INDEPENDENT CYBERSECURITY ASSESSMENT

Integrated Solutions

Table of Contents

Integrated Solutions

INDEPENDENT CYBERSECURITY ASSESSMENT

What does the Cybersecurity Assessment entail?

Integrated Solution's Independent Cybersecurity Assessment has been created to identify vulnerabilities, mitigate risks, and enhance the overall security posture of your company to ensure robust security measures are implemented. The readiness assessment utilises the CIS Critical Security Controls, which are a prioritised set of actions designed to impede the most pervasive cyberattacks. These have been developed and are continually updated by a global community of cybersecurity experts, and are a trusted framework for organisations looking to bolster their defences.

1. Comprehensive Coverage

Ensures a holistic approach to cyber security, covering a wide range of security areas.

2. Proven Effectiveness

Evidence-based controls that significantly reduce the risk of cyber attacks when implemented properly.

3. Prioristisation

Organised into three implementation groups to help organisations prioritise actions based on resources and risk profile

4. Community Consensus

Developed with input from a diverse group of cybersecurity professionals, ensuring practical, relevant, and up-to-date recommendations.

5. Alignment with Standards

Aligns with other major security frame works and regulatory requirements, facilitating easier compliance.

Readiness Assessment Scoring

Each assessment report will include a detailed breakdown of each control along with a corresponding score, assessment and recommendation. This scoring range provides a clear indication of an organisation's security capabilities and preparedness, allowing for effective communication of strengths and weaknesses in cybersecurity practices.

Score	Description
0% - 25% (0)	Indicates significant gaps and deficiencies in cybersecurity practices. The organisation is highly vulnerable to cyber threats and may be at significant risk.
26% - 50% (1)	Suggests some efforts have been made, but there are still considerable short comings in cybersecurity practices. The organisation is vulnerable to various cyber threats and needs substantial improvements.
51% - 75% (2)	Indicates a moderate level of cybersecurity maturity. The organisation has implemented several cybersecurity measures, but there are still areas that need improvement to enhance overall security posture.
76% - 100% (3)	Reflects a high level of cybersecurity maturity. The organisation has implemented robust cybersecurity practices across most areas and is well prepared to mitigate cyber threats effectively.

Integrated Solutions

Cybersecurity Business Assessment includes these controls:

01 Inventory and Control of Enterprise Assets

02 Inventory and Control of Software Assets

03 Data Protection

04 Secure Configuration of Enterprise Assets and Software

05 Account Management

06 Access Control Management

07 Continuous Vulnerability Management

08 Audit Log Management

09 Email and Web Browser Protection

10 Malware Defenses

11 Data Recovery

12 Network Infrastructure Management

14 Security Awareness and Skills Training

15 Service Provider Management

17 Incident Report Management