

The ramsac Data Security Framework

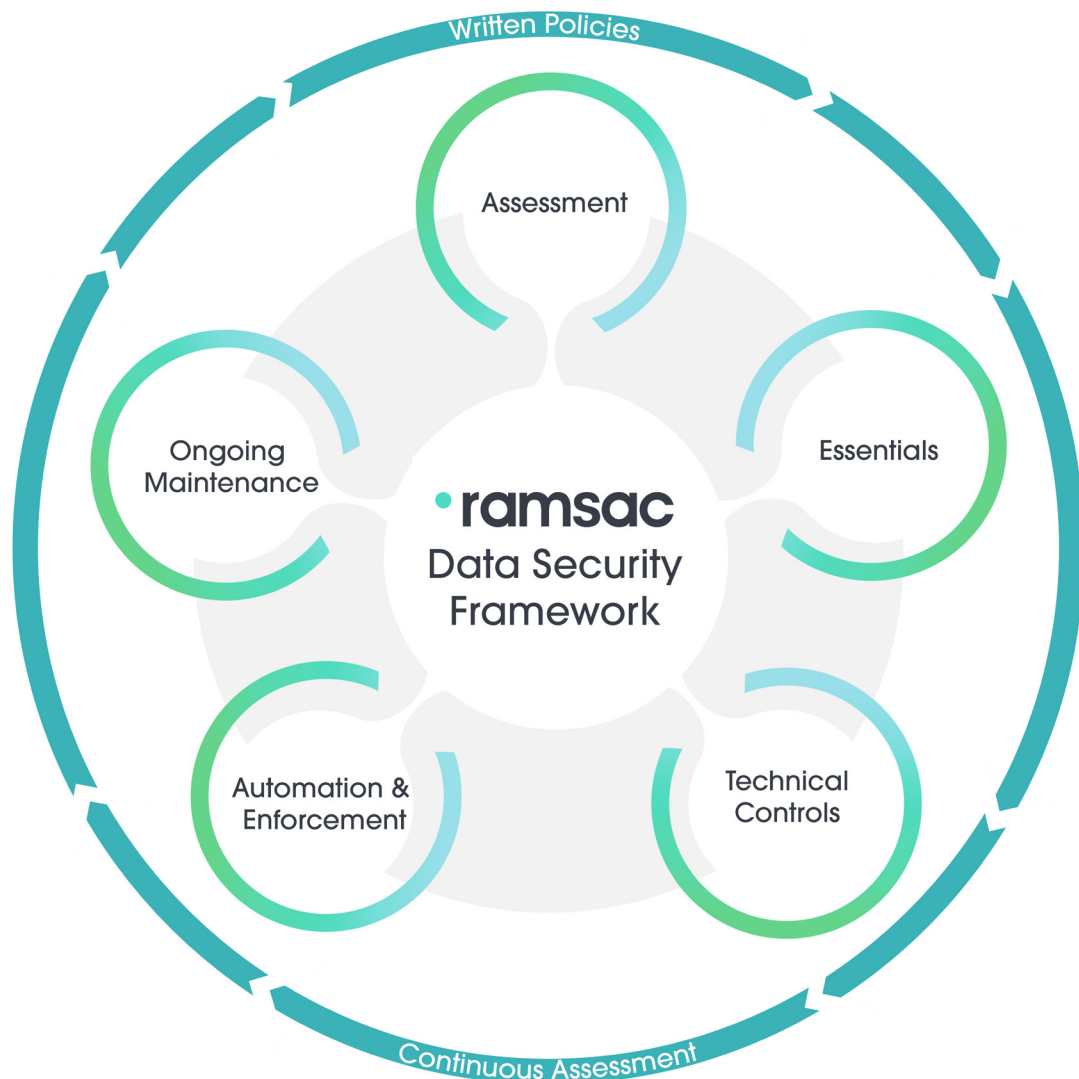
Protecting the information that matters most

Your journey to secure & compliant Microsoft data

Data is at the heart of every organisation. It fuels productivity, drives collaboration, and enables innovation. But without the right governance, it can also create risk. Overshared files, poorly managed permissions, or forgotten legacy data can all lead to reputational damage, compliance breaches, or lost opportunities.

At ramsac, we believe data management doesn't have to be daunting, that's why we have developed a comprehensive **Data Security Framework**: a strategic model designed to help organisations understand, protect, and manage their information assets more effectively. It's not a fixed roadmap or a rigid checklist. Instead, it's a flexible framework you can adopt and apply based on your unique needs and maturity level. Whether you're starting with a basic data audit or ready to implement advanced controls, this framework empowers you to make confident, risk-aware decisions about how your data is handled, stored, and shared.

