Technology Risk Management 2.0

A New Approach
The conclusions of a technology risk study, which explored whether technology risk functions have the right strategy, skills and operating models in place to enable the organization to understand, assess and manage existing and emerging risk, have reinforced Protiviti’s long-held view that technology risk is failing to keep up with the rapid pace of technological change.¹ This is particularly true for organizations that are struggling with the notion that they are becoming a “technology company.”

¹ The results of the technology risk study are set out in the Protiviti white paper, Technology Risk: The Need for Change: www.protiviti.com.
The Protiviti Technology Risk Model 2.0 framework and methodology is designed to enable better integration of the various groups performing technology risk activities. This can include activities performed by individuals in the technology risk function, the IT department, the operational risk team, information risk, vendor management, information security and cybersecurity teams, to name a few. Implementing a more integrated approach creates a more effective and efficient IT and technology risk function that focuses on the customer and user experience rather than on the downside risks impacting the organization.

* These are only examples of high-level categories.
The Protiviti Technology Risk Model 2.0 framework helps firms to visualize an ideal end state and provide a tried-and-tested methodology to realize that vision. The effective implementation of this framework drives a wholesale transformation in the organization. Success relies on firms having sponsorship at the appropriate level and an effective change management process in place.

This approach is not to be confused with the well-versed arguments for firms to implement a common governance, risk and compliance (GRC) platform. Although a common GRC platform is useful, since it can streamline and bring risk reports and data together, the focus in this approach is on how firms can fundamentally re-engineer and redesign the way the various functions that manage and/or report on technology risk work together to integrate methodologies, as well as languages and culture.

Many firms have struggled to fully implement complex GRC projects in the past, which is often caused by the tendency for such projects to be technology-led. People and functions need to align first in terms of their methodologies, processes and cultures before an integrated approach can be underpinned by a core technology platform and supporting tools.

First, organizations need to decide what they want to integrate and how. The Protiviti Technology Risk Model 2.0 seeks to deduce how different functions work together and how their varied standards, taxonomies and agendas can be brought together to align with the goals of the business. Once firms have determined common processes, common languages and common approaches, only then can they be combined in a common system. Starting with a common system and trying to superimpose a different approach is rarely successful. By approaching this from the other direction, once the risk management functions are aligned, the technology should fall into place more naturally.

**Integrating Top Down and Bottom Up Approaches**

Existing approaches adopted by almost all organizations for technology risk are conducted from the bottom up and are focused on the risk assessments of the technology components. Top-down risk analysis is typically only performed to inform the scope of the assessments. The analysis then quickly moves to a bottom-up assessment of the technology components — the systems and processes — supporting applications identified as high risk to highlight potential issues. These activities are not
informed by main business risks, identified by senior executives, which could arise from the organization’s dependence on technology. Furthermore, no consideration is given to risk appetite. This lack of focus on the customer (internal or external) and the events the risk function is seeking to prevent when performing technology risk assessments, results in technology-centric conclusions that provide limited insights for the business.

Integrating a bottom-up approach with a top-down approach, one focused on customer experience, threat analysis and an assessment of risk appetite, is a critical step that many organizations struggle with or miss completely. This must be addressed if technology risk functions are to evolve to the next level and provide real business insights for key stakeholders.
Integrating Top Down and Bottom Up

### Top-down risk assessment

<table>
<thead>
<tr>
<th>CUSTOMER (INTERNAL/EXTERNAL) SERVICES MAPPED:</th>
<th>CRITICAL RISK SCENARIOS ASSESSED:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain insurance quote online</td>
<td>Impact</td>
</tr>
<tr>
<td>Process payment online</td>
<td>C</td>
</tr>
<tr>
<td>Process mortgage application online</td>
<td></td>
</tr>
<tr>
<td>Complete an ATM withdrawal</td>
<td></td>
</tr>
</tbody>
</table>

#### # Risk Scenarios Identified (Primary Threat Actors*)

<table>
<thead>
<tr>
<th>#</th>
<th>Risk Scenarios Identified (Primary Threat Actors*)</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Failure to complete a significant number of customer payments in accordance with agreed processing deadlines (OI, SA, UA, WM)</td>
<td>√</td>
</tr>
<tr>
<td>2</td>
<td>Payments are not accurately booked (OI, SA)</td>
<td>√</td>
</tr>
</tbody>
</table>

#### PRIMARY THREATS SOURCE:

- **Internal Threats:** OI: Opportunistic Insider; WM: Well-Meaning Insider;
- **External Threats:** UA: Unsophisticated Attacker; SA: Sophisticated Attacker

