Loss Prevention Standards – Asset Classes

Data Centres – General Overview and Design Considerations

Version: 1.0

Date: 21st February 2025

The safe and effective management of data is important to all organisations, many of whom will sub-contract the management of critical data to third party data centre facilities or operate their own data centres.

This Loss Prevention Standard provides an overview of the main data centre processes, key equipment, and design considerations.

Data Centres - General Overview and Design Considerations

Introduction

Data centres are used for the housing of critical computer hardware and ancillary equipment for the processing, management, and storage of data, and other related systems and applications including telecommunications.

The first dedicated data processing and storage facilities were developed in the 1940's. The presence of very large main frame units with supporting infrastructure and air cooling requirements required specialised environments with raised floor and ceiling voids to house cabling and ventilation/cooling ducting.

Whilst these systems reduced in size, the increased deployment and use of computers across all industries in the 1980's, and the rapid growth in internet commerce in the 1990's and 2000's resulted in organisations utilising the services of data centres for the storage and management of their data. In more recent times the sector has moved towards colocation facilities, to improve efficiencies.

Whilst major property damage events within data facilities are uncommon, the consequences can be significant. Three lives were lost in a fire at the Khawaja Tower building in Bangladesh in October 2023. The fire also destroyed numerous data centre facilities within the buildings with around 40% of Bangladesh's 12 million internet users effected.

A fire at the Paris Global Switch data centre in April 2023, attributed to a water leak in a cooling system infiltrating the battery room, resulted in significant data loss including government websites and cloud services in the area.

A fire in a one of Europe's largest cloud providers data facilities in Strasbourg in March 2021 destroyed one of the four data centres and significantly damaged another, severely impacting data services and resulting in successful third-party claims for damages.

This is one in a series of Loss Prevention Standards which provide risk management guidance in respect of data centres. This document provides an overview of the main activities, management controls, critical processes, and equipment within most data centres, along with design recommendations to help improve resilience of the building and it's infrastructure. Other standards in this series are **Data Centres – Hazards and Ongoing Care** and **Data Centres – Fire Detection and Protection**.

Note: This document relates to data centres. It is not for on-site data processing and storage facilities, typically provided within business premises to support other trading activities, however, refer to Aviva Loss Prevention Standard **Server/Comms Rooms** for further guidance on such facilities. This document focusses on Property loss prevention and related risk management guidance and is not intended to address Business Interruption or Liability exposures. The presumption is that all regulatory requirements, such as Fire Risk Assessments, have been met.

Types of Data Centre

Data centres can be either managed in house, whether at individual sites or at centralised locations, or outsourced to third party providers. Types include, but are not limited to:

Co-location Data Centres. Standalone data facilities, typically owned and operated by third-party suppliers providing space and IT infrastructure but allowing organisations to use their own hardware.

Managed Services Data Centres. Managed services data centres are owned and operated by third-party suppliers to provide full data management support.

Largescale Data Centres. Very large facilities used by the main technology companies to support rapid cloud based service to individuals and organisations.

Other cloud based centres are also available providing on-demand access to computing resources, storage, and applications over the internet.

Data Centre Equipment

The equipment found in data centres commonly comprises:

- **Server Racks**. Servers process, store, administer and manage data. Data centres typically feature large halls, often over multiple floors, with extensive arrays of servers within cabinet racking.
- **Network Infrastructure**. The network system connects server equipment used for processing and storing data within the centre and also to other connected data centre facilities as well as end-user locations.
- **Cooling Systems**. Server equipment generates significant heat, which needs to be removed from the facility and replaced or blended with cool incoming air to maintain constant temperatures, typically in the region of 21° to 24° Celsius. The cooling system capability and performance is critical to the management of a data centre.
- **Other Systems**. Electrical installations; telecommunications; security hardware; fire detection and fire protection systems etc.

Management Policy and Standard Operating Procedures

A management policy should be in place detailing the key management arrangements. Where the data centre is third party managed, a copy of the management policy should be obtained and reviewed.

- Information within the management policy should include key responsibilities; security access; monitoring; maintenance and inspections; contingency planning; training and emergency arrangements etc.
- Standard Operating Procedures (SOPs) detailing the arrangements highlighted within the management policy, should be in place and subject to regular review.
- The use of clear rules and procedures helps to ensure consistent and safe processes and procedures are followed by relevant workers/persons, reducing the risks of unplanned and unexpected fire or other property damage events, and mitigating the losses associated with poor or unclear emergency planning.
  - ✓ The management policy should include standards for replacement components and equipment that are acceptable for use in the data hall.
    - Standardized components ensure compatibility and reduce the risk of failures, helping reduce the risks of downtime.
    - Using standardized equipment can help ensure all components work correctly together, optimizing performance and reducing energy consumption.
- There should be a clear reporting and escalation policy for data centre workers and other relevant persons to report incidents or issues involving property damage including compromised fire protections; cooling irregularities, unsafe or unauthorised activities; security arrangements/security breaches; water ingress however minor; inappropriate storage etc., to a responsible person within the business for immediate review.

