Cybersecurity from ramsac

Protecting your business, people and reputation

ramsac
the secure choice

Your Technology. Our Responsibility.

Cybersecurity from ramsac

Cybersecurity is no longer a single product or project. It's an ongoing cycle of governance, prevention, detection, response and recovery. At ramsac, we align our cybersecurity services to the six core elements of the NIST Cybersecurity Framework (CSF) 2.0, helping organisations protect themselves at every stage, from setting strategy, to responding to incidents and recovering quickly.

Our approach is flexible. You may need full lifecycle coverage, or support in a specific area. Either way, our services are designed to meet you where you are today and support you as your organisation matures.

The six core elements of cybersecurity

Govern · Identify · Protect · Detect · Respond · Recover

These core elements work together to strengthen cyber resilience, reduce risk, and help organisations to operate with confidence. Each stage of the lifecycle represents a different aspect of cyber resilience. Some services sit firmly within one stage, while others support multiple areas. Many services are included within our totalIT packages, while others are available as standalone solutions. We can help you prioritise the areas that will deliver the greatest risk reduction and business value for your organisation.

<table>
<tr><th></th><th>Govern</th><th>Identify</th><th>Protect</th><th>Detect</th><th>Respond</th><th>Recover</th></tr>
<tr><td>Included in:
totalIT essentials
totalIT secure
totalIT premium</td><td></td><td>Compliance checks
ramsac Cyber Resilience Certification (CRC)</td><td>OS &amp; Firmware Patching</td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">Included in:
totalIT secure
totalIT premium</td><td></td><td colspan="2">ramsac VMaaS (Vulnerability Management as a Service)</td><td colspan="2">Managed Endpoint Detection &amp; Response (MDR)</td><td></td></tr>
<tr><td></td><td></td><td>Cybersecurity awareness &amp; phishing training</td><td colspan="2">Security Information and Event Management (SIEM)</td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2">Identity Threat Detection &amp; Response (ITDR)</td><td></td></tr>
<tr><td>Included in:
totalIT premium</td><td>Information security policy review
ISO27001 Gap analysis</td><td>Cyber Essentials basic gap analysis</td><td>Board cybersecurity awareness training</td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">Standalone solutions</td><td>Information security policy writing</td><td>Cyber Essentials Plus</td><td>Board incident simulation training</td><td></td><td></td><td>Business Continuity Plan (BCP) writing</td></tr>
<tr><td>Board cyber strategy assistance</td><td>Penetration testing</td><td></td><td></td><td></td><td>Disaster Recover (DR) plan writing</td></tr>
<tr><td colspan="2">ISO27001 consultancy</td><td></td><td></td><td colspan="2">Incident Response Plan (IRP) writing</td></tr>
</table>

ramsac
the secure choice

Govern - Establishing strong cyber governance

Strong cybersecurity starts with clear ownership, accountability and direction. Governance ensures that cyber risk is understood at leadership level, supported by appropriate policies, and aligned with regulatory and business requirements.

How ramsac helps

Information security policy review – Review of existing security policies to ensure they are current, relevant, and aligned to your organisation's risk profile and regulatory requirements.

Information security policy writing – Development of clear, practical security policies from scratch, tailored to how your organisation operates and providing meaningful guidance to staff.

Board cyber strategy assistance – Strategic workshops and advisory support to help senior leaders understand cyber risk, set priorities and make informed decisions.

ISO27001 gap analysis – A structured review of your current policies, processes and controls against ISO27001 requirements, highlighting gaps and prioritised actions.

ISO27001 consultancy – Ongoing expert support to help you address identified gaps, implement improvements and prepare for certification or audit.

Implementing governance

Organisations often begin with governance support to establish clear ownership and direction before expanding into wider cybersecurity improvements.

Solution	totalIT essentials	totalIT secure	totalIT premium	Standalone
Information security policy review			✓	
Information security policy writing				✓
Board cyber strategy assistance				✓
ISO27001 gap analysis			✓	
ISO27001 consultancy				✓

Identify - Understanding risks and vulnerabilities

You can't protect what you don't understand. The Identify stage focuses on gaining visibility of your IT estate, understanding where risks exist, and identifying vulnerabilities before they are exploited.

