

From Compliance to Competitive Advantage

Building a Business Case for Cyber Security

Chris Hawksworth — CyberTeam / Speculo

GovIS • MBIE Wellington • 7 August 2026

What We'll Cover

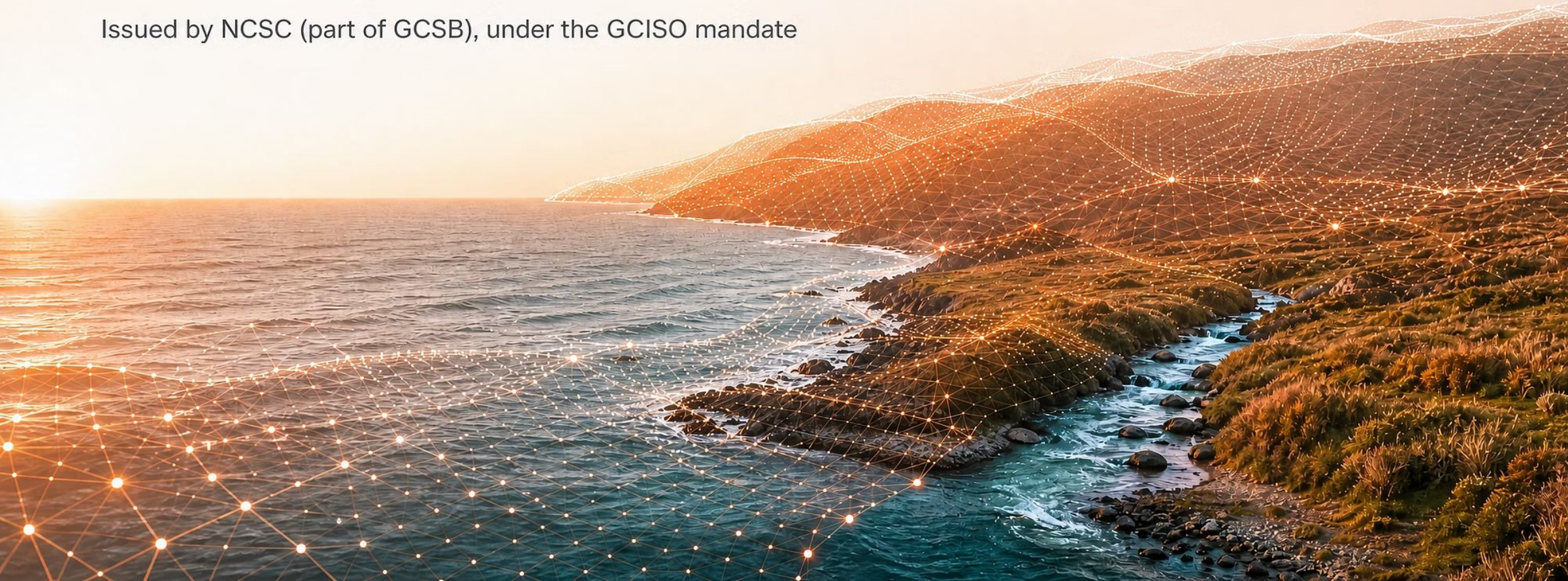
1. What MCSS actually is
2. From controls to risk
3. Speculo, live
4. The business case
5. Questions



What Is MCSS?

