Data Centres – 15 Top Tips

This Loss Prevention Standard provides 15 helpful Top Tips to help manage the risks associated with data centres.

Version: 1.0
Date: 17th April 2026

Data Centres – 15 Top Tips

Introduction

Data centres house computer hardware and ancillary equipment for the processing, management, and storage of data, and other related systems and applications.

Property damage events within these facilities are uncommon; however, the consequences of even the most minor of incidents can be significant.

This document provides summary guidance on the main risk exposures. For a more in-depth understanding of the exposures and what risk management measures to take, please see Aviva's other Data Centre 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**

Note: This Loss Prevention Standard relates to data centres and is focussed on property loss prevention and related risk management guidance. It is not intended to address liability exposures. The presumption is that all regulatory requirements, such as fire risk assessments and compliance with local building regulations, codes, or standards, have or will be met.

1. Management and Oversight

Stakeholders. Involve your insurer, broker, and any authority having jurisdiction in discussions relating to premises, equipment, business activities or risk management changes at the earliest opportunity. This can help ensure the data centre remains compliant with regulatory building requirements, standards, or codes and resilient to damage, business interruption and environmental losses.

Management of Change. Any changes to the Data Centre should be managed through a formal Management of Change process to help ensure all stages of the system design and installation are progressed with minimal exposure to the existing arrangements. Refer to the Aviva Loss Prevention Standard **Managing Change - Property** for further guidance.

Hot Works. Hot work, where permitted, must be conducted in strict accordance with the Aviva Loss Prevention Standard **Hot Work Operations.**

2. Material Damage and Business Impact Assessment

Before initiating risk management controls or designing/installing detection and protection systems, an assessment of the anticipated/potential financial losses, for both material damage and business interruption exposures, in the event of a significant or catastrophic loss event should be undertaken.

This assessment should include the current expected impacts and also future impacts as a result of planned business changes or expansions, and helps ensure risk controls, detection and protection systems, etc., are sufficient and reflective of the potential loss estimates.

Refer to the Aviva Loss Prevention Standards **Material Damage Risk Assessment** and **Business Continuity - Business Impact Analysis** for further guidance.

3. Redundancy

Data centre facilities should be designed with appropriate backup arrangements so that essential systems, such as servers, power, cooling, ventilation, etc., can continue operating if a primary system fails. This helps to reduce the likelihood of outages and minimise downtime, which are critical requirements for Data Centre operations.

Aviva recommends resilient systems, that are capable of providing continuity in service without any delay or interruption. Further guidance is provided in the Aviva Loss Prevention Standard **Data Centres - Planning and Design**.

4. Efficiency

Running data centre equipment at, or near maximum capacity, increases the risk of failure and can shorten asset life. Ensure systems are designed with spare capacity to reduce stress on individual components and lower maintenance, repair, and cooling costs.

5. Environmental and Sustainability

Flooding. Data centres should not be built in areas that are at risk of flooding. Where risk assessment suggests there is a flood exposure, ensure robust protective measures are installed, e.g., drainage backflow prevention, flood barriers and locating critical equipment above projected flood levels. Appropriate emergency response planning should be undertaken and the impacts of a flood event considered in the Business Continuity Plan.

Renewable Energy. Ensure any roof mounted solar photovoltaic systems are designed and installed by suitably experienced companies. Ensure the installation utilises voltage optimisers or other module level power electronics (MLPEs) which automatically reduce the voltage within faulty panels to safe levels, reducing the potential for fire events. Permanent roof access should be provided to support self-inspection and maintenance programmes. Battery Energy Storage Systems (BESS) should not be installed in or within 10 metres of data centre buildings.

Fire Service. Invite the local Fire Services to inspect the site and plans, evaluate fire risk exposures, determine water supplies, containment planning etc.

