

LEARISK TECHNICAL BULLETIN

3.26 DATA CENTRES

Identifying the drivers of PML/EML

Data centres: complex assets with concentrated values

Modern data centres combine high-value IT equipment with highly interdependent power, cooling, communications and fire-protection systems. This circular highlights the main factors that can influence property damage, business interruption and overall resilience.

AI facilities introduce higher power densities, greater heat loads and more sophisticated cooling requirements.

True resilience depends on eliminating single points of failure across electrical, cooling and communications infrastructure.

PML and EML assessments should consider fire, emergency shutdown capability and natural catastrophe scenarios affecting multiple campus assets.

FOR

Insurers	Re insurers	Brokers
Risk Managers	Companies	Retail brokers

Publication: September 2026 • **Focus:** Property, business interruption and risk resilience

THE RISK LANDSCAPE OF MODERN DATA CENTRES

Modern data centres have evolved from conventional server facilities into some of the most valuable and technologically complex assets in the world. A hyperscale campus may represent billions of dollars of exposed value and depend upon the continuous operation of power systems, cooling infrastructure, communications networks and IT equipment. In this circular, we highlight some of the key aspects that LEARISK's Risk Engineers consider when assessing data centre risks during both the construction and operational phases, with particular attention to those factors that may influence property damage, business interruption and overall risk resilience.



View of a hyperscale data center (image created with AI)

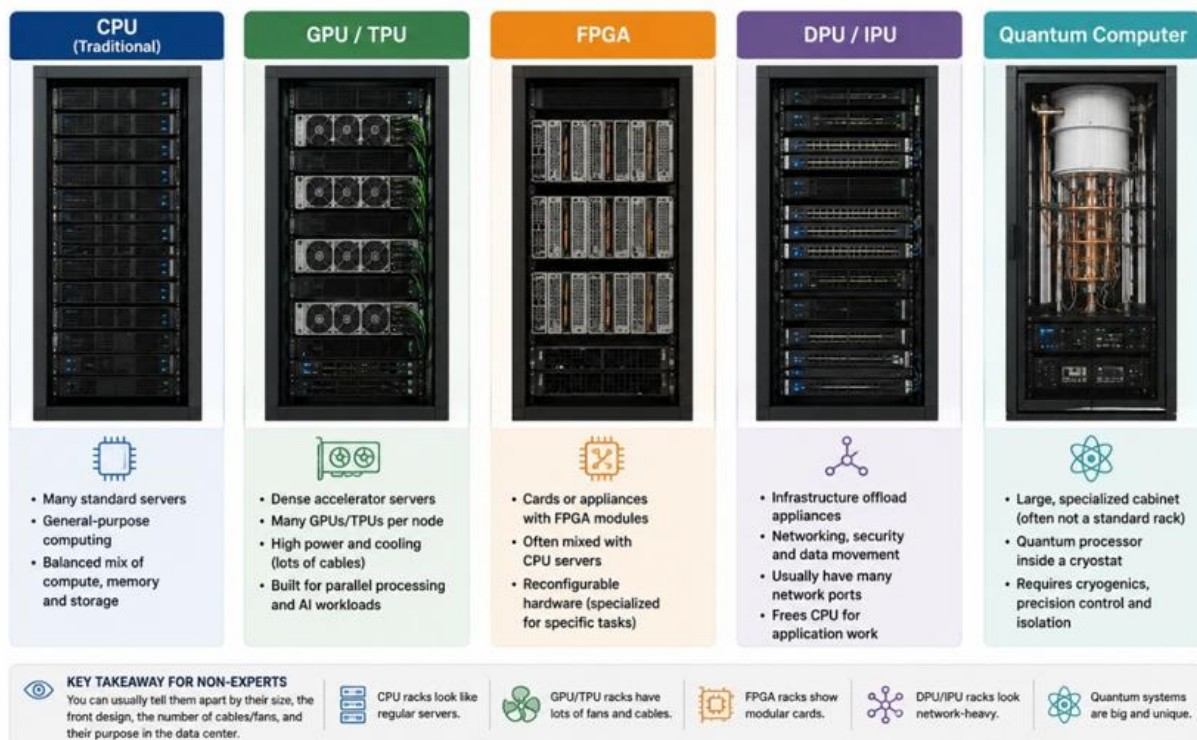
TECHNOLOGY MATTERS

Not all data centres are the same. Traditional facilities primarily rely on CPUs that support databases, business applications and web hosting. By contrast, modern Artificial Intelligence (AI) facilities increasingly depend on GPUs, which require significantly higher power densities, generate greater heat loads and demand more sophisticated cooling systems. A single AI rack may contain equipment worth several million dollars and consume many times the power of a conventional server rack.

