aphore

WHY ASIC'S CYBERSECURITY EXPECTATIONS DEMAND A HIGHER STANDARD FOR AFSL'S

An Aphore White Paper - March 2025

Executive Summary

Australian businesses, particularly those holding Australian Financial Services Licences (AFSLs), face a heightened cyber threat environment and increased regulatory scrutiny. The Australian Cyber Security Centre's **Essential Eight (E8)** framework is often touted as a baseline for cyber defence, but **relying on the Essential Eight alone is no longer sufficient** to ensure cyber resilience or meet the legal obligations set by ASIC. Recent enforcement actions – notably ASIC's lawsuit against FIIG Securities Limited (FIIG) in 2025 – underscore that a checklist of eight technical controls leaves critical gaps in governance, detection, and response. This white paper argues that AFSL holders who focus narrowly on the Essential Eight expose themselves to **unacceptable risk and regulatory non-compliance**, and it outlines a broader, more mature cybersecurity baseline aligned with international standards (ISO 27001, ISO 27035) and the NIST Cybersecurity Framework.

We demonstrate that **ASIC's expectations for cyber resilience** go well beyond the Essential Eight. ASIC now expects active board oversight of cyber risks, robust incident response planning, continuous monitoring, and adequate resourcing – areas largely unaddressed by the Essential Eight. The FIIG Securities case is used as a central example of these expectations: FIIG allegedly failed to patch systems, monitor for intrusions, or dedicate sufficient resources to cybersecurity, leading to a 385GB data breach. ASIC's action against FIIG (and the earlier RI Advice case in 2022) makes clear that "adequate risk management systems" under the Corporations Act mean a comprehensive security program, not just basic IT fixes.

Key points and recommendations:

- **Essential Eight Limitations:** The Essential Eight provides a useful foundation but covers only basic technical controls (e.g. patching, admin restrictions, backups). It lacks focus on governance, threat detection, incident response, and human factors. Organisations solely adhering to E8 remain vulnerable to sophisticated attacks and **will fall short of ASIC's cyber maturity expectations**.
- **Regulatory Expectations:** ASIC has explicitly stated that AFSL holders *must* proactively manage cyber risks. This includes board-level engagement, regular cyber risk assessments, and incident response preparedness. In the FIIG case, ASIC alleges the company's prolonged cybersecurity failures (over 4+ years) breached its AFSL obligations. Regulators now expect **cybersecurity to be treated as an ongoing, whole-of-business governance issue**, not just an IT issue.
- **FIIG Securities Case Lessons:** FIIG's breach and ASIC's ensuing legal action illustrate what is expected in practice. ASIC highlighted FIIG's lack of an incident response plan, poor patching, weak firewall configurations, no cybersecurity

training, and insufficient dedicated resources. The attack on FIIG went *undetected for nearly three weeks* until alerted by government agencies, showing the dangers of inadequate monitoring. Boards and executives of AFSLs should view this case as a warning that **cyber governance and accountability are enforceable obligations**.

- **Beyond Essential Eight – Embracing ISO and NIST:** A comparative analysis of Essential Eight vs. ISO 27001, ISO 27035, and NIST Cybersecurity Framework reveals significant gaps. International frameworks encompass **Governance, Identify, Detect, Respond, Recover** functions that E8 does not address. We provide a table mapping these differences and show how adopting ISO/NIST-based controls can elevate an organisation's cyber maturity to meet ASIC's criteria.
- **Recommended Cybersecurity Maturity Baseline:** AFSLs should adopt a more comprehensive security baseline that includes:
    - **Governance:** Establish a cybersecurity governance framework (e.g. an ISO 27001-aligned Information Security Management System) with board oversight, risk assessments, policies, and regular audits.
    - **Incident Response:** Implement an incident response plan (per ISO 27035 guidelines) that is approved by leadership, communicated to staff, and tested annually.
    - **Detection & Monitoring:** Deploy advanced detection tools like Endpoint Detection and Response (EDR) on all systems and aggregate logs into a Security Information and Event Management (SIEM) system for continuous monitoring. Ensure skilled personnel or managed services monitor alerts daily.
    - **Backup & Recovery:** Go beyond "daily backups" – ensure **secure, tested backups** and a robust disaster recovery capability, with offline backup copies and regular restoration drills.
    - **Skilled Personnel & Roles:** Designate qualified cybersecurity roles or outsource to specialists. Relying on generalist IT staff or a basic MSP is no longer sufficient – organisations need professionals certified in ISO 27001 and familiar with NIST, or *CARR-certified* consultants (Cyber Assurance Risk Rating program) from reputable firms, to provide expert guidance.
- **Human Factor and Skills Uplift:** The paper dedicates a section to the human element. We explain why building internal capability (or engaging external experts) is critical. Certifications such as **ISO 27001 Lead Auditor/Implementer**, vendor certifications (e.g. Microsoft Certified Professional in security, AWS security certs), and emerging credentials like *CARR* demonstrate the expertise now expected. ASIC's guidance to boards even suggests bringing in external cyber experts if in-house knowledge is lacking.
- **Cost Estimates and Options (Australia-specific):** To help business leaders plan, we provide indicative cost ranges (in AUD) for key security enhancements: EDR solutions (typically $50–$100 per endpoint/year), SIEM or managed log monitoring services, cyber insurance premiums for SMEs vs larger firms, external security reviews and incident response retainers, and staff training or certification programs. We outline **cost-effective options** and note that

investing in these controls now can avert far greater costs from breaches or regulatory penalties.

Overall, this white paper delivers a persuasive case that AFSL holders must **go beyond the Essential Eight**. It is a call to action for business leaders – including boards, CEOs, and compliance managers – to elevate their cyber maturity. By adopting a broader framework incorporating ISO and NIST best practices, ensuring proper governance and expert skills, and allocating budget to critical controls, organisations will not only bolster their resilience against modern cyber threats but also satisfy ASIC's stringent expectations for cyber risk management and compliance.

Introduction

Cybersecurity has rapidly evolved from a technical concern to a **strategic business issue**. In Australia, financial services companies and AFSL holders are under intense pressure to shore up their cyber defences or face legal consequences. High-profile data breaches and regulator interventions have highlighted that minimal compliance is not enough – **"tick-the-box" approaches to cyber risk can lead to devastating breaches and enforcement actions**.

The Australian Cyber Security Centre (ACSC) publishes the **"Essential Eight"** mitigation strategies as a baseline for security. Many small-to-medium enterprises (SMEs) have adopted the Essential Eight, assuming it provides sufficient protection. However, ASIC – the regulator for financial services – has signalled that it expects far more. Cyber resilience, in ASIC's view, demands comprehensive risk management. This was made evident by ASIC's groundbreaking legal actions against RI Advice in 2022 and FIIG Securities in 2025 for cybersecurity failures.

In this context, business leaders must ask: **Is our current cybersecurity baseline truly adequate?** This white paper examines that question. We argue that **focusing on the Essential Eight alone leaves organisations exposed** – both to sophisticated cyber threats that exploit gaps beyond those eight controls, and to regulatory non-compliance since ASIC deems such gaps as failures of duty. We will use the case of FIIG Securities as a cautionary tale and reference point throughout, as it provides concrete examples of what can go wrong and what regulators expect instead.

This paper is structured to first explain the limitations of the Essential Eight framework in today's threat landscape and against ASIC's expectations (Sections 2 and 3). We then compare the Essential Eight with global frameworks like **ISO 27001, ISO 27035, and the NIST Cybersecurity Framework** to illustrate the broader dimensions of cybersecurity maturity that Australian financial firms should consider (Section 4). Next, we present a recommended maturity baseline for AFSL holders – essentially a more holistic checklist of controls and practices – covering governance, incident response, detection/monitoring, recovery, and people factors (Section 5). We devote Section 6 to

the *human element*, discussing why cybersecurity expertise and certified skills are now required for resilience. In Section 7, we provide **practical guidance on budgeting and resourcing**, with localised cost estimates for key solutions like EDR, SIEM, cyber insurance, etc., to help decision-makers plan investments. Throughout, the language and framing are tailored for business audiences, focusing on risk, compliance, and solutions rather than technical minutiae.

By the end of this paper, AFSL compliance teams, company directors, and executives will have a clearer understanding of why **"doing the basics" is insufficient**, what a robust cybersecurity program entails, and how to take actionable steps beyond the Essential Eight to achieve true cyber resilience and meet ASIC's standards.

The Essential Eight Framework and Its Limitations

The **ASD Essential Eight** is a set of eight mitigation strategies recommended by the Australian Signals Directorate (ASD) and ACSC as the most effective technical controls to prevent or limit cyber intrusions. Introduced in 2017, the Essential Eight distils a longer list of 37 ASD strategies down to the top eight that **mitigate the majority of common cyber attacks**. The eight controls are:

Figure 1: The ASD Essential Eight controls cover fundamental technical defence measures (application control, patching, macro hardening, user application hardening, restricting admin privileges, OS patching, multi-factor authentication, and regular backups). These create a baseline security posture.

Implemented at higher maturity levels, the Essential Eight can significantly reduce an organisation's exposure to untargeted or commodity attacks. In fact, the ACSC has claimed that adopting the Essential Eight can **mitigate around 85% of cyber attacks** in general. For many resource-constrained businesses, E8 offers a **clear, actionable starting point**: it is relatively straightforward, cost-effective, and focuses on practical steps like keeping software up-to-date and restricting administrative access.

However, while the Essential Eight is a **valuable foundation**, it is **not a comprehensive security framework**. There are critical aspects of cybersecurity that E8 does *not* cover, and modern threats often exploit those very gaps. Even the ACSC acknowledges that "the Essential Eight will not mitigate against *all* cyber threats" and recommends additional controls beyond those eight. Similarly, independent analysts note that E8 is a **"point-in-time" snapshot of controls** and lacks the continuous risk management processes found in broader frameworks.

Where the Essential Eight Falls Short

1. Limited Scope (Technical Controls Only): The Essential Eight focuses almost exclusively on technical measures for endpoint and system hardening. It does not address **governance, risk assessment, people, or process controls**. As one comparative study noted, E8 "focuses primarily on technical controls and may not address broader organisational and management aspects of cybersecurity". For example, E8 says nothing explicit about having security policies, conducting cyber risk assessments, or ensuring executive oversight – yet these are fundamental to a mature security posture and are expected by regulators.

2. No Coverage of Detection and Response: Perhaps the most significant gap is that Essential Eight lacks controls for **detecting intrusions, responding to incidents, and recovering systems**. The framework's controls (like patching and MFA) are preventive in nature. They aim to stop breaches from happening, but **what if an attacker still gets through?** E8 provides no guidance on monitoring network activity for threats, no requirement for incident response planning, and no measures for containment or eradication of threats post-breach. Modern consensus in cybersecurity (reflected in frameworks like NIST CSF and ISO 27035) is that detection and response capabilities are just as crucial as prevention. By ignoring these, an organisation following E8 might have strong locks on the doors but no alarms or emergency plans for when the locks are picked.

3. Insufficient Guidance on *Governance and Oversight*: The Essential Eight does not require management involvement or continuous improvement processes. In contrast, frameworks like ISO 27001 demand that top management be engaged and that security controls be continuously reviewed and improved. The result is that organisations focusing only on E8 might treat cybersecurity as a one-off IT project ("set and forget"), rather than an ongoing risk management function. ASIC has warned that **"cybersecurity isn't a set-and-forget matter"** – companies must regularly check and update their measures. Essential Eight's static nature can breed a false sense of

security if organisations do not also implement processes to review emerging threats and adapt controls accordingly.

4. Not Risk-Based or Flexible: Essential Eight is a *one-size-fits-all* prescription. It does not involve any formal **risk assessment** to tailor controls to the organisation's unique threats and assets. As a result, some businesses may implement certain E8 controls that are less relevant to their environment while overlooking other critical controls not in the E8 list. The framework has maturity levels (0 to 3) indicating increasing robustness, but even at Maturity Level 3, E8 remains a finite set of controls. In contrast, a risk-based framework (like ISO or NIST) would consider the specific context – for instance, if an organisation relies heavily on cloud services, network segmentation and cloud security monitoring might be critical (areas not covered by E8). A cybersecurity program that is **solely E8-driven might miss such context-specific measures**. One notable example: **network segmentation** – a key security practice to contain breaches – is not part of Essential Eight, and has been cited as a "notable gap" in E8 by experts.