### Bottom-up risk and controls review

- **Process payment online**
- **Entity Type**
- **Relevant Entities** (mapping of entities to Customer Services)
  - Technology: Mainframe Environment
  - Technology: Web Services Environment
  - Third Party: Hosting Provider A

- **Risks and Controls** of relevant entities assessed against standard frameworks (such as CSEG, NIST)

**Consolidated view of controls in Transparency Report combined with analysis of threats used to assess likelihood**
All firms should conduct a top-down risk assessment that considers the business impact of those risks dependence on technology can present. This assessment needs to focus on the areas deemed of most importance to the organization, which are usually, but not always, those that impact the customer experience. Ideally, the assessment needs to be conducted from a board-level perspective to identify areas of critical importance.

When identifying risks, the following categories should be considered: confidentiality, integrity, availability, safety and regulatory. For example, the loss of any confidential data or information can be a major issue for a bank, while systems integrity and availability are critical to providing services to customers. Technology failures can represent genuine physical health and safety issues, if not life and death risks. The failure of an autonomous car, control system at an industrial plant or labeling system at a pharmaceutical company by way of example, can have catastrophic consequences.

Not all risks and associated business outcomes are created equally. Once identified, risks need to be ranked by taking into account the business impact. This top-down risk assessment is a critical step, which is generally not well performed by many risk functions today, as revealed by the Protiviti Technology Risk study.
### Protiviti Threat Assessment Model

<table>
<thead>
<tr>
<th>Threat actors category</th>
<th>They typically:</th>
<th>They threaten the security of company information when they:</th>
<th>Illustrative mitigation solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Well-meaning insider (WM)</td>
<td>1. Do not intend any harm 2. Are just trying to do their job</td>
<td>1. Are not aware that their actions can cause harm 2. Are forced to do things in an insecure manner because they are not aware of any secure alternatives 3. Believe they must do things in an insecure manner out of urgency</td>
<td>• Awareness training  • Data loss prevention  • Document management  • Data centric security solutions  • Anti-virus/malware protection  • Web access restrictions</td>
</tr>
<tr>
<td>Opportunistic insider (OI)</td>
<td>1. Are legitimate users but have high levels of access and/or have been given more access than they require 2. Would abuse access but not usually go as far as bypassing controls to gain access</td>
<td>1. Use their access in an unauthorised manner 2. Can ethically justify their misuse</td>
<td>• Identity and access management  • Logical access management  • Privileged access management  • User behavioral analytics</td>
</tr>
<tr>
<td>Unsophisticated attacker (UA)</td>
<td>1. May or may not have legitimate access to information 2. Choose targets opportunistically, often based on easy-to-find weaknesses 3. Have a relatively low motivation to succeed with attacks 4. Utilise simple, well-known attack methods 5. Are very noisy in their attacks</td>
<td>1. Use attack methods that don’t ultimately succeed but are otherwise harmful to our computing systems 2. Use attack methods that have been released publicly before vendors have had a chance to provide fixes 3. Are not detected early on, despite setting off alarms</td>
<td>• Vulnerability  • Patching  • Anti-virus/malware protection  • IDS/IPS  • SIEM/SOC  • Privileged access management  • End-user training (managing social engineering threat)  • Disaster recovery/crisis management</td>
</tr>
<tr>
<td>Sophisticated attacker (SA)</td>
<td>1. Have a specific interest in damaging their targets or see them as economically profitable 2. Are highly motivated to succeed with their attacks 3. Have access to the technical and financial resources they need to be successful 4. Are very stealthy in their attacks</td>
<td>1. Apply their resources to any specific target 2. Have a competing economic interest 3. Are state-supported</td>
<td>• Continuous people screening  • Threat intelligence  • Advanced user behavioral analytics  • Advanced privileged access controls (with enhanced segregation of duties rules)  • Enhanced disaster recovery/crisis management  • High security environments</td>
</tr>
</tbody>
</table>
Once high impact areas have been identified, firms should conduct a threat assessment, which can be risk ranked, to determine where the greatest threats are likely to emerge.

The Protiviti Technology Risk Model 2.0 divides threats, at least those resulting from targeted attacks, into internal and external categories. External threats primarily from hackers are classed as unsophisticated attackers (UA), while, at the far end of the scale are organized crime networks or terrorist groups, as well as state actors, or foreign governments, are categorized as sophisticated attackers (SA). Internal threats are divided into opportunistic insiders (OI) and well-meaning insiders (WM).

The types of controls and the organization’s view of the effectiveness of those controls may vary significantly depending on the source and sophistication of the attacker. Identifying the threat actors associated with each risk allows the risk function to conduct a more accurate assessment of the likelihood of a successful attack — a key component of the risk assessment process. This exercise combines an analysis of the perceived threat levels with an assessment of the effectiveness of the controls.

