CPAs & ADVISORS

2026

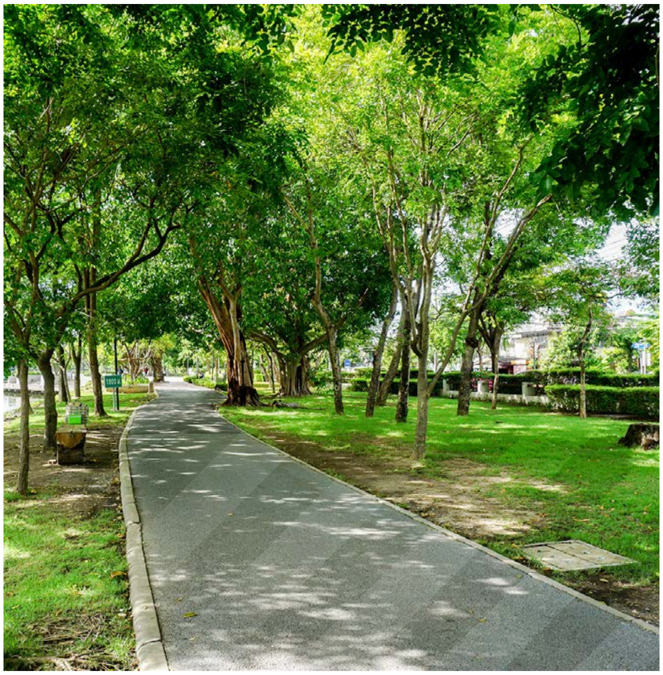
GRF Top Risks Report

Key Themes for DC-Based Organizations and their Global Communities

Executive Summary

Organizations in the DC Metro region, and the broader national and international communities they serve, enter 2026 amid accelerating geopolitical instability, economic volatility, intensifying cyber threats, and rapid digital transformation. Because of the region's unique concentration of nonprofits, associations, NGOs, and federal government contractors, these organizations face heightened exposure to federal appropriations cycles, regulatory shifts, technology mandates, and the evolving demands of a modern workforce.

The three cross-cutting risk themes outlined in this report represent the most significant challenges and opportunities.



THEME 1

Strategic Drift Amid Global, Economic, and Digital Disruption

THEME 2:

Cybersecurity, Business Continuity, and Resilience

THEME 3:

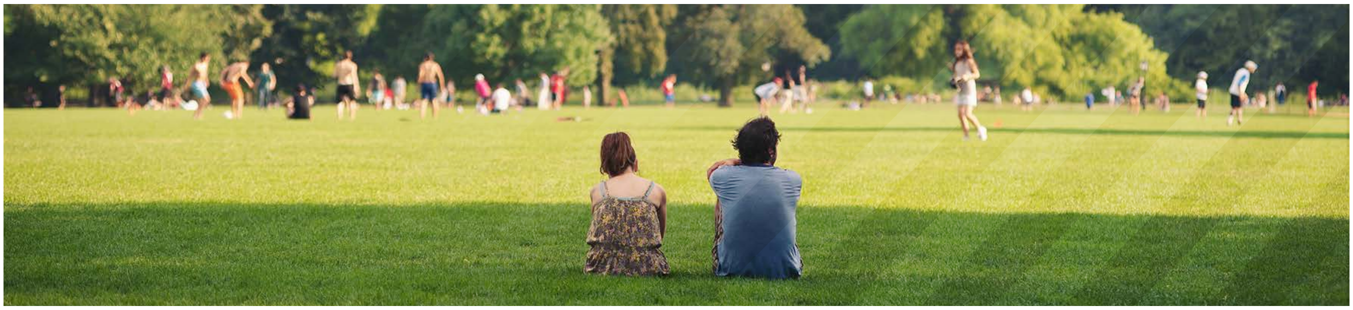
Talent Management, Culture, and Organizational Governance

Although they operate in different sectors, government contractors and tax-exempt organizations share a surprising number of core challenges and operating realities, especially when it comes to compliance, funding, and accountability. Inherent challenges for both sectors include:

- Operating in highly regulated environments
- Reliance on external funding
- Intense financial and compliance scrutiny
- Expectations for exceptional transparency and internal controls
- Balancing mission impact with operational discipline

As we look ahead, these challenges will continue to grow in complexity, with mounting regulatory requirements, shifting funding sources, and increased demands for accountability. Now is the moment to examine the strategic risks and opportunities that will define the direction of tax-exempt organizations and government contractors in 2026.

Organizations that succeed in this environment will strengthen governance, reinforce mission alignment, invest in cybersecurity and operational resilience, and prioritize culture and talent development.



THEME 1:

Strategic Drift Amid Global, Economic, and Digital Disruption

DC-influenced organizations are more exposed than most to the ripple effects of **federal appropriations, policy shifts, global conflict, and economic uncertainty**. This environment increases the risk of **Strategic Drift**, where mission alignment gradually erodes due to external pressures, funding instability, or reactive decision-making.

1 Strategic Drift and Mission Misalignment

Strategic Drift occurs when the organization gradually loses alignment with its strategic objectives, fails to adapt to changing stakeholder needs, or allocates resources ineffectively. In today's environment, geopolitical instability, inflation, supply chain disruptions, and shifting global alliances have forced organizations to make rapid decisions that may unintentionally pull them away from their long-term mission.

These pressures are amplified by **digital disruption and the emergence of artificial intelligence (AI)**. While technology offers significant opportunities for efficiency and impact, organizations risk adopting digital solutions reactively or in response to funder expectations, rather than as part of a cohesive strategy. Without a clear alignment to mission and values, digital initiatives can create new gaps, introduce bias or operational risk, or divert attention from core priorities.

Examples of How Strategic Drift Shows Up in Various Organizations

Nonprofits & NGOs

- Misaligned program expansion to chase restricted federal or foundation dollars.
- External shocks (geopolitical, economic, or social) causing abrupt donor-driven priority shifts.
- Digital adoption decisions driven by funder requirements rather than strategy.
- Poorly planned or poorly integrated mergers or partnerships that dilute mission clarity and strain operations.
- Over-reliance on a single major funder.

Associations

- Product launches or service expansions aimed at offsetting declining dues or event revenue.
- Pressure to respond quickly to industry-wide disruptions without structured governance.

