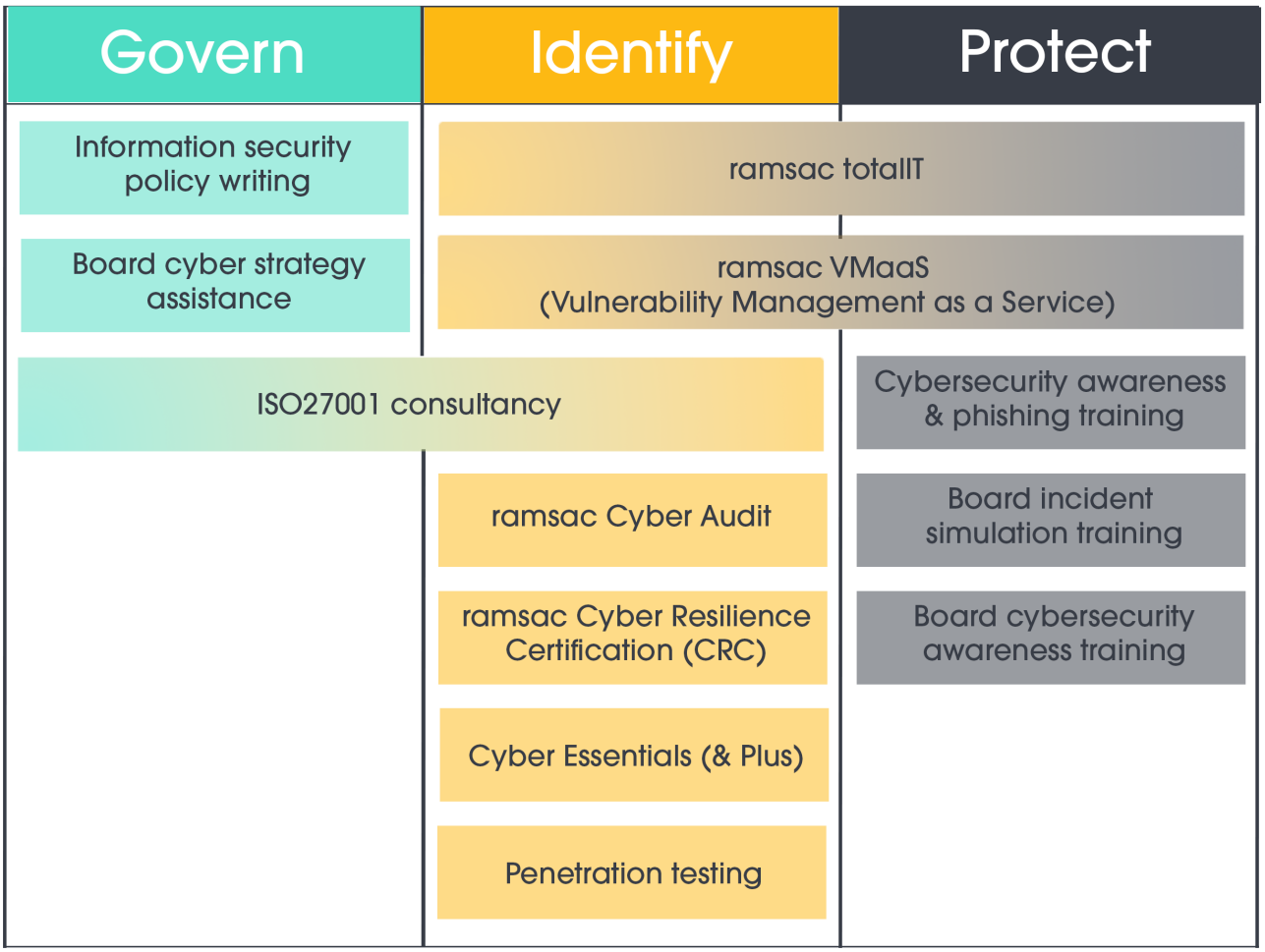
Cybersecurity from ramsac

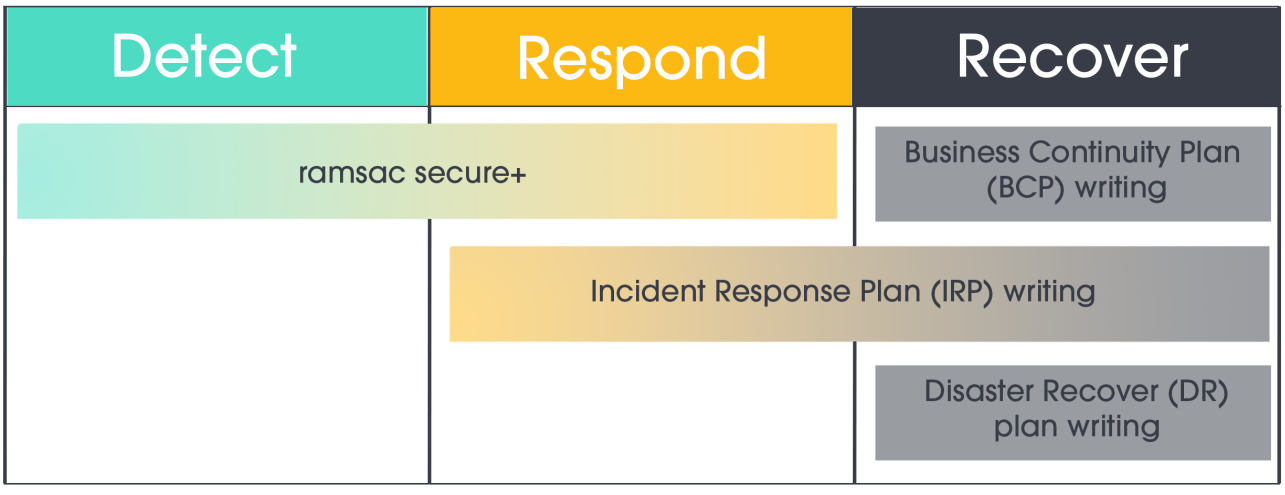
Comprehensive solutions for protecting your organisation at every stage

ramsac
the secure choice

The 6 core elements of cybersecurity.

At ramsac, we understand that cybersecurity is a dynamic and multi-faceted challenge for modern organisations. Ensuring the security of your business requires a holistic approach that covers every stage of the cyber resilience lifecycle. We have built services to assist our clients across all areas of the NIST Cybersecurity Framework (CSF) 2.0: **Govern, Identify, Protect, Detect, Respond,** and **Recover**. Each of these elements plays a critical role in safeguarding your organisation against the evolving landscape of threats. With our specialised solutions, we help you build, implement, and manage a cybersecurity strategy that's robust, compliant, and future-proof.





ramsac
the secure choice

Govern: Establishing strong cyber governance

Establish a clear cybersecurity governance structure to ensure that your policies and strategies align with best practices and regulatory requirements. Without strong governance, security efforts can become fragmented and ineffective. ramsac offers services to help you build a solid foundation, including:

- Information security policy writing
- Board cyber strategy assistance
- ISO27001 consultancy (also part of Identify).

Information Security Policy Writing

Writing a security policy can be quite time consuming and daunting. Many organisations end up writing a generic policy that does not capture their approach to security and doesn't provide proper security guidance for employees. Our cybersecurity consultants can write a jargon free security policy that reflects an organisation's approach to security.

