Singapore Financial Services Cybersecurity & Compliance Outlook 2025

In 2025, Singapore's financial services sector is entering an era of heightened cybersecurity scrutiny and complex threats, from AI-driven attacks to advanced supply chain risks. To meet evolving MAS, PDPC, and CSA requirements, financial institutions must embed robust cyber governance, adopt AI ethically, and strengthen resilience frameworks that protect customers and maintain trust in a rapidly changing digital landscape.

aphore

Singapore Financial Services Cybersecurity & Compliance Outlook 2025

Executive Summary

Key Challenges in 2025: Singapore's financial sector faces an unprecedented convergence of cybersecurity threats and evolving regulatory demands. From **AI-driven cyber-attacks** (such as deepfake-enabled fraud and automated phishing) to complex supply chain vulnerabilities, the threat landscape in 2025 is more sophisticated than ever. At the same time, regulators are raising the bar for operational resilience and data protection. The Monetary Authority of Singapore (MAS) has made clear that **"cybersecurity and trust" are critical to Singapore's ambitions as a global financial hub**, and it is enacting new guidelines to fortify financial institutions (FIs). Parallel efforts by the Personal Data Protection Commission (PDPC), Cyber Security Agency (CSA), and others signal a tightening compliance environment that demands board-level attention and strategic investment.

Emerging Regulatory Changes: Starting 2024, Singapore's regulators are introducing forward-looking rules and guidance. MAS is zeroing in on **operational resilience, third-party risk management, and technology governance**, aligning with global trends like Europe's Digital Operational Resilience Act (DORA) which mandates stringent ICT risk controls from January 2025. PDPC released new **Advisory Guidelines on AI** (March 2024) clarifying how the PDPA applies to AI systems using personal data, emphasizing transparency and accountability. The CSA amended the Cybersecurity Act in 2024 to broaden incident reporting (including supply chain incidents) and expand oversight of critical infrastructure. These developments position Singapore on par with, or ahead of, other financial hubs in regulatory rigor. Notably, MAS's 2025 industry transformation roadmap underscores that robust cyber measures and **principle-based tech regulation** will be key to maintaining trust while fostering innovation.

AI-Driven Risks & Cyber Threat Trends: Generative AI is a double-edged sword. On one hand, AI bolsters defence – automating threat detection and compliance monitoring – but on the other, it supercharges attackers' capabilities. Experts predict a surge in **AI-powered attacks** in 2025, including highly convincing deepfake impersonations and AI-crafted social engineering that are harder to detect. Deepfake fraud alone could cost the global financial sector billions (with estimates of **$40 billion in losses by 2027** and an average of $600k lost per incident). Nation-state cyber espionage also looms large, as geopolitical tensions in the Asia-Pacific region drive state-sponsored hackers to target financial institutions for intelligence or disruption. These factors create an imperative for FIs to enhance vigilance, especially as **insider threats and data leaks** may be magnified by AI tools misuse.

Governance Best Practices: In response to these challenges, leading financial institutions are embedding cybersecurity into enterprise risk management and governance. Boards and CEOs are expected to champion a **"security-first" culture** and ensure compliance readiness. Global and local regulators alike now insist on greater cybersecurity expertise in the boardroom and proactive risk management at the senior levels. Best practices for 2025 include adopting AI governance frameworks (to manage AI risks ethically), continuous cyber resilience testing (e.g. stress-testing systems for outages or breaches), and robust third-party oversight. Importantly, regulators such as MAS are taking a **collaborative approach** – working with banks and technology providers to manage cloud and fintech risks without stifling innovation.

Strategic Recommendations: To thrive in 2025 and beyond, Singapore's financial services firms should prioritize: **1)** *Enhancing operational resilience* – aligning with MAS guidelines to ensure critical services can withstand disruptions; **2)** *Strengthening cyber defences against AI-augmented threats* – leveraging advanced threat intel and AI tools for defence; **3)** *Bolstering compliance and data governance* – staying ahead of new MAS, PDPC, and CSA requirements; and **4)** *Fostering a risk-aware culture from the top-down* – with boards accountable for cybersecurity outcomes. By mapping these actions to international standards (ISO 27001, NIST CSF) and MAS's own framework, financial institutions can not only meet compliance obligations but also reinforce customer trust and business resilience in the digital age.

Section 1: Regulatory Landscape & Compliance Developments

MAS – Heightened Standards for Resilience: From 2024 onward, MAS is implementing stringent cybersecurity and technology risk requirements that keep Singapore in lockstep with global financial centres. Recent MAS guidelines emphasize **operational resilience** – ensuring FIs can maintain critical services through any disruption. Notably, MAS's revised Business Continuity Management (BCM) Guidelines (effective 2023) require a **service-centric, end-to-end approach** to resilience, including timely recovery of critical business services, mapping of dependencies (e.g. third-party providers), and continuous testing. Senior management must actively oversee these measures. Similarly, the MAS Technology Risk Management (TRM) Guidelines (last updated Jan 2021) introduced higher expectations for governance: boards must possess adequate technology risk knowledge and appoint accountable executives (CIO/CISO), and FIs must rigorously manage third-party technology services and maintain an up-to-date inventory of information assets. These guidelines underscore MAS's focus on **third-party risk management and robust oversight** of outsourced systems, in light of increasing cloud adoption and fintech partnerships.

MAS's Global Alignment: Singapore's approach is largely comparable to other leading jurisdictions, often even more proactive in certain areas. For instance, well before the EU's DORA took full effect in 2025 (mandating comprehensive ICT risk frameworks, incident reporting, resilience testing, and third-party risk controls for all EU financial entities), MAS had already embedded many of these elements into its supervisory expectations. MAS's insistence on critical infrastructure protection and incident reporting mirrors the direction of U.S. regulators (e.g. US FFIEC guidance, and new SEC

cyber disclosure rules in 2024) and Hong Kong's HKMA, which issued an Operational Resilience Policy in 2022. In fact, MAS participated in global discussions and in 2022–2023 consulted on updates to outsourcing, tech risk, and BCM guidelines to **enhance operational resilience**, much like HKMA and the UK regulators did. The outcome is that MAS now expects FIs to identify their **critical business services, map interdependencies (including fourth-party dependencies)**, and set tolerance levels for disruption – an approach aligned with Bank of England/PRA and Basel Committee principles on operational resilience. In comparison to the U.S., which relies on a patchwork of guidelines and industry standards, Singapore's regulatory regime is more centralized and prescriptive via MAS, yet flexible enough to incorporate best practices (e.g. MAS references international standards like NIST CSF in its guidance).

