Cyber Resilience Audit

Service description details

Cyber Resilience Audit

Methods' Audit Practice offers independent CRA assessments undertaken by a team of high-calibre SC/DV cleared UK IS/IT Auditors led by a Head of Service and nominated Lead Auditor qualified to Chartered status. The team have extensive experience of CNI delivering services at OFFICIAL, SECRET and ABOVE SECRET classifications.

What is the Service

Methods is an NCSC Assured Cyber Consultancy who has been assured to the highest standards as defined by NCSC and professional bodies such as UK Cyber Security Council. With a proven track record of delivering cyber security consultancy, audit and assurance, we pride ourselves on working closely with our clients. Work is undertaken by industry qualified Cyber security experts, many holding CCP Lead Practitioner and/or qualified to Chartered status, able to offer practical guidance and support to both public and private sector clients.

In line with HMG requirements, Method's Cyber Security and Data Service Portfolio are certified to Cyber Essentials Plus, ISO/IEC 27001, ISO 27017, and ISO 9001 standards, so we can provide customers with robust, consistent assurance in our quality processes and the protection of our systems and customer-related data. We adopt certified frameworks for HMG where data is classified OFFICIAL through to SECRET and above. Methods has a large pool of SC and DV cleared UK personnel and has experience of designing, building, and maintaining governance and security to deliver service offerings at OFFICIAL, SECRET and ABOVE SECRET classifications.

Methods is also a registered GovAssure Independent Assurance Reviewer (Supplier) - a risk based review based on NCSC Cyber Assessment Framework (CAF) for both baseline and enhanced profiles. In meeting the standard for undertaking GovAssure work, Methods are engaged with NCSC, Cabinet Office Government Security Group and Critical National Infrastructure (CNI) Regulators and well placed to support the upcoming Cyber Resilience Audit (CRA) scheme - provision of high quality independent and objective CAF based Cyber Audits intended to:

- improve UK CNI cyber resilience
- provide a single 'Core' scheme to support a diverse group of oversight bodies (e.g. cyber regulators), accepting that sector specific requirements to include audit approach and methodology may emerge as the scheme matures; and
- help inform a high-level view, based on CNI CAF Data, on the adequacy and effectiveness of security controls put in place by CNI operators of essential services to include the policies, procedures and processes supporting 'multi-sectors' both the public and private sectors.

Methods' Audit Practice (Cyber Security and Data Services) support the organisation by providing an objective evaluation to include the effectiveness of controls and countermeasures whilst measuring compliance against the latest security standards, frameworks as well as policies and applicable regulations.

Our Audit assessments, led by a Head of Service and nominated Principal Lead Auditor typically qualified to Chartered status and who acts as a point of focus and escalation, are designed to provide a comprehensive review and analysis of the organisation's IT security posture to include governance, processes and procedures. Methods has experience of conducting IS/IT Audit reviews against industry best practice to:

- Provide independent risk and compliance-based audit assessments based on NSCS CAF or similar frameworks;
- Support compliance with HMG security strategy and associated objectives;
- Integrate with NCSC National Cyber Security Strategy to enable a systematic and comprehensive approach to assess outcomes and to identify the extent to which cyber risks to essential services are being effectively managed by an organisation; and
- Provide an independent and objective view on the maturity of cyber security controls and countermeasures and/or compliance with relevant regulations, frameworks and standards such as NIS, NiST and ISO 27001.

What sets Methods apart is the breadth of services, technical capability, skills and wider experience covering (for example) Operational Technology (OT). We provide professional and measurable technical assessments that will enable the organisation to apply and maintain proportionate controls over information security systems and assets.

Methods has extensive experience of working with Central Government to include Department for Work and Pensions, Department for Transport, Home Office and Ministry of Defence to include CNI. Our IS/IT Audit service is designed to support the identification of security vulnerabilities across both public and private sector organisations with an independent audit assessment that:

- identifies risks, vulnerabilities and weak else ineffective controls
- allows the organisation to prioritise funding and resource to (for example) define, implement, maintain and test measures including controls intended to safeguard systems, data and people
- provides assurance that an organisation complies with required policies, standards and frameworks such as NCSC CAF

The scope of our audit assessments will be tailored to meet the specific needs of the business and/or regulatory requirement. We collaborate with and where appropriate report to key stakeholders through the full end to end audit cycle i.e. from early inception and audit planning phase to final report and follow-up – engagements are conducted using latest tooling and in line with professional auditing standards such as COBIT 5 which seamlessly map to specific applicable guidance from (for example) NCSCS, NIS or NiST. Our Audit team will deliver a service offering that:

- covers all systems to include infrastructure deemed in-scope (for example) CNI and those deemed essential in supporting the provision and continued operation of CNI systems e.g. enterprise resource planning systems
- provide practical recommendations to mitigate else address risks, security vulnerabilities else weak controls which might otherwise lead to compromise of systems, data and/or personnel
- assesses the requirement for else maintenance of certifications impacting compliance with (for example) statutory else legislative requirements

Contact details

bidteam@methods.co.uk

020 7240 1121

www.methods.co.uk

Service description details

- covers applicable cyber security policies and procedures
- covers cyber security and relevant artefacts for example architectural designs, blueprints, risk analysis and assessments
- covers Security operations to include incident response, business continuity and disaster recovery procedures
- covers governance to include organisational structures and reporting capabilities.

