



XL Risk Consulting

From Traditional to AI Data Centers: Emerging Risk Exposures and Best Practices for Risk Managers

An AXA XL Risk Consulting Whitepaper



Welcome to the comprehensive guide on Emerging Risk Exposures in Data Centers, and Best Practices for Risk Managers

This technical paper is designed for insurance professionals, risk managers, data center operators, and engineers who seek to deepen their understanding of the critical factors influencing data center risk assessment and underwriting. Whether you’re evaluating the unique challenges of traditional, AI, or hyperscale data centers, this document provides detailed insights into design, operational, and risk mitigation strategies essential for protecting these vital infrastructure assets. By leveraging this knowledge, you can better assess potential exposures and develop robust risk management solutions tailored to the evolving landscape of data center technology.

Contents

- 3 [Introduction](#)
[Data Center Types and Classifications](#)
- 4 [Loss Exposures and Natural Catastrophe Risks](#)
[Construction and Building Envelope Considerations](#)
- 5 [Utility Support Systems and Critical Infrastructure](#)
- 7 [Data Hall and Support Equipment Arrangements](#)
- 8 [Storage Areas and Hazardous Materials Management](#)
[Fire Protection and Suppression Systems](#)
[Surveillance and Security Measures](#)
- 9 [Property Loss Scenarios and Damage Assessment](#)
- 10 [Business Interruption and Continuity Planning](#)
- 11 [Conclusion](#)



Introduction

Data Center (DC) operations are supported by power and data cable networks, UPS units, server racks and mechanical & electrical infrastructures, with determined redundancy. Redundancy is critical with this occupancy due to potential business interruption losses which could exceed property losses. In order to understand up and down stream loss effects an in-depth analysis of the business model should be conducted.

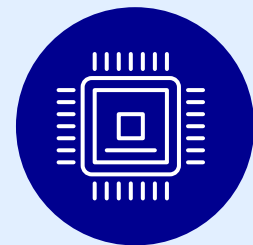


Data center types and classifications

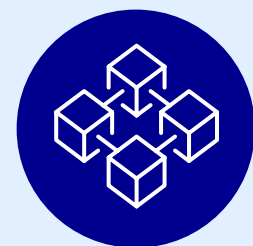
Data Center Types

- **Data Center:** Designed to process, manage and store data with the aid of server and networking equipment. Examples of operations consists of website hosting and running program applications.
- **AI Data Center:** Specialized to support artificial intelligence operations that may include unit or chip learning and deep program training and deployment of learning models and/or algorithms. The AI data center may employ a frontend operation which defines the network framework and a backend AI training operation, which may consist of numerous racks occupied by spines, leafs, and GPU servers. Training involves breaking data into smaller flows through many parallel process cycles and across the network fabric (spines, leafs and GPUs).

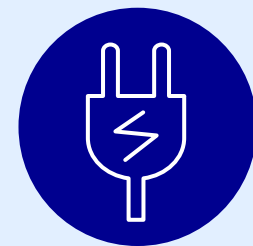
Data Center vs AI Data Center



Computational Power: Traditional data centers primarily rely on CPUs, which are sufficient for general workloads. AI data centers require high-performance GPUs, TPUs, or NPUs to handle the parallel processing demands of AI models, enabling faster training and inferencing.



Storage and Networking: Required storage for AI operations is massive and far exceeds that of the traditional data center. AI networking is designed for low-latency and high throughput.

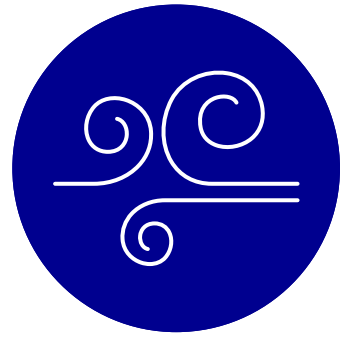


Energy and Climate Control: AI learning and operations require far more energy and cooling.

DC Classifications

- **Hyperscale (or Enterprise Hyperscale)**
Owned and operated by the company it supports. Often used for large scale cloud storage. This is significantly more common with AI data centers.
- **Colocation**
One data center owner selling space, power and cooling to multiple enterprises.
- **Edge**
Operated by colocation service providers, built for versatility and speed. Distinct by its location and connectivity, these are typically positioned in growing markets or on the outskirts of existing networks. Edge DCs allow companies to have real-time data handling, and improved performance for applications that require quick response times such as autonomous vehicles, augmented reality, and real-time analytics.
- **Modular**
Prefabricated units, rated at 1,000 volts or less.

