CISO SERVICES BY LRQA

CISO Services

Contents

What is a CISO?

The role of a Chief Information Security Officer (CISO) is to align security initiatives with enterprise programmes 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.

Organisations of all sizes must have an expert that is responsible for establishing and maintaining an information security programme, ensuring that information assets and technologies are adequately protected against threats.

Commonly a security specialist rises through the ranks from a more technically focused 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.

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 CISO service offers the expertise of a full-time CISO without the associated employment costs. Our CISO services consultants, actively engaged across multiple industries, bring a wealth of insights from diverse organisational challenges. Unlike an in-house CISO limited by a single organisational exposure, our CISO services consultants act as force multipliers, constantly enhancing their knowledge and applying valuable experiences to benefit each one of our clients.

Benefits of using LRQA CISO services

As industry-leading cybersecurity experts, LRQA empowers clients to achieve a best-in-class security posture. With our CISO services, we're not just a vendor; we are an extension of your team, a true partner committed to safeguarding your organisation.

We can provide our CISO services as well as security testing and broader information assurance services.

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

Key benefits

- A strong blend of business and technical skills
- Cost-effective solution with no recruitment fees or full-time salary
- Ability to interface with technical and operational teams, the board and the wider business
- Provide strategic guidance based on strong industry experience
- Implementation of tactical requirements such as policies, and risk assessments
- Coach and mentor in-house teams
- Flexible service approach with the option to scale up and down on demand
- On hand to support BAU activities
- Experience in a diverse range of industries
- Has access to other LRQA specialist resources, such as incident response and technical assurance

ASSESS

- Identify risks
- Review critical technology
- Measure maturity
- Improvement planning

STRATEGIC SUPPORT

- Set direction and develop strategy
- Drive improvement
- Risk management
- Governance and oversight

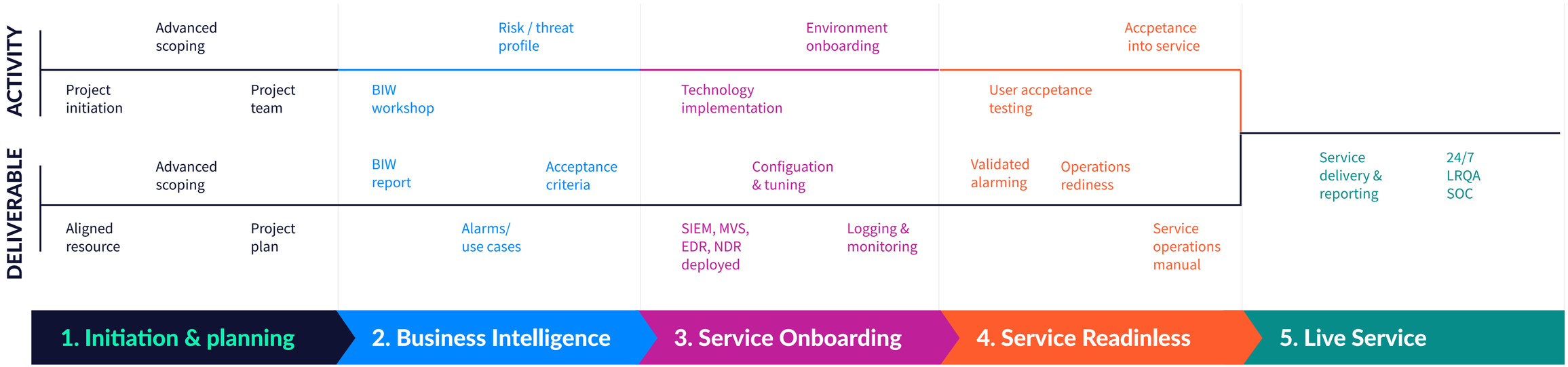
TACTICAL SUPPORT

- Augment your team
- Risk assessments
- Technology reviews
- Vendor and supply chain audits

REVIEWS & BRIEFINGS

- Industry updates
- Threat intelligence
- Management reviews
- CISO dashboard

How are CISO services delivered?



