RQA Group
Your product risk experts.

Risk Engineering
Report

Data Centres – Understanding Component and BI Risks

August 2026

Wyvols Court, Basingstoke Rd,
Swallowfield, Reading RG7 1WY
United Kingdom
Tel: +44 (0)118 405 0192

www.rqa-group.com

Table of Contents

Data Centres – Understanding Component and BI Risks

Executive Summary

Data centres have become essential infrastructure, supporting financial services, healthcare, government, telecommunications, cloud computing and an increasing number of digitally enabled industries. As reliance on these facilities continues to grow, so too does the potential financial impact arising from damage to the infrastructure that enables them to operate. Whilst physical assets remain important, the operational significance of supporting infrastructure frequently exceeds its replacement value.

This report provides an overview of the principal infrastructure systems found within modern data centres and examines them from an insurance and risk management perspective. It explains how electrical, cooling and network systems support continuous service delivery and identifies the critical components commonly encountered during underwriting and claims. It also considers how failures within these systems can lead to operational disruption and business interruption.

A key finding is that the criticality of a component is not necessarily related to its value. Comparatively inexpensive assets, such as fibre cabling, switchgear, pumps or control systems, may represent single points of failure capable of disrupting services to multiple customers or entire facilities. Conversely, high-value equipment may be installed with sufficient redundancy that its failure results in limited operational impact. Understanding where a component sits within the wider infrastructure, together with the resilience measures designed to support it, is therefore fundamental to assessing risk.

The report also considers the wider factors influencing data centre risk, including third-party dependencies, supply chain constraints, ageing infrastructure, increasing power densities associated with artificial intelligence (AI) workloads, and the growing adoption of liquid cooling technologies. These developments are changing both the physical characteristics of data centres and the operational challenges faced by owners, operators and insurers.

Rather than viewing data centres solely as collections of insured assets, insurers should assess the operational resilience of the infrastructure that supports continuous service delivery. This includes consideration of redundancy, maintenance practices, recovery capability, external dependencies and the potential consequences of component failure. Taking this broader view provides a more complete understanding of the exposure presented by a facility and supports more informed underwriting, risk engineering and claims assessment.

The report is intended as a practical reference for insurance professionals (product recall, product liability, property, business interruption etc), seeking to improve their understanding of data centre infrastructure and the relationship between physical assets, operational resilience, asset failure and business interruption risk. By combining technical explanations with insurance-focused commentary, it aims to support more consistent risk evaluation and encourage consideration of the operational context in which insured assets function.

Setting the Scene – Recent Incidents

A number of relatively recent, major incidents illustrate that data-centre losses have been driven primarily by fire and battery-related electrical failures, with impacts extending well beyond physical plant damage into prolonged service disruption and potential data loss. The OVHcloud Strasbourg fire in March 2021 was one of the most severe in direct physical and financial terms, destroying an entire building, partially damaging an adjacent facility and affecting thousands of customers. It was reported that 3.6 million websites related to 464,000 domain names were unavailable at the peak of the fire. Costs have been estimated to be in excess of EUR 100 million. The cause was initially linked to a faulty uninterruptible power supply (UPS), although this has not been confirmed.

The Kakao outage in October 2022 was presumed to be from a battery-room fire at the SK C&C data centre, causing a nationwide disruption to messaging, payments, mobility, and other digital platforms in South Korea. The Digital Realty Singapore incident in September 2024 and the South Korea government data-centre fire in Daejeon in September 2025 both highlight the growing exposure associated with lithium-ion battery thermal runaway:

In Singapore, the fire reportedly burned for more than 36 hours and affected Alibaba Cloud services, while in Daejeon a battery failure during maintenance appears to have resulted in an explosion and fire that disrupted hundreds of government servers. Another, separate, incident in Daejeon occurred within a week of this incident, where a fire was reported to have been caused by a faulty UPS.

Most recently, the STT GDC / Tata Delhi fire in 2026 demonstrated the scale of customer dependency on third-party colocation infrastructure, with reports of extensive facility damage, prolonged outages, and fears of permanent customer data loss.

Taken together, these cases show that the typical drivers of large-scale data-centre losses are concentrated in electrical infrastructure, backup power systems, and Lithium-ion battery installations, with the largest consequences arising when a local technical failure cascades into a broader operational outage.

