protiviti®
Risk & Business Consulting.
Internal Audit.

FS Insights

Financial Services Industry Newsletter • Volume 4, Issue 3

IT Challenges: What Is Next for the Financial Services Industry?

There are significant challenges facing information technology (IT) leaders in the financial services industry (FSI) today. Some of the major FSI IT challenges are the very same ones IT leaders in all industries are facing. These include mobile commerce, social media, the safeguarding of client and employee data, management and classification of data, risk management, IT infrastructure planning, business continuity, and IT asset management. However, while IT-related themes are similar across industries, the context in which the challenges are developing in FSI is directly related to the regulatory developments and end-user dynamics of the industry.

During the third and fourth quarters of 2012, Protiviti conducted a cross-industry online survey[1] of close to 200 IT executives and professionals; approximately 20 percent of the respondents were from the financial services industry, the largest industry group represented. During the same period, Protiviti also conducted a broader risk survey[2] of more than 200 C-suite executives, who reported some of the same IT concerns and challenges noted in the IT survey. This article[3] seeks to explore in more depth the IT challenges for the financial services industry.

Key Findings

For each category in the IT Priorities Survey, respondents were asked to assess, on a scale of one to five, their competency in different areas of knowledge, with one being the lowest level of competency and five being the highest. For each area, they were then asked to indicate whether they believe their level of knowledge is adequate or requires improvement, taking into account the circumstances of their organizations and industry.

Key findings in the overall cross-industry survey reveal trends and areas of priority that IT functions are currently addressing and planning for in response to what is happening in the market. These trends include:

Mobile commerce – Numerous facets of mobile commerce management have emerged as major IT function focal points, including mobile commerce security, mobile commerce policy and mobile commerce integration. IT organizations are proactively looking to put into place more control and regimen around the management of mobile commerce and related new technologies.

The management *and* classification of data – Data classification and management have together become an overarching priority for IT functions, as organizational information systems continue to generate more and more "big data" that must be managed in accordance with risk management, regulatory compliance management and performance management requirements. The more the IT function understands what comprises "sensitive" (i.e., valuable and/or high-risk) data, the more effective and cost-efficient the organization's data management capabilities will become.

Social media – IT departments are investing significant time and resources to support the integration of social media and the governance of these technologies and related activities, which include social media programs for employees, customers and other external stakeholders.

Business continuity – In the wake of several catastrophic natural disasters, IT functions are more mindful than ever of the need to plan for and respond to potential business disruptions, outages resulting from hacking, and to evaluate the location of their backup facilities.

[1] *2013 IT Priorities Survey* report, available at www.protiviti.com/ITsurvey.

[2] *Executive Perspectives on Top Risks for 2013* report, available at protiviti.com/toprisks.

[3] This article discusses the FSI IT survey findings with three Protiviti FSI IT Managing Director leaders: Tom Andreesen (Chicago), Rocco Grillo (New York) and Jonathan Wyatt (London).

Inside This Issue

IT Challenges: What Is Next for the Financial Services Industry? ..... *page 1*

Banking in a Post-Financial Crisis World: Are Regional Banks Ready? ..... *page 6*

Risk management – ISO 31000 defines risk as the "effect of uncertainty on objectives." Given the uncertainty radiating from IT issues such as mobile devices, social media, cloud computing and new compliance requirements, among many others, it's no surprise that ISO 31000, as well as risk management in general, marks an area of IT leaders' concern.

IT infrastructure planning – Planning activities, specifically platform performance planning, storage management and planning, and network performance planning, represent key priorities for chief information officers and their teams. These objectives point to an effort to make the IT function more agile in response to the accelerating pace of change.

IT asset management – Given the proliferation of smartphones, tablets and similar devices as well as the new applications and organizational data contained on these devices, IT functions have entered a brave new, highly mobile and increasingly risky world of asset management.

Overall Technical Knowledge

Understanding and responding to innovation underscore the priorities for FSI IT departments. Social media and mobile commerce capabilities, along with smart device integration, top the list of areas for which survey respondents noted a need to improve their technical knowledge.

"Need to Improve" Rank	Areas Evaluated by Respondents
1 (tie)	Social media policy
	Social media security
3	Mobile commerce policy
4	Smart device integration
5 (tie)	Social media integration
	Mobile commerce integration
	Mobile commerce security

Q&A With Protiviti Managing Directors

Tom Andreesen, Rocco Grillo and Jonathan Wyatt are three managing directors from Protiviti's Technology Consulting Practice who share below their views on IT challenges for the financial services industry.

