

Cyber – Mergers and Acquisitions Exposures

Cyber security needs to be a key consideration during the Merger and Acquisitions process.

This Loss Prevention Standard highlights the key areas for consideration to help support organisations.

Cyber – Mergers and Acquisitions Exposures

Introduction

Mergers and acquisitions (M&A) can present significant opportunities for promoting business growth, market expansion and efficiencies for organisations.

However, both the process of a merger or acquisition, and the ‘target business’ being merged with or acquired, may present new and significant cyber risks that are not immediately obvious.



Cyber security and the associated due diligence should be treated as a core consideration when embarking on a business merger or acquisition. Failure to conduct the appropriate due diligence for cyber security risks can lead to organisations being unnecessarily vulnerable, and trigger additional exposures including business interruption, reputational damage and reduced deal value to name a few.

Key Considerations

Cyber security is a critical component of M&A and can influence various elements of the process. Key areas to consider when embarking on M&A, may include, but are not limited to, the following:

- Historic or ongoing cyber incidents.
- Legacy technology and unsupported systems.
- Weak identity and access management.
- Poor security governance.
- Supply chain and third-party vulnerabilities.
- Inadequate disaster recovery capabilities.
- Non-compliance with data protection.

It is also important to consider the role of employees throughout the process and whether disgruntled employees may pose an insider threat.

Set out below are pre-merger and post-merger specific queries that may help to drive informative discussions.

Pre-Merger Cyber Security Due Diligence

It is critical that effective due diligence is conducted from a cyber security perspective, so that organisations have a clear understanding of the cyber maturity and any associated known risks of the target entity. Depending on the nature and sector of the businesses, there can be an increased risk of a cyber incident resulting from the acquisition announcement itself where threat actors may exploit organisational change.

The following steps should be considered as part of the pre-merger due diligence activities:

1. Review Security Governance

- a. Cyber security strategy.
- b. Risk management framework.
- c. Board oversight and reporting structures.
- d. Security policies and standards.
- e. Understand what cyber insurance cover is in place and what may need to change, along with any Cyber related notifications to insurers.

2. Security Culture and Awareness

- a. Understand whether any security awareness, campaigns or training programmes are in place.
- b. Phishing simulations.
- c. Penetration testing.

3. Security Controls Framework Assessment

- a. Understand what frameworks are in place, such as Cyber Essentials, the NIST Cyber Security Framework and ISO27001 Information Security Management Systems.
- b. Understand identity and access management controls.
- c. Endpoint security.
- d. Vulnerability management.
- e. Network security.

4. Incident Response

- a. Understand previous incident history if applicable.
- b. Review the Cyber Incident Response Plan.
- c. Understand wider assurance activities.
- d. Table Top Exercising.

5. Resilience and Preparedness

- a. Understand what backups are in place and whether they are immutable.
- b. Understand disaster recovery metrics and protocols.
- c. Recovery testing from backups.
- d. Review Business Continuity Plans and wider crisis management arrangements.

6. Data Protection and Regulatory Compliance

- a. General Data Protection Regulations in the United Kingdom and Ireland and Personal Information Protection and Electronics Documents Act (PIPEDA) in Canada, etc.
- b. Industry-specific regulations, where appropriate.
- c. Data storage and classification schemes.

7. Supply Chain and Third Party Risk

- a. Map suppliers.
- b. Assess key technology suppliers.
- c. Assess MSPs, cloud providers and outsourced security providers.
- d. Understand the supplier assurance process and monitoring arrangements.

8. Technology

- a. Understand whether there are any unsupported operating systems.
- b. Understand whether there are any end-of-life software and legacy applications.
- c. Conduct an Open Source Intelligence (OSINT) Review to see what, if any, open security vulnerabilities exist.

Post-Acquisition Integration

Following an acquisition, there needs to be a structured integration programme that focusses on identity, infrastructure, monitoring, resilience and governance to minimise the potential cyber exposure.

Effective integration is key to ensuring that the transition post-acquisition is managed appropriately. Some core elements of this process are set out below:

1. Establishing a Security Baseline

- a. Involve security leaders from the outset.
- b. Ensure multi-factor authentication (MFA) is enabled across all critical systems.
- c. Review privileged access and implement least privilege principles.
- d. Activate necessary security monitoring.
- e. Activate necessary vulnerability scanning.

2. Identity and Access Integration

- a. Remove any unused accounts.
- b. Align authentication methods.
- c. Consolidate accounts where possible.

3. Align and Ensure Visibility Across Security Monitoring and Detection

- a. Vulnerability management processes.
- b. Security Operations Centre (SOC) monitoring.
- c. Threat intelligence feeds.

4. Network and Infrastructure Consolidation

- a. Organisations should adopt recognised secure architecture and secure-by-design principles, drawing on guidance such as the UK National Cyber Security Centre (NCSC) Secure Design Principles, the Irish National Cyber Security Centre Cyber Security Baseline Standards, and guidance issued by the Canadian Centre for Cyber Security.
- b. Conduct security assessments and identify high risk systems.
- c. Ensure vulnerable environments are segmented.
- d. Validate asset inventories.

5. Change Programme and Remediation

- a. A clear programme needs to be in place, with governance oversight, to ensure the effective integration with clear deliverables.
- b. Align and update all policies.

Key Takeaways

Cyber security must be considered as a critical part of the M&A process. Effective due diligence should be undertaken to ensure that key risks are considered and managed appropriately.

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](#)

Ireland

- [Gov.ie Cyber Security Baseline Standards](#)

United Kingdom

- [NCSC Secure Design Principles](#)
- [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 - Incident Response Planning**
- **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

ARMSGI5112026

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.