How are CISO services delivered?

Conducting a cybersecurity review

This comprehensive cybersecurity review analyses the current state of the people, processes, and technologies your organisation uses to manage cybersecurity risks. The onboarding process provides LRQA 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 cybersecurity review of the environment, identifying potential risks and threats.
3. Understanding the current risk appetite and assessment and how it links to the business.

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

Cybersecurity review areas

- Information security policies
- The organisation of information security
- Human Resource security
- Asset management
- Access control
- Cryptography
- Confidential security documents
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Information security continuity
- Compliance

We will conduct interviews and make observations across several key areas during the cybersecurity 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

How are CISO services delivered?

Onboarding your CISO

LRQA will assign you a dedicated consulatant from our experienced CISO services team, who will work alongside your team to provide the support your organisation needs. While not a formally appointed CISO, LRQA will use a proactive, tried and tested model that maintains a regular schedule.

This is distinctly different from a more reactive relationship in that our CISO services consultant 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 with situational awareness and understanding of your organisation and current cybersecurity posture.

Ongoing CISO support

Based on the initial cybersecurity review findings, we will work with you to agree and prioritise the next steps.

As industry-leading cybersecurity experts, LRQA helps organisations in achieving the goal of best security practices. We can provide our CISO services as well as security testing and broader information assurance services.

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

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 programme.
- 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 the CISO services deliver at the strategic and tactical level

Strategic activities

Board briefings

- Inform and educate senior leadership of security posture, risk, threats and investment profiles.
- Demonstrate RoI from the security functions.

Certifications

- Provide programme and project leadership for ISO27001, PCI DSS.
- Security leadership for Data Privacy issues (e.g., GDPR).

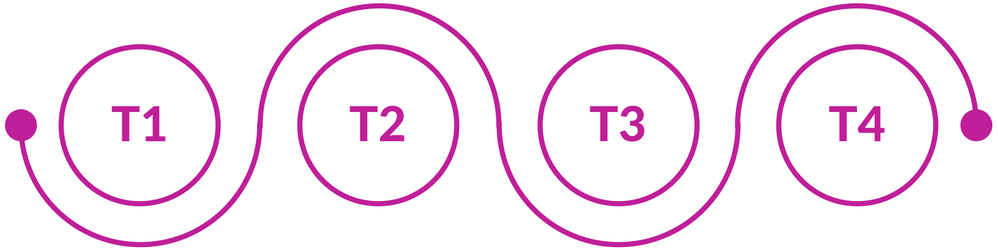
Risk management

- Deliver cyber risk measurement from a resilience and a threat perspective.
- Intertwine output from cyber risk into wider operational risk outputs.

Resilience

- Incorporate incident, business continuity management and DR strategies.
- Stress test the ability to react, respond and recover from adverse events.

Tactical activities



Governance

- Align current documentation to the aspired maturity level.
- Implementation a seamless policy to implementation for security controls.

Supply chain

- Ensure criticality of supply chain is observed and triaged.
- Monitoring of third parties to ensure resilience in supply chain.

Tools review

- Analysis of current tech to tolerate, invest, eliminate or migrate current tools.
- Provide technical assistance to enhance current systems.

Robustness

- Conduct vulnerability testing and assessment to ensure safe and secure network.
- Carry out internal audits to measure effectiveness and efficiency of controls.

About LRQA:

LRQA is the leading global assurance partner, bringing together decades of unrivalled expertise in assessment, advisory, inspection and cybersecurity services.

Our solutions-based partnerships are supported by data-driven insights that help our clients solve their biggest business challenges. Operating in more than 150 countries with a team of more than 5,000 people, LRQA's award-winning compliance, supply chain, cybersecurity and ESG specialists help more than 61,000 clients across almost every sector to anticipate, mitigate and manage risk wherever they operate.

In everything we do, we are committed to shaping a better future for our people, our clients, our communities and our planet.

Get in touch

Visit **www.lrqa.com** for more information or email **cybersolutions@lrqa.com**

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