5. Compliance ≠ Security (Checkbox Mentality): There is a danger that SMEs or any organisation using E8 might treat it as a simple compliance checklist ("we did the eight things, so we must be secure"). This mentality is risky. It's important to remember that **Essential Eight compliance by itself does not equal cyber resilience**. The Western Australian Auditor General's review of agencies' E8 implementations found many instances where controls were "partially implemented or not working as expected, leaving entities vulnerable" – and even noted that many organisations *overestimated* their E8 maturity in self-assessments. This suggests that just attempting to implement E8 isn't enough; the quality and consistency of implementation matter greatly, and without broader governance, even those eight controls may fail. ASIC's own surveillance (Cyber Pulse Survey 2023) likely found similar issues across industry, prompting its call for greater vigilance beyond basic measures.

In summary, **the Essential Eight should be viewed as the beginning, not the end, of an organisation's cybersecurity journey**. Businesses that limit their focus to these eight areas risk leaving significant blind spots. The modern threat landscape – ransomware gangs, sophisticated phishing, zero-day exploits, supply chain attacks – will find and exploit weaknesses not covered by a narrow defence. And as we discuss next, Australia's regulators have made it clear that they expect a more **comprehensive approach to cyber risk management**, especially from financial services entities entrusted with sensitive data and client assets.

aphore

ASIC's Expectations for Cyber Resilience vs. Essential Eight

ASIC has steadily raised the bar on what it considers **"adequate" cybersecurity for financial services licensees**. Under the Corporations Act 2001, AFSL holders have a general obligation to **"do all things necessary to ensure... services are provided efficiently, honestly and fairly"** and to have **"adequate risk management systems"**. In recent years, ASIC has made clear that cyber risk is included in these obligations – in other words, if you don't manage cyber risks properly, you may be in breach of your AFSL conditions.

Importantly, ASIC's expectations for cyber resilience encompass much more than a checklist of technical controls. Based on ASIC's public communications and enforcement actions, we can identify several key components of what ASIC looks for in a firm's cybersecurity maturity:

1. Cyber Risk Governance and Board Oversight: ASIC expects that organisations treat cyber risk as a matter of governance, not just IT operations. This means **board of directors and senior management involvement**. In the RI Advice judgment, the Federal Court explicitly noted that cybersecurity risk is significant to financial services businesses, and while it's impossible to reduce that risk to zero, it must be *"materially reduced... through adequate cybersecurity documentation and controls to an acceptable level."*. ASIC has published guidance for boards, posing questions such as "How often is the cyber resilience program reviewed at the board level?" and whether boards might need additional expertise or external input on cyber matters. In practice, this implies that regulators expect boards to regularly review cyber risks, allocate budget and resources, and **hold management accountable** for maintaining robust cyber defences. Simply having the IT team implement Essential Eight controls in isolation would not satisfy this expectation; the effort needs to be visible and supported at the board level.

2. Adequate Resourcing (People and Financial): One of ASIC's allegations in the FIIG Securities case was the failure to have *"adequate human, technological and financial resources to manage cyber security."*. This points to an expectation that firms invest appropriately in cybersecurity – including hiring or contracting skilled cybersecurity personnel and deploying suitable tools. In FIIG's situation, despite being a significant player in fixed-income investment services, their cyber function was under-resourced. Regulators will ask: do you have a dedicated security officer or team? Are staff trained in cyber awareness? Have you invested in technologies like firewalls, intrusion detection, backup solutions, etc., at a scale commensurate with your risk? A small business that only assigns cybersecurity as a part-time duty to an IT generalist (or outsources IT to a basic MSP with no security specialization) may be viewed as not meeting this criterion. Essential Eight doesn't spell out resource commitments, but ASIC clearly does – you need *enough* people and budget to implement and monitor controls effectively.

3. Risk Management Framework and Continuous Improvement: ASIC expects licensees to have a risk management framework that explicitly covers cyber risk. That includes identifying threats, assessing their potential impact, and implementing controls – and then **regularly evaluating those controls**. From ASIC's 2015 report *Cyber Resilience: Health Check* to the 2023 *Cyber Pulse Survey*, a common theme is that firms should integrate cyber into overall risk management. In the FIIG case, an interesting detail is that FIIG actually had policies (an IT security policy and later a Cyber and Information Security Policy) that listed certain controls – but **FIIG failed to implement many of those controls in practice**. ASIC will not be impressed by paper policies; they want to see effective execution and regular reviews. For example, ASIC would expect that **patch management is documented and ongoing**, that security controls are tested (through audits or penetration tests), and that incidents or near-misses lead to improvements. Essential Eight by itself doesn't enforce that kind of process (it's static), whereas ASIC's notion of "adequate systems" implies an active cycle of improvement.

4. Incident Response Planning and Recovery Capabilities: A glaring lesson from the FIIG breach was the lack of a proper incident response. FIIG was allegedly unaware that an attacker had been inside its network from 19 May 2023 until an external alert on 2 June. Even then, FIIG did not **investigate and respond** until 8 June, almost a week after being notified of suspicious activity. This delayed response likely exacerbated the damage (385GB of data stolen, affecting 18,000 clients). ASIC's expectations here are straightforward: firms must have a **documented and tested incident response plan**. In Annexure A of ASIC's concise statement against FIIG, the first "missing cybersecurity measure" listed is a *"cyber incident response plan, approved by the organisation, and communicated and accessible to all employees,"* covering detection, analysis, containment, eradication, recovery, and regulatory notification duties. Furthermore, that plan should be tested at least annually. This is fully outside the scope of Essential Eight, which has no control related to incident response. Yet from ASIC's perspective, having no incident response plan is a serious deficiency. Likewise, **business continuity and disaster recovery** preparations (e.g. the ability to restore systems from backups and continue operations) are expected. Essential Eight does have "daily backups" as one control, but ASIC will expect more – such as secure off-site backups, and recovery drills to ensure data integrity. In short, readiness to *detect, respond, and recover* is a pillar of cyber resilience in the regulator's eyes.

5. Technical Controls at a Higher Standard: Even within the realm of technical controls, ASIC's bar can be higher than the bare minimum. Essential Eight includes basic elements like patching and multi-factor authentication. ASIC explicitly called out FIIG for failing to patch systems and update software for years, and not enforcing MFA for all remote users until around 2022. In essence, FIIG didn't even meet the Essential Eight basics, which made ASIC's case easier. But consider that FIIG was also accused of not having "appropriately configured and monitored firewalls". Firewall configuration is not one of the Essential Eight per se; it's a lower-level detail. ASIC going into that detail indicates they expect organisations to implement *defence in depth*. In Annexure A, ASIC outlined that **"next-generation" firewalls with outbound filtering rules** (to block unnecessary internet communications and risky services like FTP) should have

been in place. They also noted disabling legacy authentication protocols (like NTLMv1) as an expected measure. These specifics align with good practice, but not specifically with E8. The takeaway is that ASIC's view of "adequate technical controls" might extend beyond the Essential Eight, especially as threats evolve. ASIC Chair Joe Longo even remarked in the context of the FIIG case that companies need to *"follow the advice of the ASD's ACSC"*– which includes E8 – but also to *"proactively and regularly check the adequacy"* of measures. If the threat environment has outpaced the Essential Eight, ASIC expects companies to adapt accordingly.

To crystallize the difference: **Essential Eight is a baseline; ASIC's expectations are a baseline plus proof of diligence and broader risk coverage.** An AFSL holder who can demonstrate they have implemented E8 *and* have strong governance, incident response, monitoring, training, etc., will be far better positioned to satisfy regulators (and, incidentally, to avoid breaches) than one who simply implements the eight controls and assumes that duty is discharged.

In the next section, we will use the FIIG Securities case details to highlight exactly what ASIC found lacking and how that compares to the Essential Eight. This case serves as a concrete reference of what regulators now demand in terms of cyber governance, incident handling, and accountability.

Case in Point: FIIG Securities Limited vs. ASIC – Lessons in Cyber Governance

The **FIIG Securities Limited** case (ASIC v FIIG, Federal Court proceeding QUD144/2025) is a watershed moment in Australian cyber regulation. It is only the second time ASIC has taken an entity to court over cybersecurity (the first being RI Advice in 2022), and it vividly illustrates the gap between a minimalist approach to security and what regulators deem acceptable. Let's unpack the case and its implications:

Background: FIIG Securities is a financial services firm providing fixed-income investment services, including custodial services for clients (holding significant client assets and data). Between 2019 and 2023, FIIG suffered a serious cyber incident – a malicious actor gained entry to its network on 19 May 2023 and remained undetected until 8 June 2023. In that time, the attacker exfiltrated approximately **385 GB of sensitive data** including personal information (names, addresses, dates of birth, IDs, bank details, tax file numbers) of around 18,000 clients. The data was later released on the dark web, putting those individuals at risk of identity theft and fraud. ASIC alleges that FIIG's cybersecurity failings "enabled" this theft.

ASIC's Allegations: ASIC's concise statement and press release outline a series of specific deficiencies at FIIG. These essentially form a checklist of what was *not* done at FIIG, and by extension, what **should** have been done. Some key allegations:

- **No effective firewall monitoring:** FIIG did not have "appropriately configured and monitored firewalls to protect against cyber attacks". It's likely the attacker gained initial access due to firewall misconfiguration. ASIC expected FIIG to not only have next-gen firewalls but also to monitor them for suspicious traffic (e.g. alerts on unusual outbound connections). This ties to the *detection* expectation.
- **Failure to update and patch systems:** FIIG allegedly failed to patch critical software and operating systems over **a multi-year period**. Court documents show that a structured patch management process was absent; there was no practice of applying critical patches within 1 month or standard patches within 3 months, as would be reasonable policy. Some systems were running outdated OS versions unsupported by vendors. This is a direct overlap with Essential Eight (patching is two of the E8 controls), meaning FIIG didn't even meet those basics. The hacker likely exploited known vulnerabilities that FIIG hadn't patched – a clear sign of lax risk management.
- **Weak access controls (privileged access and authentication):** ASIC highlighted that FIIG did not enforce multi-factor authentication (MFA) for all remote users until 2022, leaving remote access accounts (e.g. VPN, remote desktop) protected only by passwords for years. Additionally, FIIG lacked proper **privileged access management** – they did not ensure admin accounts were separate and more secure than regular accounts. In fact, FIIG's own policies said admin accounts shouldn't be used for day-to-day work, but that control was "not implemented". These failings made it easier for the attacker to move within FIIG's network and extract data without detection, possibly by compromising an admin credential. ASIC expects robust access controls, consistent with both E8 (which includes restricting admin privileges and MFA) and good practice.
- **No security monitoring or threat detection:** Perhaps the most damning aspect was that FIIG had **no Security Information and Event Management (SIEM) system or daily log monitoring for unusual activity**. Annexure A from ASIC lists that FIIG should have had SIEM software aggregating logs in real time and storing them for at least 90 days, with daily review by IT personnel capable of spotting anomalies. This was not in place. Consequently, when the attacker breached FIIG on 19 May, no alarms went off; the intruder operated freely for weeks – a period during which a well-tuned SIEM or EDR might have detected large data transfers or odd after-hours logins. FIIG only learned of the breach via an external tip-off (ASD's Cyber Security Centre) on 2 June. Even then, lacking an incident plan, they waited nearly a week to act. **Regulators now clearly expect that organisations *actively monitor* their environments.** As ASIC stated, had FIIG been monitoring, they would have detected the suspicious activity by around 23 May and possibly prevented a lot of the data theft. This is a key lesson: E8 doesn't require SIEM or 24/7 monitoring, but ASIC practically does for any organisation with valuable data.
- **No incident response plan and slow response:** The fact that FIIG took six days after notification to begin investigating indicates a breakdown in incident response readiness. Annexure A explicitly cites the absence of a formal incident response plan as a failing. Without a plan, FIIG likely scrambled to figure out roles, gather forensic data, and notify clients/regulators – all in a delayed and ad hoc fashion. ASIC's enforcement sends a message that **having an IR plan and**

swift response procedures is part of being a fit and proper licensee. In FIIG's case, client notifications and containment happened far later than they should have. It's worth noting ASIC has regulatory requirements around timely breach reporting (e.g., for privacy breaches, companies are expected to notify affected individuals and possibly the Office of the Australian Information Commissioner within set timeframes). An AFSL holder dragging its feet in an incident can be seen as failing its obligations to act efficiently, honestly, fairly.