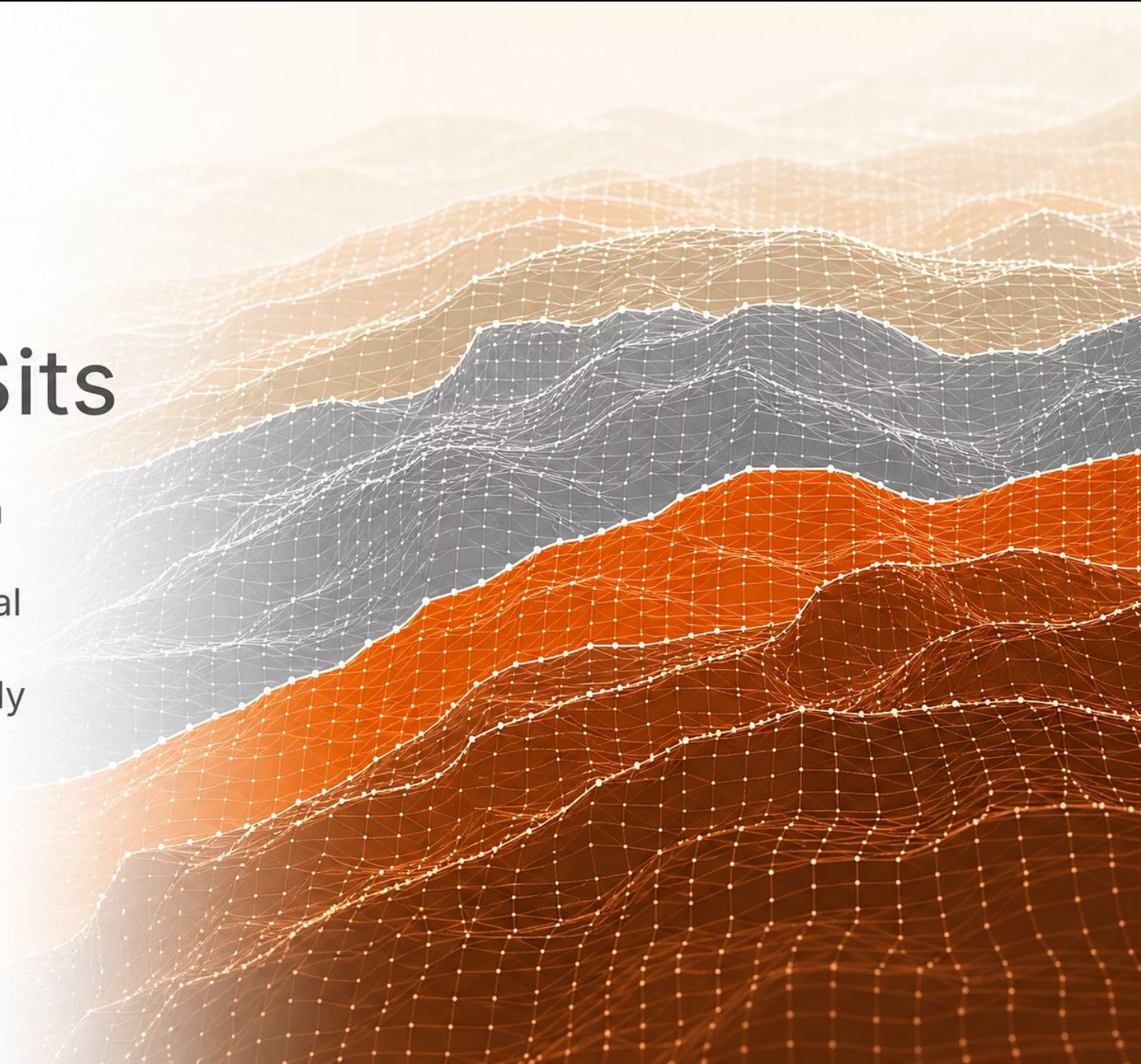
Minimum Cyber Security Standards

Issued by NCSC (part of GCSB), under the GCISO mandate



Where MCSS Sits

- PSR → the assurance mechanism
- NZISM → the full technical manual
- MCSS → the basics, done properly



The 10 Standards

- Risk Management
- Security Awareness
- Assets & their Importance
- Secure Configuration of Software
- Patching
- Multi-Factor Authentication
- Detect Unusual Behaviour
- Least Privilege
- Data Recovery
- Response Planning