Q: Were any of the FSI IT survey results related to technical knowledge surprising?

Tom Andreesen

Tom Andreesen: In the area of overall technology skills, it was interesting to see the challenges of social media and mobile commerce moving from that of awareness and how to deal with these capabilities in our previous study to now integrating them with other critical business systems. Mobile and social media capabilities are also being used to drive internal and external customer relationships to an even higher level of connectivity, which in turn drives new business opportunities. FSI IT organizations then face the resulting challenges on how to support these new business capabilities.

Rocco Grillo

Rocco Grillo: Surprisingly, social media policy and the security around social media are at the top of the findings for financial services clients. While many of the larger financial services companies have embraced social media and made substantial efforts over the years to address the risks of social media for both the use of their corporate end users as well as customers, smaller financial organizations are now following this lead and leveraging social media.

The use of mobile devices and policies appears to be well under way in the financial services industry; the larger concern is the ability of financial institutions to roll out these technical innovations to consumers and enable them to execute mobile banking and other financial transactions. Financial institutions are racing to gain a leg up on their competitors, provide consumers with efficiency, and drive consumer retention and stronger ROIs. As with most rollouts, security and other risks can be overlooked when they are delivered to the marketplace too quickly.

With the introduction and broad adoption of multiple consumer mobile payment platforms, it is not surprising to see that organizations are challenged on how to address evaluating and adopting these new media of commerce – or risk being left behind. Securely implementing mobile commerce solutions that impact their existing regulatory compliance initiatives and how to adopt policies that ensure they are implemented and maintained in a secure manner are ongoing concerns.

Jonathan Wyatt

Jonathan Wyatt: It is not a surprise to see that the financial services industry, like many other industry segments, is considering how best to respond to the demands of clients, business partners and employees to embrace new technologies. A significant challenge for many large, global financial services organizations is that they typically have very complex operating environments, which often include a mix of new and old technology. Many large financial services organizations therefore lack agility and will find it hard to respond quickly to the changes smart devices will bring.

Concerns around information security and challenges related to operating in a heavily regulated environment may result in financial services organizations taking a cautious approach to embracing new technologies and responding quickly to changing market dynamics. All organizations do however need to ensure that they do not find themselves trying to play catch-up as new businesses with new operating models take consumers and/or users by storm.

Managing Security and Privacy

Predictably, FSI IT functions are focused on enhancing security and privacy solutions and strategies, managing third-party vendors (especially with regard to compliance), and managing and classifying "big data."

"Need to Improve" Rank	Areas Evaluated by Respondents
1	Implementing security/privacy solutions and strategies
2	Managing third-party vendors
3 (tie)	Managing and classifying enterprise data
	Monitoring security events
	Incident response

Q: What is the most significant challenge your clients are facing in managing IT security and privacy?

Tom Andreesen: We are seeing vendor management become a huge priority for institutions. FSI organizations are using third-party relationships to support more critical business functions that process sensitive information and are being driven to understand the security and privacy risks of these arrangements. Additionally, the market for outsourced capabilities has grown and with it the number of providers all competing to provide an institution with functionality quickly. With this high growth of vendor-available products comes the challenge of how institutions integrate these vendors and their products into the business and include both business and IT users to ensure the institution remains compliant with all its IT, security and privacy policies, as well as regulatory requirements.

Rocco Grillo: Recent security breaches in the financial services industry caused by a new breed of criminal hackers and sophisticated cyber attacks have been highlighted by the media. These attacks present unprecedented challenges for financial corporations. While many organizations and corporations already have basic security controls in place, and regularly test IT systems and procedures, they can be caught off guard by new threats and risks that are not anticipated or brought to the attention of management. With the emergence of advanced persistent threats (APTs) and an increase in the range of types of attacks, organizations may be unaware of the unique challenges faced when making changes to implementing a more comprehensive approach to security testing.

