

Cyber – Incident Response Planning

This Loss Prevention Standard provides guidance on formulating a Cyber Incident Response Plan to help reduce the consequences of a cyber security event.

Cyber – Incident Response Planning

Introduction

With the continually evolving cyber threat landscape, it is essential for organisations to develop and maintain resilience against cyber incidents.

Organisations must be capable of detecting cyber incidents and responding to them quickly and effectively, with the aim of minimising financial, operational, and reputational impacts.

Consequently, having a well-defined and effective Cyber Incident Response Plan (CIRP), supported by documented response procedures, is critical. Equally important is regularly validating the effectiveness of the CIRP through cyber incident exercises to ensure organisational preparedness and continual improvement.



Cyber Incident Response Plan

To respond effectively to cyber incidents, organisations must maintain a robust, practical, and well understood CIRP. Regardless of size, sector, or cyber maturity, certain foundational elements should always be present. Your CIRP should consider and integrate with your broader organisational resilience functions, including:

- Business Continuity Plans.
- Disaster Recovery Plans.
- Crisis Management.
- Risk Management Processes.

The aim is to avoid siloed documentation and instead create cohesive organisational response materials. For example, consider whether the relevant executive team is consistent across each plan, and whether the plans reference each other throughout.

Core Elements of a CIRP

The following components are required to ensure a robust CIRP:

- Purpose and objectives.
- Cyber security incident response team detailing clear roles and responsibilities.
- Incident classification and severity matrix.
- Escalation channels.
- Reporting requirements for insurers, legal, regulatory, etc.
- Communications.
- Detection and analysis.
- Containment and mitigation.
- Remediation.
- Recovery.
- Lessons identified.

[ARMS Cyber](#) has created a suite of templates designed to help support organisations in developing their own CIRP, which are available to Aviva customers with Cyber covers on the Aviva Risk Insight Portal, upon request.

Important: These templates are best practice examples only and should be tailored to the specific needs of the organisation.

Once your organisation has a well-established and tested CIRP, it is worthwhile to consider developing playbooks for potential scenarios.

Template annex directory:

- **Cyber Incident Response - Pre-Incident Response Planning Checklist**
- **Cyber Incident Response - Developing a Cyber Incident Response Plan**
- **Cyber Incident Response - Categorisation and Severity Matrix**
- **Cyber Incident Response - Response Teams**
- **Cyber Incident Response - Contact Directory**
- **Cyber Incident Response - Situation Report Template**
- **Cyber Incident Response - Communications During an Incident**
- **Cyber Incident Response - Incident Log Template**
- **Cyber Incident Response - Lessons Identified Log Template**

Important: CIRPs should be reviewed on an annual basis, as a minimum, **or** when there is a notable change to internal processes.

Contact Information

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

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.

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.

Canada

For more information please visit: [Our Specialist Partner Network | Aviva Canada](#)

Ireland

For more information please visit: [Insurance Risk Management | Business Risk Management Insurance - Aviva Ireland](#)

United Kingdom

- Cyber security services - [CSA Cyber](#)

For more information please visit: [Aviva Risk Management Solutions - Specialist Partners](#)

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](#)

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**
- **Cyber - Playbooks**

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.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. By extension, any links to third-party websites do not constitute marketing by Aviva and are included solely for the reader's information and educational purposes. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise, and Aviva recommend that you obtain specific advice relevant to the circumstances.

3rd September 2026

Version 1.0

ARMSGI4482026

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.