Maturity, Not Pass/Fail

1 Informal → 2 Planned & Tracked → 3 Standardised → 4 Quantitatively Controlled → 5 Optimising

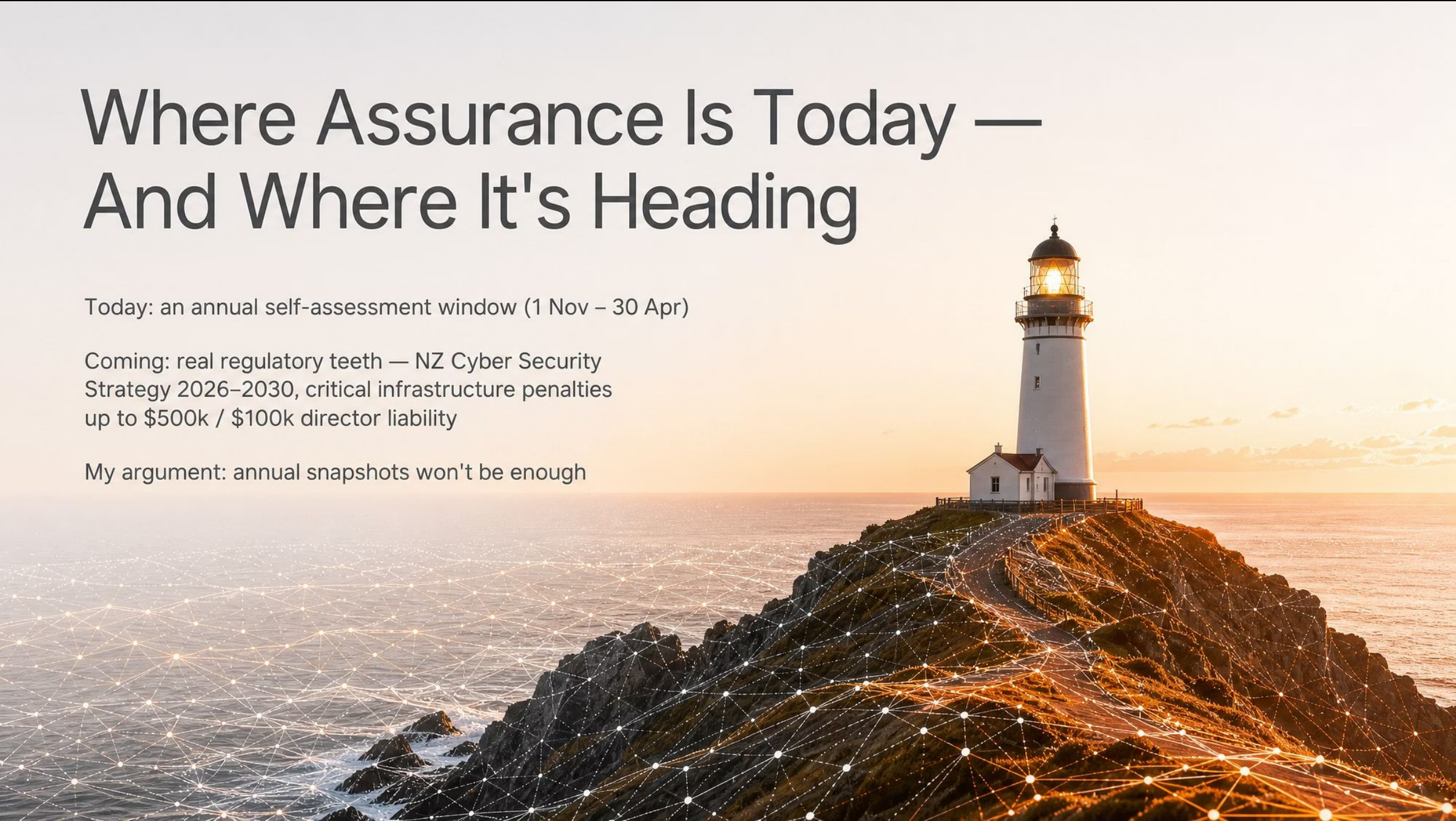
The mandated floor is Level 2

Where Assurance Is Today — And Where It's Heading

Today: an annual self-assessment window (1 Nov – 30 Apr)

Coming: real regulatory teeth — NZ Cyber Security
Strategy 2026–2030, critical infrastructure penalties
up to \$500k / \$100k director liability

My argument: annual snapshots won't be enough



A Compliant Organisation Can Still Get Breached

Waikato DHB, May 2021

The policies existed. The plan existed. It still happened.



An aerial photograph of a river with turquoise water and white rapids, flowing through a dry, brownish landscape. A semi-transparent digital mesh, composed of white dots and lines, is overlaid on the image, particularly prominent on the left and right banks. The text 'Controls Don't Tell You Your Risk. Risk Does.' is positioned on the left side, with 'Risk' highlighted in orange.

Controls Don't Tell You Your Risk. **Risk** Does.

10 standards → not a scorecard, a risk position

Each standard maps to named organisational risks

Turning Controls Into Risk: A Worked Example

- Ransomware & extortion · stolen-credential access · permanent data loss
- Not knowing what you have · trusted-supplier compromise · personal info breach

