Make more Aerials / Shutterstock

ALLIANZ COMMERCIAL

The data center construction boom: risks and claims trends

Key drivers and evolving exposures in a dynamic market

commercial.allianz.com

Contents

Overview

→ The rapid rise of AI is transforming data centers into strategic economic assets, driving one of the largest infrastructure investment cycles in decades and spurring investment across power generation, transmission networks, substations, connectivity and semiconductors.

→ While investment continues to accelerate, the pace of expansion could be constrained by power and grid limitations, supply chain pressures, regulatory hurdles, community opposition and growing climate-related risks.

→ As data centers evolve into mission-critical infrastructure, organizations must look beyond physical assets to also manage interdependencies, concentration risk, operational resilience and potential cascading failures.

→ Data center losses can arise throughout the asset lifecycle, from damage, theft and construction defects during development to outages, fire, equipment breakdown, cyber incidents and natural catastrophe activity once facilities are operational.

The AI revolution is advancing at breathless speed, redrawing business practices and reshaping risk as it accelerates towards a future where intelligent technologies are embedded in every sector of the economy.

As we enter the latest phase of the AI boom, the data centers of the cloud era are evolving into gigawatt-scale campuses that could soon become critical to next-generation infrastructure, focusing on high-performance processing and running complex computational workloads. Arguably supporting pillars of the future global economy, data centers remain a compelling investment case but delivering them at scale faces several obstacles, from grid capacity to understandable public concern about their impact on local communities.

The growth momentum is unlikely to stall any time soon, meaning risk management must adapt to new exposures presented by the latest generation of data centers. Construction complexity, compressed timelines, and increasing scrutiny from regulators and the public alike will continue to challenge the sector, while resilience will depend upon efficient ecosystems and interdependencies that extend well beyond the building envelope of any individual facility. Immediate physical risks from fire, natural catastrophe, or water scarcity are being shaped by broader trends, such as integrating lithium-ion batteries, competition for land or changing weather patterns.

Risks are further heightened by multiple stakeholders, high insured values, and geographic clustering, increasing accumulation risk across locations, perils and lines of business.

Against this backdrop, developers, operators, tenants, investors and insurers all have a role to play in building an adaptive approach to risk in a complex environment. And as AI infrastructure becomes increasingly important to the global economy, the role of insurance is evolving beyond protecting physical assets to supporting investment and operational resilience, helping to ensure the safe and financially sustainable expansion of this sector.

Thomas Lillelund
CEO
Allianz Commercial

Executive summary

AI is creating a new infrastructure supercycle ↘ page 8

As AI adoption shifts from training frontier models to deploying millions of AI-powered applications and autonomous agents, annual data center investment is projected to rise from around US$500bn in 2024 to more than $1trn as early as 2027. The investment opportunity extends well beyond data centers to electricity generation, grid infrastructure, cooling, networking and semiconductors.

Governments are becoming a major structural driver of AI infrastructure investment. Concerns over technological sovereignty, national security and geopolitical competition have prompted many countries to launch national AI strategies, sovereign compute programs, semiconductor initiatives and direct public investment into domestic computing capacity. Because these investments are driven by strategic priorities rather than purely financial returns, they tend to be relatively price-insensitive, reinforcing the long-term outlook for the sector.

The next wave of investment is increasingly global. The US and China are expected to account for around 62% of new global capacity additions through 2030, underscoring their continued central role in the data center build-out and ensuring their combined share of global capacity is expected to remain broadly stable at around 63%. In Europe, Germany, the UK and Ireland are expected to remain major markets, but faster expansion is likely in Spain, Finland and Denmark, where power availability and permitting conditions are often more favorable. Across Asia Pacific, excluding China, installed capacity is projected to increase from around 9GW today to more than 28GW by 2030. Malaysia stands out, with capacity expected to grow more than tenfold, positioning it alongside India and Japan as one of the region's fastest-growing AI infrastructure markets.

Hrach Hovhannisyan / Shutterstock

What could slow the infrastructure buildout? ↘ page 13

The key constraints are power, permitting and land. Demand for data center financing remains strong as AI demand continues to strengthen. Instead, competitive advantage is increasingly determined by access to electricity, grid connections, permitting, specialized equipment and skilled labor – for example, the US construction industry alone faces a shortage of around 439,000 skilled workers. The winners will increasingly be those that can deploy AI infrastructure fastest, not simply finance it.

The principal risks to the AI infrastructure buildout are increasingly operational rather than demand driven. Infrastructure bottlenecks, supply chain constraints, uncertainty around AI monetization, growing physical climate risks, regulatory hurdles and community opposition will increasingly determine where and how AI infrastructure is built. In the US alone, local opposition delayed or blocked at least 75 projects worth almost US$130bn during the first quarter of 2026, while the Netherlands temporarily froze new hyperscale applications in 2022. Ireland has introduced stricter requirements linking new grid connections to additional renewable generation.

With around 79% of global data center capacity already located in areas exposed to elevated natural catastrophe risk and 54% exposed to chronic heat and drought stress, resilience is becoming a strategic consideration rather than an operational afterthought. Many of the fastest-growing AI infrastructure markets are also among the most climate-exposed. Northern Virginia in the US, Johor in Malaysia, and Marseille, France rank among the highest-risk global markets. In other words, the same factors attracting investment, including abundant land, existing infrastructure and power availability, often coincide with higher climate exposure. Risk profiles also vary by region. Acute flood, wildfire and wind exposure is highest in the Americas, affecting 86% of capacity, while chronic heat and drought stress is greatest in Asia Pacific, where 89% of capacity is exposed.

It is estimated that climate risks could reduce the discounted value of the global installed data center base by around $388bn, equivalent to 38% of asset value before adaptation. Business interruption accounts for almost one-third of total modelled losses, with more than 90% arising from upstream supply chain disruption rather than direct physical damage.

Insurance is becoming a critical enabler of AI infrastructure ↘ page 18

As data centers evolve from commercial real estate into mission-critical infrastructure, the role of insurance is expanding beyond protecting physical assets to supporting investment and operational resilience. Comprehensive insurance cover has become a prerequisite for financing many large-scale AI infrastructure projects. Construction costs for a single AI campus can exceed $20bn, with insured values increasing substantially once high-performance computing equipment is installed. Lenders and investors increasingly require robust insurance programs throughout both construction and operation, making insurance an important component of project finance.

The global data center insurance market is projected to grow from around $11bn today to more than $24bn by 2030, reflecting rapid capacity expansion, rising insured values and increasing operational complexity. Demand is expected to extend beyond traditional property cover towards integrated solutions spanning construction, engineering, property, business interruption, cyber and liability, while creating new opportunities in areas such as energy resilience, operational continuity and technology risk.

The risk landscape and claims trends ↘ page 19

As data centers become critical infrastructure for the digital economy, their risk profile is changing rapidly. What were once relatively straightforward, warehouse-like facilities are evolving into large, complex campuses with multi-story buildings, high-density equipment, on-site power generation, advanced cooling systems, and extensive interdependencies with power grids, water supply, and data connectivity.

Construction complexity is a major source of risk. Multi-story data centers create high structural loads and concentrate significant value in a single location. Compressed schedules, late design changes, retrofitting, prototypical or second-hand equipment, poor ground conditions, and inadequate quality assurance can all increase the likelihood of loss. The testing and commissioning phase is especially critical because it is when systems go live for the first time and are pushed close to operating limits. Latent defects, temporary systems, contractor interfaces, and time pressure can allow small errors to cascade into major losses.

Fires in data centers are relatively rare but can have serious consequences. According to **Allianz Commercial** analysis of insurance industry data center losses, fire is the leading driver of loss severity, accounting for well over 50% of €700mn worth of insurance industry claims. Natural catastrophe activity ranks second, followed by so-called wilful acts (including crime and cyber crime) and power failure. Meanwhile, water damage is the most frequent cause of data center claims, followed by wilful acts, fire, and equipment breakdown. Business interruption is the primary driver of claims severity by line of insurance business, underlining the high financial impact of operational downtime. Europe and North America dominate the share of regional losses according to both the number and value of claims. By claims volume, Europe accounts for 53%, followed by the US at 36%. By severity, Europe accounts for 38% and North America 36%.

Fire risk is evolving as power density increases and battery energy storage becomes more integrated into facilities. Lithium-ion batteries, increasingly used in or near server environments, can create the risk of thermal runaway – a self-sustaining, high-temperature fire that is difficult to control. Fire suppression systems themselves can also introduce risk, with accidental activation, vibration, noise, contamination, or humidity potentially damaging sensitive equipment. Restoration after a fire can be lengthy and complex, requiring specialist equipment, infrastructure rebuilds, temporary solutions, and careful assessment of whether damaged systems can be safely repaired.

Make more Aerials / Shutterstock

Power is one of the most critical dependencies for data centers. Reliable, high-capacity electricity, redundancy, grid stability, and backup systems are essential to maintain uptime. At the same time, the use of refurbished or prototypical turbines, on-site generation, battery storage, and temporary power systems can introduce new reliability and fire exposures. Water availability is another key dependency, particularly as cooling demands rise and environmental restrictions tighten. Connectivity is equally important, but reliance on external fiber routes and network nodes can create vulnerability to offsite failures.

Hyperscale and colocation facilities create significant accumulation risk. A single campus may bring together operators, multiple tenants, construction works, servers, supporting utilities, and on-site infrastructure in one physical or operational space. One event can therefore trigger claims across multiple insurance policies, including property, construction, business interruption, liability, cyber, and financial lines. Shared infrastructure also means that failures affecting power, cooling, building management systems, or connectivity can have consequences for many stakeholders at once.