Government Contractors

- Pursuit of contracts outside core competencies due to shifting DoD/DHS pipelines.
- Strategic stretch caused by new compliance mandates.

Digital Disruption & AI as Drivers of Drift

AI-enabled tools offer tremendous potential, but organizations are rushing to adopt:

- AI chatbots for member/donor engagement
- Automated analytics for fundraising, grants, or contracting
- AI-transformed service delivery

Without strong governance, this creates risks related to accuracy, bias, privacy, and mission misalignment.

2 Funding Impact and Resource Allocation

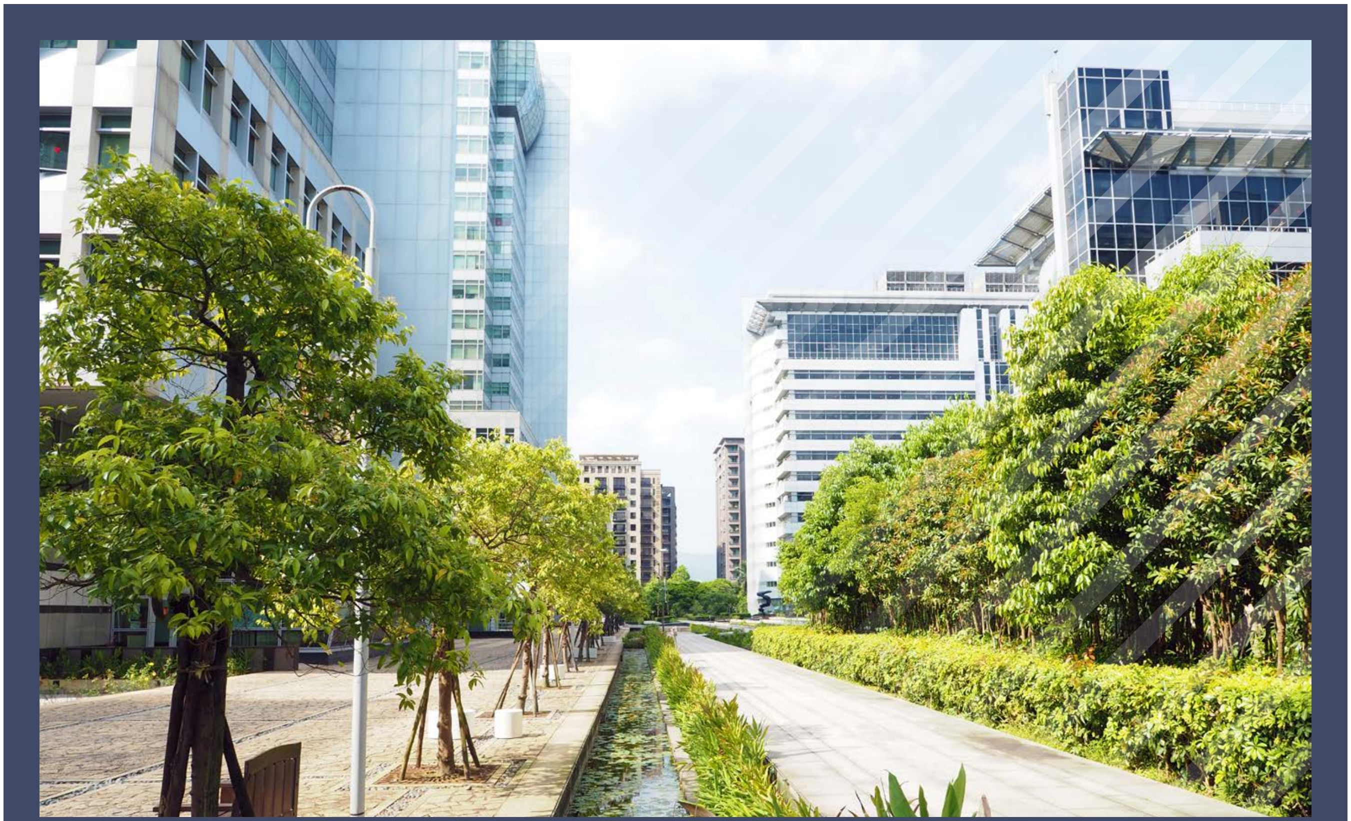
Macroeconomic challenges continue to place significant strain on traditional funding sources. Inflation, economic uncertainty, and global instability have encouraged organizations to diversify revenue streams to maintain financial resilience. Diversifying into new revenue streams can introduce risks that pull the organization away from its core strategy and mission, leading to decisions driven by donor requirements rather than organizational priorities.

The organization's actions, priorities, or programs shift away from its original purpose. This can happen gradually, for example, by prioritizing a new funding opportunity over community needs or by a subtle shift in messaging from impact to financial metrics.

While increasing funding and identifying new sources of funding is essential to continuing operations, it's important to conduct an assessment of the potential impact to the organization and its mission. Organizations should consider:

1. **Pros and cons of projects:** Will this new project or funding have an impact on our strategic alignment?
2. **Project Scorecards:** Identify how the funding advances the strategy of the organization and what strategic objectives may be improved vs. those that may be impacted.

To support mitigating this risk, organizations may consider enterprise risk management, a structured, organization wide approach to identifying, assessing, and responding to risks that could impact your organizational ability to achieve its mission.