PDPC – Data Protection and AI Governance: On the data privacy front, the PDPC is ramping up requirements as data-driven and AI innovations spread in finance. The Personal Data Protection Act (PDPA) was enhanced in recent years (mandatory breach notification and heavier fines from 2022), and now **AI usage is under the compliance microscope**. In March 2024, PDPC issued its first **Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems**, providing much-needed clarity on how PDPA applies to AI systems. These guidelines confirm that organizations can use personal data for AI model training with proper consent or under PDPA exceptions (e.g. for "business improvement" or research). They also set baseline best practices: be transparent with consumers about AI use, implement data protection measures (like anonymization where possible), and ensure accountability for AI decisions. This reflects PDPC's evolving stance that **AI governance and data protection go hand-in-hand** – companies deploying AI must do so in a way that upholds individuals' privacy rights and does not run afoul of consent requirements. Singapore's approach here is somewhat less heavy-handed than the EU (which is introducing an AI Act categorizing high-risk AI systems), but the direction is similar: encourage **responsible AI** through guidance now, with the possibility of tighter rules if industry self-governance falls short. PDPC is also actively contributing to regional standards, co-developing the **ASEAN AI Governance Framework** (released Feb 2024) to harmonize trustworthy AI principles across Asia.

CSA – Critical Infrastructure and Cybersecurity Act Updates: The Cyber Security Agency of Singapore oversees critical information infrastructure (CII) – a category that includes major banks and financial market systems. In 2024, Singapore updated its **Cybersecurity Act** (the first major amendment since 2018) to bolster resilience and incident response across CIIs. The amendments, passed in May 2024, expand CSA's oversight powers and impose new duties on CII operators. Notably, **incident reporting obligations** have widened: CII organizations (including in banking/finance) must report a broader range of cybersecurity incidents **"aimed at or affecting their systems, including supply-chain incidents"** that could impact services. This means a cyber incident at a third-party vendor that disrupts a bank's operations now falls squarely under mandatory reporting – highlighting regulators' concern over systemic risk from interconnected providers. The amended Act also enables authorities to designate "**Systems of Temporary Cybersecurity Concern (STCC)**" – critical systems at high risk during special events (for example, systems supporting pandemic response or major

financial transactions) – for enhanced monitoring. Furthermore, CSA introduced **light-touch regulation for new classes** like "Entities of Special Cybersecurity Interest" (e.g. certain fintechs or universities holding sensitive financial data) and broadened its reach to **overseas systems** that are managed from Singapore. Together, these changes ensure Singapore's legal framework keeps pace with the threat landscape and reinforces accountability for cyber defence at all levels. Financial institutions in Singapore must now navigate not only MAS's sector-specific rules but also CSA's cross-sector requirements (particularly if they are designated CIIs), which collectively demand a **holistic compliance strategy**.

Comparative Insights: Singapore's regulatory posture in 2025 can be characterized as **forward-leaning yet balanced**. MAS's principle-based but firm approach to new tech risks contrasts with, say, the U.S. where no single regulator imposes enterprise-wide cyber rules (aside from specific ones like New York's DFS regulation). Hong Kong's HKMA similarly emphasizes resilience and has its Cybersecurity Fortification Initiative, but Singapore's integration of cyber risk into its national agenda (with MAS, PDPC, CSA coordinating) is a distinctive strength. In the EU, DORA's advent on 17 Jan 2025 sets a high bar for operational resilience (covering ICT risk management, testing, and third-party contracts), and Singapore's financial institutions – many operating globally – are already aligning with such expectations. For example, MAS's outsourcing and cloud risk management guidelines echo DORA's requirements for contractual oversight and concentration risk monitoring. In short, Singapore's regulatory landscape in 2025 is **comprehensive and on par with global standards**, with a strong emphasis on resilience, governance, and the responsible adoption of emerging technologies.

Section 2: Emerging Cybersecurity Threats in 2025

AI-Driven Attacks and Deepfakes: By 2025, cyber adversaries are weaponizing artificial intelligence to a degree not seen before. Singapore's financial institutions should brace for **highly sophisticated phishing and fraud schemes powered by AI**. Generative AI can automate the creation of phishing emails that are linguistically flawless and personalized at scale, defeating traditional detection. Even more concerning is the rise of **deepfake attacks** – where synthetic audio or video is used to impersonate executives or clients. Such deepfakes have already enabled large-scale fraud globally (e.g. a deepfake CEO voice scam in 2023 tricked employees into transferring millions), and the trend is accelerating. Analysts project deepfake-enabled fraud could inflict **$40 billion in losses by 2027**, with each incident costing financial firms an average of $600,000. In Singapore's context, this means a bank officer could receive what looks and sounds like an urgent instruction from a CEO or a high-net-worth client, when in fact it's an AI-generated fake – potentially leading to unauthorized transactions or data leaks. The **erosion of digital trust** caused by deepfakes poses a serious challenge: financial services, built on trust and verification, must now verify identities and instructions in new ways. 2025 is likely to see increased adoption of deepfake detection tools and verification protocols (multi-factor authenticity checks, biometrics, etc.) as countermeasures. Regulators, too, are cognizant of this threat – with calls for stronger protections against AI-driven fraud – which could translate into guidelines on customer verification and fraud surveillance.

Advanced Persistent Threats & Nation-State Actors: Singapore's prominence as a financial hub makes it a high-value target for **state-linked hacking groups (APTs)**. We anticipate a continued uptick in nation-state cyber espionage aiming at banks, asset managers, and government-linked financial entities. Such actors may seek to steal sensitive financial information (e.g. merger deals, trading algorithms) or even sabotage systems as a form of economic warfare. The CSA's expanded mandate in 2024 explicitly aims to counter this, focusing on enhancing critical sectors' resilience to state-sponsored attacks. In 2025, nation-state attackers are expected to leverage more zero-day exploits (previously unknown software vulnerabilities) to penetrate systems undetected. They may also supply chain attacks – compromising a widely-used software or cloud provider to indirectly breach multiple financial institutions. The **supply chain threat** remains potent; as noted earlier, Singapore is compelling FIs to monitor their third-party cybersecurity closely. A hypothetical scenario could be a hostile actor inserting malware into a fintech vendor's software update, thereby infiltrating many banks at once. Additionally, **regional geopolitical tensions** (for example, in Southeast Asia or broader Asia-Pacific conflicts) could manifest in cyber domain: we might see spikes in phishing campaigns or DDoS attacks against Singaporean financial sites coinciding with international disputes. Financial services firms should therefore watch geopolitical intelligence and ensure their cyber defences are adaptable to state-grade threats (e.g. enhanced network monitoring for APT tactics, threat hunting, etc.).

