Cyber Security Assessment

G-Cloud 15 Service Definition

1. Summary

Cyber Security Assessment provides organisations with a 360-degree review of its people, technology, processes, and procedures. This review will ensure you are working towards industry standards and embed cyber security methodologies, such as “Defence in Depth”, “Least Privilege Principle”, and “Protect, Detect, Respond and Recover” within the culture of the organisation at all levels.

CSA is a perfect offering to any organisation who would like to get a full understanding of their current cybersecurity posture, regardless of their current status.

1.1 Benefits

The service helps you to evaluate, analyse and improve your security posture, on a one-off or ongoing basis, according to your needs.

All work is carried out by our in-house cyber security experts -– who are experienced, trained and certified.

With cyber security at the top of the risk agenda for members, this is a cost-effective preventative exercise which highlights areas of weakness and provides tangible recommendations for action, because it’s a tailored service, we can scope the work to your exact requirements.

We help members to understand cyber risk and develop metrics which reflect the organisation’s security posture and can be used to direct and evaluate the effectiveness of cyber mitigation investments.

Effective cybersecurity is more than simply finding and remediating vulnerabilities. It is more about developing a security-first mindset and embedding this within the organisational culture.

The IT technical and security teams responsible for delivering cyber security for their organisations, cannot do this effectively without the support and sponsorship of their executive leadership teams. The CSA report executive summary and follow-up presentation, aims to present the organisation's cybersecurity posture in risk terms which are understood by senior leaders and provide a roadmap for improvement.

As a trusted partner to member organisations, Jisc can draw on insights and best practices from across the UK education sector. The CSA provides a holistic review of an organisation's resources/internal stakeholders, technology and processes. It will assist in developing organisational cultures where security by design and by default can become embedded.

1.2 Features

Evaluate your readiness against real-world attacks

As part of the service, we assess how vulnerable you are to cyber-attacks. The evaluation has two elements:

- A vulnerability assessment analyses your network for known issues giving consistent, repeatable data on security vulnerabilities and information on weaknesses. The assessment takes the form of a series of tailored tests for misconfigurations, security patches and cryptographic flaws – which we also confirm by manual analysis.
- A configuration analysis audits the security controls you already have in place – against, for example, known best practices or standards.

Analyse the cyber security risks you face

Armed with data from your vulnerability assessment and configuration analysis, we prioritise security issues according to risk – allowing you to focus your efforts on areas critical to you.

This risk analysis helps you understand the potential impacts to your organisation – and the range of approaches you could take to remain resistant to cyber-attacks.

Take steps to harden your security

Using information from these assessments and analysis, we propose ways to secure your network – such as configuration improvements, processes and security controls – to help you make informed decisions on what to do next.

We can also let you know about areas of residual business risk that you may wish to mitigate, including legal or insurance issues.

Improve your posture on a regular basis

Because this is a repeatable process, we can conduct regular assessments – for example, on an annual basis – helping you show how your security improves progressively against a baseline. Regular assessment will also catch any new flaws in security, for example from new services or lapsed testing.

2. Service Definition

2.1 Core Service Offering

All work is carried out by our in-house cyber security experts – who are experienced, trained and certified. You are under increasing pressure to demonstrate the effectiveness of your cyber security. Partners and funding bodies, for example, may want to see cybersecurity assessment reports – while internally, you are keen to do all you can to mitigate risks. That's why Jisc offers the Cyber Security Assessment service: a tailored, cost-effective process to help you meet audit

and compliance needs. The service helps you to evaluate, analyse and improve your security posture, on a one-off or on-going basis, according to your needs.

2.1.1 Vulnerability assessment analyses your network for known issues – giving consistent, repeatable data on security holes and information on weaknesses. The assessment takes the form of a series of tailored tests for misconfigurations, security patches and cryptographic flaws – which we also confirm by manual analysis.

2.1.2 Configuration analysis audits the security controls you already have in place – against, for example, known best practices or standards.

The Cyber Security Assessment service covers:

- Security posture assessment and reporting, including Executive summary
- Support and advice for Cyber Essentials for those that are required to gain a certificate
- Account management
- Asset management
- Access control
- Patch management and vulnerability assessment
- Anti-virus
- Firewalls and network configuration
- Event management
- Mobile device management
- Back up and disaster recovery
- Training and awareness
- Information security and incident response
- Active Directory and Microsoft 365
- Endpoint protection
- Incorporates NIS (Network & Information Systems), CIS Controls (Center for Internet Security) and Cyber Assessment Framework

3. Service Level Description

At Jisc, our Cyber Security Assessment service is designed to provide organisations with robust cybersecurity solutions tailored to their unique needs. Our service level description outlines the key components and commitments associated with our service offerings:

Initial Consultation

- Response Time: Within 2 business days of initial enquiry.
- Assessment Duration: Variable, depending on the complexity of the organisation's cybersecurity requirements.
- Deliverables: Once the Cyber Security Assessment been completed, a fully comprehensive report will be delivered to the Customer. A post assessment call can then take place to discuss the findings.

Guidance and Preparation

- Response Time: Ongoing support provided throughout the assessment process.
- Preparation Duration: Variable, depending on the organisation's readiness and level of compliance with cybersecurity standards. Advice and Guidance meetings, pre-submission checks and email support offered.
- Deliverables: Guidance documentation, templates, and implementation support to facilitate compliance with assessment requirements.

