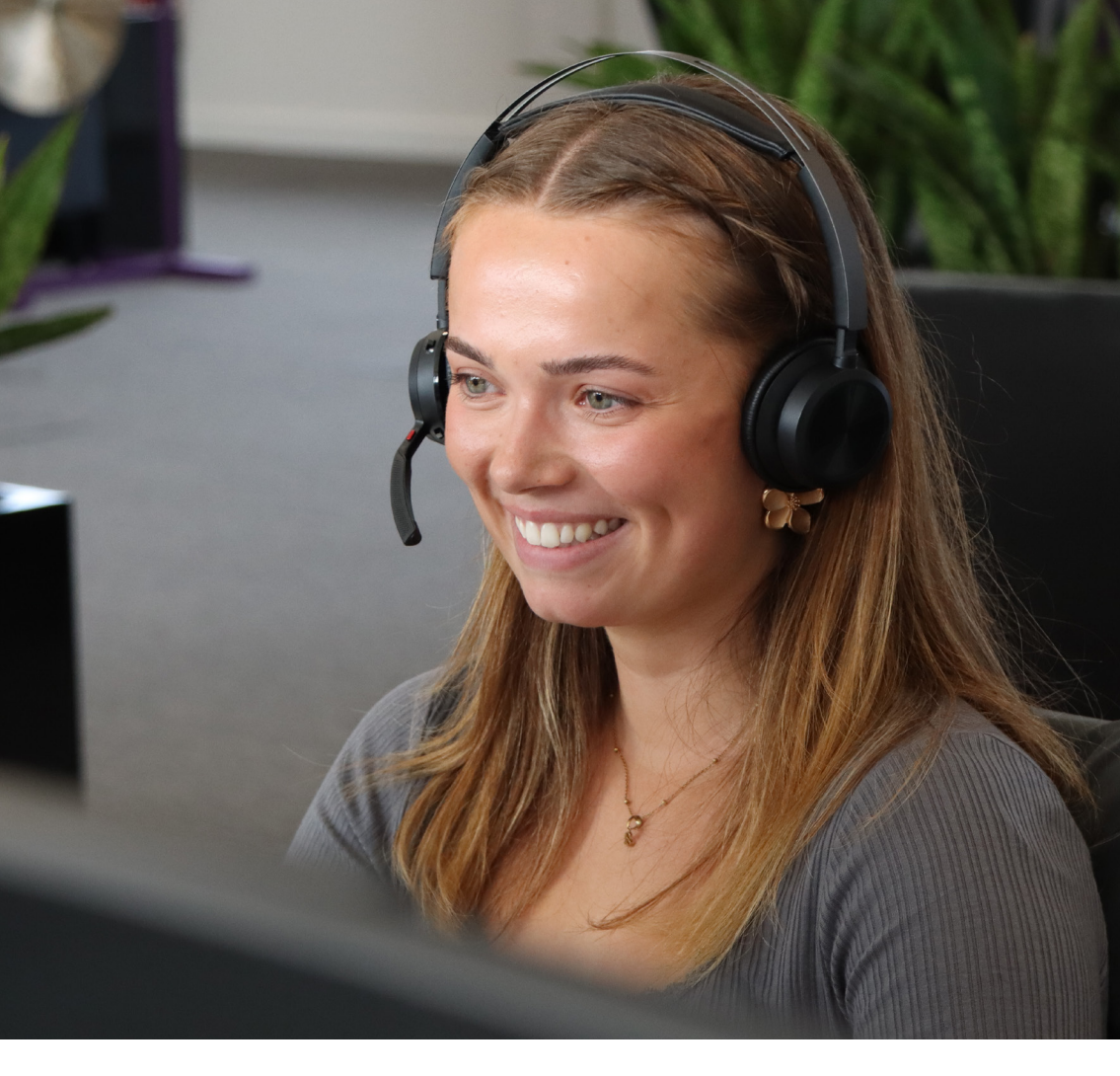
CAPABILITY OVERVIEW

Softcat

CYBER SECURITY
IN CENTRAL GOVERNMENT



In central government, you are expected to safeguard sensitive national information, critical infrastructure, and government operations from cyber threats, all whilst providing a good user experience.

