

VCISO BY LRQA NETTITUDE

# Virtual Chief Information Security Officer (vCISO)

LRQA  
NETTITUDE





# Contents

- 3 What is a CISO?
- 3 Does Every Organisation Need a CISO?
- 4 What is a Virtual CISO?
- 5 How is Virtual CISO Support Delivered?
- 5 Onboarding Your Virtual CISO?
- 6 Conducting a Cybersecurity Review
- 7 Ongoing Virtual CISO Support
- 7 What is the LRQA Nettitude Virtual CISO Unique Value Proposition?

# What is a CISO?



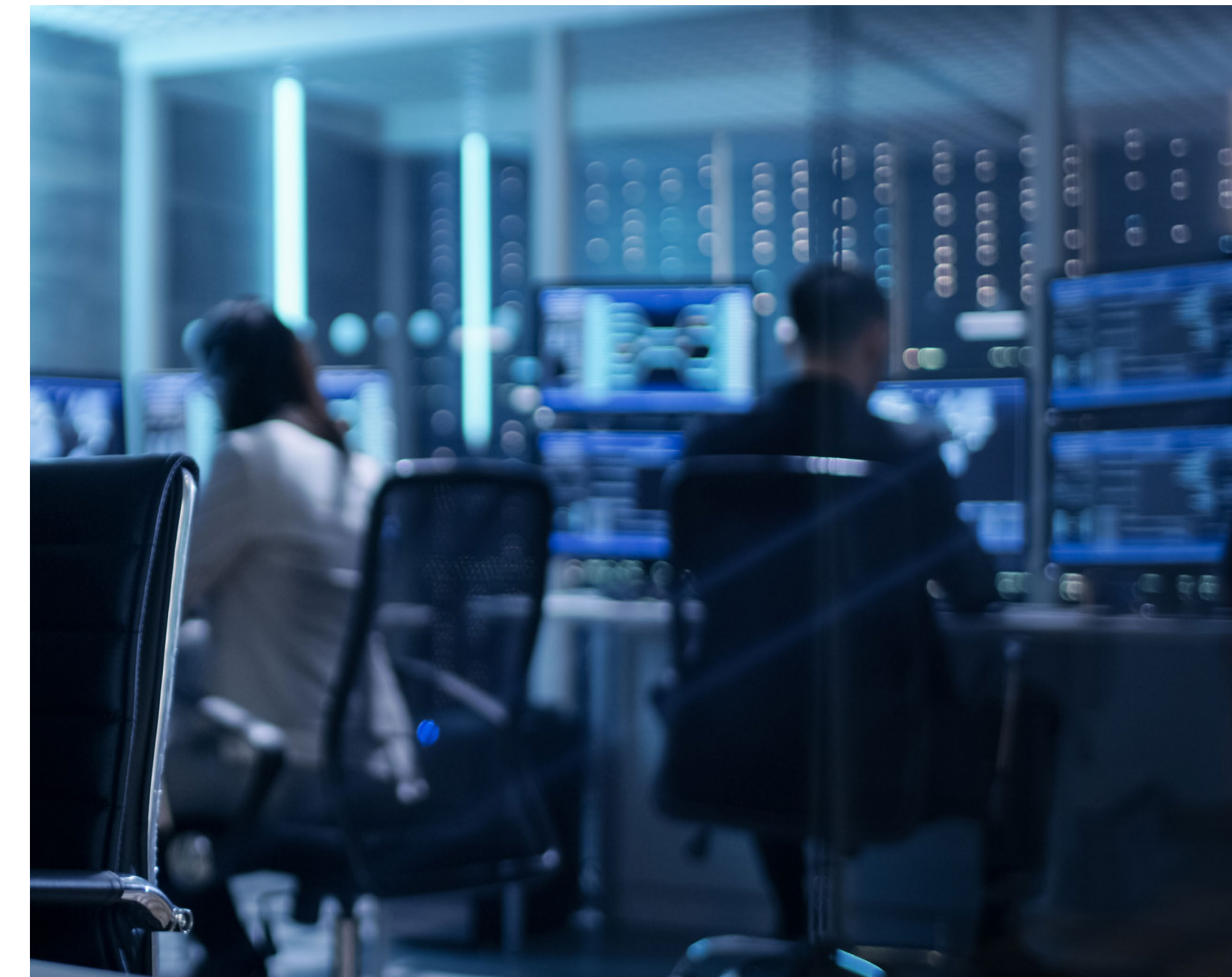
The role of a Chief Information Security Officer (CISO) is to align security initiatives with enterprise programs and business objectives, ensuring that information assets and technologies are adequately protected. CISOs working in smaller businesses may be relatively ‘hands-on’, whereas those in a large organisation will likely have a team of people to support their role.

## Does Every Organisation Need a CISO?

**Organisations of all sizes must have an individual that is ultimately responsible for information security.**

Commonly a security specialist rises through the ranks from a more technically focussed role, and a security function may form gradually over time as your business grows. It is also common for someone in another position, for example, an IT Manager, to assume responsibility for security, even if this is not an area of expertise.

Ultimately, you must have somebody in your organisation capable of and responsible for aligning information security strategy with your business objectives and protecting your organisation’s information assets.





# What is a Virtual CISO?



The skillset of a CISO is broad and recruiting experienced individuals to fill a CISO role can be a challenge.

**Talented, dedicated CISOs can also be difficult to retain, as they are highly sought individuals who often have a relatively short tenure with their role.**

Your CISO needs to possess a mixture of technical and business skills and be equally comfortable presenting your security strategy to the board as they are discussing technical controls with IT teams.

