The Hierarchy of IT Concerns and the Ambiguous Cloud of Emerging Technology

Introduction

New and emerging technologies, such as social, mobile, analytics (big data) and cloud – sometimes referred to collectively as SMAC – offer great promise in terms of innovation, agility, cost-effectiveness and resiliency. It can be difficult to know, however, what is hype and what is real, when to adopt and when to wait. As we learned from the dot-com era, first movers in applying technology innovation to the business world are often confronted with risks that outweigh the anticipated returns. On the other hand, missing a wave of innovation has risks of its own.

Financial services industry (FSI) IT leaders also face challenges and risks related to integrating these new technologies into already complex heterogeneous infrastructures that demand “always on” availability, uncompromising regulatory compliance, and high degrees of security and privacy protection. Deciding which workloads to migrate to new operating models and creating an adaptive architecture that allows the transition to occur at an appropriate pace will be critical, but the adoption of these new operating environments demands more than just new technology. These operating environments require changes in the underlying practices, policies, and operating models of IT. They require different engagement models with business partners, enhanced vendor management capabilities, improved systems management skills (particularly in complex hybrid computing environments), and new finance models and architectural frameworks.

And it’s more than just an IT concern. Business leaders also recognize the risks and rewards related to these emerging technologies. Evidence of this is in Protiviti’s annual executive risk survey,1 which found that IT challenges, particularly disruptive technology, were top of mind for C-suite executives. Ultimately, the decisions surrounding the adoption of new technologies and the resulting changes in IT operating models should be made in the context of an IT strategy that is aligned to the institution’s overall business strategy. Understanding an organization’s business priorities, its appetite for change (i.e., risk) and its approach to the marketplace should inform how IT manages its infrastructure and prioritizes its investment portfolio.

The Hierarchy of IT Concerns

Today, IT leaders in FSI are confronting a unique set of business technology drivers that require an industry-tailored IT model. Ed Page, managing director and leader of Protiviti’s FSI IT practice, views the challenges facing FSI IT executives in terms of an FSI IT maturity model based on Maslow’s hierarchy of needs.

The model is based on the belief that most FSI IT executives’ concerns fall into six areas:

- Risk and compliance
- Security and privacy
- Service assurance
- Innovation
- Disruptive technology

The foundation for the hierarchy of IT concerns (as shown in the infographic above) is formed by three fundamental concerns: risk and compliance, security and privacy, and service assurance.

---

1 Executive Perspectives on Top Risks for 2014; Protiviti and North Carolina State University’s ERM Initiative partnered to conduct this survey: www.protiviti.com/toprisks.
assurance. If these concerns are not adequately addressed, the others are unimportant. For FSI IT executives, these are the three basic areas that must be attended to before the higher-level concerns can even be considered.

Once the basics are covered – the environment is secure, and the systems are up and running and fully compliant – an organization can move up the pyramid into the operating efficiency layer. Here the focus becomes efficiency, effectiveness and incremental improvements to existing capabilities.

With the organization tactically sound, strategically focused and operating efficiently, attention can turn toward using technology to create game-changing capabilities. The innovation level 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. Given the fact that virtually every aspect of financial services is enabled by technology, creating capacity to focus on innovation is critical to long-term success.

That said, innovation often places pressure on the base of the hierarchy of IT concerns. New business models and IT capabilities very often create new risks and compliance challenges. They can lead to new or increased security and privacy concerns, and they frequently lead to new service assurance demands. An example of this is underscored in Protiviti’s recent PreView – Protiviti’s View on Emerging Risks newsletter, which describes the key considerations and implications related to the rapidly evolving world of mobile banking.2

Readers following along closely will notice that only five of the six topics listed above have been discussed so far. This is because the sixth is not a stage of maturity; rather, it is a catalyst that causes the maturity model to evolve constantly. As the name suggests, “disruptive technology” is, well, disruptive. We call it “the ambiguous cloud,” for both literal and figurative reasons. We use the term figuratively as a stand-in for the ominous word of mobile banking. It is used literally for one of the critical emerging technologies, “the cloud”: the trackless wilderness of public and private third-party infrastructures, platforms and applications that is rapidly changing how many solutions are delivered – and creating both opportunities and risks for IT leaders to consider.

The rapidly evolving SMAC technologies impact each of the other five concerns, albeit in different ways. They enable innovation. They hold the promise for lowering costs and improving resiliency. But they also create new risks, new compliance concerns, and without proper planning and implementation, added complexity. Finding a way to reap the benefits of these emerging capabilities while managing the associated risks will be a critical success factor for FSI IT executives now and in the years to come.

### Breaking It Down

#### Risk and Compliance

In the wake of the recent financial crisis, financial services firms face unprecedented regulatory pressure, with more regulations going into effect in 2014.3 This onslaught of compliance requirements is, and will be, a major burden for FSI IT executives for the foreseeable future.