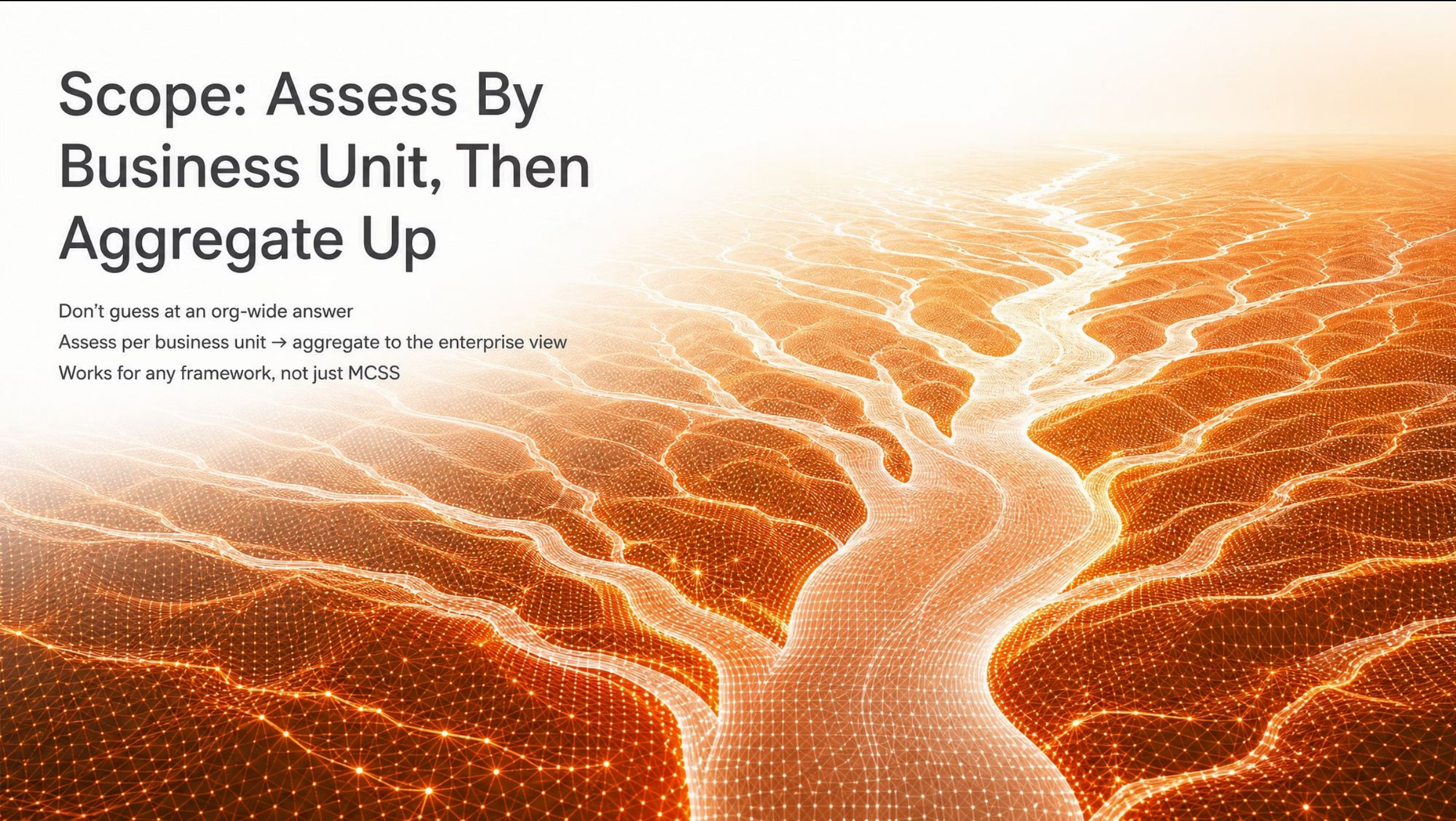
Each risk = a weighted mix of controls + a position on a 5×5 likelihood × impact grid

Scope: Assess By Business Unit, Then Aggregate Up

Don't guess at an org-wide answer

Assess per business unit → aggregate to the enterprise view

Works for any framework, not just MCSS



Prioritising the Gaps: Urgency and Effort

- 1 Urgency — how urgent is it to move this control?
- 2 Effort — how much work is it to close the gap?
(scored 0–100)