Many larger organisations employ a full-time CISO; however, this can be an expensive resource that many cannot justify. In fact, many organisations do not need a dedicated full-time CISO due to the size and nature of how they operate.

LRQA Nettitude's Virtual CISO (vCISO) service brings you the benefits of a full-time CISO without the costs associated with employing them.

- A blend of strong technical and business skills.
- Lower cost to engage, no recruitment costs or full-time salary and benefits.
- Ability to interface with technical teams, your board, and the wider business.
- Provides strategic guidance based on strong industry experience.
- Has access to other LRQA Nettitude specialist resources, such as incident response and technical assurance, and is supported by a team of information security consultants.
- Experience in a diverse range of industries, with a skill set that continues to evolve and stay current through their exposure to many multiple organisations.





# How is Virtual CISO Support Delivered?



LRQA Nettitude's vCISO Support Service comprises three phases:

1. Initial cybersecurity review and onboarding
2. Agree on prioritised actions for the next 12-24 months
3. Ongoing support in executing the agreed-upon plan

## Onboarding Your Virtual CISO

LRQA Nettitude will assign a lead senior Information Security Consultant, who will work alongside your team to provide CISO support with the support of our consultancy team. While not a formally appointed CISO, LRQA Nettitude will use a proactive delivery model that maintains a regular schedule.

This is distinctly different from a more reactive relationship in that a LRQA Nettitude will play an active role in identifying and responding to cybersecurity risks and supporting you in maturing your cybersecurity posture.

The onboarding phase provides LRQA Nettitude with situational awareness and understanding of your organisation and current cybersecurity posture.





# Conducting a Cybersecurity Review



LRQA Nettitude will conduct a comprehensive cybersecurity review to establish a baseline, covering the security domains are shown opposite.

Review Areas
<ul style="list-style-type: none"><li>• Information security policies</li><li>• The organisation of information security</li><li>• Human Resource security</li><li>• Asset management</li><li>• Access control</li><li>• Cryptography</li><li>• Confidential security documents</li><li>• Physical and environmental security</li><li>• Operations security</li><li>• Communications security</li><li>• System acquisition, development, and maintenance</li><li>• Supplier relationships</li><li>• Information security incident management</li><li>• Information security continuity</li><li>• Compliance</li></ul>

**This comprehensive review analyses the current state of the people, processes, and technologies your organisation uses to manage cybersecurity risks. The onboarding process provides LRQA Nettitude with a CISO level understanding of your current posture by:**

1. Conducting interviews with key stakeholders to gauge knowledge of documentation (policy, procedure, process) and to understand the current level of controls.
2. Completing a review of the environment, identifying potential risks and threats.
3. Understanding the current risk appetite and assessment and how it links to the business.

**We will conduct interviews and make observations across several key areas during the review. Below is an example of the stakeholders likely to be involved in the process:**

- Chief Information Security Manager/Officer
- Computer and Information Systems Manager
- Head of Risk and Compliance
- Technical Services Director
- HR Manager
- PR/Communications Manager
- Project Manager
- Operational teams

# Ongoing Virtual CISO Support



Based on the initial security review findings, we will work with you to agree and prioritise the next steps. These steps may be a combination of quick tactical wins, such as addressing high-risk technical gaps, and more strategic activities like developing or updating policies and processes.

## Typical Activities

- Participation in regular information security governance forums, for example, working groups, and helping to ensure information security requirements are considered as part of any new project.
- Review and implementation of information security management systems (ISMS).
- Providing advice and guidance on the implementation and use of a risk management framework and risk assessments.
- Implementing information security awareness training programs.
- Identifying and managing risks related to third parties and suppliers.
- Support the maintenance of compliance regimes, such as PCI DSS and ISO 27001.
- Review and creation of policies and standards.
- Coordinating technical assurance activities.
- Advising on specific technology changes.
- Responding to third-party audit requirements.

## What is the LRQA Nettitude Virtual CISO Unique Value Proposition?

**As a pure cybersecurity and risk management organisation, LRQA Nettitude can offer the option of becoming your 'Virtual' Chief Information Security Officer.**

Many organisations either cannot afford their own information security department or would instead invest in having a dedicated firm working with them to meet their needs. As the landscape for cyber breaches and malicious actors continues to increase, companies will need experienced professionals to mitigate these risks.

As an industry-leading consultancy, LRQA Nettitude is keen to assist businesses in achieving a goal of best security practices. LRQA Nettitude can provide consulting services as well as security testing and broader information assurance services.

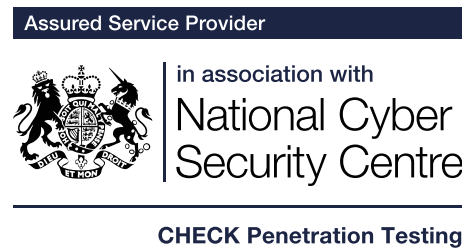
At LRQA Nettitude we are committed to delivering tailored solutions and services in an efficient, timely manner to help our clients understand the risks to their business.



QUALIFIED SECURITY ASSESSOR



APPROVED SCANNING VENDOR



CHECK Penetration Testing



### Get in touch

Visit [www.nettitude.com](http://www.nettitude.com) for more information or email enquiries to [solutions@nettitude.com](mailto:solutions@nettitude.com)



#### UK Head Office

1 Trinity Park  
Bickenhill Ln  
Birmingham  
B37 7ES

#### Americas

50 Broad Street  
Suite 403  
New York  
NY 10004

#### Asia Pacific

18 Cross Street  
#02-101  
Suite S2039  
Singapore 048423

#### Europe

Fidiou 9  
Athina  
106 78  
Greece

