Technology Risk Management 1.0

The Need for Change
Executive Summary

Across nearly all industries, organizations are becoming more and more dependent on technology, so much so that it is easy to argue that many are actually becoming technology companies. Consequently, how organizations embrace technology can have a significant impact on how they are perceived by their customers or business partners.

In some instances, technology is enabling wholesale shifts in business models, as evidenced by the impact of Uber on the taxi industry, Apple and Netflix on the media industry and AirBnB in the hospitality sector, while fintech is disrupting the financial services sector. Here, technology is redefining how consumers engage with firms and buy products. To compete, traditional companies need to become more agile and adapt rapidly to the changing business environment.

The pace of change is a constant and growing challenge, accelerating in line with digital engagement and enabled by emerging and evolving technologies. While some companies have embraced new capabilities and continuous change, innovation has been limited at more traditional institutions. These companies continue to offer products that have not changed fundamentally for several decades and are often underpinned by creaking legacy systems and processes. In response to the changing market dynamic, some of these firms are beginning to recognize the need to adopt newer technologies and operating models, such as cloud computing, and are placing greater reliance on third parties to manage their IT environments.

New technology brings both opportunities and risks. However, the predominant risk facing traditional firms today is failing to innovate. Organizations need to embrace innovation, foster cultural change and embark on digital transformation programs designed to become ever more nimble and keep pace with the rapidly changing business environment. Risk management and IT departments need to be responsive to this change and ensure they are not unintentionally blocking innovation, and provide the organization with the knowledge and the tools to conduct “good” risk tasking within a defined risk appetite.

Against this backdrop, Protiviti conducted a technology risk study to explore whether technology risk functions have the right strategy, skills and operating models to enable the organization to understand, assess and manage existing and emerging risks. The findings enhance Protiviti’s benchmarking data and measure how businesses are responding to their increased dependence on technology. The study also sought to better understand how risk management disciplines are evolving to reflect the increased importance of technology and changing operating models.
The findings from the study, set out in this paper, have reinforced Protiviti’s long-held view that technology risk is failing to keep up with the rapid pace of technological change. This is particularly prevalent in organizations that are struggling with the notion that they are becoming a technology company, for example, within industries such as financial services, where firms are just starting to recognize that technology companies and fintech start-ups pose a greater threat to their business than their more traditional competitors.

This paper details the current state of technology risk, based on our survey findings, while the accompanying document, Technology Risk: A New Approach, introduces the Protiviti Technology Risk 2.0 Model, a proven framework and methodology firms can use to create a more integrated technology risk function.¹

**OUR KEY FINDINGS**

- There is a lack of coordination between different groups performing technology risk management activities.
- Technology risk reporting tends to be technology-centric without providing real business insight.
- Business risk appetite is not driving technology risk practices.
- Many organizations’ technology risk activities are not ready to embrace a cloud-enabled world.
- Vendor risk management needs to be strengthened and integrated into core technology risk activities and reporting.
- Technology risk awareness is not effectively embedded in the culture of most organizations.
- Ironically, there is ineffective utilization of technology by technology risk teams.
- Technology risk functions are not providing adequate or effective information for executives and board members.
- The criticality of technology risk disciplines is elevated by cybersecurity issues (but cybersecurity should not be viewed as synonymous with technology risk).
- There is excessive focus on downside risk, causing organizations to miss key strategic risks and opportunities.

¹ Available at [www.protiviti.com](http://www.protiviti.com).

The term “technology risk management” often leads individuals to focus on downside risks and how to prevent incidences such as system failures, cyberattacks or leakage of confidential data. But in this fast-changing world, technology risk activities must also focus on the risks posed by not engaging technology to drive business value, to provide organizations with that “first mover” advantage or differentiation.
The Current State of Technology Risk

Protiviti’s technology risk study, completed in 2016, assessed companies on the maturity of their technology risk processes. Two-thirds of the companies interviewed were financial services firms. The study was purposely slanted toward financial institutions as they are often perceived by many to be leaders in the field of technology risk management.