Given the value of central government organisations and the responsibility that comes with the service user dependency, it's essential for security functionality to support business-as-usual experiences and compliance with NIS & Gov Assure CAF.

SECURE YOUR DATA

Securing your data is vital to protect sensitive information, which is required to maintain public trust.

You also need to ensure the integrity of your operations, safeguard national interests and comply with legal frameworks, which ultimately uphold the stability of your functions.

Secure systems and the data stored, transmitted, or processed for employees, service users, and third parties taking into consideration varied levels of sensitivity.

- Within central government, access is one of the core principles of risk management, particularly given different levels of authority clearance and clearance based on data of varied sensitivity.
- Softcat is here to assist you in finding the best solution for managing access to data based on your specific requirements. Our team can guide you through the process and provide low-level details on the most suitable solutions from a technical standpoint.

Initiating product collaboration conversation with the integration of products in a SOC for deeper threat intelligence, enhancing commercial effectiveness too.

- To enhance commercial effectiveness, we recommend leveraging existing investments in contracts that introduce integrated technical capabilities. This minimises administrative overhead and encourages efficient threat intelligence sharing.
- Our specialists can advise on integration-friendly solutions, API connectivity, optimal threat intel collection, and effective reporting. We can also leverage our visibility into security contracts to provide proactive guidance.
- Additionally, our Commercial Security Assessment yields an average of 25% cost savings, as our analysts review your data and provide consolidation recommendations.

Bring security practices into development cycles as early as possible and adopt security-as-code best practices.

- Integrating security practices early in development is crucial for a strong foundation. In central government, your security must underpin IT, addressing risks at all levels, including third-party integrations and the cloud.
- The development lifecycle should align with vulnerability management and secure-by-design principles. There are three core ways in which code is developed for modern applications: open-source, co-sourced and custom.
- Thinking about how the code is packaged and deployed in production environments is also essential. Regularly scanning CI/CD pipelines and Infrastructure as Code (IaC) is crucial for vulnerability management and your cloud runtime must be protected like your on-premise architecture.

SECURE YOUR NETWORK

Having a robust network security infrastructure helps prevent unauthorised access, data breaches, and cyber threats, ensuring the integrity and reliability of government operations and services.

Securing diverse devices across central government organisations, providing visibility and management for end-user devices, IoT, and OT to meet specific goals.

- Legacy systems in central government often feature complex and outdated infrastructure, segmented by clearance level or department. Streamlining and centralising management can enhance workforce efficiency and drive progress.
- Our specialists can advise on centralising visibility in your technology portfolio, optimising network technologies, and enhancing security capabilities for a centralised SOC approach, supporting areas such as IT/OT and IoT.

Use of both policy and network controls to support user access and rules, giving you the structure to be flexible with your workforce and your IT perimeter.

- Effective policies and controls are crucial for promptly managing and mitigating risks, fostering departmental success, and minimising the impact of changes.
- Network topologies are evolving for user-centric speed and agility, simplifying operations but still posing security challenges. Traditional segmentation alternatives are vital to keep pace with modern networks.
- Micro-segmentation offers granular, workload-level access, scaling with application needs, simplifying operations, and providing specific containment actions for incident responders.
- Access tools and micro-segmentation are essential technologies for enhancing network performance by isolating workloads and applications to reduce risk and vulnerability.
- Softcat supports a secure-by-design approach. Our security architecture resource provides an overview of vendor options, a detailed process, and insight into solutions tailored for the central government market and vendor landscape.

SECURE YOUR PEOPLE

Securing the information of employees and the public is crucial.

It's important for national security, maintaining public trust, and preventing unauthorised access to sensitive data that could compromise individuals' privacy and government operations.

Providing secure productivity and best user experience by ensuring technology isn't a barrier. Take a structured and secure data driven approach to enabling users.

- A productive digital workforce relies on a positive user experience, prioritising smooth workflows. Establishing essential data policies, structure, and security is crucial, enabling users to operate efficiently within set limitations and achieve objectives without causing IT delays.
- Softcat's security advisory specialist resource can help you understand risk management to foster a conducive culture. We recommend access controls such as Multi-Factor Authentication, Single Sign-On, Identity Management, and Governance tools, including passwordless capabilities. These streamline user access to relevant content for an enhanced experience.

