

Business Continuity – Data Centres

This Loss Prevention Standard provides guidance on the effective design and implementation of business continuity systems within data centre environments.

Business Continuity – Data Centres

Introduction

Data centres process, manage and store vast quantities of data and are considered critical infrastructure for many sectors.

Business interruption events within these facilities are uncommon; however, the consequences of even the most minor incidents can be significant. This document provides a summary overview of the main risk exposures and guidance on implementing business continuity systems.



Note: This Loss Prevention Standard relates to the handling and storage of recovered vehicles and is focussed on asset loss prevention and related risk management guidance. It is not intended to address liability/general liability exposures. The presumption is that all local regulatory territory requirements, and compliance with national/local building regulations, codes, or standards take precedence and have, or will be, met. In territories where local authorities have jurisdiction, compliance with applicable laws and regulations is assumed as a minimum requirement. The recommendations in this document are intended to supplement, not replace, local requirements.

Understanding the Risks

Common risks/exposures/issues include but not limited to:

Power Failure. Loss of power supplies, including backup systems, can cause immediate system shutdown. Without power and fuel resilience, even short interruptions can lead to major outages.

Fire and Explosion. Electrical faults and overheating equipment can result in fires, whilst faults in battery systems such as backup (BBU), uninterruptible power supplies (UPS) or Battery Energy Storage Systems (BESS) can, in some cases, lead to explosion incidents. Such events can cause severe damage and prolonged downtime if not effectively controlled.

Contractual Agreements. Delays in data transfer times caused by a loss incident can result in deviations from contract terms and potentially extensive contingency costs.

Cooling System Failure. Failure of ventilation and cooling systems can lead to rapid overheating of servers. This often results in automatic shutdowns or permanent damage to equipment, buildings and other infrastructure.

Natural Hazards. Flood, storms, lightning, extreme temperatures, etc., can damage sensitive or vulnerable equipment and disrupt power supplies and cooling systems.

Detection and Protection System Impairment. Disabled or impaired detection and protection systems can lead to delays in responding to fire events and increased damage.

Equipment Failure. Hardware failures can disrupt operations, particularly where resilience or redundancy is insufficient.

Network and Connectivity Failure. Disruptions to telecoms infrastructure can prevent or slow access to hosted systems. Poor network diversity increases the risk of single-point failures.

Water Damage and Leakage. Leaks from cooling systems, water pipes, etc., can damage or corrode critical equipment. Even small amounts of water can cause significant disruption.

Environmental, Social and Governance (ESG). Environmental dependencies, such as power, water, and climate, sustainability pressures, including resource use and supply chains, and governance factors, such as compliance and oversight can lead to operational disruption, regulatory constraints, supply limitations and increased recovery delays.

Cybersecurity Incidents. Cyber-attacks can render systems unavailable, as well as lead to data loss, regulatory breaches, and reputational damage.

Security. The siting of data centres can be the cause of local protest due to their high power and water needs and environmental impacts. Adequate perimeter and building security are critical and this is discussed in the Aviva Loss Prevention Standard – **Data Centres – Planning and Design.**

Third-Party / Supply Chain Dependency. Reliance on external providers (telecoms, maintenance and service engineers, fuel supplies, etc.) introduces risks outside direct control. Failures in these services can directly impact operations.

These factors can all lead to interruption, however, a lack of, or inadequate, business continuity planning can exacerbate the extent of loss via:

- **Extended Downtime.** The recovery of critical processes or services may be delayed, resulting in prolonged operational disruption.
- **Decision Making.** Delayed or ineffective decision-making can lead to errors and significantly increased losses.
- **Reduced Recovery Capability.** Delays can hinder recovery efforts.
- **Reputational Damage.** Prolonged disruption and delayed recovery can damage relationships with customers, suppliers, shareholders and other stakeholders.
- **Regulatory Non-Compliance.** Inadequate management may result in breaches of legal or regulatory requirements, leading to fines or other sanctions.

Note: This document discusses business interruption risks, which include insurable and uninsurable risks. Consult your policy wording or broker for guidance.