The results of the study are assessed against Protiviti’s Maturity Model. This is a four-point scale that assesses the maturity of organizations’ technology risk processes, which reflects the evolution of a technology risk function starting at Level 1, maturing through Levels 2 and 3, to ultimately reach Level 4, which is considered to be a best practice model.

Protiviti’s Maturity Model

**LEVEL 4 | OPTIMIZED | Business Value-Centric**

- All elements of Levels 1-3 maturity retained
- IT risk management (ITRM) fully integrated with enterprise operational risk management (ORM)
- IT metrics fully integrated with other operational metrics for full transparency of risk
- IT risk management mitigation efforts and investments fully integrated with enterprise operational risk efforts
- IT and operational risk management proactively incorporate emerging technology risks into the risk management equation

Focus: Protecting and enhancing the value of the business

**LEVEL 3 | MANAGED/QUANTITATIVE | Business Service-Centric/Aligned**

- All elements of Level 1 and 2 maturity retained
- ITRM framework defined primarily by business-specific risks vs. IT risks
- Key business and IT metrics calibrated to business risk tolerance
- Business outcomes directly mapped to underlying IT systems, processes, services and architecture elements
- Key IT metrics expressed in terms of business outcomes
- Risk mitigation efforts against IT risks can be substantiated by predicted improvements in business outcomes

Focus: Management of business risks/outcomes via the management of IT controls and processes

**LEVEL 2 | DEFINED/INTEGRATED | IT Application-Centric**

- All elements of Level 1 maturity retained
- IT process, service, application and service catalogs developed and mapped to business processes
- Increased risk in IT processes is linked to increased risk in related business processes
- IT risk reporting focuses on both IT processes and potential impacts to business
- IT risk tolerance and IT risk mitigation efforts are refined and informed by potential impact to business outcomes

Focus: Management of IT-specific risks with a clear understanding of business process impacts

**LEVEL 1 | INITIAL/STRUCTURED | IT Component-Centric**

- ITRM governance and oversight defined
- Defined ITRM process model deployed
- Critical IT processes and risks defined
- Controls inventoried and assessed
- Metrics captured and targets defined
- Risk tolerance defined at the IT process and IT component level
- Consistent and detailed reporting on metrics, risks and remediation items performed

Focus: Management of IT-specific risks, metrics and controls
The majority of study participants acknowledged that most of their technology risk activities in the business were at Level 1. A few were starting to perform technology risk management activities at a higher level, but the scope of these was typically limited. None of the financial services firms that participated in the study were operating at Level 4, while those assessed as Level 3 were only just starting to demonstrate such characteristics.

All of the survey participants have ambitions to mature their approach. However, given delivery and budget pressures, there remains a degree of uncertainty about whether they will be able to follow through on their desire to progress up the maturity scale.

The graph below shows the current state and anticipated future state of the organizations surveyed, as assessed against Protiviti’s Maturity Model.

**Firms’ Current State vs. Anticipated Future State**

- **LEVEL 1**
  Initial/Structured (IT Component-Centric)
  - Scope is often driven by consideration of key applications; however, the focus of risk management activities is on individual IT components and processes (e.g., networks, applications and databases). Limited aggregation of risk assessment results provides a comprehensive view of risks to confidentiality, availability and integrity of applications.

- **LEVEL 2**
  Defined/Integrated (IT Application-Centric)
  - Results of assessments performed on IT components on which an application depends are consolidated to provide application owners with a comprehensive view of the risks to confidentiality, availability and integrity of their applications.

- **LEVEL 3**
  Managed/Quantitative (Business Service-Centric/Aligned)
  - Further consolidation of the data is captured in risk assessments to provide increased visibility of business outcomes. This is often achieved by aggregating results of risk assessments around business services (e.g., online banking, processing payments and trading equities) that may be dependent on effective operating of multiple applications or systems.