Firms need to ask some fundamental questions when considering threat levels: Given a particular business risk, where does the firm believe the threat is coming from? What are the motivations for the attack? What

### Threat Assessment

*Threat Assessment is performed using Protiviti’s Threat Assessment model, which is explained on the previous page.*
tools do the attackers have at their disposal? The required controls vary significantly depending on the perceived source of the threat. The motivation and risk appetite of the perceived attacker also has a significant impact on the threat assessment. Firms should be much more concerned about control weaknesses when they are aligned with the perceived source of a credible threat.

When performing a threat analysis, the risk function needs to be aware of the effectiveness of the control environment. The assessment should consider technology controls as well as business process controls. For example, if an attacker attempts to exploit weaknesses in change management and/or privileged access controls to create and process fictitious payments, the threat is significantly reduced.
if it is anticipated that the attack would be detected and blocked by monitoring activities performed in the middle and/or the back office. This is where a GRC platform can be helpful as it provides easy-to-understand reports that give a consolidated view of controls and/or control issues impacting the relevant technology entities that are mapped to the risk being assessed. This process is referred to in the Protiviti methodology as “transparency reporting”.

Where possible, platform dashboards should emphasize the controls that are most relevant, given the perceived source of the threat, to enable a quick conclusion to any likelihood of the threat occurring.

Once the organization has succeeded in identifying the risks that could materially damage the firm by combining the assessment of potential business impact with the perceived likelihood of occurrence, it can then start to consider its risk appetite and whether the current assessment of residual risk falls outside of risk tolerance. For those risks assessed as outside tolerance, risk mitigation actions need to be defined.

Traditional technology risk approaches use the results of the bottom-up analysis to identify gaps in the control framework, which are all assumed to require remediation or risk acceptance. Many firms are finding prioritizing the required actions to be extremely difficult, as they are unable to determine the business impact and whether the gap is within risk tolerance. Using the approach set out above, firms can prioritize any required remediation identified through the risk assessment process based on the likelihood of such an incident and the severity of the impact, with the most critical and impactful risks being addressed first.

Regardless of the attention given to risk mapping and threat assessments, absolute resilience is an unrealistic goal. Incidents will occur from time to time. Risk mitigation efforts need to focus on those areas that matter most to the business. A key step in this process is to identify and understand the company’s “crown jewels” — those assets that are most critical to the business and have the lowest risk appetite. The risk function needs to understand where these assets are located assess the controls and put plans in place to respond to and minimize losses should the scenario arise.

The top-down risk assessment process provides a mechanism for understanding what the critical assets are and where they reside. And, as set out above, the association of the risk profile to those assets, is what drives risk mitigation priorities.

**Technology is Not a Silo**

In today’s organizations, technology is integral to almost all business processes. Most principal risk frameworks used by financial institutions present technology, and in many cases cybercrime, as discrete risk categories. While such risk categories are only used for reporting, adopting this approach can result in the risk assessment process focusing more on the technology than on business risks arising from the use of technology. Considered separately, it is extremely difficult to assess the business impact and/or to define risk appetite.

Separating out the technology risk team from the operational risk team gives the impression that the two risk disciplines can be considered separately, but such an approach encourages the broader operational risk team to ignore potential business process risks that relate to technology, assuming that these are assessed by the technology risk group. Technology risk teams tend to look at technology in a standardized way, and often do not consider risks that arise from the way that the system is being used or the nature and extent of business process controls provided to mitigate the risk. This can result in technology risk being misrepresented in risk reporting.
Integrating Vendor Risk Management

Threats posed by vendors and third-party contractors have been attracting regulatory attention, with financial services firms being required to perform vendor risk assessments. Information technology is no exception. IT is much more complex than it once was. While most businesses still manage and operate some in-house developed systems from their own data centers, the increasing adoption of cloud and integration with third-party solutions is driving greater dependence on vendors, increasing the importance of effective vendor management.

Even though firms’ reliance on technology is increasing, in reality they control far less of this than they ever have before. The combination of increased dependence and less direct control raises some concerns, and regulators are becoming more focused on this topic.

