Top Technology Trends in Financial Services Organizations

Disruptive Technology Brings Risks and Opportunities for Financial Services Firms
# Table of Contents

- **Introduction** .................................................................................................................................................................................. 1
- **Transformation and Innovation (a.k.a. Digitization)** .................................................................................................................... 3
- **Security and Privacy** ............................................................................................................................................................................ 12
- **Risk and Compliance** .......................................................................................................................................................................... 18
- **Cost Pressure and the Case for Simplification and Legacy Modernization** .......................................................................................... 24
- **Final Thoughts** ...................................................................................................................................................................................... 36
- **About Protiviti** ...................................................................................................................................................................................... 39
- **How Can Protiviti Help?** ......................................................................................................................................................................... 39
- **Contacts** ............................................................................................................................................................................................ 40
Introduction

Disruptive technology, including all of its competitive, regulatory, security and operational implications, is top of mind for financial services executives. But in addition to having their eyes on the future, financial services industry technology executives must also address their past, as they deal with the complexity of aging legacy systems and a dwindling pool of technicians who labor to keep outdated systems running long enough to implement more agile technology that will enable their institutions to face the future with confidence.

These views are clearly demonstrated in the responses to Protiviti’s 2016 Technology Trends Survey. The survey covers a broad spectrum of industries, but this report focuses on responses from C-suite executives and other technology leaders in the financial services industry (FSI). These responses, when compared with the results from other industries, yield a clear picture of financial services IT priorities, which have been organized into the following topics in this paper:

- Transformation and Innovation (a.k.a. Digitization)
- Security and Privacy
- Risk and Compliance
- Cost Pressures and the Case for Simplification and Legacy Modernization

In addition to the results of the trends survey, Protiviti’s experienced subject-matter experts share their unique perspectives on each of these topics, while mini-case studies presented throughout the paper illustrate how some organizations are approaching these challenges.

Within these areas of focus, several consistent IT concerns emerge, including:

- Responding to fast-evolving customer service expectations and the competitive threat of mobile and web-based financial technology (fintech) firms.
- Balancing the need for 24/7/365 system availability with need to quickly design and implement new products and services.
- Protecting data and ensuring privacy.
- Simplifying and consolidating outdated and heavily modified legacy systems, while increasing adoption of cloud-based infrastructure.
- Responding to ever-changing regulatory compliance requirements.
Methodology

Close to 400 C-suite executives (n = 396) in IT organizations, along with other technology leaders, participated in our study, which was conducted in Q2 and Q3 2016. In a change from prior years of our annual IT survey, we limited our response group to IT leaders at the C-suite or director level in order to obtain their strategic insights on emerging IT trends and views on areas including IT investments and budget allocation. We are grateful for the time invested in our study by these IT leaders.

Our participants answered a series of questions in the following categories:\(^1\)

<table>
<thead>
<tr>
<th>Current benchmarks and emerging trends</th>
<th>IT priorities for the coming year</th>
</tr>
</thead>
<tbody>
<tr>
<td>• IT Transformation</td>
<td>• Managing Security and Privacy</td>
</tr>
<tr>
<td>• Budgets and Organizational Structure</td>
<td>• General IT Technical Standards and Knowledge</td>
</tr>
<tr>
<td>• Outsourcing and Offshoring</td>
<td>• Defining IT Governance and Strategy</td>
</tr>
<tr>
<td>• Cloud Computing and Adoption</td>
<td>• Management and Use of Data Assets</td>
</tr>
<tr>
<td>• Digitization</td>
<td>• Managing Application Development and ERP Systems</td>
</tr>
<tr>
<td>• Big Data</td>
<td>• Managing IT Infrastructure</td>
</tr>
<tr>
<td>• Agile Processes</td>
<td>• Ensuring Continuity</td>
</tr>
</tbody>
</table>

\(^1\) For each of these categories, respondents were asked to rate, on a scale of 1 to 10, the level of priority for them and their organizations to improve in different issues and capabilities. A “10” rating indicates the issue is a high priority, while a “1” indicates the issue is a low priority. We have classified each issue and capability with an index of 6.0 or higher as a “Significant Priority” for IT functions. Those with an index of 4.5 through 5.9 are classified as a “Moderate Priority,” and those with an index of 4.4 or lower are classified as a “Low Priority.” (Of note, none of the more than 100 IT issues and capabilities addressed in our survey is rated as “Low Priority.”)
Transformation and Innovation (a.k.a. Digitization)

Author Malcolm Gladwell, in his best-selling book on innovation, *David and Goliath: Underdogs, Misfits and the Art of Battling Giants*, posits that in history’s most famous mismatch, the advantage was always with the agile and innovative David over his larger, but less nimble, opponent.

So it is today in the financial services industry, where smaller and more agile competitors are putting pressure on the larger, more established institutions to continuously innovate.

Like Goliath of old, traditional financial service organizations are finding that the size that once worked to their advantage has become a liability as they add up the billions of dollars required to modernize decades-old core processing systems.

Digital transformation is much more than a buzzword. Real change is happening in the financial services industry thanks to new technologies that have evolved rapidly in response to consumer expectations. New and emerging technologies — social, mobile, analytic, cloud and distributed consensus ledgers — offer great promise in terms of innovation, agility, cost-savings, security and resiliency. Mobile payment services and mobile wallets have given consumers a convenient new way to purchase goods and services. While still in its infancy, distributed ledger, or blockchain, technology is being touted as the future of transaction processing and settlement. Crowdfunding has emerged as a popular source of equity capital. In many respects, financial technology (fintech) firms are challenging the very business models that underpin traditional financial services.

*Traditional firms need to prepare for these “Uber moments” by adopting and integrating emerging technology and embracing new ways of doing business.*

— Ed Page, Managing Director
Anthony Jenkins, the ex-chief executive officer of Barclays, in a November 2015 speech, commented on how financial services are approaching an “Uber moment” — when disruptive technologies dramatically improve the customer experience or create a new experience that didn’t exist. Jenkins predicted significant disruption in the industry by fintech companies that will place massive pressure on incumbent banks, which will struggle to implement new technology at the same pace as their fintech rivals, making it difficult to deliver returns shareholders demand.

“Traditional firms need to prepare for these ‘Uber moments’ by adopting and integrating emerging technology and embracing new ways of doing business,” says Managing Director Ed Page, the company’s Financial Services Industry Technology Consulting practice leader for Protiviti. “Firms also need to figure out how to compete with and/or partner with fintech firms, as well as how to address new business models enabled by new technologies, including open APIs.”

But there are challenges and risks associated with integrating these new technologies and more agile processes into already complex infrastructures that demand “always on” availability, uncompromising regulatory compliance, and high degrees of security and privacy protection.

Fintech start-up companies, unfettered by the limitations of aging legacy “core” technology systems and expensive brick-and-mortar branch networks, innovate faster than older and more heavily regulated organizations. The problem for traditional firms is that they are seeking to adopt new technology by layering it onto existing legacy systems, most of which are unfit for this purpose.

“Many of the clients we talk to are on antiquated systems,” says Barrett Shrader, a director in Protiviti’s Financial Services Industry Technology Consulting practice. “We completed an engagement last year working on a mainframe system that was put in place before the moon landing.”

And such core systems are only part of the problem. “A lot of these older mainframes are tied to ancillary systems that rely on the core system for processing,” Shrader says. “When you change the core, you also need to account for the impact on all of the surrounding applications, which can add to both cost and complexity.”

Outdated IT infrastructure has not only made it difficult for traditional financial institutions to bring new products to market in a timely fashion, but also left them vulnerable to data breaches and a dwindling number of resources skilled at supporting the legacy infrastructure. Financial services executives, under pressure from regulators, are increasingly concerned about these risks. Survey results show that 44 percent are considering core modernization, compared with less than a third a year ago. Most (70 percent) cited risk mitigation — replacing aging technology and/or workforce — as the primary catalyst for change.

This intersection of disruptive change and the need for core modernization poses an existential threat for both large and small financial institutions. As a result, financial executives and regulators alike have embarked on a technological transformation journey that extends well beyond core modernization. Including those organizations planning to replace or upgrade their core systems, fully 70 percent of FSI survey respondents indicated that their institutions were going through some form of IT transformation, substantially higher than the 54 percent for survey respondents across all industries.