- **Lack of staff training and awareness:** Another element ASIC pointed out is FIIG's failure to provide mandatory cybersecurity awareness training to staff. Human error (like falling for phishing emails) is a leading cause of breaches. While E8 doesn't mention user training, ASIC considers it important enough to include in charges. In effect, ASIC expects a security-aware culture. Employees should know how to spot phishing, handle sensitive data, and respond to potential security incidents. FIIG apparently had no regular training program. In contrast, Annexure A lists that FIIG *should have* delivered security awareness training at onboarding and annually to all staff. The lesson: even the best technical controls can be undermined by an uneducated workforce. Regulators know this, and they want evidence that companies are educating their people.
- **Neglect of cyber hygiene and testing:** Beyond the high-level issues, FIIG missed many security best practices. Annexure B of ASIC's statement enumerates "risk management measures… that were not implemented"even though they were in FIIG's policy. These include: not using admin accounts for email/web (which they violated), not doing regular **penetration or vulnerability testing** of their network, not disabling unused services, not reviewing event logs at least every 90 days, etc. This reads like a laundry list of basic cyber hygiene tasks that were simply ignored over the years. Such negligence allowed the attackers to remain undetected and exploit weaknesses freely. It also gave ASIC a strong case to argue FIIG's systems were clearly *not* "adequate."

Regulatory Expectations Illustrated: The FIIG case shows in tangible terms what ASIC and the law expect from cyber risk management:

- A firm should have **baseline technical controls** (patching, MFA, backups, etc.) – FIIG didn't, hence an easy target.
- On top of that, it should have **governance and processes**: policies that are actually implemented, periodic security testing, training, monitoring, and response prep – all lacking at FIIG.
- The **board and senior management** of FIIG presumably failed to allocate proper attention or resources (perhaps they assumed IT had it covered). This was a governance failure, and ASIC's action effectively holds the company (and by extension its leadership) accountable for that lapse. In the RI Advice case, the court made a declaration to deter other licensees from "engaging in similar conduct" – meaning ignoring cyber risk will draw legal consequences.

It's also worth mentioning: after RI Advice's case concluded in 2022, ASIC released *Report 716* on cyber resilience of firms in financial markets, and continued to caution that cyber was a board-level issue. So, by 2023, firms had fair warning. FIIG's breach

occurring in mid-2023 could be seen by ASIC as particularly egregious given all those warnings.

Implications for AFSL Holders: If you hold an AFSL, the FIIG case should be a wake-up call. It demonstrates that **ASIC is willing to take enforcement action if they find systemic cybersecurity deficiencies**, especially if a breach occurs as a result. It's not enough to avoid a breach; ASIC could presumably intervene if they discover issues in a proactive inspection or after a smaller incident too. Compliance teams should be evaluating their own programs against the gaps FIIG had. If you find similarities (outdated systems, no SIEM, weak training, etc.), those are red flags to address immediately.

In conclusion, the FIIG case encapsulates what regulators expect in terms of **cyber governance, incident preparedness, and accountability**:

- *Cyber governance* – integrate security into business risk management, assign clear responsibilities, and ensure continuous oversight.
- *Incident response and recovery* – have a plan, practice it, and respond swiftly to incidents, involving the board when major breaches occur.
- *Accountability* – the onus is on the licensee's leadership to ensure adequate systems. They can't just blame a rogue IT contractor or an unforeseen technical glitch; they must demonstrate a proactive, diligent stance on cybersecurity.

Having understood these expectations and the inadequacy of an Essential Eight-only approach, the next logical step is to explore established frameworks that cover these broader requirements. By comparing Essential Eight with **ISO 27001, ISO 27035, and NIST CSF**, we can identify how to build a more complete cybersecurity program that aligns with what ASIC (and good practice) would consider "adequate" or even exemplary.

Beyond the Essential Eight: Comparing Frameworks (ISO 27001, ISO 27035, NIST CSF)

To achieve a higher level of cyber maturity, many organisations turn to **international standards and frameworks**. Three of the most relevant are **ISO/IEC 27001**, **ISO/IEC 27035**, and the **NIST Cybersecurity Framework (CSF)**. Each of these takes a more holistic approach than the Essential Eight. Below, we provide a comparative overview of these frameworks versus the Essential Eight, to highlight differences in scope and focus:

ISO/IEC 27001 – Information Security Management System (ISMS): ISO 27001 is a globally recognised standard for managing information security. Rather than prescribing specific technical controls only, ISO 27001 outlines a **comprehensive**

management system that includes: risk assessment, a set of security controls (reference: ISO 27002), policies and procedures, training and awareness, internal audits, management review, and continuous improvement (the Plan-Do-Check-Act cycle). Key points:

- *Scope:* **Enterprise-wide and risk-driven.** It covers confidentiality, integrity, and availability of information across all forms (digital, paper, etc.). Controls cover physical security, personnel security, supplier risk, incident management, compliance – far beyond IT-only controls.
- *Risk Assessment:* Central to ISO 27001 is conducting a risk assessment to decide which controls are necessary. This means the security measures are **customized to the organisation's context**.
- *Top Management Involvement:* Certification requires leadership commitment – ensuring security objectives align with business objectives and that roles (like a security officer) and responsibilities are defined.
- *Certification:* Organisations can get certified to ISO 27001 via external audit, which can be a way to demonstrate to regulators and clients that a certain standard of security is met.
- *Relation to E8:* Many Essential Eight controls map into the ISO 27001 Annex A controls (for instance, patch management, malware prevention, access control are in both). However, ISO 27001 also includes controls like security policies, asset management, cryptography, supplier security, incident management, and compliance checks – which cover **most areas ASIC is concerned with**. One might say E8 is *sub-set* of the technical controls one would deploy under ISO 27001, focusing on endpoint security. But ISO 27001 would ensure, for example, that a process exists to review those controls, that management approves the security policy (which might mandate Essential Eight as a baseline), etc.

ISO/IEC 27035 – Incident Response Standard: ISO 27035 is part of the ISO 27000 series but zeroes in on **information security incident management**. It provides best practices for establishing an incident response capability and handling incidents effectively. Key points:

- *Scope:* It covers preparing an incident response plan, forming an incident response team, detection and reporting mechanisms, assessment and decision procedures, responses (containing, eradication, recovery), and **lessons learned processes**.
- *Emphasis:* On *workflow and roles* during incidents. It guides how to log incidents, classify them, when to escalate to management or law enforcement, how to do post-incident reviews, etc.
- *Relevance:* This standard directly addresses one of Essential Eight's blind spots – **response and recovery**. If FIIG had followed ISO 27035 guidance, they would have had a plan and team in place, detecting the intrusion faster and reacting within days if not hours. They might have contained the breach before 385GB was taken. So, for any AFSL, aligning with ISO 27035 would mean you have the muscle to flex when an incident happens, rather than scrambling.

- *Integration:* ISO 27035 can actually be implemented as part of ISO 27001 (since incident management is one control domain in ISO 27001 Annex A), but 27035 gives the detailed how-to. It complements technical measures by ensuring people and process are ready for the worst day.

NIST Cybersecurity Framework (CSF): The NIST CSF was developed in the U.S. for critical infrastructure, but it's widely adopted globally as a **voluntary framework**. It organizes cybersecurity activities into five core functions: **Identify, Protect, Detect, Respond, Recover**. Under each function are categories and sub-categories (mapping to NIST 800-53 controls or ISO controls) that describe specific outcomes (e.g., "Detect: Anomalies and Events – anomalous activity is detected and investigated in a timely manner"). Key points:

- *Scope:* NIST CSF is comprehensive across the cybersecurity lifecycle. It's not a list of controls per se, but a framework to ensure you're covering all bases.
- *Risk-based & Flexible:* Like ISO, NIST CSF starts with understanding business context and risk (Identify function includes asset management, business environment, governance, risk assessment, supply chain risk). It allows organisations to prioritize outcomes based on risk. You can implement the CSF in a way that fits your size and industry.
- *Profiles and Tiers:* The CSF introduces Implementation Tiers (1-4) to indicate the maturity of your risk management practices (from Partial to Adaptive) and encourages creating a Current Profile and Target Profile of cybersecurity outcomes – essentially a gap analysis approach. A company might say, "Currently we are doing X, we want to be doing Y – here's how to get there."
- *Relation to E8:* Essential Eight fits mostly in the **Protect** function of NIST CSF (patching, access control, etc., are protective measures). But NIST includes **Identify** (inventory your assets and risks), **Detect** (security monitoring, continuous logging, and alerting), **Respond** (IR planning, communications, mitigation), and **Recover** (backup, restoration, improvement) – none of which E8 fully addresses. In NIST terms, an Essential Eight-only program would be very heavy on Protect and light on the other four functions – a lopsided approach.
- *Popularity:* In Australia, NIST CSF has been referenced by government and industry as a useful framework. It doesn't offer certification like ISO, but it provides a common language. For example, ASIC's 2023 Cyber Pulse Survey might have implicitly assessed firms against similar domains (governance, identity management, detection, etc., aligning to NIST categories).
- *Benefit:* Using NIST CSF helps ensure **no critical function is neglected**. It would prompt an organisation to ask: do we have capabilities in place to detect attacks (like EDR/SIEM)? Do we have a response plan (like ISO 27035 suggests)? Are we managing our supply chain risks? – All aspects that ASIC cares about.

To illustrate the differences, consider the following **comparative table** summarizing Essential Eight vs. ISO 27001 vs. NIST CSF (with ISO 27035 as a part of Respond/Recover):

Framework	Scope & Focus	Key Components	Alignment with ASIC Expectations
ASD Essential Eight	8 technical controls for system hardening. Focus on prevention of common cyber attacks. Intended as baseline for Australian orgs.	Application control, patching (apps & OS), Office macro config, user app hardening, restrict admin privileges, multi-factor auth, regular backups. Maturity model (Levels 0–3) for each control to gauge implementation depth.	Covers basic *Protect* measures (e.g., patching, MFA, backups) which ASIC expects (FIIG failed these). However, lacks governance, *Detect*, *Respond*, *Recover* depth. On its own, does **not ensure** "adequate risk management systems" as required by ASIC.
ISO 27001 (ISMS)	Holistic information security management across people, process, technology. Risk-based and certifiable.	Risk assessment & treatment plan; 14+ control domains via ISO 27002 (including HR security, physical security, supplier security, cryptography, ops security, access control, system acquisition, incident management, BCM, compliance); Policy framework; Training and awareness; Internal audit and continuous improvement cycles.	Strong alignment. Ensures **governance** (management oversight, defined roles) and **risk management** process (ASIC's core ask). Includes controls for incident management, business continuity, periodic testing – which meet ASIC's expectations for preparedness (e.g., having IR plan, doing pen tests). Achieving ISO 27001 compliance generally means surpassing Essential Eight on all fronts and would demonstrate to ASIC a commitment to best practice.
ISO 27035 (Incident Mgmt)	Specific guidance on **incident response and recovery**. Complements ISO 27001.	Establishing incident response team and plan; Incident identification and reporting processes; Triage and categorization; Containment, eradication, recovery steps; Post-incident	Directly addresses the **Respond/Recover** gap. Satisfies ASIC's expectation that firms can react quickly and effectively to incidents (e.g., had FIIG

Framework	Scope & Focus	Key Components	Alignment with ASIC Expectations
		analysis and lessons learned. Often includes testing (simulations) and continuous improvement of IR capability.	followed 27035, they would have had a tested IR plan and possibly caught the breach sooner and limited damage). Regulators would view adherence to 27035 favourably, as it shows the organisation won't be paralysed in a crisis and will fulfill obligations like timely breach notification.
NIST Cybersecurity Framework	High-level framework mapping security activities into 5 Functions (Identify, Protect, Detect, Respond, Recover). Flexible and widely used for benchmarking and improving security maturity.	**Identify:** Asset management, business environment, governance, risk assessment, supply chain risk. **Protect:** Access control, awareness training, data security, maintenance, protective tech (firewalls, etc.). **Detect:** Anomalies and events, continuous security monitoring, detection processes (SOC/SIEM). **Respond:** Response planning, communications (incl. to stakeholders/regulators), analysis, mitigation, improvements. **Recover:** Recovery planning, improvements, communications (post-incident). Each Category has sub-outcomes and mapping to controls (e.g., Detect/Anomalies maps to having tools like EDR/SIEM).	Strong alignment. NIST CSF ensures *no critical domain is ignored*. For instance, **Detect** and **Respond** functions cover exactly what Essential Eight omits but ASIC expects (monitoring, IR). **Identify** function ensures governance and risk management are foundational (ASIC's focus on board oversight and risk framework). CSF doesn't mandate specific controls, but if an AFSL reaches, say, Tier 3 (Repeatable) across all functions, it likely has in place the policies, tools, and processes ASIC would deem adequate. CSF can be used in conjunction with Essential Eight (for

Framework	Scope & Focus	Key Components	Alignment with ASIC Expectations
		Implementation Tiers indicate maturity of integration into org processes.	Protect) and ISO standards, offering a structure to communicate maturity to regulators and clients.