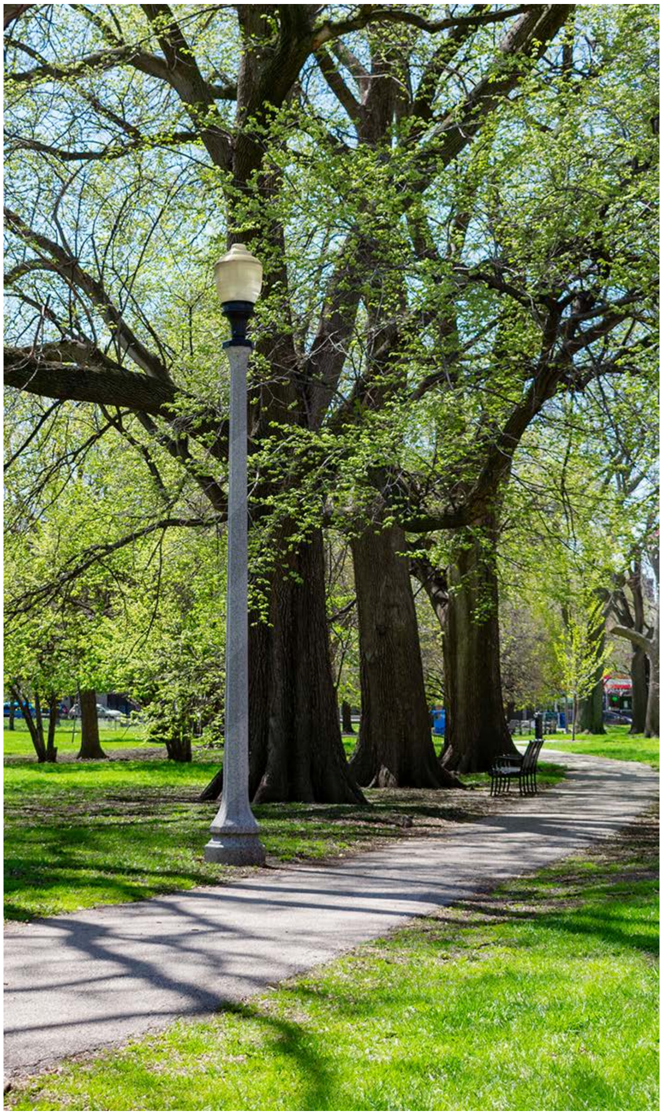


Mitigation Strategies

- **Board-led oversight** of mission alignment during major market or funding shifts.
- **ERM integration** to connect strategy, funding decisions, and risk appetite.
- **Mission-alignment scorecards** for new initiatives, funding opportunities, digital projects, or contract pursuits.
- **Strategic alignment audits:** Build on the scorecards by conducting formal reviews (semi-annually) to assess whether programs and tech initiatives still align with mission. This could be done using existing strategy implementation tools such as Objectives and Key Results.
- **Scenario planning** for appropriations delays, Continuing Resolutions, or geopolitical disruptions.
- **Technology governance** to ensure AI and modernization efforts support, not distort, core purpose.

THEME 2:

Cybersecurity, Business Continuity and Resilience



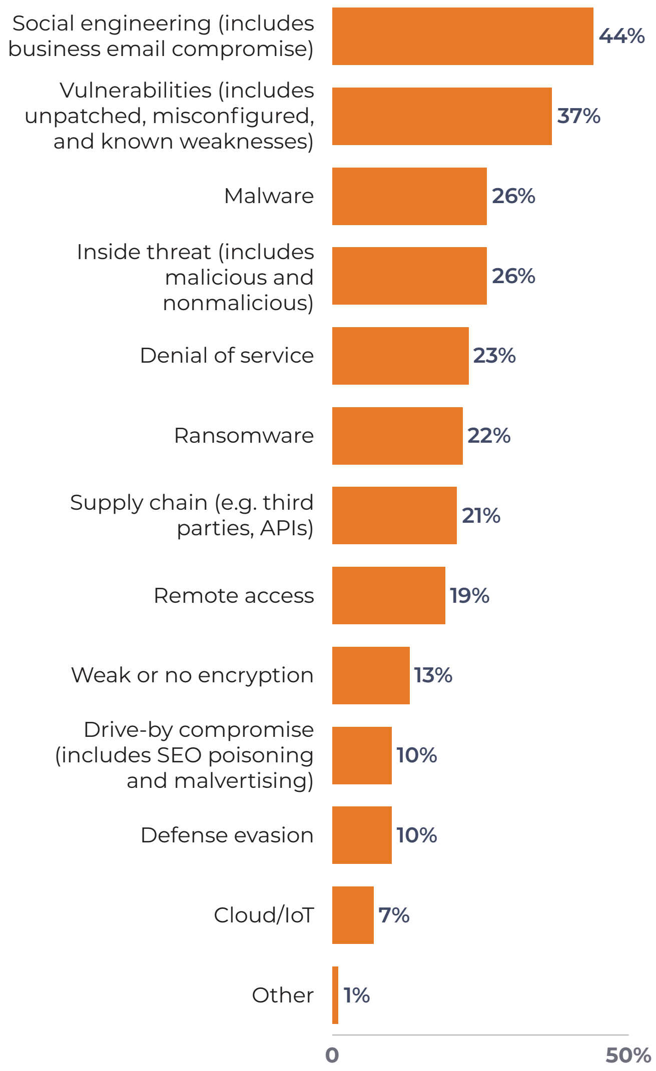
Business continuity and resilience involve an organization's ability to maintain essential functions during and after a crisis, such as a natural disaster, cyber-attack, or a pandemic. The DC Metro region is one of the **highest-targeted cyber regions in the United States** due to its proximity to federal agencies and the prevalence of sensitive data held by nonprofits, associations, and government contractors.

Organizations face escalating risks from ransomware, insider threats, nation-state actors, and supply-chain vulnerabilities—while simultaneously navigating new federal cybersecurity and AI requirements.

1 Cybersecurity and Data Security

Cybersecurity and data security risks are escalating as organizations rely more on digital platforms and cloud services. According to the ISACA State of Cybersecurity 2025 Report, 58% of respondents indicated that the number of attacks compared to a year ago were more or the same. This potential increase in attacks poses a greater issue for cybersecurity teams that are already responding to threats on a continuous basis. According to the ISACA report, the top attack vectors utilized were social engineering, exploited system vulnerabilities, malware, and insider threats.

Which of the following attack vectors were used when your organization was compromised?