Bespoke Solutions

- Response Time: Tailored solutions provided based on client requirements and feedback.
- Implementation Duration: Variable, depending on the scope and complexity of customised solutions.
- Deliverables: Customised cybersecurity solutions addressing specific organisational needs, challenges, and compliance requirements.

Trusted Partnership:

- Response Time: Ongoing support and communication provided throughout the engagement.
- Duration: Continuous partnership maintained to address evolving cybersecurity threats and requirements.
- Deliverables: Dedicated Relationship Manager/Security Specialist, regular updates, and proactive recommendations to enhance cybersecurity posture and resilience.

We are committed to delivering a high-quality Cyber Security Assessment service that will empower organisations to strengthen their cybersecurity posture and assist in mitigating potential risk. Our service level description reflects our dedication to responsiveness, expertise, and partnership in helping customers navigate the complex cybersecurity landscape with confidence.

3.1 Customer Responsibilities

Active Participation	Customers are expected to actively participate in initial consultations, assessments, and ongoing communications throughout the penetration testing engagement.
Resource Allocation	Customers must allocate necessary resources, including personnel and time to support the assessment effort effectively.
Feedback and Collaboration	Customers are encouraged to provide feedback, insights, and collaboration to improve the effectiveness and efficiency of our assessment services and support ongoing cybersecurity initiatives.

3.2 Support

We are committed to providing comprehensive support throughout the Cyber Security Assessment process. Our dedicated team of cybersecurity professionals are available to assist customers at every step, ensuring a smooth and successful assessment journey. Support includes:

Advice and Guidance
Our experts offer personalised advice and guidance to help customers understand assessment requirements, assess their cybersecurity readiness, and develop an effective strategy for achieving a robust cybersecurity posture.

Documentation Recommendations
We assist customers in obtaining the necessary documentation, including policies, procedures, and evidence of compliance, to streamline the assessment process and ensure alignment with cybersecurity best practices.

Technical Assistance
Our team provides technical assistance to help customers implement and configure security controls, address vulnerabilities, and optimise their cybersecurity infrastructure to meet assessment requirements.

Response and Communication
We maintain open lines of communication with customers, promptly addressing enquiries, providing updates on assessment progress, and ensuring alignment with customer timelines and expectations.

Issue Resolution
In the event of any challenges or issues encountered during the assessment process, our team works diligently to identify solutions, mitigate risks, and facilitate timely resolution to minimise disruption and ensure progress towards a robust cybersecurity posture.

Training and Education
We offer training and educational resources to empower customers with the knowledge and skills necessary to maintain cybersecurity best practices, address emerging threats, and sustain compliance with cybersecurity standards beyond the assessment.

Continuous Improvement
Our commitment to continuous improvement drives us to seek feedback from customers, evaluate our processes and services, and implement enhancements to deliver an exceptional assessment experience and support ongoing cybersecurity initiatives effectively.

At Jisc, our support extends beyond the assessment process to empower customers with the confidence, knowledge, and resources needed to strengthen their cybersecurity defences and navigate the evolving threat landscape with resilience.

4. Service Management

At Jisc, we prioritise effective service management to ensure the successful delivery of Cyber Security Assessments. Our service management approach encompasses various aspects, including:

Service Design and Planning

We meticulously design and plan our Cyber Security Assessment service to align with customer requirements, industry best practices, and cybersecurity standards. Our team evaluates customer needs, defines service offerings, and establishes clear objectives and deliverables.

Service Transition

During the service transition phase, we facilitate a seamless transition from the initial engagement to the assessment process. This involves coordinating with customers to gather necessary information, conduct assessments, and prepare for the Cyber Security Assessment, while ensuring minimal disruption to ongoing operations.

Service Operation

Our service operation phase focuses on the delivery of the assessment process efficiently and effectively. We leverage our expertise, resources, and technology infrastructure to guide customers through each stage of the assessment, monitor progress, and address any issues or concerns that may arise.

Incident and Problem Management

In the event of incidents or problems encountered during the assessment process, our incident and problem management processes come into play. We promptly identify, assess, and resolve issues to minimise impact and ensure the timely completion of assessment activities.

Change Management

Throughout the assessment process, we adhere to robust change management practices to manage changes to customer requirements, scope, or timelines effectively. We assess the impact of changes, obtain necessary approvals, and implement changes in a controlled and transparent manner.

Service Improvement

Continuous service improvement is integral to our approach. We regularly evaluate our service delivery processes, solicit feedback from customers, analyse performance metrics, and implement enhancements to optimise service quality, efficiency, and customer satisfaction.

Customer Relationship Management

At Jisc we thrive on building and maintaining strong customer relationships. We encourage, transparent and collaborative communication with customers, ensuring customers' needs are met and understood. Expectations are managed effectively.

Risk Management

We proactively identify, assess, and mitigate risks associated with the assessment process to safeguard customer interests and ensure the successful completion of the Cyber Security Assessment. Our risk management practices encompass risk identification, analysis, treatment, and monitoring throughout the service lifecycle.

With our robust service management practices in place, we are committed to delivering a Cyber Security Assessment service that meets the highest standards of quality, reliability, and customer satisfaction.

Our focus on service excellence enables us to empower organisations with the confidence, resilience, and assurance needed to navigate the complex cybersecurity landscape effectively.