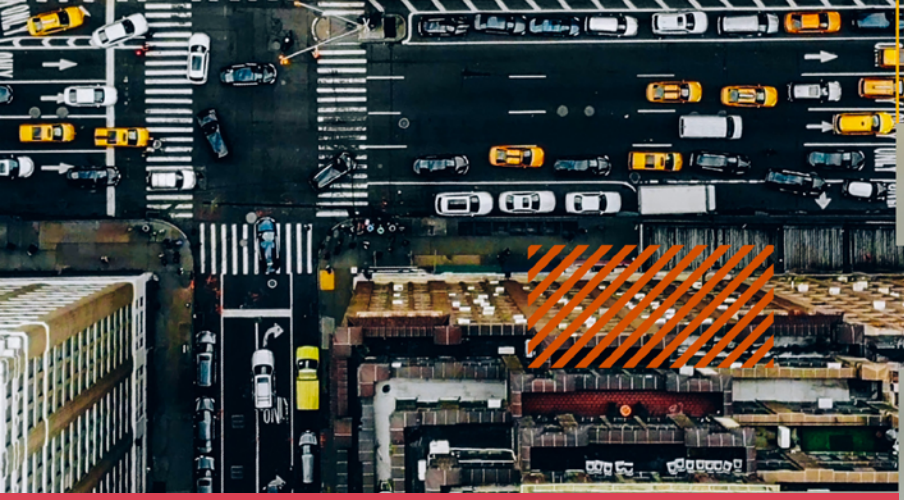


Technology risk: So pervasive, it's hard to see

How industry leaders can align to better manage it

Some risks are so all-encompassing they go unnoticed. Hiding in plain sight, their sheer scale, paradoxically, can obscure their sheer scale. Instead, we get glimpses here and there but rarely connect the dots across the enterprise.

This is a central problem of technology risk, a term describing the many vulnerabilities associated with an organization's information technology (IT), operational technology (OT) and communications technology (CT). Because technology touches everything a company does, all its assets (physical, digital, intellectual), its people, processes and systems, its vendors and suppliers, its reputation — even its very existence — the scope and layers of risk associated with technology's use can be difficult to comprehend, much less mitigate.

Compounding the challenge is a company's organizational structure, which can hinder an enterprise-wide view of risk. Different functional areas — IT, enterprise data management, cybersecurity, compliance, R&D, commercial, third-party risk management, supply chain, internal audit, etc. — have their own priorities, incentives, tools and terminology. They may view the same risk differently or give it different names. They may view impacts that stretch beyond their team's purview as someone else's problem.

In short, these functional areas tend to operate in silos, without coordination across lines of defense, in some cases working at cross purposes. The result is an untenable mix of gaps, duplication and missed opportunities — leading inevitably to greater exposure overall.

So how can your organization tackle such a pervasive risk? Where should you start?

Ultimately, assessing, managing and reducing technology risk requires an enterprise-wide level of coordination. Only by looking horizontally across organizational silos will the scope and severity of the threat become clear. This means tech, risk and other business leaders should collaborate across the silos to understand the risk and its many permutations, identify what's affected and size the gaps.

But first, everyone involved should agree on a shared lexicon or taxonomy that defines the risk and its many forms.

pwc

What is technology risk?

Technology risk can be described as the many risks associated with an organization's technology, its use and the enabling infrastructure and capabilities. Cybersecurity and data governance often come first to mind as examples, but the scope is much broader. It includes hardware, software and network failures. It also includes risks associated with IT infrastructure and the day-to-day operations that technology enables — again, because technology touches everything a company does, all of its people, data, processes and assets.

Technology risk examples

- Ineffective architecture
- Technical debt
- Capacity issues
- Unmanaged physical assets
- Tech obsolescence
- Emerging tech disruption
- Third-party failures
- Data corruption
- Human capital shortages
- Failure to deliver on business requirements

With the vast number of technology risks that can exist and emerge for an organization, how can one begin to prioritize efforts to manage them? Many organizations address IT risks related to financial reporting within their internal control over financial reporting (ICFR) frameworks, and they may highlight a few risks within their enterprise risk register that speak to cyber and data risk — but that's not sufficient.

Where are all the other technology-oriented risks identified and how are you managing them? If technology is the fuel that powers business operations and innovation, shouldn't there be

Framing technology capabilities: Is there a framework and is it current?

Before you can identify and assess the many tech risks in your organization, you need to catalog your technology capabilities. Understanding all that your business does with technology can help uncover where the risks lie. This requires having a governance framework in place that accounts for all technology capabilities across the enterprise.

Any reputable framework (COBIT, ITIL, TOGAF, etc.) can serve as a starting point, but it won't (and shouldn't) be a lift-and-shift. These frameworks require customization to fit the organization's structure and needs. The goal is to implement a widely accepted mechanism for governing your organization's technology capabilities and aligning them to business priorities, processes, functions and infrastructure.

