



*Managing the Business of IT*

## **Vendor Management by Banks – Beyond Compliance**

Research conducted by:  
The FactPoint Group

on behalf of:  
ITM Software

Author: ITM Corporation  
All Rights Reserved ©2008 ITM Corporation

## Contents

Introduction .....	2
Study Sample .....	2
Findings Highlights .....	2
Vendor Management Practices Today .....	6
A Payoff .....	9
Conclusion .....	10

## Introduction

ITM Corporation sponsored a study to learn from bank professionals:

- 1) what issues they have related to vendor management for the future,
- 2) what priority these issues have relative to others in their overall IT agenda and
- 3) what solutions they seek to manage them more effectively.

Interviews reveal major changes are underway, both in how IT professionals look at the dynamics they face and in the solutions they need to manage them.

This summary highlights findings related to this development, based on in-depth interviews conducted with representatives from 34 banks during the summer and fall of 2007. ITM engaged The FactPoint Group to conduct the research.

## Study Sample

The sample for this study focuses on medium-sized banks with assets between \$4 billion and \$50 billion, with the rationale that this would include banks large enough to have complex supply chains and yet, small enough that costs for compliance would be a burden. Representatively, Comerica, with assets of \$53 billion is the 25th largest US bank.

Participants agreed to contribute to the study, assuming confidentiality. The sample includes well-known national and regional banks. Specific quotes noted come from key executives responsible for IT and non-IT vendor management within the banks. Titles of participants include: CIO, Senior Vice President of Vendor Management, VP Corporate Operations, VP Operations Risk Management, Chief Financial Officer,

Chief Risk Officer, Chief Technology Officer, and Executive Vice President of Corporate Privacy and Management.

## Findings Highlights

Bank IT professionals have noted the following key dynamics as significant.

### Growing Vendor Management Importance and Scope

Today, regulatory compliance elevates the importance of vendor management from a department-level process to an enterprise-wide one. Banks rely heavily on IT vendors for systemic, core bank functions. Thus, IT vendors' contribution to the strategy of the business is on the rise. Managing IT vendors is more challenging than managing typical bank vendors, so it is important that IT sits at the table to define and implement vendor management business processes.

Banks look at vendor management primarily from a risk and compliance perspective. According to respondents, reputation is the highest of the various bank risks. Compliance risks are also critical, as failing to comply can force banks to stop accepting deposits or prevent them from acquiring another bank. The board of directors is personally liable for any non-compliance situations, e.g., data security, privacy breaches. These risks and regulatory compliance requirements cause bank professionals to make vendor management a bank-wide issue.

Vendor management can yield additional value beyond reducing risk and meeting regulatory compliance requirements. Managing vendors – particularly IT vendors – throughout the life cycle of the relationship, can reduce costs, improve contract terms, increase the value the banks yields from each vendor and further reduce risk.

***“Everyone is afraid of getting a memo of understanding or a cease and desist order from the OCC” confesses a manager. “We got one and it limits whether we can buy other banks.”***

***“Smaller banks may not be able to afford the impact of these regulations.”***

In this study, banks estimated savings of 10-30% – without considering these additional cost savings and benefits. Typically, half of every IT dollar is spent with vendors. For a bank spending 6-12% of revenues on IT, reducing this expense is significant. A new case can be made for **Vendor Portfolio and Lifecycle Management** which plays an integrated and more strategic role, producing more value to the bank over time. While the dominant issue of “compliance, compliance, compliance” distracts some people from the value of better management of this mission-critical function, early adopters note that the game is changing. The potential return to the business from this strategic approach is far greater.

While most professionals have yet to analyze the possible savings from well-managed contract terms, lifecycle management, vendor accountability and contract enforcement, they intuit strong vendor management can improve business operations. They need help, however, in clarifying the true potential.