Beyond CPUs and GPUs, some facilities also employ specialised technologies such as FPGAs, DPUs/IPUs and, increasingly, quantum computing systems. These technologies influence both value concentration and infrastructure requirements.

HOW THEY LOOK: DATA CENTER RACKS COMPARISON

A non-expert visual guide

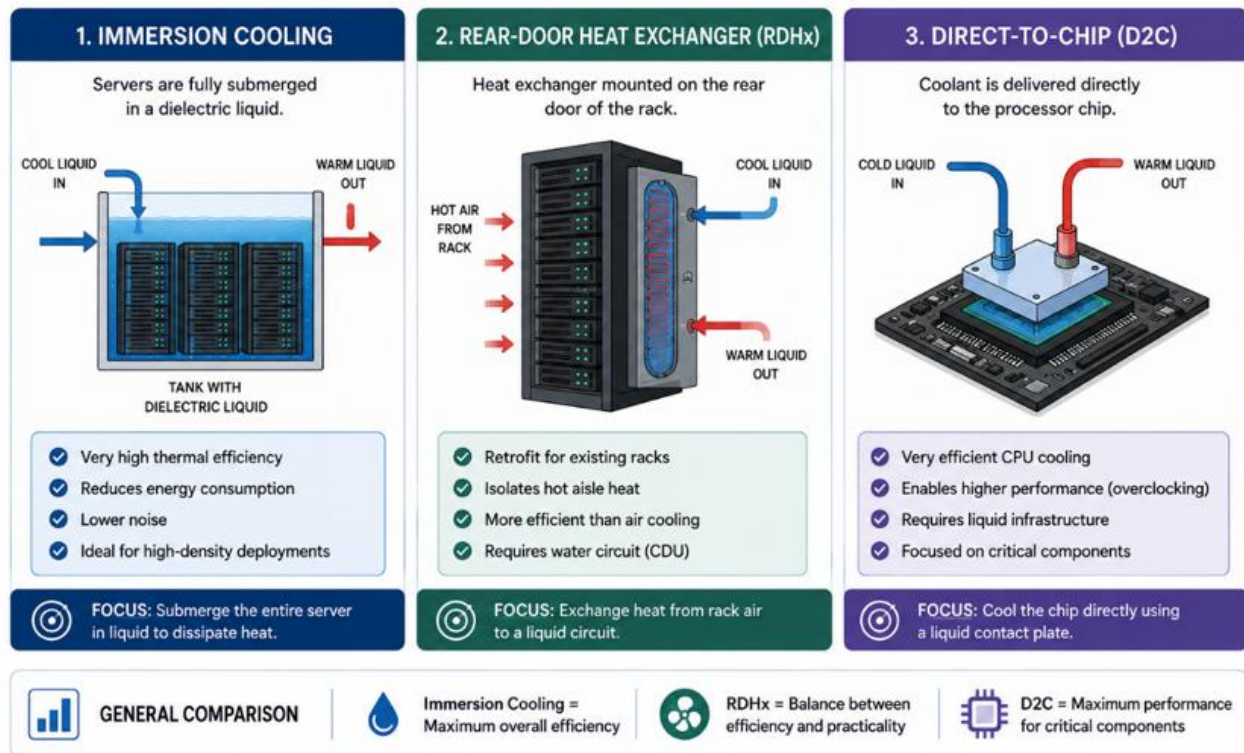


Different types of racks

As AI computing densities increase, cooling infrastructure has become one of the most critical and rapidly evolving aspects of data centre design.

Many facilities continue to rely on evaporative cooling due to its energy efficiency and relatively low operating cost. However, hyperscale facilities may consume extremely large quantities of water, while alternative technologies such as Immersion Cooling, Rear-Door Heat Exchangers (RDHx) and Direct-to-Chip (D2C) cooling are becoming increasingly common.

DATA CENTER COOLING SYSTEMS COMPARISON



Different types of liquid cooling

These technologies introduce new underwriting considerations:

- Water leaks and coolant leaks.
- Loss of cooling.
- Maintenance errors.
- Equipment failures.
- Dependency on auxiliary systems.