Managing the Risks

Business continuity planning can be addressed via seven steps. These are discussed in more detail in the Aviva Loss Prevention Standard **Seven Steps to Continuity** and the accompanying documents in the series:

- **Business Continuity – Step 1: Roles and Responsibilities**
- **Business Continuity – Step 2: Incident Management Plan**
- **Business Continuity – Step 3: Communications Plan**
- **Business Continuity – Step 4: Business Impact Analysis and Risk Assessment**
- **Business Continuity – Step 5: Solutions Design and Implementation**
- **Business Continuity – Step 6: Policy**
- **Business Continuity – Step 7: Test and Exercise Plan**

Areas to specifically consider in relation to data centres include:

Material Damage

Data centres are exposed to a range of material damage risks. These include, but are not limited to fire, explosion damage, flood and other adverse weather conditions, escape of water and other fluids and cooling system failure. The risks of damage increase significantly when detection and protection systems are faulty or inadequate.

These risks, and the recommended risk management controls, are discussed in the following Aviva Loss Prevention Standards:

- **Data Centres - Planning and Design**
- **Data Centres - Construction**
- **Data Centres - Detection and Fire Protection**
- **Data Centres - Fire and Smoke Resilience**
- **Data Centres - Cooling and Ventilation**
- **Data Centres - Escape of Water and Other Fluids**
- **Data Centres - 15 Top Tips**

Redundancy

The loss of critical systems such as power, cooling, connectivity, etc., can result in significant business disruption. Backup arrangements need to be carefully considered, including:

Secondary Facilities. Mirrored data centres, operating independently, with the capacity to operate individually at 100% of total capacity, are the most effective means of providing redundancy following loss events.

Containment. Where secondary facilities are not viable, the use of fire, smoke and water resisting compartments for the siting and apportionment of server and other critical equipment, each with independent power, cooling and control systems, can help reduce the potential for whole site failure from a loss incident.

Refer to the Aviva Loss Prevention Standards **Fire Compartmentation, Fire Doors, Shutters, Dampers and Collars** and **Heat and Smoke Venting Systems** for further guidance.

Power. Multiple, independent appropriately sized power supplies supported by sufficient generator, and UPS and BBU systems to provide immediate secondary power for critical/essential equipment and services.

Cooling and Ventilation. Ensure multiple independent cooling systems are installed along with duplicated environmental monitoring. The aim should be to maintain critical operations, despite the failure of one of more cooling systems.

Water Supplies. Water supplies are a critical component of data centre resilience, particularly where water-based cooling systems are in use. Contingency plans should be in place to ensure continued operation or controlled shutdown, and to support rapid recovery following disruption. Areas to consider include:

- Risk Assessment including external risks, such as drought, flood and associated contamination, supply restrictions, or failure of water systems.
- Secondary or alternative sources where practicable.
- On-site storage or buffer capacity sufficient to maintain operations during short-term interruption.
- Monitoring for contamination, temperature, leakage, or system failure.

Important: Any systems providing redundancy should be designed and arranged so that a single initiating loss event or point of failure cannot impact the business activities. Examples may include:

- Power supplies not being able to be switched to secondary supply or routing.
- Duty and backup equipment being in the same fire area.
- Duty and backup equipment being in the same area allowing a single water leak to impact both systems.
- Duty and backup cabling being installed in the same cable trays or same fire area.
- Ventilation or cooling systems being manifolded, etc.

Environmental, Social and Governance

Robust governance, resilience, and resource management strategies, including sustainable energy and water use, climate risk mitigation, and compliance frameworks should be implemented to help minimise disruption and enable recovery following an ESG-related event. Areas for consideration include:

- Risk assessment,
- Resilient infrastructure design,
- Secure supply chains, and
- Incident response and recovery plans.
- Reputational risks

Refer to the Aviva Loss Prevention Standard **Environmental, Social and Governance Overview** for further guidance.

Supply Chain

Recovery can be significantly affected by external suppliers, e.g., power, fuel, IT and communications equipment, network services, technical support, etc. Disruptions within the supply chain will inevitably result in delayed repairs or reinstatement following an incident.

Key considerations include:

Critical Suppliers. Identify all key dependencies and assess their importance to operations.

Supplier Resilience and Capability. Assess the continuity arrangements and recovery capabilities of critical suppliers. Involve them in test and exercise initiatives.

Alternative Suppliers. Consider arrangements for secondary suppliers.

Spare Parts and Availability. Maintain critical spares on-site.

Logistics and Lead Times. Consider delivery times, import issues (including currency fluctuations), and other potential disruption (e.g., transport issues, geopolitical risks, etc.).

Service Level Agreements (SLAs). Ensure contracts include clear response, recovery time, and priority service provisions.

Third-Party Access and Response. Ensure suppliers can access the site (or systems remotely) promptly when required.

Monitoring and Review. Regularly review supplier performance, resilience, and any emerging risks.

