CPAs & ADVISORS

2025

Top Risks for Nonprofits and Associations

Risks facing organizations are evolving at an unprecedented pace.

The Risk and Advisory Services team at GRF has analyzed the top risks predicted by political, economic, and business experts as well as insights from our 40+ years of experience serving nonprofits and associations.

Join us in exploring the dynamics of 2025's top risk themes and the potential implications for nonprofits and associations.

THEME 1

Legislation and Policy Change

As the new administration, House of Representatives, and Senate begin a new term, they will be considering many proposals for legislation and policies that could significantly impact tax-exempt organizations. Many of the proposed changes will not be enacted, but the need to prepare for potential outcomes will impose real costs associated with monitoring proposals, strengthening compliance efforts, and potentially reducing mission-related activities.

There are three areas of potentially significant impact:

1. **Funding**
2. **Tax-Exempt Status**
3. **Tax Liabilities**

1 Funding

Expected spending cuts will significantly impact nonprofits reliant on grants and contracts from the federal government. These reductions in funding could be accompanied by an increase in demand for the services of many nonprofit organizations, as individuals and communities impacted by reduced government programs turn to nonprofits for support – particularly in the areas of healthcare, education, and social services. Recent executive orders temporarily freezing funding may threaten some organizations' ongoing operations, or even their long-term existence.

Several key provisions of the 2017 Tax Cuts and Jobs Act (TCJA) are set to expire in 2025, but many are expected to be extended, including the increased standard deduction. This provision resulted in a dramatic drop in funding for nonprofit organizations since it reduced the number of taxpayers who itemize, thereby eliminating the tax advantages associated with charitable donations for most middle-class Americans. There are proposals to reinstate a charitable donation tax benefit for non-itemizers, but the outlook is not positive given projected budget deficits resulting from tax cuts in other areas.

The need to raise revenue to offset the extension of some TCJA provisions could result in the nonprofit sector being a source of revenue-raising provisions, as it was with the wildly unpopular "parking tax" in the TCJA. While this provision was eventually repealed, costs to comply, pay, and then request a refund burdened nonprofits large and small. Some

of what has been floated already may only apply to certain sectors of the nonprofit community, e.g. the increase in the endowment tax on some higher education institutions; however, all nonprofits need to remain vigilant.

Any funding gap for nonprofits that may result from revenue-raising provisions enacted could potentially be counterbalanced. If stricter timelines for payouts are imposed on donor-advised funds (DAFs), which currently have no statutory annual distribution requirements, there could be an increase in donations from these funds.

2 Tax-Exempt Status

The Stop Terror-Financing and Tax Penalties on American Hostages Act (H.R. 9495), which passed the House of Representatives in late 2024 and will likely be taken up by the new Congress in 2025, intends to target terrorist-supporting organizations. Funding and promoting terrorism are already illegal and can result in the loss of the organization's tax-exempt status. The potential lack of transparency around the Treasury Department's expanded authority to challenge organizations' tax-exempt status is raising concerns from nonprofit advocacy groups that organizations with lawful activities, such as aiding refugees and immigrants, will be affected. Under the proposal, accused organizations would bear the burden of proof and have 90 days to establish their innocence before losing their tax-exempt status. Even those that successfully overturn the designation may suffer significant reputational damage and a loss of trust among donors and the communities they serve.

Other challenges include proposals to revoke the tax-exempt status of charitable organizations working in areas considered to be "business-like," such as hospitals, universities, and professional services.

3 Tax-Liabilities

Reducing tax benefits for charitable organizations is seen by some lawmakers as an option for funding the projected budget shortfall. For example, there is a proposal to impose taxes on endowments, which, if passed, may set a precedent for extending taxation to other income sources, such as royalties. Other proposals suggest reducing the ability to fund activities such as advocacy and voter registration from tax-exempt donations.

Looking Forward

The evolving legislative landscape will pose substantial challenges for nonprofits. Proactive measures organizations can take to address these challenges include:

- **Monitoring Legislative and Policy Proposals:**
  Tax-exempt organizations should follow proposed legislative and policy changes and be ready to educate lawmakers and policymakers on their potential impact. Collaboration through formal and informal networks will be increasingly important to effectively monitor and counter proposals.