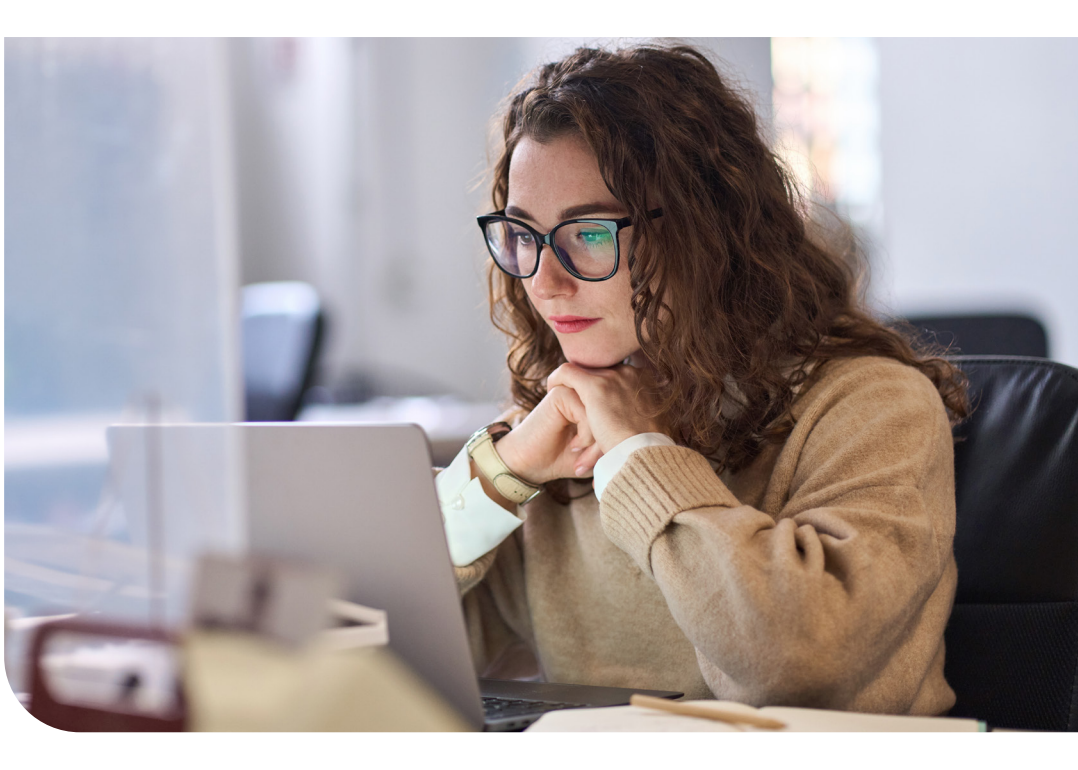
Secure communication and collaboration within your organisation and with relevant third parties.

- In central government, secure collaboration is vital due to varying content sensitivity. Validated secure communication paths are essential, requiring risk-managed collaboration. Prioritising a 'need-to-know' approach over convenience ensures asset value exceeds risks.
- Our network and security specialists can assist in comparing solutions such as email security, Multi-Factor Authentication, Privilege Access Management, secure portal platforms, and secure devices.
- Our Cyber Services can provide these resources to align with your policy. Our OCTO resource can advise on fostering a culture of secure communication and collaboration, considering both controls and policies.

SECURE YOUR PLATFORMS

Securing your platforms helps safeguard sensitive data and critical infrastructure, ensuring resilience against cyber threats and maintaining public trust.

The increasing integration of both on-premises and cloud-based systems necessitates robust security measures to prevent unauthorised access, data breaches, and potential disruptions.



Secure investments made into the cloud to ensure cyber policies are extended to protect those workloads as well as protecting traditional legacy systems.

- There has been a government push for a cloud-first strategy, prioritising continuity in on-premise and cyber policies. Ensuring consistency is challenging, but equal diligence is necessary, particularly when processes span on-premise and the cloud, so a standardised approach is crucial for managing both, irrespective of their differences.
- Our specialists can offer guidance on securing complex technologies, both on-premise and in the cloud. The team takes responsibility for advising on diverse solutions to support security needs.
- Our Cyber Services can assist in developing policies, while our consultancy resources align structures and foundations for internal discussions on both on-premise and cloud security, incorporating best practices for both environments.