Refer to the Aviva Loss Prevention Standards for further guidance:

- **Flood Guidance and Mitigation (UK)**
- **Flood Guidance and Mitigation (Global)**
- **Small Scale Battery Energy Storage Systems**
- **Planning a Battery Energy Storage System - 12 Top Tips**
- **15 Top Tips for Roof Mounted Photovoltaic Solar Panel Systems**
- **Emergency Response Planning with Fire and Rescue Services**

6. External Exposures

A clear area of at least 10 metres should be maintained around data centre buildings, free from other infrastructure such as power generation or storage equipment, transformers, vehicle parking or charging facilities, adjacent buildings, smoking areas, combustible materials, waste storage, etc. This can help reduce the risk of fire and smoke damage to data centre buildings and equipment.

7. Fire and Smoke Resilience

Compartmentation. Compartmentation between the data halls and other areas of the building helps to reduce the risks of smoke and fire damage. Ensure at least two hours fire resisting compartmentation, including any glazing and fire doors/shutters, is provided between data halls and adjoining compartment walls and floors.

Plant Rooms. Plant rooms, which include any rooms housing uninterruptible power supplies (UPS) should also be constructed to achieve at least two hours fire resistance.

Firestopping. Any openings for cabling and pipework, etc., between fire compartments should be firestopped and/or fitted with intumescent collars or fire dampers to achieve a fire resistance rating commensurate with the fire compartment walls and floors.

Smoke Control. Minor smoke contamination can cause disproportionate damage to sensitive components. Ensure smoke control systems are robust and compatible, and interlocked with data centre ventilation and cooling systems to ensure optimum performance.

Refer to the Aviva Loss Prevention Standards **Data Centres - Fire and Smoke Resilience**, **Data Centres - Cooling and Ventilation** and **Heat and Smoke Venting Systems** for further guidance.

8. Battery Back Up Systems

Battery Backup Systems (BBUs) provide instant power response to small, momentary power fluctuations and interruptions, and are often installed within server racks. These systems will generally utilise lithium-ion batteries, which can produce volatile flaming and excessive smoke when ignited. Ensure:

- The use of BBUs within server racks is minimised.
- BBUs are adequately covered by fire detection and protection systems.
- The batteries are monitored for charging and general performance, health, etc.
  - ✓ Batteries should be replaced prior to lifecycle charging thresholds and **immediately** if dropped, faulty, or if monitoring systems and/or operators have identified any performance concerns, including unusual odours, swelling, excessive heat, etc.

9. Escape of Water and Other Fluids

Escape of water/fluid incidents in data centres can cause significant and disproportionate damage to buildings and equipment. Complete a risk assessment to identify the water and fluid related sources and exposures, and ensure appropriate controls are in place, including:

Location. Do not install water services directly over data halls. This includes any condensate-return pipework, which should be located away from data hall areas.

Detection. Install leak detection and flow monitoring devices to all wet services.

Protection. Lag exposed pipework and install trace heating as necessary.

Refer to the Aviva Loss Prevention Standard **Data Centres - Escape of Water and Other Fluids** for further guidance.

10. Cooling and Ventilation

Data centres generate significant heat and rely on effective cooling, ventilation, and humidity control to maintain server performance and prevent damage to equipment.

Cooling and environmental control systems should be specifically designed for the server and IT equipment located within the data halls, based on the planned equipment load and anticipated heat output, and should allow for future growth in order to minimise the risk of disruption and costly infrastructure upgrades. System design and cooling calculations should be carried out by a suitably competent person or specialist organisation.

Refer to the Aviva Loss Prevention Standard **Data Centres - Cooling and Ventilation** for further guidance.

11. Detection and Fire Protection

Gas Detection. Automatic gas detection should be considered in UPS rooms and server racks containing battery backup units to provide early warning of lithium-ion battery off-gassing. Ensure these are interlocked to isolate power supplies upon activation.
Fire Detection. All areas of the data centre, including floor and ceiling voids, should be covered by an automatic fire detection system. Aspirating detection technology, which provides rapid detection of smoke and fire events is recommended.
Fire Protection. Automatic sprinkler protection should be installed throughout the entire data centre building.