- **Engaging in Scenario Planning:**
  Identifying key drivers of change and uncertainty and developing strategies to navigate potential future situations will help organizations anticipate changes and prepare for possible challenges and opportunities.

- **Identifying Opportunities to Diversify Funding Sources:**
  With continued federal support uncertain, private sources of funding, as well as state and local funding, will become more critical for nonprofit operations.

- **Strengthening Due Diligence and Compliance:**
  Compliance with legal and tax regulations has never been more crucial given the potential challenges nonprofit organizations face. Organizations need to ensure their due diligence and compliance processes are comprehensive, functioning as intended, and well-documented.

- **Reviewing and Aligning the Strategic Plan:**
  Every nonprofit organization should revisit its strategic plan to ensure it aligns with their tax-exempt mission and complies with laws that protect its status, such as those aimed at preventing terrorism financing. This review should confirm that all activities remain consistent with the organization's stated purpose and do not inadvertently create risks of misinterpretation. Linking the strategic plan to enterprise risk management (ERM) can help identify and mitigate potential risks, ensuring the organization remains resilient, mission-focused, and compliant with regulatory expectations.

- **Enhancing Whistleblower Programs and Risk Assurance Functions:**
  Robust whistleblower programs and risk assurance functions prevent and mitigate risks posed by rogue actors within the organization. These mechanisms promote transparency, protect against misconduct, and maintain organizational integrity.

THEME 2

Cybersecurity

When organizations become more digitally connected and reliant on third-party technologies, external data sources, and outside service providers, they are more susceptible to the financial, operational, and reputational consequences of a cyberattack on a vendor or partner. At the same time, cybercriminals are becoming more sophisticated with the assistance of artificial intelligence, leading to more frequent attacks that are harder to prevent and counter.

State-sponsored and politically-motivated cyberattacks are often orchestrated by organized crime groups rather than individual hackers. Ransomware-as-a-service enables these criminal entities to acquire credentials, custom-developed ransomware, and ransom payment processing services with minimal technical expertise. As a result, nonprofit organizations are increasingly vulnerable to sophisticated cyber threats stemming from geopolitical tensions.

Nonprofit organizations, which typically have lower budgets and fewer cybersecurity defenses, are particularly at risk. Smaller entities may be seen as prime targets due to their increased dependence on third-party service providers and remote or hybrid work environments. There is a misconception that moving to a software-as-a-service (SaaS) application moves the security burden entirely to the SaaS provider, but this is frequently not the case. A false sense of security can leave organizations vulnerable to cyberattacks. The financial and operational repercussions of cybersecurity incidents can be severe. Data breaches can lead to lasting reputational damage.

Organizations that are recipients or subrecipients of U.S. government funds are now subject to stricter cybersecurity guidelines recently released by the Office of Management and Budget (Section 200.303 of 2 CFR). The scope of required cybersecurity and information safeguarding controls has been expanded beyond just personally identifiable information to all other information the federal agency or entity designates as sensitive data. Failure to implement reasonable cybersecurity measures not only exposes organizations to increased cybersecurity risks, but also jeopardizes their eligibility for federal funding. Additionally, non-compliance may result in reputational damage, legal liabilities, and financial penalties.

Looking Forward

Nonprofit organizations can protect themselves by:

- **Performing Cybersecurity Assessments:** Tools like GRF's Cybersecurity Risk Assessment and Scorecard help pinpoint and address vulnerabilities before hackers exploit them.
- **Strengthening Cybersecurity Policies and Procedures:** Robust policies and procedures are critical for protecting digital assets, mitigating the risk of cyber threats, and the continuity of operations. Examples of essential policies and procedures include information security and privacy policies, access control measures, incident response plans, and vendor risk management policies.
- **Implementing Basic Security Measures:** Multi-factor authentication, antivirus software, routine database backups, mobile device management, and regular user awareness training can significantly reduce the likelihood of a successful cyberattack.
- **Conducting Simulated Exercises:** Testing employees' abilities to identify phishing and social engineering tactics strengthens defenses against cyber threats.
- **Testing Systems Through a Cybersecurity Audit:** Conducting comprehensive audits helps identify potential security gaps and confirms that all cybersecurity measures are effective and up to date. These audits can include vulnerability assessments, penetration testing, and reviewing compliance with industry standards and regulations.
- **Preparing Crisis Management Procedures:** Organizations should prepare protocols for responding to a cyber incident should one occur.