In addition to the implementation of new systems and controls, a common concern is the need to aggregate data from across the enterprise to understand customer risk and behavior. The data integration and data management challenges that these requirements dictate are driving FSI organizations to develop more rigorous data governance practices in an attempt to manage their critical data assets more effectively. At many institutions, this is complicated by the underlying complexity of the infrastructure, the results of merger and acquisition activity, and line-of-business or product data siloes.

FSI IT executives should use this focus on risk and compliance not only to satisfy regulators, but also as a mandate to develop IT risk, compliance, and data governance practices that enhance business value.

#### Security and Privacy

Financial services firms are constantly challenged to protect the reputation and value of the franchise as they repel attacks from “bad actors” who seek to steal client data or disrupt client servicing. Distributed Denial of Service (DDoS) attacks, data breaches, and resulting compliance burdens, such as PCI, are the new norm, as evidenced by recent U.S. Securities and Exchange Commission guidance and Federal Financial Institutions Examination Council pressure to include “material” breach events in financial reporting.

These ever-growing security and privacy concerns create additional cost and operational complexity and threaten the trust that clients have placed in FSI firms. These issues are further complicated by the fact that critical client data is often at risk outside of the boundaries of the firm, whether through customer payment transactions or through sharing of data with third parties for other legitimate business use. These are real and present dangers.

In response, FSI IT executives must develop a security architecture that constantly adapts to the ever-changing threats. The security environment must also be responsive to new technologies, including the aforementioned SMAC and BYOD challenges, as well as evolving consumer behaviors.

---


Service Assurance

Financial services customers expect real-time 24/7/365 access to data and services. Those expectations extend to a growing number of channels and devices. More often than not, critical customer services must traverse many applications and many layers of heterogeneous technology to fulfill a request successfully. Managing the “always on – always accurate” expectations in a cost-effective, secure, and compliant manner is a critical concern for FSI IT executives.

Moreover, these demands are also reflected in the needs of internal employees of FSI firms. The workforce is increasingly mobile and tech-savvy. Employees want to choose their own devices (BYOD) and their own tools. The availability of alternative solutions (e.g., end-user developed solutions [shadow IT], application service providers [ASPs], cloud solutions) creates a diverse and difficult-to-manage environment inside the enterprise itself.

“The good news for FSI IT executives is that the financial services industry has been a heavy user and early adopter of technology for decades. The bad news for many institutions is that most of those deployments are still in place, resulting in layers of diverse, complex, and interdependent systems that are difficult to manage and even harder to evolve.”

Ed Page
Managing Director
FSI IT Practice, Protiviti

We believe that managing a hybrid operating environment, one involving some combination of traditional data centers, ASPs, private cloud, and public cloud infrastructure, will be required for years to come. Creating, implementing and enforcing processes, policies, and technologies to manage this heterogeneous landscape will be critical success factors for FSI IT executives.

In the face of these complexities, FSI IT executives must seek to simplify and modernize their operating environments, reducing redundancy and overlap wherever possible. But these steps alone are not enough. IT must reorient its service assurance paradigm to align with business services, rather than traditional IT services, and architectural patterns must adapt to the need for constant change in an “always on” operating environment.

Operational Efficiency

IT costs represent one of the largest categories of expenses for FSI organizations. Not surprisingly, IT regularly receives pressure to reduce expenses, not only to drive bottom-line results but also to fund investments in innovation. The unfortunate reality for many FSI IT operations is that layers and layers of technology have developed over decades on a wide variety of architectures (e.g., mainframe, client-server, web, cloud, mobile), creating an infrastructure that is complex and costly to operate.

Emerging technologies and alternative operating models offer the promise of reduced cost, but adoption requires a substantial one-time investment and involves significant risks. More often than not, core processing systems operate on aging, but stable, technology. These systems are essential to run the enterprise, so replacing them can be a daunting challenge. Consequently, FSI IT executives are faced with critical decisions about how and when to best embrace these new solutions.

Tackling these challenges will be a critical activity for many FSI IT executives in the months and years to come. Developing and executing a roadmap to streamline both business and IT processes, while simplifying and modernizing the underlying technology, will be critical to the success of many organizations.

“Fundamentally, we believe there are significant opportunities to simplify infrastructure, streamline operations and reduce costs,” Page says. “We also see great opportunities to increase agility and improve cost transparency, but the roadmaps to those goals are not without risk, so the path forward must be carefully planned and executed.”

Innovation

Consumer expectations, behavior, and institutional loyalty are changing, fueled by the emergence of robust online and mobile solutions, social networking, and alternative offerings. In addition, regulations and nontraditional competitors are chipping away at longtime revenue streams.