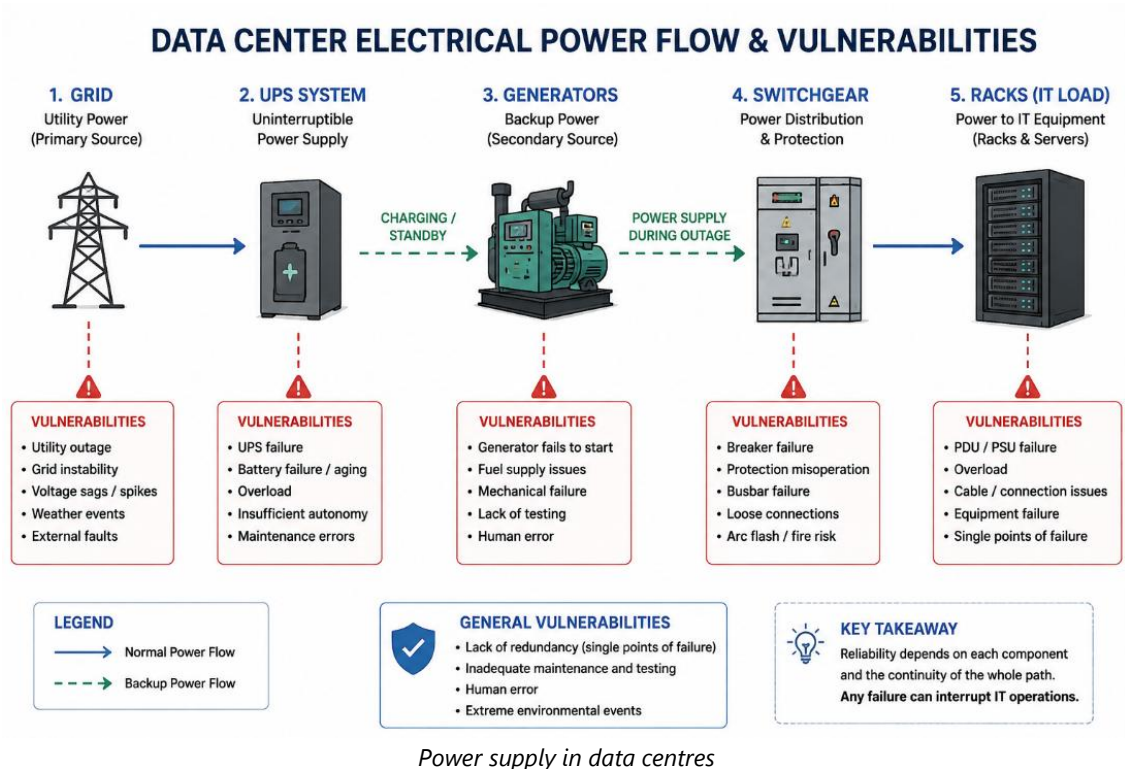
Data centres are frequently marketed according to their resilience level. However, the resilience of a modern data centre is fundamentally dependent on the reliability of its electrical infrastructure, including utility connections, transformers, switchgear, standby generators, UPS systems, battery installations and the extensive power distribution networks serving high-density IT halls. The scale and complexity of these systems, often designed to support hundreds of megawatts of critical load, require assessment by engineers with substantial experience in power generation, transmission and distribution systems.

The Uptime Institute Tier classification provides a useful benchmark:

- Tier I: Basic infrastructure.
- Tier II: Redundant components.
- Tier III: Concurrently maintainable systems.

- Tier IV: Fully fault-tolerant architecture.

Many hyperscale operators go further, targeting five nines availability (99.999%), equivalent to just 5 minutes and 26 seconds of downtime per year.