THEME 3

Significant Operational Disruption

The increased frequency of low-probability, high-impact events has become a defining feature of the post-pandemic world. The suddenness and significant impact of events in 2024 – from flooding in western North Carolina and fires in Los Angeles, to exploding pagers in Lebanon and a terror attack in New Orleans, to the CrowdStrike outage – are signs of what to expect in the years ahead. Despite the increasingly regular occurrence of extreme events, many organizations remain inadequately prepared. The likelihood of being directly affected by such events is small in the short term, but increases significantly when indirect impacts such as disruption to activities or events are considered over a longer time horizon.

Three major areas pose significant risks:

1. Climate Change
2. Conflict and Civil Unrest
3. Reliance on Critical Technologies

1 Climate Change

Each year we can expect the effects of climate change such as floods, droughts, fires, freezes, and heatwaves to become more frequent, severe, and unpredictable. These events can harm or displace staff and other stakeholders, cause damage to physical infrastructure, cancel activities, and overwhelm an organization's capacity to respond. Additionally, long-term climate change can affect resource availability and alter the needs of populations served.

2 Conflict and Civil Unrest

Security risks will become more significant as conflict and civil unrest continue and escalate in many parts of the world. Organizations operating internationally will be the most significantly affected, but domestic organizations are at risk as well. A breakdown in international cooperation could hamper counter-terrorism activities in the U.S. as well as throughout the world.

3 Reliance on Critical Technologies

Many organizations increasingly depend on digital tools and platforms for communication, data management, and service delivery. This dependence makes them susceptible to disruption from cyberattacks, technical failures, and data breaches. A significant technological disruption can compromise sensitive information, disrupt operations, and erode the trust of stakeholders.

Looking Forward

Ways to address vulnerabilities for significant operational disruption include:

- **Assessing Most Significant Risks:**

  Organizations should identify the aspects of their work that they rely on most, including donors, income-generating activities, technologies, vendors, physical assets, and individuals, and prepare plans to reduce the risks associated with disruption to these critical elements.

- **Creating or Strengthening a Business Continuity Plan (BCP):**

  A BCP is a plan to ensure the continuation of critical operations in the face of unexpected disruptions, such as natural disasters, cyberattacks, or other emergencies. It aims to clarify roles and responsibilities and minimize decision-making during a crisis to enable a more effective and efficient recovery process.

- **Testing Plans and Running Simulation Exercises:**

  Objective assessments of plans can uncover hidden vulnerabilities, ensure that all components are functioning as intended, and provide a detailed analysis of areas that require improvement. Simulation activities, such as tabletop exercises and functional drills, provide an opportunity to practice responses to potential threats, enabling a more coordinated and efficient response during an actual crisis.

Concluding Thoughts

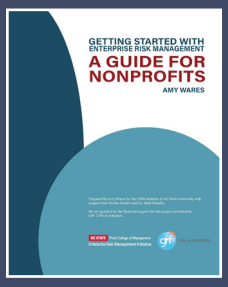
We have entered the age of permacrisis – a time characterized by continuous and overlapping crises that challenge our ability to adapt and respond effectively. Uncertainty may seem overwhelming; it also presents opportunities for growth and resilience.

The pandemic is fading in the rear-view mirror, but the lessons learned about the importance of resilience measures and cross-functional communication should stay top of mind. Establishing a Risk Council, or a management-level risk committee, facilitates dialogue and provides a forum for ensuring that risks are regularly discussed and addressed before they escalate. This collaborative approach can be the foundation for building organizational resilience and strengthening nonprofits' ability to achieve their mission and goals.