Insider Threats and Human Factor: As systems harden, attackers may increasingly exploit the **human element**. In 2025, insider threats could intensify, partly fueled by remote/hybrid work and by employees' use of AI tools. There is a risk of staff inadvertently exposing data via AI chatbots or being tricked by AI-crafted social engineering. Indeed, AI-driven impersonation can make it extremely difficult to distinguish legitimate communications from malicious ones. The *widespread adoption of AI tools raises concerns about employees unwittingly sharing sensitive data*, as one 2024 analysis noted. Moreover, malicious insiders might use AI to cover their tracks or find security gaps. Financial institutions must double down on insider risk programs – employing user behaviour analytics, stricter data access controls, and fostering an internal culture of security (so that employees themselves are vigilant about AI-generated scams). Regular training in 2025 will need to cover recognizing deepfakes and phishing that doesn't "look phony" anymore. **Zero-trust security models** are also recommended, under which no user or system is inherently trusted and continuous verification is required. This approach helps limit the damage an insider (or compromised account) can do by segmenting access.

Supply Chain and Cloud Security Concerns: The financial sector's heavy reliance on technology vendors and cloud service providers brings supply chain security to the forefront in 2025. **Third-party breaches** have been on the rise, with attackers exploiting weaker links in software providers or IT contractors to break into well-protected banks. Singapore's banks, insurers, and asset managers increasingly use multiple cloud platforms (AWS, Azure, Google) to drive digital innovation – in fact, **73% of financial firms were using multiple cloud providers by 2024, up from 54% in 2022**. This multi-cloud adoption improves agility but also **multiplies complexity**, as nearly two-thirds of

financial institutions report that securing data in the cloud is more complex than in on-premises systems. Misconfigurations, lack of visibility across environments, and inconsistency in controls can lead to data leakage or service outages. For example, one bank's critical workload might be spread across different clouds; a failure or cyber incident in one could cascade if not properly isolated. **Concentration risk** is another concern: a handful of big tech providers host the majority of banking services, so a major cloud outage or attack on a cloud vendor could have systemic impact. MAS itself has highlighted the risk of "overreliance on a small pool of cloud providers" and is urging an ecosystem approach to secure adoption. In 2025, we expect regulators to scrutinize cloud risk management more heavily – including stress tests and exit strategies if a cloud becomes compromised.

To mitigate supply chain threats, financial firms will need to enforce stringent **due diligence and continuous monitoring of vendors**. However, a 2024 study noted that most companies do not even know all the third parties handling their data, a gap that must be closed. Leading practices include maintaining an up-to-date vendor inventory, requiring vendors to meet security standards (MAS's OSPAR reports or international SOC reports), and employing threat intelligence to catch supply chain anomalies. **Cyber insurance** for supply chain incidents and contractual clauses for vendor security are also likely to become more common in Singapore by 2025. Meanwhile, cloud security posture management (CSPM) tools and encryption of sensitive data in cloud are key technical measures. Ultimately, **resilience** in a digital banking ecosystem means not only securing one's own walls, but also **ensuring partners and providers uphold strong defences** – a message that regulators and industry bodies (like the Association of Banks in Singapore) are reinforcing through guidelines and shared exercises.

Financial Fraud & Digital Banking Exploits: The rapid growth of digital banking and real-time payments in Singapore (with initiatives like PayNow and expanding fintech services) is accompanied by a surge in fraud cases. Scammers have been quick to exploit digital platforms, leading regulators to step in with protective measures. Surveys indicate that in Asia-Pacific, about **64% of financial institutions observed an increase in digital banking fraud over the past year** as online transactions soared. In Singapore, 2023 saw a wave of phishing scams, unauthorized online banking transactions, and account takeovers – prompting new industry safeguards. By mid-2025, under a new anti-scam framework, banks in Singapore will be required to implement **real-time fraud detection systems** and stronger customer authentication (e.g. Singpass biometric verification) for online services. We anticipate these measures will harden targets, but criminals are also innovating (for instance, using malware on customers' devices to hijack digital tokens, or performing SIM swap attacks to intercept OTPs). **Deepfake technology may fuel novel fraud tactics**: for example, using AI voice cloning to bypass bank call center verification, or fake "video calls" to trick relationship managers. Additionally, **synthetic identities** – where fraudsters use a mix of real and fictitious data to create new fake accounts – are expected to increase, undermining KYC processes. The financial sector is responding by deploying AI for fraud **pattern recognition** and collaborating on information sharing. In April 2024, MAS launched the COSMIC platform (Collaborative Sharing of ML/TF Information and Cases) to enable

banks to share data on suspicious accounts in real time, illustrating a proactive, collective defence against fraud and money laundering. Going forward, we expect greater fusion of fraud risk management with cybersecurity – as the line blurs between cyber-attacks and fraud (many scams now start with a cyber breach or data theft). FIs should ensure their **fraud monitoring, IT security, and compliance teams work hand-in-hand**, using AI/ML analytics to flag anomalies in transaction patterns or user behaviour. The government's move to enact a new **"anti-scam" law in 2025** (with powers to swiftly freeze suspect accounts and penalize SIM misuse) further underlines that combating financial fraud is a national priority, integral to cybersecurity resilience.

Geopolitical and Macro-level Factors: The broader environment in 2025 also influences cyber risk in Singapore's financial sector. Heightened global **cybercrime networks** (often ransomware gangs) are targeting financial data for extortion; Southeast Asia has seen a rise in ransomware-as-a-service operations. A reported **346 ransomware incidents hit Singapore's financial services sector in 2023**, making it one of the most targeted industries. While many incidents are contained, the sheer volume indicates that attackers consider banks and insurers lucrative prey (for ransom or data theft). Such criminal activity could be exacerbated if global economic conditions worsen – financially motivated hackers tend to intensify efforts during downturns. Conversely, international cooperation in law enforcement (Interpol, ASEAN cybersecurity accords) could help disrupt some cybercrime infrastructure, though results are gradual. On the nation-state front, if diplomatic relations strain (e.g. US-China tech tensions), cyberspace may become an arena for proxy battles – possibly impacting multinational banks. Singapore's neutral stance and strong laws might not deter foreign espionage entirely, but its participation in global cyber defence dialogues will be crucial. Also, emerging technologies like **quantum computing** loom on the horizon as future threats (able to break certain encryptions), and indeed MAS has begun trials on "quantum-proofing" cybersecurity with banks in 2024. While quantum attacks are unlikely in 2025, it is indicative of Singapore's forward-looking stance to anticipate and mitigate tomorrow's threats today. In summary, the threat landscape for Singapore's financial services in 2025 is dynamic and multifaceted – spanning **AI-enhanced criminal attacks, sophisticated state-sponsored operations, insider risks, supply chain pitfalls, and fraud epidemics** – requiring equally sophisticated and agile defences.