Table 1: Comparison of ASD Essential Eight with ISO 27001, ISO 27035, and NIST CSF. Essential Eight is narrow in scope (primarily technical protective controls), whereas ISO and NIST frameworks are broader and risk-driven, covering governance, detection, response, and continuous improvement.

As shown above, **the Essential Eight is essentially a subset of the "Protect" function (plus backups for recovery)**. It does not inherently address Identify, Detect, or Respond. ISO 27001 and NIST CSF push an organisation to tackle all these areas and back them with governance structure. ISO 27035 provides the depth in Respond/Recover.

It's worth noting that these frameworks are not mutually exclusive. In practice:

- An organisation might **adopt NIST CSF** as a high-level guide to ensure completeness,
- Use **ISO 27001** as a structured program (possibly even get certified for assurance purposes), and
- Still implement the **Essential Eight controls** as part of its protective measures, because E8 is well-aligned with some ISO/NIST sub-controls (patch management, etc.) and remains good practice.
- They would also **implement ISO 27035's guidance** when building their incident response plan and processes, to meet the Respond/Recover expectations.

By doing so, the company creates a layered, well-governed security environment: the Essential Eight addresses common threats and hardens the IT environment; the ISO/NIST frameworks ensure that's augmented by governance (policies, audits, management reviews), by detection capabilities (SOC monitoring, etc.), and by response readiness (IR plan, drills, backup restoration tests).

For AFSLs, this multi-framework approach is increasingly seen as necessary. Indeed, ASIC's own publications on "cyber resilience good practices" emphasize things like continuous monitoring (SIEM), red-teaming, encryption, secure software development life cycle, etc., which align more with ISO/NIST than with just E8. ASIC doesn't mandate a specific framework (they don't say "thou must be ISO 27001 certified"), but they expect the outcomes those frameworks produce. By contrast, an E8-only approach would leave too many gaps in those outcomes.

The next section will build on this understanding to propose a **Cybersecurity Maturity Baseline** specifically tailored for Australian Financial Services Licensees. This baseline takes the best of these frameworks and focuses on the key domains repeatedly highlighted: Governance, Incident Response, Detection & Monitoring, Backup & Recovery, and Personnel Competence. It will serve as a practical guide for AFSL holders to elevate their cybersecurity to meet both modern threats and ASIC's compliance requirements.

A Comprehensive Cybersecurity Maturity Baseline for AFSLs

Having established that AFSL holders need to move beyond the Essential Eight, we now outline a **recommended cybersecurity maturity baseline** suitable for these organisations. This baseline draws on ISO 27001 and NIST CSF principles, with targeted controls and practices that address ASIC's expectations. The baseline is organised into five key focus areas that have emerged throughout this paper:

1. Governance and Risk Management
2. Threat Detection and Monitoring
3. Incident Response and Recovery
4. Technical Controls (Preventive)
5. People and Skills

For each area, we'll describe the objectives, essential components, and how it maps to both Essential Eight and broader frameworks. We will also provide guidance on implementation and typical costs or resources needed (with Australia context).

1. Governance and Risk Management

Objective: Establish leadership oversight, clear policies, and continuous risk assessment for cybersecurity, integrating it into the organisation's overall governance.

Key Actions & Controls:

- **Cybersecurity Governance Structure:** Assign a responsible executive (e.g. a Chief Information Security Officer (CISO) or head of IT security) and define roles and responsibilities for cyber risk management. Ideally, form a management committee for cyber or include it in an existing risk committee. The board should receive regular reports on cyber risks and readiness. For SMEs that cannot justify a full-time CISO, consider a **virtual CISO service** or engaging external consultants to provide strategic guidance and attend board meetings quarterly for updates.
- **Policies and Procedures:** Develop and approve core information security policies (Acceptable Use, Access Control, Incident Response Plan, Business Continuity/Disaster Recovery Plan, etc.). Policies should be aligned with

industry standards (e.g., map to ISO 27001's required policies) and *enforced* in daily operations. Make sure these are not shelved documents – conduct awareness sessions so staff know the rules, and hold people accountable for following them (e.g., no sharing of passwords, no installing unauthorized software).

- **Risk Assessment & Treatment:** At least annually (and whenever major changes occur), perform a cybersecurity risk assessment. This involves identifying assets (information and systems), threats and vulnerabilities, then evaluating potential business impact. For example, an AFSL's client data and transaction systems are high-value assets – what are the top threats (hacker data breach, ransomware, insider misuse)? Assess current controls and identify gaps. **Document a risk register** and treatment plan, prioritizing high risks. If patching is slow (a vulnerability risk), plan to improve it; if an old CRM system can't enforce MFA, plan to upgrade or isolate it. This risk-driven approach ensures resources target the most critical exposures – something the Essential Eight by itself doesn't guarantee. It also creates evidence for ASIC that you are systematically managing cyber risk (supports compliance with s912A obligations).
- **Continuous Improvement (Audit and Review):** Establish metrics and regularly evaluate the effectiveness of controls. For instance, track patching timelines, number of phishing emails reported vs missed, response times to incidents. Conduct periodic internal audits or have an external party audit your security (against ISO or NIST or the Essential Eight maturity model) to identify shortcomings. ASIC expects companies to "proactively and regularly check the adequacy" of their measures. This could mean scheduling a quarterly security review meeting, using results from vulnerability scans or incident post-mortems to update controls. Penetration tests or cyber maturity assessments annually can provide independent insights (and show regulators you seek to validate your security). The goal is a feedback loop: learn and adjust continuously. In Essential Eight terms, this is akin to moving from a static maturity level to ensuring you don't regress and instead strengthen over time.
- **Supply Chain and Third-Party Risk:** Ensure that vendors or partners with access to your systems/data are also held to high security standards. This can be done via contract clauses (requiring, say, they follow E8 or ISO 27001, and notify you of incidents), and periodic due diligence (ask for their security certifications or conduct assessments). For AFSLs, this includes cloud providers, software vendors, and any outsourcers (including IT MSPs). The Protiviti summary of ASIC's survey findings highlights third-party risk management as a major focus area. So, include this in your governance – maintain a register of critical suppliers and ensure each has a cybersecurity review.

Alignment: This governance baseline aligns with **NIST CSF Identify** function and ISO 27001's management system requirements. It goes well beyond Essential Eight (which has no governance element). It directly addresses ASIC's expectations for board involvement and risk frameworks. When these governance practices are in place, an

organisation can demonstrate to regulators a proactive stance ("tone from the top" is right, cyber risk is understood and managed systematically).

Typical Costs/Resources: Establishing governance is more about internal effort than direct spending:

- Policy development might be done in-house or with a consultant's help (consulting budget perhaps $5,000–$15,000 AUD for an SME to get a basic set of policies tailored, if needed).
- Virtual CISO services can range from $2,000 to $10,000 per month (depending on involvement level), which may be worthwhile for smaller AFSLs needing strategic expertise.
- Risk assessment workshops can be facilitated internally; using a consultant for a comprehensive risk assessment might cost $10,000–$20,000 for a small organisation, more for larger.
- Training the board or adding a board member with cyber expertise might involve recruitment or advisory fees. External audits (like ISO 27001 certification audits) could cost $15,000+ annually for audit fees, plus preparation costs.
- These investments in governance often pay off by preventing incidents and demonstrating compliance. Compared to technical controls, governance costs are relatively low, but the challenge is committing management time and attention consistently.

2. Threat Detection and Monitoring

Objective: Implement capabilities to continuously monitor systems for signs of malicious activity or vulnerabilities, so that attempts to breach can be quickly detected and acted upon. "Prevention is ideal, but detection is a must" – assuming breaches **will** occur, detection is your next line of defence.

Key Actions & Controls:

- **Endpoint Detection and Response (EDR):** Deploy EDR software on all servers, workstations, and if possible, even laptops. EDR tools (like CrowdStrike, Microsoft Defender for Endpoint, etc.) go beyond traditional antivirus. They use behavioural detection to catch suspicious actions (e.g., unusual PowerShell execution, ransomware-like file encryption patterns) and can isolate infected machines. ASIC explicitly indicated FIIG should have had EDR on all endpoints and servers, with automatic updates enabled. EDR acts as your eyes on each device, crucial for detecting an attacker who bypassed perimeter defences. Ensure the EDR alerts are being monitored (either by internal IT/security staff or a contracted Security Operations Center service).
- **Security Information and Event Management (SIEM):** Set up a SIEM system to aggregate logs from various sources – firewalls, servers, cloud services, applications – into a central platform where automated analysis and correlation can identify anomalies. For example, a SIEM could catch that a single user account logged in from Sydney and Moscow 30 minutes apart, or that a

database was accessed in an unusual way at 2 AM. ASIC expected FIIG to have a SIEM with logs stored >= 90 days and alerting on suspicious events. Many SIEM solutions exist, from on-premises (Splunk, Elastic) to cloud-based (Azure Sentinel, Sumo Logic) to managed SIEM services. The right choice depends on your in-house expertise. For many SMEs, a *managed SIEM/SOC service* is attractive – you pay a provider to collect and monitor your logs 24x7 and notify you of incidents. This ensures constant vigilance even if your team is small.

- **Network Monitoring and Intrusion Detection:** In addition to endpoint and log monitoring, consider network-level detection. This might include an Intrusion Detection System (IDS) that analyses network traffic for malicious patterns (some next-gen firewalls have this built-in), or even anomaly-based detection on network flows. Given many workloads are moving to cloud, ensure you also enable cloud security monitoring tools (like AWS GuardDuty or Azure Security Center) for any cloud infrastructure. The key is to cover all environments where your data lives.
- **Regular Vulnerability Scanning:** While not real-time "threat" detection, vulnerability scanners (run monthly or quarterly) help detect known weaknesses in your systems before an attacker does. ASIC highlighted FIIG's lack of vulnerability scanning; in Annexure A, running network and endpoint vulnerability scans quarterly and acting on results was expected. Adopt a tool (OpenVAS, Nessus, Qualys, etc.) or service to scan your IPs and critical systems for missing patches or misconfigurations, and feed that into your remediation process. This is part of being proactive in detection – catching security gaps (like an open RDP port or outdated software) and fixing them reduces the chance of successful breach.
- **Alert Management and Response Integration:** Detection is only useful if it's hooked into response. Define processes: Who gets the alerts (internal IT, on-call engineers, an external incident response provider)? What actions should they take on high severity alerts (e.g., EDR detects malware – isolate machine, begin investigation)? Make sure alerts aren't ignored. This often means tuning the systems to reduce false positives and having at least some staff with bandwidth to triage alerts daily. If using a third-party SOC, agree on an escalation matrix (e.g., they call your IT manager at any time if critical incident). Testing this process with drills (simulate an alert and see how the team handles it) can improve readiness.
- **Metrics:** Track detection metrics such as number of incidents detected internally vs externally. A sobering fact in FIIG was that they were alerted by ASD (external) because they didn't detect it themselves. Your goal should be to detect incidents in-house first. Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) are good metrics to improve. Organisations aiming for cyber maturity often target MTTD in hours (not days/weeks).