It is crucial to regularly scan the landscape for emerging threats and assess long-term trends. Proactive risk management allows organizations to take quicker, more decisive action when crises arise. Having a well-tested plan in place ensures that responses are coordinated and effective. Near misses—situations where something almost went wrong but didn't—offer valuable insights into an organization's risk landscape. Regularly reviewing these incidents can uncover hidden vulnerabilities and inform future risk mitigation strategies. This practice helps organizations understand why some risks were averted and how similar threats can be managed in the future.

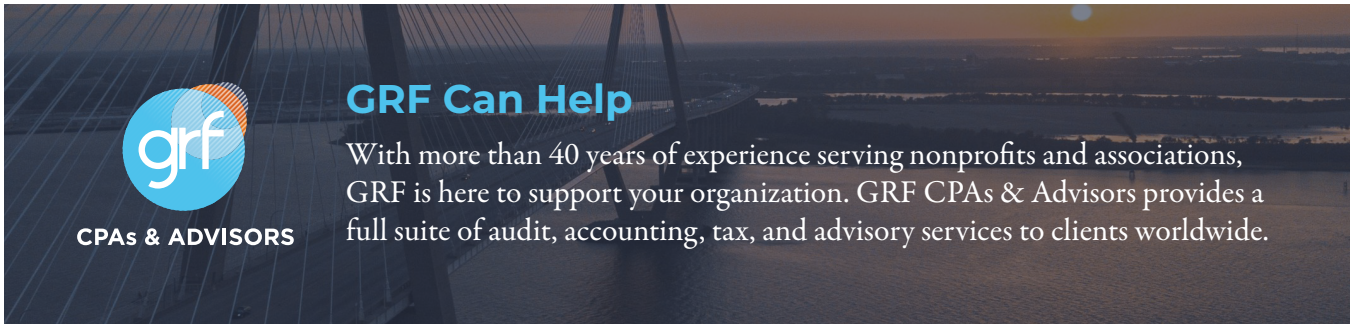
Understanding the organization's top risks is a fundamental board responsibility. Board members should ensure they are provided with top risk information and should actively inquire if such information has not been shared. The board's risk oversight responsibility requires members to have a clear understanding of how top risks are identified, assessed, and managed, as well as the strategies in place to address them. Discussions regarding top risks should be a regular part of board agendas and should be formally documented in meeting minutes. The age of permacrisis demands that organizations remain vigilant, proactive, and resilient. By implementing robust risk management practices and fostering a culture of continuous improvement, organizations can face the uncertainties of today and emerge stronger from future challenges.

Additional GRF Risk Management Resources



DOWNLOAD
Getting Started with Enterprise Risk Management

DOWNLOAD
ERM for Associations



CPAs & ADVISORS

GRF Can Help

With more than 40 years of experience serving nonprofits and associations, GRF is here to support your organization. GRF CPAs & Advisors provides a full suite of audit, accounting, tax, and advisory services to clients worldwide.

Our risk & advisory experts can help you address today's emerging risks:

ERM & ESG Advisory

Enterprise risk management (ERM) integrates strategic planning and risk management to improve responses to uncertainty, strengthen organizational resilience, and support mission fulfillment. ERM provides a framework for determining an organization's most critical risks and developing plans to monitor and manage these risks. GRF's approach to enterprise risk management merges technical expertise and pragmatism. Our ERM solutions are right-sized for your organization and we deliver actionable recommendations that organizations can implement immediately. Our clients range from organizations just beginning ERM to those with sophisticated programs seeking to further enhance their risk management activities.

Business Continuity Planning

Organizational resiliency relies on proactive planning to tackle threats to your organization before they occur. Unplanned events can adversely affect the operations of organization of all sizes, putting them and their stakeholders at significant risk. Business continuity plans (BCP) are an important element of risk management and prepare your organization for major risk events such as public health emergencies, government shutdowns, natural disasters, and cyberattacks. The advisors at GRF bring industry knowledge combined with cybersecurity expertise to help clients anticipate and mitigate potential disruptions to their operations.