One of the major changes facing FSIs today is the evolution of channel strategy. No longer is physical location (e.g., the branch or local office) king. We believe that while a physical presence will remain a critical component of most institutions’ overall channel strategy, it must be more fully integrated into an overall strategy that incorporates branch, ATM/kiosk, contact center, online, mobile, and social into an omnichannel customer experience. It will require data and systems integration on a scale that has not been fully contemplated until recently.

Payments processing is another area poised for massive change. The adoption of mobile technology has led to myriad new payment methods and new competitors. These trends have a profound impact on the payments landscape. However, which technology or combination of technologies (e.g., near field communication, bar codes, EMV smart cards, mobile wallets, or something yet to emerge) and which business model will win out remain in question. Security and privacy concerns, heightened by recent breaches in retail point-of-sale transactions, are paramount in this area. In the end, we believe that the winners in this space will be those that solve the risk (i.e., security and fraud), usability, and ubiquity (i.e., where the transaction can be performed) equation.

Given the pace of change, FSI IT executives must embrace the “need for speed” in the business environment. Providing support for innovative thinking in the form of technology “greenhouses” and creating adaptive, service-oriented
architectures that support the ability to innovate will be critical success factors. Many organizations will also choose to embrace agile development methods to support the need for more rapid development and deployment cycles.

Disruptive Technology

Technology is always evolving, and the pace of that change is ever-increasing. Against this backdrop, it is absolutely critical to evaluate the technology landscape constantly. Some new technologies will emerge as game-changers, while others will fade away.

We believe that many of today’s emerging technologies will have a profound impact on the financial services industry, so it is incumbent on IT executives to make prudent bets on how and when to adopt them.

Social media offers the promise of engaging customers in new ways, but it creates challenges related to providing consistency across channels and opens the door to additional security, privacy and compliance concerns.

Mobile is the frontier for new innovation in many areas, but it too presents new security, privacy and compliance concerns.

The broad world of analytics, which we view as encompassing both big data technologies and predictive analytics, offers the promise of both cost efficiency and new capabilities. New technologies offer the ability to manage unprecedented amounts of data at increasingly lower price points, and new analytic capabilities enable more and greater abilities to glean insights about customer behavior and risk. Still, it is a challenge to integrate these into existing environments, and they introduce significant new data governance challenges.

Cloud computing in all its various forms (e.g., private, public, SaaS, PaaS, IaaS) promises benefits from speed to market to cost (e.g., shift CapEx to OpEx, improved transparency) to resiliency, and much more. But what style of cloud computing is right for a given enterprise, and how will the resulting hybrid environment be managed in terms of security and privacy, risk and compliance, and service assurance? These issues have profound implications for the base of the FSI IT maturity model. Disruptive technologies represent a fundamental shift in how IT services will be managed. It’s critical that the implementation of these new capabilities be managed to consider risk, compliance, security and privacy, and service assurance implications.

It also will be crucial to manage the architectural and organizational changes resulting from shifts in the IT operating model.

Conclusion

FSI IT executives will be called upon to play the role of “urban planners” in the challenges they face. They must balance the need to operate their current infrastructure in a compliant, secure, “always on,” and cost-effective manner, yet they also will be asked to adapt to emerging risks and opportunities, fuel innovation, and generally become more nimble. The status quo is not an option.

This is consistent with the results of Protiviti’s recent 2014 IT Priorities Survey, which indicated that two out of three IT organizations are undergoing a major IT transformation. Successful FSI IT executives will align their “urban renewal” to the business strategy and risk appetite of their organization. They will transform both their infrastructure and their operating model, developing and executing plans to manage risk throughout the ongoing transformation. This will demand that they sometimes create “detours and scaffolding” to allow progress and to position their organizations to take advantage of the promise of emerging capabilities without disrupting operations. It’s a formidable task, but one that cannot be ignored, and if properly managed, holds great promise to simplify and transform FSI IT infrastructure for the better.

---

For More Information ...

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit.

Protiviti’s dedicated Financial Services practice includes professionals with deep industry experience in banking, insurance, brokerage and investment companies. These financial services professionals can work with you to find approaches to help improve and establish strategies for your business as changes in the industry and regulatory environment impact your organization. Their guidance on regulatory reform can be found at www.protiviti.com/regulatoryreform.

For additional information about the issues reviewed in FS Insights or about Protiviti’s services, please contact:

Carol M. Beaumier
Managing Director
+1.212.603.8337
carol.beaumier@protiviti.com

Andrew Clinton
Managing Director
+44.20.7024.7570
andrew.clinton@protiviti.co.uk

Cory Gunderson
Managing Director
+1.212.708.6313
cory.gunderson@protiviti.com

Giacomo Galli
Managing Director
+39.02.6550.6303
giacomo.galli@protiviti.it