Section 3: AI & Financial Services – Compliance, Risk & Governance

Transformative Potential of AI in Finance: Artificial Intelligence is revolutionizing financial services from front-office to back-office. In wealth management and retail banking, AI-driven **robo-advisors** offer personalized investment advice; in insurance, AI algorithms expedite underwriting and claims; in trading, AI models execute strategies at lightning speed; and across the board, AI chatbots and virtual assistants improve customer service. This widespread adoption brings efficiency and new revenue opportunities but also raises **regulatory and ethical implications**. By 2025, MAS and other regulators are intensifying oversight on how FIs deploy AI, ensuring that innovation does not undermine fairness, transparency, or stability. **Algorithmic decision-making** in finance can lead to biases (e.g. in credit approvals or pricing) if not

properly governed. There is a risk that an AI model might unintentionally discriminate against certain demographics or make opaque decisions that even the firm's developers can't fully explain. Therefore, regulators are concerned with **algorithmic transparency and accountability** – essentially, FIs should be able to explain "why did the AI make this recommendation or decision?" especially in high-stakes areas like credit, insurance, or investment advice.

MAS's Oversight and FEAT Principles: Singapore has been ahead of the curve in promoting responsible AI use in financial services. MAS introduced the **FEAT principles (Fairness, Ethics, Accountability, Transparency)** back in 2018 as voluntary guidelines for AI and data analytics in finance. Moving into 2024 and beyond, MAS is operationalizing these principles. In June 2023, MAS and an industry consortium released the **Veritas Toolkit 2.0**, an open-source toolkit to help financial institutions **assess and implement the FEAT principles in their AI models**. This toolkit provides methodologies to test AI systems for fairness (e.g. checking for bias in loan approvals), ethics, accountability (clear roles for oversight), and transparency (explainability of outcomes). Seven major FIs piloted the integration of Veritas into their internal governance and identified best practices such as the importance of a **consistent, robust AI governance framework spanning all geographies**, a **risk-based approach** to determine the level of governance needed per AI use-case, and investing in training for the next generation of AI professionals. MAS has signalled that it expects FIs to adopt these practices. Although FEAT/Veritas are not "regulations" per se, they strongly influence supervisory expectations. When MAS examines an FI's AI use (for instance, during inspections or risk assessments), it will likely look for evidence that the firm has applied these responsible AI frameworks.

Additionally, MAS's **principle-based regulation of new tech** means it may issue guidelines or notices if specific AI-related risks need addressing. We might see, for example, guidance on **model risk management** for AI models, similar to how banks manage financial risk models – ensuring proper validation, monitoring for drift, and contingency plans if models fail. MAS is also concerned with **algorithmic trading AI** – ensuring that AI trading bots do not disrupt markets (there are rules on algo trading testing and kill-switches which could be extended as AI gets more autonomous). By 2025, we expect MAS to increasingly integrate AI considerations into its existing risk management guidelines. Vincent Loy of MAS highlighted that MAS takes a **"principle-based approach"** to regulating new technologies including AI, carefully managing cyber and systemic risks without stifling innovation. This suggests that rather than heavy-handed new AI laws, MAS will embed AI risk oversight into things like TRM guidelines, conduct codes, and require clear accountability when AI is used in decision-making.

Ethical and Data Privacy Concerns: The deployment of AI in financial advisory and operations comes with **ethical dilemmas**. For instance, if an AI-driven robo-advisor makes a poor recommendation that causes client losses, who is responsible – the advisor, the firm, the AI developer? Or consider an AI credit scoring system that inadvertently redlines certain neighbourhoods – it raises issues of fairness and consumer protection. Singapore's regulators emphasize that human accountability

cannot be abdicated to machines. Financial institutions must therefore institute governance where **AI outcomes are reviewed by humans**, especially in significant customer-impact decisions. The **ethical use of data** is another pillar – AI systems require vast amounts of data, much of it personal financial data, raising privacy issues. PDPC's new AI guidelines (2024) directly tackle this by setting expectations for **transparency and consent**. They encourage practices like informing customers when AI is used to make decisions about them and allowing some form of recourse or human review. We may also see the PDPC or MAS encourage **"ethical AI charters"** within financial firms – internal policies that commit to avoiding bias, ensuring data quality, and respecting customer privacy in AI development.

A significant compliance aspect is **data management for AI**. Under PDPA, using customer data for new purposes (like training an AI model for a new service) might require additional consent or fall under certain exceptions. The 2024 PDPC guidelines clarify that *if using personal data for AI training, organizations should either obtain meaningful consent or ensure it fits under allowed exceptions like legitimate business improvement*. They also underscore the need to **anonymize data where possible** during AI model training to minimize privacy risk. In practice, financial institutions in 2025 will need robust processes for data governance – tracking what data is fed into AI, ensuring it's legally collected, and controlling outputs (some AI models could infer sensitive information). The **Model AI Governance Framework** (a guideline first issued by Singapore in 2019 and since evolved) remains a useful reference, providing detailed measures for internal governance (like having an AI ethics committee, bias testing protocols, etc.). Banks and insurers are increasingly adopting these measures not just to satisfy regulators but also to build **customer trust** – knowing that their bank uses AI prudently can be a competitive advantage.

Balancing AI Innovation with Risk Management: One of the central challenges for CEOs and leaders is to harness AI's benefits while keeping risks in check. AI can significantly enhance risk management itself – for example, AI systems can detect fraud or cyber intrusions in real-time (as discussed earlier), and they can help compliance teams sift through transactions for AML concerns with greater accuracy. So, the relationship between AI and compliance is two-way: AI introduces risks **and** mitigates risks. Forward-looking financial firms in Singapore are adopting **governance frameworks that integrate AI into the enterprise risk fabric**. This means when rolling out an AI-driven product or feature, the firm conducts a thorough risk assessment: What are the legal implications? Could the algorithm make a biased decision? How do we explain its output to a regulator if asked? Leading banks have started **AI risk committees** or expanded existing risk committees to include AI expertise. They are also using tools (some provided by MAS's Veritas initiative) to audit AI models for fairness and explainability.