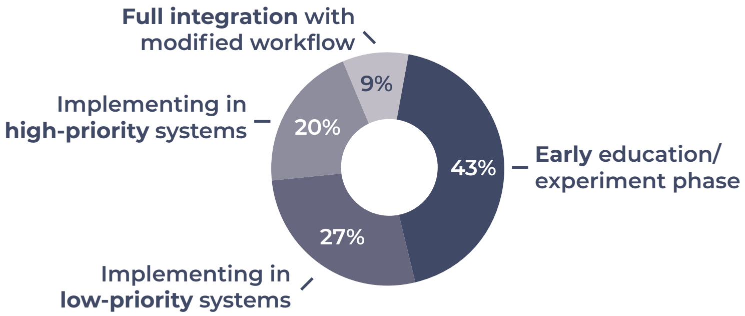
Source: State Of Cybersecurity 2025: Global Update on Workforce Efforts, Resources, and Cybersecurity Operations, State of Cybersecurity 2025

Organizations continue to be susceptible to social engineering and system vulnerabilities, but new threats are evolving all the time. With the increase in cyber attacks and attack vectors, it is critical to understand your organization's current landscape, risks, and potential vulnerabilities, as cyber incidents can result in financial loss, legal consequences, and impact of stakeholder trust.

As we move into the next phases of cybersecurity, AI will play a role in both system attacks and protections. According to the CompTIA State of Cybersecurity Report, AI adoption and prioritization in cybersecurity are evolving. This shift toward using AI to support internal efforts, defend against new threats, and balance internal and external usage will continue to evolve as AI is implemented across organizations.

CPAs & ADVISORS

Organizations are largely in early stages of adoption with AI



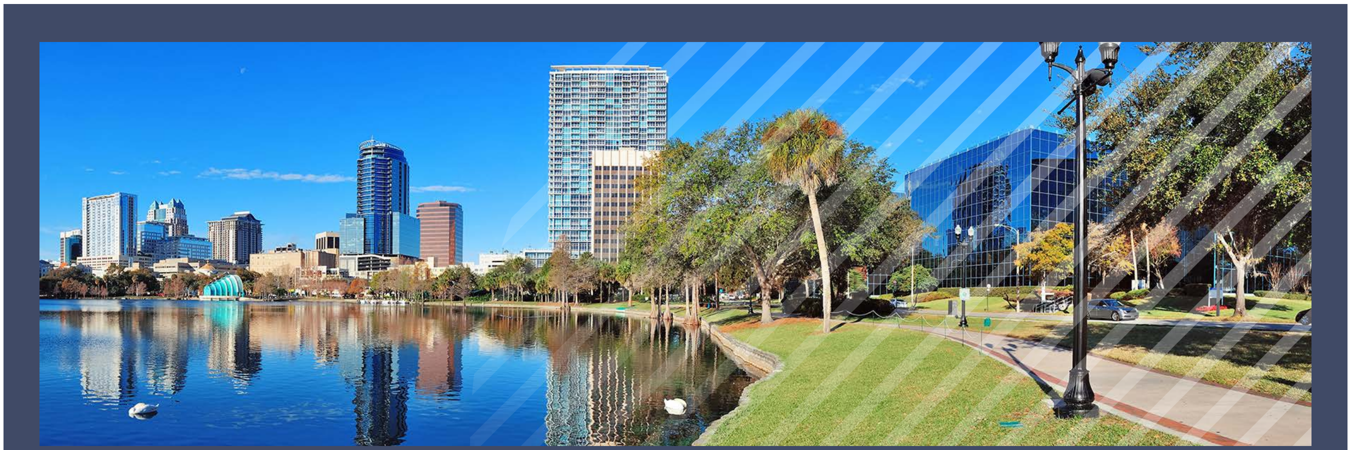
AI priority within cybersecurity

37% Improving internal efforts

31% Defending new threats

32% Balancing internal/external

Source: CompTIA State of Cybersecurity 2025 | n=1026



Mitigation Strategies

To mitigate these risks, organizations should consider:

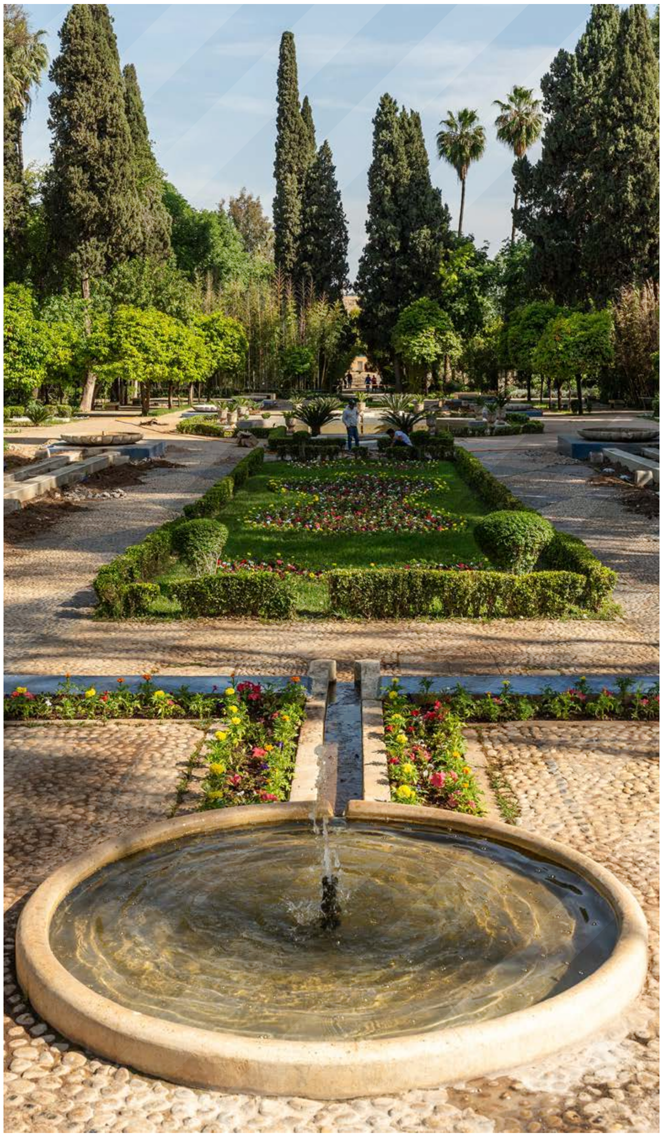
- Undergoing a **baseline cyber assessment** to understand what you have, how you are protecting it, and potential gaps.
- Implement and track using **cybersecurity frameworks**.
- **Train users** on cyber best practices, acceptable use, and reporting incidents.
- Conduct **periodic cybersecurity audits** and consider **continuous monitoring/protections**.