- **LEVEL 4**
  Optimized (Business Value-Centric)
  - IT risk management is fully integrated with enterprise-wide operational risk management. Risk management activities provide a complete end-to-end view of the customer or user experience. IT risk management activities consider operational risks and strategic risks (e.g., inability of business to respond to potentially disruptive technologies).
The Protiviti Perspective

Technology governance and risk management disciplines, at most organizations, are unfit for the intended purpose and are not evolving quickly enough to keep up with the pace of change within the business. More detailed observations from the study, set out below, demonstrate the main areas where the majority of firms are falling behind, as well as insights and best practices from leading companies.

Limited Integration of Technology Risk Functions and Methodologies

Most technology risk functions operate as stand-alone functions, reporting on either enterprise risk or operational risk at the higher levels of the organization. However, little integration of the two functions was observed at the lower levels.

Not all firms have central technology risk functions. Technology risk employees are scattered throughout distinct functions and teams — such as vendor risk, operational risk and compliance, among others — each performing individual technology risk activities with their own distinct methodologies. The trend is to more clearly delineate first and second lines of defense, which have been blurred in relation to technology risk in many organizations, with separate teams focusing on core processes, applications and infrastructure. Few companies were found to be effectively integrating all of these functions, which has led to gaps, duplication of effort and difficulties in reconciling findings/conclusions.

In large firms communication between functions is poor, with most teams operating in silos. Smaller companies displayed better communication. This was more a consequence of their size and subsequent ease of communication, rather than process design.

Call to Action:

- Companies need to implement a holistic technology risk framework, with consistently applied methodologies and common language appropriate for all groups across the enterprise, whether applied to technology or compliance risk activities.
- Organizations should identify all teams working on technology risk activities, align their activities against this framework and define their roles within the context of the framework.

Providing Real Business Insight

Most technology risk teams are good at understanding technology and highlighting its potential risks, but very few organizations translate this effectively into providing business insights. As a result, gaining senior executive engagement is extremely difficult, particularly when conclusions are presented in terms of technology issues rather than business impacts.

For example, a business might conclude that it is “not effective at managing privileged access or patching servers,” but a more insightful presentation to senior management could use a forward-looking assessment to show how often a customer experience (internal or external) would be adversely impacted, as well as some insight into how long such an impact would take to address.

---

2 In the three lines of defense model, management control is the first line of defense in risk management, the various risk control and compliance over-sight functions established by management are the second line of defense, and independent assurance is the third. Each of these three “lines” plays a distinct role within the organization’s wider governance framework.
Presenting risks in this way ensures attention from executive management and prompts meaningful discussions about business impact and risk appetite. Gaining stakeholder engagement is essential for effecting change; this can be gained by changing the way technology risk is reported.

Today, most firms report technology risk to the board level as a vertical, tier one risk. Although this approach may have originally been intended to raise awareness of technology issues at the board level, it has had the unintended consequence of divorcing the impact analysis of technology risk from the true impact to the business. Without aligning technology risk metrics to business impact, incorrect decisions are frequently made about remediation priorities. Technology risk reporting remains very IT-component centric, ignores business process controls and fails to answer the key questions that business leaders are asking.

**Call to Action:**

- Technology Risk is usually presented as a distinct risk category in operational risk frameworks and, as result, is often assessed in isolation. While this helps increase focus on technology risk, it tends to result in it being assessed in isolation, with no clear consideration given to business impact. Technology risks should be assessed as a sub category of risk. For example, when considering fraud risk or financial crime, technology risk should be considered as a contributory factor.
- Firms need to revisit how they report on the business impact of technology risks. It is essential that technology risk reporting focuses more on adverse business outcomes and not the control weaknesses that may cause generic issues to arise.
- Organizations should review the metrics they are capturing to ensure they are measuring business outcomes rather than focusing on technology outcomes (e.g. system downtime is a technology centric metric, whereas number of failed ATM withdrawals and or value of late or failed processing of payments are metrics focused on business outcomes).
- Mainstream technology risk functions are focused too much on managing downside risk stemming from their core IT processes, including security, integrity, resilience and availability. Technology risk teams need to assess firms’ agility and effectiveness at supplying the information that will allow the business to exploit the benefits of technology.