### **A Single Version of Truth**

To meet compliance requirements, it is critical to have “a single version of truth” among the disparate data sets, one which will stand the test of auditing with consistency and integrity. Centralizing the function of vendor management helps achieve this goal, but a software system that captures the data and business process is vital. A central data repository of vendor information and the business processes related to managing them allows for vendor categorization (e.g., critical/non critical), controls, performance measurements, compliance testing, reporting and other functions important to managing vendors and reducing risk.

### **Centralization**

Participants want their **enterprise vendor management** system to include a view across all vendors and all departments – IT and non-IT. Banks want all vendor management information stored within a single system and workflow.

In the process of centralizing, it is important not to lose sight of the specialized requirements for managing IT vendors. IT vendor management should be considered as a specialized activity led by IT and accountable to the corporate vendor management function – possibly a vendor management office (VMO) reporting to the CFO or CRO. The system of accountability for overall vendor management and data integrity to meet regulatory requirements should embrace the specific management requirements for **IT vendors**.

### **A New Approach: Portfolio Management**

Progressive CFOs, CROs, and IT executives are shifting their perspective about vendor management from a transactional view of selecting and initiating vendors to a strategic view of building and leveraging vendor value with full lifecycle management. This is particularly true of IT vendors, as it can be difficult and disruptive to terminate a vendor relationship once initiated. Executives look at vendors as a total portfolio to manage. This allows them to evaluate how to better balance risk within the entire portfolio, similar to the way financial and strategy professionals analyze business portfolios.

### **The Need for Tools**

Enterprise-wide vendor management is a relatively new category and IT vendor management is even newer.

***“The FDIC is increasing its focus on third-party vendor relationships. There is a need for better IT Vendor Management, better due diligence and increasing privacy requirements.”***

***“We look at compliance as a competitive advantage. It gives us the ability to grow through acquisitions of banks which are less compliant and it protects our reputation.”***

***“As soon as an application flickers, someone is on it.”***

***“OCC increases Vendor Management requirements around IT. For GLBA, we have to take a look at third parties and their access to information. If you have hundreds of vendors, how do you know who has access to the bank’s information? The vendors sign a contract that they won’t lose data, but that doesn’t protect banks from their bad internal practices. We have to audit.”***

While participants acknowledge IT vendor management is more complex than non-IT vendor management, most note few vendor solutions are available to help them account for the IT- specific management issues.

General vendor management software solutions for contract management, purchasing and ERM do not address IT vendor management needs. Systems optimized for purchasing and supplier management do not address the portfolio of vendors and balancing of risks. They do not categorize vendors based on criticality or allow for scoring performance criteria. They do not provide for on- boarding/off-boarding and “get well” processes for managing vendors’ delivery and execution of contract obligations. While they help compare terms from one contracting firm to another, they are limited for IT’s purposes.

While all bank professionals interviewed do vendor management today, room clearly exists for more effective, efficient methods.

On a scale of 1-10, the group surveyed rates its ability to meet regulations at an average of 8.3. Yet, they know they can do better. Within this sample, 52% do not have a centralized vendor management group. In fact, respondents have an average of fewer than three full-time people handling vendor management.

Absent holistic tools, 50% of these professionals currently resort to spreadsheets and homegrown solutions to manage their critical IT vendors. Couple this with the small IT staff available for vendor management and many costly vendor issues will go unnoticed.

#### **Potential Payoff**

Participants see potentially valuable payoffs from improving their vendor management. Efficient regulatory compliance and report management is one. Another is, quite simply, saving money. One company saved \$350,000 in three months as a result of rationalizing its vendors. In

general, participants believe they can save about 10-30% in vendor expenditures, although most of the participants have not formally analyzed the potential savings.

Neither have they budgeted to purchase a vendor management solution to achieve this savings. As the importance of vendor management escalates, budgets will need to increase to support it.

The value proposition also includes data integrity from a single version of truth, vendor cost savings based on a view across all vendors, the ability to monitor vendor commitments, reducing risk to bank reputation, and competitive advantage in the market.

#### **Trends Driving Change In Banks**

Participants note several emerging trends relative to IT vendor management today.

