ZED
⟨binary⟩

Project Cyber Toolkit

Supporting Secure Delivery Without Slowing Progress

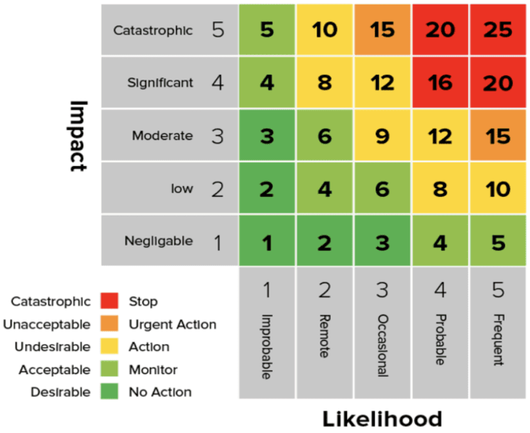
1. Where Cyber Touches Your Deliveries

- Initiation – Risk discovery, vendor checks
- Planning – Governance setup, policy drafting
- Delivery – Ongoing stream monitoring
- Closure – Compliance reporting, handover docs

Smart delivery leaders integrate cyber from Day 1 — not as an afterthought.

2. Risk Snapshot Template

Matrix to identify cyber risks by impact, likelihood, and mitigation strategy.



Impact						
Catastrophic	5	5	10	15	20	25
Significant	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
low	2	2	4	6	8	10
Negligable	1	1	2	3	4	5
		1 Improbable	2 Remote	3 Occasional	4 Probable	5 Frequent
		Likelihood				

Catastrophic	🟥	Stop
Unacceptable	🟧	Urgent Action
Undesirable	🟨	Action
Acceptable	🟩	Monitor
Desirable	🟩	No Action

Using a risk driven approach:

1. Targets your organisation towards meaningful goals, without investing in unnecessary technologies, changes, and products.
2. Assessing risks, allows the ability to accept risks that are unlikely to be realistic.
3. Also helps to prioritise effort and realise tangible outcomes.
4. Provides clarity for stakeholders

3. Mini Policy Starter Kit

- Information Security Policy
- Access Control Policy
- End-user device Policy
- Vendor Due Diligence Checklist

Delivering these key policies allows organisations to quickly get every department and line of reporting onto the same page regarding cybersecurity.

This includes how data is stored and transmitted, how permanent and temporary access is controlled, how users access systems and data on their devices, and how the company works with vendors without introducing risk.

4. Essential 8 Cheat Sheet

A simplified reference of cybersecurity controls tailored for your organisation.

- **Governance** - Making sure everyone is aware and doing the right thing.
- **Patching** - Ensuring all operating systems and applications are up to date and as secure as they can be made by the vendors.
- **Configuration** - Locking down applications and operating systems to their most secure settings, but still making sure they are usable.
- **Access Restrictions** - implementing Multi-Factor Authentication, making sure the right people can access the right information, and restricting access for non-essential staff.
- **Application Control** - Restricting the installation of insecure and non-essential applications on business infrastructure and systems.
- **Backups** - Ensuring data can be recovered safely, quickly, and efficiently. Providing confidence to the recovery of data under any circumstances

5. Our Deliverables at a Glance

We provide:

- Cyber risk registers
- Policy documents
- Stream reporting for PMOs
- Cyber maturity assessments

Need a walkthrough of how this applies to your roadmap?

🗓️ Book your 15-min Cyber Alignment Call