How ramsac helps

Compliance checks – We regularly check your devices for compliance with device encryption and anti-virus policies.

ramsac Cyber Resilience Certification (CRC) – A structured, tiered certification that assesses and strengthens your cyber defences against recognised best practice.

Vulnerability Management as a Service (VMaaS) – Identification and prioritisation of software vulnerabilities across your IT estate, providing visibility of risk and supporting informed remediation decisions.

Cyber Essentials and Cyber Essentials Plus – Support through government acked certifications to protect against common cyber threats and build customer confidence.

ISO27001 consultancy – Ongoing expert support to help you address identified gaps, implement improvements and prepare for certification or audit.

Penetration testing – Controlled, real-world attack simulations to uncover technical weaknesses before attackers do.

Identifying risks and vulnerabilities

Organisations typically use Identify services in different ways depending on the totalIT package selected.

Solution	totalIT essentials	totalIT secure	totalIT premium	Standalone
Compliance checks	✓	✓	✓	
ramsac Cyber Resilience Certification	✓	✓	✓	
Vulnerability Management as a Service (VMaaS)		✓	✓	
Cyber Essentials & Cyber Essentials Plus			✓*	✓
ISO27001 consultancy			✓*	✓
Penetration testing				✓

*Gap analysis only with totalIT premium

Protect - Fortifying your defence strategy

Protect focuses on putting practical safeguards in place to reduce exposure to cyber threats. This includes keeping systems up to date, addressing vulnerabilities, and ensuring people understand their role in keeping the organisation secure.

How ramsac helps

OS and firmware patching – Ongoing management of operating system and firmware updates to reduce exposure to known vulnerabilities.

Vulnerability Management as a Service (VMaaS) – Continuous scanning, prioritisation and remediation of software vulnerabilities across your IT estate.

Cybersecurity awareness and phishing training – Regular, engaging training and simulations to help employees recognise threats and reduce human risk.

Board cybersecurity awareness training – Focused sessions to help senior leaders understand their responsibilities and the real-world impact of cyber incidents.

Board incident simulation training – Scenario-based exercises that test decision-making, communication and response during a cyber incident.

Implementing protective controls

Solution	totalIT essentials	totalIT secure	totalIT premium	Standalone
OS and firmware patching	✓	✓	✓	
Vulnerability Management as a Service (VMaaS)		✓	✓	
Cybersecurity awareness and phishing training		✓	✓	
Board cybersecurity awareness training			✓	
Board incident simulation training				✓

ramsac
the secure choice

Detect & Respond - Detecting threats early and stopping attacks fast

In today's threat landscape, detection without response is not enough. Detecting and responding to cyber threats are inseparable activities that must work together to limit damage and disruption. Detect focuses on identifying suspicious activity as early as possible, while Respond is about taking swift, decisive action to contain threats and protect the organisation. At ramsac, this capability is delivered through our Security Operations Centre (SOC), where continuous monitoring and expert-led response enable threats to be identified early and rapidly contained before they escalate.

How ramsac helps

Managed Detection & Response (MDR) – Constant monitoring of endpoints and servers to identify malicious activity, investigate suspicious behaviour and automatically isolate or neutralise threats such as malware and ransomware.

Identity Threat Detection & Response (ITDR) – Dedicated protection for Microsoft 365 identities, detecting unusual logins, risky behaviour and unauthorised access, with rapid response to prevent account takeover.

Security Information & Event Management (SIEM) – Centralised collection and correlation of security logs across your IT estate to uncover hidden risks, identify patterns of attack and support rapid investigation and response.

Incident Response Plan (IRP) writing – While managed detection and response focuses on live incidents, preparation is equally important. IRP supports the Respond stage by defining roles, decision-making and communications during an incident.

