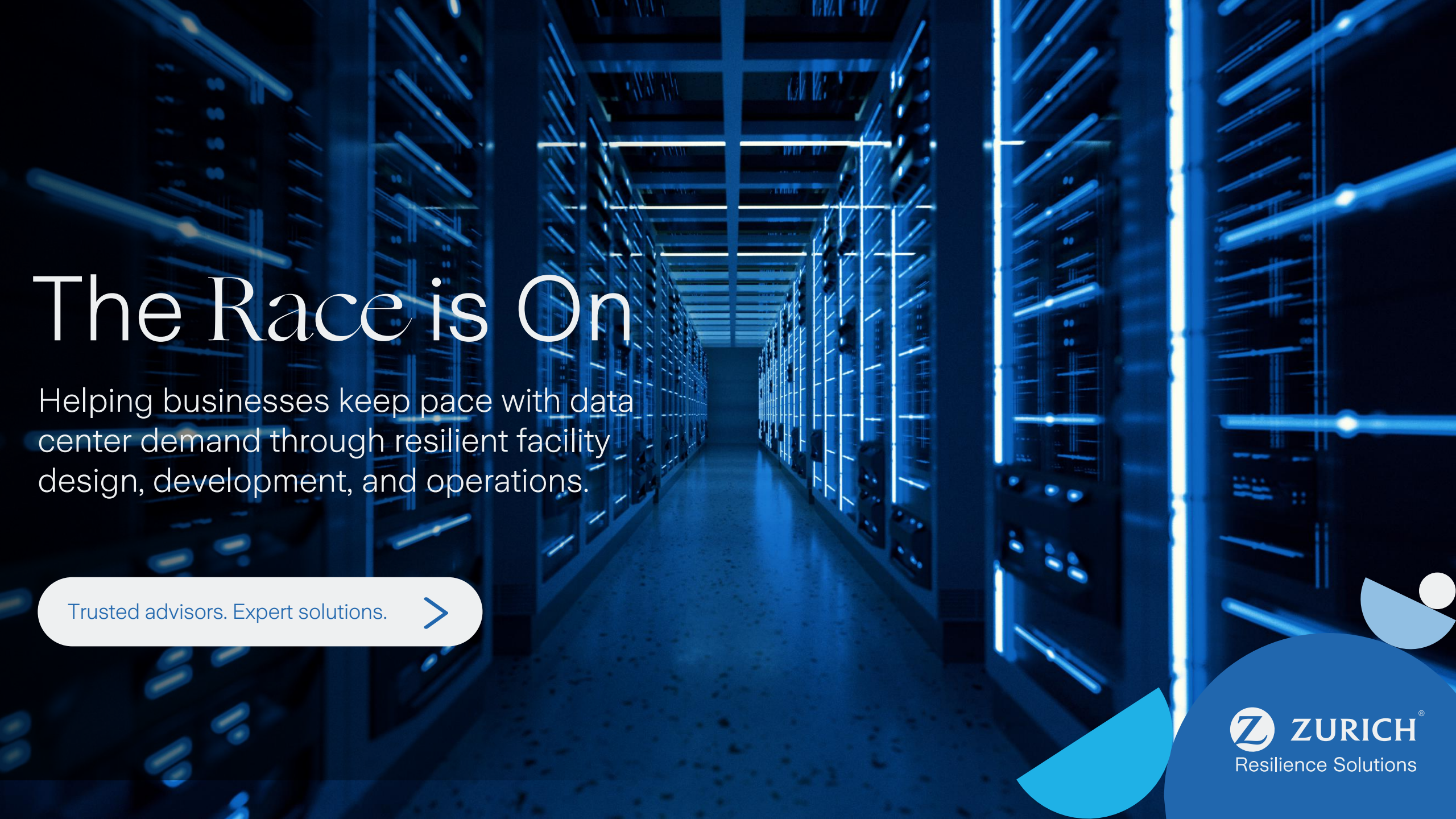


The Race is On

Helping businesses keep pace with data center demand through resilient facility design, development, and operations.

Trusted advisors. Expert solutions. >

ZURICH
Resilience Solutions

Building a resilient backbone for today's technology revolution

Data center construction projects are rapidly expanding to meet surging digital demand, and the expectations placed on them is relentless. These facilities combine high power density, tightly interconnected systems and narrow operating tolerances, meaning that minor design, installation or commissioning issues can escalate into outages, equipment damage, and safety incidents, or worse reputational harm.