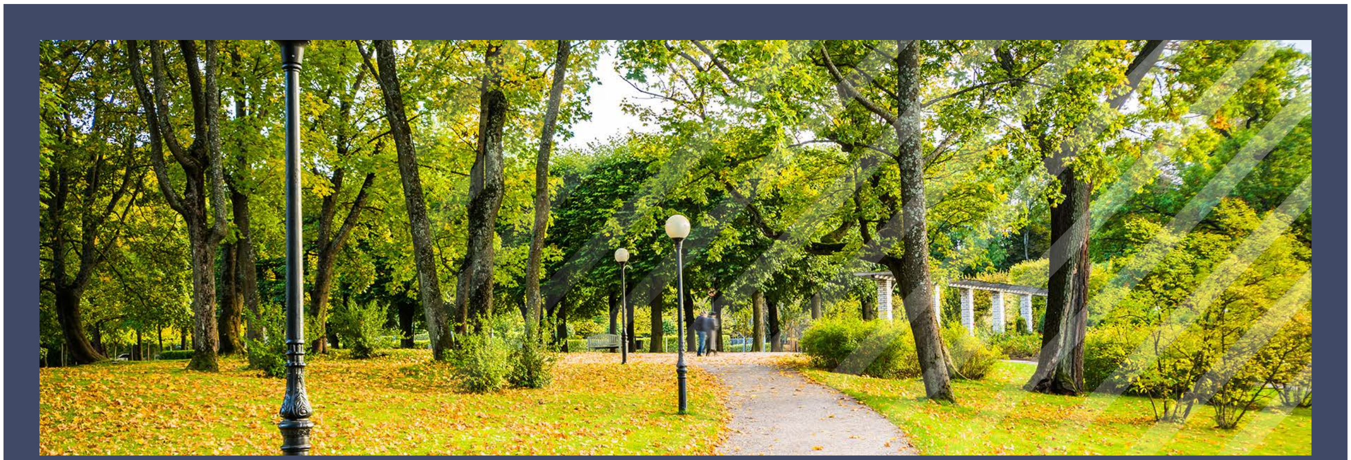
2 AI Governance

Data protection and privacy risks increase with the adoption of AI power tools such as chatbots, cybersecurity analytics, and fraud detection. According to the ISACA State of Cybersecurity 2025 Report, survey respondents report an increased use of AI in their work to support security related operations such as automating threat detection/ response, endpoint security, and automating routine security tasks. Respondents are also stepping up their involvement in the development, onboarding, and implementation of AI tools and the creation of policies governing the use of AI technology.

While AI can support in the automation of many areas within an organization, it is imperative that organizations consider the impact that this can have on data security, bias, misinformation, and accountability. Additionally, many third-party tools have AI enabled within their platforms, which poses an additional risk to the organization. With the rapid adoption of AI, many third-party vendors may have implemented AI after they have already been vetted and approved to work with the organization. This exposes your organization to the additional risk of AI usage that has not been vetted by your cyber, IT, or legal team.

Without clear and proper governance, organizations may be vulnerable to data breaches or exposures to the public through AI tools, reputational harm, and inaccurate information utilized for core operations and strategy.





Mitigation Strategies

To support both the risks and opportunities presented by AI, your organization should consider the following:

- **Develop a clear AI usage policy** that outlines what AI tools may be used, what data may be shared, and requirements for usage. Without clear policies enforcing AI usage, users may not understand the implications of their actions and the impact on the organization.
- **Train and communicate around AI usage** so end users can learn the best practices for AI use. Users may not understand how the data that is fed into public AI tools may be used for learning and training purposes and may be exposed to the public through the AI Tools and Large Language Models.
- **Engage your legal, cybersecurity and IT experts** for analyzing AI tools and contracts to understand how your data may be stored, used, and potentially exposed. Through the analysis, your experts may identify areas that can pose additional risk to the organization such as sharing your organizational data with the LLM, having a lack of security protections in place, and/or lack of controls in the system setup.
- **Set a requirement for AI Governance Methodology to be provided by AI/Third Party vendors.** There are various AI frameworks vendors can follow, such as the NIST AI Risk Management Framework, EU AI ACT, or ISO 42001. Aligning with an AI framework shows a commitment to managing risks associated with AI and responsible use and governance of AI. If the vendor is not following an AI framework, ask if they are following another AI governance model, which you should review to best understand how AI may interact with your data.

CPAs & ADVISORS

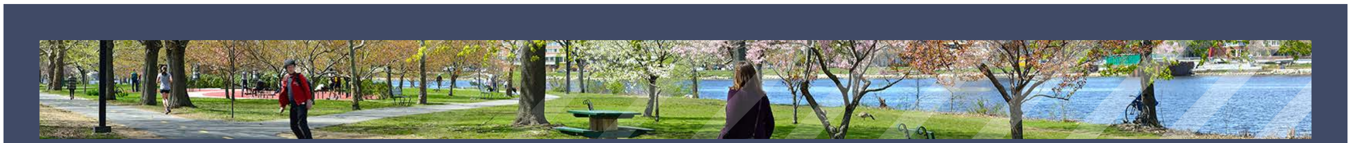
3 Digital disruption and Transformation

Five years after the pandemic accelerated the shift to remote work, use of digital tools, and reliance on technology, a continued digital evolution is taking shape. Digital disruption refers to the impact of emerging technologies that change traditional ways of work, while digital transformation is the proactive adoption of these technologies to enhance operations.

GRF is seeing organizations increase their use of technology to support outdated and manual processes within accounting, operations, finance, and security. For example, many organizations require a manual transfer of data from one system to the other. This time-consuming and tedious task is susceptible to errors, delays, and frustration among end users. Through digital transformation, organizations are identifying these pain points and bottlenecks to develop more automated and efficient processes such as:

- **Two-Way API integrations/Real Time Sync:** The systems communicate bi-directionally, automatically updating and reconciling in real time. This requires strong system compatibility, ongoing maintenance, and review.
- **One-Way API integrations:** The platform automatically pushes data to the system, reducing manual entry. This is often done from a banking application to an accounting system. This setup may require manually making corrections or adjustments, as the data doesn't flow back and forth.
- **Batch Import with Human Review:** The system processes data in scheduled batches to the central system with review and approvals before being recorded. This requires oversight to catch discrepancies, which can cause delays in data processing and potential bottlenecks if review processes are inefficient.

