FINANCIAL SERVICES

Cybersecurity resilience in financial services

In today’s hyper-connected financial ecosystem, cybersecurity is no longer a technical issue. It’s a critical business risk. The stakes are particularly high for banks, investment firms and payment processors as any breach can lead to regulatory penalties, reputational damage and financial loss.

With cyber threats growing in scale and sophistication, financial institutions must adopt a proactive, risk-based approach to cybersecurity. From identifying vulnerabilities and aligning with regulatory expectations to responding quickly to incidents and embedding resilience, cybersecurity must be integrated throughout operations and governance.

How we partner with you, wherever you are on your cyber maturity journey

Governance, risk and compliance

Meet obligations for data protection, financial regulations and compliance with industry and legislative frameworks

Security testing

Understand cybersecurity effectiveness, identify weaknesses and your ability to withstand a cyber-attack

Advisory services

Maintain cybersecurity maturity and resiliency in line with your risk tolerance. Improve your risk management of threat and vulnerabilities

Security and network solutions

Design, implement, maintain and remediate security and networking technologies

Managed security services

Implement systems for the effective detection of and response to cyber threats

Incident response

Understand how to respond to a potential cyber incident while minimising the impact to your brand, data, people and clients. If an incident occurs, minimise the impact of a breach, mitigate and recover

Assurance

Don’t assume you can stop attacks – validate your security controls across your attack surface

Security testing

The challenges organizations like yours can face

- High-value targets for cybercrime and nation-state actors
- Complex, distributed IT environments
- Verifying the effectiveness of the organization's cybersecurity posture
- Preventing and withstanding a cyber attack against credible threat actors
- Complying with regulatory framework requirement
- Benchmarking cybersecurity controls against DORA, PCI DSS, TIBER-EU, NIS2, ISO 27001 and GDPR
- Complying with requirements from the organization's customers or supply chain
- Identifying the weaknesses in the organization's infrastructure, networks, apps, people and processes
- Having a plan of action for vulnerability and incident remediation

LRQA solutions

- Red teaming
- Penetration testing
- Regulated testing (CBEST/GBEST/iCAST/ STAR/TIBER)
- Application testing
- Infrastructure testing
- Social engineering
- Cloud security assessments
- Code review
- Digital attack surface assessment
- ASM
- Purple teaming
- Vulnerability assessment
- Continuous Assurance
- Bug bounty
- Developer training

Effective cybersecurity isn't just about technology – it's about governance, accountability and continual improvement. LRQA supports financial institutions in embedding cyber risk management at every level, from executive reporting to board-level cyber risk committees. By integrating proactive cybersecurity with clear oversight, institutions can reduce risk exposure, protect customer data and strengthen market and stakeholder trust.

Red teaming

Expose the gaps, test the response, build the resilience

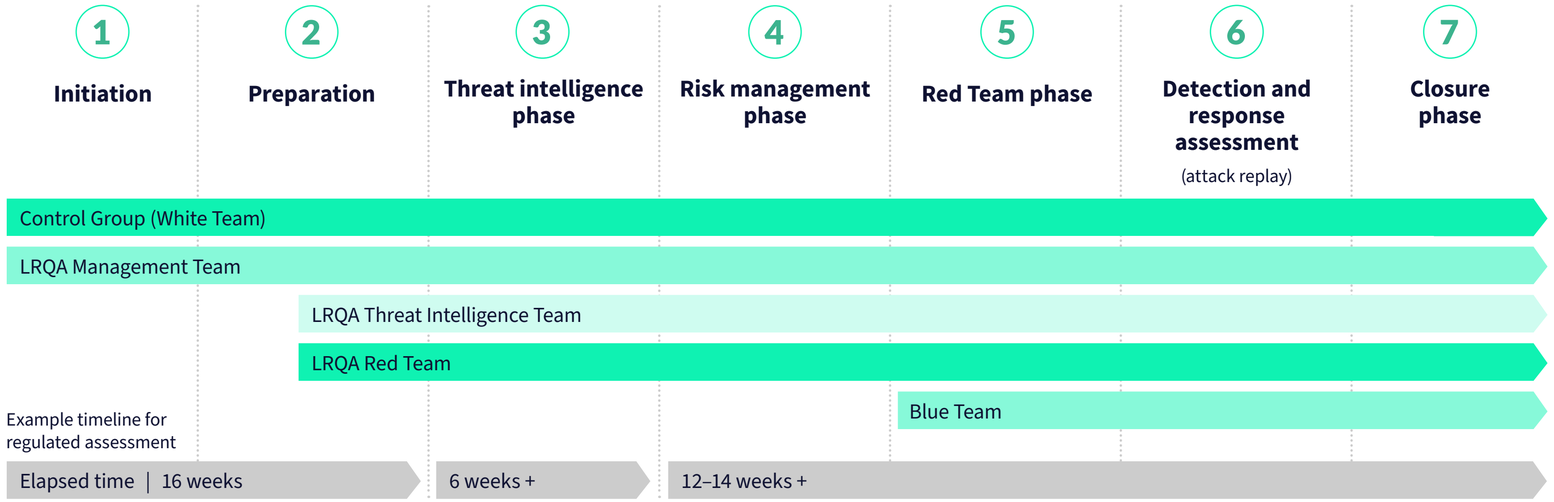
For financial services, red teaming isn't about ticking a box, it's about building resilience against adversaries already targeting you. We help you find the cracks before someone else does by focusing on seven key areas:

1. Realistic threat simulation
2. End-to-end risk exposure
3. Defensive layers test
4. Strategic risk insight for boards and executives
5. Crisis simulation and response hardening
6. Regulatory readiness
7. Elevating security culture

Process

Our tried and tested approach

Using our experience to partner with you to deliver a successful engagement



Our testing experience

50+
regulatory assessments delivered
(TIBER, CBEST, GBEST, iCAST, AASE, i-CRT)

Multiple
cross-jurisdictional tests
(collaboration with multiple EU authorities)

300+
systems listed in scope of completed assessments

150+
scenarios designed and tested

Multiple
engagements testing regional differences and interactions between SOCs globally

Penetration testing

Designed to uncover what matters most, first

At LRQA, we view penetration testing as more than just a checkbox exercise – it's about finding out how real your risks are, how attackers can move through your environment and what you can do about it before they do.

- Penetration testing uncovers real, exploitable weaknesses in your systems, applications and infrastructure. It's not just theoretical – it shows how attackers can chain those issues together to reach something valuable
- We don't just give you CVEs and severity scores. We show how those vulnerabilities could lead to data exposure, financial fraud, or operational disruption – putting risk into a business context your stakeholders can act on
- A good penetration test filters the noise. It tells you not just what's vulnerable, but what's exploitable and how deep the issue goes. That helps you focus your remediation efforts where they'll have the biggest impact
- Whether it's PCI-DSS, ISO 27001, or internal governance requirements, regular penetration testing helps demonstrate that you're not just compliant – you're secure by design
- Build a Culture of Continuous Assurance by feeding findings into a larger cycle of hardening, testing and improving. Done right, it becomes a core part of your offensive security strategy – not just an annual task

Process

Our tried and tested approach

Using our experience to partner with you to deliver a successful engagement

- Kick-off
- Recon/Enumeration
- Vulnerability analysis
- Exploitation
- Post exploitation
- Reporting
- Debrief

Why LRQA?

We understand that every organization has slightly different requirements in how they manage their security testing program. Our experience shows that these are often large-scale programs involving high volumes of processes and project management. A key challenge is managing the output effectively so it can be used to reduce risk through timely remediation.

Our expertise can help with this and reduce the mean time to remediate (MTTR), by providing a platform that allows your organization to gain:

- A single view of vulnerabilities across an organization's estate
- Holistic analysis to make decisions
- Data visualization
- Real time collaboration with consultants and program team
- Access to findings and remediation advice
- Reduced scheduling time
- Continuous penetration testing

More importantly, we understand the nuances of your operations. We can operate in more traditional project management methods and offer integrations to commonly known and unique ticketing systems too.

What makes LRQA unique?

- **Dedicated research and innovation team** focused on developing and exploring ideas that add value to our capabilities. Including core tooling, honey traps, zero-day exploits, blockchain and SOC maturity
- **Strong portfolio** of professional and managed services adaptable to customer needs
- The only organisation in the world with a **full suite of CREST accreditations**
- Through the use of proprietary tooling we're able to automate parts of our testing to allow our security professionals to focus on more obscure threats
- We find zero-day vulnerabilities in mainstream applications and systems, all of which are awarded unique CVE numbers

- LRQA is certified by a range of governing bodies for work in the financial sector and payment card industry. We're approved as a Qualified Security Assessor (QSA), PCI 3DS, PCI ASV and have consultants who are ISO 27001 lead auditors
- We are an accredited supplier of CBEST, GBEST/GCASE, CAA ASSURE and other xBEST assurance services as an approved CREST STAR testing services provider
- ISO 27001 (Information Security), ISO 9001 (Quality), ISO 14001 (Environmental) and PCI DSS underpin our rigorous quality practices and procedures

500+
Financial services clients globally

100+
Penetration Testers and Red Team consultants on staff

50+
Regulatory driven tests completed
(TIBER, CBEST, ICAST, AASE, I-CRT)

4,500
Penetration tests conducted for financial institutions

"LRQA are always on hand to offer a solution and work with us as we encounter internal challenges. They also provide experience and technical expertise in everything they do for us."

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 **lrqa.com** for more information or email **enquiries@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.