---

**Case Study 1: Assessing the True Impact of Technology on Business Risk**

System downtime is one example where service managers are often incentivized, usually measured via metrics such as 99.99 percent uptime. Unfortunately, this technology-focused approach takes no account for differing impacts to the business.

One very large retail bank augmented its traditional IT risk metrics to include measurements of successful critical business transactions, to better measure the impact of technology on business risk. This simple move yielded interesting, if not surprising, results. After years of focusing on IT-focused metrics, including system availability and reducing the number and duration of high-severity incidents — which had yielded significant improvements in IT metrics — the new, business-oriented metrics highlighted the need to focus on different areas.

The bank’s customers had adopted a 24/7/365 operating expectation and the organization had expanded to operate in multiple time zones. This renewed metric showed that the highest percentage of failed business transactions happened during planned-maintenance windows. This realization led the organization to adopt new architectural and operational patterns that significantly reduced the need for and duration of these planned-maintenance events.

Not coincidentally, this shift also changed the dialogue between the IT organization and its business partners by creating a common language. Another unanticipated, albeit indirect, benefit was that this work enabled the organization to become more nimble and enable digital services. All this was achieved because the organization shifted its focus from internally facing IT service metrics to business-centric outcome metrics.
Excess Focus on Downside Risk; Missing Key Strategic Risks

Technology risk managers are good at highlighting issues with the technology that firms are using today and at identifying problems that arise when embracing new technology. Very few consider the risk posed by not adequately responding to change or embracing new and emerging technologies. In financial services organizations, this is a reflection of the fact that those working on technology risk reporting form a part of the operational risk function, with a specific focus on the risks the business is carrying today.

As traditional taxicab companies are now discovering following the advent of Uber (see case study 2 below), the risks associated with failing to adopt or respond to potentially disruptive technologies can be much more significant than those attached to imperfect operational processes.

Few technology risk management approaches consider agility and assess the ability of the business to respond to potentially disruptive technologies as part of their risk management approach. Almost all technology risk groups are focused on the operational risks of today and the security and efficiency of their business processes. This approach is as a result inhibiting innovation by providing many reasons why firms should not do something, rather than why they should.

Companies need to be prepared for rapid change. Horizon scanning and anticipating the impact of disruptive technologies is an essential task, while firms also need to ensure that their core systems are fit for purpose by supporting anticipated digital transformation activities. Most financial institutions, for example, have creaking proprietary legacy systems in place that make it much more difficult for them to rapidly embrace new technologies.

Technology risk reporting needs to incorporate forward-looking as well as pure operational risks. These are very rarely considered by technology risk teams today. Unfortunately, almost all technology risk functions would claim that those decisions are out of their scope of responsibility or influence, and as a result no one owns the burden of reporting on these strategic technology risks. Firms need to look more holistically at technology risk, and in doing so increase the likelihood that they will become more agile and able to respond to change over time. Organizations should be encouraged to experiment with disruptive technology, which is just as important to the business in the long term as the management of operational and technology risk.

A study by the Economist Intelligence Unit (EIU) found that 36 percent of banks believe that their main threat is from technology companies rather than their traditional or challenger bank competitors.
The technology giants (commonly referred to as GAFA — Google, Apple, Facebook and Amazon) have embraced technology to exploit available opportunities, although for the moment they are not challenging the banking sector. In banking organizations, digital development teams are often separated from the legacy IT teams, with a very different culture and vision than the more traditional aspects of IT. These teams sometimes have separate technology risk teams, operating independently of the core technology risk team.