#### **New Accountabilities**

Banks must address new accounting and compliance obligations with the emergence of new and evolving regulations, e.g., SOX, FFEIC, GLBA, and OCC. These reporting requirements can impact a bank’s reputation with its customers, regulators and investors. The stakes are higher still, as banks unable to demonstrate reliable governance and compliance can be barred from accepting new deposits and from strategic acquisitions of other banks. “Everyone is afraid of getting a memo of understanding or a cease and desist order from the OCC” confesses a manager. “We got one and it limits whether we can buy other banks.”

The requirements pose a pressure for smaller banks with limited resources. “Smaller banks may not be able to afford the impact of these regulations,” cites a participant. Finding efficient, affordable ways to meet these requirements is valuable.

***“How big is IT vendor management as part of our overall risk profile? Big in the sense that everything goes through IT!”***

***“Of our critical vendors, 75-80% deliver a product or service to customers that impact on revenue streams and can cause customers to move.”***

***“One of the problems is that IT doesn’t want the line of business to sign a contract without IT being involved. We have 20,000 employees. If a senior vice president signs a contract, it’s legal, even if it happens outside of the normal process.”***

***“We are trying to centralize all contracts. The hard part is starting from scratch, finding out what and where all the contracts are.”***

***“Vendor management information is not in a centralized database. There is a duplication of effort.”***

***“With lots of subsidiaries, it’s hard to track vendors. They all talk to me separately – it is not coordinated.”***

Other participants seek tools and methods to assist them with compliance. One suggests: “The FDIC is increasing its focus on third-party vendor relationships. There is a need for better IT vendor management, better due diligence and increasing privacy requirements.”

Those who solve this challenge see an upside. “We look at compliance as a competitive advantage. It gives us the ability to grow through acquisitions of banks which are less compliant and it protects our reputation” acknowledges one participant. Finding effective ways to do this is an advantage.

### **Strategic Role of IT Vendors**

IT budgets within banks run as high as 25% of revenues today. Since banking services rely predominantly on IT-driven processes, IT’s impact on customers and service delivery is vital to the core business.

The investment in vendors to meet this need is robust. “Half of every IT dollar spent goes to vendors,” cites a respondent. “IT vendors include technology suppliers, consultants, contractors and service providers.”

“As soon as an application flickers, someone is on it,” notes a participant. “There are no applications, projects or services in which IT is involved that don’t have a complex supply chain required to deliver it,” acknowledges another.

Fully functioning vendor management is not about administration. It is about the business of *staying* in business. Bank representatives see vendor management as an enterprise-wide contribution to their overall business performance.

This is especially true in weighing business operational risk. As one professional puts it, “How big is IT vendor management as part of our overall risk profile? Big in the sense that everything goes through IT!”

First, banks realize one of the biggest risks is any privacy breach. Whether or not privacy and security clauses are in third-party contracts, data breaches are the bank’s responsibility. If the bank also provides third-party processing services, they must comply with SAS70 rules. And risk assessments for IT vendors are difficult. While IT vendors are few in number, they are a major source of risk. Assessments involve specialized expertise and involvement from IT and the lines of business. There is also a high level business risk in the enterprise risk management (ERM) process. IT vendor management feeds into ERM.

The growing practice of outsourcing IT functions to third parties in banks presents new challenges.

Managing privacy of customer data is one such challenge. The Graham Leach Bliley Act holds banks responsible for the way third-party vendors protect the privacy of their customers’ non-public information. A participant notes “OCC increases IT Vendor Management requirements. For GLBA, we have to look at third parties and their access to information. If you have hundreds of vendors, how do you know who has access to the bank’s information? The vendors sign a contract that they won’t lose data, but that doesn’t protect banks from their bad internal practices. We have to audit.”

Managing vendors without compromising compliance is also a factor. “Of our critical vendors, 75-80% deliver a product or service to customers that impact on revenue streams and can cause customers to move.” Mitigating this risk is a growing duty of IT managers.