Key drivers of these broader transformative changes include operational improvement, new functionality and regulatory compliance.

---

Which of the following would you consider to be a driver of your organization’s IT transformation efforts?

<table>
<thead>
<tr>
<th>Driver</th>
<th>All Respondents</th>
<th>Financial Services Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational improvement</td>
<td>41%</td>
<td>54%</td>
</tr>
<tr>
<td>New functionality</td>
<td>53%</td>
<td>46%</td>
</tr>
<tr>
<td>Regulatory/compliance</td>
<td>30%</td>
<td>46%</td>
</tr>
<tr>
<td>Cost optimization</td>
<td>43%</td>
<td>43%</td>
</tr>
<tr>
<td>Business/IT alignment</td>
<td>38%</td>
<td>39%</td>
</tr>
<tr>
<td>Business transformation</td>
<td>30%</td>
<td>32%</td>
</tr>
<tr>
<td>Adoption of emerging technology</td>
<td>40%</td>
<td>29%</td>
</tr>
<tr>
<td>Time to market/IT agility</td>
<td>32%</td>
<td>25%</td>
</tr>
<tr>
<td>Service assurance</td>
<td>24%</td>
<td>25%</td>
</tr>
<tr>
<td>Outsourcing/third-party hosting</td>
<td>15%</td>
<td>14%</td>
</tr>
<tr>
<td>Innovation enablement</td>
<td>32%</td>
<td>11%</td>
</tr>
<tr>
<td>Merger &amp; acquisition activity</td>
<td>17%</td>
<td>11%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Building a Better Infrastructure

A typical large financial institution may have more than a thousand applications running within the enterprise. And while core systems may be supported by long-established vendors, it is not unusual to find any number of undocumented customizations, patches and work-arounds created by long-gone IT programmers or by defunct third parties.

Over the years, these customizations and add-ons proliferated with every new product offering and process change, to the point that it might take hundreds of IT staff just to manage user authentication and access control. Small wonder that efforts to add even more technology, more reporting and more functionality might be met with some resistance from an already overburdened IT staff.
Which of the following would you consider to be a barrier to your organization’s IT transformation efforts?

<table>
<thead>
<tr>
<th></th>
<th>All Respondents</th>
<th>Financial Services Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy processes</td>
<td>36%</td>
<td>54%</td>
</tr>
<tr>
<td>Cost/budget limitations</td>
<td>36%</td>
<td>39%</td>
</tr>
<tr>
<td>Legacy infrastructure</td>
<td>43%</td>
<td>32%</td>
</tr>
<tr>
<td>IT skills gap with desired state</td>
<td>37%</td>
<td>32%</td>
</tr>
<tr>
<td>IT collaboration with the business</td>
<td>30%</td>
<td>29%</td>
</tr>
<tr>
<td>IT culture not agile to change</td>
<td>39%</td>
<td>21%</td>
</tr>
<tr>
<td>Vendor capabilities</td>
<td>20%</td>
<td>21%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
<td>4%</td>
</tr>
</tbody>
</table>

But change they must. Protiviti’s 2015 analysis of consumer banking and payment behaviors underlined the increasing demand for mobile payments and omni-channel solutions to improve the customer experience. Some 51 percent of survey respondents said that they used the website only for their banking needs, while 33 percent used mobile devices only for their banking rather than branches.³

Survey responses prove the FSI establishment is committed to change, and Shrader says he has seen an increased acceptance of the idea that transformation means developing more efficient and agile processes, not just automating old ones.

Generally speaking, modernization efforts are undertaken to achieve one or more of the following objectives:⁴

- Increase operating agility and efficiency
- Add new capabilities
- Reduce costs
- Improve customer service
- Mitigate the risk of maintaining aging infrastructure

Legacy modernization does not necessarily imply a full-scale, “big bang” replacement. There are several approaches to legacy modernization, ranging from efforts to preserve the existing core to a complete overhaul and replacement with modern systems. (Each of these are reviewed in greater detail on page 34.) Given the 24/7/365 nature of financial service accessibility, a common obstacle encountered at this point is the IT corollary to the industry’s well-known “too big to fail” argument — the idea that a reliable core system, even an outdated one, is indispensible, and therefore, effectively irreplaceable. We call this “too big to fix.”

As daunting as it may seem, the issue can and must be addressed through increased innovation and more modular thinking. There is evidence that firms are beginning to develop their strategies and supporting implementation plans. These are typically multi-year journeys, making effective program, change and risk management essential cornerstones to success.

### Responsible Innovation

Even regulators, which are often viewed as impediments to change, acknowledge the need for transformation — with a few caveats. In August 2015, U.S. Comptroller of the Currency Thomas J. Curry launched an initiative to identify technology trends and innovations affecting federally insured financial institutions and develop a framework to simultaneously facilitate innovation and understand and mitigate the risks of technology-enabled processes, products and services. Curry calls this “responsible innovation.” The operative word being “responsible.”

The OCC defines responsible innovation as “The use of new or improved financial products, services, and processes to meet the evolving needs of consumers, businesses, and communities in a manner that is consistent with sound risk management and aligned with the bank’s overall business strategy.”

An OCC paper published in March 2016 speaks to innovation and the regulator’s acknowledgement that financial services must transform to survive and thrive.5

Based on industry feedback from the March white paper, the OCC introduced a new framework to support responsible innovation in a new document, Recommendations and Decisions for Implementing a Responsible Innovation Framework, published on October 26.6

The OCC’s Innovation Framework Development Team, set up in June 2016, has called for the OCC to establish a stand-alone Office of Innovation to implement its proposed innovation framework, and also recommends action in the following five areas that form the core components of the framework:

1. Outreach and technical assistance
2. Awareness and training
3. Coordination and facilitation
4. Research
5. Interagency collaboration

The OCC is proposing providing technical assistance to banks and nonbanks, which would involve designing “rules of the road” material for nonbanks. The paper doesn’t expand on what these rules are, but it appears to indicate that the regulator is considering issuing guidelines for financial technology firms and its partners.

---


Other regulatory bodies and legislators are proposing their own guidance about how to encourage “responsible” innovation, and the recent U.S. presidential elections create additional uncertainty in this space. “We are encouraged by this dialog,” says Page, “but the ultimate outcomes are unknown, so this will be a critical area to monitor in the coming months.”

Barriers to Innovation

In a recent global survey conducted by North Carolina State University’s ERM Initiative and Protiviti, board members and C-suite executives were asked to assess the most significant risks to their organizations in the coming year. For financial services industry executives, innovation didn’t rank among the top five concerns.⁷ We believe that this can be attributed to the anesthetizing effect of day-to-day concerns that demand immediate attention. This common barrier to innovation, though perfectly understandable, is dangerous.

“Financial institutions are so preoccupied with the problems of today — cybersecurity, proving resilience and keeping the lights on — that they think the problems of tomorrow can wait,” says Managing Director Jonathan Wyatt, Technology Consulting practice leader in the UK. “Tomorrow will be here before they know it.”

FSI responses to Protiviti’s Technology Trends Survey showed that specific barriers vary, depending on which particular type of innovation is being considered, but common themes included:

- Cost
- Competing priorities
- Regulatory compliance
- Security and privacy concerns
- Implementation risk

⁷ Executive Perspectives on Top Risks for 2017 — Summary of FSI Results; Protiviti and North Carolina State University’s ERM Initiative, Protiviti: www.protiviti.com/toprisks.
### Which of the following have been barriers to your organization's efforts with regard to digitization?

<table>
<thead>
<tr>
<th></th>
<th>All Respondents</th>
<th>Financial Services Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>52%</td>
<td>44%</td>
</tr>
<tr>
<td>Time — disruption to other priorities</td>
<td>43%</td>
<td>44%</td>
</tr>
<tr>
<td>Security and privacy risks</td>
<td>33%</td>
<td>40%</td>
</tr>
<tr>
<td>Lack of executive buy-in</td>
<td>24%</td>
<td>32%</td>
</tr>
<tr>
<td>Regulation/compliance</td>
<td>23%</td>
<td>28%</td>
</tr>
<tr>
<td>Vendor product/service challenges</td>
<td>18%</td>
<td>20%</td>
</tr>
<tr>
<td>Implementation risk</td>
<td>23%</td>
<td>16%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
<td>8%</td>
</tr>
</tbody>
</table>

### Which of the following have been barriers to your organization's efforts with regard to the adoption of agile processes?

