JLT PUBLIC SECTOR RISK REPORT QLD

7th Edition

SUMMARY

In Queensland, the ranking of risks faced by local government reveals significant insights into the challenges and priorities faced by councils. The data indicates that financial sustainability and cyber security/IT infrastructure are the most pressing concerns, each ranked this position by 58% of respondents.

This dual emphasis on financial health and technological resilience demonstrates that councils recognise the need for robust fiscal management for the management of operations as well as protecting their digital assets and systems against an increasing and evolving cyber threat landscape.

The management of ageing property, assets and infrastructure was ranked the next most pressing concern by respondents in Queensland. This highlights a critical issue for many councils, as aging infrastructure can lead to ballooning maintenance costs, safety or environmental impact, disruption in services and reputational damage. The need for strategic asset management is essential, as councils balance the demands of current residents with the necessity of planning for future growth and sustainability. The relatively high ranking of this risk compared to national results, indicates that Queensland councils may be facing more immediate challenges related to their existing assets.

High Risk	1-3 Rank
Medium Risk	4-8 Rank
Low Risk	9-12 Rank

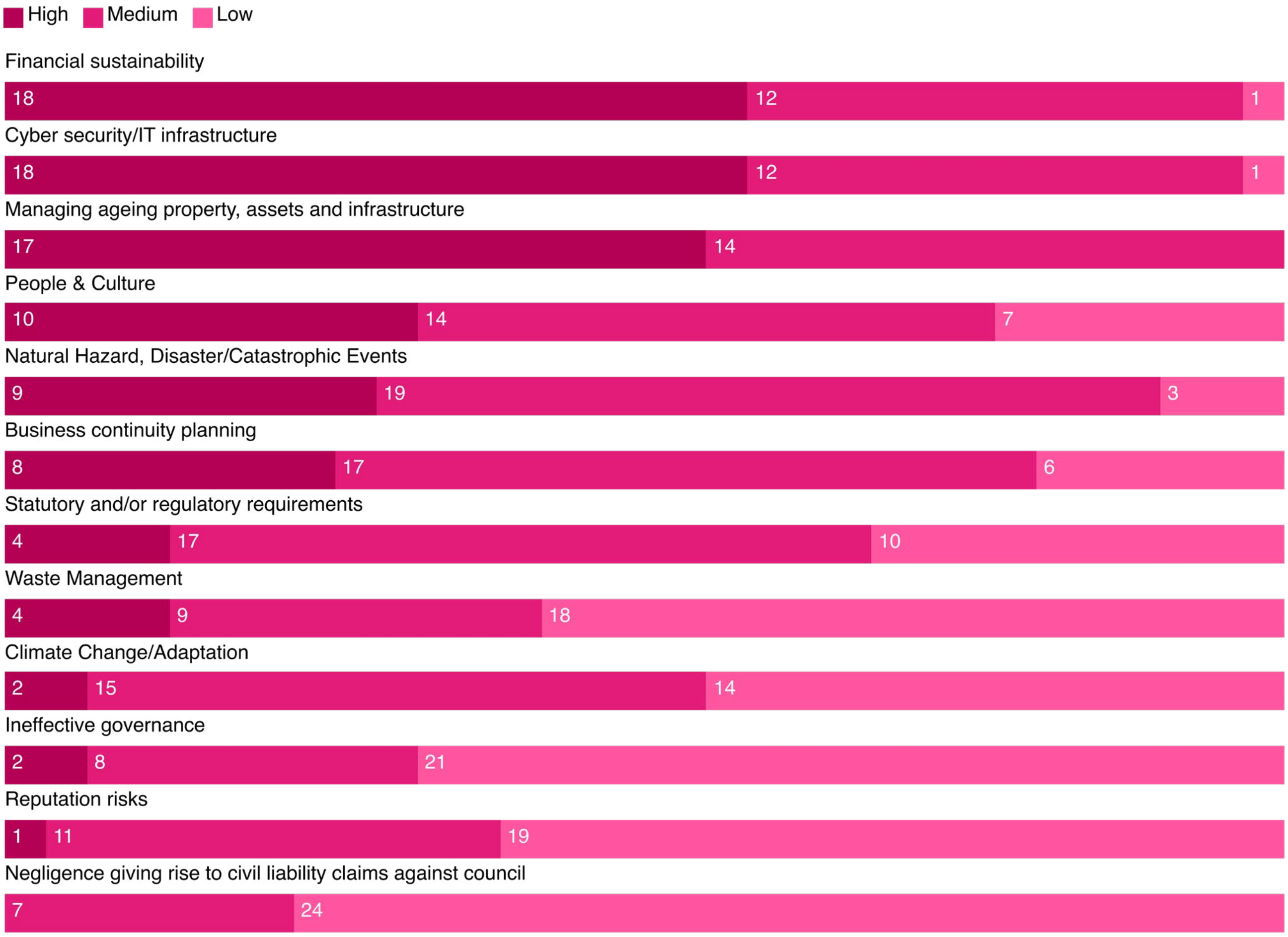


Figure 1: Ranking of Risks – QLD risk heat map