Automated processes can support end users in synchronizing data by reducing bottlenecks and inefficiencies. Many ERP solutions and ancillary applications have pre-built connections to consider when starting the process of automation and transformation.



Mitigation Strategies

Digital transformation can help your team become more efficient, but there are risks associated with implementing new technologies without first defining a sound, controlled, and documented process. Without a defined process, you run the risk of implementing a system that does not meet your needs, resulting in an implementation failure. We recommend the following steps:

1. **Evaluate and document your current processes**
   a. Identify pain points, inefficiencies and bottlenecks
   b. Identify ways to solve these issues: Is this issue due to a lack of technology, people, or a process issue?
      i. *This will help to determine if a technology will help the process or if it is something that is inherently wrong with the process.*
2. **Systems Assessment Process including developing a project scope and procurement strategy** (See more information and a case study here)
   a. Document requirements, current pain points, integrations, and expectations of the new system.
   b. Do research on vendors to identify potential solutions. Peer review sites are good sources of information.
   c. Develop a formal RFP to define how you expect to be supported by the system.
   d. Complete vendor demos, work in sandbox environments, and determine integration capabilities.
   e. Select a vendor that meets your requirements now and is scalable into the future.

Systems implementations often fail when end users do not buy in to the change and object to the time commitment, training, and setup required for new systems. Doing your due diligence and following a defined process for reviewing vendors and onboarding new systems will reduce the potential for failed implementations and improve your chances for having effective technology implemented into the organization.

Technology disruption and transformation are ongoing, but a structured approach to technology selection and integration can greatly improve user acceptance and organizational efficiency.

THEME 3

Talent Management, Culture, and Organizational Governance

Talent shortages, burnout, and leadership gaps directly affect mission delivery, compliance readiness, and organizational resilience. At the same time, **organizational culture, sustainability practices and governance** have become critical components of talent strategy. More often, employees are choosing to work for organizations that show:

- strong ethical governance
- meaningful commitments to sustainable values
- transparency in leadership decision-making
- a performance-driven but inclusive culture
- authentic mission orientation and community impact

Weak or inconsistent culture can intensify turnover, hinder employee engagement, and reduce the organization's ability to attract and retain high-performing staff. Boards and leadership teams play a key role in setting expectations for culture, monitoring talent risks, and ensuring alignment between organizational values, leadership behaviors, and strategic goals.

There is also opportunity to find new talent, as funding cuts and organizational closures reshape the nonprofit and government contracting landscape, a significant pool of skilled professionals is entering the job market. This shift creates both risk and opportunity: while talent shortages remain a concern, organizations that act strategically can attract high-caliber individuals seeking stability and purpose-driven work. By leveraging this moment, organizations can strengthen their workforce, reinforce culture, and ensure continuity in mission delivery.

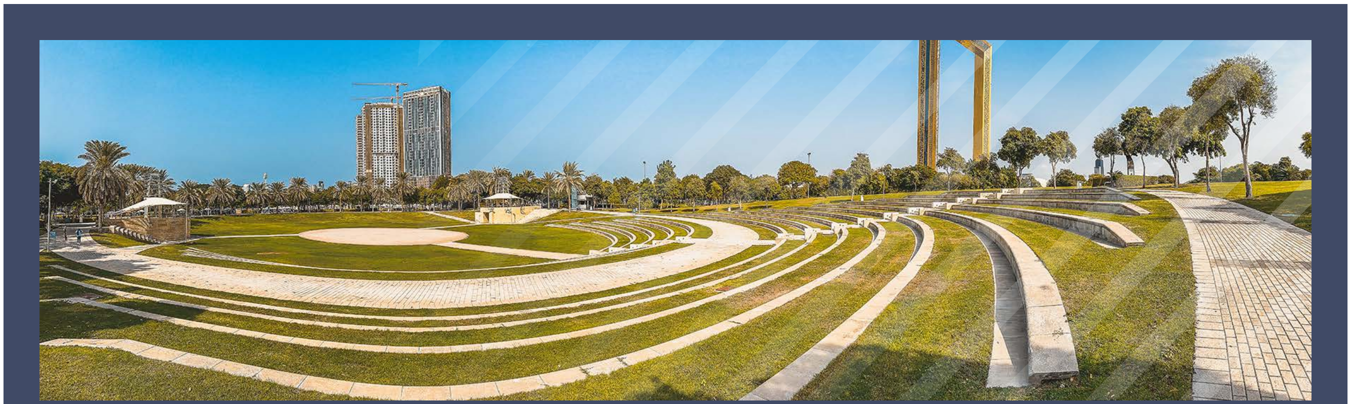
1 Culture & Governance as Risk Drivers

Strong culture and governance improve:

- Retention and engagement
- Performance and accountability
- Leadership continuity
- Succession planning
- Compliance and ethical behavior

Weak culture accelerates turnover and increases operational fragility.

Organizations can strengthen workforce resilience, improve retention, and ensure continuity in fulfilling their mission by integrating talent strategy with culture and governance.



Mitigation Strategies

These strategies uses the Stakeholder Value framework, which incorporates ESG principles while expanding to include culture, talent, governance, and community impact.