Our experienced high-calibre Auditors work flexibly, using latest tools, technologies and ways of working.

What it can do for you

Methods' IS/IT Audit Practice (Cyber Security and Data Services) will perform an independent and objective NSCS Cyber Resilience Audit (CRA) of CNI and supporting systems against NCSC Cyber Assessment Framework (CAF).

The CRA will help you to:

- provide an independent and objective assessment against NCSC Cyber Assessment Framework (CAF)
- identify risks, vulnerabilities and weak else ineffective controls
- prioritise funding and resource to (for example) define, implement, maintain and test measures including controls intended to safeguard systems, data and people
- provide assurance that you comply with required policies, standards and frameworks

In meeting the objectives of the CRA Scheme, you will help:

- improve UK CNI cyber resilience;
- inform a high-level view, based on CNI CAF Data, on the adequacy and effectiveness of security controls put in place by CNI operators of essential services to include the policies, procedures and processes supporting ‘multi-sectors’ both the public and private sectors.

Service Features

1. Independent and objective CRA assessment against NSCS CAF
2. Work undertaken by UK IS/IT Auditors vetted to SC/DV
3. CRA led by a Head of Service and Lead Auditors
4. Audit team meet/exceed all NCSC criteria
5. Audit team have extensive experience of CNI for Central Government
6. Audit team use latest tools, technologies and ways of working
7. Experienced team able to meet sector specific requirements including methodologies
8. Audit team able to align with the GovAssure Scheme
9. Breadth and Depth of Cyber Security and Data Services experts
10. IS/IT Audit Practice with experience across all sectors

Service Benefits

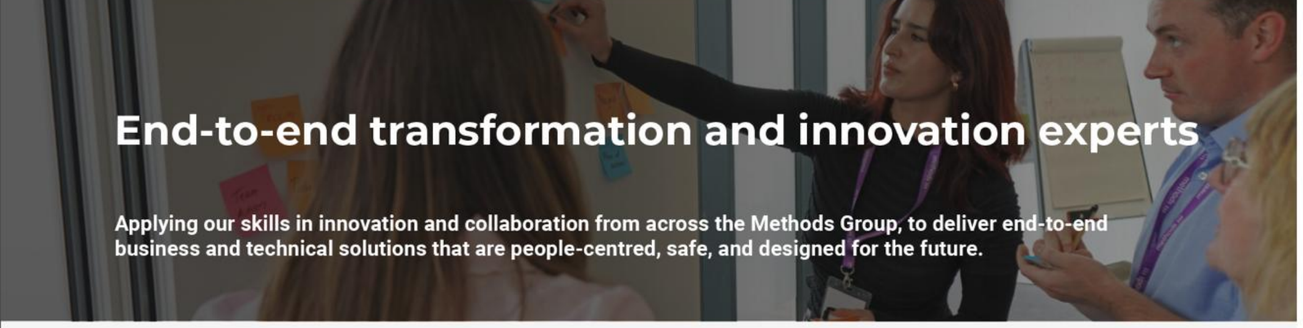
1. Cyber Resilience Audit against NCSC Cyber Assessment Framework
2. Practical recommendations to address risks, vulnerabilities and weak controls
3. Prioritise funding and resource, identify inefficiency and waste
4. Compliance with policies, standards and frameworks
5. Meet statutory and legal requirements
6. Independent and objective insight and assessment of security posture
7. Inform decision making, Business & System improvements
8. Help improve UK CNI Cyber Resilience
9. Provide a view on the adequacy of CNI CAF Data
10. Assess the controls provided by CNI Operators of Essential Services

Contact details

bidteam@methods.co.uk

020 7240 1121

www.methods.co.uk



End-to-end transformation and innovation experts

Applying our skills in innovation and collaboration from across the Methods Group, to deliver end-to-end business and technical solutions that are people-centred, safe, and designed for the future.

Methods provide collaborative and innovative solutions to help Central Government adapt to the changing landscape and deliver better outcomes for citizens.

With a focus on driving interoperability and innovation in UK Central Government, we have helped multiple organisations in the sector modernise their IT architecture, systems, strategy, and operating models to improve organisational resilience and service delivery.