From a regulatory compliance perspective, documentation is key. By 2025, institutions will need to maintain documentation on their AI models – data lineage, design objectives, validation results – to demonstrate control. For high-impact AI (like credit scoring engines), regulators might expect regular independent audits or validation akin to model validation in Basel II frameworks. **Accountability** is another governance

element: MAS will want to know that a senior officer (maybe the Chief Risk Officer or a newly appointed Head of AI Governance) holds responsibility for the outcomes of AI systems. Internally, firms are crafting **"human-in-the-loop"** policies where needed – ensuring human review or override is possible in AI-driven processes, especially in customer-facing decisions.

Singapore's approach also involves industry collaboration in AI governance. MAS has fostered a sandbox environment where FIs can experiment with AI in a controlled setting and share learnings. We see the continuation of initiatives like **Veritas** into 2025, perhaps expanding to cover new AI use cases (e.g. climate risk modelling with AI or regtech solutions for compliance). In the ethical realm, financial firms are increasingly aware that AI decisions must align with values and customer expectations. Cases of AI failures overseas (e.g. biased algorithms in credit limits) have been cautionary tales. Thus, many institutions in Singapore are instituting **AI ethics training** for their data science teams and developing internal checklists to vet AI applications before deployment (covering bias, privacy, robustness, etc.).

In summary, AI's transformation of financial services is in full swing by 2025, but it comes under the watchful eye of regulators and risk managers. MAS's combination of **principle-based guidelines (FEAT), practical toolkits (Veritas), and potential regulations** ensures that AI innovation does not run unchecked. Compliance requirements revolve around **transparency, fairness, and accountability**, demanding that FIs treat AI models with the same rigor as any other critical process. The financial institutions that thrive will be those that successfully **embed AI governance into their DNA** – leveraging AI for competitive advantage while maintaining customer trust and meeting regulatory standards.

Section 4: Cyber Resilience & Governance Best Practices

Strategic Governance Models for Cyber Resilience: In the face of escalating cyber threats, Singapore's financial institutions are re-engineering their governance structures to elevate cybersecurity to a core business risk. A key best practice for 2025 is to treat **cyber risk as an enterprise risk**, not merely an IT issue. This means establishing clear governance frameworks where the Board of Directors and senior management take ownership of cyber resilience. MAS's TRM Guidelines explicitly call for boards to have members with the necessary knowledge to oversee technology risks and to ensure an independent audit of cyber controls. Many leading banks in Singapore have responded by forming dedicated **Board Risk Committees or sub-committees for IT and Cybersecurity**. These committees receive regular reports on cyber posture, threat intelligence, and compliance status. At the management level, the role of the CISO (Chief Information Security Officer) has been empowered – CISOs now often report directly to the CEO or board in progressive firms, ensuring cyber strategy aligns with business objectives.

One emerging model is the **"Three Lines of Defence"** tailored for cybersecurity: (1) IT and business units manage cyber risks day-to-day (with security integrated into projects and operations), (2) a risk management function (or cyber risk office) provides

oversight, sets policies, and monitors adherence, and (3) internal audit (potentially with specialized cyber auditors) independently evaluates the effectiveness of controls. This model helps ingrain accountability at each level. Additionally, institutions are embracing **cyber risk appetite statements** – the board defines how much cyber risk the organization is willing to accept (e.g. zero tolerance for customer data loss, specific recovery time objectives for critical services, etc.), and this guides investment and control decisions. Setting these tolerances aligns with the operational resilience concept of impact tolerances (as encouraged by MAS and global regulators).

Integrating Cybersecurity into Enterprise Risk Management (ERM): A hallmark of resilient financial institutions is the integration of cybersecurity considerations into the overall ERM framework. In practice, this means when the firm looks at its top risks (credit, liquidity, operational, etc.), cyber is considered within each. For example, scenario planning for operational risk now invariably includes cyber-attack scenarios (ransomware taking down systems, data breach causing reputational damage, etc.). Progressive organizations conduct **enterprise-wide cyber risk assessments** that feed into risk registers and influence capital allocation (for banks under Basel rules, operational risk capital may implicitly cover cyber events). MAS has stressed that unexpected incidents will occur and that FIs must **"operate under the assumption of compromise"**. This has led to the adoption of frameworks like the **NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover)** as a structure to evaluate maturity across all business units. Many Singapore FIs map their controls and processes to NIST CSF or ISO 27001 and report this in ERM dashboards. Integrating cybersecurity into ERM also entails cross-functional collaboration: risk managers, IT security, compliance, and business continuity teams working together on risk mitigation strategies.

A concrete practice is the inclusion of **cyber risk scenarios in enterprise stress tests and exercises**. For instance, a major bank might simulate a scenario where a cyber-attack knocks out its online banking for 3 days during a peak period – the ERM team assesses financial, operational, and reputational impacts relative to risk appetite. Such exercises, often done in conjunction with MAS (which runs industry-wide cyber drills), inform investment in resilience (e.g. deciding to build more redundancy or buy insurance). Another best practice is linking **cybersecurity KPIs/KRIs** (Key Performance/Risk Indicators) to enterprise risk metrics. Examples include time to detect and respond to incidents, number of high-severity vulnerabilities open, training completion rates, etc., which are regularly reviewed by top management. This ensures cyber health is measurable and managed just like other business KPIs.

Consequence Management & Incident Response Governance: No defence is foolproof, so **incident response and consequence management** are critical components of governance. Financial institutions are establishing clear playbooks and decision frameworks for cyber incidents. A "Consequence Management" framework refers to how an organization manages the aftermath of a cyber event to minimize impact on customers, financial markets, and the institution's viability. MAS's guidelines and the new CSA requirements mandate timely reporting and action. Best practice here includes setting up a **Crisis Management Team** that includes not only IT, but also

executives from business, communications, legal and compliance. This team, often chaired by a C-suite executive, is empowered to make rapid decisions (for example, disconnecting systems, shutting down certain services to contain an attack, or notifying affected customers) in the event of a severe incident.