Design for resilience

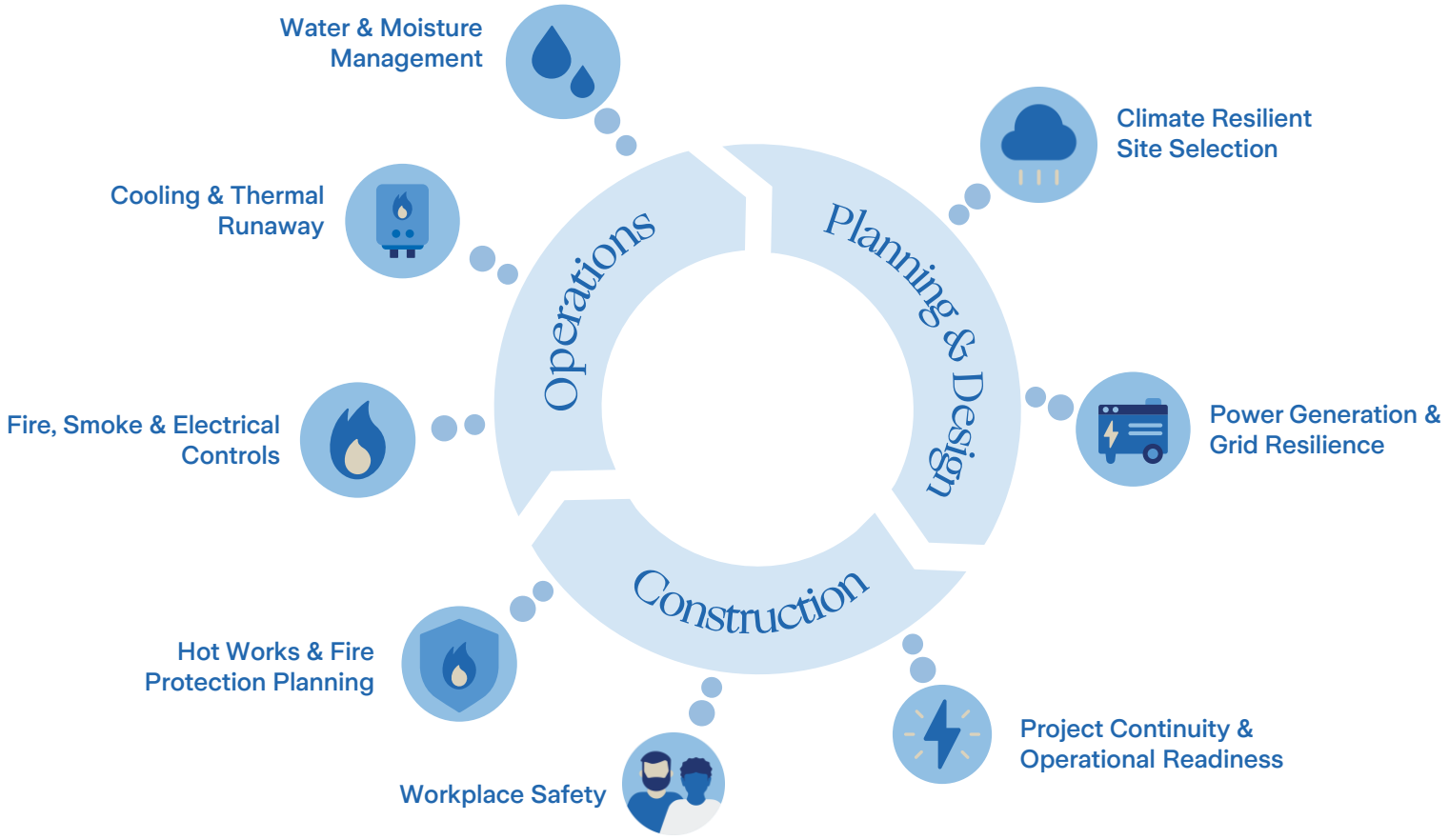
Building resilience into site design, development, and operations ensures that projects are delivered safely, on-time, and in a manner that provides long-term physical and commercial output. During the construction phase, defects are reduced and clear acceptance standards are set to achieve smoother commissioning and handover, while general liability concerns (damage or safety impacts to 3rd parties) are minimized. For facility operators, resilience translates into more reliable performance from day one, fewer disruptions, and stronger incident response.