Alignment: This maps to **NIST CSF Detect** and parts of **Identify** (vulnerability management) and **Protect** (continuous maintenance). It addresses exactly what Essential Eight lacks – continuous security monitoring. ASIC clearly expects detection capabilities (as evidenced by their emphasis on FIIG's undetected dwell time and missing SIEM/EDR). By implementing EDR and/or SIEM, an AFSL demonstrates that

even if an attacker slips past preventive controls, they have a net to catch them. It's also a strong mitigator for risk – e.g., quick detection can prevent a breach from turning into a massive data loss.

Typical Costs/Resources: Detection capabilities often require ongoing investment:

- **EDR:** Many EDR solutions are licensed per endpoint. In Australia, prices vary by vendor and volume, but ballpark might be $50–$120 AUD per endpoint per year for enterprise-grade EDR. For example, 100 endpoints could cost on the order of $5,000–$12,000 annually. Some vendors bundle EDR in broader packages (Microsoft includes Defender for Endpoint in its E5 licensing, etc.). There might also be initial deployment costs if using a consultant to set it up.
- **SIEM:** Costs depend on log volume (often priced per GB of data ingested or events per second) and whether it's self-managed or a service. A cloud SIEM like Azure Sentinel could cost a few thousand dollars per month for a mid-sized environment (with optimization). Managed SIEM/SOC services for an SME might start around $3,000–$5,000 AUD per month and go up based on complexity – which might sound significant but consider it's like hiring a few dedicated security analysts available 24x7 at a fraction of an FTE cost. Simpler log management (for compliance) could be done with open source and modest cost if internal staff can manage it.
- **Vulnerability scanning tools:** Could be a few hundred to a couple thousand dollars per year in licensing, or you might use free ones with in-house labour. Some managed security providers include scanning in their package.
- **Staffing:** Ideally, an internal IT/security person dedicates part of their time daily to checking dashboards or responding to alerts. If no one looks at the SIEM, it's wasted money. Training someone on incident monitoring or leveraging a service is crucial. Some companies opt to join threat intelligence sharing communities (like ACSC's threat feeds) – which usually is more about receiving info and doesn't cost much beyond time.

In Australian context, one might also consider the ACSC's **Cyber Threat Alert** services or the availability of government-supported threat feeds. While those can supplement, they don't replace internal detection – they just give you heads-up on known indicators of compromise (IOCs) to watch for.

3. Incident Response and Recovery

Objective: Be fully prepared to respond to and recover from cybersecurity incidents, minimizing damage and downtime. This means having plans, backups, and practiced procedures so that when an incident occurs, everyone knows their role and the business can get back on its feet swiftly.

Key Actions & Controls:

- **Incident Response Plan (IRP):** Develop a written incident response plan that outlines steps to take during various incident scenarios (data breach,

ransomware, system outage, etc.). As noted earlier, the plan should define *roles and responsibilities* (Who is the incident lead? Who contacts customers or regulators? Who coordinates with IT? Does legal or PR need involvement?), *communication flows* (internal escalation, when to inform executives/board, external notifications like ASIC or OAIC if required by law), and *detailed procedures* for triage, containment, eradication, and recovery. The IR plan must be readily accessible (printed copies or stored securely offline in case your network is compromised). **Crucially, test this plan at least annually** via drills or tabletop exercises. For example, run a simulated phishing-induced breach: walk through how teams would discover, decide to shut down systems, what they tell clients, how they remediate. Testing reveals gaps (maybe contact lists are outdated, or people aren't sure who decides on system shutdown) so you can improve before a real incident. A well-tested IR plan can drastically reduce response time and confusion in a crisis.

- **Business Continuity and Disaster Recovery (BCP/DR):** Ensure you have a Business Continuity Plan for various disruptions, including cyber incidents. Disaster Recovery, specifically for IT, focuses on how to restore systems and data after an incident. Key elements:
    - **Regular Backups & Offline Copies:** As per Essential Eight, daily backups are recommended. But more importantly, **backup data must be secure and separate** from your main network (to avoid ransomware encrypting backups too). Use offsite or cloud backups with strong access controls. Maintain multiple generations of backups. For critical systems, consider real-time replication to a secondary site (if budget permits) or at least daily full backups with the most recent copy offline.
    - **Backup Restoration Drills:** It's not enough to have backups; you must ensure you can restore them quickly. Do periodic test restores of random files and full systems. Many companies only discover in a crisis that their backups were incomplete or corrupted. Don't be that company.
    - **Alternate Systems and Workarounds:** Plan for how operations will continue if IT systems are down. E.g., can trading or customer service continue manually or via alternate systems if core systems are hit? This crosses into BCP – you might prepare manual forms or an alternate communication method with clients in case email is down due to an attack. For AFSLs, consider obligations: if your trading platform is down from a cyber incident, do you have an obligation to notify markets or clients? Plan those communications in advance.
- **Engage External Incident Response Support:** Consider having an external incident response firm on retainer or at least identified in advance. During a major cyber incident, having expert responders (forensic specialists, negotiators if it's ransomware, etc.) a phone call away is invaluable. Some cyber insurance policies require or include access to such experts. Retainers can cost some money annually (maybe $10k–$30k for an SME for on-call services), but they buy peace of mind that you won't be alone during a big incident. At minimum, know whom you will call (have 24/7 contacts at an IR firm). ASIC will look kindly on organisations that handle incidents professionally – which often means bringing in experts to ensure thorough investigation and proper containment.

- **Regulatory and Legal Response:** Incident response isn't just technical; it's also regulatory. AFSL holders should integrate into their IRP the steps for notifying ASIC in certain scenarios. ASIC RG 78 (Breach Reporting by AFS licensees) likely covers when a cybersecurity incident triggers a breach report (for example, if it results in inability to provide services or significant data loss affecting clients). Also consider Privacy Act Notifiable Data Breaches (NDB) scheme – if personal information is compromised, you may need to notify OAIC and affected individuals expediently. The plan should contain a decision tree for notification: involve legal counsel early to determine if thresholds are met. Documenting how you complied with these requirements during an incident is part of demonstrating that you managed the incident "efficiently, honestly and fairly" as required by your license obligations.
- **Post-Incident Review:** After any significant incident (or even a drill), conduct a retrospective. Identify what went well and what didn't. Update the IR plan and other controls accordingly (lessons learned). Perhaps an incident exposed that an obscure system had no monitoring – fix that. Or that staff were unclear on communication – clarify that. A culture of learning from incidents leads to continuous improvement (which would be evidenced to ASIC that you're serious about resilience, tying back to governance).

Alignment: This aligns with **NIST CSF Respond and Recover** functions and ISO 27035 guidance. It directly addresses ASIC's focus on incident readiness. As we saw, FIIG lacked an IR plan and delayed responding – exactly the failures this baseline fixes. Ensuring strong backup and recovery ties to Essential Eight's "daily backups" but extends it to actual recovery ability, which is what counts (backups are useless if you can't restore quickly). By having IR and DR plans, AFSLs fulfill what ASIC would likely consider an "adequate risk management system" in terms of being prepared for incidents.

Typical Costs/Resources:

- **Incident Response Planning and Testing:** Often done internally with some consulting help. If you hire a consultant to develop an IR plan and run a tabletop exercise, budget ~$5k–$15k for a small org. Doing it in-house might just cost internal time. Training staff on the plan (perhaps a few hours of all-hands or team workshops) is minimal cost beyond time.
- **Backups & DR:** Costs depend on data volumes and solutions. For example, using a cloud backup service could cost a few cents per GB per month. If an AFSL has, say, 5TB of critical data, at $0.10/GB/month that's $500/month (~$6k/year) – a reasonable cost for ensuring data safety. More advanced DR like real-time replication to a hot site is more expensive (could be tens of thousands per year). Many SMEs opt for cloud-based backups (Azure Backup, AWS Backup, or third parties like Veeam, Acronis etc.). Also consider the *labour* in managing backups – might be part of IT admin duties.
- **IR Retainer and Tools:** Retainers as mentioned can be 5-figure annual costs but are optional. If not on retainer, at least ensure you have emergency funds or insurance coverage for incident response. Cyber insurance is discussed later,

but typically if you have insurance (costing maybe $10k/year for small firms for $1M coverage), they often cover incident response expenses.

- **Downtime costs:** worth noting in planning – the cost of not being prepared can be huge (lost business during downtime, regulatory fines, etc.). For context, the cost of a significant breach for an SME in Australia can easily hit hundreds of thousands in incident response, notifications, remediation, and intangible reputational harm. This underscores that spending, say, $20k a year on robust IR preparedness is a smart investment.

4. Preventive Technical Controls: Moving Beyond the Essential Eight

Objective:

To implement technical controls that **genuinely reduce risk**, satisfy **regulatory obligations under the Corporations Act**, and protect the organisation from modern cyber threats. This means **moving beyond the outdated Essential Eight**, and aligning with **NIST, ISO 27001, and ASIC's enforcement expectations**, particularly in light of the FIIG Securities case.

The Board's Reality: The Essential Eight Is No Longer Fit for Purpose

While the Essential Eight once offered a basic foundation, it was built for traditional IT environments and legacy threats. It does **not protect against the ways most cyber incidents occur today** — especially in **cloud-first, Microsoft 365-based financial firms**.

Modern attackers use stolen credentials, session hijacking, phishing, cloud misconfigurations, and supply chain gaps — all things the Essential Eight was **never designed to prevent**.

More importantly, **ASIC has made it clear**: relying solely on these eight controls will **not** be accepted as adequate cyber risk management under your AFSL obligations. The expectations have moved.

What ASIC Now Expects (And What Every AFSL Board Should Demand

To fulfil your legal duties under **s912A of the Corporations Act**, the following technical controls must be in place, tested, and governed. Each aligns with ASIC's position following the FIIG case, as well as modern best practices under ISO 27001 and the NIST Cybersecurity Framework.

1. Identity, Access, and Password Management

Why this matters: Most cyber breaches start with stolen credentials. ASIC expects strong, enforceable identity protection — not basic password policies and outdated MFA.

Controls:

- **Single Sign-On (SSO):** Use a central login platform like Azure AD or Okta to manage all user access. This allows control, monitoring, and fast access removal.
- **Multi-Factor Authentication (MFA):** Enforce for all users and critical systems. Use app-based or hardware-based MFA — SMS-based MFA is no longer considered safe.
- **Password Management:**
  - Ban shared passwords and shared logins.
  - Require strong passphrases and password expiry for privileged accounts.
  - Deploy a business-grade password manager (e.g. LastPass, Dashlane, Keeper, 1Password) to store and manage credentials securely.
  - Monitor for leaked credentials using dark web scanning tools or cyber insurance services.
- **Privileged Access Controls:**
  - No admin accounts should be used for daily tasks.
  - All admin access must be logged and reviewed.
  - Remove access as soon as roles change, or staff leave.

📌 ASIC specifically criticised FIIG for not revoking admin access and not separating privileged accounts — putting client data and systems at risk.

2. Endpoint Security and Device Control

Why this matters: Every staff member's device is a front door to your business. You must know what devices are accessing your systems and have the power to protect, monitor, and disable them.

Controls:

- **Endpoint Detection & Response (EDR):** Install across all laptops and desktops. EDR detects and isolates suspicious behaviour in real-time. Tools like Microsoft Defender for Endpoint, CrowdStrike, or SentinelOne are now considered the baseline.
- **Mobile Device Management (MDM):** Secure all company phones and laptops with central policies — encryption, remote wipe, screen locks, and updates enforced.

📌 ASIC expects daily monitoring of endpoints and the ability to isolate compromised devices immediately.