Loss exposures and natural catastrophe risks



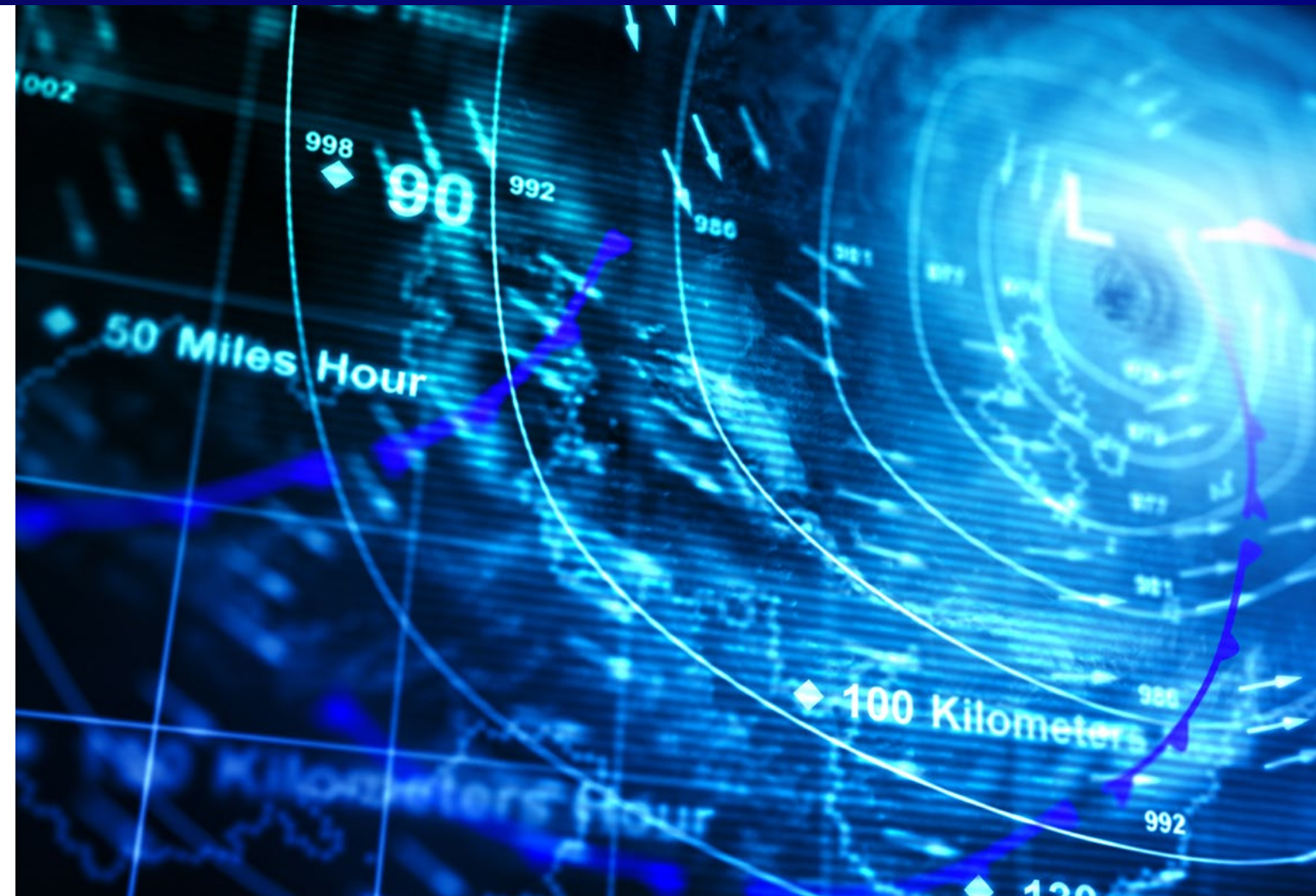
NatCat exposures for single and multiple building campuses should be considered:

- **Windstorm:** Design buildings, roofs and ground mounted equipment to resist maximum anticipated wind forces in accordance with local building design standards and/or account agreeable standards.
- **Flooding:** Avoid locations that are susceptible to flooding from either natural or man-made sources.
- **Earthquake:** In areas of known earthquake activity, design earthquake-resistant structures and provide seismic bracing and anchoring for all fire protection system components and data processing equipment.
- **Exterior fire:** Air supplies may be a concern in regions with possible exposure to forest or field fires or from industrial operations in the area. This includes on-site outdoor fires.
- **Social/Political:** Although not truly a NatCat exposure, consideration should be given to terrorism, civil disorders, labor unrest, and events which could influence or reduce workforce.
- **Wildland and Urban Interface:** Impact on wildlife, waterways, runoffs, and neighboring communities.



