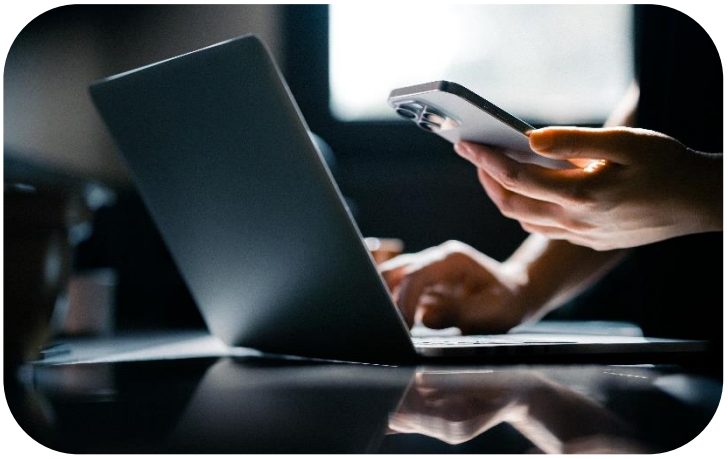
Cyber – Security Testing

This Loss Prevention Standard discusses the importance of security testing in helping to avoid cybersecurity related interruption.

Version: 1.0
Date: 29th July 2026

Cyber – Security Testing

Introduction



Security testing is a fundamental element of providing cyber assurance for organisations, but it can also provide assurance more broadly across different security domains.

Whilst there is generally more cost associated with security testing, it is a fundamental means of understanding what known, or unknown, internal vulnerabilities are present and how to remediate them. This can enable organisations to act proactively to prevent threat actors exploiting any weaknesses within their security architecture.

This Loss Prevention Standard discusses the following forms of security testing:

- Penetrating testing,
- Red teaming and adversary simulation,
- Blue teaming,
- Purple teaming, and
- Physical testing and insider testing.

What is Security Testing?

For the purposes of this document, 'security testing' is a catch-all term for different types of penetration testing across cyber, physical and insider vectors.

Where possible, to implement a robust assurance testing programme, organisations should combine technical penetration testing, adversary simulation, physical security assessments and insider risk exercises.

A mature security testing programme should:

- Be aligned to organisational risk and critical assets,
- Test people, processes and technology,
- Validate both preventative and detective controls,
- Use realistic threat scenarios,
- Support continuous improvement and remediation, and
- Measure security effectiveness rather than compliance alone.

Where appropriate, security testing should complement risk management frameworks, ISO 27001 controls, Cyber Assessment Framework (CAF) activities, and wider operational resilience programmes.

Generally, across the different types of security testing, the following methodology is used:

1. **Scoping**
   a. Ensure relevant stakeholders are involved including staff with the relevant knowledge of the system or procedure being targeted.
   b. Boundaries need to be agreed regarding what is in scope and out of scope, including the need for out of hours testing and any special handling around systems or procedures.
   c. Risk owners should demonstrate transparency in areas of special concern.
   d. A testing plan should be developed setting out the core elements of the pen test.
2. **Testing**
   a. Ensure there is a clear point of contact within the organisation for the 'testers' who can be contacted at short notice in case of any critical issues.
   b. The scope may change depending on what the 'testers' find.
3. **Reporting**
   a. Include security issues uncovered, the associated vulnerability exposures, methods for resolving issues found, and advice on how to improve internal processes.
   b. Debriefs are generally delivered, with a technical debrief to the operations team and an executive level debrief to the board.
4. **Severity Rating**
   a. Generally, 'testers' use the Common Vulnerability Scoring System (CVSS).
5. **Report**
   a. Ensure that the report is effectively reviewed internally to enable informed decision making on what to address and when.

Penetration Testing

The National Cyber Security Centre (NCSC) defines penetration testing (or pen testing) as a method of gaining assurance in the security of an IT system by attempting to breach security controls using techniques similar to those employed by real threat actors. It helps provide a vulnerability assessment and subsequent management processes.