Data Centre Design

Consideration to the design and layout of the facility is essential in reducing loss potential.

Fire Resistance

Modern data centre buildings are often multi floored with each floor housing a data hall, ancillary rooms, and services e.g. cooling, comms, control, battery rooms etc. The building should be designed to prevent the spread of fire between compartments via the use of fire resisting construction.

The building should be of non-combustible construction providing a fire resistance rating (integrity and insulation).

External walling should provide at least 60 minutes fire resistance (insulation and integrity).

- ✓ Where external wall cannot achieve 60 minutes fire resistance, the area directly in front of the wall, extending to at least 10 metres, should be maintained clear of combustible materials, vehicle parking and/or infrastructure such as generators, plant buildings, vehicle chargers etc.

Internal walling between the data hall and other internal areas of the floor should provide at least 120 minutes fire resistance (insulation and integrity).

- Internal walling of low risk areas external, remote and not connected to data halls e.g. offices, stores etc., may not need to achieve fire resistance ratings in excess of national requirements, standards, or codes, however at least 60 minutes fire resistance is recommended.
- In the United Kingdom and Ireland **LPS 1208: LPCB Fire Resistance Requirements for Elements of Construction used to Provide Compartmentation** provides guidance on achieving fire resistance ratings.
- Installers should be competent and preferably accredited to an installer standard, such as **LPS 1500: Requirements for the LPCB Approval and Listing of Companies Installing Construction Elements used to Provide Compartmentation in Buildings** in the United Kingdom and Ireland.

Supporting steel framework should achieve the same fire resistance rating (insulation and integrity). This is typically achieved via encasing with concrete or the use of intumescent protective coatings.

- Systems should be tested and certificated to a recognised standard, such as EN1364, EN1634 and/or classified in accordance with **EN 13501-2/BS EN 13501-2 : Fire classification of construction products and building elements - Classification using data from fire resistance tests, excluding ventilation services**.
- In the United Kingdom and Ireland, **LPS 1107: Requirements, tests, and methods of assessment of passive fire protection systems for structural steelwork** provides an approval standard for non-intumescent coatings.
- Application of Intumescent coatings should be in accordance with a recognised standards, such as **ASTM E2924-14(2020) Standard Practice for Intumescent Coatings**.

Internal openings between the data halls and other internal areas e.g. doors, ducts and viewing windows, should be fitted with automatically operating fire doors/shutters providing a fire resistance rating commensurate with the data hall areas. At least 120 minutes fire resistance (insulation and integrity) is recommended.

- In the United Kingdom and Ireland fire shuttering should be certificated to LPCB Loss Prevention Standard - **LPS 1056: Requirements for the LPCB Approval and Listing of Fire Door-sets, Lift Landing Doors, and Shutters**.
- The installation of fire shutters and fire doors should be completed by a reputable and accredited company, such as those certificated to LPCB Loss Prevention Standard **LPS 1271: Requirements for the LPCB Approval and Listing of Companies Installing Fire or Security Doors, Door-sets, Shutters and Active Smoke/Fire Barriers** in the United Kingdom and Ireland.

Internal compartment flooring should provide at least 120 minutes fire resistance (insulation and integrity).

Openings for cabling and pipework etc., between fire compartments should be adequately fire stopped and/or fitted with intumescent collars or fire dampers to achieve a fire resistance rating commensurate with the fire compartment wall or floor.

- Ensure the fire resistance integrity of the compartment is maintained in the event of ignition.
- Intumescent collars should be used to protect pipework which could collapse or melt in the event of fire filling any voids created and providing a fire barrier.
- Installation of other passive fire protection products such as fire stopping should be completed by a company certificated to LPCB Loss Prevention Standard - **LPS 1531 Requirements for the LPCB approval and listing of companies installing or applying passive fire protection products**.
- The use of intumescent pillows for temporary fire stopping around service openings is not recommended.

Raised/suspended flooring should also be of non-combustible construction e.g. concrete based flooring materials achieving a classification of A1 or A2 under **EN 13501-1/BS EN 13501-1 Fire Classification of Construction Products and Building Elements - Classification Using Data from Reaction to Fire Tests**.

Floor and ceiling voids should not breach any fire compartmentation strategy/planning.