Risk Management Silos

Most organizations have adopted approaches to managing risks arising from contractual obligations, but their approaches are rarely coordinated or consistent. This includes failing to meet obligations to customers imposed on the company by regulators (contractual compliance), the risks presented by suppliers’ operating processes, managing and holding firms’ data (vendor risk management), and the risks arising from the technology firms use in-house (operational risk management). These varied approaches, if all are performed, are typically owned by different teams, using different systems, with relatively little information shared between them.
This lack of integration presents a number of discrete risks:

- The potential for significant misrepresentation of risk exposures in operational risk reporting, due to the under representation of the impact of vendor and/or contractual compliance risk in operational risk reports;
- The potential for significant duplication of effort when performing assessments, resulting in unnecessary cost and frustration as auditees are repeatedly asked the same questions;
- The lack of coordination of remedial actions taken, as different teams agree to different risk mitigation strategies in a non-coordinated way, puts a strain on those responsible for driving remediation efforts.

The Protiviti Technology Risk Model 2.0 proposes a much more integrated approach, with a common methodology for both operational risk management and vendor risk management. The same principles should be applied whether the technology is operated in-house or by a third party. This “integrated” approach to vendor risk is illustrated in the diagram below.

---

**Integrated Approach to Vendor Risk Management**

1. Third-party entity identified through operational risk process
2. Vendor risk team perform top-down risk assessment of vendor to identify key risks
3. Vendor provided access to its third-party entity record in GRC system to document controls
4. GRC platform automatically engages supplier periodically to submit evidence
5. Vendor risk team review controls submission and decide evidence requirements
6. If gaps are identified, remediation plan agreed with supplier

---

INTEGRATED TECHNOLOGY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE PLATFORM
Adopting this integrated approach to vendor risk presents numerous benefits, as compared with a more traditional approach:

1. Existing third parties that require inclusion in the vendor risk program are derived from the top-down assessment of potential risks to the business, rather than from an analysis of procurement spend (which can result in smaller, high-risk suppliers being missed).

2. The vendor risk team’s effort is focused on determining the main, specific risks the supplier/service provider presents to the business, rather than drawing on standard schedules (e.g., information security requirements) to prescribe the required controls.

3. Vendors are granted access to a system that provides details of the controls they have put in place within their organization to manage the risks on the company’s behalf. This approach allows vendors to manage their own businesses, but also provides transparency to the buyer of the service on how risks are managed. It also reinforces the vendors’ responsibilities.

4. The system engages with suppliers on a regular basis to reaffirm those controls are operating effectively. This reminds suppliers of their commitments and responsibilities, while providing increased assurances the controls are operating continuously.

5. A process is established to track and manage the closure of remediation plans agreed with vendors when risks are identified.

6. The approach is fully integrated with operational risk reporting (if the same process and/or systems are used). This ensures that third-party risks are fully considered in operational risk reporting, when threat assessments are performed.

Effectiveness of Management Reporting

One significant observation from the Protiviti Technology Study was how few organizations have been able to develop insightful reports. Reporting in general was found to lack impact. This stems from the fact that approaches adopted are typically from the bottom up. Businesses have lots of information about technology risks, but provide limited insight on business impact and whether the risk profile of the organization is increasing or decreasing and why.

Once the integrated approach has been implemented, firms can utilize tools such as The Protiviti Risk Index™ to provide executives with a complete view of risk, showing how risk is changing over time. Firms can aggregate their 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.

---

In Conclusion

This paper provides a high-level overview of some of the key components of Protiviti’s Technology Risk Model 2.0. This is a common methodology and approach that can be used to fully integrate all functions tasked with assessing and helping the organization to manage operational risks arising from the use of technology.

As highlighted in the whitepaper Technology Risk: The Need for Change, there is a strong case for transformation. Almost all participants in our study acknowledged that their current approach to technology risk management is not adequate.

The challenge for many firms will be deciding where to start and receiving buy-in from discrete operating units to work together to drive the required change. Chief risk officers will have a critical role to play in this process.

Agreeing upon a common approach to the top-down risk assessment — a process that is ineffective in most technology risk management activities — can be a good place to start.

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 into a single view of risk, new and changing risks are more easily identified and the firm can track if it is getting better as a result of certain mitigation efforts, for example.

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, however firms can populate the index with bottom-up, business-centric, technology risk metrics to experience real benefits in months, while also helping to engage senior management and board members.
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.

HOW CAN PROTIVITI HELP WITH TECHNOLOGY RISK?

Based on our research and industry participation, it is apparent that there is enormous pressure for financial services technology and IT leaders to become more nimble and adaptive, yet there is also 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 been helping clients to design and implement effective approaches to risk management. We have a strong reputation in risk management, security and privacy, 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
- Regulatory risk and compliance
- Security and privacy
- Service assurance
- Operations improvement
- Data management
- Risk technology
- Risk reporting (Protiviti Risk Index)
- Vendor management
- Technology risk management (Protiviti Risk 2.0 Model)
- Operational risk management

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