Data hall, support equipment, and storage within a data center are vulnerable to:

- **Heat:** Permanent heat damage can begin at temperatures as low as 125°F (52°C).
- **Smoke:** Smoke particles can lead to erratic equipment behavior.
- **Corrosive Fume Contamination:** Hydrogen chloride gas is generated during the breakdown of PVC insulation and if exposed to moisture becomes hydrochloric acid.
- **Water:** Although subject to damage, solid-state equipment is not as prone to destruction by fresh water. Avoid routing non-sprinkler water and drainage pipes in critical areas.



Permanent heat damage to data hall and support equipment can begin at temperatures as low as 125°F (52°C).



Construction and building envelope considerations

Building Envelope

Materials used or installed should be inherently noncombustible. If this is not practical, then use materials listed by an acceptable laboratory.

Interior Separation

Provide at least 1-hr. fire rated full height (from structure floor to structure ceiling above) interior partitions, ceilings and floors for the data halls, offices, and network, UPS, storage, mechanical and electrical rooms. Doors to the area should consist of automatic closing and latching fire resistive doors with a minimum ¾ hr. fire rating.

Utility support systems and critical infrastructure

Electrical

This includes transformers, transfer switching stations, circuit breakers, generators, UPSs, PDUs, RPPS, cabling, etc. In order to maintain continuous and uninterrupted operations, these features may be required for a high-quality and reliable power supply. With added equipment, comes added exposures. In order to reduce potential losses, adequate redundancy, protection features, precautions, SOPs, maintenance and testing programs should be inclusive and well established.

Features that should be analyzed:

- Primary and secondary supplies, including Battery Energy Storage Systems (BESS).
- Distribution of power
- UPS sources, including battery location and chemistry*
- Availability of spare equipment and services

**Lithium-ion (Li-ion) BBU/UPS systems offer several advantages over the VRLA batteries including quicker installation, smaller occupied area, less maintenance, greater power and longer life. Li-ion BBU/UPSs may be centralized or located within individual server racks. With the advantages associated with Li-ion, there are some inherent hazards, including thermal runaway and the release of dangerous gases. In order to reduce the potential hazards, a combination of active and passive controls should be integrated in the BMS.*

Data Transmission

Data transmission network technologies used in most DCs consist of:

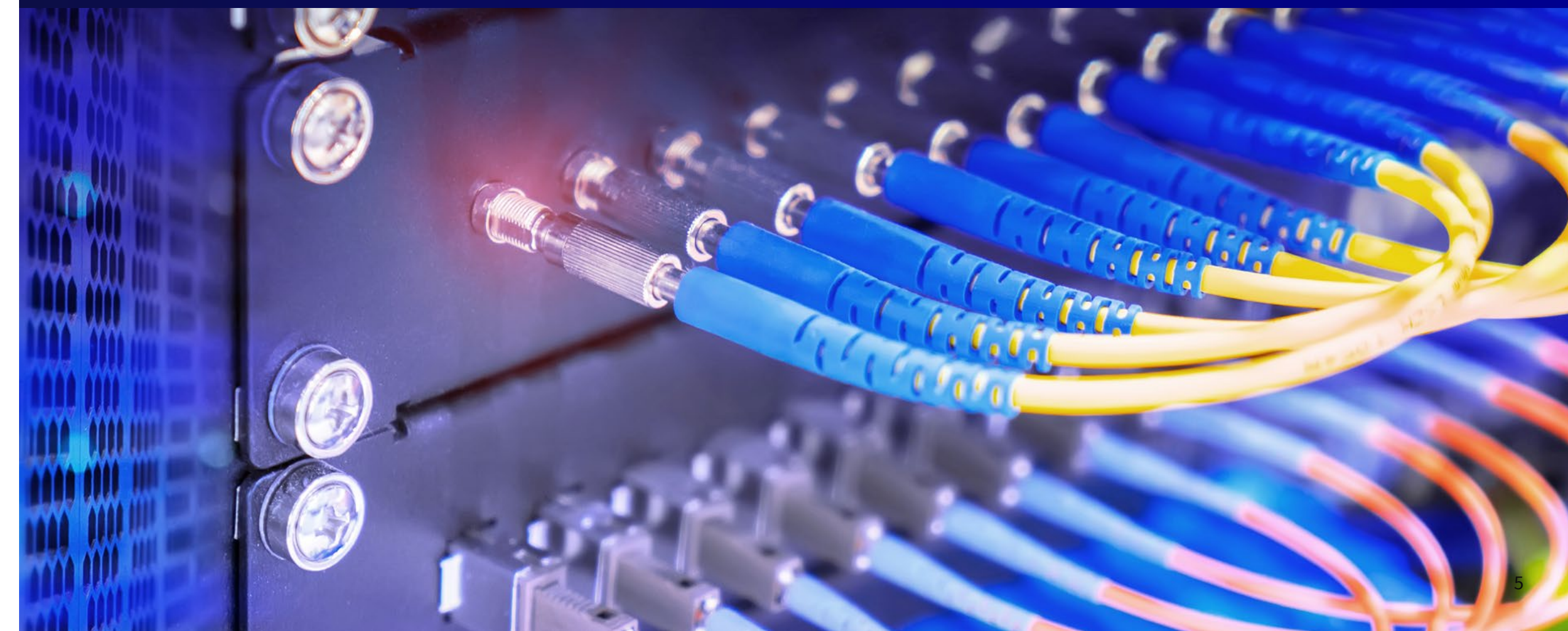
- Fixed-line networks: Utilizing copper and/or fiber optic cables. This technology may require the assistance of IP addresses, DNS servers, amplifier, cell towers, routers, etc.
- Mobile/wireless networks: Signals are transmitted via satellite or antenna.