Refer to the Aviva Loss Prevention Standard **Supply Chain Risk Management** for further guidance.

Cyber Exposures

Data centres are significantly exposed to cyber-attacks and should implement robust security arrangements. The Aviva Loss Prevention Standard **Cyber Governance for Boards** discusses five governing pillars of a cybersecurity framework, namely:

1. **Risk Management.** The risk assessment process identifies and evaluates risks, and the necessary control measures.
2. **Strategy.** This details how the data centre should:
 - Plan its response to an incident.
 - Exercise incident response procedures.
 - Detect, respond to and recover from a cyber-attack.
 - Manage employee cyber awareness training.
3. **People.** Ensure staff are adequately trained, and aware of cyber risks and common and evolving attack methods.
4. **Incident Planning, Response and Recovery.** This explains how data centres can prepare for, respond to, and recover from cyber incidents, with a focus on resilience, coordination, and recovery.
5. **Assurance and Oversight.** This outlines how data centres ensure ongoing assurance through effective questioning, governance integration, external validation, and a culture of continuous improvement.

Data centres should liaise with customers, suppliers and other stakeholders when formalising a cybersecurity framework to ensure that it aligns with expectations, regulatory requirements and any specific contractual requirements relating to cyber security.

Refer to the following Aviva Loss Prevention Standards for further guidance:

- **Cyber - Ransomware**
- **Cyber - Akira Ransomware**
- **Cyber - Respond and Recover**
- **Cyber - General Exercising Principles**
- **Cyber Governance for Boards**

Human Resources

The design, construction, commissioning, operational oversight and ongoing maintenance and upkeep of data centres require specialised skills. Securing those skills following a loss event to assist with prompt recovery is likely to present a number of challenges, including, but not limited to:

Key Workers. May seek alternative employment elsewhere.

Availability. Designers, contractors, operators, etc., are unlikely to be available at short notice to carry out repairs or reinstatement.

Training. Training and oversight will be required for new employees or temporary contractors.

Working Hours. It is a common assumption that shifts or working hours can be increased to help address reinstatement and repairs promptly. This is not always possible for a variety of reasons, e.g., neighbour objections, local or regulatory authority oversight, health and safety concerns, etc.

Ensure these factors are considered in the business impact analysis risk assessment.

Strategic Development Plan

To ensure the data centre and all associated business impacts are fully understood, both now and in the future, a formal and continually maintained Strategic Development Plan (SDP) should be established. This should be a live document that considers both the physical infrastructure of the facility and the business activities it supports, ensuring that business impacts are fully identified, understood, and quantified.

The insights gained from the SDP should inform both operational and strategic decision-making, influencing the design, maintenance, and development of the facility, as well as wider business planning activities.

The SDP should assess all physical aspects of the data centre, including building infrastructure, critical systems, capacity, and resilience, alongside the organisation's current and future business model. Its purpose is to ensure that resilience requirements are understood, validated, and maintained as the business evolves.

Ultimately, the SDP should provide assurance that both the facility and the business are capable of supporting future growth, changing operational demands, and emerging risks—in effect, determining whether the data centre and its supporting business functions are adequately future-proofed.

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

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.

United Kingdom

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

- [The Business Continuity Institute - Canada](#)

Ireland

- [The Business Continuity Institute - Republic of Ireland](#)

United Kingdom

- [The Business Continuity Institute](#)

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:

- **Business Continuity - Step 1: Roles and Responsibilities**
- **Business Continuity - Step 2: Incident Management Plan**
- **Business Continuity - Step 3: Communications Plan**
- **Business Continuity - Step 4: Business Impact Analysis and Risk Assessment**
- **Business Continuity - Step 5: Solutions Design and Implementation**
- **Business Continuity - Step 6: Policy**
- **Business Continuity - Step 7: Test and Exercise Plan**
- **Supply Chain Risk Management**
- **Environmental, Social and Governance Overview**
- **Cyber Governance for Boards**
- **Data Centres - Planning and Design**
- **Data Centres - Construction**
- **Data Centres - Detection and Fire Protection**
- **Data Centres - Fire and Smoke Resilience**
- **Data Centres - Cooling and Ventilation**
- **Data Centres - Escape of Water and Other Fluids**
- **Data Centres - 15 Top Tips**
- **Fire Compartmentation**
- **Fire Doors, Shutters, Dampers and Collars**
- **Heat and Smoke Venting Systems**

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.

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.

15th July 2026

Version 1.1

ARMSGI4232026

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.