1. Embed Stakeholder Value into Talent Strategy

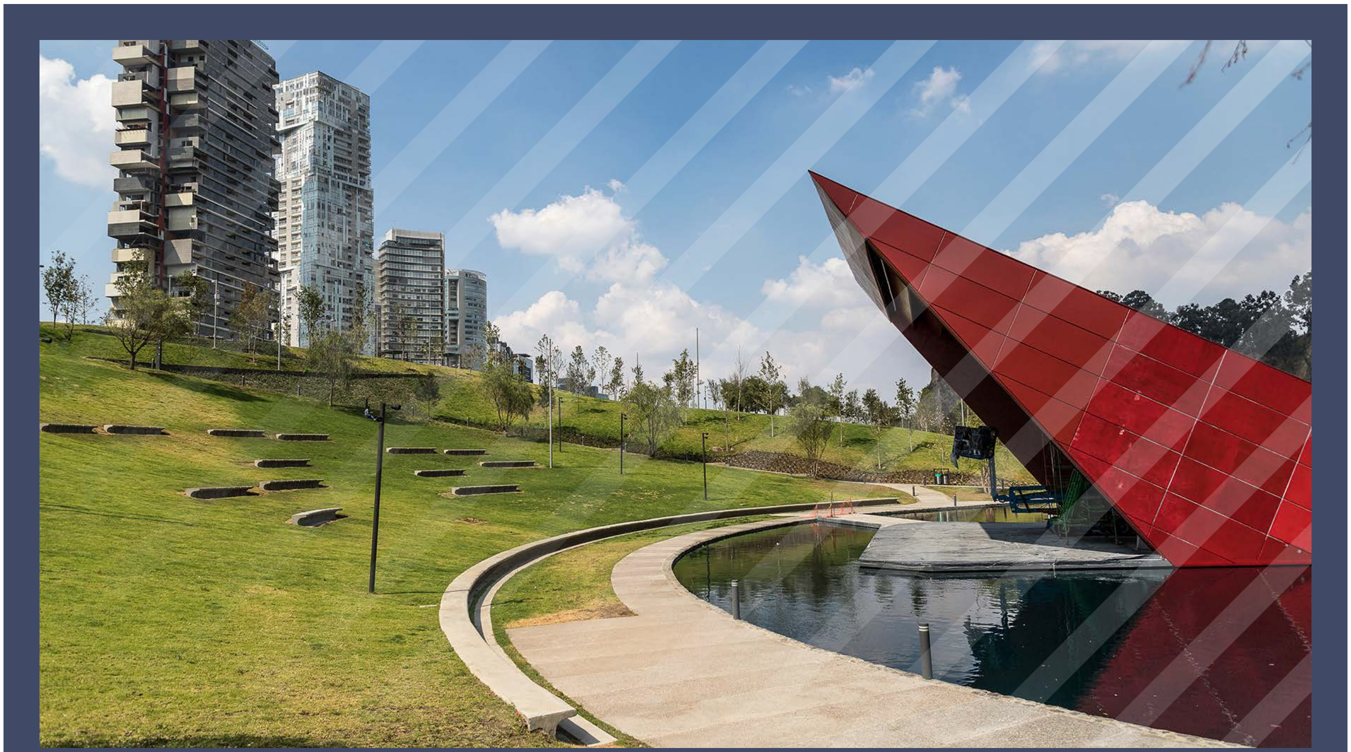
Organizations can mitigate talent risk by adopting a stakeholder-centric model in which employees, clients, partners, and the community are treated as core stakeholders—not simply recipients of HR initiatives.

Strategic actions:

- Integrate Stakeholder Value commitments into the employer brand (environmental stewardship, strong governance, ethical leadership, community impact).
- Communicate progress transparently so employees see alignment between stated values and actual practices.
- Use Stakeholder Value as a differentiator in a competitive labor market where workers increasingly choose employers based on purpose and values.

Why it works:

Research shows that employees, especially early-career professionals, frequently forgo higher salaries to work for organizations whose mission, values, and societal impact they believe in. Purpose and alignment matter deeply.



2. Conduct a Double Materiality Assessment for Workforce Priorities

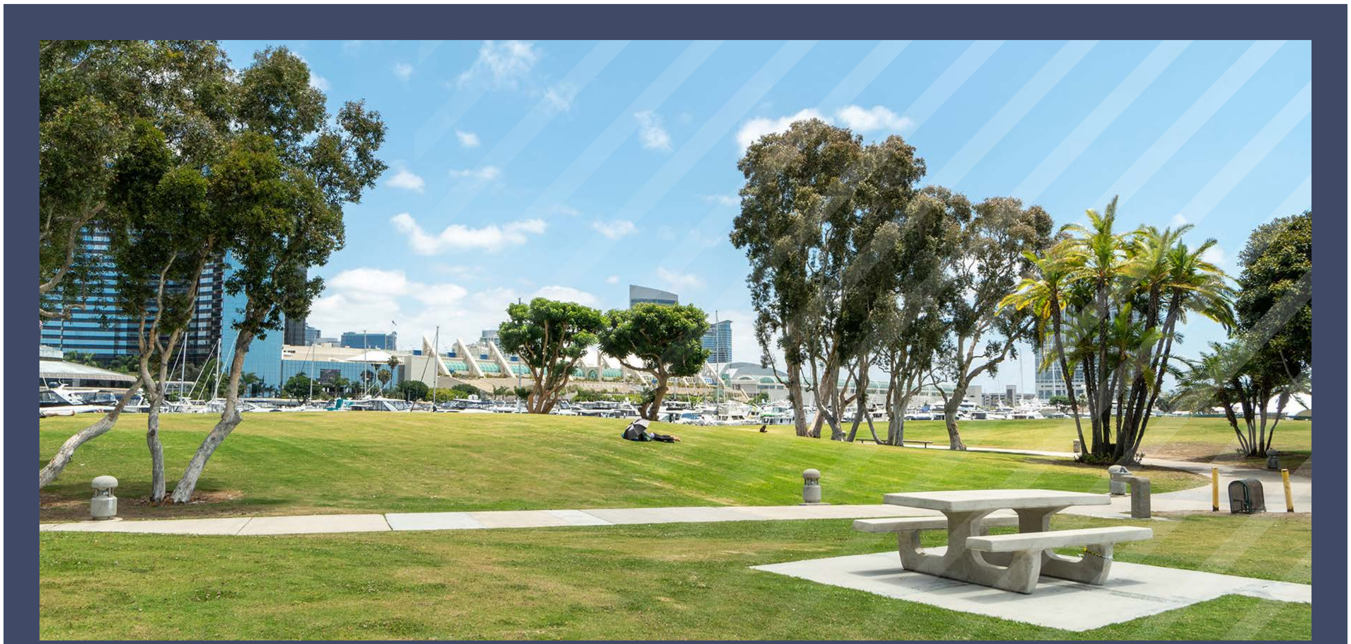
Take an outside-in approach to define and understand what's most important to your stakeholders (employees, customers, community, beneficiaries, donors).

A double materiality assessment integrates surveys, listening sessions, and direct engagement to identify priorities related to mission alignment, impact, workplace culture, sustainability practices, or operational transparency.