Trusted advisors

Our risk experts partner with you from the outset to anticipate failure modes, quantify loss scenarios, and embed practical controls – helping to protect capital, safeguard uptime and create lasting competitive advantage.

360° risk engineering expertise focused on critical risk factors

Data centers are high voltage, technical environments that require highly specialized planning, precise installation and rigorous operational controls. Holistic risk expertise is required to help stakeholders tackle elevated exposures including electrical hazards, thermal events, structural issues, vulnerability to extreme weather, and general liability hazards.



Specialist Risk Hub

Our risk engineers focus on the most critical factors that can impact your operation. With deep data center sector expertise, you will be working with a proven leader in the industry.

- Dedicated global data center risk advisory practice
- 100 construction and 550 property risk engineers around the world
- 20+ years experience supporting complex critical infrastructure projects
- Site assessments and adaptation strategies to drive tailored risk reduction programs
- Financial impact analysis through forward-looking loss scenarios to prioritize CAPEX and OPEX investments

1 Climate Resilient Site Selection

Use climate and infrastructure intelligence to shape smarter, more resilient site investments.

For investors and developers, site selection is an early value lever: it can reduce downside risk, protect capex and support long-term uptime before design is locked in. Candidate plots should be screened against current and future extremes - flood, windstorm, wildfire, heatwave, and convective storms - prioritizing locations with low exposure or clear safety margins.

While the future cannot be predicted precisely, science-based climate scenarios help explore plausible outcomes and quantify loss impacts against early design concepts and asset values.

Alongside site exposure, assess wider “system resilience”, grid strength and restoration times, diverse telecom routes, access for staff and fuel, emergency services capability and water availability.

Power Generation & Grid Resilience 2

Confirm upstream power resilience and build redundancy into design and procurement decisions.

Practical validation of the strength and deliverability of the grid connection is an essential first step. New or enhanced connections can be delayed by capacity and resourcing constraints, while “quality of supply” issues and wider grid failures remain residual exposures even in well-designed facilities.

Where resilience is achieved through on-site or hybrid generation, risk typically shifts into design and operational complexity, especially when land constraints drive tighter layouts and increased on-site fuel storage. Co-location of batteries, gaseous fuels and high-voltage equipment can raise the severity of an event.

Hybrid systems require bespoke protection and control integration to manage safe start-up, operation and shutdown.

3 Project Continuity & Operational Readiness

Stress-test power-loss scenarios to reduce DSU/BI and operational disruption.

From a continuity lens, upstream network and transformer failures can remove supply abruptly, so the key question is whether redundancy and protection are truly fit for purpose. Planned utility work is a recurrent, sometimes underestimated threat: if grid connectivity is compromised, operations may depend on UPS and face an elevated shutdown risk.

When alternative supply is limited, incidents can escalate quickly into DSU/BI impacts. Operational risk also increases where configurations are immature, the track record at scale is limited, or reliance on sophisticated energy management systems outpaces their hardening to data center standards.

Regular, evidenced testing of failover, shutdown and recovery procedures is central to controlling the exposure.

Workplace Safety 4

Prioritizing on-site safety to protect lives, program delivery and reputation.

Data center builds concentrate many high-risk activities in a tight footprint. Early stages bring deep excavations, heavy lifts and intensive steelwork, with fall, crush and collapse exposures. Later, risk shifts indoors: congested MEP installation, complex cable routing, hot works around packaging and insulation, and growing interaction with live or part-live electrical systems.

Working at height above raised floors or within ceiling voids adds further complexity, especially when multiple trades overlap. General liability concerns are important considerations, where safety issues with contractors and site visitors can have serious consequences.

Managing this exposure requires thoughtful phasing, strong supervision and controls that keep people out of harm's way, and keep projects moving forward.

5 Fire, Smoke & Electrical Controls

Reduce ignition sources and stop smoke spread to protect IT and continuity.

Fire and smoke can escalate quickly in data centers because of dense electrical infrastructure, high power usage and sensitive hardware – and smoke can be as damaging as flame.