FINANCIAL SUSTAINABILITY

In 2024, financial sustainability remains the top-ranked risk for councils in Queensland, with 58% of CEOs identifying it as a critical concern. This ranking is indicative of an urgent and ongoing imperative to secure adequate revenue in a backdrop of inflation and constrained resources and is certainly reflective of the chronic and acute fiscal challenges faced by councils. The importance of financial sustainability cannot be overstated, as it directly impacts councils' ability to deliver essential infrastructure and services and support the social, economic and environmental outcomes expected by local communities.

The percent of CEOs ranking this as the leading risk slightly decreased in 2024 from 2023. Notwithstanding, the persistent high ranking emphasises the need for continued vigilance and proactive financial support to navigate economic uncertainties and ensure long-term organisational sustainability.

High Risk	1-3 Rank
Medium Risk	4-7 Rank
Low Risk	8-12 Rank

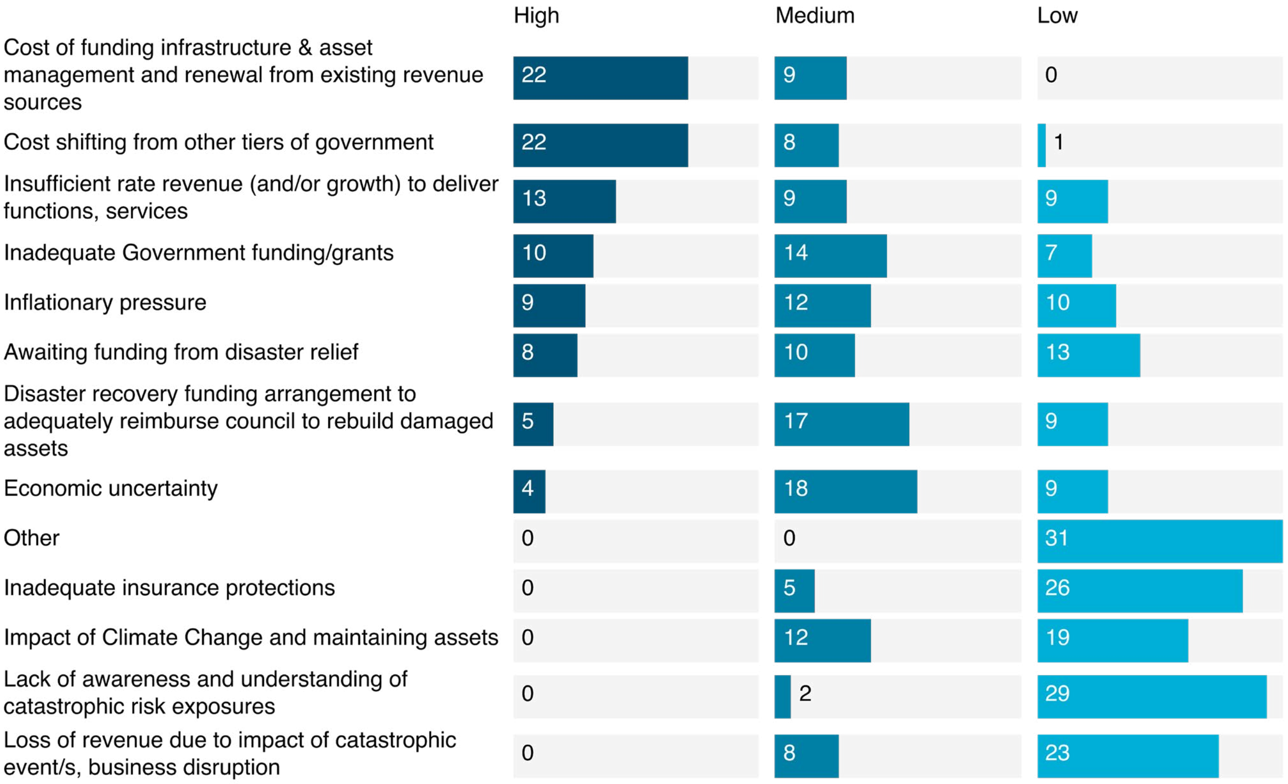


Figure 2: Financial Sustainability – underlying factors ranked

CYBER SECURITY

Cyber security & IT infrastructure risks were equally ranked with financial sustainability as the most pressing critical risk in 2024. While some councils are making progress in enhancing the resilience of their ICT systems, the persistent high ranking underscores the ongoing threat posed by malicious actors to cyber security.