Understanding the shared responsibility model between you and cloud providers for IaaS, PaaS, and SaaS, ensuring security accountability.

- Central government organisations must follow the NCSC website's shared responsibility model, which emphasises your ongoing responsibility for ensuring service security, secure configuration, and data management in chosen services.
- Softcat can provide expertise in managing relationships with cloud service providers (CSPs). We offer support in case of engagement challenges, facilitating communication.
- Our Cyber Services consultancy ensures clear documentation of your responsibilities and expectations.

COMPLIANCE & REGULATIONS

Regulations ensure standardised security measures, protecting sensitive information from cyber threats.

These rules promote accountability and coordinate efforts to safeguard national assets from evolving risks.

Taking a proactive approach to Cyber Security regulations mapped against NCSC's Cyber Assessment Framework and Government Cyber Security Strategy, 2022-2030.

- Central government organisations must ensure CAF compliance annually by 1st April for the upcoming financial year. Adhering to CAF improves security practices, aligns with NCSC recommendations, and fosters better communication with non-technical stakeholders.
- Softcat can provide expert guidance on the diverse tools and policies associated with GovAssure CAF. Our Public Sector specialists are dedicated to comprehending vertical-specific challenges and are adept at aligning with conversations related to GovAssure CAF.
- Additionally, our Cyber Services consultancy is available to conduct essential audits for GovAssure CAF.

Securing investments in both public and private cloud and extending cyber policies to both cloud-based workloads and traditional on-premise systems.

Securing investments and extending cyber policies across platforms is crucial to safeguard sensitive data, ensure uninterrupted access to educational resources, and maintain the integrity of digital learning environments against evolving cyber threats.

To do this, we recommend:

- **Protecting your cloud workloads, as you would on-premise** - implementing Cloud Workload Protection ensures monitoring and securing diverse cloud workloads.
- **Understanding your share responsibility model** - typically your CSPs manage cloud infrastructure security, you must secure your data, applications, and workloads. We can assist you in understanding these responsibilities better.
- **Protect your legacy systems** – ensure regular patching, vulnerability monitoring and updates for legacy systems. You can also employ intrusion detection systems to help mitigate the risk of exploitation.

  Protect IoT devices - utilise specialist tooling to protect IoT devices that are not protected by traditional endpoint security solutions or patch management.
- **Control and manage access to cloud services** - enhance the transparency of engagement by providing regulated control to approved, secure applications, reducing the risk of data in unregulated cloud services.
- **Prepare for disaster recovery** - implement monitoring, alerting, and observability solutions to track the security and performance of both cloud services and on-premises infrastructure. Real-time issue detection also enables more timely responses.
- **Aim for close alignment to NIS regulations for Operators of Essential Services** - though NCSC encourage close alignment to CAF, the NIS regulations for OES are good fundamentals to keep in mind.

Key Services we can offer:

Managed Security Services

- **Managed SIEM Service** – Reduces your cyber risk by monitoring and detecting security threats, enabling you to respond quickly without disrupting student services with guidance from our cyber analysts.
- **Managed Sentinel Service** – Helps you proactively defend yourself against threats and breaches by combining the threat protection, security intelligence and automation of the Sentinel security platform with expert monitoring and management by Softcat's Security Operation Centre.
- **Managed Firewall Service** - Provides continuous monitoring, updates, and expert technical support, reducing your cyber risks and protecting student and organisational data by applying security best practices and swiftly addressing security incidents while easing the burden on your security team.