The general focus on downside risk is primarily due to regulators’ concentration on such risk events, specifically those that impact consumers. This situation persists despite supervisors praising innovation in the financial services industry. Mindful of a risk-averse regulatory focus, firms have been unable to naturally develop capabilities that encourage risk-taking or technological innovation.

For companies to engage innovation and embed it into the firm’s culture, it is essential that risk functions assess how good the organization is at embracing risk. Risk functions need to encourage risk-taking and reward innovation, while ensuring the legacy business is protected from the risks innovation presents. Although lack of agility is one of the greatest risks an organization faces, risk management processes are often blamed for applying the brakes.

**Case Study 2: The Uber Effect**

In 2012, when the online transportation network company Uber entered the market, revenues for San Francisco’s taxicab industry were approximately $250 million. By the end of 2013, revenues for the city’s traditional taxi companies were cut in half to about $125 million, while Uber’s revenues were approximately $400 million.

In the span of a year, Uber expanded the market cap by close to 110 percent, and the company now accounts for about 64 percent of the existing market share in San Francisco. The city’s largest taxi company, the Yellow Cab Co-operative, filed for bankruptcy in January 2016.\(^3\)

Uber, which continues to disrupt other markets internationally, including London’s taxicab industry, is now often cited as an example of how disruptive technology is affecting established industries.

The impact of Uber has been so disruptive that it has become commonplace to describe the sudden, fundamental reinvention of commonly accepted business models using advanced technology as “Uber moments”, a term coined by Anthony Jenkins, the former chief executive officer of Barclays, in a November 2015 speech. Traditional organizations need to prepare for these “Uber moments” by adopting and integrating emerging technology and embracing new ways of doing business.

---

Using Business Risk Appetite to Drive Process

Almost all of the companies examined in the study do not have a true definition of their technology risk appetite, which is fettering effective decision making. Risk appetite statements are defined currently by IT metrics, such as the 99.99 percent available or the number of acceptable priority 1 incidents. It is very difficult to define the right level for these generic IT metrics. This is the reason so many organizations have been assessed as being at Level 1 or Level 2 in Protiviti’s Maturity Model.

Setting technology risk appetites for specific business-centric risks is relatively simple. Business-centric risks relate to questions such as: “How many failed payments are acceptable?” “How many customers are impacted by online banking outage or failure?” and “How many failed attempts to withdraw cash from an ATM machine can be tolerated in one week?” By measuring risks that focus on outcome rather than cause, the business can assess whether its risk profile is improving or deteriorating and amend accordingly. Some companies have shown some progress toward implementing business-focused metrics but most have adopted a bottom-up approach to those risk assessments that remain centered on technology components.

The lack of top-down analysis of the business risks arising from technology failures limits the company’s ability to effectively assess risks. One investment bank surveyed had identified over 100 critical issues requiring attention to address significant cyber risks, but there was no suitable framework within the organization to prioritize these issues based on a defensible risk-based approach.

Integrating this bottom-up approach with a top-down approach that is focused on customer experience, threat assessment and risk assessment is a critical step many organizations are struggling with or missing. This needs to be addressed if organizations are to progress to the next level and seek to provide real business insight.

Furthermore, companies need to base management information and reporting on business-centric information provided by tracking business-centric metrics. Such metrics could include how many days have elapsed since the last significant consumer-impacting event or how many minutes in the last month the firm has been unable to execute trades or payments. Even better metrics, if the data can be obtained, would be the total value of trades, or payments, the business was unable to complete on time due to a technology failure. Companies are then able to aggregate these top-down business risks using a dashboard, which can give a macro-level view of whether the company’s risk exposure is rising or falling. The Protiviti Risk Index™ is a customizable solution designed specifically to capture, calculate and evaluate a large volume of complex risk data and reduce it to a single-number snapshot of organizational risk. By amalgamating the reports of these top-down business risks in a single view of risk, new and changing risks are more easily identified and the company can track whether it is getting better as a result of certain mitigation efforts.