AI can help estimate effort consistently, at scale



Let's See It Live



Why 10 Becomes 78

MCSS: 10 standards

Speculo: those 10 expand to 78 mapped controls, out of a 354-control catalogue

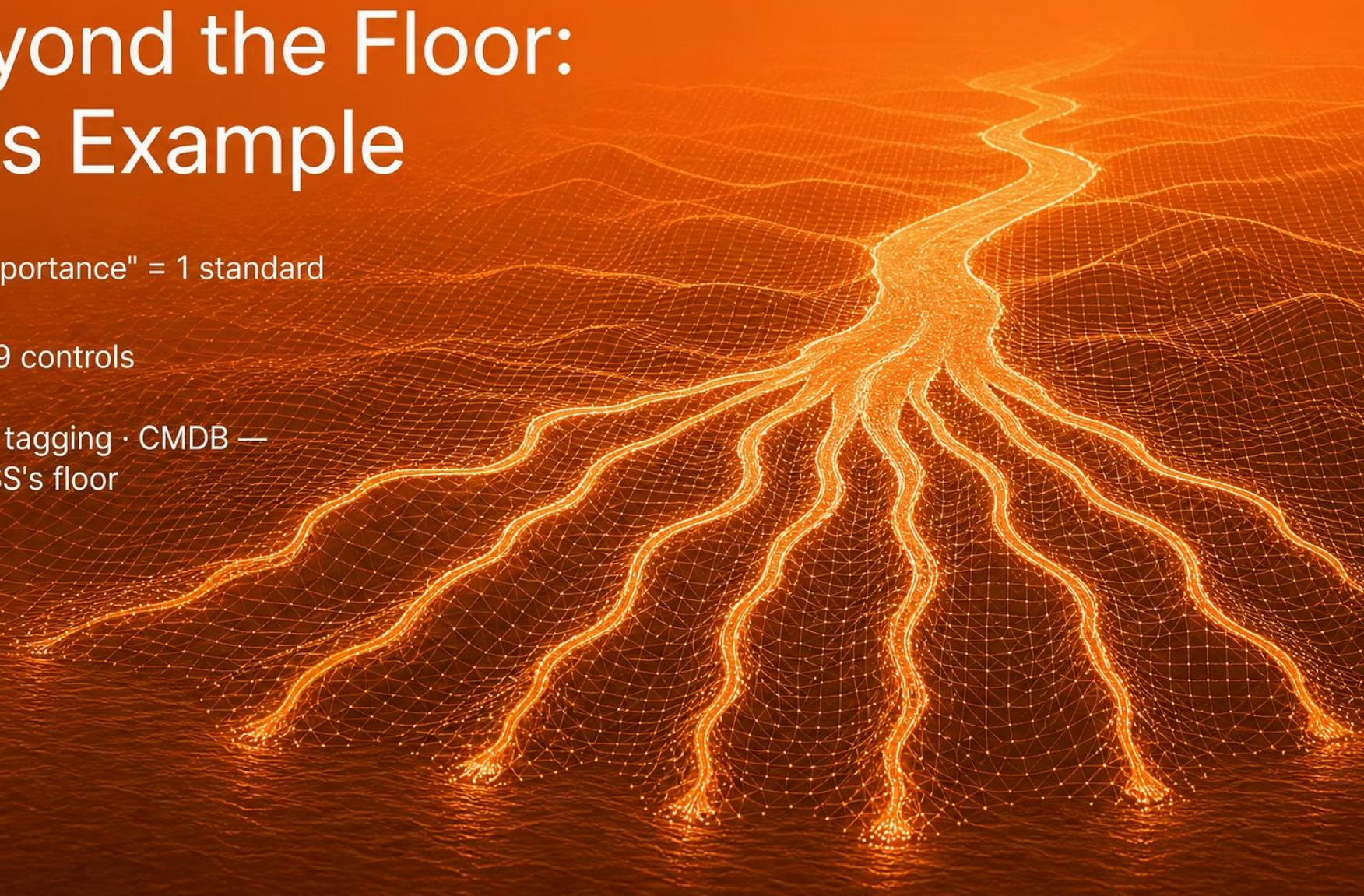
Two reasons: scale, and no duplicated work across frameworks