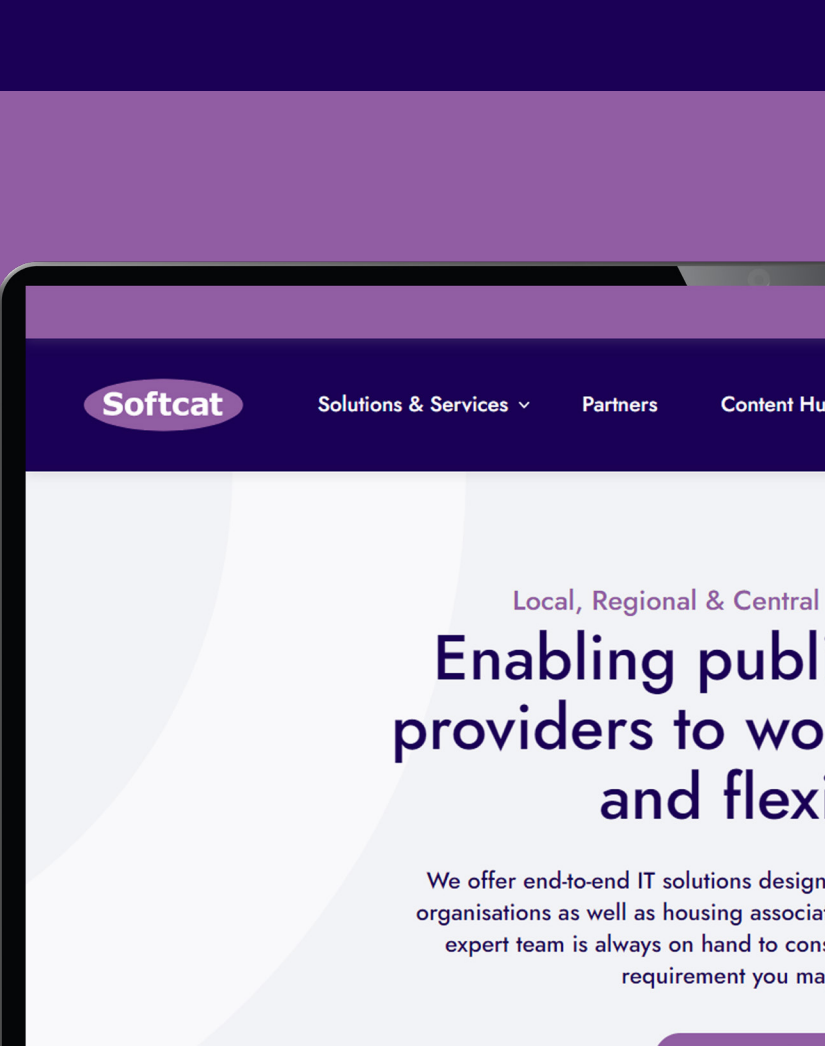
Cyber Security Baseline Assessments to better understand technology usage, consolidation, and opportunities to generate annual cost savings to Education institutions as well as help guide
Cyber Risk investment.

Cyber Security Regulatory and Compliance Services to help map outcomes against key strategic frameworks to perform a gap analysis such as Cyber Essentials/ Cyber Essentials Plus, ISO27001 etc.

FRAMEWORKS

We sit on the top frameworks for Central Government, including the following:

- **RM6098** CCS Technology Products & Associated Services 2
- **RM3764.3** CCS Cyber Security Services 3 (DPS)
- **RM1557.13** CCS G-Cloud 13
- **RM6100** CCS Technology Services 3
- **RM6259** CCS Vertical Application Solutions
- **Scots Gov** Cloud Hosting & Services



WHY SOFTCAT?

Our experienced team delivers tailored solutions, based on industry-leading technologies and best practices. We'll work closely with you to help you remain agile and prepared for changing cyber demands with independent advice and services

Expert team – our 80+ specialist security technology team is supported by chief technologists, solution architects and an extensive professional services team.

Putting you first – we're here to support you as your business needs evolve and change over time; from expansion to transitioning to the cloud, our services will adapt to suit you.

Industry best practice – we keep up to date with the threat landscape, sharing a view of industry best knowledge, recent cyber threats, and recommended patches.

Top tier vendors – by working with innovative, industry-leading vendors, we're able to deliver best of breed, not best of brand; we offer bespoke solutions that are right for you.

Holistic approach – by understanding each customer's unique needs, we're able to adopt a more holistic approach to business intelligence, powered by our transformation framework.

TAKE THE NEXT STEP

If you would like to find out more about how Softcat can support you on your cyber security journey, please contact your Softcat Account Manager today.

Softcat