As a result, evaluating costs and means for compliance for potential acquisitions becomes more complex. All of these emerging dynamics cause executives to now reconsider the scope and definition of IT vendor management for the future.

Consider the number of professionals involved in emerging compliance and risk business processes. Complexity and coordination call for more effective solutions. See **Figure 1**.

**What is IT Vendor Management?**

For organizations less attuned to these current dynamics, it could be easy to view IT vendor management as simply a part of contract management, purchasing or compliance reporting. Understanding the broadening role and value to the business requires a new perspective.

The new framework changes the current transactional view of selecting and initiating vendors to a strategic view of building and leveraging vendor value with full lifecycle management. Thinking about vendors as a total portfolio to manage helps evaluate how to better balance risk. Every vendor has overhead and some responsibility. A balanced number of vendors can improve administrative efficiencies.

A portfolio allows for better understanding of vendors by category, type, volume, and value. IT executives can improve consistency in governing processes and procedures, e.g., the on-boarding of contractors and consultants.

Full IT vendor management must address the IT vendor relationship across the complete vendor lifecycle. This includes traditional purchasing functions, contract management and enforcement, vendor accountability, enterprise risk management, governance and business continuity planning, as depicted in **Figure 2**.

With this understanding, participants discuss their broader need. “What we really need is to evaluate overall vendor effectiveness better. Are vendors performing the services well for the price? This needs to be done on a more comprehensive basis,” highlights one. “ITVM is more complicated than normal vendor

management,” notes another. “If we solve it for IT, then the same solution should work for non-IT, too.”

Considering the full view, the chain of IT vendor management rises to the top of a bank organization. The board of directors must consider compliance, risk management and efficiency for the organization. Yet, they do not have ready visibility into the mechanics of the IT vendor

management process. It is difficult for them to evaluate risks and opportunities if they receive only aggregated reports.

C-level executives need information to help with these increasing responsibilities. The CFO must address overall compliance and operational efficiencies. “Our CFO cares about meeting regulatory requirements as well as negotiating with and consolidating vendors,” notes a participant.

Similarly, the CRO must focus on enterprise risk management and reputation. “IT vendor management will be driven by internal audit and regulators. As CRO, it’s high on my list, especially in audit situations. You

have to be able to say to regulators that you have a comprehensive list of vendors,” mentions a participant. And, CIOs must address data security, business continuity, contract monitoring and enforcement.

Information to help each do their jobs is now increasingly important.

**Vendor Management Practices Today**

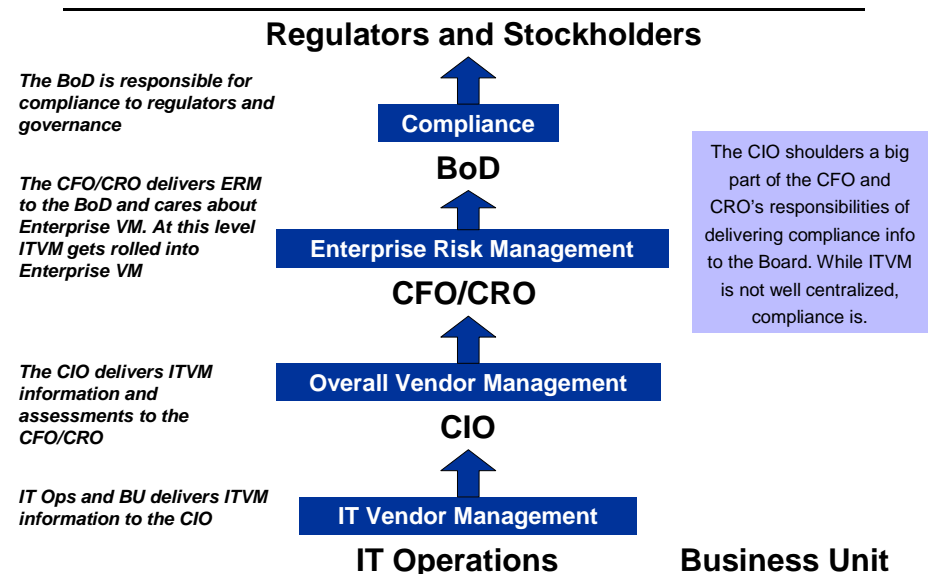
Overall, 61% of respondents believe IT vendor management is more complex than management of non-IT vendors. In part, this is because use of high volumes of vendors is pervasive: the average number of total IT vendors for this sample is 239, of which 33 are considered critical. Secondly, respondents lack a central control point for managing so many vendors.