Board Cyber Strategy Assistance

It is crucial that an organisation's Board take an active role in understanding the level of cyber risk they are exposed to, and work to establish a meaningful and effective strategy to protect against cyber threats.

Our Cyber strategy workshop is designed to help Board members understand what they should be doing in their organisation, questions that they need to be asking of their IT advisers, and devise a strategy for minimising risk of prosecution.

ramsac
the secure choice

Govern

Identify

Identify: Uncovering vulnerabilities and risks

Proactively identify and assess risks, vulnerabilities, and weaknesses in your systems before they are exploited. Knowing where your vulnerabilities lie is the key to stopping potential threats in their tracks. ramsac provides identification services, such as:

- ISO27001 consultancy (also part of Govern)
- ramsac Cyber Audit
- ramsac Cyber Resilience Certification (CRC)
- Cyber Essentials (& Plus) certifications
- Penetration testing
- Vulnerability Management as a Service (VMaaS) (also part of Protect)
- ramsac totalIT (also part of Protect)

ISO27001 Consultancy

The ISO 27001 Gap Analysis Review helps you identify any gaps in your security practices, ensuring you're fully prepared for certification or audit. Whether you're new to ISO 27001 or already certified, our expert team will guide you through the process. We offer tailored gap analysis for:

First-time certification: If you're looking to achieve ISO 27001 certification, we'll help you identify where your biggest gaps are, so you can confidently work towards compliance.

Surveillance audit preparation: For businesses already certified, we provide a detailed gap analysis to ensure you're ready for your next annual surveillance audit, keeping your certification in good standing.