<table>
<thead>
<tr>
<th></th>
<th>All Respondents</th>
<th>Financial Services Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>33%</td>
<td>44%</td>
</tr>
<tr>
<td>Regulation/compliance</td>
<td>30%</td>
<td>38%</td>
</tr>
<tr>
<td>Implementation risk</td>
<td>27%</td>
<td>31%</td>
</tr>
<tr>
<td>Time — disruption to other priorities</td>
<td>40%</td>
<td>19%</td>
</tr>
<tr>
<td>Lack of executive buy-in</td>
<td>30%</td>
<td>19%</td>
</tr>
<tr>
<td>Security and privacy risks</td>
<td>26%</td>
<td>19%</td>
</tr>
<tr>
<td>Vendor product/service challenges</td>
<td>13%</td>
<td>13%</td>
</tr>
<tr>
<td>Other</td>
<td>6%</td>
<td>13%</td>
</tr>
</tbody>
</table>
What estimated percentage of your current IT budget is allocated to each of the following areas?

<table>
<thead>
<tr>
<th>Area</th>
<th>All Respondents</th>
<th>Financial Services Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT operations (Run the business)</td>
<td>33.1</td>
<td>27.5</td>
</tr>
<tr>
<td>Security (Protect the business)</td>
<td>15.8</td>
<td>22.9</td>
</tr>
<tr>
<td>Maintenance (Maintain the business)</td>
<td>21.5</td>
<td>20.5</td>
</tr>
<tr>
<td>Discretionary enhancements (Improve the business)</td>
<td>14.1</td>
<td>11.9</td>
</tr>
<tr>
<td>Innovation (Transform the business)</td>
<td>12.5</td>
<td>12.1</td>
</tr>
<tr>
<td>Compliance</td>
<td>10.2</td>
<td>11.8</td>
</tr>
</tbody>
</table>

Cost is a major factor, with IT budgets generally only allocating 12 percent for innovation, according to our survey.

Wyatt maintains that the most significant barrier, in many cases, is one of perception.

“There is a genuine understanding and acknowledgment that there is a digital revolution going on, and that it is going to have huge impact on financial services,” Wyatt says. “But there is a major challenge culturally in how they react and respond to that.”

Rightly or wrongly, Wyatt adds that financial services organizations tend to operate in perpetual fear of offending their regulators. “Often, when we go into a financial services firm and start asking about various policies, frameworks and standards, there is a mind-set that these are necessary, because a regulator insists they are necessary, which makes it extremely hard to experiment,” he says. “There is a perception that we have to convince the regulators we should be allowed to innovate, when in fact it is the policies, and not the regulations themselves, that are the problem.”

This is a common reaction. People respond to a regulation by making a policy. The policy may be prohibitive, whereas the regulation itself allows for more flexibility, but people are trained to follow policy and often do not really understand the regulation at all. Over time, the accumulation of misunderstandings, rigidity and complexity causes people to get locked into policies that don’t work very well in a rapidly changing world, a position many financial institutions find themselves in today.
Integrating a bottom-up approach with a top-down perspective is essential to fostering a culture of innovation. Whereas a bottom-up assessment might focus on confidentiality, integrity, availability, safety and regulatory compliance, a top-down analysis might look for strategic risks such as excessive maintenance costs, process and decision-making friction, degraded business agility, and the need for renewal.

Organizations that have reached this level of maturity in risk analysis have generally come to the conclusion that “responsible innovation,” as defined by the OCC earlier in this paper, requires a new hybrid IT model, combining traditional systems with more experimental and agile applications and infrastructure, often deployed in the cloud. Bimodal IT is becoming the typical pattern for FSI innovators.

Enabling Experimentation

From mobile payments and instant credit approvals to real-time digital settlement via distributed consensus ledgers, financial institutions are demanding more and faster technology capabilities. This demand for new products and services, and the attendant need to protect customer data in an increasingly diverse and porous user environment, poses a strategic risk for financial institutions approaching an existential threat.

And yet, for the most part, many financial institutions still view technology risk from a siloed, bottom-up perspective, focusing on systems and processes to the exclusion of customer experience. This lack of a holistic risk-based focus can result in technology-centric conclusions of limited value to the business or customer.

Bimodal Strategy Busts “Too Big to Fix” Myth

A large global financial services company, on its way to digital transformation, found its path blocked with legacy technology challenges. The main hurdle was a core system running on decades-old technology, increasingly difficult to maintain, and incompatible with the kinds of large-scale data mining, real-time processing, cloud computing and mobile applications required by the competitive landscape.

This presented a dilemma for the financial institution. On the one hand, there was the risk of technical obsolescence, lost revenue, and competitive decline, on the other, the risk of service interruption, lost data, delays and reputation damage often associated with large-scale technology projects. The system, in its current state, had served the company well. The business relied on the system 24/7/365, and IT executives couldn’t help but feel as if they were trying to replace the engine on a long-haul truck barreling down the highway with a full load and a firm deadline. Despite its limitations, there was a very real concern that the current system was indispensable to the point of being “too big to fix.”

IT executives turned to Protiviti. Having worked through similar dilemmas for financial service organizations around the world, Protiviti’s FSI IT subject matter experts mapped current operations to identify gaps and hurdles, and worked with stakeholders to develop a detailed road map to the desired future state.

Instead of replacing everything at once, the company will continue to service clients on the old core system as it implements and grows its new digital platform.

This bimodal IT transformation strategy provided the company with a way forward without having to go “all in” on a new system, allowing management to face the future with confidence.

---

8 The term “bimodal IT” was coined by Gartner in 2014 to refer to the use of two divergent software development lifecycle methods — waterfall and agile.

Financial institutions are bombarded by criminal attacks seeking to steal and profit from personal information. And because failure of security and privacy controls can have dire consequences for the institution and for consumers, security understandably ranks as the second largest expense category — 23 percent versus 16 percent for all respondents — after basic operating expenses for financial institutions participating in this year’s IT Technology Trends Survey.

 Omni-channel access capabilities, including mobile and cloud, create new vulnerabilities that make it even harder for the IT and security functions to stay ahead of the threat curve.

 Although the IT function is seeking to innovate and adopt new practices, it and the security function are struggling to understand and address risks and stay current in a growing and constantly changing threat landscape. In such a situation, it is only reasonable that both functions may balk at taking on new responsibilities. Little wonder that nearly two-thirds (64 percent) of FSI respondents listed security and privacy as a barrier to cloud adoption — well above the overall survey average of 48 percent — and 40 percent cited them as a barrier to digitization in general.

The financial services world is both complex and dynamic, and that causes a lot of headaches for data security personnel. There are a lot of attack vectors, and the IT environment is constantly shifting.

— Michael Walter, Managing Director
Which of the following have been barriers to your organization’s efforts with regard to cloud adoption?

<table>
<thead>
<tr>
<th>Barriers</th>
<th>All Respondents</th>
<th>Financial Services Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and privacy risks</td>
<td>48%</td>
<td>64%</td>
</tr>
<tr>
<td>Cost</td>
<td>48%</td>
<td>52%</td>
</tr>
<tr>
<td>Regulation/compliance</td>
<td>25%</td>
<td>44%</td>
</tr>
<tr>
<td>Time — disruption to other priorities</td>
<td>38%</td>
<td>32%</td>
</tr>
<tr>
<td>Implementation risk</td>
<td>24%</td>
<td>28%</td>
</tr>
<tr>
<td>Vendor product/service challenges</td>
<td>18%</td>
<td>16%</td>
</tr>
<tr>
<td>Lack of executive buy-in</td>
<td>20%</td>
<td>8%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
<td>—</td>
</tr>
</tbody>
</table>

Which of the following have been barriers to your organization’s efforts with regard to digitization?

