Silver Cyber Resilience Certification from ramsac

ramsac is committed to helping organisations to protect themselves against cybercrime, to help organisations understand where they are on their cyber resilience journey, we have created the ramsac cyber resilience standards.

Drawing on 30 years' experience of managing IT risks for a wide range of organisations, the ramsac Cyber Resilience Certification is a comprehensive standard which provides a best practice guide for organisations to work towards.

Securing your organisation from the ground up

ramsac's **Silver** Cyber Resilience Certification helps your organisation achieve industry standards to protect your whole organisation against cybersecurity threats. The **Silver** measures put a focus on advanced technical measures to safeguard your organisation from cyberattacks, as well as your people and strengthening your human firewall.

By achieving the ramsac **Silver** Cyber Resilience Certification, you are demonstrating to your customers your commitment to total protection through investment in your employees.

How to achieve the Silver Cyber Resilience Certification

To achieve this level, organisations will need to have met the requirements of the **Bronze** Cyber Resilience Certification and the following:

Anti-Spam

As a further layer of protection between your employees and threat actors, Anti-Spam services reduce risk by detecting and quarantining potential malicious email such as phishing attacks.

Anti-Ransomware

Your Anti-Virus services should provide an anti-ransomware or encryption rollback service to safeguard against ransomware attacks.

Enhanced patching & software update processes

Servers and hardware devices, including device firmware, should be patched as regularly as possible. Enabling automatic updates for business applications means that you are protected from vulnerabilities as soon as patches are available.

*continued overleaf

ramsac
the secure choice

How to achieve the Silver Cyber Resilience Certification

To achieve this level, organisations will need to have met the requirements of the **Bronze** Cyber Resilience Certification and the following:

Mobile Device Management tools

MDM not only affords better control over the deployment and management of work devices but provides a facility for better protection of work data on personal devices, preventing data loss or leakage should a device be lost or stolen or from insider threats.

Password manager

Password Managers significantly improve the ability of your employees to manage their various passwords for key business systems, encouraging the reduction of simple, repetitive passwords, and passwords being stored in non-secure systems or written down.

Cybersecurity awareness training

Your employees are your best defence against cyberattacks as well as your biggest weakness. Its critical that employees are up skilled on cyber issues through regular, ongoing cybersecurity awareness training.

Phishing simulation training

Training your employees on how to spot and report phishing emails is another important layer to protect your organisation from phishing attacks.

Disaster Recovery or Business Continuity Plans

Knowing what to do when disaster strikes or you lose a key piece of business-critical software is important, especially for board/exec members. Having a clear plan for a crisis can reduce business impact to you and your customers.

Cyber breach response plan

Experiencing a cyber breach is a "when, not if" scenario, so knowing what steps to take to minimise further impact or damage is vital for all employees in the organisation.

Cyber assessment

ramsac can perform a cyber assessment with you to determine any potential gaps and can assist with remedial actions to help you achieve **Silver.**

Tel: **01483 412 040** email **info@ramsac.com**

ramsac
the secure choice