CLOUDBASE

Cloudbase Cyber Review

Powered by THINKING

Avoid making the wrong Cybersecurity decision

What

The Cloudbase Cyber Review from THINKING leverages cloud technology to review your organisation's cybersecurity assets. It provides objective, data-driven visibility on what's working and what is not and what to do about it.

Why

Increasingly onerous New Zealand and international compliance and regulatory requirements placed on company executives and board directors today put the senior leadership on the front line of an escalating cybersecurity crisis. Your ability to make an informed decision is critical to protecting your business and reputation.

How

The Cloudbase Cyber Review is modular and objective. Using data and professional tools, the review identifies risk issues for remediation and includes tactical and strategic recommendations. Presented in a traffic light format with supporting documentation, remediation tasks are ranked according to priority.

Benefits

Complete visibility, smarter investment decisions

Are you overwhelmed with technical jargon and relying on reports that raise more questions than answers? The Cloud-based Cyber Review will give you a bird's eye view of what is and isn't working.

Manage risk

Privacy and other regulatory compliance, cyberattacks and malware, insurance exclusions, supply chain partners vulnerabilities, and reputational damage are risks that senior business leaders need to prepare against. The Cloudbase Cyber Review will give you the confidence to move forward proactively.

Governance and Compliance

- **Privacy Act 2020**

  Established to regulate how organisations collect, store, use, and share personal information, hefty fines – between $10,000 and $500,000 – await those who have failed to take reasonable steps to protect personal data or who do not notify the Privacy Commissioner of any breaches.

- **AML and CFT**

  Established to prevent cybercrime and financial crimes, the Anti-Money Laundering and Combating of Financial Terrorism regulations put the onus on organisations to take all reasonable steps (across hardware, software, cloud applications and expertise) to protect against cybercrime and minimise risks as they relate to the AML and CFT framework.

  The Financial Markets Authority (FMA) also requires that all cybercrime and breach incidents are reported to the FMA itself. Lack of expertise or reliance on company officers who do not have the requisite experience is not considered a mitigating factor.

  Consideration should be given to creating a cyber-security framework, risk assessment, technical security assurance, determining current risks, remediation plans and ongoing risk management.

- **ISO27001**

  A global standard for information security management systems, ISO27001 sets a high specification for legislative compliance and the cyber safety and security of the organisation, its people and data. Organisations that comply with ISO27001 not only exhibit rigorous cybersecurity management, they also enjoy the confidence of partners and customers.

- **Payment Card Industry Data Security Standard (PCI)**

  An information security standard for organisations that store, transmit and process credit card information do so in a secure environment.

- **NZ Code of Good Manufacturing Practice (GMP) Therapeutic Goods**

  Defending against cyber-attacks in the GMP environment (primarily in pharmaceuticals) means that the exchange of data electronically should include appropriate checks for secure processing, security of stored data, regular back-ups, and measures to prevent unauthorised entry.

Features
Data led, objective and modular

Your Cloudbase Cyber Review will review and provide guidance backed by data around select areas of the organisation or across the entire ecosystem including but not limited to:

- **NIST Survey:** US National Institute of Standards and Technology framework-based review.

- **Professional tools and data-based:** Examples include Tenable.io, Nessus Pro (commercial vulnerability scanners) and DMARC Analysis, using industry standard toolsets.

- **Documentation:** Review of all policies, procedures and documentation.

- **Cloud security posture management (CSPM):** Cloud security posture management (CSPM) to identify risks across all cloud platforms.

- **Risk Reconnaissance:** External viewpoint using RiskRecon data (optional module, suitable for more extensive engagements).

- **Objective:** Technology agnostic, the review is not an opinion; it is data-driven and based on fact.

- **Modular:** The modular nature of this product allows you to be selective about what is included in the review. Recommendations are designed for staged, priority-driven implementation.

- **CIS Review of SaaS platforms:** The Centre for Internet Security review is based on a set of best practice standards for cybersecurity.

- **Network Detection and Response:** Onsite Security Information and Event Management (SIEM) consolidation of network traffic with further analysis provided by a cloud based NDR (Network, Detection and Response) solution.

What's involved
Plug privacy leaks, get staff cybersecurity ready and reduce wasted spend

Designed to review, understand and ultimately inform remediation of your cybersecurity ecosystem, the Cloudbase Cyber Review may include:

- On-premises cybersecurity defences like your firewall and VPN.

- Identify out-of-support software, including patches and hardware upgrades.

- Cybersecurity training and staff awareness needs.

- Effective endpoint protection from malware attacks and other malicious activity threats.

- Cybersecurity governance-related policies, procedures and guidelines, such as your information security policy.

- Sanctioned and unsanctioned cloud applications, e.g. Facebook file-sharing and WeTransfer.

- Email protection as it relates to your email reputation score.

- External facing systems such as your organisation's website.

- Patching and recommendations around system hardening processes.

- Asset Management Solutions.

- Review of physical network cable infrastructure.

- Server audit and gateway health check.

Together with THINKING's expertise and experience, the Cloudbase Cyber Review is invaluable for helping senior leadership set priorities to help you journey towards a more secure, cyber-resilient position that aligns with business priorities as budget and scheduling permit.

Want more
information?

Visit www.thinking.net.nz

General Enquiries: enquiries@thinking.net.nz

Follow: Thinking

Postal Address: PO Box 26 Waimauku, Auckland
0842, New Zealand