Real-life claims case studies show that in hyperscale facilities such loss factors as damage to external cooling systems, hot works-related fire, and a delay in start-up caused by power disturbances have resulted in losses in the €50mn to €100mn range alone.

Claims can also lead to contractual disputes, liability issues, and reputational damage. Failure to meet uptime commitments, power capacity requirements, backup obligations, or service level agreements can result in penalties, service credits, litigation, and customer losses. Supply chain constraints compound this challenge, with long lead times for critical equipment such as switchgear (as long as 80 weeks) and transformers (as long as 50 weeks), potentially extending reinstatement periods and increasing business interruption costs.

Such risk and claims trends developments raise important questions about insurability. Underwriters are increasingly focused on value concentration, site location, natural catastrophe exposure, interdependencies, resilience, business continuity planning, and accumulation across multiple insured interests. Probable maximum loss calculations are often driven by equipment and server values.

Effective risk mitigation must begin early and continue throughout the data center lifecycle. During design, purpose-built facilities, spatial separation, structural load planning, compartmentalization, vertical pathway control, and early fire and battery detection systems are important. During construction, realistic schedules, strong quality assurance, management of temporary systems, and protected equipment storage are essential. During testing and commissioning, adequate time for fault-finding, clear contractor coordination, and a robust safety culture are critical. During operations, preventative maintenance, component monitoring, cooling redundancy, leak detection, fire suppression maintenance, and business continuity planning all help reduce loss potential.

Ultimately, data center risk management requires a holistic and coordinated approach. Owners, operators, tenants, brokers, insurers, investors, contractors, and technology providers need transparency around design changes, tenant changes, scope changes, and operational dependencies. A unified risk framework can help reduce uncertainty, avoid coverage gaps or overlaps, improve claims response, and support the long-term resilience of this increasingly vital digital infrastructure.

PeopleImages / Shutterstock

OUTLOOK

Managing the risks of the next infrastructure boom

The rapid rise of artificial intelligence is transforming data centers from supporting infrastructure into strategic economic assets. **Allianz Research** economists explore how this shift is reshaping investment, creating new opportunities and risks, and fueling a powerful new infrastructure supercycle.

Hrach Hovhannisyan / Shutterstock

AI is creating a new infrastructure supercycle

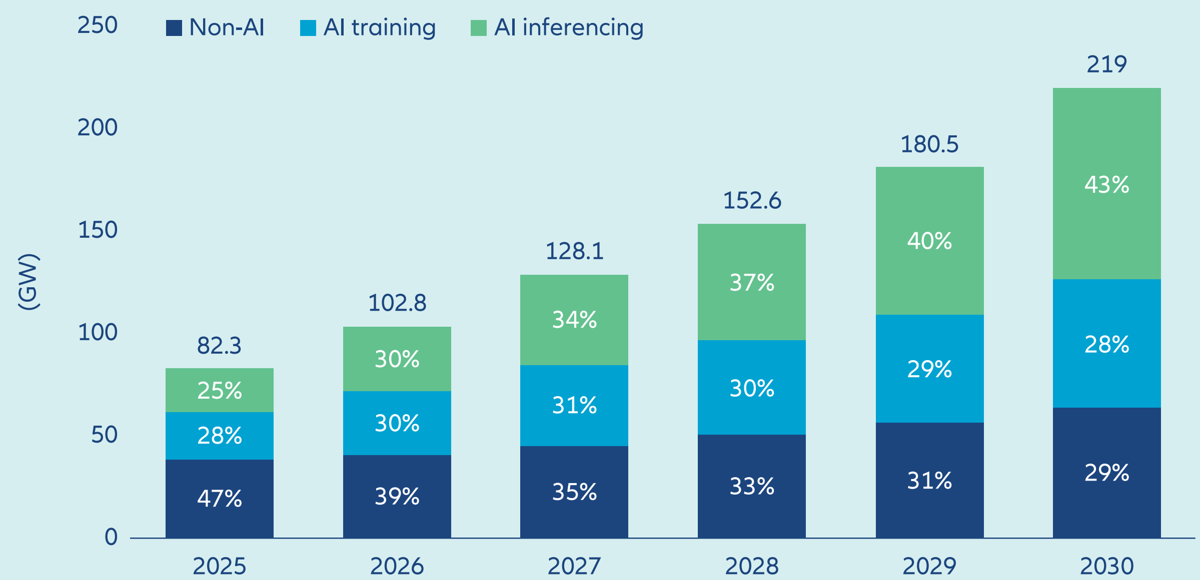
As AI moves from experimentation to widespread deployment across businesses, governments and consumer applications, demand for computing capacity is entering a new phase, one that is likely to drive one of the largest and most sustained infrastructure investment cycles in decades.

The current AI infrastructure boom has evolved through three successive demand waves. The first began in the early 2010s as enterprises migrated workloads from on-premises servers to the public cloud. This transformation concentrated demand in the hands of a small number of hyperscale cloud providers and drove the construction of increasingly large, standardized facilities optimized for general-purpose computing and storage. The second wave began with the emergence of generative AI following the launch of ChatGPT in late 2022. Training increasingly sophisticated foundation models required dense clusters of specialized AI processors, significantly increasing power density, cooling requirements and networking complexity within data centers.

The third demand wave – AI inference

AI inference is expected to become the dominant long-term driver of infrastructure demand. The industry is now entering a third – and potentially much larger – phase in which AI inferencing, the deployment of trained models in real-world applications, is expected to overtake model training as the largest source of compute demand. Unlike training, which is concentrated among a relatively small number of technology companies, inferencing scales with the number of users, applications and interactions. As AI becomes embedded across enterprise software, industrial automation, financial services, healthcare and consumer products, demand shifts from training a handful of frontier models to serving hundreds of millions of users.

AI workloads, especially inferencing, become the dominant driver of future data center demand.



Sources: McKinsey, AIM GIS

AI agents are set to multiply computing demand. While today's AI assistants typically respond to individual prompts, AI agents are designed to autonomously complete complex, multi-step workflows. A single task can require repeated planning, reasoning and interactions with multiple models and external tools, consuming around 1,200 times more tokens than a conventional single-turn query (a question that gets an answer straightaway). At the same time, reasoning models deliberately allocate additional computing resources during inference to improve the quality and reliability of responses, further increasing compute intensity.

Greater efficiency is accelerating – not reducing – infrastructure demand. The computing power required to achieve a given AI capability currently halves roughly every eight months, driven by advances in models and hardware. Yet lower costs have historically stimulated rather than suppressed demand. As AI becomes cheaper, it is deployed across more industries and use cases, causing overall compute consumption to rise despite rapid efficiency gains. Similar to previous general-purpose technologies, efficiency gains are more than offset by expanding adoption.

"Meeting AI demand requires investment across an entire infrastructure ecosystem," says **Patrick Hoffman, Environmental, Social, and Governance, and AI Economist, Allianz Research.** *"The expansion extends far beyond data centers themselves to include electricity generation, transmission networks, substations, cooling systems, fiber connectivity and advanced semiconductors. Gigawatt-scale AI campuses are gradually replacing the tens-of-megawatts facilities that characterized the cloud era, while liquid cooling, high-speed optical networking, GPUs, custom AI accelerators and high-bandwidth memory are becoming essential components of next-generation infrastructure."*

"

The challenge is no longer whether AI infrastructure will be needed, but whether it can be deployed quickly enough

Governments are becoming a second structural driver of AI infrastructure investment

Commercial demand is increasingly being reinforced by sovereign AI initiatives. Concerns over technological sovereignty, national security and geopolitical competition have prompted many countries to launch national AI strategies, sovereign compute programs, semiconductor initiatives and direct public investment into domestic computing capacity. Because these investments are driven by strategic priorities rather than purely financial returns, they tend to be relatively price-insensitive, reinforcing the long-term outlook for the sector.

"The challenge is no longer whether AI infrastructure will be needed, but whether it can be deployed quickly enough," says **Yao Lu, Investment Strategist, Allianz Research.** *"AI infrastructure is no longer being built to support a single technology trend but to underpin the next generation of the global economy. As AI adoption broadens across industries and governments accelerate investment in strategic computing capacity, the central question is becoming less whether demand will continue to grow, and increasingly whether sufficient infrastructure can be deployed at the required scale."*

vectorfusionart / Shutterstock

Why the investment cycle is likely to remain strong

The scale of planned investment suggests that AI infrastructure is entering a multi-year investment supercycle.