Internal Audit and Investigations

GRF has seen a sizable increase in fraud among our nonprofit and association clients. A fraud risk assessment can help your organization prevent and detect fraudulent activity. This assessment identifies the processes that could be exploited (for example, due to lack of controls or staffing constraints) and focuses on these and other high-risk processes, such as accounts payable and expense reimbursement. This enables your organization to allocate resources to mitigating the most significant risks and develop a monitoring plan for less significant risks. A fraud risk assessment feeds into an internal audit plan to mitigate risks and identify opportunities for process improvements. If you suspect fraud has occurred, GRF's certified fraud examiners can investigate allegations and recommend remedial actions.

Cybersecurity Audits and Assessments

GRF is dedicated to safeguarding the integrity of our clients' information technology systems. Our CISA-certified auditors and certified ethical hackers use their in-depth understanding of the cyber risk landscape, regulatory requirements, and recommended frameworks to provide practical, right-sized solutions. Our Cybersecurity Scorecard takes a hacker's perspective into your organization to identify vulnerabilities in 19 security related categories and one informational category with results presented in an easy-to-read scorecard. The report details risks, remediation steps, and best practices to increase your score. In addition to reducing your vulnerability to cyber threats, implementing the Cybersecurity Scorecard's monitoring and remediation activities can reduce the cost of cyber insurance.

CONTACT US

Our Risk & Advisory Services team is here to help. We take a pragmatic approach that combines expertise with cutting edge technology, enabling our clients to achieve the best possible results.

Melissa Musser, CPA, CIA, CITP, CISA
Partner and Director, Risk & Advisory Services
mmusser@grfcpa.com

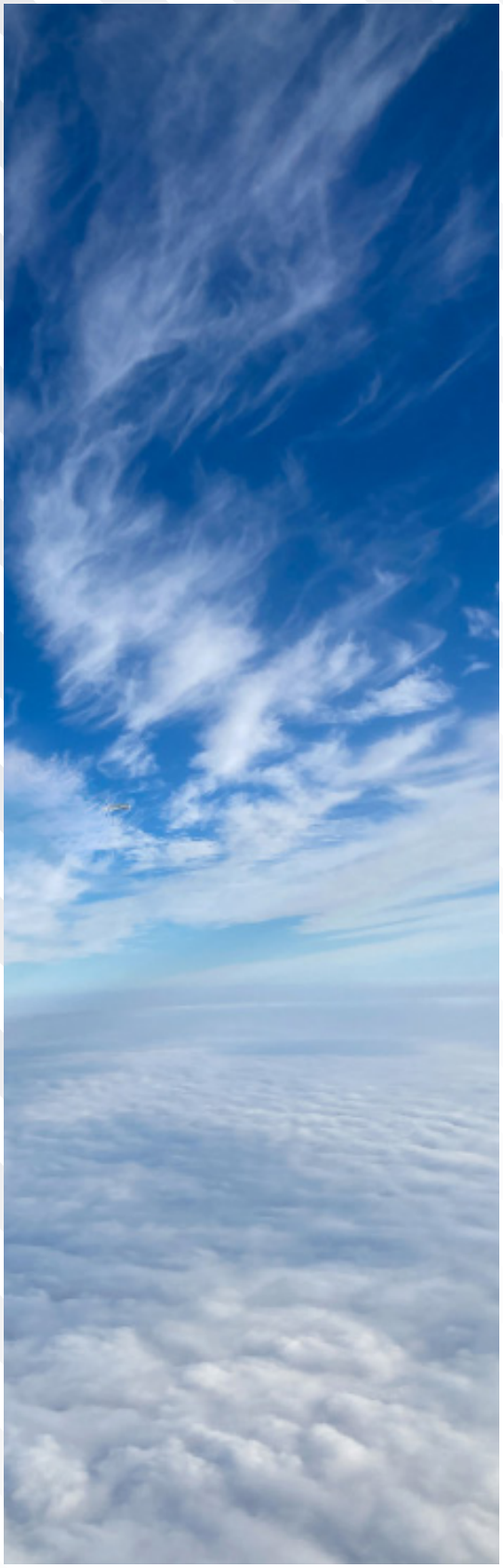
Amy Wares, CPA, MBA
Senior Manager, Risk & Advisory Services
awares@grfcpa.com

Mac Lillard, CPA/ABV/CITP, CIA, CFE, CISA/CRISC
Senior Manager, Risk & Advisory Services
mlillard@grfcpa.com

