CYBERSECURITY FRAMEWORKS CHEAT SHEET

THE INSTILLERY

NIST Cybersecurity Framework

- **Focus:** Flexible, risk-based approach to improving cybersecurity
- **Core Components:** Identify, Protect, Detect, Respond, Recover
- **Ideal For:** Long-term cybersecurity posture management
- **Key Industries:** Critical infrastructure sectors (finance, healthcare, energy)
- **Key Benefit:** Clear, structured approach to risk management

ISO/IEC 27001

- **Focus:** Information security management systems (ISMS)
- **Core Elements:** Risk assessment, security controls, continuous improvement
- **Implementation:** Requires documentation, internal audits, compliance demonstration
- **Best For:** International compliance or strong customer data protection
- **Key Industries:** Finance, IT services, telecommunications

SOC 2 Type 2

- **Focus:** Security, availability, processing integrity, confidentiality, privacy
- **Implementation:** Requires independent audit, detailed evidence of control operation
- **Best For:** Service organisations handling sensitive customer information
- **Key Industries:** Cloud services, SaaS, financial services
- **Key Benefit:** Evaluates design and operational effectiveness of controls over time

CERT NZ 10 Critical Controls

- **Focus:** 10 practical controls to protect against common cyber threats
- **Core Components:** Patch management, access control, monitoring and alerting
- **Best For:** Quick improvement of security posture
- **Key Industries:** Small to medium-sized businesses
- **Key Benefit:** Straightforward and easy to implement

Choosing the Right Framework

Consider:

1. Your organisation's size and industry
2. Your specific security needs
3. Your regulatory & governance requirements

Implementation Best Practices:

1. Conduct initial assessment
2. Develop a clear plan
3. Ensure top management buy-in
4. Continuously improve and update