-gathering powers. Meeting these legislative reporting requirements has the potential to be extremely time-consuming and laborious for organisations that don't have the right technology infrastructure or systems in place.

In addition, Australian FinTech organisations are also required to adhere with the requirements of regulatory authorities such as the Australian Securities and Investments Commission (ASIC), Australian Prudential Regulation Authority (APRA), and the Australian Transaction Reports and Analysis Centre (AUSTRAC) — all of which are taking an increasingly thorough approach to enforcement.

Lack of compliance management skills in-house

While Australia is a fertile ground for FinTech, many firms are lacking the in-house skills to effectively manage growth — particularly from a compliance perspective.

In a recent KPMG survey, only 4% of those FinTech firms surveyed were completely satisfied with their ability to recruit in their required areas.⁷

This survey also revealed that concerns about international recruitment and general economic performance due to COVID-19 may be hindering business confidence.

Australian businesses are feeling acute labour shortages in areas historically filled by temporary visa holders that have been restricted from entry due to border closures.⁸

6. KPMG, [Critical Infrastructure Financial Services Fact Sheet](#), 2022 7, 8. KPMG, [Australian Fintech Survey Report](#), 06/2022

9. KPMG, [Major Australian Banks: Full year 2021 results analysis](#), 11/2021



Escalating cyber-security costs

While Australia’s financial sector has made a significant investment in cybersecurity, it’s certainly not immune from attack. Chairman of the Australian Prudential Regulation Authority, Wayne Byrnes, recently said an attack on one of Australia’s financial institutions “will happen” at some point in the future.¹⁰

The costs of preventing — and mitigating — the impact of a cyber-attack are also escalating constantly. These include both the widely understood costs (those related to customer notification, credit monitoring and the possibility of legal judgements or penalties) as well as the ‘hidden’ costs (intellectual property theft, espionage, data destruction, attacks on core operations or attempts to disable critical infrastructure).¹¹

“Beneath the surface, these (hidden) attacks can have a much more significant impact on organisations and lead to additional costs that are both more difficult to quantify and often hidden from public view,” suggests a recent Deloitte report.¹²

Budgets and resources diverted from innovation

When employees and budgets are tied up with meeting compliance requirements, there is inevitably less capacity for innovation. A report by KPMG revealed that in Australia’s financial services sector, risk and compliance expenditure consumed 51.1% of total investment spend in 2021.¹³

Legacy or non-optimised technology infrastructure

Many FinTech organisations — especially those which are more established — are still relying on dated legacy infrastructure. This inhibits transparency and makes it hard to effectively meet compliance-related reporting requirements.

Newer, cloud-native organisations may also not have their infrastructure fully optimised, and may be paying more than they need to.

10. MPA Mag, [Cyberattack on Australia’s banks is inevitable](#), 10/2022 11, 12. Deloitte, [CFO Insights: Seven Hidden Costs of Cyberattack](#) 13. KPMG, [Major Australian Banks: Full year 2021 results analysis](#), 11/2021

Achieving sustainable innovation

5 ways to minimise compliance-related costs as you grow

1

Outsource to an expert partner

Meeting compliance requirements is complex and potentially time-consuming. Understanding the full scope of what needs to be reported is just one aspect — extracting, collating and supplying the required data, and ensuring compliance with detailed industry requirements, is another.

The challenge of fulfilling compliance requirements can be overcome by outsourcing to an expert technology partner who can provide you with the strategic insight and compliance services you need, at every step.

How Macquarie Cloud Services can help >

Our team has a deep understanding of compliance for the FinTech sector. Working as your partners, we can help you save time and money by:

- Always implementing technology which has compliance and auditability considerations ‘built in’, ensuring you have rock-solid, fully accredited foundations upon which to grow and innovate.
- Assuming responsibility for compliance-related reporting or ‘book-keeping’ for the parts of the technology stack we implement and support on your behalf.
- Staying abreast of all relevant industry standards, such as PCI DSS, to ensure your technology is appropriately managed from a compliance perspective.
- Leveraging our proven processes and systems to efficiently manage the ‘heavy lifting’ of compliance reporting — freeing your internal team to focus on other areas.

2

Appropriate application management

Many FinTech organisations are still relying on on-premise legacy applications and infrastructure, which can potentially inhibit effective compliance. As well as posing a security risk, legacy applications can stand in the way of streamlined reporting — making it difficult to extract, consolidate and use data.

Yet at the same time, taking a ‘blanket’ approach to digital transformation — and simply shifting all applications to the cloud to enhance compliance and security — isn’t always the most suitable strategy either. This is where relying on an expert partner like Macquarie Cloud Services is vital.

How Macquarie Cloud Services can help >

Our team of FinTech specialists can provide you with the advice and ongoing support you need to ensure each of your applications, workloads and infrastructure components is ideally located, configured and managed from a compliance perspective — without any unnecessary expense. This includes:

- Providing expert guidance regarding which applications should be modernised and shifted to the cloud, versus those which should be retained in a legacy or private cloud environment.
- Ensuring the compliance of new apps, as well as specific legacy applications which aren’t suited to modernisation nor a cloud-based location — providing all required patching, routine maintenance and security.
- Alleviating workload and ongoing expense for organisations by managing the day-to-day security and compliance of infrastructure, regardless of their level of digital transformation.
- Freeing up IT teams to focus on innovation and product development rather than maintenance and meeting compliance requirements.