One key aspect is **board-level accountability in crises**. Boards are increasingly expected to be involved or at least kept apprised during significant cyber incidents. In 2025, it's advisable for boards of financial institutions to have a protocol: e.g. if a breach hits a certain threshold (data of X customers compromised or systems down >Y hours), the board chair and risk committee get notified within 24 hours and possibly convene an urgent meeting. Regulators (MAS and CSA) will certainly look at how leadership responds post-incident. Institutions should maintain an **incident response plan** that incorporates regulatory notification requirements (MAS, PDPC, CSA each have timelines and forms for reporting incidents) and ensures **communication is managed transparently and effectively** – both with regulators and with the public. The MAS BCM guidelines urge FIs to enhance **threat monitoring and environmental scanning** and to **conduct regular industry-wide exercises**, which speaks to the importance of practicing incident response in peacetime.

Another best practice in consequence management is having a **concrete recovery strategy and playbook**: for example, data backups that are offline (to survive ransomware), pre-negotiated contracts with forensic firms and PR agencies, and "clean environment" procedures to restore systems. Some Singapore banks have even established secondary secure operations centres (SOC) to coordinate response if the primary network is compromised. Additionally, **post-incident review** is a governance must-do: after any significant incident or even a near-miss, the organization should convene a review to identify root causes, control gaps, and lessons learned, and report these to the board and MAS. This continuous improvement loop is part of a mature cyber governance culture.

Cybersecurity Maturity Models: To gauge and improve their cyber resilience, financial institutions are leveraging maturity models tailored to their industry. A maturity model provides a structured way to assess current capabilities and plan improvements along a scale (from ad-hoc processes to optimized, adaptive ones). In Singapore, many institutions use the **NIST Framework tiering** or custom models influenced by MAS guidelines. For instance, a bank might assess its identity and access management processes as "Level 3 – defined" and aim to reach "Level 4 – managed" in the next year by implementing stronger privileged access controls and monitoring. The Association of Banks in Singapore (ABS), in partnership with MAS, previously rolled out the **Cyber Resilience Assessment Framework (C-RAF)** for banks, which is essentially a maturity assessment covering governance, defences, detection, and response. By 2025, such assessments are often integrated with regulatory expectations – MAS may ask for results of a bank's maturity assessment during supervisory reviews.

Tailored maturity models also help differentiate between various types of FIs (banks, insurers, payment services) – recognizing that a small fintech startup won't have the same capabilities as a large bank but can still chart a course to mature its controls

appropriate to its size/risk. **Continuous improvement** is the mantra: cybersecurity is not a one-and-done effort but an evolving journey, and maturity models provide the roadmap. We see institutions establishing dedicated programs to uplift their maturity in key domains: for example, a "Cloud Security Uplift" program to reach a target state of controls before moving more core systems to cloud, or a "Third-Party Risk Enhancement" project to implement new tools and governance for vendor risk in line with MAS's higher standards.

Importantly, these efforts are being tied back to international standards. Many Singapore financial firms seek alignment with **ISO 27001 certification** as a baseline. Some are also adopting the **MITRE ATT&CK framework** to ensure their detection capabilities cover known adversary tactics or using **Benchmarks like the FS-ISAC** (Financial Services Information Sharing and Analysis Center) maturity model to compare themselves against global peers. By 2025, cybersecurity maturity in Singapore's finance sector will be at the forefront in Asia – but the threat landscape will keep raising the bar. Thus, strong governance ensures that as new risks (like those from AI or quantum computing) emerge, the institution's risk management processes can adapt and incorporate those into their maturity roadmap.

Board and Executive Accountability: A recurring theme in best practices is the accountability of top leadership. Regulators worldwide (and MAS is no exception) increasingly expect CEOs and Boards to be **personally invested in cybersecurity oversight**. The tone from the top is critical for resilience – when leadership prioritizes cyber risk, the entire organization follows. In practical terms, boards should regularly schedule cybersecurity deep-dives, perhaps quarterly, where they review threat assessments, major projects (like security architecture upgrades), and regulatory compliance status. Some banks have even brought external cybersecurity experts onto their boards or as advisory members to strengthen oversight. Executive performance evaluations now often include cybersecurity objectives (e.g. reducing average incident response time or achieving certain training completion rates) to instil accountability. With MAS's focus on operational risk, there is an expectation that if a major breach occurs, the regulator will scrutinize whether management had taken due care – lacking proper governance could lead to regulatory actions or censure of individuals. Therefore, "**cyber literacy**" at the executive level is a best practice: many boards are undergoing cybersecurity training to understand risks like ransomware, AI threats, and to interpret technical risk reports.

Convergence of Cybersecurity and Business Strategy: Lastly, governance best practice involves embedding cybersecurity considerations into **business decision-making**. When a bank launches a new digital product or enters a partnership with a fintech, cyber risk assessment should be part of that strategic decision. This is sometimes facilitated by having the CISO or CIO involved early in product development and by using frameworks like **Secure-by-Design/Privacy-by-Design** as standard practice. By doing so, cybersecurity is not a blocker but rather an enabler of innovation – the business can move fast, but safely, because the risks have been addressed up front. In 2025's complex environment, the institutions that maintain trust and resilience

will be those that have made cybersecurity a foundational element of governance – championed from the boardroom to every employee.

Section 5: Strategic Recommendations for 2025 & Beyond

In light of the evolving landscape of 2025, Singapore's financial institutions – from large banks to boutique wealth managers and fintech firms – should undertake a set of strategic actions to enhance cybersecurity and ensure regulatory compliance. The following recommendations are tailored to the financial sector and mapped to both global best practices and MAS's anticipated direction:

1. Embrace a Proactive Cyber Risk Management Posture: FIs should shift from a reactive to a **proactive stance** on cybersecurity. This involves continually **updating risk assessments** for new threats (AI-driven attacks, cloud vulnerabilities, etc.) and scanning the horizon for emerging risks (e.g. quantum threats or new fraud tactics). Firms ought to implement **continuous threat intelligence and cyber monitoring** programs. By 2025, leveraging AI for cyber defence is essential – for example, deploying AI-driven security analytics that can detect anomalies indicative of an attack in real-time. This is in line with Gartner's cybersecurity trends which foresee AI integration in all aspects of cyber defence. Additionally, organizations should participate actively in information-sharing networks (such as ABS' Cyber Incident Response and Threat Intelligence sharing initiatives or **FS-ISAC** membership) to stay ahead of threat actors. Proactive risk management also means **regular red-team and penetration testing** – ideally aligned with frameworks like TIBER-EU (threat-led penetration testing) which could influence MAS's future approach. These tests help identify weaknesses before attackers do. Ultimately, a proactive posture demonstrates to regulators that the institution is not waiting for incidents but constantly hardening its defences.