Features that should be analyzed:

- Transmission supplier, reliability and security
- Configuration both to the site and on premises
- Supplier and/or 3rd party support, maintenance and service
- From a root factor in a well-designed system to catastrophic event for a stand-alone platform, understanding of each system is a critical factor for developing and implementing the appropriate plans and procedures.



In order to reduce potential losses, adequate redundancy, protection features, precautions, SOPs, maintenance and testing programs should be inclusive and well established.



Utility support systems and critical infrastructure (continued)

Climate Control

A critical feature in the data halls and is responsible for > 35% of the energy consumption. These systems should be designed for proper load and redundancy, where needed. Operational equipment in data halls generate elevated heat loads. This exposure needs to be controlled to reduce the possibility of equipment failure. Climate control systems come in various forms:

- **CRAC/CRAH Air Handlers:** Computer Room Air Conditioner (CRAC) (and Computer Room Air Handler (CRAH) systems. Each employ air filters, cooling coils and fans. CRAC units remove the heat by forcing warm air over the cooling coils filled with refrigerant while CRAH units utilize water in the coil as a heat sink and require more equipment in the operating process.
- **Free Cooling:** Ambient air is filtered, cooled, and humidified by evaporative coolers. The air will enter the data hall aisle containment configuration. Hot air is drawn out of the area by fan. There are some limitations to this system since it can only be used in certain regions where the ambient conditions are met.
- **Heat Wheels/Heat Exchangers:** Like free cooling; however, the filters and evaporative cooling are replaced by heat wheels/heat exchangers which allows thermal energy to be transferred from one stream to another.
- **Liquid Immersion:** Components are completely submerged in the heatsink liquid (ex. Dielectric fluid, mineral oil, water, etc.) for cooling.
- **Liquid Cooling:** Liquid (usually water or specialized coolants) is circulated through cold plates or heat exchangers attached directly to hardware components such as CPUs, GPUs, or server racks.



Features that should be analyzed include:

- Primary and secondary cooling medium supply.
- Availability of spare equipment and services.
- Means of aborting and/or directing cooling air during an alarm condition.
- Fan arrangements that will spread contaminants through equipment. Hydrogen chloride generated by burning cable and wiring insulation is a major concern.
- Intake and exhaust should be separated to reduce the possibility of outside recirculation.
- Intake should be separated from generators or other features that could affect the air quality to the data hall.
- If liquid immersion or liquid cooling is used an alarm indicating fluid leakage should be provided.

Building Management System

All aspects of operation, support and protection should be monitored in a designated area on site.

Features that should be analyzed include:

- The system is continuously monitored and controlled by well-trained personnel. These individuals should have the authority to control and override various systems in order to reduce potential losses.
- Power isolation of the data hall and climate control systems minimizes the potential for reignition and circulation of smoke to sensitive electronic equipment on site. When the fire suppression system operates, the electrical service to the data hall and supporting air-handling systems should be deenergized. If this is not feasible, and in most modern DCs, then the 24/7 fully trained and capable personnel should adhere to strict and appropriate SOPs in the event of an emergency situation.

The system is continuously monitored and controlled by well-trained personnel. These individuals should have the authority to control and override various systems in order to reduce potential losses.