See www.protiviti.com/riskindex for more information.
Getting to the stage where the organization has a top-down view of its business-centric technology risk to enable real-time business decision-making is a significant and time-consuming project. A complete transformation from bottom-up to top-down can take time to achieve. A targeted effort, focused on specific risk areas and/or high risk business areas, can be achieved much more cost effectively. The business can use these targeted efforts to embed the concepts and over time look to extend and embed the concepts enterprise wide.

Call to Action:

- Risk appetite statements should be reviewed to assess their business focus and revised where required.
- Companies should complete a top-down technology risk assessment.
- Companies need to consider how risk appetite is being used when determining scope and assessing the design effectiveness of controls – a one-size-fits-all approach is inappropriate.
- Business-centric metrics should replace technology-focused metrics and inform better risk reporting.
- Business-centric metrics can be aggregated using a dashboard to provide a clear picture of the firm’s technology risk profile.

Case Study 3: Balancing Metrics

The study revealed one IT infrastructure team that was struggling to apply patches to its servers because service managers were so focused on system uptime that they did not allow for change windows for maintenance work to be carried out. While the team was meeting its key performance indicator of maintaining constant system uptime, keeping those systems available was increasing information security risk because issues were not being patched on a timely basis.

This scenario is partly driven by the culture of the organization and by their existing metrics, but it can also be caused by a lack of data. Firms need to ensure they are not becoming too focused on one metric or risk causing other issues. Implementing a balanced program of end-to-end business outcome metrics, provided by data from an integrated technology risk methodology, would overcome such a scenario and allow the business to make more informed decisions.
Not Ready for Cloud; Poor Vendor Risk Management

Operating in the fast-moving, technology-connected environment, organizations are becoming increasingly open to the outside world. The proportion of technology managed outside the organization, whether through cloud services or third-party managed services, is increasing and will continue to do so, creating both opportunities and risk.

A consequence of this is that an increasing proportion of firms’ information assets are being managed outside of the remit of the technology risk function, increasing the importance of vendor risk management. However, risk assessments of third parties in almost all organizations studied were found to be woefully inadequate. In many cases third-party risk assessments were completely absent or limited to sending standardized schedules or questionnaires to suppliers to fill in. There were a few occasions where firms performed onsite audits, but these were very superficial.

Most organizations determine their critical vendors by spend — in other words, the most critical vendors are those that cost the most. But it is possible that lower cost, smaller vendors may house firms’ most critical data. The study also found that many firms consider it too difficult to effect change in a third party, in many cases, they accept the risk and move on.

An increasing risk profile from vendors requires greater investment in order to protect the organization and its assets. Without an effective linkage between technology risk methodologies and associated control disciplines, these functions will continue to struggle for priority and suitable investment. Currently, vendor risk is managed separately from other technology risk activities. The results of vendor risk assessments are very rarely integrated with technology risk assessments to provide a complete view of risk. The most commonly cited reason for this lack of integration was differing requirements. This separation makes it increasingly difficult for vendor risk teams to demonstrate value to the business. Another key issue is that aspects of third party risk are not being considered as part of operational risk reporting; a vendor attains the generic standard, that it can or cannot be used. Companies need to work with their suppliers in a collaborative way to understand risks and agree on risk mitigation plans. To do this effectively, however, vendor risk management must be integrated with other risk management activities, including technology risk.

Call to Action:

- Consider whether vendor risk management activities are providing an appropriate level of insight into the risks at key third parties.
- Consider how findings from vendor risk reviews are being reflected in conclusions reached in technology risk/operational risk reports.
- Ensure that vendor risk programs are not too restrictive when it comes to collaborating with fintech companies and/or innovating.
Risk Management Culture Not Embedded

There is some debate over where the technology risk function should reside within the three lines of defense model. There is the perception of a general lack of risk management skills or mindset within first-line IT operational roles. Although IT teams are very good at the day-to-day management and operation of technology, they are not trained to think like risk professionals. As a result, separate teams of risk professionals are created to take on these responsibilities, which tend to operate between the first and the second line of defense.

