

Gold 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.

Provide the best possible security for your organisation.



ramsac's **Gold** Cyber Resilience Certification reflects industry-leading protection against cybersecurity threats, giving your organisation the best defence from cyberattack. Our secure+ monitoring service gives you piece of mind, as we monitor your environment 24/7 from potential malicious activity.

By achieving the ramsac **Gold** Cyber Resilience Certification, you are demonstrating to your customers that you are doing everything it takes to be the most cybersecure business around, with the safeguarding of their data and your services being top priority.

How to achieve the Gold Cyber Resilience Certification

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

Bronze Cyber Resilience Certification



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.

Silver Cyber Resilience Certification



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.



*continued overleaf

How to achieve the Gold Cyber Resilience Certification

To achieve this level, in addition to the **Bronze** and **Silver** Cyber Resilience Certification requirements organisations will need to have:



Penetration testing

Regular penetration testing of your external facing systems is recommended to identify any potential vulnerabilities. On a different vector, social penetration testing is a great way of seeing how your employees react to a simulated social engineering attack on your organisation, identifying areas for improvement to prevent the real thing.



Software approval processes

Locking down your devices to prevent unauthorised software installs or using a tool to effectively manage the controlled installation of software is a great way to maintain control of your environment and minimise your attack surface.



Exec-level training

Your executives are some of your most important employees, and therefore this makes them the most highly targeted through spear-phishing attempts. As executives tend to have significant business oversight or access, a compromise of an exec can have devastating repercussions. Training aimed at executives, as well as table-top cybersecurity exercises, can have a significant impact on your protection from spear-phishing attacks.



Proactive cybersecurity monitoring

The ultimate level of protection from cyberattack is the use of proactive cybersecurity monitoring services. ramsac's secure+ provides 24/7 monitoring and detection services from our highly skilled Cybersecurity Analysts, who relentlessly hunt for potential malicious activities across your environment and prevent cyber incidents from occurring.

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 **Gold**.

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