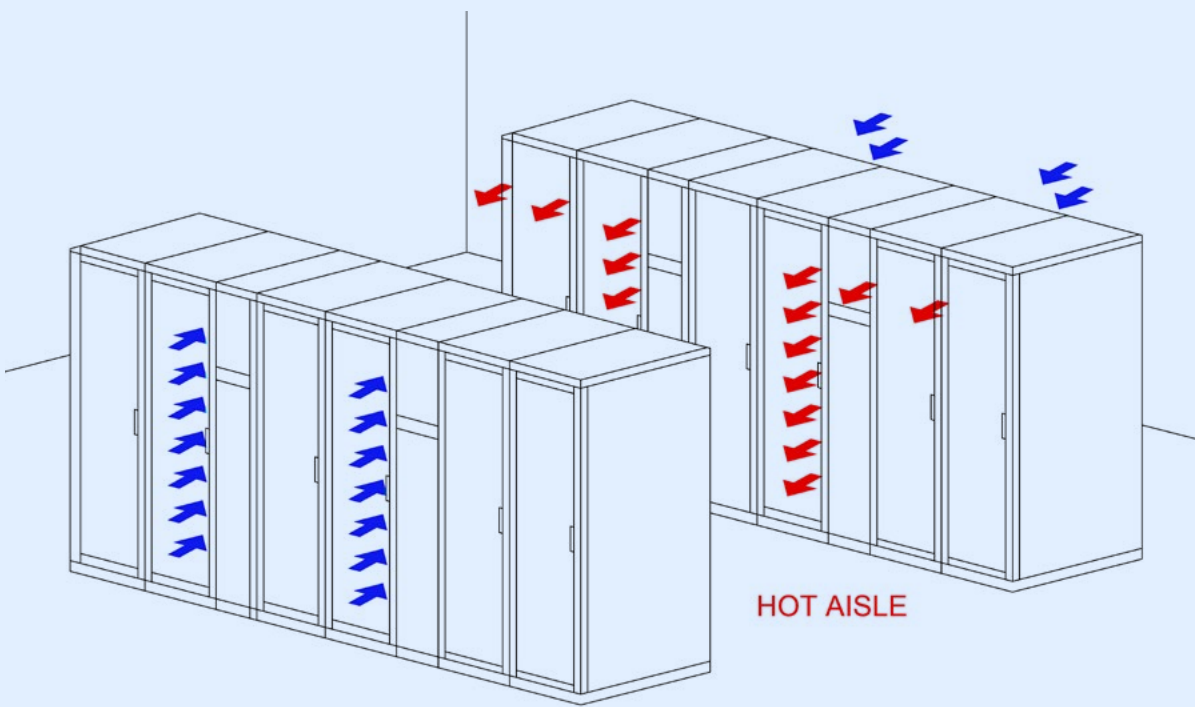
Data hall arrangements

It should be noted that the typical data hall is unoccupied, except during service or maintenance. N+1 access permission and continuously monitored cameras are typically used for security.



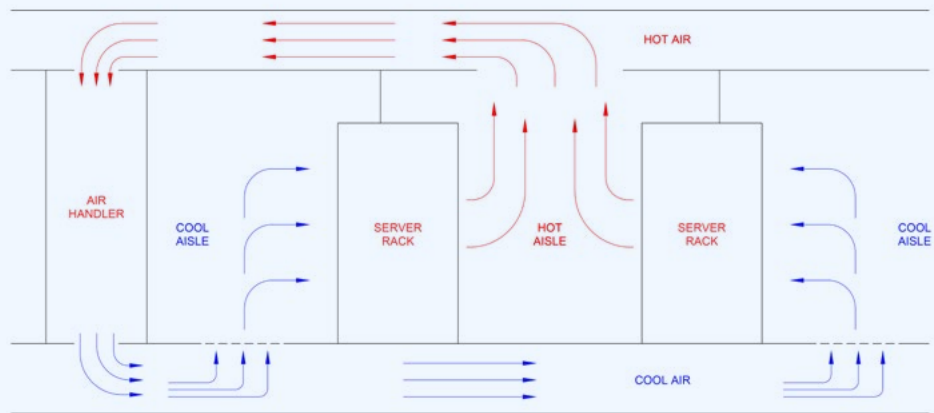
Legacy

Conditioned cooled air from the air handling units is directed below the raised floor, upward through perforated floor tiles, through the racks and back to the air handling units via air circulation below the fixed ceiling, through above ceiling air plenums, or non-combustible duct work.