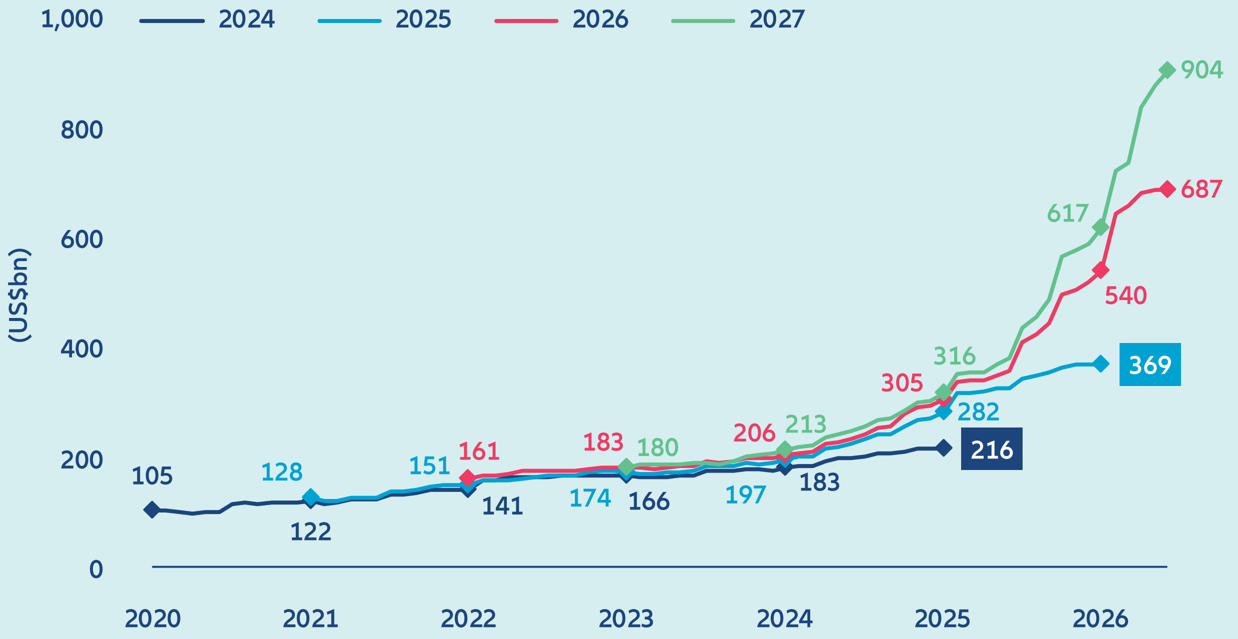
Global data center investment increased from around US$100bn in 2015 to more than $500bn in 2024. Only one year ago, the International Energy Agency projected annual investment would exceed $800bn by 2030 under its base-case scenario[1]. Since then, however, the outlook has strengthened considerably as the world's largest technology companies have accelerated their AI investment plans.

Hyperscaler spending has risen much faster than previously expected. Capital expenditure by the leading cloud providers has increased by more than 75%[2], prompting a broad reassessment of future infrastructure requirements.

Recent estimates now suggest annual global data center investment could exceed $1trn as early as 2027 and approach $1.6trn by 2030, making AI infrastructure one of the largest investment cycles in decades[3].

AI is changing not only the scale of investment but also where capital is being deployed. Accelerated computing infrastructure is expected to account for around 45% of total data center investment by 2030, up from only around 10% in 2015. Investment is increasingly concentrated in GPUs, custom AI processors, high-bandwidth memory, advanced networking equipment and liquid cooling technologies, with hyperscalers expected to account for roughly half of this spending.

Hyperscaler investment projections (in US$bn)



Sources: Bloomberg, AIM-GIS-PM; Notes: Data as of June 30, 2026; Hyperscalers include Alphabet, Amazon, Meta, Microsoft, Oracle

Growth momentum goes global

The next wave of investment is becoming increasingly global. The US and China are expected to account for around 62% of new global capacity additions through 2030, underscoring their continued central role in the data center build-out. Driven by this growth momentum, their combined share of global capacity is expected to remain broadly stable at around 63% with China projected to rise slightly from today's 21% to 24%, while the US loses five percentage points of market share, reaching 39% in 2030[4].

However growth is accelerating well beyond today's established hubs as developers are increasingly directing investment towards locations that can offer abundant electricity, available land, efficient permitting and competitive operating costs. In Europe, Germany, the UK and Ireland are expected to remain major markets, but faster expansion is likely in Spain, Finland and Denmark, where power availability and permitting conditions are often more favorable.

Across Asia Pacific, excluding China, installed capacity is projected to increase from around 9GW today to more than 28GW by 2030. Malaysia stands out, with capacity expected to grow more than tenfold, positioning it alongside India and Japan as one of the region's fastest-growing AI infrastructure markets.

"The long-term investment case therefore remains compelling. Demand, capital and public policy all point to continued expansion. The critical question is no longer whether investment will take place, but where it will concentrate. Increasingly, capital is flowing towards markets that can support large-scale AI infrastructure efficiently," says **Yao Lu, Investment Strategist, Allianz Research.**

NK_Studio.TH / Shutterstock

What could slow the AI infrastructure buildout?

The long-term investment outlook remains compelling, but delivering projects at the required speed and scale is becoming increasingly challenging.

While capital remains abundant and demand continues to strengthen, the expansion of AI infrastructure faces growing constraints across energy, supply chains, regulation and physical risk. Together, these factors will increasingly determine where investment continues and how quickly new capacity can come online.

Power infrastructure is becoming the primary constraint on future expansion. While large data centers can often be built within 18 to 24 months, the transmission infrastructure, grid connections and additional power generation needed to support them frequently require several years to develop. This growing mismatch delays projects, postpones revenue generation and extends the payback period on invested capital.

"As AI-driven electricity demand begins to exceed available grid capacity in major markets, competition for power is intensifying, increasing both development risk and operating costs," says **Patrick Hoffman, Environmental, Social, and Governance, and AI Economist, Allianz Research.** *"If electricity infrastructure cannot expand at the same pace as data center investment, it could become the principal constraint on the next phase of industry growth."*

"

If electricity infrastructure cannot expand at the same pace as data center investment, it could become the principal constraint on the next phase of industry growth

WILLIAM LUQUE / Shutterstock

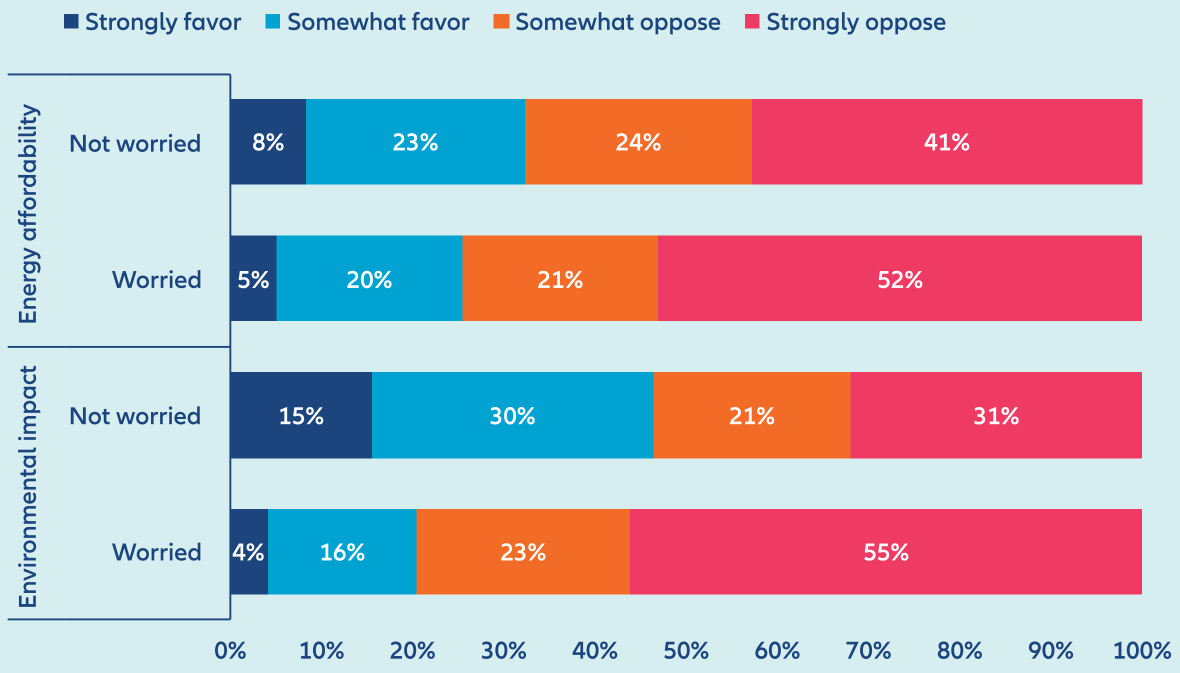
Supply chain pressures and community oppositions mount

The broader AI infrastructure supply chain is also under increasing pressure. Beyond electricity, developers face growing shortages of transformers, switchgear, high-voltage cables and other critical grid equipment, with lead times extending to several years in some markets. Current estimates suggest supply shortfalls of around 30% across key grid equipment categories[5]. At the same time, demand for GPUs, high-bandwidth memory and advanced semiconductor packaging continues to rise rapidly, with shortages of high-bandwidth memory already emerging as a constraint on AI deployment[6].

The physical construction of new facilities is becoming more difficult as well. The US construction industry alone faces a shortage of around 439,000 skilled workers[7], particularly in electrical and mechanical trades, while an estimated 349,000 additional workers may be needed in 2026[8]. Suitable sites are also becoming scarcer as developers compete for locations offering reliable power, fiber connectivity, water availability and favorable permitting conditions.

Regulation and community opposition are becoming increasingly important project risks. As data centers grow larger and more energy intensive, local concerns over electricity consumption, water use, land availability and environmental impacts are becoming more pronounced. In the US alone, local opposition delayed or blocked at least 75 projects worth almost US$130bn[9] during the first quarter of 2026, while 71% of Americans oppose having a data center built near their community[10]. Similar trends are emerging elsewhere. New York recently introduced a one-year moratorium on permits for large facilities[11], the Netherlands temporarily froze new hyperscale applications in 2022[12] and Ireland has introduced stricter requirements[13] linking new grid connections to additional renewable generation.