In addition, financial organizations are reliant on outsourced service organizations managing or storing their corporate data and supporting business services such as IT, HR, legal, marketing and facilities. Although there is a strong business case for outsourcing processes, areas that cannot be outsourced are the risks associated with the loss of data, corporate branding, breaches of confidentiality, and failure to comply with legal and regulatory requirements. These factors become increasingly important because of more regulatory enforcement as data is transferred across countries and jurisdictions and the ability to govern risk moves beyond corporate boundaries.

With all of these threats at the forefront of financial services organizations, it is imperative not only to have an effective incident response program that addresses company-specific incidents, but also incidents of third-party business partners and vendors as well. We continue to witness firsthand that many organizations do not have the capabilities or availability in-house to manage security incidents adequately. It is not enough just to have a plan. It is imperative that organizations as well as third parties maintaining outsourced data have programs in place that are tested regularly for their effectiveness in responding to the next emerging threat. Successful management of incidents or breaches includes the identification of the event, containment and minimization of the incident, and eradication of the incident; it also requires having qualified personnel to respond to these attacks. Financial organizations must maintain sufficient executive sponsorship and support for their incident response programs.

Jonathan Wyatt: Information security will always be a priority for financial services organizations. Many organizations are looking at better utilizing identity and access management systems to manage user access, with specific consideration being given to privileged access and enforcing segregation of duties controls to avoid the so-called "toxic combinations" of access.

The emergence of new technologies and the need to find solutions that embrace these technologies and do not block their use will require organizations to develop new capabilities.

Consumer demand will put organizations under pressure to respond uncomfortably quickly to these technologies.

Another area of focus for some organizations will be regulations such as the Payment Card Industry Data Security Standard (PCI DSS). To date, much of the focus has been on merchants and service providers, but there is now increased focus on issuers and ATM networks. This shift in focus will require banks to make a significant investment over the next few years to ensure compliance.

Compliance with other standards such as ISO 27001 are increasingly being expected of service providers, and large financial services organizations will find themselves considering how best to achieve compliance with these types of standards as they look to partner with other organizations.

Defining IT Strategy and Organization

FSI priorities in this category, which differ significantly from the overall cross-industry survey response, include establishing strong standards around security/privacy and operations management, and IT risk analysis and reporting.

"Need to Improve" Rank	Areas Evaluated by Respondents
1 (tie)	Developing and maintaining security and privacy standards
	Developing and maintaining operations management policies and standards
3	IT risk analysis and reporting
4 (tie)	Developing and maintaining enterprise information architecture
	Developing and maintaining end-user support policies and standards
	Managing and monitoring policy exceptions

Q: What is the largest challenge your clients are facing with managing IT strategy and organization?

Tom Andreesen: Our clients are facing two large challenges with managing IT strategy within their organizations. First is the ability to organize and develop a long-term IT strategy specific enough to meet regulatory and business strategy requirements, and flexible enough to encompass changing business and customer needs. To combat this challenge, an increasing number of project management offices (PMOs) are being created within IT and cross-functionally to prioritize initiatives and allocate resources. The PMOs are focused on project portfolio resource management, reporting and ensuring the highest and best use of resources against the strategy. Organizations are also intent on tracking the benefits of these expenditures and validating that they are being achieved.

The second IT challenge relates to developing and maintaining enterprise data architecture. IT groups are designing the data architecture to be flexible enough to handle different data types and feeds from legacy and new data platforms. However, they need business and management user requirements to ensure they are creating the architecture in the most efficient and effective way for users. Most institutions have enterprise data groups, finance groups, lines of business and management all pulling information to perform customer analytics, and report operational and product information. Data ownership therefore can be difficult to establish and impacts the ability to make good decisions in how to address data design.

Rocco Grillo: The responses reflect the critical strategic challenge that the security of information technology of financial institutions is continually subject to increasing regulatory scrutiny in today's environment fueled by rampant security breaches occurring, as well as other disruptions to services and network availability caused by natural disasters. In parallel, companies are struggling with designing and implementing emerging technologies that employees and customers are asking for, while balancing appropriate information security and compliance measures.

Companies are finding that if they don't explore these technologies, employees and organizations will implement technologies themselves in a less secure manner. Organizations must balance between their heavily regulated IT environment and emerging technologies such as mobile, social media and cloud computing.

With new technologies come new forms of risk and attack vectors that must be considered and evaluated. As indicated by the survey results, organizations must become more proactive in integrating levels of IT and security risk management into the evaluation, testing and deployment of new and emerging technologies. This re-evaluation process must be ongoing in order to address new and emerging vulnerabilities and their potential impact on the organization.