2. Strengthen Operational Resilience and Incident Response Capabilities: Aligning with MAS's focus, financial firms should invest in robust **operational resilience frameworks**. Concretely, this means identifying **Critical Business Services** and mapping end-to-end dependencies now (if not already done), and then developing specific resilience plans for each. For each critical service (payments processing, trading, customer online access, etc.), define clear **impact tolerances** – how much downtime or data loss is acceptable – and ensure plans are in place to meet those tolerances even under extreme scenarios. These plans should encompass technology recovery (disaster recovery sites, cloud failovers) as well as business process workarounds. Perform **regular joint exercises** that involve both IT recovery and business continuity teams, simulating scenarios like a major cyber attack coupled with a technology outage. The goal is to cultivate muscle memory and inter-department coordination. Additionally, update incident response plans to incorporate **new regulatory reporting requirements** (for example, CSA's expanded incident definitions). FIs should ensure they can detect and report incidents, including third-party incidents, within required timelines (MAS expects prompt reporting, CSA now covers supply chain incidents too). We recommend creating a **"severe incident playbook"** that outlines the first 24-48 hour actions for various incident types (ransomware, data

breach, system outage) and includes draft communications to regulators and customers – this preparation greatly enhances response speed and efficacy.

3. Enhance Third-Party and Supply Chain Risk Management: Given the interconnected nature of financial services, an institution is only as secure as its weakest vendor. We recommend immediately **reviewing and bolstering third-party risk management (TPRM)** programs. This includes maintaining a comprehensive inventory of all third parties and fourth parties (sub-contractors) who handle sensitive data or critical systems. For each, ensure there are up-to-date security due diligence records – ideally moving toward an *continuous monitoring* approach rather than a checkbox annual review. Leverage standardized assessments where possible (e.g. the CSA's Cloud Controls Matrix or the Shared Assessments Program) and insist on right-to-audit and breach notification clauses in contracts. Align these efforts with MAS's outsourcing guidelines and the new expectations that critical service providers meet the institution's own recovery objectives. A strategic move is to implement **risk-based segmentation of suppliers**: focus more resources on auditing and testing those deemed high-risk (e.g. cloud providers, fintech partners with access to core systems). In addition, consider technical controls such as **network segmentation for third-party connections**, and requiring multi-factor authentication and encryption on any third-party access. By 2025, regulators might push for more assurance from critical tech vendors (the way DORA in EU will oversee cloud providers). Singapore FIs can get ahead by engaging key providers in resilience discussions now – e.g., joint incident exercises with cloud providers or key fintech partners.

4. Adopt International Cybersecurity Standards and Best Practices: To ensure a robust and recognized security posture, financial firms should map their internal controls to global standards like **ISO/IEC 27001**, **NIST Cybersecurity Framework**, and where applicable, **PCI-DSS** for payment data. This mapping not only helps in meeting MAS guidelines (which are broadly consistent with these standards) but also prepares firms for international operations and assessments. Many Singapore institutions already use NIST CSF as a reporting tool (covering Identify, Protect, Detect, Respond, Recover). We recommend conducting a **gap analysis** against these frameworks in 2024 if not done recently, and addressing any gaps in 2025. For example, NIST might highlight the need for better anomaly detection or more comprehensive response planning – areas which can then be improved. Additionally, stay aligned with sector-specific frameworks: the **Basel Committee's cyber resilience paper**, the **FFIEC Cyber Assessment Tool** (used by U.S. banks), or **ENISA guidelines** for EU operations. By aligning with these, Singapore FIs will meet not just local but international expectations. In doing so, map recommendations to MAS's own publications – for instance, if MAS is anticipated to release further guidance on **ICT third-party risk (similar to DORA's requirements)**, having adopted such controls early will ensure compliance and smooth audits.

5. Invest in AI and Automation – Securely and Ethically: Embracing new technology is a necessity for both business competitiveness and security effectiveness. We recommend financial institutions leverage **AI and machine learning for cybersecurity** – such as user behaviour analytics, threat hunting algorithms, and automated incident

response (SOAR – Security Orchestration, Automation and Response). These tools can significantly reduce detection and reaction times. However, when implementing AI, do so **with strong governance** (per Section 3): apply the FEAT principles to any in-house AI security systems to ensure they do not inadvertently violate privacy or fairness (e.g., if monitoring employee behaviour, be mindful of PDPA and ethical boundaries). On the flip side, manage the risks of AI usage in business processes by establishing an **AI governance committee** and internal controls as discussed. It is advisable to pilot new AI innovations in a controlled environment (perhaps under MAS's regulatory sandbox if appropriate) to validate safety and compliance before scaling up. One actionable strategy is to **develop an AI inventory** – catalogue all AI/ML models in use, their purpose, data inputs, and have a designated owner for each. This will aid in monitoring and compliance (especially as regulators like MAS/PDPC may ask about AI deployments).

6. Cybersecurity Culture and Training 2.0: Strengthening human defences is as important as technology. Firms should implement next-generation training that reflects 2025 realities – for example, running drills where staff are exposed to highly realistic phishing emails or deepfake calls to test their alertness. Regular training should cover new scam typologies hitting Singapore (like those highlighted by the police and CSA) so employees and front-line staff (who deal with customers) can also educate customers. Cultivate a culture where cybersecurity is part of everyone's job – incentivize reporting of suspicious activities and treat near-misses as learning opportunities rather than failures. Board and executive cyber education is crucial too (as noted, ensure leadership attends at least annual training or seminars on emerging cyber risks and regulatory changes). A strong security culture is often cited by regulators as a hallmark of resilient institutions.

7. Align with MAS's Future Direction & Engage Regulators Proactively: MAS has laid out a vision in its Industry Transformation Map 2025 that includes secure digital infrastructure as a pillar. Financial firms should align their strategy to support this vision – for example, participating in national initiatives like **digital identity (Singpass) integration, secure payment hubs, and MAS's Quantum Computing risk study**. Engaging with regulators through consultations and forums can provide insight into MAS's anticipated moves. We foresee MAS may issue further guidance on areas like cloud concentration risk, fintech partnerships, or even **environmental cyber risks** (like climate-related outage scenarios). Firms that engage in dialogue can help shape pragmatic regulations and be early adopters of best practices. Also, be prepared for **increased regulatory scrutiny**: for instance, MAS could conduct thematic examinations on AI governance or third-party risk. To be ready, institutions should consider **internal audits or independent reviews** of these domains in 2025, addressing any weaknesses before the regulator knocks.