The framework consists of five interdependent stages that address every aspect of data governance and security, all underpinned by Written Policies and Continuous Assessment, which ensure consistent, documented best practice at every step.



How the Data Security Framework supports compliance

The ramsac Data Security Framework gives organisations a clear, scalable route to achieving and maintaining compliance with evolving data protection and cybersecurity standards. Aligned with frameworks such as ISO 27001 and GDPR, it embeds best practice across five key stages **Assessment**, **Essentials**, **Technical Controls**, **Automation & Enforcement**, and **Ongoing Maintenance**, all underpinned by clear **Written Policies** that ensure consistent, documented governance at every step.

Standard	Compliance focus	Data Security Framework
ISO 27001	Focuses on ISMS controls including asset classification, access control, policies, and continual improvement	♦ Assessment: Identifies risks and sensitive data ♦ Technical Controls, Automation & Enforcement: Enforces controls like DLP and access restrictions ♦ Ongoing Maintenance: Provides alerts, reports, and audit trails ♦ Written Policies: Sets formal handling and retention policies
UK GDPR	Requires data minimisation, integrity, confidentiality, and accountability.	♦ Technical Controls, Automation & Enforcement: Security controls and audit logs ♦ Ongoing Maintenance: Ongoing oversight and evidence of accountability ♦ Written Policies: Policy-driven classification, retention and access
NCSC 10 Steps to Cybersecurity	Covers risk management, user awareness, secure devices, and incident response.	♦ Assessment: Data mapping and risk identification ♦ Ongoing Maintenance: Alerts and incident visibility ♦ Written Policies: User guidance and policy clarity
NHS DSP Toolkit & PCI-DSS	Requires structured governance, access control, and incident logging.	♦ Technical Controls, Automation & Enforcement: Secure access, classification, sharing restrictions ♦ Ongoing Maintenance: Audit trails, breach detection
M365 Copilot Readiness	Safe deployment of AI tools, protection of sensitive content.	♦ Technical Controls & Automation & Enforcement: Access restrictions and automation to prevent data exposure ♦ Written Policies: Data labelling and structure

Assessment: “Know what you’ve got.”

Assessment

Every journey begins with clarity. In this stage, we help you understand the full picture of your Microsoft 365 data, where it’s stored, who can access it, and what risks may exist. We’ll identify sensitive information, highlight areas of oversharing, and uncover compliance gaps. From here, you’ll receive practical recommendations to start improving your security posture straight away.

Benefits of Assessment:

- Clear visibility of your data landscape.
- Confidence that risks are being identified.
- A roadmap for compliance with GDPR, ISO, and other standards



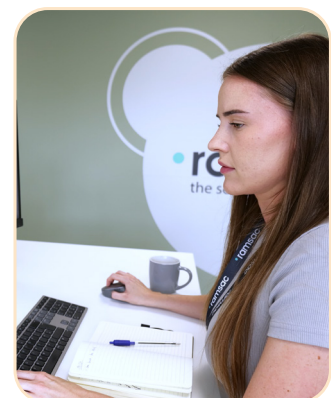
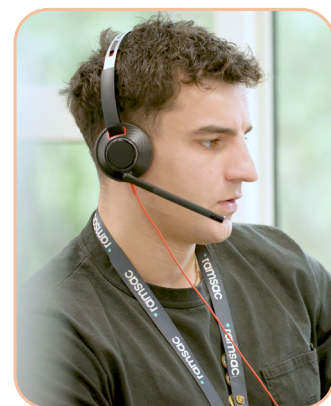
Essentials: “Get the basics right”

Essentials

Once risks are known, we focus on the quick wins and essential fixes. This may include tidying up SharePoint structures, adjusting permissions, setting safer defaults for sharing, or archiving outdated data. These changes often deliver immediate impact, reducing the chance of accidental oversharing and making it easier for staff to collaborate securely.

Benefits of Essentials:

- Immediate improvement to security and compliance.
- A simpler, tidier environment for your users.
- Reduced exposure in the event of a breach.



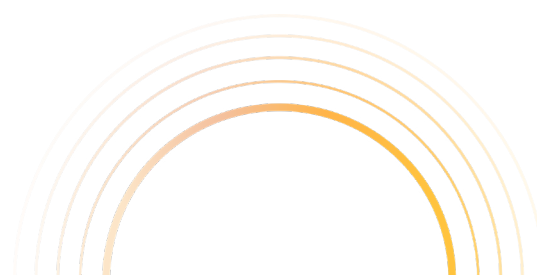
Technical Controls: “Protect and prevent”

Technical Controls

With the essentials in place, we strengthen your defences by deploying Microsoft’s built-in tools. This could include applying sensitivity labels in SharePoint and Exchange, enabling data loss prevention (DLP) policies, or creating structured rules for external collaboration. These technical controls help prevent mistakes before they happen, giving peace of mind to leadership and users alike.