Jonathan Wyatt: Many financial services organizations have complex IT environments; therefore, it can be extremely challenging for these organizations to drive change or respond to new regulations in a timely and cost-effective manner. However, it is also extremely difficult for large organizations to consolidate and standardize while responding to the immediate operational demands of the business. Failure to define and implement programs that seek to simplify the operating environment will result in escalating costs and leave many organizations to falling market shares as new entrants that are more agile embrace new technology more quickly.

Additional challenges in such a complex environment are how to assess and manage risk. This includes assessing and prioritizing technology risks, or understanding the true operational risks arising from the use of technology. We are working with many organizations to help them implement

more effective frameworks and processes to quantify risk. It is therefore no surprise to see the focus on standards and risk management.

Ensuring Continuity

Not surprisingly, in the wake of recent natural disasters and weather-related disruptions, IT leaders and professionals are focusing on risk assessments and business impact analyses, along with building strong business resumption plans.

"Need to Improve" Rank	Areas Evaluated by Respondents
1 (tie)	Developing and maintaining risk assessment/business impact analysis
	Developing and maintaining business resumption plans
	Developing and maintaining IT disaster and recovery plans
4	Ensuring executive management support and sponsorship
5	Developing and maintaining crisis management plans

Q: What is the largest challenge your clients are facing with ensuring IT continuity?

Tom Andreesen: Institutions have extensive plans in place to ensure continuity and are better at the recovery process as they meet regulatory requirements and leverage the capabilities offered by third parties. However, every new natural disaster, like Hurricane Sandy in October 2012, challenges these continuity and recovery plans. Natural disasters can expose the weaknesses of these plans; for example, not having a plan in place to move data centers and backup facilities further inland and away from the coasts.

Rocco Grillo: The financial services industry has had to deal with business continuity management (BCM) and disaster recovery planning for years now due to multiple federal regulations and the reality of dealing with natural disasters. Natural disasters always increase awareness of BCM and cause organizations to enhance their plans in ways they may not have thought about before. They also bring about more awareness in an organization to ensure plans are adequate and address continuity in all areas of the business. However, this focus may wane once the disaster drops from the headlines.

Many organizations bypass the business impact analysis and risk assessment components of BCM and jump into the development of recovery strategies and plans, often spending time and resources on strategies that do not address the recovery and restoration of critical components of their business. The industry is seeing a large increase in organizations' use of business impact analysis and risk-based approaches to re-evaluate their recovery strategies and plans. Even though tools have matured, allowing for an ease of central development and repository of plans, this does not compensate for the fact many organizations are not spending time and effort to document quality plans that will adequately address recovery in the event of a natural disaster. Until organizations build resiliency into their IT and business processes, BCM will be in a reactive and catch-up mode.

Jonathan Wyatt: IT continuity has always been a priority for financial services organizations and, as such, it is not a surprise to see business resumption planning and disaster recovery highlighted as business priorities. We have seen numerous high-profile financial services organizations suffer outages due to technology failure. The continuing pressures on organizations to respond to emerging information security threats and the associated business continuity implications may well be drivers.

The complexities associated with embracing the cloud as businesses increasingly utilize third-party service providers and software-as-a-service solutions present businesses with new challenges from both an information security and business continuity perspective. While financial services organizations are more cautious in their adoption of the cloud, we are starting to see our clients embrace these technologies as the marketplace matures.

In Closing

These IT themes resonate throughout the entire FSI landscape. Financial services organizations are going to need to determine priorities and business requirements, and focus resources on their highest and best use to ensure the long-term sustainability of their businesses. For each financial services institution, the larger issues are going to be those that require the most planning, organization and management support. Institutions also will need to re-evaluate their progress against regulatory developments, end-user industry dynamics and future trends that may impact the industry.

Banking in a Post-Financial Crisis World: Are Regional Banks Ready?

Escalating regulatory pressures are driving a structural shift in how banking organizations approach their enterprisewide risk management and assurance activities. To meet growing regulatory requirements, firms will need to commit considerable management time to enhancing business architecture and reassigning resources.

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act or the Act) is the most sweeping and pervasive of these new regulations. The Dodd-Frank Act aims to further define, expand and strengthen the role of risk management and internal audit by driving the creation of a mandated framework that meets enhanced regulatory expectations and standards.