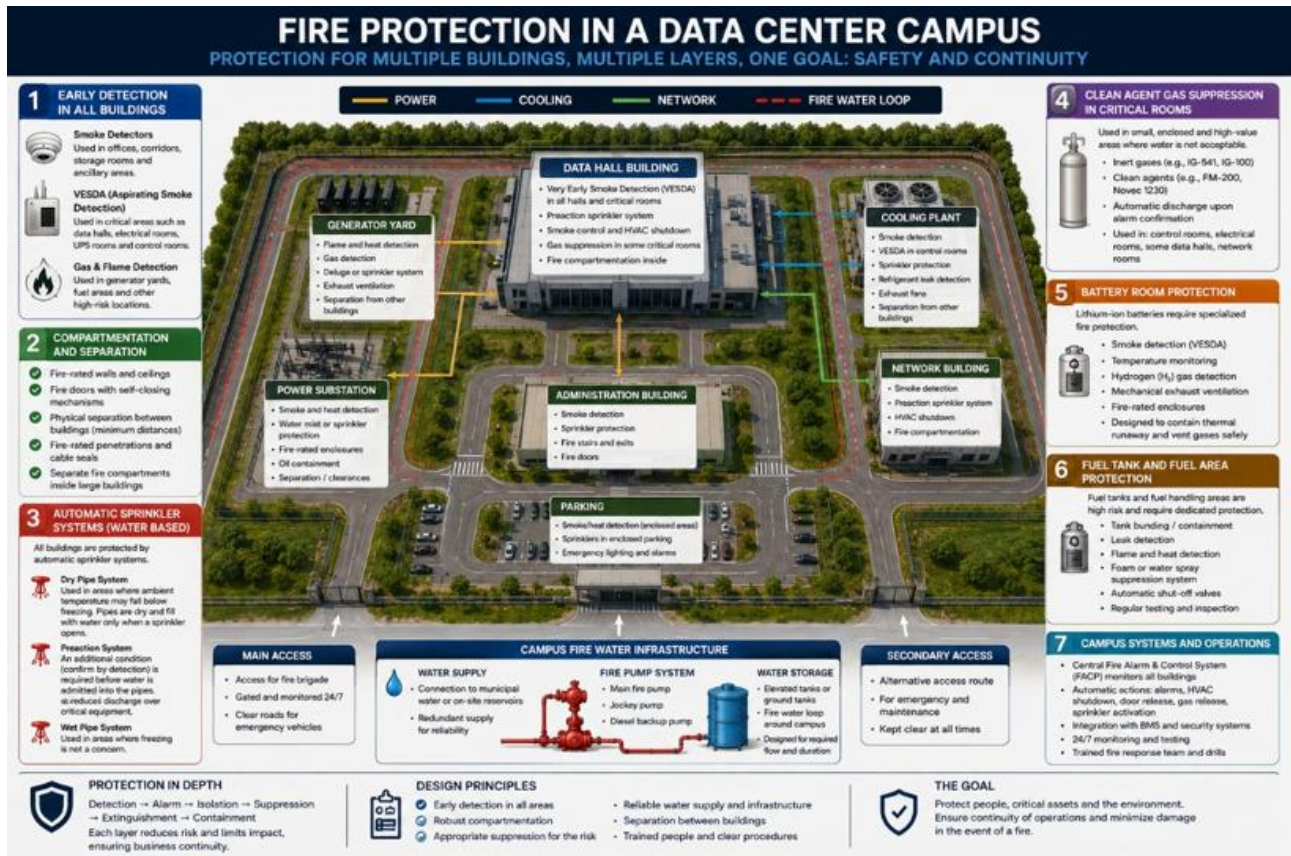


Hyperscale data centres are increasingly being designed with dedicated on-site power generation, including gas-fired turbine plants, renewable energy systems and even small modular nuclear reactors (SMRs). As a result, the risk profile is shifting decisively towards the power sector, making expertise in generation, transmission and electrical distribution systems an essential component of any meaningful risk assessment.

For underwriters, the key question is not simply how much redundancy exists, but whether the facility can continue operating when critical systems fail. True resilience depends on eliminating single points of failure and ensuring that incidents affecting one component do not compromise the entire operation.

FIRE PROTECTION: BEYOND COMPLIANCE

Modern data centres typically feature multiple layers of fire protection, including VESDA early warning detection, compartmentation, automatic sprinklers, clean agent suppression systems, battery protection and redundant firewater supplies.



Fire protection of a data centre

Historical losses demonstrate that compliance with standards does not necessarily guarantee resilience. A notable example occurred in 2016 at an ING Bank data centre in Bucharest where an accidental discharge of an inert gas suppression system damaged numerous hard drives despite the absence of a fire. The incident highlighted that protection systems themselves can become sources of loss if not properly designed, tested and maintained.



The OVHcloud fire in Strasbourg (2021) provides another important lesson. During the incident, firefighters repeatedly requested that the facility be de-energised. However, switchgear, generators and battery systems continued supplying power to portions of the site, resulting in continued electrical arcing and significantly hindering firefighting operations.