Firms need to embed a risk and compliance culture into the IT function; starting by integrating operational risk activities into the day-to-day operational processes, and providing better training and risk management tools.

Individuals in IT support and incident management roles should be expected to quantify business impact, understand which controls failed when incidents occur, and be able to recommend enhancements to the control environment. Such analysis will boost management’s understanding of the operating effectiveness of controls, and embed an understanding of risk management.

Change-management teams need to maintain the entity mappings (a mapping of IT components to top level business risks), as well as associated risk and controls libraries and perform the top-down and bottom-up risk analyses as a default part of any change project. Doing so will help the business design controls into operational systems.

Technology teams need to understand that it is normal to accept risk, as long as it is suitably assessed. As firms look to experiment with new solutions, they will inevitably need to take risks; the benefits of being first to market and of being an innovator must not be overlooked. Embedding risk analysis into the business-as-usual processes in the first line, overseen by the second line that facilitates the process, is essential for encouraging innovation.

Call to Action:

- Firms should review training provided to the first line of defense on IT and assess wider technology risk awareness.
- A review of core business processes can identify opportunities where key risk management activities can be incorporated into business-as-usual processes (e.g., root cause analysis following an incident should consider risk appetite and tolerance to determine if the failure puts the business above tolerances, assess which key controls failed, which is reflected immediately in risk reporting with an assessment of control design effectiveness that takes into account risk appetite. This should be part of a single, integrated process).
Ineffective Utilization of Technology; Poor Management Information

Despite being an integral segment of the technology function, technology risk teams are poor innovators when it comes to using technology. Processes and supporting tools used at most firms are comparable to those used many years ago. This is in part a consequence of technology risk teams’ failure to provide insightful reports to executives, demonstrating the value that they are adding to the business. This is never more important than when looking to invest in change projects.

Few organizations are making good use of continuous controls monitoring technologies to automate the testing of operating effectiveness of common controls. While the technology function frequently uses continuous monitoring tools, these are not integrated in any way with governance, risk management and compliance platforms that technology risk teams use to report on operating effectiveness of controls. As a result, costly, labor intensive processes, with relatively low sample sizes, are used to support attestation processes.

Additionally, technology risk systems are rarely making use of service management platforms to facilitate analysis of what types of incidents are rising and, conversely, what controls are failing, or using configuration management platforms to understand the technology landscape.

Risk assessments are completed infrequently and cannot be used to support any real-time decision-making by the business; firms’ failure to link technology issues to business risks has disengaged stakeholders from the business impact of technology risk events. Companies need to embrace continuous monitoring, automated testing and real time reporting to monitor the impact on its risk profile. Periodic, manual testing is not enough as such data can be upwards of 12 months out of date.

Leaders should be demanding reports that provide relevant stakeholders with near-real-time information on emerging threats or recently identified control failures to assess their impact on the most important business risks. Dashboards should provide quick access to progress updates on key risk mitigation actions underway and should include risk indexes that provide executives with an immediate view as to whether risk levels are increasing or decreasing daily.

Call to Action:

- Businesses should consider opportunities to use continuous monitoring technology and data analytics to drive efficiencies, provide greater coverage and to enable real-time risk remediation.
- Technology risk teams should reassess the effectiveness of risk reporting (using data visualization tools and dynamic real time reporting).
- Firms should assess effectiveness of GRC technology implementations to identify opportunities to drive efficiencies.
Cyber Risk Exposes Inadequacies of Technology Risk Processes

Challenges in assessing exposure to cyber risks and inadequacies in controls has exposed the shortcomings of firms’ technology risk management activities. Existing technology risk activities and reporting should provide all the information a chief information security officer (CISO) needs to design a business-orientated cybersecurity plan. Organizations have been assessing information security for many years, so this should be a simple task. However, when CISOs have needed to assess exposures and perform gap analyses, they have been unable to obtain the information they need. Instead of attempting to address the issues they have with their technology risk models, information security teams have instead created new risk assessment processes, managed independently of the existing technology risk activities, in order to meet the additional requirements. Although this addresses a short-term need, it ultimately compounds the problem and leaves business leaders with two, often inconsistent, views of the truth. Cyber risk analyses often highlight many risks that are not represented, even at a high level, in operational risk reporting.