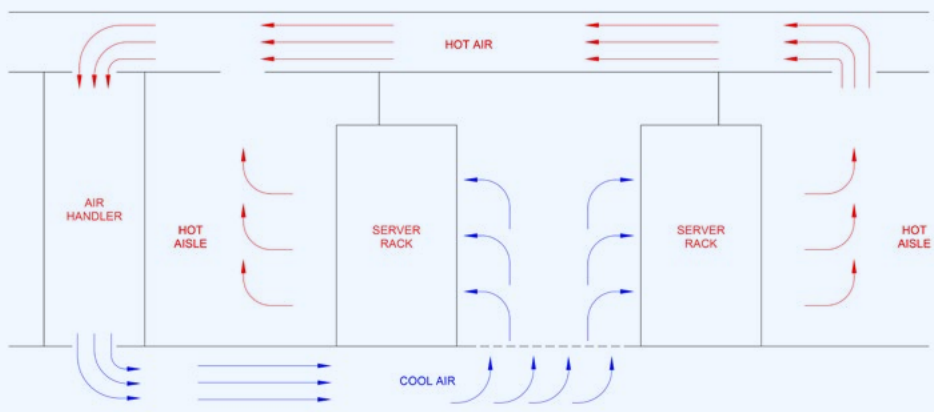


Raised Floor Hot/Cold Aisle

Increased cooling efficiency is provided using this configuration. Containment walls or hot collars may be installed separating the cold from hot aisles.



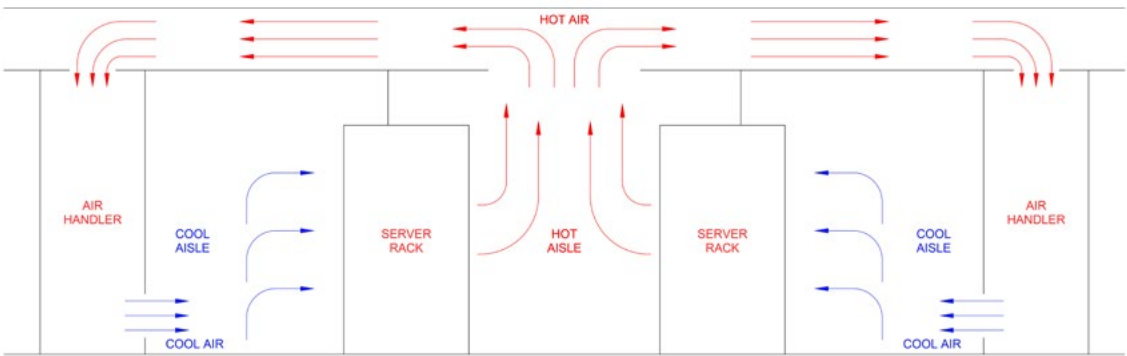
Hot aisle containment



Cold aisle containment

Non-Raised Floor Hot/Cold Aisle

Like the image to the immediate left; however, without a raised floor. This eliminates the hassle of accessibility to below floor utilities and cabling.



Features that should be analyzed include:

- Exposures from or located directly above, below, or adjacent to boilers and/or compressor rooms, hot water tanks, pressure vessels, and operations involving ignitable liquids or hazards materials.
- Pipes containing any liquids or gases should not be routed through or adjacent to the data halls.



Storage areas

Outside the typical storage, including Group A plastics, Li-ion BBUs are a concern. The BBUs are normally delivered from the manufacturer with a 30% charge. If damage or short circuiting should occur, the chemicals inside the BBU begin to heat up which can lead to thermal runaway and an explosion.

- If Li-ion batteries are being used in the BBUs the following features should be analyzed:
- BBUs should be located in a storage area with adequately designed automatic sprinkler protection
- All BBUs not in use should be stored in acceptable Li-ion storage cabinets which are UL listed.
- When outside of acceptable hazardous substance cabinets and not in operation, they should be in acceptable sealed Li-ion battery containers.
- BBUs should not be stored in the data hall.
- SOP should be specific on handling and transport of the BBUs.
- Damaged BBUs should be removed from the building.

Fire protection

Fixed automatic fire protection should be provided throughout the occupied building. Controls and system monitoring annunciators should be readily available and located outside the protecting area. Although there are various acceptable means of providing fixed fire protection, pre-action fire sprinkler systems are most common in modern data halls. These systems should be designed and installed based on an Ordinary Hazard Group I occupancy as addressed in NFPA 13, Standard for the Installation of Sprinkler Systems. However, if Li-Ion BBUs are within the racks, then the sprinkler design density should be reinforced.

Note: The pre-action sprinkler system should incorporate single-interlock activation utilizing fixed photoelectric smoke detection or air sampling. If a double-interlock system is used the design area should be increased by 30%. In addition, the pre-action sprinkler piping should be filled with nitrogen.

For energized electrical equipment provide carbon dioxide or clean agent fire extinguishers.