- Insulation materials used in any roofing system should also achieve a classification of A1 or A2 (non-combustible) under **EN 13501-1/BS EN 13501-1 Fire Classification of Construction Products and Building Elements - Classification Using Data from Reaction to Fire Tests**.

Note: An increased fire resistance rating in excess of 120 minutes may be required with national standards, regulations, or codes, or as stipulated within the premises Fire Risk Assessment.

Refer to Aviva Loss Prevention Standards **Fire Compartmentation** and **Fire Doors, Shutters and Dampers** for further guidance.

Redundancy

The data centre processing/storage facility should be designed to provide sufficient back-up arrangements that can take over immediately should the primary system fail. This can help reduce the impact of outages, ensuring that services remain available, and downtime is minimised. There are two redundancy strategies normally considered within data centre facilities:

2N – Refers to a fully mirrored system with independent power and distribution systems. If one facility fails, the mirrored system should immediately activate and limit any potential downtime. These are generally considered the most robust redundancy system with a highest fault tolerance however requires significant cost to establish, operate and maintain, and is the approach typically followed by data centres in respect of data storage and processing equipment.

N+1 - If N equals the capacity needed to run the facility, N+1 indicates an additional component added to support a single failure or cover downtime for maintenance. This is generally considered a simpler and more cost effective redundancy strategy and is typically employed for supporting systems such as UPS, monitoring, generators, or generator start up equipment etc.

It is important to include other associated systems such as heating, cooling, air handling, fire protections etc., when considering redundancy arrangements.

Conducting a risk assessment can help identify such systems, their potential vulnerabilities or those where single points of failure exist. These risks should be prioritized, based on their potential impact, and redundancy management strategies developed to mitigate their potential to cause downtime, loss or damage.

Regardless of the strategy employed, the critical data requirements should have sufficient backup to minimise interruptions to trading activities.

Cabling

Most cabling will feature polymer insulation which can be combustible and produce harmful smoke in a fire event. To help reduce the potential for cable related fire damage, fire resistant cabling should be used wherever possible, or fire retardant cabling where a fire resistant option is not available.

Refer to Aviva Loss Prevention Standard **Data Cabling** for further guidance.

- Implementing a cable management plan for ethernet, fibre-optic, power, and patch cables can prevent electrical shorts and fires.
  - ✓ This includes organizing cables neatly, conducting regular inspections, and timely replacement of frayed or damaged cables.
  - ✓ Cabling should be minimized in floor and ceiling voids and ideally limited to fire detection related cabling only.
- Following any works, all redundant and legacy cabling should be removed, and any openings fire-stopped to the same fire resistance rating as the data processing and storage facility.

Efficiency

- Stressing the systems can contribute to breakdowns, longevity issues and performance concerns.
  - ✓ Where possible increasing the capacity of data equipment and servers etc. thereby reducing the operating requirements of each component in the system can reduce the potential for breakdown etc., as well as reducing replacement, repair, and cooling costs. This should be factored into the system design.

Cooling/Environmental Controls

Date centres require intelligent cooling, ventilation, and humidity control to maximise system performance and reduce the potential for damage to sensitive server equipment.

The recommended temperature for data halls is between 21° to 24° Celsius, and fluctuations in processing power usage significantly impact the heat generated. As such, the cooling systems need to adapt swiftly to maintain constant temperatures.

Ambient relative humidity levels of between 45% and 55% are recommended for optimal performance, however this can fluctuate depending on local air conditions. Low humidity can lead to electrostatic discharge and high humidity can lead to condensation build up and the associated corrosion and shorting.

Air Cooling

Most data centres utilise air cooling technology. The systems work by removing heat from the circulating air and replacing with cooler air. This is typically done in one of two ways:

- Removing/extracting hot air and replacing with drawn in air, which is cooled (unless already sufficiently cold) and circulating through the data hall.
- Recycling air within the data hall by cooling it, typically via a 'hot and cold aisle' system.

Most data centres utilise Computer Room Air Conditioners (CRAC) or Computer Room Air Handlers (CRAH) to deliver cold air within a raised floor. As the pressure below the raised floor increases, cold air is pushed out and into the equipment inlets. The cold air displaces the hot air, which is then returned to the CRAC or CRAH, where it is cooled and recirculated.

To aid efficiency of air cooling systems, most server cabinets are configured into hot and cold aisle arrangements. The cabinet rows face other in opposite directions so that cold intake and hot air ventilation create alternating aisles of cold and hot air, enabling hot air to be vented via the hot aisle and cold air delivered in the cold aisle.

Evaporative Cooling

Evaporative cooling is a method of cooling air without the use of refrigerants. The system works by passing air across wet filter pads, where the evaporation process cools the air and is then ducted around the data hall. Heat exchangers may be employed in more complex systems to isolate the cooling process from the air delivered into the data hall.