Given the continuously evolving nature of risks impacting financial institutions and poor performance of many banks and non-banks during the recent crisis, regulators in general – and the Office of the Comptroller of the Currency (OCC) in particular – are no longer accepting minimal satisfactory ratings when it comes to risk management systems and assurance functions such as internal audit.

A Look at Sections 165 and 166 of the Dodd-Frank Act

The Dodd-Frank Act was enacted in January 2010 primarily "to promote the financial stability of the United States by improving accountability and transparency in the financial system." Much has been written about the Act and the complexity associated with the implementation of the requirements enumerated in its 848 pages. This article, however, will focus primarily on Sections 165 and 166 of the Act. We see these sections as the basic roadmap that banks with assets of more than US$10 billion will be required to implement and follow. In many cases, the efforts to achieve compliance with these directives will be an enormous, expensive and resource-challenged undertaking by the banks. (What is noteworthy is that this critical section of the law, which likely will cost billions of dollars to implement, only accounts for nine of the 848 pages of the Act.)

Section 165 of the Act directs enhanced prudential standards for financial companies and increased supervision by the regulatory community. Section 166 orders a series of specific remedial actions to be taken by a financial company in distress to ensure that no harm is caused to the financial stability of the United States. The major areas covered under the enhanced prudential standards are listed below:

- **Risk-based capital and leverage limits**
  Demonstrate a robust, forward-looking capital planning process, accounting for unique risk profiles and continued operations during financial and economic stress. Provide underlying analyses and stress test results.
- **Liquidity requirements**
  Meet higher liquidity standards and comply with new rules related to the liquidity coverage ratio (LCR) and net stable funding ratio (NSFR). Conduct monthly stress testing under internal stress scenarios.
- **Single-counterparty credit limits**
  Verify credit limits and credit exposure to any affiliated company exceeding 25 percent of a company's capital stock and surplus.
- **Risk management and risk committee requirements**
  Establish a functioning board risk committee.
- **Stress testing requirements**
  Complete annual supervisory stress tests and semi-annual company-run stress tests and publish the results.
- **Debt-to-equity limits**
  Maintain a debt-to-equity ratio of no more than 15-to-1.
- **Early remediation framework**
  Provide for the early remediation of financial distress.

Heightened Regulatory Environment After the Financial Crisis

In addition to other various proposals adopted by regulators, Sections 165 and 166 of the Dodd-Frank Act were mandated as a consequence of the hard lessons learned from the recent financial crisis. The crisis exposed significant gaps in overall corporate governance and risk management practices of many U.S.-based financial institutions, both bank and non-bank.

The extraordinary circumstances of the financial crisis, the resultant negative impact on the larger economy, coupled with the difficulty of both banks and non-banks in navigating the complex domain of the financial sector have compelled regulators to re-evaluate their minimum requirements and standards in relation to risk management systems. Given the continuously evolving nature of risks impacting financial institutions and poor performance of many banks and non-banks during the recent crisis, regulators in general – and the Office of the Comptroller of the Currency (OCC) in particular – are no longer accepting minimal satisfactory ratings when it comes to risk management systems and assurance functions such as internal audit.

Recent communications with larger, more complex banks in the national banking system have indicated that the OCC expects banks to build risk management systems and internal audit capabilities that far exceed a "Satisfactory" rating and begin to meet its definition of "Strong."[1] This enhanced

[1] *Large Bank Supervision, Comptroller's Handbook,* OCC, January 2010: www.occ.gov/publications/publications-by-type/comptrollers-handbook/lbs.pdf.

requirement, augmented by new complex regulations and compliance mandates, necessitates a significantly altered approach to governance, enterprise risk management and regulatory compliance.

The financial crisis exposed a wide range of deficiencies in many aspects of enterprise risk management, including the first, second and third lines of defense, at many financial institutions. Failings included weaknesses in corporate governance structures, which resulted in an overall lack of credible challenge in the boardroom during critical times of the crisis. This lack of credible challenge also was witnessed at all levels of the organization and was particularly present in the second and third lines of defense at many institutions. Where firms had established corporate risk appetite statements, often the objectives adopted at the line-of-business level did not reflect the strategic objectives of executive management and the board. In addition, metrics used to track the level of risk at the line of business were often inconsistent and not well-defined. This led to an inability to accumulate, aggregate and advance these risk metrics to the "top of the house," which resulted in insufficient exception tracking and the absence of an effective escalation process.