Public opinion on local data center construction in the US



Source: Gallup, as of March 2026

Current investment plans also assume AI demand will continue to expand rapidly for many years. However, uncertainty remains over how much businesses and consumers will ultimately be willing to pay for frontier AI models, while continued improvements in model efficiency could reduce the amount of infrastructure required to deliver comparable performance. This risk came into sharp focus in January 2025, when the release of China's DeepSeek model, reportedly trained at a fraction of the cost of comparable frontier models, erased almost $600bn[14] from Nvidia's market value in a single day as investors reassessed future compute demand. China already provides a cautionary example of overbuilding. A local government-led construction boom has left utilization rates at only 20% to 30%, while project cancellations have risen sharply over the past two years[15].

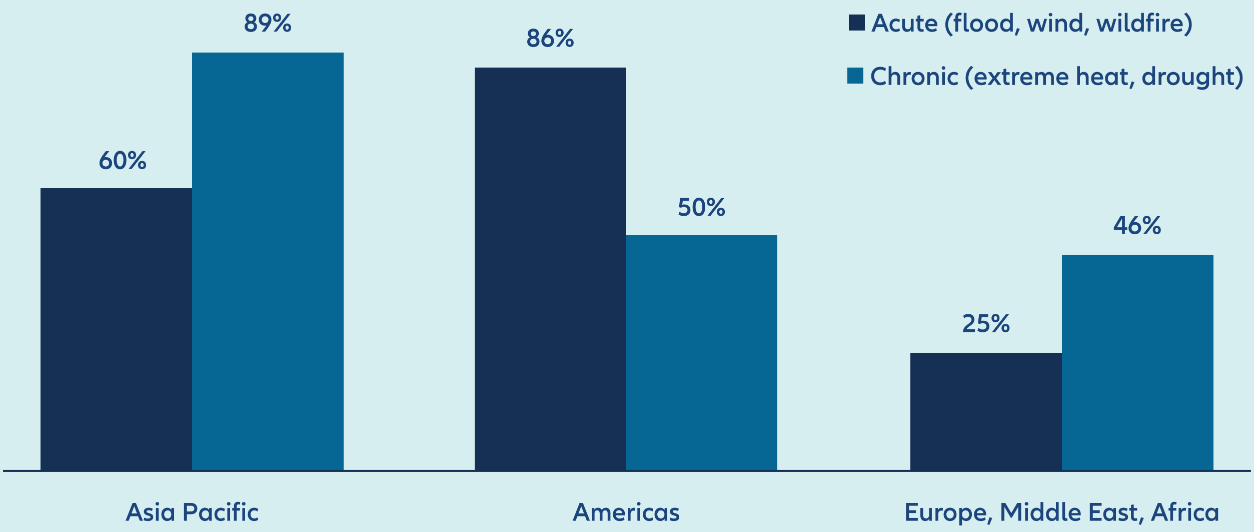
"Given the scale of capital already committed by the largest US technology companies, a similar mismatch between capacity and demand in Western markets would have significant implications for investment returns across the AI value chain," says **Yao Lu, Investment Strategist, Allianz Research[16].**

Climate risk now a cause for concern

Physical climate risk is emerging as one of the sector's most significant and underappreciated long-term challenges. A June 2026 assessment covering 97 global data center markets found that 79% of global capacity is located in areas with elevated exposure to acute natural hazards, including flooding, tropical cyclones and wildfires, while 54% is exposed to chronic heat and drought stress[17]. Acute hazards create volatility through physical damage, downtime and insurance claims, whereas chronic heat and water scarcity steadily increases operating costs through higher cooling requirements, lower efficiency and growing pressure on local water resources.

Many of the fastest-growing AI infrastructure markets are also among the most climate-exposed. Northern Virginia in the US, Johor in Malaysia, and Marseille, France rank among the highest-risk global markets, while Stockholm in Sweden and Oslo in Norway benefit from significantly lower physical risk. In other words, the same factors attracting investment, including abundant land, existing infrastructure and power availability, often coincide with higher climate exposure. Risk profiles also vary by region. Acute flood, wildfire and wind exposure is highest in the Americas, affecting 86% of capacity, while chronic heat and drought stress is greatest in Asia Pacific, where 89% of capacity is exposed.

Physical climate risk exposure of data center capacity, by region



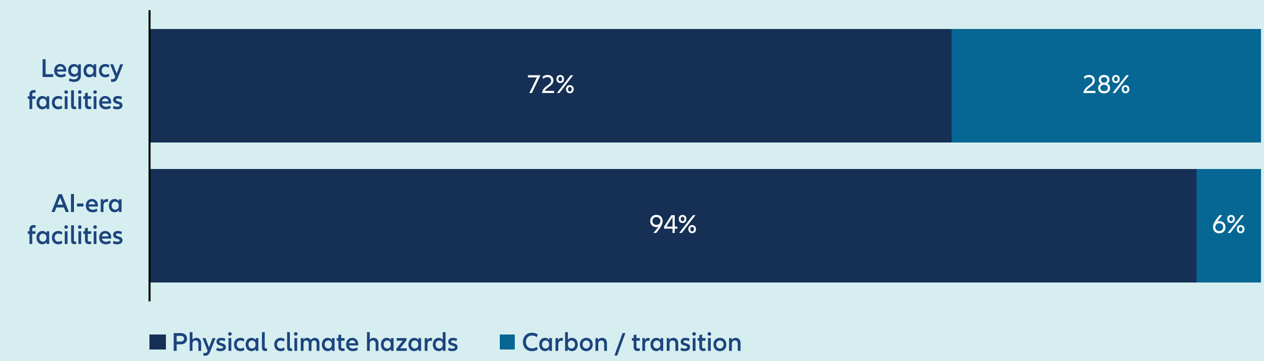
Sources: First Street, Allianz Research

Water has become a critical resource for AI infrastructure, with US data centers consuming around 80bn liters in 2025, a figure projected to exceed 167bn liters by 2030[18]. In water-stressed regions, cooling requirements can constrain operations independently of extreme events while attracting greater regulatory scrutiny and community opposition[19].

Schneider Electric's ClimVaR model estimates that climate risks could reduce the discounted value of the global installed data center base by around US$388bn, equivalent to 38% of asset value before adaptation[20]. Business interruption accounts for almost one third of total modeled losses, with more than 90% arising from upstream supply chain disruption rather than direct physical damage. For next-generation AI facilities, physical hazards account for around 94% of modeled climate value-at-risk, making resilience an increasingly important consideration in site selection, engineering, underwriting and investment decisions.

"The next phase of AI infrastructure investment will therefore be defined as much by risk management as by technology. Capital, demand and innovation remain powerful tailwinds for the sector. The projects that succeed will increasingly be those that can secure reliable infrastructure, navigate regulatory hurdles, manage physical risks and deliver resilient assets that can operate reliably over decades," says **Hazem Krichene, Senior Climate Economist, Allianz Research.**

Composition of climate value at risk for legacy and AI-era data center facilities



Sources: Schneider Electric Research Institute, Allianz Research

Insurance is becoming a critical enabler of AI infrastructure

As data centers evolve from commercial real estate into mission-critical infrastructure, the role of insurance is expanding beyond protecting physical assets to supporting investment and operational resilience.

Comprehensive insurance cover has become a prerequisite for financing many large-scale AI infrastructure projects. Construction costs for a single AI campus can exceed US$20bn, with insured values increasing substantially once high-performance computing equipment is installed. Lenders and investors increasingly require robust insurance programs throughout both construction and operation, making insurance an important component of project finance. As facilities become larger and more technologically complex, business interruption and operational continuity are becoming at least as important as protection against physical damage. According to the Uptime Institute[21], 45% of outages originate from power-related failures, highlighting the importance of engineering expertise alongside underwriting.

Three structural shifts are reshaping commercial insurance for AI infrastructure. First, underwriting is becoming engineering-led. As AI infrastructure evolves faster than historical claims data can accumulate, underwriting will increasingly rely on engineering expertise, technical assessment and forward-looking risk modeling rather than traditional actuarial experience alone. Second, insurers are moving further upstream in risk management. Companies increasingly value insurers that combine risk transfer with engineering advice, resilience planning and operational risk management to reduce losses before they occur. Third, concentration risk is emerging as the defining underwriting challenge.

"AI campuses combine exceptionally high insured values with growing geographic clustering, increasing accumulation risk across locations, perils and lines of business. Managing these concentrated exposures while providing sufficient insurance capacity will become a key differentiator for commercial insurers," says **Katharina Utermöhl, Head of Thematic and Policy Research, Allianz Research.**

A fast-growing specialty market

The rapid expansion of AI infrastructure is creating one of the fastest-growing specialty markets in commercial insurance. Global insurance premiums associated with data centers are projected to more than double by 2030, from around US$11bn today[22] to more than US$24bn reflecting rapid capacity expansion, rising insured values and increasing operational complexity. Demand is expected to extend beyond traditional property cover towards integrated solutions spanning construction, engineering, property, business interruption, cyber and liability, while creating new opportunities in areas such as energy resilience, operational continuity and technology risk.

"As AI infrastructure becomes increasingly important to the global economy, insurance is evolving alongside it," says **Katharina Utermöhl, Head of Thematic and Policy Research, Allianz Research.** *"While its primary role remains the transfer of financial risk, insurers are increasingly contributing engineering expertise, risk modeling and resilience planning throughout the project lifecycle. As data centers become larger, more complex and more interconnected, these capabilities will play an increasingly important role in supporting the safe, resilient and financially sustainable expansion of AI infrastructure."*

The data center risk landscape

Rapid growth, technological complexity, and rising exposures are reshaping risk profiles.