However, pens tests only validate that targeted IT systems are not vulnerable to known issues on the day of the test. Pen tests should be regarded as an audit, just as you would have a financial audit. As such, pen tests should only be conducted by qualified and experienced individuals, ideally from an external third party.

There are two broad categories of pen testing:

1. **Assumed level of compromise.** Where the testers have a 'leg up' and full information about the target is shared in advance. This type of testing provides assurance around the internal vulnerability assessment and management controls.
2. **External compromise**. Where the testers have no privileged information about the internal architecture of the target. This is aimed at identifying how a threat actor can access an organisation from an external perspective.

Pen testing focusses on technology, and commonly includes but is not limited to:

- Application testing,
- Infrastructure testing,
- Cloud testing, and
- Product testing.

Red Teaming and Adversary Simulation

Red teaming is an objective and goal-based exercise, simulating realistic threat actors attempting to achieve specific goals. People, processes and technologies can be targeted to provide a full picture of an organisations defensive posture and overall resilience.

Red teams apply advanced Tactics, Techniques and Procedures (TTPs) and generally operate under the following parameters:

- Full chain of attack, from social engineering, malware introduction, lateral movement, privilege escalation to achieve objectives.
- Use of the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework to model a specific threat actor or Advanced Persistent Threat (APT) known to target a specific industry.
- No notice for internal teams (such as blue teams) to replicate a realistic response.
- Specific achievable objectives, such as bulk downloading of data.

Benefits of red teaming include, but are not limited to:

- Allows organisations to evaluate incident detection and response capabilities in a true-to-life environment.
- Identifies gaps in technical controls.
- Identifies training needs.
- Improves the capability of internal response teams.
- Identifies areas where investment into additional controls, people and / or processes is needed to reduce risk.

Blue Teaming

‘Blue teams’ are an organisation’s defensive team, who aim to protect their critical assets and networks from cyber-attacks. Blue teams can defend against red teams during testing to enhance their effectiveness.

Testing activities can include:

- Threat hunting assessments.
- Security Operations Centre (SOC) review.
- Security monitoring validation.

Purple Teaming

'Purple teaming’ is a combination of red and blue teaming, where teams work together in a collaborative exercise aimed at providing extremely worthwhile learnings and outcomes. The red team simulates real-world attack techniques based on real world threat intelligence, whilst the blue team monitors their systems and responds to the simulated attack. Both teams share their insights and testing data in real time through a constant feedback loop.

Benefits of purple teaming include, but are not limited to:

- Better understanding between offensive and defensive teams, bridging knowledge gaps and improving knowledge sharing.
- Maximising budget by combining the two techniques, especially by utilising the knowledge and skills of the internal security team.

Physical Testing

The physical security of your premises and assets is critical to protecting your cyber assets and should not be overlooked. This forms an essential part of overall protective security, securing defences against hostiles. Some typical areas of physical security that are tested, but not limited to are:

- Building access controls.
- Visitor management procedures.
- Effectiveness of security guards.
- Tailgating and unauthorised access.
- Asset protection controls.
- Data centre security.

Physical testing can generally take the form of physical penetration testing and red teaming and whilst there are similarities between the two, they are different testing mechanisms:

Red teaming. Accurate and realistic replication of threats organisations face. As with other types of red teaming and threat replication, the testing looks to emulate a realistic hostile approach to identifying vulnerabilities and how compromise can be achieved.
Physical penetration testing. Predefined testing to assess compliance against standards.

Some key benefits from physical testing include, but are not limited to:

- Identifies vulnerabilities that cyber testing does not.
- Enhances the protection of critical assets and premises.
- Validates the organisational security procedures and policies.
- Reduces the likelihood of hybrid physical compromise leading to a cyber-attack.

Insider Testing

It is important to remember that not all threats originate externally. Insider threats can arise from disgruntled employees, accidental compromise of employees, contractors or suppliers who have legitimate access to organisational assets.