In many financial institutions required to comply with these new standards, senior management and the board have yet to acknowledge the magnitude of the undertaking and evaluate the degree of effort, resources, costs and personnel that will be required to comply with the heightened regulatory expectations.

To meet regulatory requirements effectively, executive management and the board must first establish and approve risk tolerances across the organization, define the metrics that will be tracked and reported, and clearly define the targets to be established by these metrics. Tolerances also must be assigned to limit variability of reported metrics from targets to an acceptable degree. These tolerances, metrics, targets and thresholds must be defined in the risk appetite statement, written at the enterprise level and implemented at the line of business level. This approach will enable effective monitoring and tracking of risks and allow for timely identification of anomalies across the enterprise.

All three lines of an organization's defense now must be aligned to focus on complying with the risk appetite statement at both the enterprise and line-of-business levels. Exceptions must be rolled up and reported across the organization, ensuring that management at all levels are suitably apprised, and the problem is being owned and actively remediated at multiple layers through policy directives and risk initiatives, and by addressing process deficiencies.

As noted in Protiviti's *Executive Perspectives on Top Risks for 2013*, regulatory changes and heightened regulatory scrutiny are a significant concern for financial services institutions.[2] However, we contend that in many financial institutions required to comply with these new standards, senior management and the board have yet to acknowledge the magnitude of the undertaking and evaluate the degree of effort, resources, costs and personnel that will be required to comply with the heightened regulatory expectations.

New Challenges for Internal Audit

Regulators are particularly sensitive that internal audit be prepared to challenge the assumptions of executives at the line-of-business level and determine if they are outside the risk parameters, as defined by the risk appetite statement established at the enterprise level.

In our view, one of the greatest challenges will be in the area of internal audit. This is one discipline where regulators have significant, new heightened expectations for the industry. Under these new standards, internal audit will now be required to opine on the readiness and design of risk management structures that accommodate enhanced prudential standards. Internal audit also will be required to audit and opine on the effectiveness of risk management systems at both the enterprise and the line-of-business level.

Regulators are particularly sensitive that internal audit be prepared to challenge the assumptions of executives at the line-of-business level and determine if they are outside the risk parameters, as defined by the risk appetite statement established at the enterprise level. In many cases, this will require significant changes to the internal audit functions within banks. The impact will be on staffing levels, areas of expertise, increased scope of reviews, and more in-depth review and understanding of risk management practices and risk appetite statements within the organization. For many chief audit executives, this may require the addition of skill sets to their staff that do not currently exist.

Organizations complying with enhanced prudential standards will face enormous challenges in staffing, acquisition of new skill sets, and in some cases, a total restructuring and/or re-engineering of their risk management systems.

[2] *Executive Perspectives on Top Risks for 2013*, Protiviti Inc. and North Carolina State University's ERM Initiative, 2013: www.protiviti.com/en-US/Documents/Surveys/NC-State-Protiviti-Survey-Top-Risks-2013.pdf.

Moving Forward With a Regulatory Compliance Plan

It is important that executive management design and execute a plan to move toward the heightened standards. The plan must articulate responsibilities, accountabilities, goals, milestones with specific dates, potential results, and steps to deal with contingencies. It must be developed in consultation with line-of-business executives, risk managers and assurance functions, and there must be consensus for the defined plan from the board and executive management on down. The organization also must cohesively move to execute the plan and demonstrate compliance with the enhanced prudential standards to regulators.

Once implemented, the plan to address the heightened standards will strengthen risk management practices and enhance corporate governance. In turn, this will drive sustained improvement in board reporting and monitoring, resulting in protection of the institution's assets, and if done effectively, facilitate prudent risk-taking by the organization.

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 you improve and establish strategies for your business as changes in the industry and regulatory environment impact your organization.

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

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

Jonathan Wyatt
Managing Director
+44.20.7024.7522
jonathan.wyatt@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

Rocco Grillo
Managing Director
+1.212.603.8381
rocco.grillo@protiviti.com

protiviti®
Risk & Business Consulting.
Internal Audit.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.
© 2013 Protiviti Inc. An Equal Opportunity Employer. PRO-0413