Ensure robust disaster recovery and backup

A critical requirement of evolving industry regulations is having disaster recovery and backup in place. So if something unexpected happens, like a security breach, you can get back up and running quickly — without any interruption to the service you provide your customers.

[How Macquarie Cloud Services can help >](#)

The Macquarie Cloud Services team is highly experienced in the provision of both disaster recovery and backup services. We understand the vital importance of having rigid metrics in place around recovery, including both recovery point objectives (RPOs) and recovery time objectives (RTOs), and we work closely with clients to define solutions which are uniquely matched to their needs.



This includes:

- Facilitating and supporting a wide range of multi-cloud and multi-data centre disaster recovery and disaster avoidance solutions.
- Helping define, design, and implement robust testing processes and systems.
- Conducting non-disruptive failover testing on an ongoing basis, to ensure an organisation's technology is always operating as it should — a vital aspect of compliance requirements.
- Our partnership with Dell and VMWare also means we can scale performance and capacity with efficiency, while delivering 100% service-level guarantees and reducing operational overhead.

4

Insist on built-in compliance

Too often, FinTech organisations rely on technology or partners which are not inherently optimised for compliance. Without the right processes, tools and structures in place, meeting compliance requirements can be very time-consuming and complex.

This can also expose the organisation to unnecessary risk and inefficiency and inhibit its ability to secure funding for next-level growth.



How Macquarie Cloud Services can help >

Ensuring that your FinTech organisation can easily and seamlessly meet compliance requirements is a core priority for our experienced team. We achieve this by:

- Only recommending, designing, and implementing technology solutions which have compliance ‘baked in’ – rather than attached as an ‘add on’ component.
- Staying up to date with all relevant industry requirements, and providing any required updates to ensure your technology remains compliant on an ongoing basis, as requirements evolve.
- Ensuring that all information needed to demonstrate adherence with industry regulations is easy to report on and provide to authorities.
- Managing any compliance reporting on your behalf, for the components of your infrastructure for which we are responsible.

Our expertise in, and focus on, compliance is one of the key reasons we are the chosen partner for the Australian Federal Government, as well as many Fortune 500 companies, and trusted by organisations such as the Australian Taxation Office, Westpac and BPAY.

5



Prioritise security

The security of customer data is a growing risk in FinTech, and — as such — a core component of compliance. To maintain a license to operate, your organisation must demonstrate that you have robust data security provisions in place, as well as a solid plan for how to deal with a breach should it occur.

This requires having comprehensive, next-generation security in place, and in the current climate, relying on ad-hoc, point-based security solutions is no longer sufficient.

How Macquarie Cloud Services can help >

Our team is highly experienced in the provision of sovereign, multi-cloud security services, benchmarked to meet the highest technical and operational standards. We can help you achieve your security obligations by:

- Continuously challenging the status quo to not only mitigate risk for your organisation, but ensure your data is protected with the best possible solutions.
- Taking a holistic view of security — helping you understand the real and ongoing risks to your business.
- Saving you time and effort by providing practical remediation and resolution assistance focused on genuine threats, not false positives.

Our security and compliance programs are extensive and ongoing, and we offer one of the most certified data centres in Australia and the world.

About Macquarie Cloud Services

As the Australian specialists in cloud services for business and government customers, we are:

Personal and accountable — with multi-level support by in-country, certified experts with industry-leading service level guarantees.

Flexible for now and tomorrow — enabling scalable hybrid cloud environments which offer true solutions, not just individual products.

A business built on trust — we secure the internet for over 40% of federal government agencies, with industry certifications.

Sound business process — we have an ITIL based service model and ISO27001 certified processes, vetted by industry and partners.

Our partners

Macquarie Cloud Services is also proud to partner with some of the world's leading technology organisations to enhance the support and services we can provide FinTech sector. This includes:



Working with your Dell Technologies team, we can create specific solutions that work best with your existing platform and your Macquarie Data Centre or Cloud Solutions.

We have the highest level of support available from the Dell Technologies' technical teams to protect the environments powered by their storage and backup solutions, and Dell Technologies is fully integrated into the Macquarie Cloud Environment for enterprise grade storage solutions, which are designed, built and maintained by Dell Technologies' trained engineers.



We are Australia's only dedicated VMware Showcase Service Provider. This partnership allows us to offer deeper access to technology — enabling you to take advantage of multiple VMware components to create the solution you need.

With solutions such as our VMware Cloud, Data Centre Extension based on NSX, and Zero Downtime VMware clusters, only Macquarie Cloud Services can get you to the cloud easily and with VMware's full backing.

Get in touch

If you're looking for a local partner with deep expertise in secure, sovereign and compliant cloud solutions and the proven ability to support the growth of your business, get in touch today.



1800 004 943
macquariecloudservices.com