Common operational ignition sources include electrical faults (arc faults in UPS, PDUs and busways), overheating or loose cable connections, and overloaded circuits in high-density racks. UPS battery issues add a distinct hazard profile, including thermal runaway and flammable vapour off-gassing. Cooling and mechanical systems can also initiate events, such as fan motor/CRAC electrical failures, refrigerant leaks contacting hot surfaces, or generator-room fires linked to exhaust or fuel leaks.

Controls should prioritize early detection, effective suppression, and smoke containment that limits spread through cable pathways and airflow systems.

Hot Works & Fire Protection Planning 6

Control hot works and ensure temporary protections don't create hidden fire gaps.

Hot works remain a predictable but preventable cause of loss, particularly when welding, cutting or grinding occurs near packaging, insulation or combustible debris without tight supervision and fire watch.

Risk increases materially when systems are temporary or incomplete - such as fire alarms or suppression not yet installed, not active, or impaired - as small ignition sources can grow rapidly. Planning should also address transient combustibles introduced during projects, including paints, solvents, cardboard, plastics, cable reels and improperly stored generator fuel.

Strong planning combines these elements; clear permit-to-work, segregation and housekeeping standards, defined impairment management, and incident readiness to prevent fire and smoke spreading.

7 Cooling & Thermal Runaway

Assure cooling capacity and controls to prevent overheating and cascading equipment damage.

Cooling control is a critical dependency for IT uptime and asset protection. When capacity is reduced - through equipment faults (CRAC/CRAH, chillers, compressors, fans), poor airflow management, or blocked intakes/returns - hotspots can develop quickly. This can lead to overheating, equipment damage and service interruption, with potential knock-on hazards such as fire or power overloads.

The loss pathway often starts earlier, in design and delivery: incomplete installation, weak commissioning, mis-calibrated sensors and poor controls can leave hidden fragilities. External stressors such as heatwaves, high humidity and airborne pollution further reduce margins.

The control focus is clear evidence of tested redundancy, rigorous commissioning, continuous monitoring, and disciplined change management as heat loads evolve.

Water & Moisture Management 8

Reduce water ingress and leaks with containment, detection and disciplined maintenance.

Water damage is a high-severity threat because it can short-circuit electrical systems, corrode equipment and disrupt cooling, sometimes escalating to fire. Risks exist in construction (temporary plumbing, incomplete roof and drainage works, and water used for cleaning or testing) and persist in operations through condensate and chilled-water leaks, pipe failures, inadvertent sprinkler discharge, and raised-floor pooling that can affect cable and power infrastructure.

External events such as heavy rainfall, river/coastal flooding, sewer backup and seismic damage can overwhelm building protections. But human factors are often the differentiator, caused by maintenance errors, poor housekeeping during upgrades, and mismanaged humidity control.

Effective management combines segregation and drainage, leak detection with clear response actions, and regularly exercised incident playbooks.

Building resilience throughout the project lifecycle.

Throughout planning, construction, commissioning and operations, Zurich Resilience Solutions supports with specialized risk engineering expertise to help identify vulnerabilities and strengthen controls.

Proactive risk management is critical to maintaining continuity and building strategic advantage in an industry where uptime equals revenue, and reliability is a competitive differentiator.

Risk Engineering and Resilience Services

Strategic Site Selection
Climate and infrastructure intelligence to shape smarter, more resilient site investments.

Reliable Site Development
Manage design, construction and commissioning risks to help deliver projects with precision.

Worker Safety Culture
Embed strong safety leadership and practices to protect people and keep projects on track.

Uninterrupted Site Operations
Strengthen resilience, maintenance and response to safeguard uptime and critical customer services.

Benefits for Project Developers and Investors

Fewer Delays and Overruns
Prevent rework and critical-path disruption to deliver reliable customer outcomes.

Risk Transparency
Quantify top loss drivers and severity ranges to prioritize risk reduction investments.

Future-Proof Investments
Help reduce short and long-term impacts of extreme weather and natural hazard-related events.

Better Risk Transfer Outcomes
Enhanced risk management leading to greater insurability and unearth blind spots that can be managed in line with risk appetite.

ZURICH
Resilience Solutions

Meet tomorrow prepared.

For more information, please visit our website, or contact our team of risk experts