<table>
<thead>
<tr>
<th>Barriers</th>
<th>All Respondents</th>
<th>Financial Services Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>52%</td>
<td>44%</td>
</tr>
<tr>
<td>Time — disruption to other priorities</td>
<td>43%</td>
<td>44%</td>
</tr>
<tr>
<td>Security and privacy risks</td>
<td>33%</td>
<td>40%</td>
</tr>
<tr>
<td>Lack of executive buy-in</td>
<td>24%</td>
<td>32%</td>
</tr>
<tr>
<td>Regulation/compliance</td>
<td>23%</td>
<td>28%</td>
</tr>
<tr>
<td>Vendor product/service challenges</td>
<td>18%</td>
<td>20%</td>
</tr>
<tr>
<td>Implementation risk</td>
<td>23%</td>
<td>16%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
<td>8%</td>
</tr>
</tbody>
</table>
The Changing Risk Landscape

Data breaches are increasing at the same time that customers are demanding a more fluid and accommodating customer experience. Consequently, financial services firms are under tremendous pressure to be more vigilant in protecting personal data and become more accommodating in providing customers with 24/7/365 access to their money and credit.

There was a time when financial services firms could take some comfort in the fact that sensitive financial information was delivered through infrastructure owned and controlled by the firms themselves. In the mobile world, there are more variables: the devices are owned by the customer; there are dozens of variations of smart phones, with varying operating systems; an increasing percentage of banking transactions are being outsourced to third-party vendors; and, of course, there are the financial technology, or fintech, companies.

“The financial services world is both complex and dynamic, and that causes a lot of headaches for data security personnel,” says Michael Walter, managing director in Protiviti’s Cybersecurity and Privacy Practice. “There are a lot of attack vectors, and the IT environment is constantly shifting.”

Many financial service organizations are beginning to recognize this challenge and are escalating data security and privacy to an enterprise–level concern. Those companies are moving information security out from under the control of the chief information officer (CIO) and placing it under the aegis of the chief executive officer (CEO), chief operating officer (COO) or chief risk officer (CRO) in order to better align with strategic goals and objectives.

A majority of respondents (65 percent) confirmed that they have a chief information security officer (CISO), but the survey results also highlight the fact that the importance of the function has been elevated since the CISO now reports outside of the IT function to other parts of the organization. While the most common reporting structure (42 percent) still has the CISO reporting to the CIO, a significant number (27 percent) report to the COO, 15 percent answer to the CRO and another 12 percent report directly to the CEO.

Generally speaking, however, financial institutions have a long way to go when it comes to understanding and managing information security risk.

“A lot of financial clients are asking us about reporting security metrics to the board, but I don’t see much maturity there,” Walter says. “While financial services firms have invested heavily in other business risks, such as operational or model risk, that has not yet propagated to the information security domain.”

Financial services executives listed information security and privacy vulnerabilities as one of the keys risk for financial institutions in Protiviti’s 2017 Executive Perspectives on Top Risks Survey. That is consistent with FSI responses to Protiviti’s 2016 Internal Audit Capabilities and Needs Survey, which listed information security knowledge among the top five areas for improvement.

---


Cyber Risk Rises

Everyone, from individuals to large businesses, are at high risk of cybercrime of some description, identity theft, account takeover, account cloning, fraudulent payments and/or transfers — the list goes on. But it is financial institutions that are battling against cyber criminals on the frontline.

Cyber risk is the foremost risk for financial services firms, which for the moment remain liable for any losses. Moreover, financial institutions are increasingly reliant on their technology and systems infrastructure, with many firms’ growth strategies shifting to digital models. Such a high degree of dependence on digital technology exponentially increases the risk, and the potential severity, of cyberattacks for financial institutions.

A flurry of high-profile breaches at banks, insurers, and credit card and payment providers, as well as large retailers, has succeeded in embedding the message that every firm will be the victim of a cyberattack at some point. The only unknowns are when an attack will happen and if the firm is prepared for the counterattack with processes in place to deal with the aftermath.

The insurance industry has been particularly hard hit by cyberattacks. More than 100 million Americans have had their personally identifiable information compromised in insurance sector data breaches. And this wave of cyberattacks will predictably continue because perpetrators know that insurance companies need to use and store large amounts of personal information about their policyholders. As such, U.S. regulators have prioritized the issue of cybersecurity, with the National Association of Insurance Commissioners (NAIC) implementing several initiatives to better protect firms, while the New York Department of Financial Services (DFS) has updated its proposed cybersecurity regulation, effective March 1, 2017, that will require banks, insurance companies and other financial services institutions regulated by the DFS to establish and maintain a cybersecurity program designed to protect consumers and ensure the safety and soundness of the financial services industry.11

Aside from the need to strengthen security and privacy controls, insurers and other financial services firms will have to contend with the heightened scrutiny of their risk and compliance programs.

Leveling the Playing Field

Heavily regulated brick-and-mortar financial institutions have expressed concern that they are at a competitive disadvantage against financial technology start-ups that have been gaining traction among consumers attracted to a new generation of easy online credit approvals and simple and secure mobile wallet and electronic payment applications.

“Banks feel like they are in a position where they are not as nimble because they have to adhere to all these regulatory requirements,” says Protiviti’s Michael Walter. “They want the playing field leveled.”

Regulation, like infrastructure, often requires time to catch up to emerging risks. Fintech is clearly in the regulatory crosshairs — both from an information security perspective and a credit risk perspective. But while that might address the fairness issue, traditional financial service organizations still need to be moving, with utmost speed, toward a better understanding of information security risk management.

Security at a Crossroads

Information security budgets are increasing at 78 percent of responding financial services institutions, compared with 63 percent for all industries. Some reported increases of more than 20 percent.

“It remains to be seen whether budgets will continue to increase,” Walter says. “Many are going to have to spend more money just to maintain their risk posture at current levels.”

For better or worse, much of that increased budget is likely to be spent in reaction to regulatory mandates instead of in support of strategic goals and objectives.

“A lot of institutions will start out trying to deal with security and privacy problems strategically,” Walter says “Inevitably, due to the budget process, they’ll end up going with a tactical solution to satisfy regulators.”

This make–do approach has led to layers of compensating controls and purpose–built security patches that may or may not be supported by current technology or IT personnel. As a result, many institutions are stuck with brittle risk control environments that don’t hold up well in an evolving risk landscape.

In a world where IT and business are inextricably interconnected, information security can no longer be considered supplemental. Ryan Rubin, managing director in Protiviti’s Cybersecurity and Privacy practice sees an opportunity for institutions to transcend short–term fixes and address information security and privacy in a more strategic manner. As companies are looking to evolve past legacy systems, they need to rethink security instead of just trying to leverage practices they have used in the past.

“If there are going to be new systems brought online, it gives organizations the opportunity to start afresh, which might be easier than retrofitting,” says Rubin.

Andrew Retrum, managing director in the Cybersecurity and Privacy practice, agrees. “Evolution of security within the financial services industry needs to continue, and continue at a pace faster than banks are accustomed to moving.”

The bottom line? At a time when both banks and fintechs are looking to innovate, information security and privacy are the table stakes required of anyone wishing to enter the game. Unless an organization can get those two things right, nothing else they do really matters.

Fintech Fined for Security Concerns

Traditional brick–and–mortar financial institutions have been calling for federal regulators to level the playing field by holding the new breed of online electronic payment services (fintech) to the same or similar standards imposed on federally insured banks. Security and privacy is one area where the same standards already apply.

The Consumer Financial Protection Bureau (CFPB), a federal watchdog agency created in 2010 by the Dodd–Frank Wall Street Reform and Consumer Protection Act, recently levied a six–figure penalty against a fintech firm that had built a reputation on claims of superior customer data security.

An investigation by the CFPB found that the company’s security and privacy practices were deficient and that it failed to encrypt sensitive information, conduct risk assessments or train employees in proper data risk management. The finding is significant because the penalty was assessed based on the fact that the company represented that it had taken steps to secure personal information when it had not.

In addition to paying a fine and legal fees, the company agreed to:

• adopt and implement reasonable and appropriate data–security policies and procedures
• use appropriate measures to identify reasonably foreseeable security risks
• ensure that employees who have access to or handle consumer information received adequate training and guidance about security risks
• use encryption technologies to properly safeguard sensitive consumer information;
• practice secure software development, particularly with regard to consumer–facing applications developed at an affiliated website.