Methods deliver wide-ranging services and thought leadership to support delivery including:

Onboarding and offboarding process

1. **Understand Requirements**

   It is essential that we work with you to understand the requirement so that we provide the right resources with directly relevant experience at an appropriate level of seniority

2. **Protect Team Availability**

   Having the right team on board from the start and maintaining continuity throughout the project ensures timely delivery of desired outputs

3. **Work Synergistically and Innovatively**

   Drawing from our past experiences, we can frequently recommend optimal delivery methods and/or alternative solutions which will deliver benefits (or cost-savings) over time

4. **Service Scope**

   Ensuring that the scope of the service to be delivered is properly quantified involves agreeing on logistics (e.g., deliverables, timelines, quality criteria, etc.) and understanding your constraints, sensitivities, and key drivers to match your expectations accurately

5. **Review/Agree Engagement**

   After initial discussions and planning, you'll review and amend a draft Statement of Work(s)/Services to ensure mutual agreement and alignment of objectives before starting the assignment. We may iterate the Statement of Work(s) with you to finalise the requirements

Ordering and Invoicing

Once we have agreed a Statement of Work(s) we will sign the appropriate agreement and complete a Call Off contract with an attached Statement of Work(s), and submission of a Purchase Order. We will then set up a mutually acceptable start date and commence work.

Payment terms are 30 days or less as may be agreed.

Please note - we are unable to accept Government Procurement Card (GPC) payments.

Customer Responsibilities

For any given requirement, we will identify any dependencies on the customer (e.g. access to key stakeholders, facilities, documentation, etc.) and agree these at the start of the work.

Making a difference

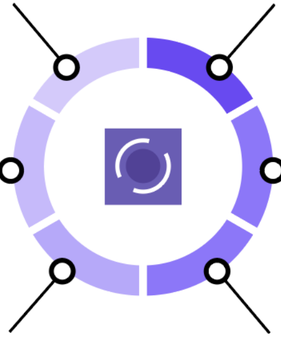
The work we do each day is focused on delivering a positive difference for the public sector for the benefit of society as a whole.

Environment

We use the 'recycle, reuse, repair, refuse' approach to waste reduction to minimise landfill waste, support climate initiatives, and enhance biodiversity, creating a sustainable environment for our colleagues and community

Volunteering

We continue to support charitable causes that align with and support our values including our charity partner and VCSE initiatives



Investment in Talent

We cultivate young talent through our GRAVITATE programme, championing vibrant apprenticeship and graduate schemes while aiding tech career exploration for individuals aged 14-24

Diversifying our Supply Chains

We diversify our local supply chains, promoting small business enterprise and engaging local people, SME, and micro-business suppliers

Staff Wellbeing

We support colleague wellbeing through clear career pathways, strengthened PDPs, and our continued commitment to the Armed Forces Covenant, including achieving Gold Employer Status. Moreover, we continue to support our colleagues holistically, considering them as complete individuals at every career stage with Methods

Safeguarding Services

We continue to provide insightful thought leadership on leveraging modern technology to secure our public services for future generations. This involves speaking at industry events, educating youth on tech career paths, and offering pro-bono advice to senior policymakers

Customer stories

Cloud Hosting & Service Modernisation
Modernised digital services using secure cloud hosting, streamlined legacy workflows, and improved data insights. Delivered faster decisions, reduced manual effort, and a more transparent, **user-friendly experience** for internal teams and external users.

Cloud-Based ITSM Consolidation
Unified multiple service desks onto a cloud-based ITSM platform, standardising processes and automating workflows. Improved incident, change, and problem management, **boosting** overall **service reliability, efficiency, and organisational visibility**.

Large-Scale Cloud Migration (100+ Apps / 120TB)
Delivered cloud migration of **100+ legacy applications** and **120TB of** data with **100% availability**. Strengthened compliance, improved transparency, and significantly enhanced operational resilience across critical digital services.

Azure Migration & Modern Workplace Enablement
Migrated data centres to Azure and deployed modern workplace cloud services, delivering secure, scalable infrastructure. Achieved improved user experience, strengthened security posture, and **£1m savings** - all with zero service disruption.

Cloud ITSM Migration (ServiceNow SaaS)
Successfully migrated from a legacy ITSM tool to a modern, cloud-based ServiceNow platform. Delivered scalable, robust service operations, strengthened governance, and enabled faster, more consistent digital service delivery across the organisation.

Cloud-Native Data Pipelines (Azure Integration)
Built automated Azure Data Factory pipelines into a Lakehouse architecture, using Bronze/Silver/Gold layers and Delta with CI/CD. Delivered secure daily refreshes, improved data quality, lower manual effort, and more efficient reporting.