Going Beyond the Floor: the Assets Example

MCSS "Assets and their Importance" = 1 standard

Speculo's asset domain = 9 controls

Discovery · fingerprinting · tagging · CMDB —
4 of the 9 go beyond MCSS's floor

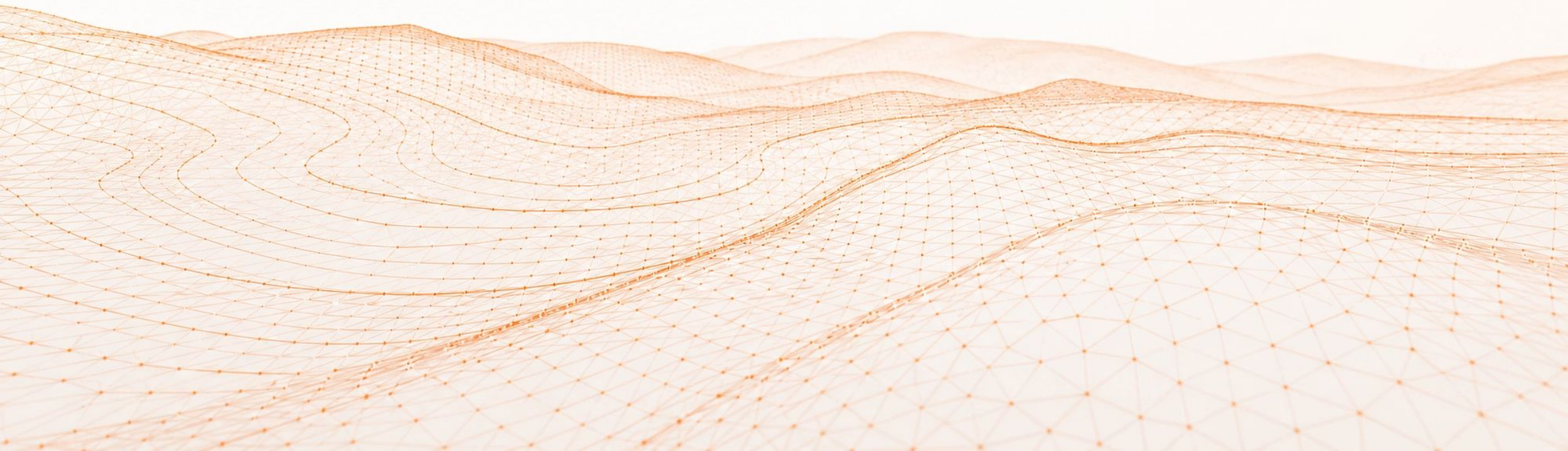


Qualitative vs Quantitative

Most organisations stop at a qualitative gap list

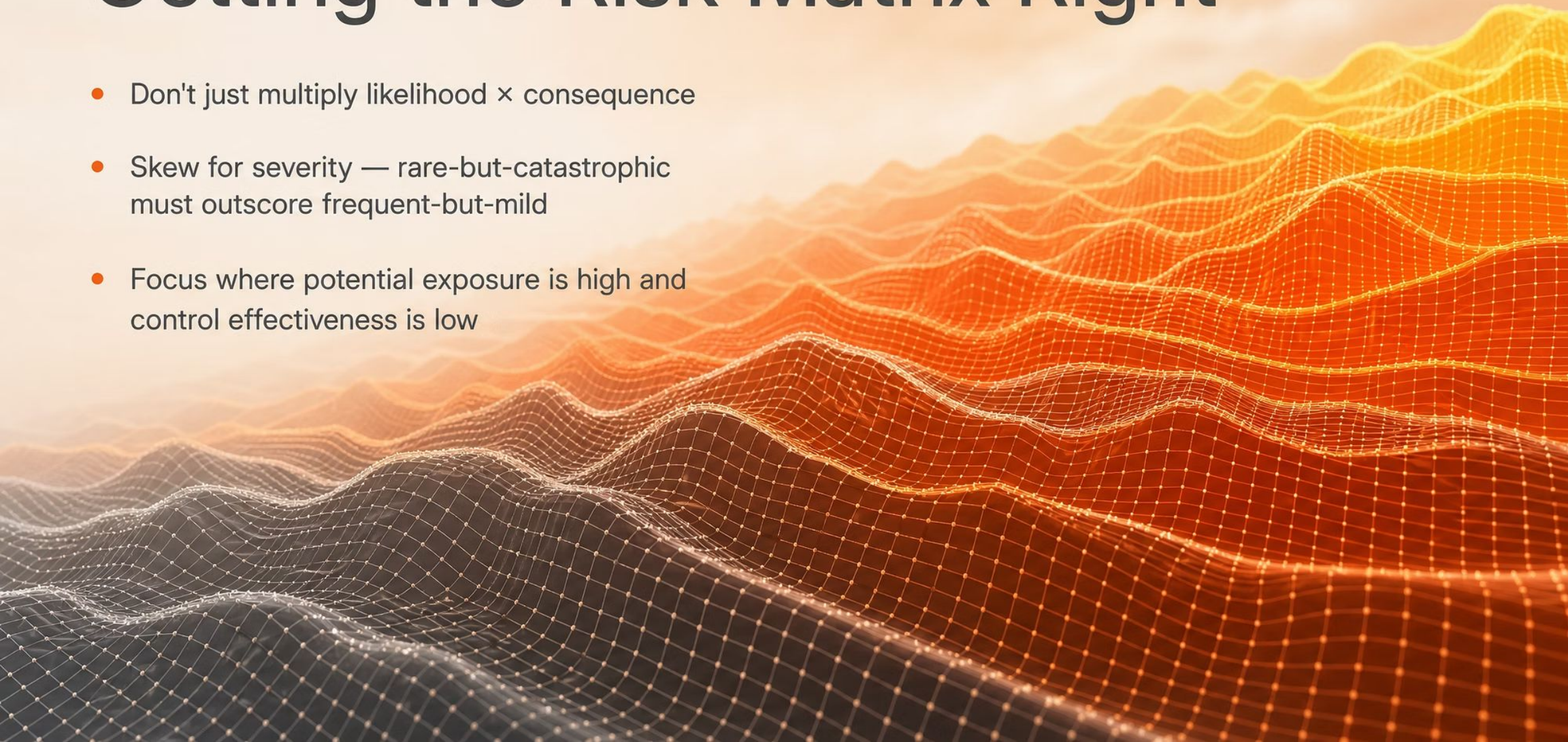
A platform can compute an actual % risk reduction per control

Beyond most orgs to build by hand — but it's the direction worth aiming at



Getting the Risk Matrix Right

- Don't just multiply likelihood $\times$ consequence
- Skew for severity — rare-but-catastrophic must outscore frequent-but-mild
- Focus where potential exposure is high and control effectiveness is low





The Underlying Principle

Know exactly what you're looking at

Know exactly how you're measuring it

Everything in this talk depends on getting that right first

MCSS Is a Government Checklist

Done right, it becomes your funding engine



Metrics: What "Good" Actually Looks Like

- Assets & Importance — % of estate discovered & inventoried
- Patching — % of criticals patched within SLA, mean time to patch
- MFA — % of accounts (and % of privileged accounts) enrolled
- Data Recovery — backup success rate %, # successful restore tests
- Detect Unusual Behaviour — % coverage, mean time to detect