As data center projects scale up to meet mushrooming demand, facilities are morphing from simple single-story warehouse premises to campus-like hyperscale parks with multi-story facilities and on-site power generation.

Commercial imperatives and land constraints are seeing developers expand into less-than-ideal locations, operating under compressed construction timelines, and facing scrutiny from regulators and local communities. This pressure comes as data centers take on an ever more critical role.

What makes a data center construction project complex?

Simple project
- Low natural catastrophe exposure
- Single story / spatially-separated buildings
- Value spread across campus
- Simple topography, greenfield
- Purpose-built for tenant
- No prototypical elements
- Adequate construction timeline

Complex / higher risk project
- Higher natural catastrophe exposure
- Multi-story facilities
- High value concentration
- Steep terrain, poor ground conditions
- Retrofitting existing buildings
- Second hand / prototypical equipment
- Compressed schedules, late scope changes

"Data centers are developing into deeply integrated infrastructure assets within the digital economy," says **Daniel Schroeder, Senior Risk Engineer, Allianz Commercial.** *"Successful operation depends upon the seamless interaction of power grids, water supply, and data connection. Power, capacity, and resilience will be the differentiators going forward, not simply floor space.*

"Recognizing data centers as critical infrastructure hubs compels clients and insurers to take a more holistic approach to risk. Rather than focusing solely on the building envelope, we must look at interdependencies, single points of failure, and systematic exposures."

Construction complexity brings uncertainty

Data centers are highly complex structural and technological projects with a set of attendant risks. Scale, increased structural loads, shortened timeframes, ongoing scope and design alterations, and late changes all introduce uncertainty, particularly with issues around quality assurance.

"These projects need to be conceived, managed, and addressed with the potential impacts of decisions made known from the very beginning and adequately designed for," adds **Schroeder.**

Data center developments are increasingly incorporating substantial on-site power generation infrastructure, blurring the traditional boundaries between civil construction and power risks. Technologies ranging from large fleets of internal combustion engines to prototype turbine designs create additional risk assessment, reliability and resilience considerations, particularly where developers have limited power-generation experience.

Another key risk driver is the use of multi-story facilities, as they have high structural loads (data centers are very heavy) and high concentrations of value. They also present heightened fire risk, as fire and smoke can spread throughout the building via risers and vents. Adapting designs for different loads, such as changing where the penetrations are (openings in walls, floors or ceilings), can also introduce high complexity.

Common loss scenarios in construction and operation

Punyawee / Adobe Stock

Fire and smoke

Fires in data centers are relatively rare, but they can have serious consequences. Risks are intensified by the increasing scale and density of equipment, temporary power and generators being used because of grid constraints, compressed construction schedules leading to human error, and the increased scale of power generation and battery installations.

Unlike lead-acid batteries, which are traditionally stored in separate battery rooms, lithium-ion batteries are increasingly being integrated directly into server racks. *"This is like letting the fox into the henhouse,"* says **Schroeder.** *"Damaged cells in a lithium-ion battery can remain dormant for days or weeks before a defect surfaces. When it does, the result could be a 'thermal runaway' – a high-temperature self-sustaining fire that is very hard to control."*

shutterstock0012 / Shutterstock

Natural catastrophes

The race for space and the renewable energy demands of data centers are pushing construction into areas with greater natural catastrophe exposure, particularly from tornados, floods, wildfires, and severe convective storms. Nearly 80% of global data center capacity is located in areas with elevated exposure to acute natural hazards, while over half (54%) is exposed to chronic heat and drought stress.

Data centers in remote locations are at further remove from emergency services and could also face potentially higher losses from natural catastrophe events due to lack of permanent flood protection and stormwater management.

AY Amazefoto / Shutterstock

Water damage

Water risk can be presented by flooding, water scarcity, and leaks.

Flooding is a particular concern with basements, excavations, and – importantly – stored equipment. Care needs to be taken when deciding how and where storage is placed, what type of concentration of storage is used on the site, and how this is being protected.

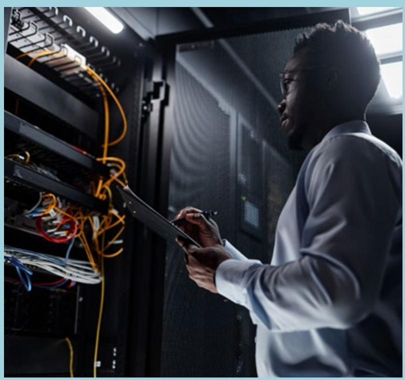
Water shortages can lead to equipment overheating and disrupt operations. Leaks are also a growing concern in the construction space, typically caused by cooling and fire systems. *"Leak detection tools are a powerful defence,"* **Schroeder** advises. *"You can't always prevent the loss, but you can significantly reduce the consequences if you take a proactive rather than reactive approach to managing water leaks."*

Tossatis chongjiraqal / Shutterstock

Power risk

The increasing use of refurbished or prototypical turbines in data centers raises questions about condition and reliability. Accessing original equipment manufacturer (OEM) support for a used component could be more difficult than if it were new, which would be a particular concern during testing and commissioning, says **Chris Fancher, US Head of Construction Property at Allianz Commercial:** *"This risk could be compounded where combustion engines are used as alternatives or supplements, often in high-density layouts with complex fuel control and exhaust systems that elevate the risk of fire and equipment damage during construction."*

Demand uncertainty is another key risk driver, with late changes to capacity and redundancy requirements often resulting in design revisions and scope adjustments. The growing integration of battery storage systems also alters power risk profiles and compounds the potential for loss.



SeventyFour / Shutterstock

Testing and commissioning – when risk peaks

Testing and commissioning (T&C) is a vital stage of any construction project. *"However, it is not a single event, but a series of controlled risk steps,"* says **Fancher.** *"T&C represents one of the single highest risk phases in data center construction. It is the point when systems go live for the first time and are pushed close to their operating limits."*

Unlike earlier parts of a project, T&C has an immediate and high-impact loss potential. Often, there are no early warning signs at this stage, unlike structural overload, for example.

"We all understand that construction projects have to be completed in a timely fashion so they can become operational and start to generate revenue," says **Fancher.** *"However, some stages cannot, and must not, be rushed."*

Four testing and commissioning risk factors

Latent defects: Defects can surface when a data center becomes live. Small errors can cascade across multiple systems (for example, incorrect settings, sequencing, torquing).

Temporary systems: Interim power and cooling systems are often used before permanent systems are resilient and ready. These might lack full redundancy and the same protections offered by permanent installations.

Time pressure: Commercial deadlines can compress schedules, reducing time for fault-finding and corrections.

Human element: With multiple contractors, OEMs, and specialists working simultaneously, overlapping responsibilities can create complications. A robust health and safety culture must be embedded in the project and upheld on-site.

Hyperscalers and accumulation risk

The evolution of data centers from traditional warehouse-like premises to large-scale campus facilities calls for a 360 approach to underwriting and risk assessment, as **Stefan Zink, Global Property Industry Lead, Telecoms and Data, at Allianz Commercial**, explains:

"With a hyperscaler, accumulation risk arises when multiple insured interests converge in one physical or operational space. You have the operators, multiple tenants, ongoing construction, and supporting utilities, all concentrated in one location. This risk builds across layers."

The **operator** of the data center is the foundation layer of insurance and involves property damage coverage to the physical structure and loss of rent coverage. Fire, flood, and power failure can become major losses due to the scale of the facility.

Tenants add a layer of further complexity – densely packed servers, networking hardware, and storage all increase the value per square meter at the insured location. Single events can trigger multiple equipment and business interruption claims, while storing equipment during upgrades or migration can cause exposure spikes and even stock policies can be involved.

Construction introduces risks from live expansion projects adjacent to operational halls, hot works, contractor interfaces, and transitional power configurations. These overlap in time and space, meaning one loss event can trigger multiple policies simultaneously.

Finally, **supporting infrastructure** such as on-site power plants and water pumping stations, bring their own risk profiles. Machinery breakdown or fuel supply failure can escalate into campus-wide business interruption.

Data center evolution and risk implications

Traditional

Company-owned, on premises, predictable workloads

Risk profile: Manageable, well-understood

Edge

Smaller, distributed, low-latency Internet of Things (IoT) applications

Risk profile: Less redundancy, localized risks

Colocation

Multi-tenant, shared infrastructure, anchor tenants

Risk profile: Higher aggregation, interdependency

Hyperscale

Purpose-built campuses, 100s of MW, grid connections, onsite substations

Risk profile: Critical infrastructure, systemic exposures

Infrastructure interdependencies

The role of data centers as critical infrastructure hubs creates dependencies that extend far beyond a facility's building envelope, particularly power, water, and connectivity needs.

Power is the most critical dependency, as data centers need reliable, high-capacity electricity and have a low tolerance for interruption. This makes grid stability, redundancy, and onsite backup essential. It also introduces exposure to upstream failures and new onsite risks such as lithium-ion battery fires.

Water availability and environmental restrictions can affect operational continuity, while liquid cooling systems carry potential damage risks. High-efficiency cooling, optimized airflow, and renewable energy sourcing can help reduce both energy consumption and carbon intensity.

Connectivity is a priority for data centers, as proximity to fiber routes and network nodes is a major competitive advantage. However, this creates dependency on external data links as well as vulnerability to cable damage and regional power outages originating offsite.


hrui / Shutterstock


Nutruja Phongsupat / Shutterstock


asharkyu / Shutterstock


Gorodenkoff / Shutterstock

Common claims and loss trends

The rapid expansion of advanced data centers is still a relatively new phenomenon, but emerging claims trends show that major losses can impact multiple stakeholders across the whole value chain.

