Bronze 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 Certifications is a comprehensive standard which provides a best practice guide for organisations to work towards.

Laying the foundations of a secure organisation.

ramsac's **Bronze** Cyber Resilience Certification represents our minimum recommendations that organisations must have for protection against cybersecurity threats. The **Bronze** measures are achievable for all organisations, regardless of how many employees you have or the industry you work in.

By achieving the ramsac **Bronze** Cyber Resilience Certification, you are demonstrating to your customers that you take sensible steps to safeguard their data and the services you provide to them.

How to achieve the Bronze Cyber Resilience Certification

To achieve this level, organisations will need to have:

Enterprise Anti-Virus

Your servers and workstations should be protected with an enterprise-grade Anti-Virus solution to safeguard against malware and viruses.

Enterprise firewall

Any physical sites and company networks should be behind an enterprise-grade firewall to protect against unauthorised access.

Air-gapped backup and recovery solution

An important recovery method following a ransomware or other cyberattack or data loss scenario is to restore from protected/ air-gapped Cloud backups.

*continued overleaf

ramsac
the secure choice

How to achieve the Bronze Cyber Resilience Certification

To achieve this level, organisations will need to have:

Up to date operating systems & software

All device Operating Systems and business-critical software should be in support with the vendor to ensure that vulnerability fixes are applied.

Server room security

Physical IT hardware needs to be behind a locked door and limited to key personnel to prevent unauthorized access and potential data loss or leakage.

Device encryption

All laptops, or any device that leaves the office, should have whole-disk encryption applied to prevent data loss or leakage in the event of the device being lost or stolen.

Multi-Factor Authentication

The biggest safeguard against phishing attacks, MFA is proven to reduce the impact of phishing attacks by over 90% and is a must for business-critical systems access.

Control over administrator rights

Administrator rights should be limited across your organisation, especially local admin rights which should be locked down on local devices to prevent malware from running malicious programmes that would otherwise be prevented with normal privileges.

Patching schedule

All servers and workstations should have a regular patching schedule, with devices periodically audited for patching compliance. Patches are continuously released by software vendors to fix potential vulnerabilities in systems.

New-starter cybersecurity training

The ICO mandates that all new-starters should have some basic cybersecurity training within their first 30 days or before they have access to customer data.

IT security policy

An IT Security Policy is critical to clearly outline the responsibilities of your employees in relation to protecting customer data and helping to prevent cyberattacks.

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 **Bronze.**

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

ramsac
the secure choice