Cyber **security**

CYBER ASSESSMENT SERVICES

THREAT READY





LRQA

Your Risk Management Advantage

CONTENTS

3 Introduction

4 Cybersecurity assessment process

5 Types of cybersecurity assessment

6 Our cybersecurity assessment methodology

7 NIST CSF maturity assessment

INTRODUCTION

LRQA's cybersecurity assessment services help you identify and understand the potential security weaknesses that leave your organisation at greater risk from threats such as data breaches and ransomware.

Based on industry-standard good practices and guidelines such as the NIST Cybersecurity Framework and NCSC 10 Steps to Cybersecurity, our review will help identify technical and procedural vulnerabilities, and provide you with clear recommendations to address any gaps and reduce your overall risk levels.

Our experienced consultants work alongside your teams to get a real-world view of your security posture, focusing on your actual working practices through a 'show and tell' approach that goes well beyond tick-box auditing.

Findings are presented in a clear and actionable format that will help you:

- Understand your current position and vulnerabilities in your environment.
- Get better visibility of your maturity via a snapshot view provided in an executive report.
- Gain a comprehensive understanding of areas for improvement via a detailed technical breakdown.
- Make strategic decisions and support the creation of an improvement plan.
- Identify tactical recommendations that help you to address any urgent issues and quickly reduce risk.



CYBERSECURITY ASSESSMENT PROCESS

A cybersecurity assessment can be delivered remotely or from your offices and can be tailored depending on your specific circumstances and objectives.



PROJECT INITIATION, SCOPE IDENTIFICATION, AND PLANNING

- Introduction to our team.
- Create an agenda for assessment.
- Identify key resources, systems, data, and assets.



CONDUCT ANALYSIS

- Review documented policies and diagrams.
- Conduct interviews with key personnel.
- Technical and process observations.



REPORTING

- Executive summary providing high-level findings and recommendations.
- Detailed findings with specific notes and actions.



DEBRIEF

- Consultant-led debrief session.
- Review findings and what they mean for your organisation.
- Discuss recommended next steps.

TYPES OF CYBERSECURITY ASSESSMENT

LRQA's cybersecurity assessment services can be tailored to suit organisations of all sizes, with differing concerns, priorities, and budgets.

NCSC 10 STEPS ASSESSMENT

- Aligned to the NCSC's 10 Steps to Cybersecurity.
- Typically takes three to five days to complete.
- Findings reported on a red-amber-green basis.
- Identifies good practices as well as medium and high-risk findings.
- Focuses on current implementations and working practices.
- Details of possible quick wins and recommendations for improvement.

NIST CYBERSECURITY MATURITY ASSESSMENT

- Based on the NIST Cybersecurity Framework (NIST CSF).
- Provides recommendations to develop your cybersecurity strategy and mature your capabilities to help manage and reduce risk.
- Analyses capability maturity across all six NIST CSF functions.
- Considers implementation (what you do) and policy (what you say you do) maturity.
- Identifies high-risk areas where prioritised attention is required.
- Feeds into the creation of an improvement plan and development of your cybersecurity strategy.

OUR CYBERSECURITY ASSESSMENT METHODOLOGY

Areas covered by our cybersecurity assessment services as standard are displayed in the table. Assessments can be tailored to meet specific requirements and expanded to include or focus on areas not listed opposite.

COMPARISON OF NCSC 10 STEPS AND NIST CSF MATURITY ANALYSIS

NCSC 10 steps cybersecurity assessment	NIST CSF maturity assessment	
• Risk management • Engagement and training • Asset management • Architecture and configuration • Vulnerability management • Identity and access management • Data security • Logging and monitoring • Incident management • Supply chain security	• Organisational context • Risk management strategy • Roles, responsibilities, and authorities • Policy • Oversight • Cybersecurity supply chain risk management • Asset management • Risk assessment • Improvement • Identity management, authentication, and access control • Awareness and training	• Data security • Platform security • Technology infrastructure resilience • Continuous monitoring • Adverse event analysis • Incident management • Incident analysis • Incident response reporting and communication • Incident mitigation • Incident recovery plan execution • Incident recovery communication

NIST CSF MATURITY ASSESSMENT

1. PROJECT INITIATION, SCOPE IDENTIFICATION, AND PLANNING

- Introduction to LRQA delivery team.
- Confirm priorities and scope for the analysis.
- NIST Cybersecurity Framework overview.
- Maturity level overview.
- Discuss your objectives and any specific areas of concern.
- Create a project plan and agendas.
- Identify relevant resources, systems, data, and assets.
- Define target maturity levels.

2. CONDUCT ANALYSIS

- Maturity review aligned to NIST CSF functions.

  Govern: Your organisation must have an effective cybersecurity risk management strategy. Cybersecurity expectations and policies should be established, communicated, and monitored.

  Identify: It is crucial to establish a baseline understanding of the assets you are trying to protect.

  Protect: Implementation of appropriate protective controls that protect your assets.

  Detect: Your ability to detect cybersecurity incidents plays a crucial role in minimising the potential impact on your organisation.

  Respond: The impact of cybersecurity incidents can be reduced by responding efficiently when they are detected. Timely responses can minimise the impact on operations, as well limiting financial and reputational damage.

  Recover: Your organisation must be able to promptly recover and restore to business as usual.

- Review of written policies.
- Interviews with key personnel.
- Technical and process observations.
- Review of evidence to understand the current position.

3. REPORTING

- An executive summary report that provides an overview of the analysis process, recommendations, and suggested next steps.
- The report identifies your current position against the NIST CSF using a maturity model.
- Detailed findings for each NIST CSF category provided.
- Detailed findings are provided along with notes from our consultant and can be used to track progress.
- Notable findings highlighted where high-priority tactical changes are recommended to reduce risk.

4. DEBRIEF

- Consultant-led debrief session and Q&A.
- Review the findings of the analysis, recognising good practice and areas for improvement.
- Understand the findings and what they mean for your organisation.
- Discuss recommended next steps.

ABOUT LRQA

LRQA is a leading global risk management partner.

Through our connected risk management solutions, we help you navigate an evolving global landscape to keep you one step ahead.

From certification and cybersecurity, to safety, sustainability and supply chain resilience, we work with you to identify risks across your business. We then create smart, scalable solutions, tailored to help you prepare, prevent and protect against risk.

Through relentless client focus, backed by decades of sector-specific expertise, data-driven insight and on-the-ground specialists across assurance, certification, inspection, advisory and training, we support over 61,000 organisations in more than 150 countries.

LRQA – Your risk management advantage.

GET IN TOUCH

Visit **LRQA.com** for more information or email **enquiries.uk@lrqa.com**

LRQA
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom

Care is taken to ensure that all information provided is accurate and up to date; however, LRQA accepts no responsibility for inaccuracies in or changes to information.

LRQA
Your Risk Management Advantage