Transition to ISO 27001:2022: If you're transitioning from ISO 27001:2013 to the latest ISO 27001:2022 standard (required by October 2025), we'll assess your current compliance and highlight the necessary changes to ensure a smooth transition.

ramsac Cyber Audit

A cyber security audit is a comprehensive review of an organisation's IT estate, policies, and procedures to identify vulnerabilities that could lead to a data breach. Our consultants perform audits to ensure IT systems meet compliance requirements with relevant laws and regulations.

ramsac Cyber Resilience Certification (CRC)

CRC is designed to help organisations assess and strengthen their defences against cyber threats by following best practice standards. The certification is split into 3 levels, allowing organisations to choose the level that best fits their needs and current security posture.

Bronze: Represents the minimum good practice, covers essential aspects like antivirus, encryption, firewalls, backups, and cybersecurity training.

Silver: Building on the Bronze level, the Silver certification includes more advanced protection measures, including web/spam filtering, mobile device management, and a breach response plan.

Gold: The highest level of certification, Gold, demonstrates industry-leading cybersecurity practices. It includes third-party penetration testing, executive training, enhanced security monitoring, and proactive response measures.

The assessment includes a detailed IT audit, followed by a prioritised report. The certification reduces cyber attack risks and demonstrates your commitment to data protection.

Penetration testing

ramsac offers expert penetration testing services to help identify and address vulnerabilities in your IT infrastructure. Our consultants simulate real-world cyberattacks to assess your defences, providing actionable insights and recommendations. This proactive approach enhances your cybersecurity posture, mitigates risks, and ensures your systems are resilient against potential threats.

Cyber Essentials (& Plus) certifications

Cyber Essentials is a government-backed certification helping UK businesses defend against common threats. ramsac supports both certification levels:

Cyber Essentials: ramsac guides businesses through the self-assessment, helping to ensure all basic security controls are in place.

Cyber Essentials Plus: ramsac provides hands-on support, including pre-assessments, gap analysis, and coordination with certifying bodies to help businesses pass the independent technical verification.

Achieving Cyber Essentials with ramsac enhances cybersecurity, improves client trust, and ensures expert guidance throughout the process.

Protect: Fortifying your defence strategy

Implement the necessary defences to secure your organisation's data and systems from attacks. Building strong protection mechanisms helps to reduce the likelihood of successful breaches. ramsac supports your protection efforts with services including:

- ramsac totalIT (also part of Identify)
- Vulnerability Management as a Service (VMaaS) (also part of Identify)
- Cybersecurity awareness and phishing training
- Board incident simulation training
- Board cybersecurity awareness training

ramsac totalIT

Our totalIT clients benefit from a fully managed OS (Operating System) patching service from ramsac covering workstations and servers. Using a combination of automated patch deployments and controlled OS patching for servers, we ensure that all devices in the organisation receive security patches and updates as soon as they are safe and ready to deploy. We also provide regular reports to ensure devices are patch compliant and encrypted.

Vulnerability Management as a Service (VMaaS)

ramsac's Vulnerability Management as a Service (VMaaS) is a proactive solution designed to help organisations manage software vulnerabilities and reduce the risk of cyberattacks. VMaaS begins with deploying advanced monitoring tools to continuously scan workstations and servers for potential weaknesses. It automates patching for third-party software, significantly reducing the workload on internal IT teams.

The service includes a baselining activity to address existing vulnerabilities and ongoing real-time monitoring to keep systems secure. Monthly reports provide clear visibility into vulnerability reduction efforts and expert recommendations for further improvements. VMaaS ensures organisations stay ahead of evolving threats while improving overall cybersecurity posture.

Cybersecurity awareness and phishing training

ramsac's cybersecurity awareness training delivers 10-minute engaging videos monthly to employees' inboxes, featuring content like interactive modules, games, and the award-winning series Inside Man. Tailored campaigns focus on problem areas, and ramsac offers a management service to track and report progress.

Phish Threat training from ramsac simulates phishing attacks with realistic emails from brands like LinkedIn and Microsoft. Reports track which employees fall for the attacks, offering targeted guidance and ongoing education. Regular reports identify vulnerabilities in your team, helping improve your "human firewall" and reduce risks.

Board incident simulation training

When a cyber breach hits, it is important the whole organisation knows how to respond and what to do to minimise the damage. During a cyber incident, the Board carries significantly more responsibility than other employees, needing to consider such things as PR, controlling brand damage, involving insurers or specialist cyber forensics firms, and how to keep services running for customers. In this training product, ramsac will run through a number of scenarios for an organisation's Board to test how they would follow their Incident Response Plan and identify areas for improvement.

Board cybersecurity awareness training

This 3-hour workshop is designed for board members, partners, and senior leaders to understand their responsibilities in safeguarding their organisation from cybercrime. Through discussion and planning, attendees will leave with a clear action plan for protection and guidance on how to respond to a cyber breach.