The event demonstrated that a resilience strategy designed solely to maximise availability may create unintended difficulties during emergency response. The fire originated within the UPS installation, and its propagation throughout the building was exacerbated by the forced-air ventilation system, which contributed to the movement of smoke and hot gases.

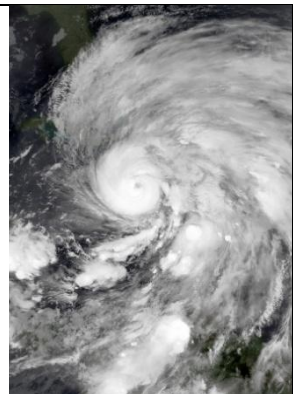
For insurers, fire protection assessment should therefore extend beyond verifying the presence of protection systems. Equal attention should be given to emergency shutdown capability, electrical isolation, operational procedures and business continuity arrangements.

ESTIMATED MAXIMUM LOSS (EML) AND NATURAL CATASTROPHES

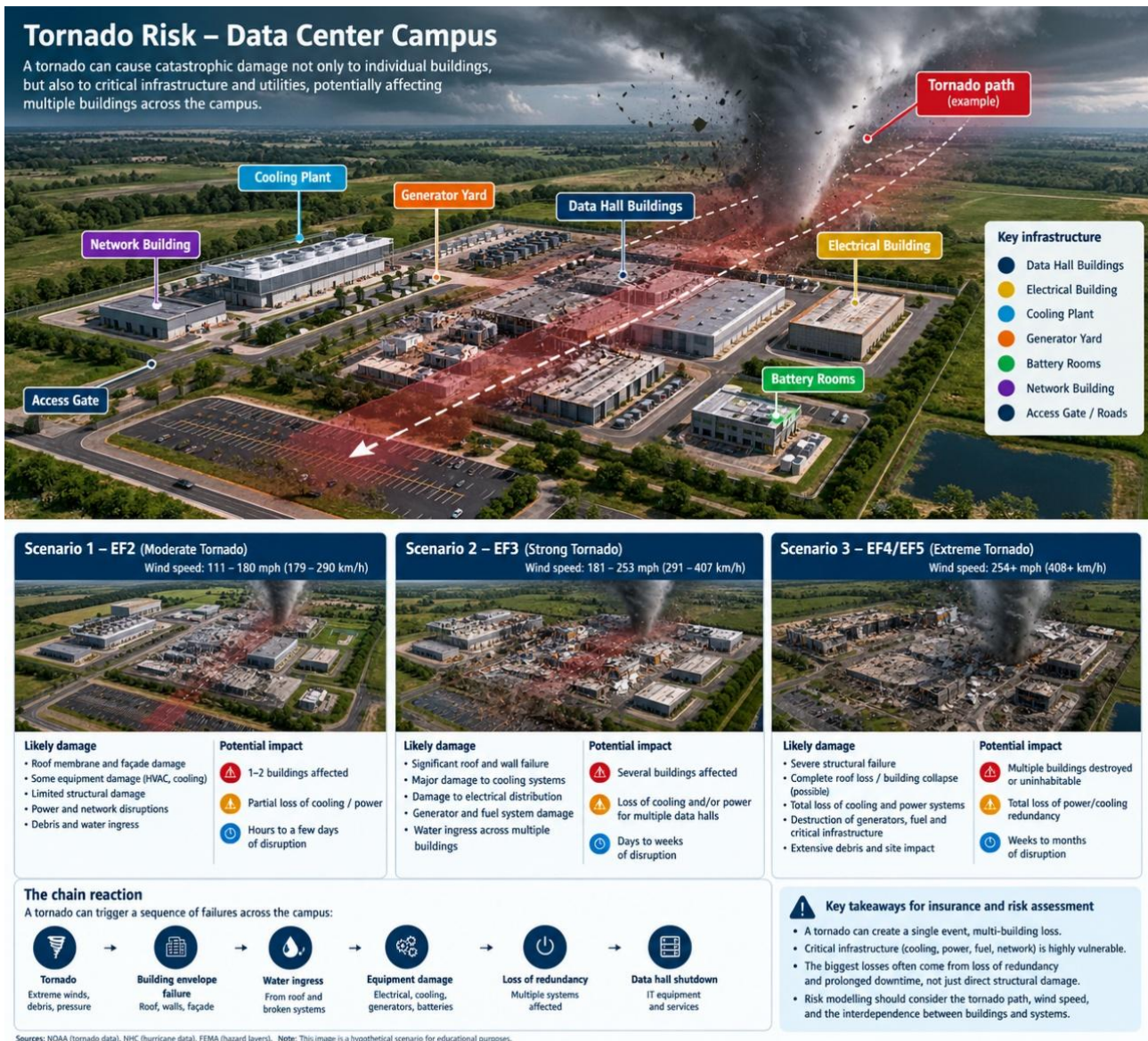
One of the most important aspects of data centre underwriting is the estimation of EML and PML. Unlike conventional industrial properties, a data centre is an interconnected ecosystem of data halls, cooling plants, electrical substations, generators and communications infrastructure. The loss of a single critical element may affect the operation of the entire campus.

