MARSH

Scaling up insurtech and fintech businesses while managing risks

Growing a tech business in the insurance and financial services sector offers great opportunities, though it also introduces unique risks that require careful management. As your organisation grows the complexity of compliance, operations, and stakeholder expectations also increases.

As a business looking to scale, to support your customers and operate as seamlessly as possible, implementing tools and frameworks are core to supporting your business. **This guide outlines key risk management and insurance considerations to help safeguard your business through each stage of expansion**. While not exhaustive, it highlights essential areas to address to support sustainable and responsible growth.

1 Minimum coverage to consider for growing insurtech businesses

As your business expands, securing the right insurance coverage is a critical foundation for managing risks and protecting your people, clients and stakeholders. As a minimum, scaling businesses should consider the following policies and practices:

- ☐ **Tech professional indemnity (Tech PI):** Can cover for claims related to data breaches, system failures, or professional negligence from services or platforms your business provides.
- ☐ **Professional indemnity (PI):** Insurtechs with an Australian Financial Services Licence (AFSL) should prioritise comprehensive PI coverage that complies with ASIC Regulatory Guide 126.
- ☐ **Directors & officers (D&O) insurance:** Can help protect your leadership team and board if they face legal claims related to their strategic decisions, regulatory investigations, or shareholder disputes, particularly during rapid growth or M&A transactions.
- ☐ **Cyber insurance:** With technology at the foundation of your business model, cyber insurance should be considered to help safeguard your business against data breaches, ransomware and business interruption that could disrupt core operation and growth.

Policy reviews and adjustments:

Regularly review and update your insurance policies to ensure coverage limits and terms evolve with your business, addressing increasing complexities and scale of potential claims.

Access our comprehensive incident response framework to enhance your preparedness.

2 Building a resilient incident response and cybersecurity strategy

Cyber threats remain a top concern for insurtech businesses. In 2023, financial and insurance services ranked among the top five industries reporting cybercrimes to law enforcement.[1]

A robust incident response plan is essential to help detect, analyse, and remediate a cyber issue quickly and effectively, reducing potential damage and downtime.

An effective Cyber Incident Response Plan should include:

- ☐ **Escalation strategy:** Define clear steps for escalating severe or prolonged attacks to the right stakeholders.
- ☐ **Severity matrix:** Use a framework to prioritise responses based on potential business, operational and regulatory impacts.
- ☐ **Clearly define roles and responsibilities:** Assign tasks for both internal and external incident response teams.
- ☐ **Communication templates:** Prepare templates for notifying regulators, media, and affected parties, saving valuable time during an incident.
- ☐ **Backup communication channels:** Establish alternative communication methods in case your primary channels are compromised.
- ☐ **Cyber insurance integration:** Understand your notification obligations under your cyber insurance policy (if insured).

Beyond the response plan, businesses should also focus on strengthening their overall cyber readiness and compliance practices:

- ☐ **Understanding your cyber risk:** Understanding your cyber risk and exposure and considering what could go wrong helps you approach the risk with clarity and confidence to manage it.
- ☐ **Ransomware positioning:** Define your organisation's position on ransom payments. It is recommended that organisations discuss their stance on this complex issue ahead of an event. Under the Cyber Security Act 2024 in Australia, certain businesses must report ransomware payments, including those made on their behalf, within 72 hours of payment.[2]
- ☐ **Employee training:** People represent the strongest defence against cyber risk, but also are the weakest link with many cyber issues traced to human error. Conduct ongoing training to help staff recognise what constitutes a cyber threat and avoid behaviours that could unintentionally trigger an incident.

3 Managing people risk during team growth

As your business expands, people-related risks increase, from employee disputes to management liability issues. Addressing these risks proactively is key to protecting your organisation and its leadership team:

- ☐ **Strengthening HR policies and compliance:** Implement clear policies, training and internal controls, to minimise disputes and support a positive work environment.
- ☐ **Enhance directors & officers protection:** Ensure your D&O insurance adequately addresses risks associated with rapid growth and regulatory scrutiny.
- ☐ **Employment practice liability coverage:** Consider extending coverage for claims related to wrongful termination, harassment or discrimination. This is particularly relevant for companies operating or expanding operations in litigious markets such as the US.
- ☐ **Employee benefits:** Offer benefits that match industry standards and ensure they align with your Employee Value Proposition to help attract and retain the talent you want and need.
- ☐ **Employee listening:** Understand what benefits employees value most, to help boost loyalty and engagement.
- ☐ **Benefits communication:** Clearly communicate why you have chosen the benefits in a way that resonates with employees, to help encourage overall engagement and improved ROI.
- ☐ **Benefits access:** Make benefits simple to find and use for your employees. Also consider the use of reporting tools to monitor and track utilisation of benefits. This will help your organisation to continuously assess and improve your program.
- ☐ **Foundational wellbeing:** Establish an Employee Assistance Program offering holistic support to enhance employee wellbeing. Global companies, should focus on vendor harmonisation early by selecting global vendors to reduce vendor management workload, improve cost efficiency and vendor relationships.
- ☐ **Vendor audit and assessment:** Choose vendors who can support your long-term goals, not just immediate needs.
- ☐ **Attracting top talent in new markets:** Conduct targeted benefits benchmarking to ensure benefits are fair and competitive. Use this information, to differentiate your offering based on budget. For example, by adding low-cost benefits or investing more where it matters.

[1] Annual Cyber Threat Report 2023-2024 | Cyber.gov.au
[2] Factsheet-ransomware-payment-reporting

4 Funding, M&A, capital raising and entering new markets

Growth activities such as funding rounds, mergers, or entering new markets often introduce complex financial, legal and regulatory risks. Proactive planning is essential to manage these exposures and protect investors and the business:

- ☐ **Understand regional and market-specific risks:** Research local regulations, legal requirements and market-specific conditions to ensure compliance, and tailor insurance policies to meet requirements for new jurisdictions.
- ☐ **Liability allocation in transactions:** During M&A activity, clearly define how liabilities will be allocated between buyer and seller to avoid disputes and unexpected financial exposure. Warranty and indemnity (W&I) insurance can help facilitate commercial negotiations and transfer deal-related risk effectively.
- ☐ **Insurance due diligence:** Conduct thorough reviews of existing policies to identify gaps and mitigate risks associated with financing or M&A transactions. Lenders often rely on this process to ensure that assets are adequately protected and to make informed decisions about loan terms and conditions.
- ☐ **Review pre-closing liabilities:** Pay close attention to the insurance policies covering cyber, E&O, PI and D&O exposures, as gaps can create significant risk after deal completion. A robust review of sale documentation is critical for assessing and mitigating these liabilities.
- ☐ **Engage early:** Involve legal and insurance advisors from the outset to navigate transaction or market complexities, ensuring your policies align with strategic goals and regulatory requirements.

Contact Marsh

To explore how Marsh can support your growth journey and safeguard your organisation, please connect with your Marsh representative or contact us here.

How we can help

Scaling your insurtech and fintech business presents exciting growth opportunities — along with new complexities and risks.

At Marsh, we combine deep industry expertise with a global network and innovative risk solutions tailored for fast-growing technology companies like yours. By working with Marsh, you gain a trusted advisor who can:

- Proactively identify and mitigate emerging risks before they impact your business.
- Customise insurance programs that evolve alongside your strategic goals and expansion plans.
- Guide you confidently through complex transactions, regulatory requirements, and compliance challenges.

Our dedicated team understands the unique challenges of scaling technology-driven financial services and is committed to helping you protect your business's long-term success.