8. Enhance Data Protection and Privacy Compliance: With PDPC's new guidelines and ongoing public concern about data privacy, financial institutions must double-down on data governance. Implement **privacy-by-design** in projects, minimize personal data collection to what is necessary, and ensure robust encryption/tokenization of sensitive data (both at rest and in transit). Establish

workflows for handling data subject requests efficiently (access, correction, withdrawal of consent) as awareness grows. Also crucial is to have a strong data breach response process to meet PDPC's reporting timeline (within 72 hours of assessment that a breach is notifiable, typically). Given the hefty fines PDPC can levy (up to 10% of annual turnover for serious breaches), compliance is not just regulatory but financial risk management.

9. Leverage Frameworks for Cyber Risk Assessment and Insurance: As cyber risks grow, transferring some risk through **cyber insurance** is increasingly common. However, insurers are raising requirements and premiums. Use recognized frameworks to **assess cyber risk in monetary terms** (there are models like FAIR – Factor Analysis of Information Risk) to inform how much risk to retain vs. insure. Ensure any insurance purchase aligns with the institution's actual risk exposure and that policy terms cover likely threat scenarios (some policies may exclude state-sponsored attacks, for example, which needs consideration given the threat landscape). While insurance doesn't reduce risk, the process of obtaining it often reveals gaps (via insurer security questionnaires or underwriting assessments), which can be addressed.

10. Continuous Improvement via Cybersecurity Maturity Roadmap: Develop a 3-year cybersecurity roadmap that aligns with business strategy and the evolving threat/regulatory environment. Include milestones such as achieving certain maturity level improvements, adopting new security technologies (e.g. zero trust architecture components, SASE for secure access, etc.), and meeting upcoming regulatory deadlines. Tie this roadmap to budget and resources – make the business case that cybersecurity and compliance investments are foundational to maintaining customer trust and operational continuity (thus avoiding far greater costs of breaches or regulatory penalties). This strategic plan should be reviewed annually against the threat landscape and MAS guidelines updates, adjusting course as needed. Boards should be apprised of progress regularly, reinforcing oversight.

By implementing these strategies, financial services firms in Singapore can significantly **enhance their cybersecurity posture and compliance readiness** going into 2025 and beyond. They will not only meet the immediate requirements of MAS, PDPC, and CSA regulations, but also build adaptive capacity to handle the unknown challenges of the future. The overarching aim is to create a **virtuous cycle of security and trust** – robust cybersecurity earns customer trust, which in turn enables Singapore's financial industry to innovate and grow confidently in the digital era. As Vincent Loy of MAS aptly noted, "If there's no trust, FinTech will not survive or develop further"– hence, investing in cybersecurity and governance is investing in the very future of financial services.

Appendices & References

- **MAS Guidelines and Notices (2024-2025):** Key references include MAS's **Technology Risk Management Guidelines (2021)** for governance and controls, the **Business Continuity Management Guidelines (2022)** emphasizing operational resilience, and MAS's various **Notices** (e.g. on Cyber Hygiene, TRM for Digital Payment Token service providers) which set minimum standards.

MAS's press releases on initiatives like the **Veritas Responsible AI Toolkit (2022-2023)**and the **COSMIC platform (2024)** are also pertinent.

- **PDPC Regulations and Guidelines:** The **Personal Data Protection Act (PDPA)** and its recent amendments form the legal baseline for data protection. The PDPC's **Advisory Guidelines on Use of Personal Data in AI Systems (Mar 2024)** are critical for understanding how AI and privacy intersect. PDPC also provides sector-specific guidance and the Model AI Governance Framework which can be used as reference for best practices.
- **Cyber Security Agency (CSA) Framework:** The **Cybersecurity Act (2018, amended 2024)** and associated **Codes of Practice** for Critical Information Infrastructure operators outline mandatory incident reporting and security requirements. Financial institutions classified as CII should refer to these, alongside MAS guidelines. CSA's annual **Singapore Cyber Landscape** reports (latest 2023) offer insights into threat trends.
- **International Standards and Regulations:** For benchmarking, FIs should look at **DORA (EU Digital Operational Resilience Act)**, which from Jan 2025 imposes comprehensive ICT risk management obligations – useful for firms operating in the EU or as best-practice. The **NIST Cybersecurity Framework** and **ISO 27001/27701** (for information security and privacy) are widely recognized standards that complement MAS's requirements. In AI governance, the upcoming **EU AI Act** and OECD AI Principles provide a view of global regulatory direction, reinforcing the themes of fairness and transparency in AI.
- **Industry Reports and Surveys:** Numerous industry publications informed this outlook. For example, the **WEF Global Cybersecurity Outlook 2024** and experts' predictions highlight the prominence of AI threats and the need for board-level cyber expertise. Security firms' reports like **Kaspersky, FireEye, IBM X-Force** etc., often detail financial sector threat trends (malware, APT campaigns). The **Thales Data Threat Report 2024 – Financial Services Edition** provides data on cloud security perceptions and breach statistics. Local surveys, such as those by **Deloitte or KPMG on financial services cybersecurity 2024**, can offer Singapore-specific insights and metrics.
- **Notable Statistics (Post-2023):** A selection of data points underpinning our analysis: "346 ransomware attacks on SG financial sector in 2023"(QBE Insurance report), "73% of financial firms using multi-cloud in 2024" (Thales), "64% of APAC FIs saw increase in digital fraud" (Fintech News Asia survey), "Deepfake fraud losses to hit $40B by 2027" (DeepMedia/VentureBeat), and "over 80% of orgs faced a cyber incident in 2023" (CSA Cybersecurity Health Report 2023). These illustrate the scale of issues at hand.
- **Frameworks and Tools:** Appendices may include frameworks like the **MAS-ABS Cyber Incident Response Guidelines**, the **FEAT Checklist** (to operationalize Fairness, Ethics, Accountability, Transparency), a sample **Cyber Incident Playbook**, and a template for a **Third-Party Risk Assessment Checklist** aligned with MAS expectations.
- **Strategic Frameworks:** To implement recommendations, FIs can reference frameworks like **NIST SP 800-61** for incident handling, **COBIT 2019** for governance, and **Carnegie Mellon's CERT Resilience Management Model**

(CERT-RMM) for maturity modelling. Aligning these with the organization's context in Singapore will support a structured improvement in cyber resilience.