Many underwriters instinctively focus on fire as the dominant loss scenario. However, recent hyperscale projects demonstrate that natural catastrophes may represent an equal or greater threat. A severe tornado, hurricane or flood can simultaneously damage multiple data halls, cooling plants, substations and network buildings across the same campus.

When discussing data centre risks fire often receives most of the attention. However one of the industry's most important loss lessons came from Superstorm Sandy in New York in 2012 when flooding affected several Manhattan data centres. In some facilities generators remained operational but the floodwaters damaged fuel tanks fuel pumps switchgear and other critical support systems located in basement levels resulting in prolonged service outages.



Buildings currently being constructed are unlikely to withstand an EF5 tornado, simply because the associated wind speeds exceed the design assumptions adopted for most structures. Likewise, data centres located in hurricane-prone regions should pay particular attention to drainage and flood management systems, especially in an environment where climate change is challenging the reliability of historical records and traditional design assumptions.



Estimating the EML associated with a tornado event requires the consideration of multiple tornado track scenarios, as the extent of potential damage will depend significantly on the assumed path, width and intensity of the storm relative to the location and layout of the facility. More importantly, it requires a realistic assessment of the consequences of extreme wind pressures and wind-borne debris on buildings and critical infrastructure, a task that can only be performed reliably by specialists with extensive experience in the analysis of historical loss events and post-loss investigations.

At LEARISK, we believe that independent risk engineering provides an essential complement to the perspectives of brokers, insurers and owners, supporting the development of realistic EML assessments through the combined expertise of multidisciplinary risk engineers and loss adjusters who continuously analyse loss experience across the global insurance market.

Technical note

This technical bulletin is intended for general information and loss-prevention purposes. The observations and considerations presented should be assessed in relation to the specific design, location, technology, operating conditions, contractual requirements and risk profile of each data centre. This document does not replace a detailed risk engineering assessment, property valuation, business interruption analysis, fire protection study, natural catastrophe assessment or review of applicable insurance policy terms and conditions.



RISK ENGINEERING SERVICES

WHO WE ARE

We are a company specialized in risk engineering with over 50 years of experience in the sector.

We provide independent consulting and services to identify, prevent, and mitigate risks affecting insured assets. Additionally, we offer industrial asset valuation and detection of underinsurance situations.

We have an interdisciplinary team composed of engineers from various specialties, architects, accountants, and NFPA-certified specialists (among others).

We operate in several countries across the Americas, Europe, Africa, and Asia, providing risk engineering services with a global reach.



Since 2005, we have implemented a quality management system based on ISO 9001 and continuously specialize in advanced technologies, such as catastrophic event simulators, hydraulic fire protection design, and virtual training platforms.

WHAT CAN WE OFFER

We have experience in:

- Power Generation and Renewable Energy
- Petrochemical, Oil, and Gas
- Mining and Heavy Industry
- Manufacturing and Construction
- Industry and Services
- Properties
- Jewelry Block
- Agriculture

Risk Engineering (Insurers, Brokers, and Policyholders)

- Property Risks (large and small); Machinery Breakdown; BI (Business Interruption); Construction/DSU (Damage to Works Under Construction); Maximum Loss Estimates (PML/EML); Civil Liability; Others (e.g., Jewelry Block).

Risk Assessments and Asset Valuations (Industrial and Non-Industrial Companies)

- BCP (Business Continuity Plan); Customized Risk Assessments for Clients; Risk Mapping; BI/DSU Exposure (Business Interruption/Damage to Works Under Construction); Fire System Performance Evaluation; Emergency Preplanning.

Engineering

- HAZOPS, ATEX, DHA; Fire System Design; Engineering Support.
- Determination of insured sums, valuations for accounting purposes, construction progress.