Reference Links

1. STT, Tata Delhi data centre fire leaves clients fearing decades of data lost; Google hit, June 2026.
https://www.reuters.com/business/media-telecom/tata-unit-says-extensive-damage-fire-delhi-data-centre-hampers-recovery-2026-06-24/

   Google Cloud – Incident Report, June 2026.
https://status.cloud.google.com/incidents/5fGQt4VbkDnr3Yp8PXPr

2. South Korea scrambles to restore services after major state data centre fire, Sept 2025.
https://www.reuters.com/markets/emerging/south-korea-state-data-centre-fire-knocks-out-online-services-quick-response-2025-09-26/

   South Korea raises cyber threat level after huge data centre fire sparks hacking fears, Sept 2025.
https://www.theguardian.com/world/2025/sep/30/south-korea-raises-cyber-threat-level-after-huge-data-centre-fire-sparks-hacking-fears

3. Second data center in a week catches fire in Daejeon, South Korea. Oct 2025
https://www.datacenterdynamics.com/en/news/second-data-center-in-a-week-catches-fire-in-daejeon-south-korea/

4. Fire at Digital Realty's Singapore data center "under control", Sept 2024.
https://www.datacenterdynamics.com/en/news/fire-at-digital-realtys-singapore-data-center-under-control/

   Firefighting operations at Loyang data centre spill into second day, blaze linked to Li-ion batteries, Sept 2024.
https://www.straitstimes.com/singapore/firefighting-operations-at-loyang-data-centre-spill-into-second-day-blaze-linked-to-lithium-ion-batteries

5. Kakao, SK in blame game over fire at data center, Oct 2022.
https://www.koreatimes.co.kr/business/companies/20221020/kakao-sk-in-blame-game-over-fire-at-data-center?utm_source=legacy_url&utm_medium=redirect&utm_campaign=news_manager_id

   SK Group takes full responsibility for data center fire that led to Kakao outage, Oct 2022.
https://www.datacenterdynamics.com/en/news/sk-group-takes-full-responsibility-for-data-center-fire-that-led-to-kakao-outage/

6. OVHCloud hit with customer class action over March 2021 datacentre fire, Jan 2022.
https://www.computerweekly.com/news/252511906/OVHCloud-hit-with-customer-class-action-over-March-2021-datacentre-fire

   Fire could cost OVHcloud €105 million, IPO filing reveals
https://www.datacenterdynamics.com/en/news/fire-could-cost-ovhcloud-105-million-ipo-filing-reveals/

   The OVHcloud fire still smolders, March 2024.
https://www.datacenterdynamics.com/en/analysis/ovhcloud-fire-france-data-center/

1. Introduction

Data centres underpin many of the digital services that individuals, businesses and governments rely upon every day from cloud computing and financial transactions to healthcare, telecommunications and public services. As society becomes increasingly dependent on uninterrupted digital services, the resilience of data centre infrastructure has become a matter of growing commercial and operational importance.

For insurers, this presents a distinct challenge. While the physical assets or components within a data centre may resemble those found in other industrial environments, the consequences of their failure can be markedly different. The loss of a single transformer, cooling pump, fibre connection or control system may interrupt services relied upon by thousands of customers, generating business interruption losses that are disproportionate to the replacement cost of the damaged asset. Experience shows that the operational impact of an incident is not always determined by the value of the asset damaged; failures involving comparatively low-value components can interrupt services across an entire facility and produce losses that significantly exceed the cost of physical damage.

This report has been prepared to bridge the gap between technical infrastructure and insurance practice. It provides insurance professionals including underwriters, claims specialists, brokers and risk managers with a practical understanding of how data centres function, the assets likely to be encountered during underwriting and claims activities and the operational and business interruption consequences of component failure.

It assumes no prior specialist engineering knowledge and introduces technical concepts only in the context of their relevance to insurable risk, operational resilience and BI exposure.

The report progresses from an explanation of data centre types and supporting infrastructure through to failure mechanisms, business interruption, insurance considerations, third-party dependencies and emerging technologies, concluding with key questions to assist product recall underwriters as well as a practical underwriting framework for property and BI insurers. It is intended as a practical reference guide rather than the basis of an insurance rater model or a data centre design manual or engineering specification.

2. Scope

The report provides a general overview applicable to a broad range of data centre facilities, including enterprise, colocation, hyperscale, edge and other specialist environments. It examines the major engineering systems that enable continuous operations such as electrical distribution, backup power, cooling, telecommunications, monitoring and supporting building services. It also covers the individual components that comprise them, their operational purpose, typical failure mechanisms and the potential impact of damage or failure on service continuity and BI exposure.

In addition to physical infrastructure, the report discusses broader factors that influence data centre resilience, including operational practices, third-party dependencies, supply chain considerations and emerging technologies such as AI infrastructure and liquid cooling. Additional commentary is provided on their relevance to underwriting, risk engineering and claims assessment where appropriate.

The report does not seek to provide detailed engineering design guidance, construction standards, regulatory compliance advice or site-specific or component-specific risk assessments. It also does not cover in any detail security, vandalism or cyber considerations which are major topics in themselves. As individual facilities vary considerably in design, redundancy and operational practice, the information presented should be considered alongside site-specific surveys, engineering assessments and policy requirements.