A wide range of claims can arise from both the construction and operational stages of a data center, says **Christian Kolbe, Global Head of Construction Claims at Allianz Commercial:** *"These might include damage to servers from improperly secured equipment during transit, or the theft of materials from temporary storage, construction sites, or in transit. We see claims stemming from faulty workmanship, faulty design, construction defects, and claims arising during testing and commissioning.*

"Once a data center is operational, claims can result from power outages or surges, thermal runaways, and fire. HVAC [heating, ventilation, and air-conditioning] and chiller malfunctions and cyber-attacks are increasing. Natural catastrophe risk extends across the entire data center value chain."

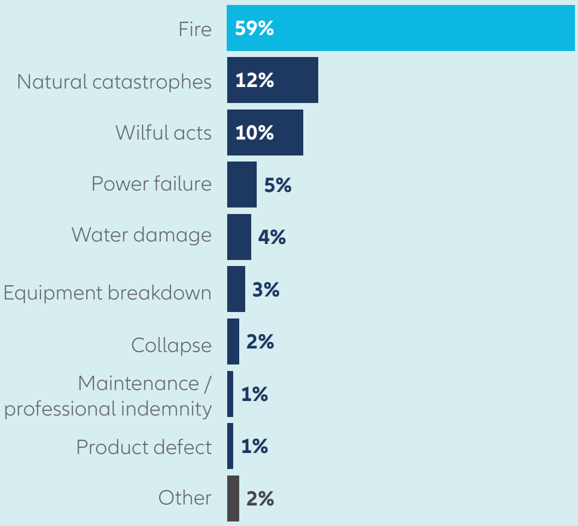
Allianz Commercial claims analysis shows water damage is the most common cause of loss for data centers, followed by wilful acts (largely cyber crime related), fire, and equipment breakdown *[see charts]*. However, fire overwhelmingly drives loss severity, followed by natural catastrophes, wilful acts, and power failure, with water damage ranking fifth.

By line of insurance business, business interruption – covered under property – is the primary severity driver, highlighting the operational phase as the major source of data center claims. Construction ranks second followed by financial lines (including professional indemnity claims).

Geographically, Europe accounts for the highest volume of claims (53%), followed by the US (36%), and Asia (8%). However, severity tells a different story: Europe still leads (38%), but North America is almost on an equal footing (36%), with Asia accounting for 21%.

Top causes of loss

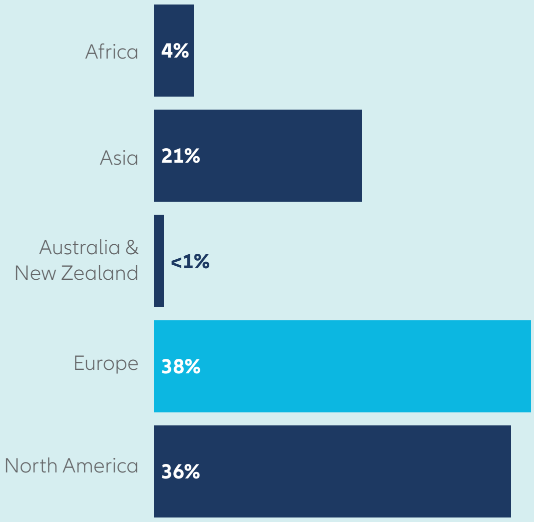
by claims value (% share)



Fire is the most expensive cause of data center losses, followed by natural catastrophe activity and wilful acts (including crime and cyber crime).

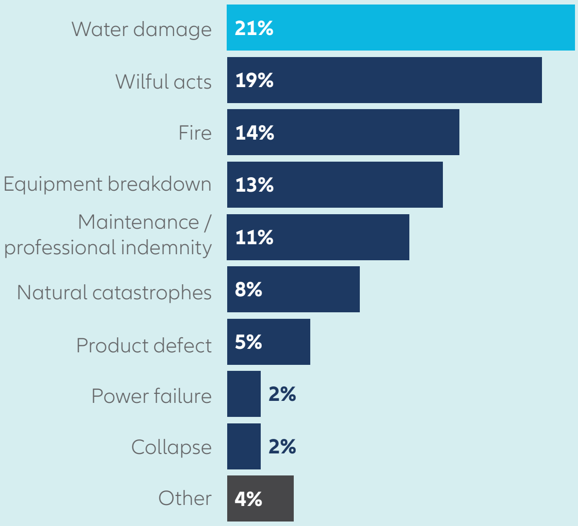
Value of claims by region

% share



Top causes of loss

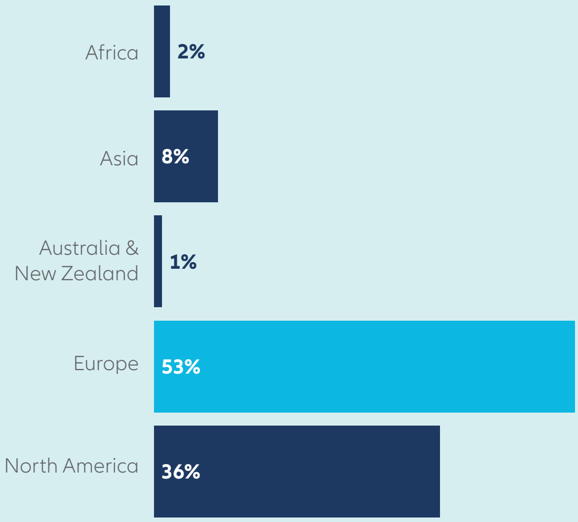
by number of claims (% share)



Water damage is the most frequent cause of insurance claims, followed by wilful acts (including crime and cyber crime), and fire / explosion.

Number of claims by region

% share



Europe and North America dominate the share of losses according to both the number and value of claims.

Based on analysis of 221 claims with a total value of approximately €677mn (based on the 100% loss event total, including the shares of other insurers in addition to Allianz Commercial).

Common data center claims types

Beyond immediate physical losses, incidents at data centers can give rise to liability claims, contractual disputes, and lasting reputational damage.

High-rise data centers face significant physical risks, with structural defects in cooling and power systems often leading to major, costly delays and disputes.

Data center failures can lead to significant financial loss and reputational damage for both operators and clients, requiring robust business interruption and property insurance coverage.

As infrastructure is shared, cyber-attacks targeting building management systems or servers can cause widespread damage, triggering complex liability claims across multiple tenants.

Increased scrutiny regarding energy and water consumption, along with noise or vibration complaints from surrounding areas, present increased environmental and liability risks.

Failure to meet technical specifications, such as uptime standards or power capacity, can result in significant legal disputes and contractual penalties.

Different phases, different interests

Data center projects encompass different project phases with several stakeholders and interests involved, which can create complications, says **Charlotte Field, Regional Head of Short-Tail Claims, Asia, at Allianz Commercial.** *"Under construction, you have the owner, developer, contractor, and subcontractors, then in the operational phase, there are the owner-operator and potentially multiple tenants, or end users.*

"Clarity is critical with an insurance claim. Clearly documented handovers are essential between your CAR [construction all-risk] policy and operational policy. There must be no ambiguity about practical completion, in order to avoid disputes over which policy responds to a particular event and the extent of cover."

"Clarity is critical with an insurance claim

panumas nikhomkhai / Shutterstock

Make more Aerials / Shutterstock

What can go wrong at a data center?

Five case studies of claims arising from real-life events

Where	When	Damage / loss	Cause	Claimant	Claim amount
AI data center	Testing and commissioning	Cracking in chiller units	Operation beyond design limits	General contractor	**US$25-50mn**
Hyperscaler / cloud data center	Late construction, near completion	Smoke and soot migration through air circulation systems to large parts of the building	Hot works-related fire	Owner / future operator	**US$50-100mn**
Hyperscaler / cloud data center	Construction	Damage to external cooling systems, with 60 chillers affected at a replacement cost of US$360,000 each	Hail and strong winds	Owner / future operator	**US$50-100mn**
Hyperscaler / cloud data center	Construction	Delay in startup caused by power disturbances	Power surge and trip	Owner / future operator	**€25-50mn**
AI data center	Construction	Structural failure of internal site access and a logistics bridge spanning protected wetland	Collapse	Owner / developer	**US$5-10mn**

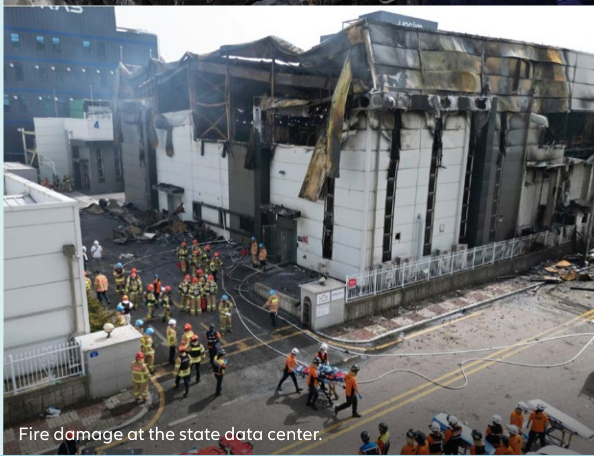
Fire protection and a stress test from South Korea

A 2025 fire at a state data center in South Korea illustrated how quickly a single incident can escalate – knocking out digital systems across the country and causing widespread disruption to government services.