Benefits of Technical Controls:

- Prevents accidental or malicious oversharing.
- Builds confidence in the secure use of Microsoft 365.
- Supports regulatory compliance with minimal disruption.



Automation & Enforcement: “Make it effortless”

Automation & Enforcement

The most effective governance happens in the background. At this stage, we introduce automation and advanced Microsoft features to reduce reliance on manual processes. From auto-labelling documents with sensitive data, to applying stricter DLP rules that stop unauthorised sharing, these tools create consistent protection without slowing your people down.

Benefits of Automation & Enforcement:

- Less reliance on user behaviour to “do the right thing.”
- Smarter use of Microsoft licensing and advanced features.
- Stronger data security, with less effort from your team.

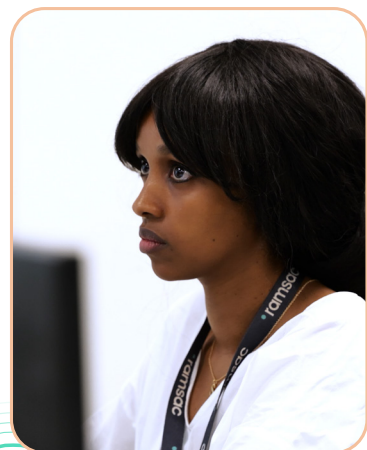
Ongoing Maintenance: “Stay secure, stay compliant”

Ongoing Maintenance

Data management isn’t a one-off project; it’s an ongoing commitment. We provide regular reviews, audits, and maintenance to ensure your environment continues to align with the controls you’ve put in place. Through policy reviews, proactive monitoring, and detailed reporting, we help you keep control of your data and prevent issues before they arise.

Benefits of Ongoing Maintenance:

- Long-term confidence in your data governance.
- Early detection and resolution of emerging risks.
- Continuous assurance that your systems remain compliant.



The foundations of Data Governance

Every part of the ramsac Data Security Framework is supported by two key foundations, **Written Policies** and **Continuous Assessment**. These work hand in hand to make sure your data management is clear, consistent, and always improving.

Written Policies

Written policies define how data is classified, handled, stored, and shared, creating a consistent framework that aligns with your governance standards. They provide the blueprint for technical settings and automated controls, ensuring people and technology operate by the same principles. Clear documentation promotes accountability and efficiency, helping your organisation demonstrate compliance and maintain business continuity.

Continuous Assessment

Governance isn't static. As your organisation grows and regulations shift, policies and systems must evolve too. Continuous assessment ensures that your framework remains aligned with how your business actually operates and the risks it faces. By working with your ramsac team, you can identify the right technical controls to support new challenges, stay compliant with changing requirements, and maintain best practice by adopting the latest Microsoft 365 features.

Together, written policies and continuous assessment create a living framework, one that captures how you work today and adapts seamlessly to how you'll work tomorrow.

Microsoft 365 Copilot Readiness



It's worth noting that by following these stages, as well as better clarity and security of data, your organisation will also be in an excellent position to take advantage of emerging technologies within Microsoft 365. One key example is Copilot, Microsoft's AI-powered productivity tool. A well-governed, clearly labelled, and securely managed data environment ensures that tools like Copilot can work safely and effectively from day one. If your data is messy, poorly structured, or accessible to the wrong people, AI tools will only amplify those problems. But when you've implemented the ramsac Data Security Framework, you create a strong, structured foundation for future innovation.

Microsoft 365 Copilot is an AI assistant embedded in Microsoft 365 applications like Word, Excel, Teams and Outlook. It can draft emails, summarise meetings, analyse documents, generate reports, and answer questions based on your organisational data. However, Copilot relies entirely on the information available to it. Without proper controls in place, it may surface outdated, irrelevant, or even confidential data to the wrong users. That's why preparing your data environment with strong governance and access management is not just good practice, it's essential for safe and effective AI adoption.

ramsac Data Security Framework - Compliance ready

The stages of the Data Security Framework are vital for modern data protection. Clean data, clear permissions, and well-applied policies give you the confidence to manage your information securely and effectively.

Most importantly, our approach doesn't require you to be perfect on day one. Whether you're starting from scratch or fine-tuning a mature data estate, the Data Security Framework gives you a structured, human-first way to reduce risk, build trust, and stay in control.



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.



● Ready to take control of your data?

Let's talk about how the **ramsac Data Security Framework** can help you stay secure, compliant, and in control of your data.

Book a free consultation to take the first step towards IT peace of mind.

Call **01483 412040**, email **info@ramsac.com** or visit **www.ramsac.com**