---

3. Network Security — Where It Still Matters

Why this matters: For cloud-only businesses with no on-premises infrastructure, firewalls are **less critical**. However, for any business with an office, shared networks, or printers, **network security must be managed**.

Controls (if applicable):

- **Segment the network:** Separate devices handling client data (e.g. accounting, Xplan) from general-use devices.
- **Block unnecessary outbound traffic:** ASIC explicitly stated FIIG should have blocked high-risk outbound protocols (e.g. FTP, RDP).
- **Maintain firewall configurations:** If a network is in use, review firewall rules quarterly. Only allow ports that are needed. Ensure intrusion prevention is turned on.

📌 If you're a fully cloud-native, mobile team using only Microsoft 365 and Xplan — and all devices are managed and protected — a Next-Gen Firewall is not essential. But if you're hosting anything locally or have an office LAN, **this becomes a board-level risk if not addressed**.

---

4. Cloud Security and Microsoft 365 Hardening

Why this matters: If you're using Microsoft 365, your data is in the cloud — and it's where most attackers now go first. ASIC expects visibility and active management of cloud risk.

Controls:

- **Conditional Access Policies:** Enforce rules so logins from unknown countries, devices, or risky behaviour are blocked or require extra verification.
- **Audit Logging:** Ensure logging is turned on across M365 (Exchange, SharePoint, admin actions) and stored securely for at least 90 days — ASIC explicitly expects this.
- **Email Security:**
  - Enable SPF, DKIM and **DMARC (with a reject or quarantine policy)** to prevent domain spoofing.
  - Use phishing protection tools and sandboxed links/attachments.
- **Data Loss Prevention (DLP):** Enforce rules that prevent staff from emailing or sharing sensitive client data externally without approval.
- **Backup M365 Data:** Microsoft does not back up your data by default. Use a third-party service (e.g. SkyKick, Dropsuite) to back up email, SharePoint, and Teams content to another location.

📌 Cloud misconfiguration and phishing via M365 are the **top causes of breaches** in SME financial firms. ASIC holds boards accountable if cloud settings are insecure or unmanaged.

---

5. Encryption and Data Protection

Why this matters: ASIC — and the Privacy Act — expects that client data is protected even if it is lost, stolen, or mishandled.

Controls:

- **Encryption in Transit:** All data between systems must be encrypted using TLS 1.2+.
- **Encryption at Rest:** All devices (laptops, servers, backups) must have full-disk encryption enabled.
- **Key Management:** Use secure key storage (Microsoft KMS, AWS KMS, etc.). Never store passwords or encryption keys in plain text.

📌 In the FIIG case, ASIC noted that data exfiltration and poor endpoint controls led to major client harm. Encryption would have helped contain that.

---

6. Testing and Continuous Validation

Why this matters: Cybersecurity is not about installing tools once — it's about knowing that those tools actually work. ASIC is explicit: controls must be tested, validated, and continuously improved.

Controls:

- **Vulnerability Scanning:** Automatically scan all systems (internal and cloud) monthly for missing patches or misconfigurations.
- **Penetration Testing*:** Hire a qualified security firm at least once per year to test your defences — including phishing, cloud, and access controls.
- **Configuration Reviews:** Check that password policies, conditional access, and privileged accounts are functioning as intended. Don't rely on assumptions — test and document.

📌 FIIG did not test or enforce many of its documented controls. ASIC is seeking penalties on that basis alone.

**We don't believe Penetration testing is truly necessary for any organisation utilising cloud based infrastructure.*

Alignment with Legal and Regulatory Standards:

These controls map directly to:

- **Corporations Act (s912A)** — Adequate risk management, technological and human resources
- **ASIC's case against FIIG** — Endpoint monitoring, privileged access separation, firewall config, IR plan, log review, training, backup
- **NIST Cybersecurity Framework** — Identify, Protect, Detect, Respond, Recover
- **ISO/IEC 27001:2022** — Annex A controls: access management, encryption, vulnerability management, incident handling, supplier risk, etc.

Typical Costs & Practical Advice for Smaller AFSL Holders:

Control	Cost Estimate (per year)	Notes
EDR (Microsoft Defender)	~$60–$100 per device	Included in Microsoft 365 Business Premium
Password Manager	~$5–$10 per user/month	LastPass, Dashlane, 1Password, Keeper, etc.

Control	Cost Estimate (per year)	Notes
M365 Backup	~$4–$10 per user/month	Tools like Rubrik, Veeam, SkyKick or Dropsuite
Penetration Test*	$5,000–$15,000	Annual external test – we don't believe this is truly necessary*
Awareness Training	$20–$30 per user	KnowBe4, or free ACSC training
vCISO (if needed)	$2,000–$5,000/month	Strategy, board reporting, audits
M365 Licences	~$30–$60 per user/month	Business Premium, E5 includes EDR, MDM, email protection

🔹 Many features are already available in Microsoft 365 — they just need to be properly configured and governed.

Final Message to the Board:

✅ **If you only implement the Essential Eight — you are exposed.**
✅ **ASIC does not accept minimalism — especially after the FIIG case.**
✅ **You must be able to detect, respond, and prove governance.**

By adopting the above control set, you move from **basic IT hygiene** to **real cyber resilience** — protecting your licence, your clients, and your reputation.

5. People and Skills (The Human Dimension)

Objective: Ensure that the people managing and using the systems have the right security awareness, skills, and support. Also ensure that you have access to cybersecurity expertise, either in-house or via trusted partners, rather than relying solely on generalist IT knowledge.

Key Actions & Focus:

- **Security Awareness and Training for All Staff:** We've touched on this, but to reiterate: conduct mandatory cybersecurity awareness training for all employees at onboarding and at least annually. Training should cover phishing, safe use of systems, reporting incidents, and specific policies (like clean desk, data handling procedures relevant under privacy law). Use engaging methods – e-learning modules, phishing email simulations, workshops with real examples. Many breaches start with an unwitting employee's mistake. A well-trained

workforce is literally the last line of defence (and first detector, if someone reports something strange). ASIC cited lack of training at FIIG as a failure. Don't let that be said of your company. Also train staff on the incident response process (so they know whom to call if something seems wrong).

- **Defined Security Roles – Avoid Sole Reliance on Generalists:** In SMEs, it's common one or two IT people do everything (servers, network, helpdesk, security, etc.). Their intentions are good, but cybersecurity has become too specialized and critical to be just a side task. Wherever possible, define specific security responsibilities. If you can't hire a full-time security analyst, maybe assign a current IT person to be "Security Champion" for a portion of their time and give them additional training for that role. Ensure someone is tasked with keeping up with threats and ensuring controls remain effective (for example, someone who reads ACSC alerts or vendor security bulletins and acts on them). Many businesses also create cross-functional **"incident response teams"** including IT, legal, and business reps – names and roles are pre-defined even if those people have other day jobs normally.
- **Professional Certifications and Skills Development:** Encourage and invest in IT/security staff obtaining relevant certifications if you have internal IT teams. If you have outsourced your IT, it is critical, even mandatory to ensure that they have truly dedicated cyber specialists available and not just individuals who communicate they understand cyber security. This accomplishes two things: improves their skills to better protect the company, and signals to stakeholders/regulators that qualified people are at the helm. Relevant certifications and qualifications include:
    - **ISO 27001 Lead Auditor/Implementer:** Validates knowledge of how to build or audit an ISMS aligned to best practices. Personnel with this can help ensure your program meets international standards (which align with ASIC's expectations on risk management).
    - **NIST Cybersecurity Framework Training/Certification:** There are courses for implementing NIST CSF, which could be useful for a governance or compliance officer.
    - **Vendor-specific certs (MCP/Microsoft Certified Professional or newer role-based certs like Azure Security Engineer, MS-500 Security Administrator, etc.):** These ensure your team knows how to securely configure the technologies you use. Since many AFSLs are heavy Microsoft shops, having staff certified in Microsoft security features is beneficial.
    - **CISSP, CISM, CRISC or other industry certs:** For broader security management knowledge, CISSP (Certified Information Systems Security Professional) or CISM (Certified Information Security Manager) are gold standards. CRISC (Certified in Risk and Information Systems Control) focuses on risk management. Having one of these can be helpful for whoever leads the security program.
    - **CARR (Cyber Assurance Risk Rating) Certification:** As mentioned, *CARR* is an emerging program (pioneered by Security in Depth, an Australian firm). CARR-certified personnel are trained in assessing cyber risks using a hybrid model that integrates NIST and ISO frameworks with a

risk scoring mechanism. Engaging a **CARR-certified consultant** or training one of your staff in CARR can provide a structured way to gauge and improve cyber maturity. It's an example of how the industry is moving towards standardized cyber risk ratings, which might even become something regulators look for.

- **Other technical certs:** Depending on needs, consider SANS/GIAC courses (very in-depth but pricey), or specialist ones (ethical hacking, digital forensics, etc.) if relevant.

From ASIC's perspective, having certified and knowledgeable personnel managing cybersecurity is evidence of adequacy. Conversely, if an incident reveals that those responsible had no security training or credentials, it might and has with FIIG, reflected poorly.

- **Use of Specialist Providers (MSP/MSSP):** If in-house capability is limited, judiciously use specialized providers:
  - **Managed Security Service Providers (MSSPs):** These firms can handle SOC monitoring, incident response, or even act as your virtual security team. However, pick a reputable one (perhaps one that is CREST ANZ certified or has a strong track record in finance sector). Make sure their contract includes service level agreements for incident response and periodic reports to your management.
  - **Security Consultants:** for periodic reviews, audits, or to design security architecture. For instance, bringing in experts from firms like *Security in Depth* or *Aphore* (mentioned since they have CARR-certified staff) to do an annual cyber health check or to assist in strategy can be very valuable. It's akin to having an external auditor for financial accounts – a fresh, expert set of eyes can catch issues and reassure stakeholders.
  - **Cyber Insurance Advisors:** Some insurance brokers or insurers (e.g., Chubb, AIG) offer risk assessments as part of the underwriting. Even if not, having cyber insurance is itself part of resilience (discussed in cost section), and insurers will often require certain controls be in place; their questionnaires can serve as a checklist to improve your posture.
- **Culture and Accountability:** Finally, build a culture where cybersecurity is seen as everyone's responsibility (not just IT's). Leadership should talk about its importance, include it in company objectives, and celebrate good security behaviour (like employees reporting phishing attempts promptly). Make it safe and encouraged to report mistakes – if someone clicks a bad link, they should feel comfortable reporting it immediately so damage can be contained, rather than afraid of punishment. A positive, vigilant culture is one of the best defences and something money can't directly buy. Boards should also hold management accountable: ask tough questions ("When was our last cyber incident and how did we handle it? When did we last test backups? Are we sure all our systems are patched?"). This pressure ensures the human elements don't get complacent.

Alignment: This human-centric approach aligns with what ASIC and good practice demand:

- ASIC expects training (FIIG's missing training was cited).
- They expect board and staff awareness (board should consider adding cyber expertiseand ensure training investment).
- Using certified experts and external reviews shows "all things necessary" are being done to manage risk.
- NIST CSF's Protect function explicitly includes Awareness and Training; ISO 27001 has A.7, A.6, etc., covering people aspects.
- The concept of professional standards (like having CARR-certified personnel) is akin to hiring qualified accountants for financial controls – it's becoming the norm for cyber.

Typical Costs/Resources:

- **Training Programs:** Many options exist. Online modules can be as cheap as $10 per user annually for a full suite (some vendors charge per user/year for unlimited training and phishing simulations). For 100 staff, that's perhaps $3k–$5k/year. You can also get free resources from ACSC for basic guidance. The ROI on user training is high if it prevents even one successful phishing attack.
- **Certifications for IT staff:** Exam and course fees vary:
  - CISSP exam ~$1,000 AUD (plus cost of study materials or course $3k+ if formal training).
  - ISO 27001 Lead Auditor course ~$2,500–$3,500 for a week training + exam.
  - Vendor certs (like Microsoft) might be a few hundred dollars for exam, training maybe another few hundred or self-study if the staff is capable. Investing in a couple of certifications might be $5k–$10k per staff but again yields better security management. Some companies tie this to staff development (and retention – paying for their certs can keep talent happy).
- **External Services:**
  - Virtual CISO or security consulting – previously mentioned, could be a retainer or hourly. Small engagements (like annual audit) maybe $10k, ongoing vCISO $3-5k/month.
  - MSSP/SOC – $3k–$8k/month as noted earlier for SMB range.
  - Cyber insurance (transfers some risk and provides incident support): premiums for a $1m coverage for a mid-sized firm might range $5k–$30k depending on revenue and controls in place (insurers often give better rates if you have MFA, good backups, etc. – another incentive to implement those).
- **Opportunity cost of internal time:** Don't underestimate the time internal people will spend on security tasks – but this is a necessary allocation, like time spent on compliance. As an example, an IT manager may spend 20% of their time on security coordination – that's time well spent compared to dealing with a breach aftermath full-time for weeks.