The growing reliance on digital systems for service delivery and data management makes cyber security a paramount concern. The equal ranking with financial sustainability highlights the interconnectedness of these risks; a cyber incident could severely impact a council's financial standing, leading to significant operational and reputational damage.

Examining the underpinning factors contributing to the risk of cyber security reveals important insights into the evolving landscape of threats faced by councils. In 2023, the leading concern identified by 76% of respondents was the ability to respond to a cyber-attack. This remains relevant in 2024, but it has dropped to third position, with 64.5% of respondents recognising it as a critical factor. This change may indicate that councils are increasingly focusing on proactive measures rather than solely reactive responses. The ability to respond effectively to a cyber-attack remains highly relevant, but the emphasis appears to be shifting towards prevention and preparedness.

In 2023, the second most significant factor identified by 69% of councils was cyber security failure. In 2024, this concern increased to number one with 71% of respondents identifying it as the concern at their council. This shift highlights the need for increased focus on cyber security and the focus on preventing cyber security failures has intensified as councils become more aware of the vulnerabilities within their systems. This increased awareness is likely responding to the rising frequency and sophistication of cyber-attacks targeting public sector organisations, prompting councils to prioritise measures that mitigate these risks.

The third ranked factor identified by 62% of councils in 2023 was the ability of IT infrastructure and providers to proactively manage cyber security. This factor shifted to second position in 2024, with 69% of respondents identifying it as critical. This change indicates that councils are increasingly aware of the important role that their IT infrastructure and service providers play in maintaining cyber security. As cyber threats become more sophisticated, the need for proactive management of ICT systems is essential to prevent breaches before they occur. This proactive approach includes regular system updates, vulnerability assessments, multifactor authentication for remote and administrator functions as well as the management of critical infrastructure, and the implementation of advanced security measures.

The evolution of these underpinning factors reflects a broader trend in local governance, where councils are not only reacting to past incidents but are also taking a more strategic approach to cyber security. The increased focus on preventing cyber security failures and enhancing the capabilities of IT infrastructure providers suggests that councils are investing in training, resources, and technologies that bolster their defences against potential threats.

As cyber threats continue to evolve, councils must prioritise investments in robust IT infrastructure and comprehensive training programs for their staff. This dual approach will help safeguard sensitive information and maintain public trust, which is essential for effective governance. The interconnectedness of cyber security and financial sustainability emphasises the need for councils to adopt a holistic view of risk management, ensuring that all aspects of their operations are resilient against potential disruptions.

The rising prominence of cyber security as a critical risk in 2024 highlights the ongoing challenges faced by Queensland councils. By addressing the underpinning factors that contribute to this risk, councils can enhance their preparedness for future cyber incidents, ultimately fostering greater community confidence in their ability to protect sensitive information and maintain operational integrity. As the digital landscape continues to evolve, a proactive and comprehensive approach to cyber security will be essential for councils to navigate the complexities of modern governance effectively.