The workshop equips leaders with the knowledge needed in today's connected business world, where remote working and agile operations increase the risk of cyberattacks. Attendees will learn to:

- Understand the impact of cybercrime
- Recognise current scams
- Prepare for cybersecurity risks
- Address GDPR implications.

ramsac
the secure choice

Detect: Staying ahead with proactive threat detection

Detect threats early by continuously monitoring for suspicious activity in your network. Timely detection can drastically limit the damage caused by cyber incidents. ramsac's detection services include:

- ramsac secure+ (also part of Respond)

ramsac secure+

Secure+ offers advanced 24/7 cybersecurity monitoring, protecting businesses with real-time threat detection and rapid incident response. Its comprehensive service ensures that cyber threats are identified and addressed instantly, safeguarding your IT environment.

secure+
from ramsac

Continuous Monitoring and Incident Response

Secure+ provides round-the-clock surveillance tailored to your business needs. Key elements include:

- **Continuous monitoring:** Ongoing surveillance of your IT infrastructure to detect malicious activity and unusual behavior.
- **Rapid response:** Immediate response to any security incidents to minimise damage.
- **Tailored Monitoring:** Customisable security monitoring to fit your organisation's unique needs
- **Patch management:** Priority patching for critical vulnerabilities.
- **Quarterly audits:** Auditing of privileged user accounts to manage potential risks.

Proactive Security Management

secure+ also offers ongoing maintenance to enhance protection:

- Critical/priority patch management
- Regular security audits
- Monthly reports summarising security events and improvements

secure+ is the **watchful eye** over your IT estate

Detect

Respond

Respond: Incident response for minimising impact

Develop and execute a well-defined incident response plan to manage and mitigate the effects of a breach. A quick, effective response reduces both the impact and duration of a cyber attack. ramsac helps you prepare to respond with:

- ramsac secure+ (also part of Detect)
- Incident Response Plan (IRP) writing (also part of Recover)

Incident response plan (IRP) writing

A cyber breach can happen at any time, and how you respond in those crucial first moments can make all the difference. We help organisations develop clear, actionable plans to detect, contain, and recover from incidents, reducing impact and disruption.

Our process ensures your team knows exactly what to do, including how to communicate with key stakeholders and meet regulatory requirements. With a well-prepared response plan, you can act quickly and confidently when it matters most.

Respond

Recover

Recover: Ensuring business continuity and rapid recovery

Plan for recovery to ensure your organisation can bounce back quickly from any security incident. Fast recovery minimises downtime and helps to maintain business continuity. ramsac provides support for recovery through:

- Incident Response Plan (IRP) writing (also part of Respond)
- Business Continuity Plan (BCP) writing
- Disaster Recovery (DR) plan writing

Business continuity plan (BCP) writing

Should an IT system be made unavailable, for example during a cyber attack or service outage, it is important that members of the organisation know how they should continue to work and provide services to customers. The Business Continuity Plan outlines how employees should respond and what the responsibilities are of the Board or Senior Leadership Team. ramsac can assist organisations with ensuring that an appropriate BCP is in place, and then help simulate a scenario to test that the plan is sufficient.

Disaster recovery (DR) plan writing

In the event of a prolonged or sustained outage of an organisation's IT equipment, it may become necessary to invoke the organisation's Disaster Recovery plan. This plan details what long terms processes or replacement systems would need to be put in place, how to communicate with internal teams and customers, and who needs to be involved. ramsac can assist organisations with ensuring that an appropriate DR plan is in place, and then help simulate a DR scenario to test that the plan is sufficient

About ramsac

ramsac has a clear mission
- to be the secure choice

ramsac provide so much more than just IT support. We help our clients to get the best out of technology – implementing, managing and supporting secure, resilient, flexible IT solutions. We work with small and mid-sized organisations, providing them with strategic IT input, proactive management, jargon-free IT support and solutions that help them to grow their own organisations efficiently and securely. Our exclusive Cyber Resilience Certification programme helps organisation achieve the highest level of cybersecurity protection and allows them to demonstrate their commitment to their own stakeholders via our Gold certification standard.

Whether it's designing a new infrastructure, migrating services to the cloud, implementing enhanced security practices or providing end users with really efficient and friendly 24 hour IT support, ramsac manages IT on your behalf, so that you can focus on achieving your organisation's goals, safe in the knowledge that IT is secure, staff are working efficiently, and the IT investment is delivering tangible benefits to the business.

More information

For more information on **cybersecurity services from ramsac** please contact us on **01483 412040**, **email info@ramsac.com** or visit **ramsac.com**

ramsac
the secure choice

ramsac Limited

www.ramsac.com
01483 412 040

ramsac
the secure choice