By implementing this comprehensive baseline across governance, detection, response, technical controls, and people, an AFSL will be in a strong position. It would

significantly reduce the risk of incidents (or their impact) and also place the organisation in a defensible position should ASIC or another regulator inquire into their cyber resilience. Essentially, you could show a regulator: *"We follow ASD and ACSC guidance (Essential Eight)* ***and*** *international best practices from ISO/NIST, we regularly assess and improve, our board is engaged, and we have trained professionals managing our cybersecurity."* That narrative is exactly what ASIC wants to hear – because it demonstrates you are **taking cyber resilience seriously and actively fulfilling your duties** to protect clients and markets.

Next, we will address the practical side of implementing these recommendations: what are the costs and options in Australia for key solutions like EDR, SIEM, cyber insurance, etc., and how can organisations approach these enhancements in a cost-effective manner.

Practical Considerations: Cost Estimates and Investment Areas in Australia

Upgrading cybersecurity maturity comes with costs – but so do data breaches and regulatory penalties. This section provides **Australian-localised cost estimates and options** for key security controls and services mentioned in our baseline. The aim is to give business decision-makers a rough idea of budgeting and to highlight that investments can be scaled to the size of the organisation. We will cover:

- Endpoint Detection & Response (EDR)
- Security Incident & Event Management (SIEM) / Log Management
- Cyber Insurance
- External Governance/Incident Response Reviews
- Staff Training and Capability Uplift

We'll present some of this information in a tabular format for clarity, and discuss options from basic to advanced to suit SMEs vs larger entities.

Cost and Options Overview

Security Measure	Basic Option (SMB-friendly)	Advanced Option (Higher maturity)	Indicative Annual Cost (AUD)
Endpoint Detection & Response (EDR)	- Use built-in EDR if available (e.g., Microsoft Defender ATP included in Microsoft 365 Business Premium/E5).	- Enterprise EDR solution (CrowdStrike, Carbon Black, etc.) with 24/7 managed monitoring service.	Basic: ~$50–$100 per device. *(e.g., ~$5k/year for 50 devices using Defender with minimal add-on*

Security Measure	Basic Option (SMB-friendly)	Advanced Option (Higher maturity)	Indicative Annual Cost (AUD)
	- Deploy on all endpoints with default policies. Monitoring by IT on best-effort basis (or via alerts to email).	- Fine-tuned policies and threat hunting.	*cost).* Advanced: ~$150+ per device with MDR service. *(e.g., ~$30k/year for 200 devices with managed CrowdStrike).*
SIEM / Log Management	- Use a cloud logging service (e.g., AWS CloudWatch, Azure Sentinel pay-per-use) with key logs (firewall, server, O365) forwarded. - IT staff review alerts during business hours. - Alternatively, a lightweight log aggregator like OSSIM (open source) if in-house expertise.	- Fully managed SIEM/SOC (e.g., Trustwave, Secureworks, CyberCX SOC-as-a-Service) covering 24/7 monitoring and incident response assistance. - Dedicated SIEM platform (Splunk, QRadar) with trained analysts tuning and watching it.	Basic: ~$1k–$3k/month for cloud SIEM handling moderate log volumes. *(e.g., Azure Sentinel for 100GB/month of logs ~$2k/mo).* Advanced: $4k–$10k+/month for MSSP SOC service. *(e.g., a mid-sized firm might pay $60k–$120k/yr for a full SOC).*
Cyber Insurance	- Basic cyber insurance policy covering incident response costs and some liability (suitable for SMEs). Coverage perhaps $250k–$500k for breach response. - Higher deductibles to reduce premium.	- Comprehensive cyber insurance with $1M+ coverage, including business interruption, ransomware payments (if legal), and third-party liability. - Lower deductibles, insurer provides proactive risk assessments.	Basic: $2k–$10k/year premium (SME with <$10M turnover, assuming baseline controls in place). Advanced: $15k–$50k/year premium (larger org or higher coverage). *Premiums vary by sector and security posture; better security often reduces cost.*
External Security Reviews & IR Readiness	- Engage a security consultant annually for a "health check" (e.g., Essential 8 gap assessment or basic pen-test).	- Hire a firm for an **ISO 27001 pre-audit** or **NIST CSF maturity assessment** to benchmark against industry and regulators'	Basic: $10k–$20k for annual assessment and basic testing. *(e.g., $12k for a pen-test of critical*

Security Measure	Basic Option (SMB-friendly)	Advanced Option (Higher maturity)	Indicative Annual Cost (AUD)
	- Optional: subscribe to ACSC Small Business Cyber grants or local IT security firms' fixed-price assessments.	expectations. - Maintain an IR retainer: an incident response firm on standby (with SLA) in case of a major incident, includes annual IR drill facilitation.	*systems and policy review).* Advanced: $30k–$50k/year for continuous consulting. *(e.g., $25k for ISO 27001 gap analysis + $15k IR retainer).*
Staff Training & Certification	- Use free/low-cost platforms for security awareness (many insurers or banks offer free modules; ACSC has free resources). - Budget for 1-2 IT staff to attend local training or earn an entry-level cert (CompTIA Security+, MS Azure Security cert).	- Enrol staff in professional courses (SANS Institute courses ~$7k each, local training by ALC or SLI on ISO 27001 etc. ~$3k each). - Support multiple certifications (CISSP, CISM) and possibly hire already certified professionals. - Conduct company-wide phishing simulation campaigns with detailed metrics (could use paid services).	Basic: ~$50 per employee for training content. *(e.g., 50 employees = $2.5k/year for a platform).* Certifications: $5k per staff for exam/training. *(e.g., 2 staff = $10k in a year).* Advanced: $15k–$30k for broad program. *(e.g., hire a trainer for on-site workshops, plus multiple staff certs, plus monthly phishing tests).*

Table 2: Estimated costs and options for key cybersecurity investments for AFSLs in Australia. Actual costs can vary based on specific products, number of users, and organisation size, but these ranges provide an order-of-magnitude planning guide.

A few additional notes to contextualize these costs:

- **Return on Investment (ROI):** While these expenses can seem significant, one must weigh them against the potential cost of a cyber incident. For instance, an ASIC enforcement action could result in penalties (RI Advice had to pay $750k towards ASIC's costs), remediation costs, not to mention reputational damage that could cost client trust. A serious breach at an AFSL could even imperil its license if mishandled. By investing proactively, organisations are effectively buying down risk. Cyber insurance can offset financial impact, but it cannot

prevent reputational or regulatory fallout – that's where having the controls and governance (the other line items) saves the day.

- **Scalability:** Small firms (say a boutique financial advisory with 10 staff) might opt for the basic options: use Microsoft's built-in security with a Business Premium license, outsource IT to an MSP that can do some security, get a cyber insurance policy for say $250k coverage, and do staff training via a packaged solution – perhaps altogether costing under $15k/year incremental to their normal IT spend. Larger firms (say 200 staff wealth manager) will need the advanced layers: maybe a dedicated security headcount ($120k+ salary), a SOC service, enterprise tools – easily spending $200k+ per year on security, but that might be just 5-6% of their IT budget, and perfectly justifiable given their risk exposure.
- **Australian context:** It's worth noting some local initiatives. The Australian government sometimes offers grants or subsidies for small business cybersecurity improvements (e.g., through Austrade or industry bodies). In terms of providers, Australia has reputable security companies (CyberCX, Aphore, etc.) that understand local business needs and APRA/ASIC expectations. Engaging local experts can ensure alignment with Aussie regulatory nuances.
- **Cybersecurity as a continuous investment:** The costs outlined are recurring (yearly subscriptions, annual services). Boards should recognize cybersecurity is not a one-time project but an ongoing operating expense akin to insurance or compliance. Many organisations now present cyber budgets in terms of a percentage of overall IT or as part of risk management costs.
- **Opportunity for efficiencies:** Some investments can cover multiple requirements. For example, an **Microsoft 365 E5** license (~$57/user/month) includes Defender (EDR), Azure AD Premium (MFA/identity protection), Cloud App Security, and basic Azure Sentinel credits – this might be cost-effective if you leverage those features fully, rather than buying separate products. Similarly, an insurance policy might cover an incident response provider's fees, effectively combining insurance and IR retainer (if you use the insurer's panel). A good strategy is to see where you can get "more bang for the buck" by leveraging ecosystems or packaged services.

Finally, one must consider **intangible costs**: implementing strong security may introduce some friction (like MFA login steps or blocking certain software). It's important to communicate to staff and even customers why these measures are necessary – to protect everyone's data and the business's stability. In a compliance sense, these costs and measures should also be documented as part of meeting AFSL obligations. Including cybersecurity improvements in the AFSL compliance reports or risk management statements ensure the organisation gets credit for its efforts when regulators come knocking.

With planning, even smaller AFSLs can achieve a high security standard without breaking the bank, especially compared to the potential costs of inaction.

Conclusion

Appendix A: Glossary of Terms

AFSL (Australian Financial Services Licence) – A licence granted by ASIC that permits an entity to conduct financial services business in Australia. AFSL holders have regulatory obligations including managing risks (which ASIC interprets to include cyber risks).

ASIC – Australian Securities and Investments Commission, the regulator for corporate and financial services. Relevant here for enforcing cybersecurity obligations of AFSL holders.

ASD / ACSC – Australian Signals Directorate and its Australian Cyber Security Centre. ASD produces the Essential Eight strategies and other cyber guidance. ACSC is the lead agency for cyber threat response and advice in Australia.

Essential Eight (E8) – A set of eight essential cyber mitigation strategies recommended by the ACSC to help Organisations protect against cyber threats. Includes: Application control, Patch applications, Configure MS Office macro settings, User application hardening, Restrict admin privileges, Patch operating systems, Multi-factor authentication, Regular backups.

Maturity Levels (for E8) – The Essential Eight Maturity Model defines levels 0 through 3 indicating how well each control is implemented (Level 0 = not implemented, Level 3 = fully aligned with ACSC's highest standard). Organisations often self-assess their level for each of the eight.

ISO 27001 – An international standard for Information Security Management Systems (ISMS). It provides a framework for managing security with a risk-based approach and has an associated certification scheme.

ISO 27035 – An international standard providing guidelines for incident management (how to prepare for, respond to, and learn from information security incidents).

NIST Cybersecurity Framework (CSF) – A framework developed by the U.S. National Institute of Standards and Technology. It organizes cybersecurity practices into five core functions: Identify, Protect, Detect, Respond, Recover. Widely used as a baseline for evaluating and improving cybersecurity maturity.

SIEM (Security Information and Event Management) – A system that aggregates and analyses activity from many different resources across your IT infrastructure. It helps in

real-time threat detection, logging, and forensics by consolidating logs and generating alerts for suspicious patterns.

EDR (Endpoint Detection and Response) – Security tools focused on detecting, investigating, and responding to suspicious activities on hosts/endpoints (computers, servers). EDR solutions often record endpoint activities and use algorithms to detect possible threats, enabling swift response (like isolating a machine).

Incident Response (IR) Plan – A documented set of procedures to detect, respond to, and recover from cyber incidents. It typically includes roles and communication plans for handling incidents such as data breaches or malware outbreaks.

Backup and Disaster Recovery (BDR) – Strategies and solutions for making copies of data (backups) and restoring systems and data after a disruptive event (disaster recovery). The goal is to ensure business can continue or quickly resume after incidents like ransomware, hardware failure, etc.