The fire was believed to have been sparked by a battery explosion at the National Information Resources Service in Daejeon, south of the capital, Seoul. The resulting thermal runaway produced extreme heat in the server room, preventing firefighters from taking aggressive action to contain the blaze. 600 servers[23] were forced into shutdown to protect data while firefighters worked to extract around 400 battery packs from the building as a safety measure.

"This was a devastating example of the potential ferocity of battery fires and the challenge thermal runaway presents to emergency response," says **Charlotte Field, Regional Head of Short-Tail Claims, Asia, Allianz Commercial.** *"Integrating lithium-ion batteries into server rooms introduces significant complexities."*

Yonhap News Agency



Newsis via AP

Fire damage at the state data center.

Restoration complexity after fire

Reinstatement after a data center fire is a complex process that can involve the replacement of specialized equipment, infrastructure rebuild, fire sprinkler systems, reinforced floors, specialized HVAC systems, and cooling networks.

"When it comes to reinstating services or complex electrical equipment, we need to assess the extent of damage and whether restoration is possible," **Field** adds. *"A repair might be technically feasible, but could create uncertainty about future reliability, which then raises questions linked to manufacturer warranties.*

"We also have to consider temporary locations, solutions, and interim hardware to minimize operational disruption while permanent repairs are made. Timelines and costs will vary significantly based on the size, location, and power capacity of the facility. It is a massive undertaking that might require specialized IT asset disposition vendors."

Fire suppression and unintended consequences

Fire suppression measures themselves can introduce risks and complexities. Their operation can produce vibrations and noises that damage sensitive server equipment, particularly clean-agent and gaseous suppression systems used in server rooms and data centers. Any resulting damage can be compounded by installing racking too close to sprinklers.

Aspirating smoke detectors (designed for microscopic particle detection) can be falsely activated by dust, condensation or construction debris, leading to the accidental emission of a gaseous fire suppressant (a 'gas dump').

"Best practice here would be a 'double knock' approach," says **Field.** *"This is where two separate sensors must detect smoke to activate the system.*

"There is also a risk with contamination and humidity from mistakenly activated fire suppression systems, which can reduce the lifespan of server equipment and lead to hardware failure."

Broader risk factors and barriers to reinstatement

Supply chain disruptions can occur anywhere in the data center value chain, from suppliers, manufacturers, distributors, and even customers.

Strong demand from data centers has stretched manufacturers to capacity, leading to component shortages affecting utility companies and other industries. According to McKinsey, lead times for critical equipment in North America – such as medium-voltage switchgear and transformers – now extend to 80 and 50 weeks respectively[24]. With domestic manufacturing unable to keep pace, the US has relied on imports from Asia and other regions.

"This can result in delays to reinstatement periods and, consequently, increase business interruption losses," says **Christian Kolbe, Global Head of Construction Claims, Allianz Commercial.**

"Business interruption can include the loss of revenue, lease payments during downtime, potential contractual terminations, and increased costs to relocate services," **Kolbe** adds. *"Data center operators can pay significant contractual penalties arising from downtime, which might not be covered by traditional property insurance."*

Failure to meet technical specifications, such as uptime standards or resilience requirements, can lead to substantial financial consequences.

British Airways' 2017 data center outage cost an estimated £80mn ($102mn)[25] and resulted in legal action against facilities manager CBRE, while OVHcloud was ordered to pay €250,000 ($270,000)[26] to customers after a court found it had failed to deliver promised backup services following its 2021 Strasbourg data center fire.

Even less severe incidents can be costly. Data center operators that miss contractual uptime commitments are often required to provide service credits under Service Level Agreements (SLAs). These credits are typically limited to a percentage of the customer's monthly service fees and, while often modest relative to the customer's total losses, can become a significant expense when an outage affects multiple customers simultaneously.

Current infrastructure is not yet fit for future demand, making power supply and stability a significant claims issue. Maintenance, in particular, is critical to ensure 24/7 uptime, prevent catastrophic high-cost failures, and maximize the lifespan of equipment IT hardware, **Kolbe** says: *"Regular monitoring of components so they can be replaced before they fail is essential. Preventative maintenance is far preferable to a catastrophic failure and a lengthy reinstatement."*

Geopolitical instability is amplifying supply chain risks, with data centers emerging as strategic targets given their increasingly vital role in national and economic infrastructure.

> "Failure to meet technical specifications, such as uptime standards or resilience requirements, can lead to substantial financial consequences

panumas nikhomkhai / Shutterstock

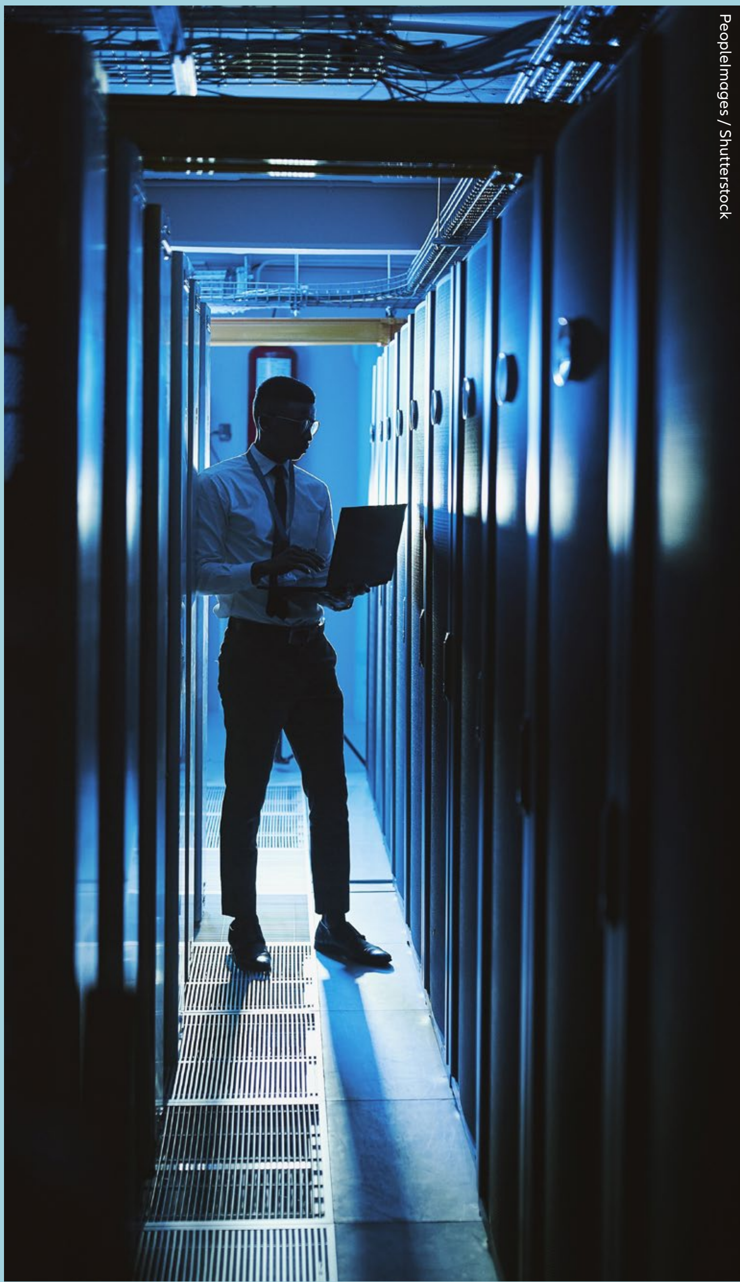
Risk evaluation, mitigation, and insurability

Rapid data center evolution calls for a rethink of risk management – and poses new questions about insurability.

When it comes to fundamental risk management, the location of a data center is clearly important, says **Stefan Zink, Global Property Industry Lead, Telecoms and Data, at Allianz Commercial:** *"It's particularly key for reducing natural catastrophe risk, such as avoiding flood plains and ensuring access to emergency services."*

Building quality and design, business continuity planning, access to critical supporting infrastructure such as water and reliable grid connections, are also key to long-term insurability, **Zink** adds: *"Systems should be designed for replaceability and resilience. There should be physical separation between fuel sources and battery systems to reduce fire risk. Operational discipline must be maintained, including regular component monitoring, replacement before failure, and preventive maintenance programs."*

If material changes occur during construction or operation, insurers need to know, says **Zink.** *"Transparent, proactive communication ensures that an insurance program evolves with the asset, providing continuous coverage, stable capacity, and more consistent terms over time."*



PeopleImages / Shutterstock

> "
>
> If material changes occur during construction or operation, insurers need to know

Challenges to insurability

The core challenge to insurability is interdependency. Data centers combine real estate, industrial infrastructure, and highly sensitive technology in a single location. This means the same loss event can trigger multiple claims, whether it's a power outage, cooling failure, or severe weather. *"The value concentration of these facilities means that a low probability event like a direct tornado hit could produce unprecedented losses,"* says **Stefan Zink, Global Property Industry Lead, Telecoms and Data, Allianz Commercial.**

Effective and coordinated insurance buying is essential to avoid both gaps and overlaps in coverage, according to **Zink,** with emerging risk profiles continuing to raise the bar: *"Hyperscale facilities are evolving so quickly. Server architectures are changing, power densities increasing, direct-to-chip cooling is coming in. New business models are also emerging, with developers providing full management services or performance SLAs [service level agreements] rather than simply leasing space. This all calls for a completely new approach to risk assessment."*

Underwriters focus on several key factors: value concentration; interdependency, including connectivity; power; water sources; site uptime, and back-up plans; and accumulation, which examines whether the operator, a single tenant, or multiple tenants are insured, and the total exposure across policies at the same site.