The Three-Box Business Case

1. The problem, in their words
2. The quantified risk position
3. The funded intervention: cost band, timeframe, decision forum



Speak to the Room That Actually Approves It

- 1 CE — reputational risk carried upward
- 2 CIO/CDO — defensibility, "can I answer the minister"
- 3 CFO — "this funds itself"
- 4 Audit & Risk Committee — board-ready evidence



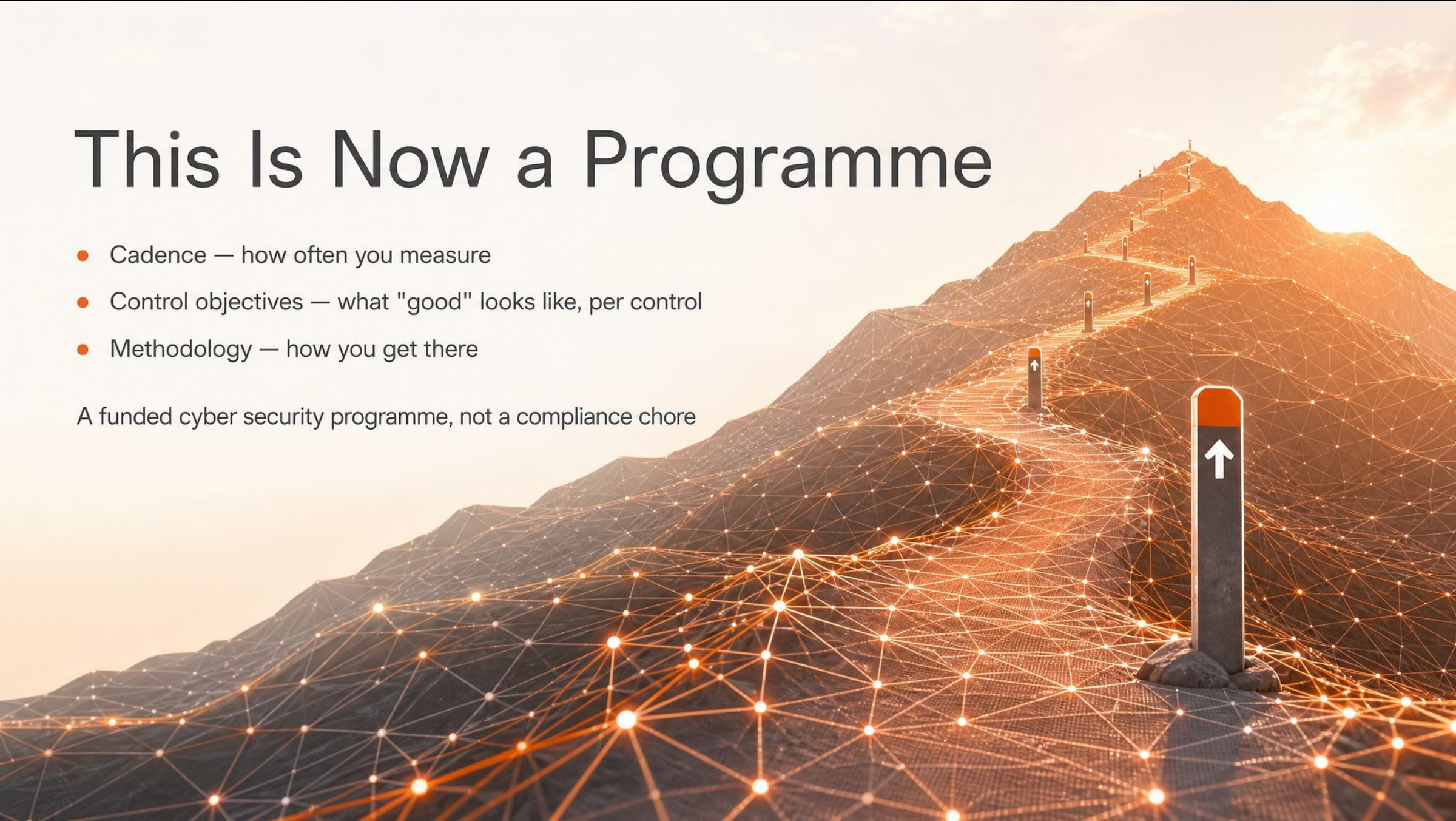
Scaffold Your Reporting: Three Layers

1. Board – outcomes & risk position
2. Planning & strategy – programme progress, priorities, funding asks
3. Operational metrics – the real per-control numbers

This Is Now a Programme

- Cadence — how often you measure
- Control objectives — what "good" looks like, per control
- Methodology — how you get there

A funded cyber security programme, not a compliance chore



MCSS, Free for Public Sector

The MCSS Simple report is free — for any NZ public sector agency

We can have you up and running in under an hour.