MSSP (Managed Security Service Provider) – A third-party company that provides security monitoring and management services (e.g., running a Security Operations Center for you, managing firewalls, etc.) typically via subscription.

CISO (Chief Information Security Officer) – The senior executive or role responsible for an Organisation's information security program and strategy.

CARR (Cyber Assurance Risk Rating) – A program/methodology (not yet mainstream like ISO or NIST) referenced in this document. It appears to be an approach to rate cyber risk maturity, blending elements of different frameworks, possibly championed by Security in Depth (an Australian security firm). "CARR-certified" would imply someone trained in this risk rating method.

Phishing – A common cyber attack vector where fraudulent emails (or messages) trick individuals into revealing credentials or installing malware. Often mitigated by user training and technical email filters.

Penetration Test (Pen Test) – An authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. It involves attempting to exploit vulnerabilities to determine whether unauthorized access or malicious activity is possible.

Multi-Factor Authentication (MFA) – A security mechanism that requires multiple forms of verification to prove identity (for example something you know – password, and something you have – a code on phone). Considered a critical control to prevent account breaches.

Vulnerability Scan – An automated scan of systems to identify known vulnerabilities (such as missing patches or misconfigurations). Less intensive than a pen test, but a useful regular practice.

SOC (Security Operations Center) – A dedicated team or facility for monitoring and responding to cybersecurity incidents. Can be in-house or outsourced (MSSP).

Notifiable Data Breach (NDB) – Under Australia's Privacy Act, certain breaches of personal information must be notified to the Office of the Australian Information Commissioner (OAIC) and affected individuals if they are likely to result in serious harm. This is often triggered in the event of significant data breaches.

CREST ANZ – A regional chapter of CREST (Council of Registered Ethical Security Testers), which is an Organisation that certifies companies and individuals for quality in penetration testing, SOC services, etc. If a vendor is CREST certified, it's a mark of assurance in the cyber services space.

APRA CPS 234 – (For completeness) A regulation by the Australian Prudential Regulation Authority (APRA) focusing on cybersecurity for banks, insurers, etc. Not directly for AFSLs unless they're also APRA-regulated, but relevant as context that regulators across sectors are enforcing cyber controls.

Appendix B: Framework and Control Mapping

This appendix provides a high-level mapping between the Essential Eight controls and how they map to the broader categories of NIST CSF and ISO controls, as well as highlighting which key areas ASIC expects that are **not** covered by E8.

Essential Eight to NIST CSF Mapping:

Essential Eight Control	NIST CSF Function(s)	Notes on Coverage
Application Control (whitelisting)	Protect (PR.IP – Protective Technology)	Limits execution of unapproved apps. Good for malware prevention (Protect). No direct impact on Detect/Respond.
Patch Applications	Protect (PR.MA – Maintenance)	Reduces vulnerabilities in software. Tied to Identify function as well (knowing what needs patching).
Configure Office Macro Settings	Protect (PR.DS – Data Security) and PR.IP	Hardens common attack vector via documents.
User Application Hardening	Protect (PR.IP)	E.g., disabling Flash, which reduces attack surface in user apps.
Restrict Administrative Privileges	Protect (PR.AC – Access Control)	Also Identify (knowing who has admin) and somewhat Detect (if monitoring admin use). Essential for limiting damage from attacks.
Patch Operating Systems	Protect (PR.MA)	Similar to patch applications – basic cyber hygiene.
Multi-Factor Authentication (MFA)	Protect (PR.AC)	Ties into Access Control; prevents unauthorized access. Also relates to Detect (DE.CM) if monitoring login attempts.
Regular Backups	Recover (RC.RP – Recovery Planning) and Protect (PR.DS)	Backups primarily support Recovery function (recover from ransomware etc.). They also protect data availability. However, backup alone doesn't equate to having a full recovery plan.

From this, you can see:

- Essential Eight heavily populates the **Protect** function of NIST CSF (preventative controls).
- It touches **Recover** slightly via backups.
- It does not directly address **Identify** (asset management, governance), **Detect** (security monitoring), or **Respond** (incident handling).

So, the gaps to fill, which our recommended baseline adds, are:

- *Identify:* (Asset management, Risk assessment, Governance) – via ISO 27001 processes, etc.
- *Detect:* (Anomalies and events, continuous monitoring) – via SIEM/EDR.
- *Respond:* (Response planning, communications, analysis) – via IR plan, training, drills.
- *Recover:* (Recovery planning, improvements) – via DR plan, backup testing, business continuity.

Essential Eight vs ASIC Expectations (Gap Analysis):

ASIC Expectation / Requirement (from cases & guidance)	Covered by Essential Eight?	How to Address (beyond E8)
Board oversight of cyber risk, regular review at board level	**No.** E8 is silent on governance.	Establish governance framework, board reporting (ISO 27001 governance clauses). Possibly have a board member with cyber expertise.
Adequate resources (staff and budget) for cybersecurity	**No.** E8 doesn't cover resourcing.	Organisation must assign roles, hire/train staff or engage MSSP. Show a cyber budget line.
Documented cyber risk management (policies, risk assessments)	**No.** E8 is just controls.	Implement ISMS elements: risk assessment, security policy, risk register updates.
Continuous improvement / control effectiveness reviews	**No.** E8 has maturity model but doesn't enforce review.	Conduct periodic audits, vulnerability scans, management reviews (quarterly as FIIG should have). Possibly align with ISO's PDCA cycle.
Properly configured & monitored firewalls	**Partly.** E8 implies good practice but doesn't specify firewall rules or monitoring.	Implement network segmentation, outbound filtering (Annexure A item), and include firewall logs in SIEM for monitoring.
Security monitoring (SIEM) and daily log review	**No.** Not in E8.	Deploy SIEM/central logging and assign monitoring responsibilities (internal or via SOC).
Endpoint detection (EDR) with skilled monitoring	**No.** Traditional AV in E8's scope but not EDR specifically.	Use advanced EDR on all endpoints and ensure staff or MSSP monitors it (Annexure A expected this).
Incident Response Plan (with defined	**No.** E8 doesn't include IR.	Develop and test IR plan (ISO 27035). Assign an incident leader, team, and follow through tests.

ASIC Expectation / Requirement (from cases & guidance)	Covered by Essential Eight?	How to Address (beyond E8)
roles, actions, tested)		
Timely incident response (detect & act quickly, e.g., within days)	**No.** E8 no guidance on response speed.	With 24/7 monitoring + IR plan, aim for quick detection (MTTD) and response (MTTR). E.g., have on-call arrangements.
Staff cybersecurity awareness training	**No.** Not in E8.	Implement mandatory training (as per Annexure A) file-tdhhaazxyqxgkzffggu6em . Use phishing simulations to reinforce.
Ongoing scenario testing (e.g., cyber war-gaming)	**No.** E8 doesn't mention this.	Conduct incident simulation exercises, tabletop drills, include in BCP tests. Align with advanced "response planning" good practice.
Regular vulnerability assessment / pen testing	**No.** E8 doesn't require testing, though it assumes you maintain things.	Schedule external pen tests and internal vuln scans at least annually. This verifies controls (e.g., see if any E8 control is bypassable due to misconfig).
Third-party risk management	**No.** E8 is internal focus.	Maintain vendor security due diligence, get attestations from critical suppliers, ensure contracts have cyber clauses. Possibly use questionnaires or request ISO 27001 certs from them.
Compliance with breach notification (NDB/ASIC) and efficient client comms	**No.** E8 doesn't cover legal compliance.	Incorporate into IR plan the notification process. Train execs on when/how to notify clients/regulators. Possibly prepare draft communications in advance.

This mapping shows that **most gaps** in Essential Eight correspond to areas that frameworks like ISO 27001/NIST cover, or that must be addressed through Organisational process (not just technology).

For an AFSL, a combined approach might be:

- Use **Essential Eight as a subset** of controls in the Protect function.
- Use **NIST CSF** to ensure Identify/Detect/Respond/Recover functions are also populated with capabilities.
- Use **ISO 27001** to systematize governance, risk, and compliance processes around those controls.
- Use **ISO 27035** to flesh out the incident management part of Respond/Recover.

By doing so, the organisation covers all bases: from preventing incidents to detecting them if they occur, responding properly, and continually improving – all under strong governance. That is essentially what ASIC is looking for when they say “adequate cyber risk management systems.”

Appendix C: Source References

(The following sources were referenced in the preparation of this white paper for factual accuracy and context.)

1. ASIC Media Release 25-035MR – *"ASIC sues FIIG Securities for systemic and prolonged cybersecurity failures"*, 13 March 2025. – Details of ASIC's allegations against FIIG Securities, including duration of failures and breach impact.
2. ASIC Media Release 25-035MR (continued). – Further specifics from ASIC on FIIG's failures: lack of firewall monitoring, patching, training, resources.
3. ASIC Media Release 22-104MR – *"Court finds RI Advice failed to adequately manage cybersecurity risks"*, 5 May 2022. – Outcome of RI Advice case, establishing precedent that cybersecurity lapses can breach license obligations; includes ASIC commentary.
4. Federal Court Judgment Excerpt – RI Advice (Justice Rofe's comments). – Judge's statement on importance of cybersecurity risk management for licensees.
5. ASIC "Cyber resilience good practices" guidance. – ASIC's observations on good practices in detection (continuous monitoring, SIEM) and response planning.
6. ASIC "Key questions for board" guidance. – Emphasizes board expertise, possibly using external experts, and ensuring staff training and investment.
7. FIIG Securities v ASIC – Concise Statement Annexure A (Missing Measures). – Lists of controls ASIC expected FIIG to have (IR plan, MFA, SIEM, EDR, etc.) but were missing.
8. FIIG Securities v ASIC – Concise Statement Annexure B (Policy controls not implemented). – Additional expected practices (no admin use for daily tasks, pen tests, disable unused services, log reviews) that FIIG failed to do.
9. Reuters News Article on ASIC vs FIIG. – Summary of the case, noting data volume stolen and regulatory context (increase in scrutiny).
10. CyberHeed Blog – "5 Key Lessons from the FIIG Cybersecurity Breach". – Emphasizes that compliance is an ongoing obligation, patching and resources are crucial (aligning with lessons drawn here).
11. Proaxiom Cyber Blog – *"Is ASD Essential Eight Enough? Comparing it to NIST CSF and ISO 27001"*. – Provided analysis of differences in scope, flexibility, and risk management between E8 and comprehensive frameworks.
12. WA Office of Auditor General Report 2023 – *"Implementation of the Essential Eight"*. – Noted that E8 will not stop all threats and that additional controls are recommended by ASD; also gave context on maturity and agencies' overconfidence.
13. CNS Blog – *"Essential 8 vs NIST vs ISO27001 Pros and Cons"*. – Listed pros/cons of E8; specifically, that E8's limited scope and focus on technical controls means it might not cover more advanced needs, which corroborates the argument that governance and processes are lacking in E8.
14. Cevo Blog – "Automation as a Key to Essential Eight Compliance". – Gave a refresher on what the Essential Eight controls are and how maturity levels work (reinforcing definitions).

15. Protiviti Flash Report – *“ASIC’s cybersecurity survey: Key takeaways”*. – Highlighted areas to focus like third-party risk, indicating broader risk considerations beyond one’s own IT, aligning with governance recommendations.
16. ACSC Essential Eight Maturity Model documentation (via ACSC or secondary sources). – Described backup control (daily backups) as part of E8, and the concept of maturity implementation.
17. ACSC Threat Reports / Statistics (referenced by OAG report). – Provided context on volume of cyber incidents and need for vigilance (94k reports, etc., showing scale of issue in Australia).
18. Channel Insider – “5 Essential Australian Security Certifications for MSPs” (not directly cited above, but knowledge used) . – Gave insight into trending certifications for Australian IT providers, which influenced recommendations on certifications.
19. Aphore / Security in Depth (from context, not a specific doc) – Understanding that these firms provide specialized cyber services in Australia (with CARR program etc.), supporting the point that external expertise is available.

(Note: The above references are cited in-line in the document where applicable using the 【†】 notation. They provide evidence for the statements made and highlight industry perspectives in support of the arguments.)