The company was also ordered to retain an independent data security expert to conduct an annual data security audit and help the company develop a compliance plan.

This action is historic also in that it marks one of the first times the CFPB has taken action against a financial services company based solely on its data security and privacy practices. It certainly won’t be the last.
The compliance burden on financial services firms is significant and unabating. Financial services industry (FSI) respondents to Protiviti’s 2016 IT Technology Trends Survey ranked risk and compliance as their top technology priority, and a driver of digital transformation, but they also refer to the compliance burden as a main barrier to implementing many new technologies such as cloud adoption (44 percent), digitization (28 percent), new payment technologies (50 percent) and agile adoption (38 percent) — all of which could help firms to become more efficient.

The heavily regulated financial services industry is still dealing with the after-effects of the global financial crisis, where many firms invested in ad hoc risk and compliance initiatives at a time when they were cutting back in other areas. To make matters worse, the new processes were built on inadequate, outdated infrastructure, slowing down other critical procedures to the point that risk and compliance efforts have become a barrier to transformation. Today, firms continue to face more stringent regulatory compliance requirements from more advanced anti-money laundering systems to capital modeling with CCAR and DFAST requirements and even dealing with the regulatory implications of rules such as the GDPR in Europe and Privacy Shield in the USA. IT departments have to assist with the response to this heightened regulatory environment, which is squeezing resources for other projects.

Compliance spend is significant and increasing. The survey shows that almost 12 percent of the total IT budget is devoted to compliance, which is effectively equal to the innovation spend. Monitoring and adhering to legal and regulatory compliance is ranked as the foremost concern for IT functions. This burden will only increase as firms grapple with new regulations, leaving less available income to spend on much-needed modernization of core systems or innovation, to be able to launch new products and services to compete with the more nimble fintech disruptors.

Financial institutions are, at their cores, technology organizations, but technology risk is very much underreported compared to operational risks, and it is the biggest risk of them all.

— Jonathan Wyatt
For each of the following areas: Given your current knowledge and skill level, as well as the importance your organization is placing on this area at the present time, please rate each area on a scale of 1 to 10 where “1” indicates this is a low priority for you and your organization to improve and “10” indicates this is a high priority for you and your organization to improve.

<table>
<thead>
<tr>
<th>Area</th>
<th>All Respondents</th>
<th>Financial Services Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulation/compliance</td>
<td>6.9</td>
<td>6.9</td>
</tr>
<tr>
<td>Customer relationship management</td>
<td>6.8</td>
<td>6.8</td>
</tr>
<tr>
<td>Data warehousing and analytics</td>
<td>6.2</td>
<td>6.2</td>
</tr>
<tr>
<td>Back-office operations</td>
<td>6.2</td>
<td>6.2</td>
</tr>
<tr>
<td>Digital channels</td>
<td>6.0</td>
<td>6.0</td>
</tr>
<tr>
<td>Payments</td>
<td>5.9</td>
<td>5.9</td>
</tr>
<tr>
<td>Physical channels</td>
<td>5.7</td>
<td>5.7</td>
</tr>
<tr>
<td>Account origination/underwriting</td>
<td>5.6</td>
<td>5.6</td>
</tr>
</tbody>
</table>
One of the main mitigation strategies for dealing with this ever-present and growing compliance burden is to increase the use of technology to automate business processes and make them more efficient.\textsuperscript{13}

IT spend within banks, for example, has already increased significantly in areas such as AML where firms are working to leverage and update existing technologies to drive efficiencies. “Companies are also utilizing governance, risk and compliance (GRC) systems, which they may have had in place but never fully optimized, while there has also been a significant uptick in upgrades of applications in the compliance, risk and AML space,” says Vishal Ranjane, a managing director in Protiviti’s Risk & Compliance practice.

There are also efforts by larger companies to reduce the number of systems and applications they are operating to drive efficiencies. “Most of our larger clients have multiple solutions, often doing the same job. They are now attempting to integrate where possible and or align their taxonomies to be able to measure, manage and correlate information across the different lines of business,” says Scott Wisniewski, a managing director in Protiviti’s Risk Technologies practice. “IT and technology decisions made in the long past are now being re-evaluated to drive efficiencies, while we may start to see technology spend creep up in the attempt to drive down operational spend.”

Business process automation, including robotics, is another area where firms can find efficiencies. Protiviti has conducted extensive research in this area and has developed methodologies to help financial service organizations navigate these challenges with confidence and deliver value to shareholders and stakeholders.

Prevailing risk management and compliance practices tend to be siloed, manual and reactive, with control functions stratified by first, second and third lines of defense. This find-and-fix model expends time and resources firefighting immediate issues, such as regulatory actions or internal audit findings within silos, rather than working collaboratively on value-adding activities such as risk identification and mitigation. Protiviti’s Agile Risk Management philosophy aims to maximize value and embed risk management within, rather than external to, business processes.\textsuperscript{14} This inside-out approach provides for continuous monitoring and improvement, as opposed to lagging point-in-time samples or surveys. Designing risk management and compliance reporting into a process eliminates reporting delays and frees time and resources to focus on growth and risk-enabled decisions.

Ultimately, the most effective process management will come from a highly automated monitoring and testing program working continuously behind the scenes, using consistent data, a common methodology, shared tools and effective reporting across all lines of defense. One such tool is the Protiviti Risk Index\textsuperscript{™}, which executives with a comprehensive view of risk, showing how risk is changing over time.\textsuperscript{15} Firms can aggregate 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.


Bridging the Gap Between Compliance and Technology Risk

Adopting regulatory technology, or regtech, tools such as The Protiviti Risk Index™ is bridging the gap between compliance and technology. Firms need to become more prepared for the fact that the fast-moving digital future will be different from the crises of the past and will require agile and effective risk management and compliance functions that can move away from historical review and become more adept at identifying and addressing emerging risks as they appear on the horizon. This requires better data management and analytics.

Technology Risk 2.0

“Financial institutions are, at their cores, technology organizations, but technology risk is very much underreported compared to operational risks, and it is the biggest risk of them all,” says Jonathan Wyatt.

Technology risk activities ultimately need to go through a digital transformation of their own, if they are going to be fit for purpose.

The Protiviti Risk Index™ can also be used to measure technology risk exposure when implemented as part of The Protiviti Technology Risk 2.0 framework and methodology, which is designed to enable integration of the various groups performing aspects of technology risk activities, including the technology risk function, IT, the broader operational risk team, information risk, vendor management and cybersecurity teams.¹⁶

The framework helps financial institutions visualize an ideal future state while providing a proven methodology to realize that vision. This approach adds value by building bridges to a desired customer and user experience, rather than the less constructive current practice of running from one downside risk to another, putting out fires.

Protiviti’s Tech Risk 2.0 model seeks to determine how different functions work together and how their varied standards, taxonomies and agendas can be brought together to align with an organization’s business goals, threat analysis and risk appetite. By approaching this from a holistic rather than a technology-driven perspective, the GRC technology implementation is likely to meet with a much higher degree of success.

Protiviti’s Tech Risk 2.0 Model

Customer-Facing (Internal/External) Service Catalogue
- Deposits
- Mortgages
- Insurance
- Trading Equities
- Financial Reporting

Top-Down Business Risk Assessment

RISK CATEGORIES:
- C
- I
- A
- S
- R

THREAT ANALYSIS:
- OI
- WM
- OI
- OI

Risk Scenarios Identified (Primary Threat Actors*)
1

Risk Analysis

<table>
<thead>
<tr>
<th>Business Impact</th>
<th>Likelihood of occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>(includes consideration of identified controls)</td>
</tr>
<tr>
<td>Med</td>
<td>1</td>
</tr>
</tbody>
</table>

Technology Entity Mapping
- Platforms
- Processes
- Third Parties

Bottom-Up Risk Assessment
- Risk and Controls Library
- Remediation Plans
- Incident Response Plans

Compliance
- Frameworks
- Standards
- Regulations

Transparency Reporting
- Incident Analysis
- Continuous Monitoring
- Internal Audit
There is a need for firms to adopt a more integrated approach as outlined in Protiviti’s Tech Risk 2.0 model. This approach offers numerous benefits for vendor risk management, including:

- Vendor risks prioritized by top-down strategic risk assessment, rather than total spend
- Vendor risk controls derived from specific prioritized risks, rather than standardized schedules
- Self-reporting of vendor-managed controls increases vendor accountability
- Continuous monitoring engages with suppliers on a regular basis to verify that controls are operating effectively
- Remediation tracking and management process ensures vendor compliance with remediation plans
- Integration with operational risk ensures that third-party risks are fully considered in operational risk reporting.
Most institutions expect their technology spending to increase this year — some by more than 20 percent, according to the Protiviti IT Technology Trends Survey.