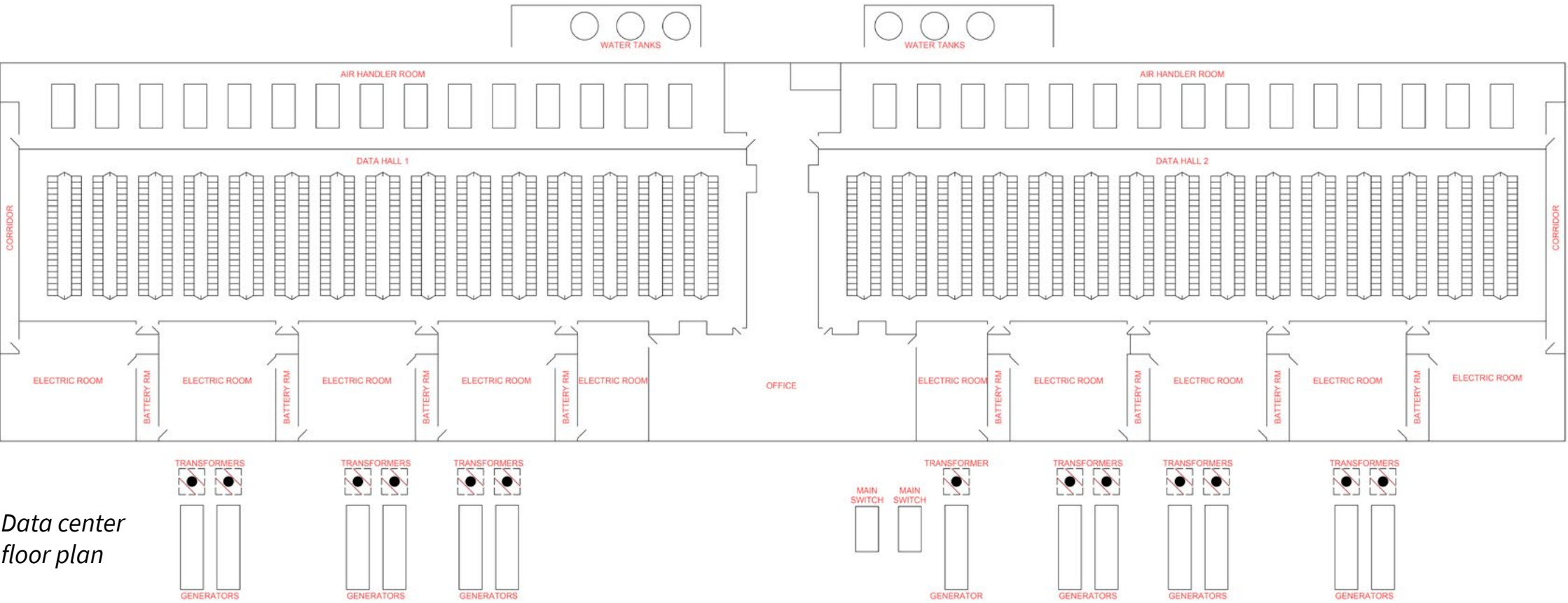
Surveillance/security

Early detection and prompt response from personnel are vital in avoiding serious damage to electronic equipment. The following supervisory service combination is recommended.

- A constantly attended fully addressable fire alarm system including, but not limited to, sprinkler water-flow and early warning smoke detection.
- Standard, recorded, hourly guard rounds during periods when the DC may be unoccupied, or provide an acceptable fully addressable central station signaling system and video surveillance.
- Water leak sensors should be provided below all liquid cooled and cooling equipment in and around the data hall and monitored by a continuously attended signaling system.
- Use a secure access system at entrances to the property, the building, and critical operations to verify employees and visitors.
- Critical areas and operations should remain secured with access granted to only qualified individuals.



Property loss scenarios and damage assessment



The above diagram closely represents the general layout of a modern non-raised floor data center, with 2 data halls. The data halls, networking rooms, electrical rooms, air handler rooms, storage rooms, loading dock and office areas are separated by 1-hour fire rated barriers extending from the concrete floor to the underside of the roof deck. Barrier penetrations are protected by automatic closing 1-hour fire rated doors or dampers. The dampers are activated by the fire alarm system. The data halls and networking rooms are accessible through >2 security clearance means. Automatic closing ¾ hour rated fire doors to all barrier separated areas. Security cameras throughout the buildings.

The data hall cold and hot aisles run in the width direction of the hall. Server racks are commonly 7 ft.

in height. The cold and hot aisles are normally 4 ft. in width. The elements of aisle containment are typically polycarbonate panels supported by light metal framing. Minimal N+1 evaporative air handlers force cooling air into the dedicated data hall through the cold aisles, into the racks, then the hot aisles and through the exhaust fans or regulated louvers back to the data hall, depending on the climate conditions. Room temperature is typically between 65°F and 85°F, with a humidity level between 15% and 80%.