Running an insider exercise programme and / or having an insider scenario in a wider cyber tabletop exercise, is a great way to evaluate some of the following procedures:

- Privileged access management.
- Data loss prevention controls.
- Monitoring capabilities.
- Joiners, movers and leavers processes.
- Segregation of duties.
- Data exfiltration detection.

The NCSC highlights the importance of controls that prevent, monitor and audit attempts to remove sensitive data from organisations. Ensuring an organisation has a strong security culture can significantly improving the overall risk posture in this space.

Cross-cutting Security Testing

Security should not be thought of in separate silos, instead, a holistic approach to strengthening and maintaining organisational resilience to hostile threats should be adopted.

Hybrid exercising is a great way to implement this approach, be it a physical intrusion leading to cyber compromise, or an insider leading to cyber compromise, the options are vast and ARMS Cyber can provide further advice where required.

Accreditations

When selecting a provider for security testing, it's important to ensure that they are appropriately qualified and accredited. Key industry recognised accreditations include, but aren't limited to:

- **CREST**. An international not-for-profit membership body that audits and accredits cyber security providers for a variety of services.
- **CHECK**. NCSC's scheme for assured organisations that can conduct penetration testing of public sector, Critical National Infrastructure (CNI) and networks.
- **The Cyber Scheme**. An accreditation body for ethical security testing and penetration testing.
- **CyberSecure Canada**. A Government backed certification programme aimed at improving cyber security assurance.

Contact Information

United Kingdom

Please visit Aviva Risk Management Solutions or email us at riskadvice@aviva.com. To speak to one of our advisors, call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Canada

Please visit Aviva Risk Management Solutions | Aviva Canada or email us at arms.canada@aviva.com

Ireland

Please visit Insurance Risk Management | Business Risk Management Insurance - Aviva Ireland or Email us at armsireland@aviva.com

Specialist Partner Services

Aviva have created a network of Specialist Partners to complement our in-house capabilities and to enable our policyholders to benefit from a wide range of risk management solutions at preferential rates and terms. Together, we provide solutions to help with the significant challenges of modern-day risk management.

Note: These partner relationships are wholly for the benefit of our policyholders with no income to Aviva.

The following Specialist Partners provide products or services in relation to risk guidance provided, discussed or referenced in this Loss Prevention Standard.

United Kingdom

- Cyber security services - **CSA Cyber**

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

Ireland

For more information please visit: Insurance Risk Management | Business Risk Management Insurance - Aviva Ireland

Canada

For more information please visit: Our Specialist Partner Network | Aviva Canada

Standards, Sources and Useful Links

Canada

- Canadian Centre for Cyber Security

United Kingdom

- NCSC – Cyber Essentials
- National Cyber Security Centre (NCSC)
- CHECK
- The Cyber Scheme

Other

- The European Union Agency for Cybersecurity (ENISA)
- CREST

Additional Information

Loss Prevention Standards

These documents set out best practice recommendations to help reduce the likelihood and impact of losses.

Relevant Aviva Loss Prevention Standards include:

- **Cyber - Respond and Recover.**
- **Cyber - Supply Chain Risk Management**
- **Cyber - Ransomware**
- **Cyber - Respond and Recover**
- **Cyber - Incident Response Process**
- **Cyber - Homeworking Security**
- **Cyber - 12 Top Tips to Protect Against Cyber Attacks**
- **Cyber - Security Certifications for Organisations**
- **Cyber - Back-ups**

Please visit Loss Prevention Standards to view the full library.

Aviva Risks Training Solutions (United Kingdom Only)

Aviva Risk Training Solutions, delivered through our Specialist Partner, SafetyCulture, provide free, bite-sized learning modules exclusively for Aviva policyholders.

Relevant courses include:

- **Cyber Fundamentals**
- **Social Engineering**

Please visit Aviva Risk Training Solutions for further guidance.

29th July 2026

Version 1.0

ARMSGI4466026

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.