Cyber Resilience Certification from ramsac

In a world of ever-increasing cyber threat events, it's never been more important to ensure that you have the necessary protection in place to safeguard your business and customer data. In 2024 a third of all UK charities reported a cyber breach and 70% of medium sized businesses in the UK experienced a cyber-attack. **How confident do you feel in your organisation's resilience against cyber threats?**

Your cyber resilience journey

All organisations are on a cyber resilience journey. For some, they are right at the beginning and just starting to think about how they can better secure their data, for others, they are ahead of the curve, they've taken all reasonable steps and they are doing their best to continue to evolve in line with best practice and the latest threats. To help our clients understand where on that journey they are, we have created the ramsac Cyber Resilience Standards.

By assessing your organisation's position against our standards, you can assess your risks, strengthen your protection and demonstrate to your customers and stakeholders that you take the protection of their data seriously.

Cyber Resilience Certification

Based on over 30 years of managing IT risks for a wide range of organisations, ramsac has defined 3 cyber resilience levels , **Bronze**, **Silver** and **Gold**.

Our **Bronze** certification represents the minimum level of good practice that all organisations should strive for. By achieving Bronze, organisations will be committing to implementing and maintaining a solid foundation of a secure organisation and will benefit from significantly reducing the organisations attack risk, minimising the chances of easily avoidable breaches.

The **Silver** certification represents great cyber resilience, reflecting practices that protect both end user devices, IT hardware and cloud stored data.

Organisation's that achieve **Gold** certification really are demonstrating the best in cybersecurity practices and they are implementing proactive measures to assess their vulnerability on an ongoing basis.
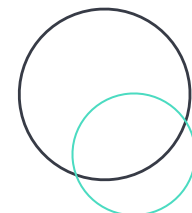
The assessment & certification process

Our experienced IT security professionals will undertake an indepth audit of your IT estate. The result of our assessment will be a detailed report identifying IT and cyber risks, with a practical suggestion of how each finding can be addressed. We will establish where you are against each of the three levels of our standard, Bronze, Silver or Gold and then issue you with your certificate, which you can use to demonstrate your commitment to cybersecurity.

The criteria for each level will include;

Service	Bronze	Silver	Gold
Next-gen Anti-Virus or EDR tool	✓	✓	✓
Enterprise grade firewall at company sites	✓	✓	✓
Air-gapped backup for servers/storage and 365 accounts	✓	✓	✓
Appropriate patching schedule	✓	✓	✓
Supported OS & software	✓	✓	✓
Encrypted devices	✓	✓	✓
Mobile Device Management	✓	✓	✓
Server room security	✓	✓	✓
Multi Factor Authentication	✓	✓	✓
Email protection	✓	✓	✓
Segregated Admin accounts	✓	✓	✓
Cybersecurity training for new starters	✓	✓	✓
Documented IT security policies	✓	✓	✓
Software Vulnerability Management		✓	✓
Segregated office networks		✓	✓
Mobile Application Management		✓	✓
Managed cybersecurity monitoring		✓	✓
Ongoing cybersecurity training and phishing testing		✓	✓
Documented breach response plan		✓	✓
Documented business continuity plan		✓	✓
3rd party penetration testing			✓
Asset information register			✓
C-suite cyber training and planned testing exercise			✓
Privileged Identity Management			✓
Data Loss Prevention			✓