Moreover, the framework must be current. Having an enterprise tech governance program does little good if it hasn't kept pace with the organization's evolving technology. In our experience, many companies haven't inventoried their tech capabilities formally in years, if at all.

With an updated tech governance framework in place — and a resulting, current inventory of tech capabilities and the associated stakeholders, processes and metrics — your organization can begin identifying the universe of risks with confidence. Ask yourself, what are the potential vulnerabilities in each tech capability and the business implications of failure, error, degradation, delay or other weakness?

Categorizing risks: Does a common language exist?

The range of risks and the many different, overlapping names applied to them makes it a challenge to identify and assess them all. Organizing them into a logical, hierarchical taxonomy can be harder still as there are endless possibilities and getting agreement across the enterprise can be elusive. The good news is that there's no single right answer — a tech risk taxonomy can take many forms, any one of them potentially useful, as long as the risk language translates to the organization and stakeholders can reach consensus.

At a high level, technology-related risks fit into broad categories.

Strategic and governance risk
Risk that an organization will miss its goals due to internal or external events. Examples include poor decision-making, governance failures, financial mismanagement, missed opportunities, competitive threats and new market entrants, M&A, shifting customer demands, macroeconomic pressures or geopolitical uncertainty.

Operations risk
Risk related to the day-to-day operations of technology systems and how they may impact business activities. These include system failures, network and cloud outages, business continuity risks, software bugs, tech obsolescence and human errors that can disrupt business processes and limit productivity.

Cybersecurity risk
Risk of unauthorized access, data breaches, malware attacks and other threats that can compromise the confidentiality, integrity and availability of technology systems and data.

Compliance risk
Risk of noncompliance with laws, regulations and industry standards related to technology, such as privacy and data protection regulations, financial regulations and industry-specific requirements.

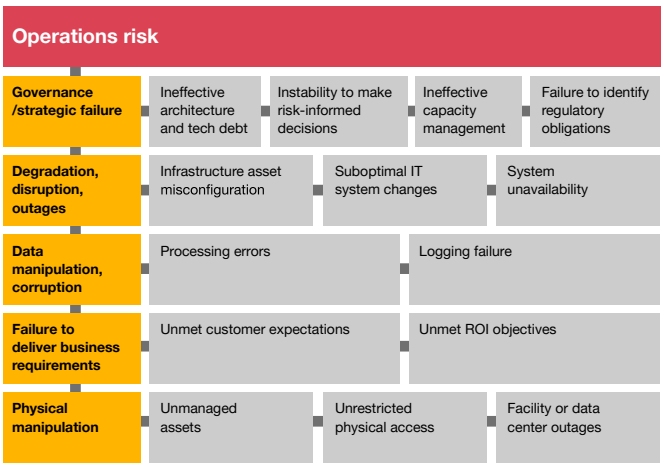
Third-party risk
Risk associated with third-party vendors, suppliers, contractors, logistics partners and cloud services, including their ability to deliver products and services, their security practices and their potential impact on the organization's technology infrastructure.

Software development risk
Risk related to application development, software development life cycle (SDLC) and application change management.

Emerging tech risk
Risk associated with adopting new and emerging technologies, such as generative AI, cloud provider convergence, intelligent applications and web3, including security vulnerabilities, lack of standards and uncertain outcomes. Failing to adopt new technologies can also introduce risk, as legacy systems become less sustainable.

Data integrity risk
Data is the "devil in the details" and the risk of poor data quality, incomplete or inaccurate data and the lack of governance or traceability can all lead to misinformed decisions or reporting (financial, regulatory, customers).

Taking the second category (operations risk) and drilling down two levels, for example, you might arrive at the following hierarchy:



Every organization will have its own take on technology frameworks/capabilities, risk taxonomy, and approach to grouping the many sub-risks, which themselves will vary by organization (and sector). Within an organization, individual teams and stakeholders may have different views and terminology. What's more, those views will likely evolve over time as the company and technology itself evolves. The point is to forge a consensus on a working taxonomy that will serve as a foundation for identifying, assessing and managing technology risk across the enterprise.

Bottom line

Understanding what tech risk is, identifying which parts of your organization it touches and agreeing how to categorize it are three foundational steps you should take from the outset. You can't diagnose a problem — much less implement an effective, enterprise-wide solution — without this baseline understanding and framework to guide you.

Once you've done this foundational work, you'll be well-positioned to take meaningful action. You'll be able to accurately identify where each risk lies, assess your current capabilities to manage those risks and determine your residual exposure. From there, stakeholders can then align on priorities and allocate resources needed to manage this exposure.

But first things first. Understand the risk and its many forms, know where it lives and align on terminology for describing and categorizing it.

Contact us

Michelle Horton
Principal, Cyber, Risk & Regulatory, PwC US
michelle.r.horton@pwc.com

Elizabeth McNichol
Principal, Enterprise Technology Solutions Leader, Cyber, Risk and Regulatory, PwC US
elizabeth@pwc.com