On the surface, that sounds like a good thing for FSI IT leaders, but the fact is that much of this investment is being used to buttress aging and complex infrastructure and to support multiple stand-alone applications built over time in response to the need to offer new products and services using aging core processing systems. Industry analysts suggest FSI IT operating expenses could be cut by as much as a third through a combination of lower-cost computing platforms and application rationalization.

And while IT budgets have been increasing, financial institutions are under increasing pressure to simplify operations and reduce operating costs.

Cost pressures are made even more acute by the rise of technologically advanced online lenders and electronic payment companies that have proliferated in recent years, unfettered by branch networks and expensive outdated processing systems.

Traditional financial service providers have awakened to the challenge, with 63 percent reporting that they are undergoing digital transformations over the next six months to two years. But they got a late start, and only about a third (36 percent) rate their institutions as having made substantial progress, compared with 51 percent for our cross-industry survey population.

Without simplification, the technology lever enables a misdirected process that won’t help to achieve the outcomes organizations desire.

— Atul Garg

On a scale of 1 to 10, where “10” represents substantial progress and “1” represents minimal progress, how would you rate your organization’s progress to date with regard to digitization?

![Progress Ratings](chart)

**Why Simplify?**

Imagine how difficult it would be to get anywhere by car if highways hadn’t been expanded since the 1960s, and even the shortest journey required navigating a complex series of detours and patches. Drivers would adapt, cobbling together shortcuts and work-arounds designed to get them where they needed to go with the least hassle and disruption. Logic suggests that when it came time to update the road system, designers would focus on eliminating the shortcuts and streamlining traffic flow instead of widening all of the detours to make them faster.

The same principle holds true for core modernization in the financial services industry. Aging information technology poses several significant problems — excessive maintenance costs, process and decision-making friction, degraded business agility, and more.

A logical first step in any digital transformation is the rationalization of current processes and procedures to simplify transition and avoid wasting money automating obsolete or redundant tasks. The goal is to find better ways to do things, not just accelerate outdated processes.

IT departments have a tendency to put the cart before the horse when it comes to core modernization, says Atul Garg, a Protiviti managing director and the company’s Financial Services Business Performance Improvement practice leader. They will buy a system, and have it installed, without giving users a chance to think through what they need or want. As a result, the company is often unable to achieve the anticipated benefits of the new system.
“Without simplification, the technology lever enables a misdirected process that won’t help to achieve the outcomes organizations desire,” says Garg. “Things move along and ultimately a system is implemented that essentially enables legacy processes.”

Getting to simple isn’t always easy, but it’s a journey worth taking.

The poet Oliver Wendell Holmes, father of the U.S. Supreme Court justice of the same name, is quoted as saying: “For the simplicity that lies this side of complexity, I would not give a fig, but for the simplicity that lies on the other side of complexity, I would give my right arm.”

Simplicity on the far side of complexity should be a fundamental goal of any core modernization initiative.

- Simple alleviates cost pressures by streamlining processes, eliminating redundancies, reducing maintenance requirements and freeing up resources for more value-adding strategic initiatives.
- Simple mitigates operational risk by aligning systems with desired outcomes and eliminating potential failure points, security weaknesses, documentation gaps and opportunities for error.
- Simple mitigates compliance risk, and reduces compliance costs, by consolidating data, streamlining reporting and automating compliance workflows.
- Simple breaks down information siloes to optimize reporting and facilitate data analytics at the enterprise level.
- Simple mitigates strategic risk by aligning core technology capabilities with customer expectations and eliminating obsolete and non-supported systems.

“I think, with any simplification initiative, it is important for business units and the IT department to work together, starting with, ‘What are our strategic priorities?’ and ‘What is our desired future state?’ so that there is a clear understanding of where the organization is trying to go,” Garg says. “You have to get the heads nodding around the table with a shared understanding of what the future looks like, and then you translate that back into what needs to change from a technology perspective.”

Protiviti’s six elements of infrastructure provide a good framework to begin discussions. The non-linear model addresses the effects of change on business policies, practices, and methodology, people and reporting, in addition to the actual changes to systems and data. This holistic approach is designed to help surface gaps and identify opportunities for simplification, business process improvement, reporting and training.
Six Elements of Infrastructure

- The six elements of infrastructure is a useful tool for categorizing issues, understanding where problems are occurring within the organization and drawing conclusions to form the basis for recommendations.
- In Protiviti’s view, the elements of infrastructure should be considered when designing a new process or assessing an existing process. Also, the six elements are common to each process or function.
- These elements represent the capabilities that each process or function should possess; and they provide a comprehensive and consistent framework to communicate the requirements for the appropriate operation of a process or function.
- While these elements are not necessarily intended to be a strictly linear process, the components of the framework are generally designed from left to right. The use of this structure helps organize the otherwise complex network of risk management activities into a comprehensive and consistent framework. In particular, it ensures that all key components are appropriately considered.
- In planning to adopt the new revenue standard, companies would benefit from considering the six elements of infrastructure.

Spending Money to Save Money

It takes money to make money. When it comes to digital transformation, it also takes money to alleviate cost pressure. While it may seem counterintuitive to view investing in new technology as an austerity measure, there are substantial savings to be realized by shifting away from the escalating cost of maintaining complex and outdated legacy systems, and toward simplification and modernization.

One large European bank, for example, has announced that it will spend more than a billion dollars over five years for an entirely new IT infrastructure designed to reduce costs, mitigate risk and create new revenue opportunities.

A Protiviti analysis of cost-cutting initiatives reported in the public filings of major global financial institutions found many major institutions listing technology investments and business process improvements alongside more traditional measures, such as closing branches and reducing headcount.
One of the biggest cost pressures appears to be driven by rising compliance costs, as new financial regulations increase the frequency and complexity of audits and reporting. This is another area where new technology and systems alignment could help cut costs and alleviate cost pressure.

Some studies estimate core modernization cost savings ranging from one-quarter to one-third of IT operating costs, depending on the range of opportunities for business process improvements. These savings may be achieved by consolidating several stand-alone applications — optimizing the costs associated with core applications and hardware processing, as well as reducing the number of systems requiring maintenance and integration.

Core modernization creates the opportunity for cost savings from the digitization of operations by “straight-through processing,” eliminating the need for manual processing of transactions meeting certain business rules. Even an interim solution, such as robotic automation, can relieve cost pressure by automating redundant tasks, such as the need to manually populate multiple databases with identical data.

Robotic automation has been used effectively to repatriate business processes that had been outsourced overseas. It should be noted, however, that while it can help relieve cost pressure, it is not simplification, because it helps to perpetuate the viability of redundant systems.

Finally, a significant portion of FSI IT operating budgets are allocated to support all of the work-arounds and detours required to cobble new products and services onto an incompatible core system. The modern service-oriented architecture and business process management built into newer systems, again with a thorough vetting and purging of outdated processes, can help IT functions spend less on maintenance.

---

18 Ibid.

Real-Time Banking Gets Real

Although a majority of financial institutions remain on the fence about core modernization and systems simplification, at least one major U.S. bank has already gone all-in.

Looking past the price tag, which ran in the hundreds of millions of dollars, executives and directors of this institution set their sights on a specific desired customer experience, and moved forward boldly to realize their vision.

The business case was simple. Bank executives reasoned that in a time of instant messaging and live-streaming video, it shouldn’t take two days for a bank to process and post an electronic transfer of funds.

Achieving that simple improvement, however, required a fundamental change and simplification in the complex core technology underlying the bank’s business. Instead of collecting transactions and processing them in daily batches — the standard industry practice — the bank wanted to process and post payments and deposits in real time. That is easier said than done, when most of the banks in the United States run on cookie-cutter technology provided by a handful of vendors.