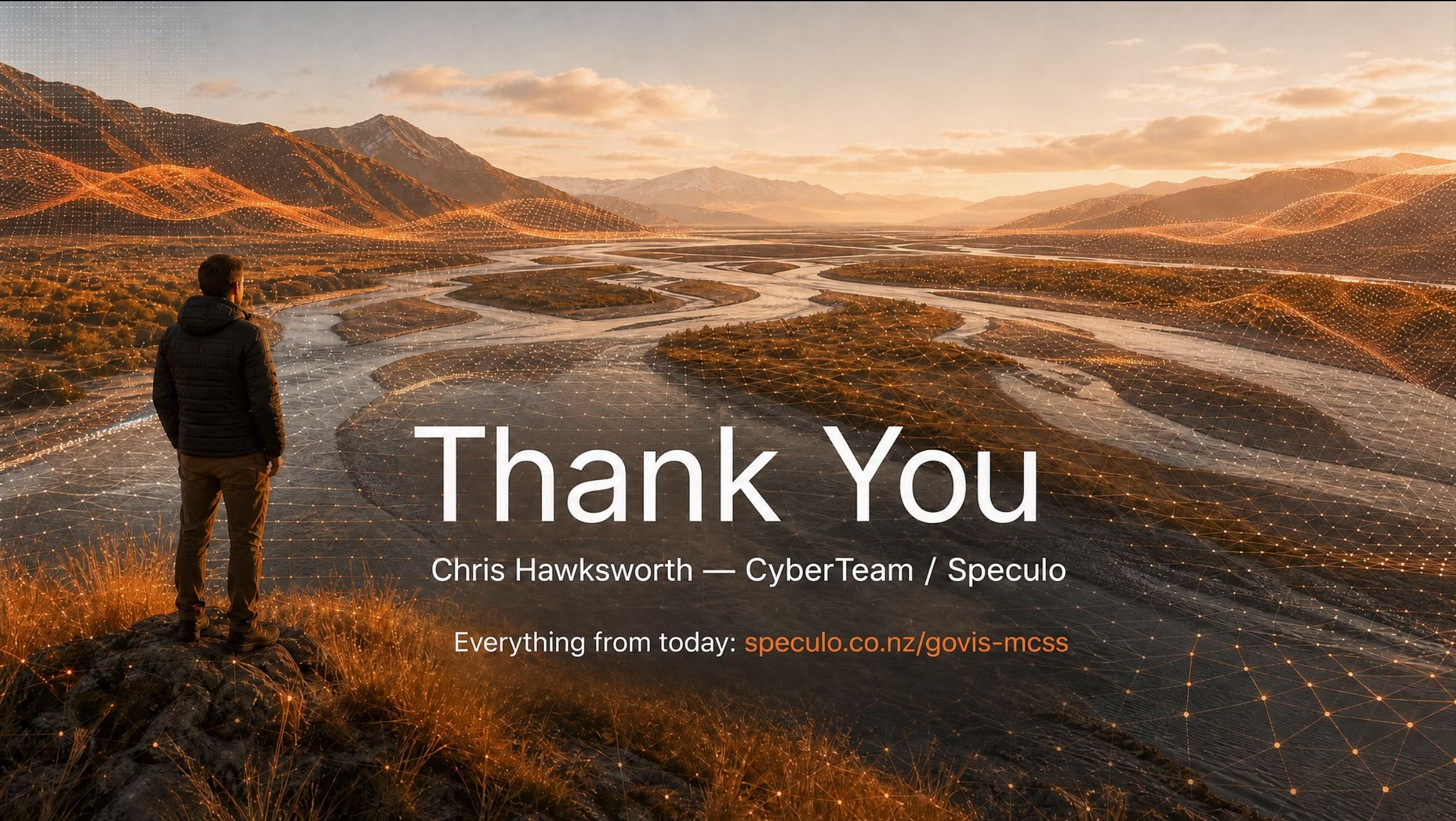
We don't believe this should be chargeable.



Take the Skills Away With You

- 1 Skill 1 — Organisation Risk Discovery
- 2 Skill 2 — Control Weighting & Target Maturity
- 3 Skill 3 — Business Case Conversion

Download all three + this deck: speculo.co.nz/govis-mcss

A person in a dark jacket and pants stands on a rocky outcrop in the foreground, looking out over a wide, winding river valley. The scene is set at sunset or sunrise, with warm orange and yellow light illuminating the landscape. In the background, there are rolling hills and mountains. A digital wireframe overlay, consisting of a network of glowing orange dots connected by thin lines, is superimposed over the entire scene, creating a futuristic, data-driven aesthetic.

Thank You

Chris Hawksworth — CyberTeam / Speculo

Everything from today: speculo.co.nz/govis-mcss



Questions