Evaporative cooling is most commonly used in warm and dry environments with low relative work humidity and is a very energy efficient and environmentally friendly method of cooling.

Other

Other cooling systems are available, including liquid cooling systems; geothermal cooling which use the natural cool temperatures of the earths substrata to cool agents within closed loop systems; solar cooling, all of which are relatively new technologies and outside of the scope of this document.

- ✓ The system should be designed and the cooling requirements, calculated by a competent person or firm.
- ✓ The cooling systems designer and the installers of any fire detection and fire protections should consult to ensure the air movements within the data processing/storage facilities do not impact performance of the fire systems.

Cooling/Environmental Monitoring Systems

- **Environmental monitoring**. These systems are essential in managing the cooling processes and reducing the risks of breakdown, leaks, overheating and other damage. Monitoring should include:
  - ✓ **Temperature monitoring**. Temperature probes should be present throughout the racks at varying heights to ensure the most accurate monitoring.
  - ✓ **Coolant flow and return temperatures**. Ensures unusual high temperatures are identified for rectification.
  - ✓ **Differential air pressure monitoring**. Poor air pressures and air flow within server racks can reduce cooling efficiency, typically as a result of poor containment e.g. missing or poorly fitted panels.
  - ✓ **Humidity monitoring**. Helps avoid excessive condensation, corrosion, electrical shorting and mould accumulation, all of which can lead to damage or loss.
  - ✓ **Electrical current monitoring**. Power related faults can cause disproportionate levels of damage and outage. Continuously tracking and analysing the flow of electrical current to the various components and systems within the data centre can help reduce the potential for such damage. Monitoring should include real time monitoring, residual current leaks and load balancing.
  - ✓ **Leak monitoring.** Water accumulation or ingress can occur due to excessive humidity and escape of water and cooling fluids where present. Water leakage sensors are essential in detecting such issues and should extend to all areas of the data hall including concealed floor and ceiling voids/plenums.
- Monitoring systems should be subject to maintenance, checks and calibration as per Original Equipment Manufacturers (OEM) or installer guidelines.

Important: Any false ceilings or screens installed to reduce room height and improve efficiency of cooling systems should not obscure/impair fire detection or fire protection systems.

Key Action Steps

- Ensure the data centre has an appropriate fire resistance rating (insulation and integrity).
  - ✓ Your Property Insurer and Broker can provide guidance in this regard.
- Cooling and ventilation systems should be designed specifically for the server and other IT equipment within the data halls based on the planned equipment.
  - ✓ Ensure the systems can accommodate reasonable changes to layout and additional equipment.
- Monitoring should be in place in respect of cooling and environmental systems with response procedures formalised.
  - ✓ Redundancy should be considered for communications systems.
- Redundancy/back-up arrangements should be designed to provide sufficient back-up arrangements that can take over immediately should the primary system fail.
  - ✓ Fully mirrored systems with independent power and distribution systems are recommended in most cases.

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, including:

- Fire risk assessment: **Cardinus Risk Management**
- Electrical/Lightning installation testing and explosion/DSEAR Risk Assessments: **Bureau Veritas**
- Thermographic imaging and PAT testing: **PASS**
- Automatic fire detection and portable extinguishers: **SECOM**
- Business continuity: **Horizonscan**

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

Sources and Useful Links

- LPS 1531: Issue 1.2 Requirements for the LPCB approval and listing of companies installing or applying passive fire protection products.
- EN 13501-1 Fire classification of Construction Products and Building Elements - Classification Using Data from Reaction to Fire Tests.
- BS EN 13501-2:2016 - Fire classification of construction products and building elements - Classification using data from fire resistance tests, excluding ventilation services
- LPS1208: LPCB Fire Resistance Requirements for Elements of Construction Used to Provide Compartmentation
- LPS 1500: Requirements for the LPCB Approval and Listing of Companies Installing Construction Elements Used to Provide Compartmentation in Buildings
- ASTM E2924-14(2020) Standard Practice for Intumescent Coatings

Note: Whilst UK standards and legislation are referenced in this document, other international standards and legislation should be referenced where applicable.

Additional Information

Relevant Aviva Loss Prevention Standards include:

- **Data Centres – Hazards and Ongoing Care**
- **Data Centres – Fire Detection and Protection**
- **Fire Safety Legislation.**
- **Heat and Smoke Venting Systems.**
- **Managing Change - Property.**
- **Managing Contractors.**
- **Business Continuity.**
- **Power Outage.**

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.

Please Note

21st February 2025

Version 1.0

URN - ARMSGI2192024

Aviva Insurance Limited, Registered in Scotland Number 2116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.