PML (probably maximum loss) calculations usually place the bulk of value in equipment or servers, says **Zink.** Fire is the most common PML driver, but flood and tornado can be governing loss scenarios, depending on a data center's layout and location.

Risk mitigation best practices by project phase

Design phase: purpose-built buildings preferable to retrofitted; spatial separation strategies; adequate structural load planning for multi-story buildings; compartmentalization and vertical pathway control; and early detection systems integrated from the outset. For lithium-ion batteries, these systems include VESDAs (very early smoke detection apparatus), ASDs (aspirating smoke detectors), and off-gas detection, which detects lithium-ion battery vapors.

Construction phase: realistic scheduling (resist compressed timelines); robust quality control (QA) for late scope changes; temporary condition management protocols; and equipment storage protection, such as elevation or separation.

Testing and commissioning: adequate time for fault-finding; managed transition from temporary to permanent systems; coordination protocols for multiple contractors; and embed a robust safety culture.

Operational phase: preventative maintenance programs; component monitoring and replacement before failure; cooling system redundancy; leak detection systems; and fire suppression system testing and maintenance.

Coordinated insurance solutions for data center risk

Data centers bring together multiple stakeholders and assets in one location, making coordination essential across clients, brokers, insurers, investors, and tenants.

Single events impacting a data center, whether natural or human-caused, can trigger multiple claims across different policies. This requires an integrated approach to risk management to prevent coverage gaps or overlaps. As circumstances evolve, timely communication of tenant, design, or scope changes ensures insurance remains aligned with actual exposures.

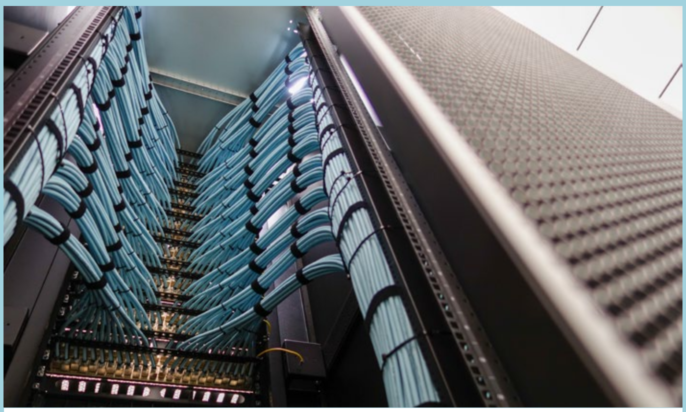
While location and building risk quality are key considerations, so too is business continuity management (BCM) and a thorough evaluation of potential cascading failure scenarios.

"Projects of this scale demand bespoke insurance structures. When construction values reach into the billions, a standard commercial policy cannot provide the breadth of coverage or precision of terms that all parties require," says **Darren Tasker, Head of Construction, Americas, at Allianz Commercial.** *"A well-structured program encompasses casualty coverages including project-specific or wrap-up liability and workers' compensation, professional liability for engineers, builder's risk during construction, and project cargo for the transportation of highly specialized equipment."*

Tasker adds that large-scale data centers represent a fundamentally different underwriting challenge from traditional construction risks: *"The pace at which AI infrastructure is evolving means engineering expertise and risk modelling assessments are critical. For the largest and most complex exposures, alternative risk transfer solutions, including structured solutions, captives and parametric solutions, are becoming an increasingly important part of how large technology companies manage risks that the traditional insurance market alone cannot always fully absorb."*

New risk assessment methods are needed to keep pace with rapidly changing designs and technology, as well as new business models being adopted by developers, says **Stefan Zink, Global Property Industry Lead, Telecoms and Data, at Allianz Commercial.**

"Underwriting, claims handling, and risk engineering across all insurance lines can be improved by a unified risk framework – a single, integrated approach to managing all risk types across an organization or project. Coordinated solutions simplify governance, reduce uncertainties, and enhance resilience during critical incidents. Proactive engagement between stakeholders builds trust and creates the long-term partnerships that are needed to insure these emerging types of digital infrastructure."



panumas nikhomkhai / Shutterstock

Cross-domain risk consulting

Allianz Commercial offers a Data Center Resilience advisory package spanning site validation, construction, and cyber, physical, climate, and operational risk assessments.

"Designed around the evolving risks of modern data center operations, the data center advisory package delivers a structured, end-to-end risk evaluation – from site selection and construction through to cyber security, physical protection, climate exposure, and operational uptime – integrating specialist expertise into a single, actionable resilience strategy," says **Lena Fuldauer, Head of Risk Consulting Resilience and Business Development, Allianz Commercial.**

↗ Find out more here.

References

1 International Energy Agency, Energy and AI, World Energy Outlook Special Report, April 10, 2025
2 International Energy Agency, Key Questions on Energy and AI, April 16, 2026
3 Omdia, Cloud and Data Center Market Snapshot, December 2025
4 Allianz Trade, Code, Carbon, Kilowatts: AI's Hidden Toll And The Race To Green The Grid, June 30, 2026
5 Wood Mackenzie, Transformer Troubles: Manufacturing And Policy Constraints Hit US Transformer Supply, August 13, 2025
6 International Energy Agency, Key Questions on Energy and AI, April 16, 2026
7 Information Technology & Innovation Foundation, Fact of the Week: Construction Industry Facing a 439,000-Worker Shortage Driven by the Growth of Data Centers, January 12, 2026
8 Associated Builders and Contractors, Construction Workforce Shortage: Causes, Impacts, and Practical Solutions, January 26, 2026
9 Data Center Watch, Q1 2026, Data Center Watch Report
10 Gallup, Americans Oppose AI Data Centers in Their Area, May 13, 2026
11 Washington Post, New York Becomes First State To Impose Data Center Moratorium, July 14, 2026
12 Data Center Dynamics, Dutch Government Halts Hyperscale Data Centers, Pending New Rules, February 17, 2022
13 Energy Connects, Ireland Ends Moratorium on New Power Links to Data Centers, December 12, 2025
14 CNBC, Nvidia Sheds Almost $600 Billion In Market Cap, Biggest One-Day Loss In US History, January 27, 2025
15 Data Center Dynamics, Chinese Government Plans Data Center Capacity Reseller Network Amid Overbuild Concerns, July 26, 2025
16 Allianz Research, AI Capex Cycle: War-Proof For Now, March 25, 2026
17 First Street Technology, 79% of Global Data Center Capacity Faces Elevated Climate Risk, June 18, 2026
18 Allianz Trade, Code, Carbon, Kilowatts: AI's Hidden Toll And The Race To Green The Grid, June 30, 2026
19 Pew Research Center, What We Know About Energy Use At US Data Centers Amid The AI Boom, October 24, 2025
20 Schneider Electric Research Institute, The Repricing of Compute, The Economics Of Climate Risk And Resilience for AI-Era CapitaL June 2026
21 Uptime Institute, Annual Outage Analysis 2025, May 2025
22 Swiss Re, Sigma Insights 07/2026: Insuring AI: Data Centre Value Accumulation Risks, March 27, 2026
23 Reuters, South Korea scrambles to restore services after major state data centre fire, September 27, 2025
24 McKinsey & Company, The $7 trillion data center build-out: How industrials can capture their share, March 27, 2026
25 Data Center Knowledge, CBRE Settles British Airways Lawsuit Over Costly Data Center Outage, February 12, 2019
26 Data Center Dynamics, OVHcloud ordered to pay €250k to two customers who lost data in Strasbourg data center fire, March 22, 2023

About Allianz Commercial

Allianz Commercial is the center of expertise and global line of Allianz Group for insuring mid-sized businesses, large enterprises and specialist risks. Among our customers are the world's largest consumer brands, financial institutions and industry players, the global aviation and shipping industry as well as family-owned and medium enterprises which are the backbone of the economy. We also cover unique risks such as offshore wind parks, infrastructure projects or film productions.

Powered by the employees, financial strength, and network of the world's #1 insurance brand, as ranked by Interbrand, we work together to help our customers prepare for what's ahead: They trust us to provide a wide range of traditional and alternative risk transfer solutions, outstanding risk consulting and multinational services as well as seamless claims handling.

The trade name Allianz Commercial brings together the large corporate insurance business of Allianz Global Corporate & Specialty (AGCS) and the commercial insurance business of national Allianz Property & Casualty entities serving mid-sized companies. We are present in over 200 countries and territories either through our own teams or the Allianz Group network and partners. In 2025, the integrated business of Allianz Commercial generated around €17.3 billion in gross premium globally.

Further information and contacts

commercial.allianz.com

Email: az.commercial.communications@allianz.com

Disclaimer & Copyright

Copyright © 2026 Allianz Commercial / Allianz Global Corporate & Specialty SE. All rights reserved.

The material contained in this publication is designed to provide general information only. While every effort has been made to ensure that the information provided is accurate, this information is provided without any representation or warranty of any kind about its accuracy and neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group can be held responsible for any errors or omissions.

All descriptions of insurance coverage are subject to the terms, conditions and exclusions contained in the individual policy. Any queries relating to insurance cover should be made with your local contact in underwriting and/or broker. Any references to third-party websites are provided solely as a convenience to you and not as an endorsement by Allianz of the content of such third-party websites. Neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group is responsible for the content of such third-party websites and neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group does make any representations regarding the content or accuracy of materials on such third-party websites.

Allianz Global Corporate & Specialty SE, Königinstraße 28, 80802 Munich, Germany.

Commercial Register: Munich, HRB 208312

August 2026