Preferred electrical supply is from two utility feeds from separate grids to a site dedicated substation. The two supplies are separated by automatic/manual transfer switches. A ring supplies power to multiple outside transformers. Between each take-off from the power

supply is an automatic isolation switch and an additional switch for each transformer. The transformers support electrical switchgear rooms. Within each electrical room there are data hall and mechanical systems switchgears. The power from the data hall switchgears is delivered to PDUs for the data halls. The switchgears that support the mechanical systems are equipped with UPS systems, also located in the electrical rooms. This may not be the case for the server racks. UPS systems may be in each individual rack and not in a dedicated electrical room. The UPSs are designed to carry the full load until the associated generator gets up to full speed. Each electrical switchgear feed is supported by a separate generator. The generator network for the data center should be equipped with one or more on-line spare generators.

In a Normal Loss Expectancy (NLE) scenario, which may involve an electrical failure, the ensuing fire, smoke, heat and water damage is contingent on the adequacy of the fixed protection/detection and response from employees and/or first responders. Damage may include servers, electrical and data busways, aisle containment, structural steel and wall and ceiling coverings.

If the data center has a data structure that supports redundant (N+1) operations, the business interruption to the operation or customer, may not be compromised. However, if this is not the case, operations could be interrupted, depending on the availability of equipment.



Room temperature is typically between 65°F and 85°F, with a humidity level between 15% and 80%.



Business interruption and continuity planning

In order to calculate an estimated business interruption, a deep dive into the networks should be performed. There are many aspects to take into consideration when developing a scenario. Below is a limited list of concerns that may trigger additional paths of interest.

Supply Chain Vulnerabilities

- Availability of specialized equipment
- Availability of Chips/CPU/APU/GPU/NPU
- Transit of supplies (weather, workforce, availability, etc.)
- Tariffs
- Political agreements or restrictions

Cyber

- Ransomware
- DDoS attacks
- Insider threats
- Advances Persistent Threats (APTs)
- Malware infections
- Zero-day exploits

Client Support Systems

- 911
- Public safety
- BMS
- DOD
- Healthcare
- Administrative
- Industrial process controls
- Business inventory and financial data
- Self-driving cars
- Traffic controls

Operation

- Alternative means operations
- Future technology R&D
- Market demand and participation
- Qualified contracts, operators, and support





Conclusion

Effective risk management for data centers requires a thorough understanding of technical, operational, and environmental factors. AXA XL’s risk consultants are here to assist you in identifying vulnerabilities and designing tailored solutions to mitigate potential losses.

Contact us today to learn how our expertise can help safeguard your data center assets and ensure business resilience in an increasingly digital world.



axaxl.com

Global Asset Protection Services LLC, XL Catlin Services SE and their affiliates (“AXA XL Risk Consulting”) provide loss prevention and risk assessment reports and other risk consulting services, as requested. In this respect, our property loss prevention publications, services, and surveys do not address life safety or third party liability issues. This document shall not be construed as indicating the existence or availability under any policy of coverage for any particular type of loss or damage. The provision of any service does not imply that every possible hazard has been identified at a facility or that no other hazards exist. AXA XL Risk Consulting does not assume, and shall have no liability for the control, correction, continuation or modification of any existing conditions or operations. We specifically disclaim any warranty or representation that compliance with any advice or recommendation in any document or other communication will make a facility or operation safe or healthful, or put it in compliance with any standard, code, law, rule or regulation. Save where expressly agreed in writing, AXA XL Risk Consulting and its related and affiliated companies disclaim all liability for loss or damage suffered by any party arising out of or in connection with our services, including indirect or consequential loss or damage, howsoever arising. Any party who chooses to rely in any way on the contents of this document does so at their own risk.

AXA, the AXA and XL logos are trademarks of AXA SA or its affiliates. AXA XL is a division of AXA Group providing products and services through three business groups: AXA XL Insurance, AXA XL Reinsurance and AXA XL Risk Consulting. In the US, the AXA XL insurance companies are: AXA XL Insurance Company Americas, Greenwich Insurance Company, Indian Harbor Insurance Company, XL Insurance America, Inc., XL Specialty Insurance Company and AXA XL Excess & Surplus Lines Insurance Company. Not all of the insurers do business in all jurisdictions nor is coverage available in all jurisdictions. Information accurate as of March 2026.

The AXA, AXA XL, AXA XL Insurance, AXA XL Reinsurance and AXA XL Risk Consulting trademarks and logos are registered trademarks of AXA SA. © 2026