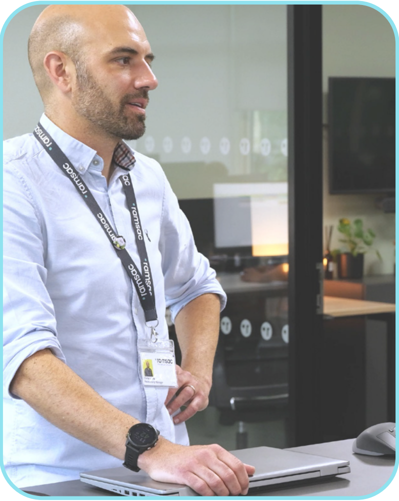
Delivering detection and response

Solution	totalIT essentials	totalIT secure	totalIT premium	Standalone
Managed Detection & Response (MDR)		✓	✓	
Identity Threat Detection & Response (ITDR)		✓	✓	
Security information & Event Management (SIEM)		✓	✓	
Incident Response Plan (IRP) writing				✓

Recover - Returning to normal operations quickly

Recovery ensures your organisation can continue operating and restore services following a cyber incident. Clear plans reduce downtime, protect reputation, and support long-term resilience.

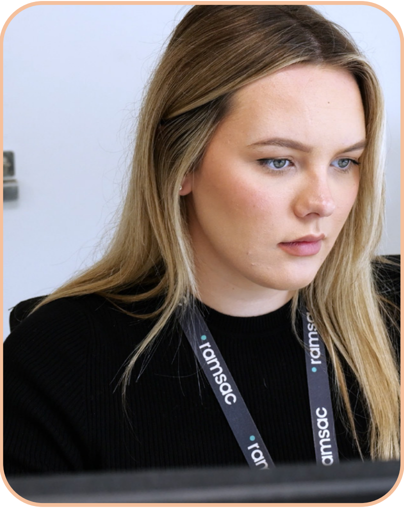
How ramsac helps



Business Continuity Plan (BCP) writing – Documentation of how your organisation continues operating during disruption, including roles, priorities and workarounds.

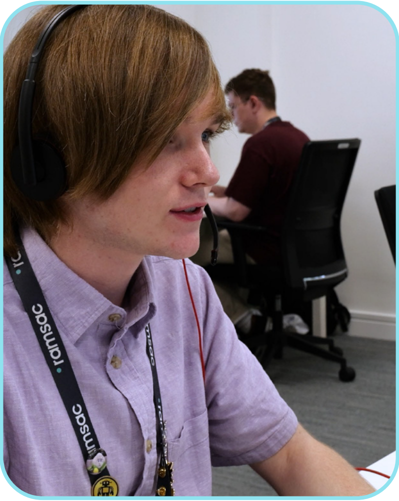
Disaster Recovery (DR) plan writing – Planning for restoration of systems and services following major IT outages or cyber incidents.

Incident Response Plan (IRP) writing – Defined processes for managing incidents that support both response and recovery activities.



Planning for recovery

Recovery services are delivered as standalone engagements, supporting organisations that need to plan for disruption, meet regulatory requirements or strengthen operational resilience. Business continuity, disaster recovery and incident response planning are typically delivered on a project basis and are often supported by simulations and testing exercises to validate effectiveness.



totalIT cybersecurity coverage

Our totalIT packages provide integrated cybersecurity support aligned to the six-stage lifecycle:

- **totalIT essentials**

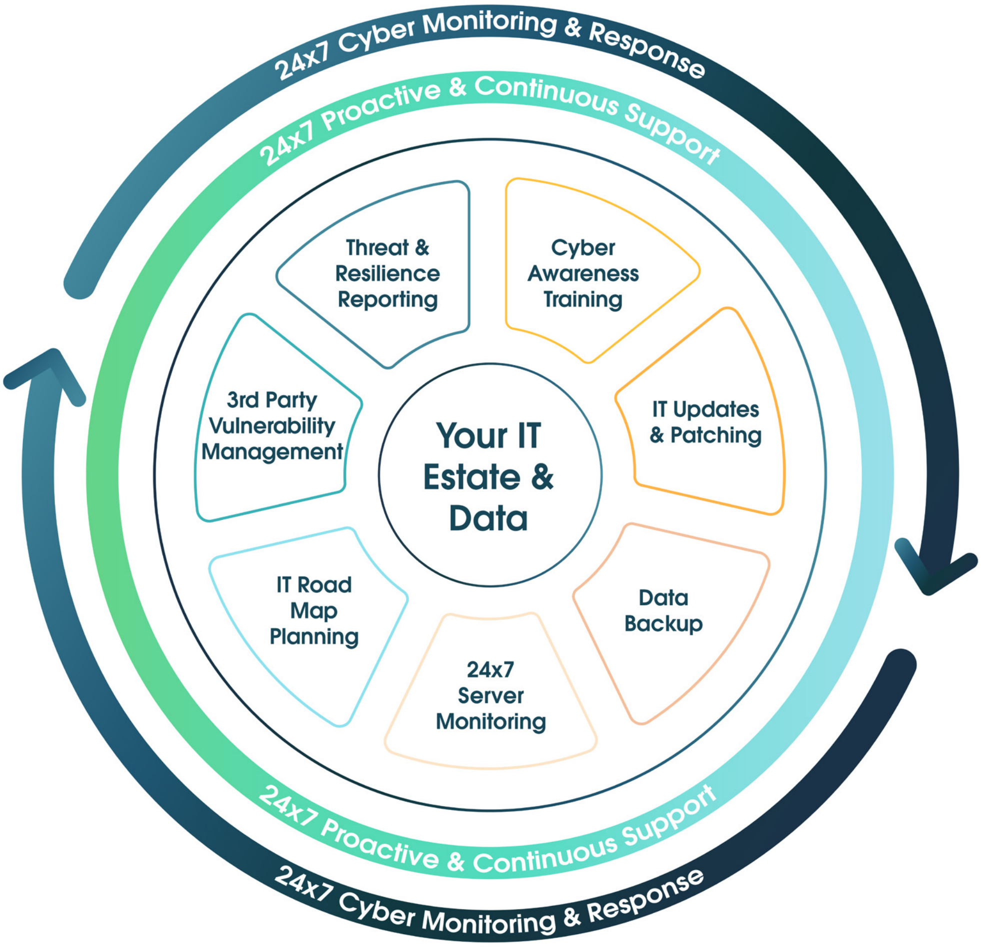
Designed to give organisations a clear view of their current security posture, **totalIT essentials** focuses on visibility, baseline controls and compliance readiness. It helps identify risks, demonstrate good practice, and establish a solid foundation on which stronger cybersecurity can be built.

- **totalIT secure**

Building on **totalIT essentials**, **totalIT secure** introduces enhanced protective controls and proactive risk reduction. This package is suited to organisations looking to reduce the likelihood of successful attacks through improved patching, vulnerability management, user awareness and strengthened technical defences.

- **totalIT premium**

totalIT premium provides comprehensive coverage across the full cybersecurity lifecycle, from governance and risk identification through to detection, response and recovery. It is designed for organisations with higher risk profiles, regulatory requirements, or a need for board-level assurance and resilience planning.


24x7 Cyber Monitoring & Response
24x7 Proactive & Continuous Support
Threat & Resilience Reporting
Cyber Awareness Training
3rd Party Vulnerability Management
Your IT Estate & Data
IT Updates & Patching
IT Road Map Planning
Data Backup
24x7 Server Monitoring
24x7 Proactive & Continuous Support
24x7 Cyber Monitoring & Response

About ramsac

Since 1992, ramsac has been helping organisations thrive with secure, reliable technology.

We are proud to be different. We are a people-first business, committed to making IT simple, jargon-free and friendly. We are independent consultants, offering advice based on your needs, not on sales targets. And we are focused on long-term relationships, with many clients trusting us for over 20 years.

Our commitment to quality is backed by ISO 9001, ISO 27001 and Cyber Essentials Plus certifications, and we are proud winners of multiple national and regional business awards. Most importantly, we have been recognised as a Best Companies 3 Star World Class Employer, proof that our team love what they do, and that passion shows in the service we deliver.

Your Technology. Our Responsibility

ramsac's mission is to be the secure choice. We help organisations get the best out of technology by delivering secure, resilient and flexible IT solutions.

Speak to us about your organisation's cybersecurity.
Call **01483 412040**, **email** **info@ramsac.com** or visit **www.ramsac.com**

ramsac
the secure choice