Technology risk and cybersecurity teams need to start afresh and design an integrated approach that works for both CISOs and CROs. This will ultimately save the business time and money, and ensure that the organization has a clear understanding of the investment priorities.

Call to Action:

- Companies should consider whether it makes sense to integrate cyber and technology risk approaches.
In Conclusion: The Need for Change

Almost without exception, the companies assessed in this study have ambitions to mature their technology risk activities, but it is uncertain, given delivery and budget pressures, whether they will be able to achieve their goals.

In many cases, to address the issues identified previously, significant changes will be needed not only with risk management processes and tools but also in the way governance, risk and compliance teams are organized. For the majority of organizations, this process does not require additional people or cost to operate once it has been established. Technology governance, risk and compliance activities need to be consolidated and better integrated. This integration can be achieved by using technology more effectively, but the operating model needs to be in place first. Once the framework has been established, the risk function will then be able to think creatively about how it is brought to life using technology.

A risk management culture needs to be embedded into IT. Technology risk assessment activities should be fully integrated with service and change management activities in order to achieve this goal. Implementing a unified, enterprise wide, top-down analysis focus enables the company to prioritize its technology risk efforts while eliminating duplicate efforts and systems, resulting in more efficient processes.

Technology risk needs a digital transformation of its own if it is going to be fit for purpose as the business seeks to drive forward its digital transformation agenda. It is time to reimagine the way firms manage technology risk and how the risk function can become an innovator, if it is going to remain relevant to the business. The accompanying document, Technology Risk: A New Approach, introduces the Protiviti Technology Risk 2.0 Model, a proven framework and methodology firms can use to create a more integrated technology risk function. This approach goes much deeper than utilizing a common platform; it seeks to reengineer and redesign the way technology risk and information security work and integrate methodologies to create a more holistic view of risks in the enterprise.

Available at www.protiviti.com.
How Can Protiviti Help with Technology Risk?

There is enormous pressure for financial services technology and IT leaders to become more nimble and adaptive. Furthermore there is pressure to maintain controls and manage costs. Our blend of consulting expertise and deep industry experience uniquely positions us to design and deliver pragmatic, risk-sensitive solutions in response to these challenges.

Protiviti has a strong reputation in risk management, security and privacy, as well as IT governance and analytics, and a loyal base of clients based on the breadth of our skills. We also seek to overlay a deep understanding of industry-specific concerns in our solution development. Our dedication to develop pragmatic solutions to address the real, underlying client needs helps us produce value for our clients. This combination has made us a trusted partner to our clients.

We seek to help organizations assess the effectiveness of current technology risk models and assist with the design and implementation of a more effective approach.

We can provide the following services:

- IT strategy and governance
- Enterprise architecture
- Risk and compliance
- Security and privacy
- Service assurance
- Operations improvement
- Data management
- Technology
ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

CONTACTS

Ed Page
Managing Director
+1.312.476.6093
ed.page@protiviti.com

Andrew Struthers-Kennedy
Managing Director
+1.410.454.6879
andrew.struthers-kennedy@protiviti.com

Michael Thor
Managing Director
+1.317.510.4685
michael.thor@protiviti.com

Carl Hatfield
Managing Director
+1.617.330.4813
carl.hatfield@protiviti.com

Jonathan Wyatt
Managing Director
+44.20.7024.7522
jonathan.wyatt@protiviti.co.uk

Jeff Weber
Managing Director
+1.412.402.1712
jeffrey.weber@protiviti.com

Barbi Goldstein
Managing Director
+1.212.603.8351
barbi.goldstein@protiviti.com