To get to its desired future state, the bank hired a “user experience” consultant, it partnered with a real-time payment network and it purchased a small fintech that had mastered the customer service culture it wanted to achieve.

It is too soon to quantify the bank’s return on investment, but the initiative has already drawn positive headlines around the globe. Other institutions are following suit, and industry watchers say this is the beginning of a sea change in the way banking services are delivered.

The Case for Legacy Modernization

Seeking to mitigate the competitive risks of moribund infrastructure and the operating agility of new technology, financial service providers are tentatively embarking on the biggest industrywide systems upgrade in more than 40 years.

Three-quarters of FSI respondents to this year’s IT Technology Trends Survey indicated that their organization is already using some type of cloud-based application software, and almost half (43 percent) have begun the migration to cloud-based infrastructure. Gartner research indicates that more than half of all banks worldwide (60 percent) will be processing a majority of their transactions in the cloud as early as this year.20

The question remains, what to do with aging core systems? Financial executives identified aging legacy infrastructure (43 percent) and processes (36 percent) as the primary impediments to essential digital transformation. It is not surprising, then, to find that almost half (44 percent) of FSI respondents are considering the renewal or replacement of core processing or accounting systems.

That percentage is expected to grow as the number of transactions processed in-house dwindles and there are fewer transactions over which to spread the fixed cost of operating an on-premise data center.

---

Are you considering a modernization through a renewal or replacement of core processing/accounting systems?

<table>
<thead>
<tr>
<th></th>
<th>44%</th>
<th>44%</th>
<th>12%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Don’t know</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The majority of FSI respondents are modernizing their legacy systems to mitigate risk (76 percent). That is a broad category encompassing everything from competitive risk to data security, system complexity and the difficulty of supporting mainframe technology in an increasingly cloud-based ecosystem.

But changing critical systems is risky in its own right, as well as costly and time-consuming. These facts are reflected in the survey results, which show that implementation risk is the top barrier to change, cited by 41 percent of respondents, followed by competing priorities (24 percent) and the failure of new technology to perform as promised (24 percent).

Older technology, for all its flaws, is generally reliable — a critical requirement in an operation requiring 24/7/365 availability and error-free performance. So any strategy for legacy modernization must be carefully considered. Each comes with its own risks and benefits that need to be evaluated in the context of individual business models as well as short- and long-term goals.

**Modernization benefits**

1. Operational agility
2. New capabilities
3. Simplified operations/lower costs
4. Reduced maintenance risk
What is the primary catalyst for the change?

<table>
<thead>
<tr>
<th>Risk mitigation</th>
<th>76%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue generation</td>
<td>12%</td>
</tr>
<tr>
<td>Cost savings</td>
<td>6%</td>
</tr>
<tr>
<td>Other</td>
<td>6%</td>
</tr>
</tbody>
</table>

Although risk mitigation — mostly technology and workforce related — is the most commonly cited expected benefit of core modernization, others include increased new product revenue and reduced operating costs. Core renewal also helps with regulatory compliance by eliminating much of the technology friction and work-arounds required to create reports under older systems.

Overcoming Objections

Despite the obvious and well-documented benefits, a majority of financial services companies (56 percent) have not yet begun to consider modernization. This could be attributed to the reliability of aging technology and the fact that the basic business of banking continues to get done. ATMs continue to dispense money; customer statements are accurate and timely. That, combined with the multibillion-dollar cost of a new system, and some highly disruptive, costly and prolonged core modernization failures at other institutions, has contributed to a persistent “wait and watch” attitude.
What are the barriers to change?

<table>
<thead>
<tr>
<th>Factor</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation risk</td>
<td>41%</td>
</tr>
<tr>
<td>Time — disruption to other priorities</td>
<td>24%</td>
</tr>
<tr>
<td>Vendor product deficiencies</td>
<td>24%</td>
</tr>
<tr>
<td>Cost</td>
<td>11%</td>
</tr>
</tbody>
</table>

Key risks to consider include:

- **Customer service** — Protiviti’s 2015 survey of consumer banking and online retail payments found increasing demand for omni-channel customer experiences that are difficult, if not impossible, to deliver with legacy systems. At the same time, customer-facing systems need to be handled with great care to prevent glitches, interruptions and errors that could damage reputation and brand.

- **Regulatory compliance** — Increasing regulatory rigor and a trend toward real-time continuous monitoring is making it increasingly tough for financial institutions

Moving forward requires an understanding of the long-term and rising risks of continuing to utilize an aging core and the strategic benefits of modernization, as well as the different approaches to accomplishing that goal.

“(Core modernization) is like a heart surgery,” says Protiviti’s Ed Page. “It’s a high-risk proposition, but when it’s needed, you don’t take chances. You have to be careful to get the right surgeon and plans in place to ensure the best possible outcome.”

For a modernization project to succeed, project managers would do well to anticipate and plan to mitigate several key risks.

---

to meet regulatory expectations without systems modernization. Similar to customer service, in the sense that compliance systems can never be switched off, all existing regulatory controls need to be present and functional in new systems before transitioning from legacy technology.

- **Program fatigue** — As hard as it is to get approval for a core systems upgrade, it is even more important to maintain momentum through implementation and beyond. As with any large-scale, long-term project, there is a tendency for core modernization initiatives to run out of steam, or decline in quality control, in the middle and later stages.

- **Competing priorities** — Even the most worthy long-term projects are bound to come under scrutiny as the adrenaline of initial expectation and launch is replaced by the day-to-day details of implementation. Resource envy is common in a scarce-resource environment, and it is only natural for advocates of other projects to find fault with competing projects. The challenge here is to establish and maintain the enterprisewide strategic value of core modernization as top of mind and avoid being pigeonholed as an IT boondoggle.

**Strategies for success**

A lot can happen over the time — often measured in years — required to complete a core systems modernization. Executives may come and go; strategic priorities and budgetary conditions might change.

That is why a clear project road map with interim milestones that demonstrate value along the journey is so important. In addition to executive support and an effective program management office required of any major long-term transformative project, a successful core modernization plan requires clear and concise answers to key continuity questions:

- Why are we doing this?
- What is the business case?
- When should we proceed?
- What will the new enterprise architecture design be?
- Where will the technology be located (i.e., hosted and/or internal)?
- Who will help us (our technology and implementation partners)?
- How will we manage a project of this size in a risk-savvy manner?

All of these questions should be asked and answered during the business case and road map development process.

It is important to keep in mind that modernization does not necessarily mean replacement. There are five common strategies for answering the last question, each representing a fundamentally different approach determined by risk appetite and short and long-term goals. The first involves starting from scratch, and the last phases in new technology gradually to minimize disruption.22

---

Each strategy comes with its own benefits and implementation risks, summarized in the chart below.

### Core Modernization Strategies: Risk and Benefits

<table>
<thead>
<tr>
<th>Approach</th>
<th>“Greenfield”</th>
<th>Preserve and Protect</th>
<th>Simplify</th>
<th>“Big Bang”</th>
<th>Phased Core Replacement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benefits</td>
<td>Builds new technology and avoids unnecessary complexity in design</td>
<td>Leverages existing investments in legacy infrastructure and focuses investment on customer-facing solutions</td>
<td>Leverages investments in legacy infrastructure and simplifies back-office operations to reduce operating costs</td>
<td>Targeted, comprehensive approach to modernizing existing core infrastructure; preserves existing customer experience by leveraging existing channel solutions</td>
<td>Mitigates risk to existing processes and systems while implementing new capabilities</td>
</tr>
<tr>
<td>Implementation Risks</td>
<td>Does not leverage well-proven IT infrastructure</td>
<td>Defers mitigation of underlying technology risks</td>
<td>Defers mitigation of underlying technology risks</td>
<td>Highest risk of failure and customer impact</td>
<td>Creates additional costs and complexity during the transition to new technologies</td>
</tr>
</tbody>
</table>
“How many times do we see clients make the mistake of putting in new technology and not changing how they fundamentally conduct their business?” asks John Rao, a Protiviti managing director and the company’s Insurance practice leader. “They invest in the technology but continue to execute the processes the way they used to, so the cost structure remains high.”