Important: Any detection and fire protection systems should be designed, installed and maintained in accordance with local or national regulations, standards or codes by competent and accredited companies. System designs and proposed interlock strategies should be reviewed and accepted by the property insurer or authority having jurisdiction prior to installation.

12. Self-Inspection

Data centres and all associated equipment, including cooling and ventilation equipment, electrical equipment, power generation, detection and fire protection systems, battery systems, charging equipment, compartmentation, housekeeping, etc., should be subject to a formal self-inspection programme. This can help to identify faults, issues and concerns that could develop into breakdown, damage and/or downtime.

Thermographic cameras should be used to check equipment for unusual heat patterns, electrical faults, leaks, etc.

Refer to the Aviva Loss Prevention Standards **Self-Inspections** and **Use of Thermographic Cameras - General Considerations** and **Checklist** for further guidance.

13. Maintenance, Inspection and Testing

Data centre buildings and equipment should be subject to formal maintenance arrangements as per the Original Equipment Manufacturer (OEM) or installer guidelines.

Maintenance programmes should be routinely audited to ensure ongoing adequacy of arrangements, compliance with standard operating procedures and corrective actions are being completed appropriately.

Refer to Aviva Loss Prevention Standards **Maintenance Regimes** for further guidance.

14. Emergency Response Planning

Effective emergency response planning can assist with the management of unexpected events or incidents. Appoint a dedicated Emergency Response Team (ERT) to help manage emergency events, and ensure key responsibilities are allocated and appropriate training provided. Refer to the Aviva Loss Prevention Standard **Emergency Response Teams** for further guidance.

15. Business Continuity Planning

Business Continuity Plans should be formalised to ensure disaster recovery and continuity arrangements are in place and aligned with the business impact assessments and any contractual obligations.

The following Aviva Loss Prevention Standards provide further guidance.
Business Continuity Management
Business Continuity - Communications
Business Continuity - Incident Management Plan
Business Continuity - Roles and Responsibilities
Business Continuity Planning - Testing and Maintenance

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

- Fire risk assessment **Cardinus Risk Management.**
- Electrical/Lightning installation testing and explosion/DSEAR Risk Assessments **Bureau Veritas.**
- Thermographic imaging and PAT testing **PASS**
- Automatic detection systems **SECOM**
- Leak detection and prevention - **Leaksafe**
- Leak detection and prevention – **Quensus**
- Flood protection Services - **Apex Flood Solutions**
- Flood risk management - **Ashfield Solutions**
- Flood risk assessments - **JBA Consulting**
- Business Continuity - **Horizonscan**

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

Additional Information

Relevant Aviva Loss Prevention Standards include:

- **Data Centres – Planning and Design**
- **Data Centres – Construction**
- **Data Centres –Detection and Fire Protection**
- **Data Centres – Cooling and Ventilation**
- **Data Centres – Fire and Smoke Resilience**
- **Escape of Water and Other Fluids**
- **Escape of Water – Installation and Maintenance**
- **Escape of Water – 10 Top Tips**
- **Escape of Water – Responding to Incidents**
- **Escape of Water – Water Management Planning**

- **Work on Wet Systems**
- **Self-Inspections**
- **Use of Thermographic Cameras - General Considerations** and **Checklist**
- **Heat and Smoke Venting Systems**
- **Managing Change - Property**
- **Emergency Response Planning**
- **Maintenance Regimes**
- **Small Scale Battery Energy Storage Systems**
- **Planning a Battery Energy Storage System - 12 Top Tips**
- **15 Top Tips for Roof Mounted Photovoltaic Solar Panel Systems**
- **Emergency Response Planning with Fire and Rescue Services**
- **Business Continuity Management**
- **Business Continuity - Communications**
- **Business Continuity - Incident Management Plan**
- **Business Continuity - Roles and Responsibilities**
- **Business Continuity Planning - Testing and Maintenance**

To find out more, please visit Aviva Risk Management Solutions **or speak to one of our advisors.**

Email us at riskadvice@aviva.com or 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.

17th April 2026

Version 1.0

ARMSGI4072026

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.