High Risk	1-3 Rank
Medium Risk	4-9 Rank
Low Risk	10-13 Rank

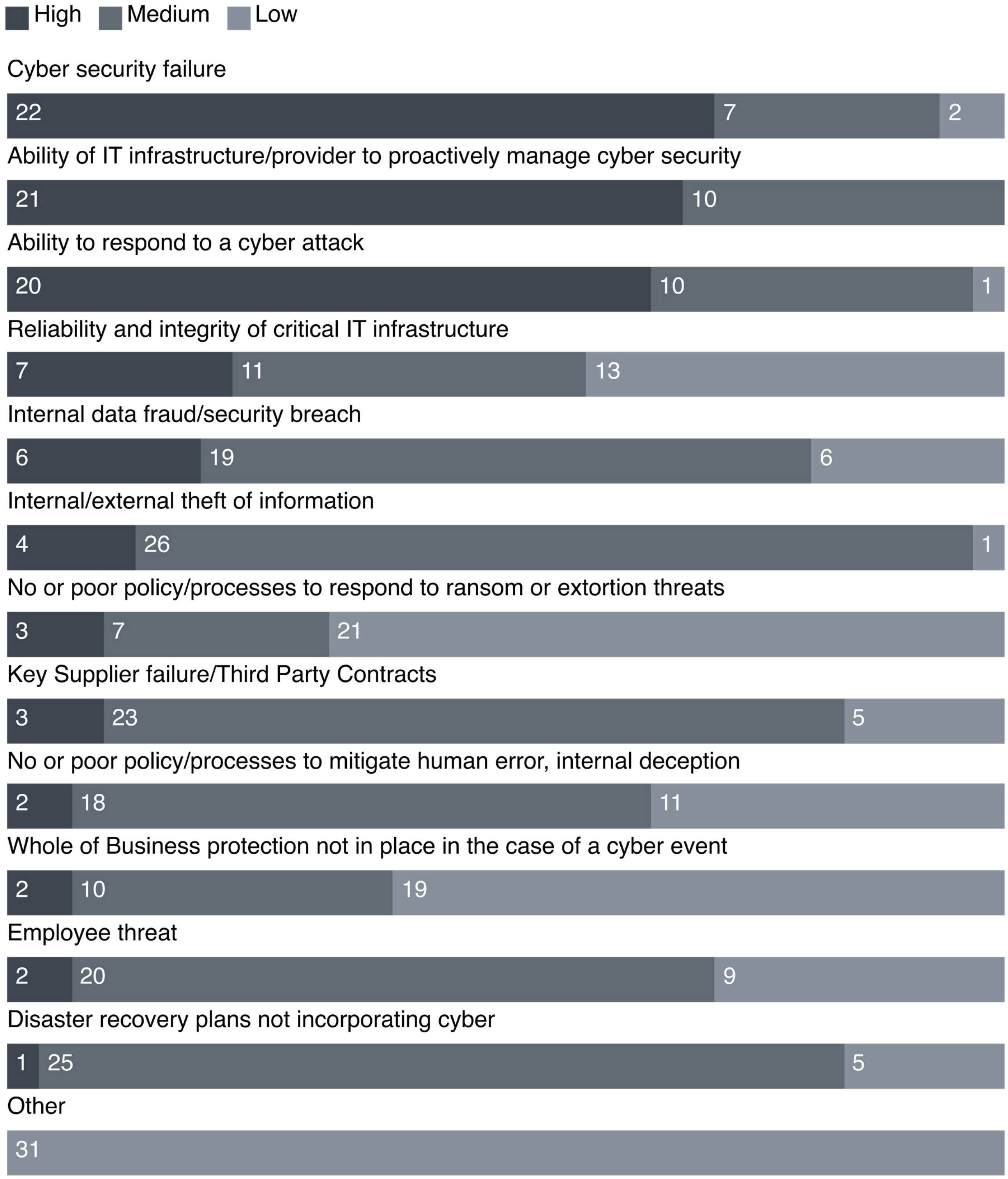


Figure 3: Cyber Security – underlying factors ranked

ASSETS & INFRASTRUCTURE

The third underpinning factor in 2023 was the destruction of council assets and infrastructure due to insured perils, such as fire, storm, or vandalism, which was recognised by 59.5% of respondents. In 2024, this concern continues to be seen as highly relevant, ranking third highest at 58%. The consistency in this ranking indicates that while councils are focused on natural disasters, they also recognise the importance of addressing risks associated with insured events. This dual focus on both natural and insured perils highlights the need for comprehensive risk management strategies that encompass a wide range of potential threats.

The evolution of these risk drivers is indicative of a broader trend in local governance, where councils appear to be increasingly prioritising resilience and preparedness. The rise in the importance of workforce-related risks indicates a shift towards recognising that effective business continuity planning is not solely about physical assets but also about the people who manage and operate those assets. As councils continue to navigate an increasingly complex risk landscape, the integration of human resource considerations into business continuity strategies will remain essential for ensuring operational resilience.

The significant rise of business continuity planning as a top risk in 2024 reflects a growing awareness among Queensland councils of the multifaceted challenges they face. By addressing the underpinning factors that contribute to this risk, councils can enhance their preparedness for future disruptions, ultimately fostering greater community confidence in their ability to govern effectively in times of crisis. The ongoing commitment to developing robust business continuity plans will be crucial in navigating the uncertainties that lie ahead, ensuring that councils remain resilient and responsive to the needs of their communities.