This is a significant challenge. Business process improvement is the single largest driver of cost savings in a core modernization project, and unless financial service organizations are willing to redesign their workflows to match the new technology, cost reduction goals are likely to fall short.

The ultimate objective of each approach is to renew the core and/or critical systems so that all of the risks posed by those aging systems are mitigated. The least disruptive approaches ease the steep challenges of a pure “rip and replace” strategy but may require subsequent renewal efforts down the road.

More Than Machinery

Platform and processes go hand in hand. A successful modernization requires taking a hard look at business process improvement.

Digitization can be a powerful business tool, but the payoff is going to come from an organization’s ability to eliminate manual processes, freeing up resources for more value-adding strategic and customer-facing roles.

Parallel Processors Pave Way for New Core

A major bank, anticipating a new product push, found itself at the limits of its core processor — a homegrown technology stack that had been patched and modified so many times over multiple decades that it was hard to distinguish the original code from all of the customizations (much of it undocumented) that had been written to postpone “tech death.”

The bank hadn’t made a significant investment in core systems for years, but they could not justify halting operations to build a new system from scratch, or rip out the old one and replace it with something better. Bank executives and directors were worried about the institution’s future. Doing nothing was no longer an option. They contacted Protiviti to help them find a way forward.

With Protiviti’s help, the bank’s IT team initiated a phased core replacement, establishing a parallel system outside the old core. The new system became the platform for the planned product launches. Over time, core functions were migrated, starting with parallel systems, and gradually switching to the new platform upon successful completion of validation and employee training.

By breaking the migration into bite-sized pieces and moving gradually, the bank was able to reap the benefits of a more agile technology and improved customer service, while mitigating execution risk and spreading the cost of modernization over several years.

In the end, the bank was able to modernize everything, without disrupting anything.

Reaching the Tipping Point

As firms start to migrate functions to the cloud, there are fewer transactions over which to spread the fixed cost of operating an on-premise data center, creating a greater and greater imperative to move off of legacy platforms.

A phased legacy modernization approach adds some complexity but allows for the rapid deployment of new applications and technology while maintaining service levels and mitigating execution risk.
Final Thoughts

Whether they recognize it or not, financial services firms are inherently technology firms. Virtually every product, service and business process is enabled by technology, and advances in product offerings, customer experience and operating efficiency are inevitably rooted in some form of “digitization.”

The importance of technology, however, is a double-edged sword for financial services technology executives. On the one hand, emerging technology is fueling innovation opportunities and holds the promise to streamline operations. On the other hand, many must also deal with the complexity and risks associated with legacy systems and processes.

The stakes are high, both financially and operationally. Large firms are spending billions of dollars to achieve digital transformation. Mobile apps and real-time transaction processing in the cloud are replacing traditional branch networks and daily batch processing on in-house servers. Transformation is also occurring behind the scenes as manual operations are streamlined, automated, and digitized to enable straight through processing and advanced analytics using big data.

Amid all this disruption, financial executives are expected to maintain high service levels, impeccable data security and privacy and run an ever-expanding gauntlet of risk management and regulatory compliance testing and reporting.

Finally, as information technology changes, so do the skills required to build, deploy and support the environment. Retaining the talent to maintain the current legacy systems, while recruiting, training and retaining the set of skills necessary to lean into the opportunities presented by new technologies, will be a critical success factor for many organizations.

The Hierarchy of IT Concerns

Today’s technology executive is faced with a number of competing challenges. In that respect, IT priorities are similar to Maslow’s hierarchy of needs, in which higher-order needs for self-esteem and self-actualization are addressed only after basic needs — food, safety and belonging — have been met.
Protiviti created the following FSI IT maturity model based on Maslow’s hierarchy:

**FSI IT Executives’ Dilemma**

The foundation is formed by three fundamental concerns: risk and compliance, security and privacy, and service assurance. These concerns align with Level 1 of Protiviti’s IT Risk Maturity Model. This is the level at which most FSI IT departments rank, according to Protiviti research.  

Only after the environment is secure, and the systems are up and running and fully compliant, can an IT operation move up to the next tier of the hierarchy (Level 2 on the IT risk maturity model). Here the focus becomes efficiency, effectiveness and incremental improvements to customer experience.

---


The innovation apex is attained when executives are able to rise above the day-to-day fray of running their operations and focus on future needs, emerging trends and changing user behaviors. With the organization tactically sound, strategically focused and operating efficiently, FSI IT executives can turn their attention toward using technology to create game-changing capabilities. Given that virtually every aspect of financial services is enabled by technology, creating capacity to focus on innovation is critical to long-term success.

Innovation comes with its own set of risks. Change often places pressure on the base of the hierarchy. New business models and IT capabilities create compliance challenges. That can lead to new or increased security and privacy concerns, and frequently to new service assurance demands.

A sixth concern is not a stage of maturity, but rather a catalyst for change. As the name suggests, disruptive technology is disruptive. It is a change agent that impacts every part of the hierarchy, adding both risks and opportunities. In so doing, it also creates variability that requires IT organizations to be vigilant and adaptive.

Firms are at varying levels of maturity, but all are facing similar challenges that need to be addressed comprehensively to ensure they remain competitive in the changing environment. Below are several action items technology executives should consider when finalizing their IT transformation plans.

- **People:** Firms need to ensure they hire, train and retain employees with the appropriate skills and expertise to enable IT transformation with a view to developing more advanced technology to support new products and services. At the same time, they need a plan to retain legacy skills until systems can be modernized.

- **Processes:** Business models and processes need to be reviewed and updated to adopt a more agile environment to enable innovation to flourish. Adoption of agile or bimodal software development processes are examples of the changes underway in many organizations, most aimed at increasing agility.

- **Adaptive Architecture:** Traditional architectural patterns are not sufficient to support the pace of change underway in the industry. They must evolve to become more responsive to emerging technologies and even new business models.

- **Enabling Technologies (DevOps, Cloud Computing):** Technology executives should seek to responsibly leverage emerging technologies to support business and IT transformation in response to rapidly changing business models and new market entrants. For example, firms should take advantage of the cloud’s elastic capacity to support scaling up and down based on business demand, while also utilizing cloud service providers’ investments to reduce and manage “technical debt” and improve resiliency and business continuity management capabilities.²⁵

- **Legacy Modernization:** For those organizations that are burdened with aging legacy infrastructure (and most are), a plan to simplify, streamline and update these systems is becoming more and more critical. This doesn’t necessarily mean a full-on replacement of all legacy infrastructure, but it demands a thoughtful, risk-sensitive and strategy-aligned approach.

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?

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 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
CONTACTS

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

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

John Rao  
Managing Director  
+1.212.708.6372  
john.rao@protiviti.com

Kurt Underwood  
Managing Director  
Global Leader, Technology Consulting Practice  
+1.503.889.7771  
kurt.underwood@protiviti.com

Tom Andreesen  
Managing Director  
+1.312.476.6318  
tom.andreesen@protiviti.com

Ryan Rubin  
Managing Director  
+44.207.389.0436  
ryan.rubin@protiviti.co.uk

Michael Schultz  
Managing Director  
+1.713.314.5001  
michael.schultz@protiviti.com

Michael Walter  
Managing Director  
+1.404.926.4301  
michael.walter@protiviti.com

Scott Laliberte  
Managing Director  
+1.267.256.6825  
scott.laliberte@protiviti.com

Atul Garg  
Managing Director  
+1.704.972.9612  
atul.garg@protiviti.com

Scott Wisniewski  
Managing Director  
+1.312.476.6302  
scott.wisniewski@protiviti.com

Andrew Retrum  
Managing Director  
+1.312.476.6353  
andrew.retrum@protiviti.com

Tyrone Canaday  
Managing Director  
+1.212.603.5435  
tyrone.canaday@protiviti.com

Mark Lippman  
Managing Director  
+1.571.382.7807  
mark.lippman@protiviti.com

Jason Brucker  
Managing Director  
+1.415.402.6937  
jason.brucker@protiviti.com

Vishal Ranjane  
Managing Director  
+1.704.998.0778  
vishal.ranjane@protiviti.com

40 · Protiviti