This assessment should:

- Identify what employees value most (e.g., flexible work, cybersecurity, community engagement, diversity, leadership transparency, sustainability).
- Map stakeholder values against organizational capabilities and strategic objectives.
- Prioritize investments where employee expectations and organizational impact and value overlap.

A resulting materiality matrix guides leadership on which culture investments yield the greatest retention and engagement returns.



3. Strengthen the Employee Value Proposition (EVP) Beyond Salary

Rather than competing solely on compensation, organizations can emphasize non-monetary motivators that drive loyalty, purpose, and engagement.

Potential differentiators:

- Flexible and remote work options
- Robust PTO and well-being programs
- Sustainability initiativesCommunity involvement or volunteer programs
- Ethical, transparent leadership
- Leading-edge digital capabilities
- Strong cybersecurity posture
- AI-enabled tools that improve efficiency and innovation
- Mission-driven culture with authentic societal impact

Mitigation requires identifying what uniquely motivates your workforce —then operationalizing, measuring, and communicating it.

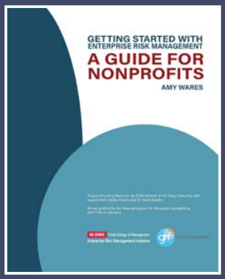
4. Communicate Progress Through Impact Reporting

Finally, ensure that findings and progress toward these goals are communicated effectively through impact reports and regular updates to stakeholders. Transparency reinforces trust and demonstrates how the organization is addressing top workforce and culture priorities.

Concluding Thoughts

Organizations face unique and elevated risk exposure as geopolitical shifts, federal funding dynamics, cyber threats, and workforce constraints converge. Organizations that enhance governance, strengthen mission alignment, and invest in cybersecurity, talent, and digital capability will be better positioned to thrive in 2026 and beyond.

Additional GRF Risk Management Resources



GETTING STARTED WITH ENTERPRISE RISK MANAGEMENT
A GUIDE FOR NONPROFITS
AMY WARES

DOWNLOAD

Getting Started with Enterprise Risk Management

CPAs & ADVISORS

Enterprise Risk Management (ERM)
The Handbook for Association Board Members

DOWNLOAD

ERM for Associations

About GRF CPAs and Advisors

Headquartered in the Washington, DC metropolitan region, GRF CPAs & Advisors (GRF) is a full-service professional services firm providing clients with audit and assurance, tax services, outsourced accounting, and advisory solutions. For 45 years, GRF has leveraged a deep bench of industry expertise to assist nonprofit organizations, government contractors, privately held businesses, trusts, and individuals with their most challenging financial and operational issues.

For more information on GRF CPAs and Advisor, visit grfcpa.com.

CPAs & ADVISORS

Advancing
TALENT, CLIENTS
and COMMUNITIES

CONTACT US

The GRF 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 and Advisory Services

Thomas Brown, CISA, CIA, Security+. CAPM
Supervisor, Risk and Advisory Services

Alex McNeill, PMP
Enterprise Risk Management Advisor, Risk and Advisory Services

CPAs & ADVISORS

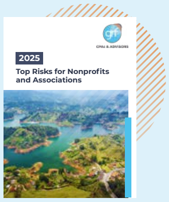
Appendix Sources

2026 Top Risks Report

www.grfcpa.com

Appendix: Top Risk Reports and Sources

Prior GRF Top Risks Reports



2025 Top Risks for Nonprofits and Associations

2024 Top Risks for Nonprofits and Associations

2023 Top Risks for Nonprofits and Associations

2026 Top Risk Reports

Executive Perspectives on Top Near-Term and Long-Term Risks, NC State

https://erm.ncsu.edu/resource-center/report-executive-perspectives-on-top-near-term-risks-and-long-term-risks/

Top 10 Near Term Risks (2025-2027)

1. Economic conditions, including inflationary pressures
2. Cyber threats and data breaches
3. Ability to attract, develop and retain top talent, manage shifts in labor expectations, and address succession challenges
4. Talent and labor availability
5. Increasing labor costs impacting profitability
6. Heightened regulatory changes, uncertainty and scrutiny
7. Third-party risks, including supply chain vulnerabilities
8. The rapid speed of disruptive innovations in AI and emerging technologies
9. Challenges in adopting AI and advanced tech requiring new labor skills in short supply
10. New and emerging risks arising from AI implementation

Global Risk Summary: Survey, The Institute of Internal Auditors

https://www.theiia.org/globalassets/site/foundation/latest-research-and-products/risk-in-focus/2026/2026-global-briefing-en-riskinfocus.pdf

Top 5 risks that your organization currently faces

1. Cybersecurity
2. Digital Disruption (Including AI)
3. Business Resilience
4. Human Capital
5. Regulatory Change

Top 10 Global Risks to Watch in 2026, Everbridge

https://www.everbridge.com/blog/global-risks-to-watch-in-2026/

Top 10 Global Risks for 2026

1. Cyberattacks and systemic cyber risk
2. The dual edge of AI
3. Natural disasters and climate-driven extremes
4. Geopolitical conflict
5. Business interruption from supply chain shocks
6. Misinformation and disinformation
7. Regulatory fragmentation and trade restrictions
8. Macroeconomic and financial instability
9. Talent shortages and skills mismatch
10. Polycrises

Additional Reports and Sources

From Risk Awareness to Value Creation: Internal Audit Strategies for 2025-2026, GRF CPAs and Advisors

https://www.grfcpa.com/resource/internal-audit-strategies-for-2025-2026/

State of Cybersecurity 2025 Report, ISACA

https://www.isaca.org/resources/reports/state-of-cybersecurity-2025

New ISACA Study: Despite Understaffed Cybersecurity Teams, Fewer Enterprises Are Training Staff for Security Roles, ISACA

https://www.isaca.org/about-us/newsroom/press-releases/2025/state-of-cybersecurity-2025-global-press-release

State of Cybersecurity 2025, CompTIA

https://www.comptia.org/en-us/resources/research/state-of-cybersecurity/

North American Pulse of Internal Audit, The Institute of Internal Auditors

https://www.theiia.org/en/resources/research-and-reports/pulse/

Risk in Focus Report, The Institute of Internal Auditors

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