High Risk	1-2 Rank
Medium Risk	3-4 Rank
Low Risk	5-6 Rank

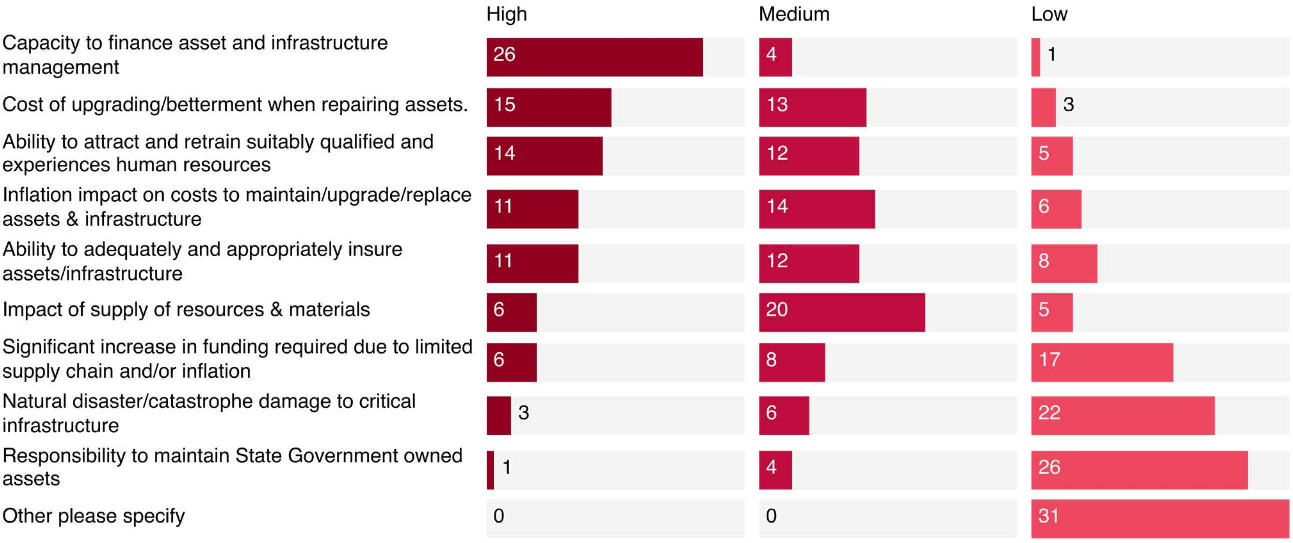
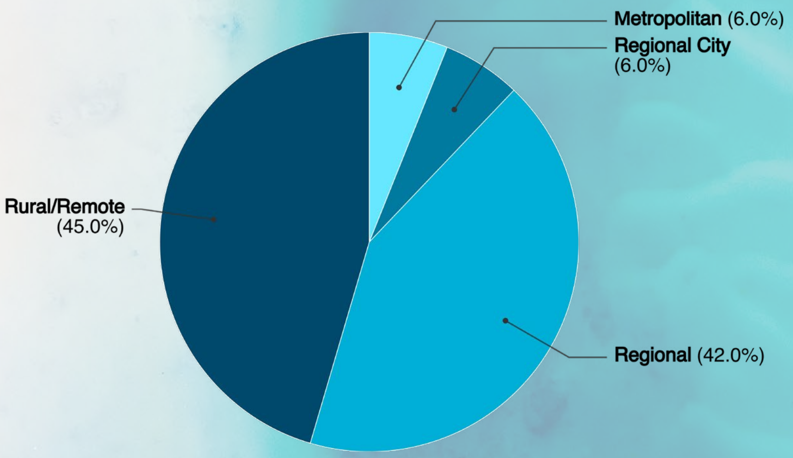


Figure 4: Assets & Infrastructure – underlying factors ranked

SURVEY RESPONDENTS

The 2024 JLT Public Sector Risk Survey engaged 31 local government CEOs and General Managers from QLD. Participants represented a diverse range of communities, including metropolitan, city, regional, regional city, and rural/remote areas. Below is a detailed breakdown of the respondents by community type:



This document and any recommendations, analysis, or advice provided by JLT (collectively, the 'JLT Analysis') are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. This document contains proprietary, confidential information of JLT and may not be shared with any third party, including other insurance producers, without JLT's prior written consent. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modelling, analytics, or projections are subject to inherent uncertainty, and the JLT Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Except as may be set forth in an agreement between you and JLT, JLT shall have no obligation to update the JLT Analysis and shall have no liability to you or any other party with regard to the JLT Analysis or to any services provided by a third party to you or JLT. JLT makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or re-insurers. JLT makes no assurances regarding the availability, cost, or terms of insurance coverage.