Darren Hulem, CISA, CEH, Security+
Senior Manager, Risk & Advisory Services
dhulem@grfcpa.com

Richard J. Locastro, CPA, J.D.
Partner and Director, Nonprofit Tax
rlocastro@grfcpa.com

Thomas Brown, CISA, CIA, Security +, CAPM
Supervisor, Risk & Advisory Services
tbrown@grfcpa.com



CPAs & ADVISORS

Appendix: Sources

Survey-Based Reports

World Economic Forum's *Global Risks Report 2025*

https://www.weforum.org/publications/global-risks-report-2025/

The World Economic Forum is an international organization that engages political, business, and other leaders of society to shape global, regional, and industry agenda. The Global Risks Report draws on survey input from over 900 experts across academic, business, government, international organizations, and civil society. The responses were collected from September 2 to October 18, 2024.

Top Global Risks (2 years)

1. Misinformation and disinformation
2. Extreme weather events
3. State-based armed conflict
4. Societal polarization
5. Cyber espionage and warfare
6. Pollution
7. Inequality
8. Involuntary migration or displacement
9. Geoeconomic confrontation
10. Erosion of human rights and/or civic freedoms

Top Global Risks (10 years)

1. Extreme weather events
2. Biodiversity loss and ecosystem collapse
3. Critical change to Earth systems
4. Natural resource shortages
5. Misinformation and disinformation
6. Adverse outcomes of AI technologies
7. Inequality
8. Societal polarization
9. Cyber espionage and warfare
10. Pollution

Internal Audit Foundation *Risk in Focus 2025: North America*

https://www.theiia.org/en/internal-audit-foundation/latest-research-and-products/risk-in-focus/regional-pages/north-america/

The Internal Audit Foundation, part of the Institute of Internal Auditors, conducts research and funds initiatives to support the internal audit profession. Risk in Focus 2025: North America combines input from a survey of 417 chief audit executives and heads of internal audit in the United States Canada and Caribbean, 2 roundtable events with 14 participants, and 3 in-depth interviews. The research was conducted in the first half of 2024.

Top 10 Risks

1. Cybersecurity
2. Human capital
3. Digital disruption (Including AI)
4. Regulatory change
5. Business continuity
6. Market changes/competition
7. Supply chain (including third parties)
8. Financial liquidity
9. Geopolitical uncertainty
10. Organizational culture

FERMA (Federation of European Risk Management Associations) *Global Risk Manager Survey Report 2024*

https://www.ferma.eu/publication/global-risk-manager-survey-report-2024/

FERMA is a representative organization for the risk management profession in Europe. Its Global Risk Manager Survey Report draws on over 1,000 responses from risk management practitioners in 77 countries. Data was collected between January and April 2024.

Top 5 Risks Within the Next 12 Months

1. Cyberattacks
2. Geopolitical uncertainties
3. Uncertain economic growth
4. Talent management
5. Data breach

Top 3 Risks Within the Next 3 Years

1. Regulation
2. Geopolitical uncertainties
3. Speed of technological change

National Association of Corporate Directors (NACD) *2025 Trends and Priorities*

https://www.nacdonline.org/all-governance/governance-resources/governance-research/outlook-and-challenges/2025-governance-outlook/preparing-for-five-crucial-board-balancing-acts-in-2025/

NACD is an association for board directors. Its 2025 Top Trends survey captures the views of 251 directors. The survey was conducted from October 21 to November 14, 2024.

Director's Top Trends for 2025

1. Shifting economic conditions
2. Regulatory requirements
3. Cybersecurity threats
4. Competition for talent
5. Geopolitical volatility
6. Artificial intelligence
7. Growing business model disruptions
8. Inflation rate
9. Technological change (apart from AI)
10. Supply chain disruptions

Auditboard's *2025 Focus on the Future Report*

https://www.auditboard.com/resources/ebook/2025-focus-on-the-future-inflection-point-for-transformation-at-mid-decade/

AuditBoard is an audit, risk, and compliance software provider. The Focus on the Future Report presents results from a global survey of 376 internal audit professionals conducted online in August 2024.

