



GOVERNANCE RISK & OPERATIONS

The Essential Eight: The Specific Questions Behind General Cyber Assurance

Not all MFA is equal, and not all backups actually protect you. Australia's own framework tells you exactly what to ask

The cyber governance and insurance discipline discussed earlier in this series established that a board's job is oversight, not hands-on technical configuration. That does not mean a board should remain vague about what adequate technical protection actually looks like. This article goes one level deeper than the rest of this series, translating Australia's own authoritative technical framework into the specific questions a board should be able to ask, and evaluate the answers to, without needing to configure anything itself.

Which rules apply to your association?

The law depends on how your association is set up. A **company limited by guarantee** follows the Corporations Act 2001 (Cth) and its constitution. An **incorporated association** follows its state or territory associations Act and its rules. A **registered charity** also follows the ACNC Act and the ACNC Governance Standards, and some Corporations Act rules are replaced for charities that are companies. Check your own governing documents, and get advice before decisions with legal consequences.

In this resource

1. [The Authoritative Framework Most Boards Have Never Heard Named Directly](#)
2. [The Specific MFA Distinction Worth Asking About Directly](#)
3. [The Specific Backup Architecture Worth Verifying Directly](#)
4. [Why This Requires Ongoing Verification, Not A One-Time Check](#)

The Authoritative Framework Most Boards Have Never Heard Named Directly

The Essential Eight, published by the Australian Signals Directorate and the Australian Cyber Security Centre, is the authoritative Australian Government framework for baseline cyber security controls, covering eight mitigation strategies including multi-factor authentication and regular backups, each assessed against four maturity levels from zero to three. ASD advises each organisation to identify and plan for a target maturity level suitable for its own environment and risk. Many organisations, and some insurers and clients, treat Maturity Level 2 as a reasonable target, connecting directly to the cyber insurance discussion earlier in this series. A board that has never asked which Essential Eight maturity level its association sits at has not yet asked the single most useful technical oversight question available to it.

The Specific MFA Distinction Worth Asking About Directly

Not all multi-factor authentication is equal, and the distinction matters considerably more than most boards realise. At Maturity Level 2 and above, the Essential Eight Maturity Model requires multi-factor authentication for users of online services and of systems, which includes administrator accounts, to be phishing-resistant, for example security keys, passkeys or certificate-based authentication, not a text message one-time code. SMS-based codes remain vulnerable to SIM-swapping and phishing attacks and are not phishing-resistant. The specific, actionable question is not simply whether MFA exists. It is

whether MFA for privileged, administrator-level accounts is phishing-resistant, or whether it still relies on SMS codes that a sophisticated attacker can intercept.

The Specific Backup Architecture Worth Verifying Directly

Given ransomware attacks specifically target backup systems before encrypting production data, connecting directly to the cyber insurance discussion earlier in this series, the Maturity Model protects backups by restricting who can change or delete them. At Maturity Level 2, privileged accounts other than backup administrator accounts cannot modify or delete backups, and at Maturity Level 3, even backup administrator accounts cannot modify or delete them during their retention period. Restoration from backups must be tested as part of disaster recovery exercises, at a frequency your association sets and records, not merely assumed to work, and access to backup systems should be restricted to accounts entirely separate from everyday production administration. A backup that can be deleted by the same credentials an attacker has already compromised in the main system offers considerably less protection than its existence alone might suggest.

Why This Requires Ongoing Verification, Not A One-Time Check

Technical control maturity degrades over time as new software is installed, staff change, and configurations drift, connecting directly to the cyber insurance application discussion earlier in this series, where declared controls that no longer match reality can reduce or defeat a claim. Reassess maturity at least annually and after any significant change to the organisation's technical environment. If your association runs mainly on cloud services with no in-house IT staff, ASD's guidance for small businesses may be a more proportionate starting point, and an independent IT provider can give the board assurance.

- Ask directly which Essential Eight maturity level your association's technical environment currently sits at, and treat this as a specific board-level oversight question rather than an unanswerable technical detail.
- Confirm specifically whether MFA for administrator-level and privileged accounts is phishing-resistant, not SMS-based, particularly if your association is aiming for or claims Maturity Level 2 or above.
- Verify who can change or delete your association's backups, and that restoration is actually tested in disaster recovery exercises at a frequency you have set and recorded, rather than assumed to function.
- Confirm backup system access uses credentials separate from everyday production administration, preventing a single compromised account from reaching both live systems and their backups.
- Commission an annual maturity reassessment, and after any significant technical change, rather than treating an initial assessment as a permanent, static answer.

A board does not need to become technically fluent in cyber security to ask these specific questions credibly. It needs to know which questions actually matter, and Australia's own authoritative framework has already identified them. Asking whether your association's MFA is phishing-resistant and whether its backups are protected from deletion is a considerably more useful board-level question than asking whether cyber security has been addressed in general terms. This is one of the practical governance topics built into our Board Director course, alongside the papers, tools and frameworks that turn the principle into your board's actual practice. [Explore the course](#)

Annie Gibbins

Founder and CEO, Nexus Leadership

BOARDROOM ACTION WORKSHEET

The Essential Eight: The Specific Questions Behind General Cyber Assurance

Turn the resource into evidence, a decision and an accountable next step. Keep the completed record in your association's approved board records system.

1 What is the issue or decision?

State the governance question in one clear sentence.

2 What evidence do we already have?

Record the facts, source documents and stakeholder evidence available now.

3 What evidence is still needed?

Identify the legal, regulatory, financial, member or operational information still required.

4 What is the agreed next action?

Capture the owner, timeframe and how the matter will return to the board.

Action owner	Review date	Board decision or resolution

General education, not legal, financial, tax, clinical or governance advice. Confirm specifics at the relevant primary source or with your own qualified adviser. Nexus Leadership is operated by Lipstick Consulting Pty Ltd · ABN 15 619 120 482.

CONTINUE YOUR LEARNING

Turn governance principles into practical board action.

Self-paced courses, editable resources and practical support for association boards and CEOs at nexusleadership.com.au.