Top 7 Risks

1. Cybersecurity and data security
2. Changing economic conditions
3. Regulatory and legislative changes
4. Information Technology
5. Attract and retain talent
6. Third-party risk management
7. Business continuity and crisis response

AXA's Future Risks Report 2024

https://www.axa.com/en/news/2024-future-risks-report

AXA is large global insurance provider. Its Future Risks Report is based on survey responses from a panel of 3,012 risk experts from 50 countries and a representative sample of close to 19,003 people from 15 countries conducted May 14 – June 27, 2024.

Global Top 10 Emerging Risks

1. Climate change
2. Geopolitical instability
3. Cybersecurity risks
4. Risks related to AI and big data
5. Social tensions and movements
6. Natural resources and biodiversity risks
7. Energy risks
8. New security threats and terrorism
9. Pandemics and infectious diseases
10. Financial stability risks

Allianz *Risk Barometer 2025*

https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Allianz is a large provider of insurance and asset management products and services. The Risk Barometer provides the results of a survey of 3,778 global businesses, brokers, industry trade organizations, and risk management professionals in 106 countries and territories. The survey was conducted during October and November 2024.

Global Risks in Focus

1. Cyber incidents (e.g., cybercrime, IT network and service disruptions, malware/ransomware, data breaches, fines, and penalties)
2. Business interruption (incl. supply chain disruption)
3. Natural catastrophes (e.g., storm, flood, earthquake, wildfire, extreme weather events)
4. Changes in legislation and regulation (e.g., new directives, protectionism, environmental, social, and governance, and sustainability requirements)
5. Climate change (e.g., physical, operational, and financial risks as a result of global warming)
6. Fire, explosion
7. Macroeconomic developments (e.g., inflation, deflation, monetary policies, austerity programs)
8. Market developments (e.g., intensified competition/new entrants, M&A, market stagnation, market fluctuation)
9. Political risks and violence (e.g., political instability, war, terrorism, coup d'état, civil unrest, strikes, riots, looting)
10. New technologies (e.g., risk impact of artificial intelligence, connected/autonomous machines)

Expert Analysis

S&P Global Ratings' *Global Credit Outlook 2025*

https://www.spglobal.com/ratings/en/research-insights/special-reports/global-credit-outlook

S&P Global Ratings is a credit rating agency and publishes financial research and analysis.

Top Global Risks

1. Geopolitical tensions threaten supply chains, market sentiment, and budgets
2. Growing protectionism threatens global trade
3. The interest rate descent could disappoint
4. A sharper global economic slowdown would lead to greater credit stress
5. Global real estate markets are facing multiple challenges

Eurasia Group's *Top Risks 2025*

https://www.eurasiagroup.net/issues/top-risks-2025

The Eurasia Group is a political risk advisory and consulting company.

Top Risks 2025

1. The G-Zero Wins: We're entering a uniquely dangerous period of world history on par with the 1930s and the early Cold War.
2. Rule of Don: The erosion of independent checks on executive power and the rule of law will increase the extent to which the U.S. policy landscape depends on the decisions of one powerful man.
3. U.S.-China Breakdown: Trump's return to office will unleash an unmanaged decoupling in the world's most important geopolitical relationship.
4. Trumponomics: Donald Trump is about to inherit a robust U.S. economy, but his policies will undermine its strength this year through higher inflation and reduced growth.
5. Russia Still Rogue: Russia will do more than any other country to subvert the global order in 2025.
6. Iran on the Ropes: The Middle East will remain a combustible environment in 2025, for one big reason: Iran hasn't been this weak in decades.
7. Beggar Thy World: The U.S. and China will export disruption to everyone else this year, short-circuiting the global economic recovery and accelerating geoeconomic fragmentation.
8. AI Unbound: As most governments opt for lighter-touch regulation and international cooperation falters, AI capabilities and risks will continue to grow unchecked.
9. Ungoverned Spaces: The deepening G-Zero will leave many people, places, and spaces thinly governed and forgotten.
10. Mexican Standoff: Mexico will face formidable challenges this year in its relations with the U.S. at a time of ongoing constitutional overhauls and fiscal stresses at home