Five other reasons respondents find IT Vendor Management difficult are:

- (1) **Cost.** The budget required to comply can be prohibitive. “If you look at this as only expense, there is no end to it. You would go broke if you did

**Figure 1**

**Many Groups are Involved in Compliance and Risk Assessment Activities**



everything the regulators ask you to do. Banks are leaving the business because they don't want to deal with compliance risk," comments a respondent.

Another concedes, "We outsource the SAS 70s and audits to Big 4 accounting firms. We spend millions with Accenture on compliance."

(2) **Lack of Centralization.** On a scale of 1-10, the average score for centralizing the IT Management function is only 5.7. Without central coordination for vendors, management is difficult. Participants share their frustrations.

- "Tracking 400-600 vendors is very hard without an automated system. A lot of people in different groups deal with regulatory requirements."

"One of the problems is that IT doesn't want the line of business to sign a contract without IT being involved. We have 20,000 employees. If a Senior Vice President signs a contract, it's legal, even if it happens outside of the normal process."

- "Vendor management information is not in a centralized database. There is a duplication of effort."
- "With lots of subsidiaries, it's hard to track vendors. They all talk to me separately – it is not coordinated."

While 56% of participants cite vendor consolidation is a business goal, 57% report it is not one of the top 3 priorities for their CIO.

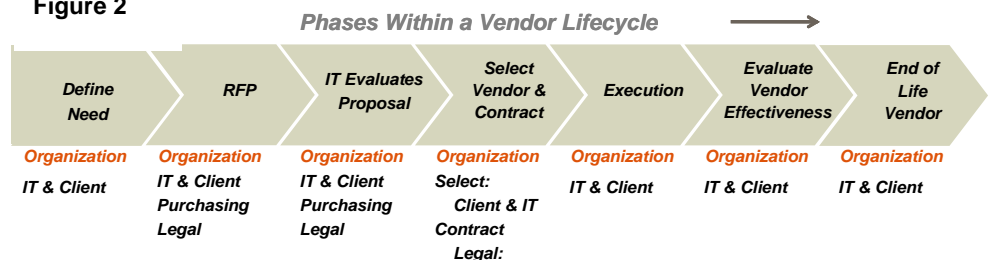
Vendor Management is typically led by IT, but is distributed across the CRO, CFO and business units. Without a unified view of vendors, it is difficult to identify the waste and inefficiency of the distributed vendor management process. "The information for vendor management, e.g., risk assessment results, renewal dates, alerts of key contract dates, are scattered all over the place. Contracts are on paper," reports a participant. Another person notes, "We are trying to centralize all contracts. The hard part is starting from scratch, finding out what and where all the contracts are."

With a distributed vendor management function, it is difficult to discern what banks are spending on this function. Decentralization also impairs "corporate memory" and leaves banks vulnerable, since there is no system for recording key operating facts often held in people's minds. "The part that fails is that whoever signed the contract has the most knowledge about it, especially around renewal. The owner leaves the organization (often due to reorganization) and the files go with him," a participant explains.

(3) **Compliance is Confusing.** Participants feel compliance is a "moving target." The focus for regulatory issues shifts, with IT infrastructure emphasized last year and information security the focus this year. "Each year, the regulators have a new hot button. Now, it's information security. There is still enough newness with information security and vendor management that folks are not sure what to do. What are the right things to do? What activities come first, second and third?" laments a participant.

These shifts drive up auditing costs. Respondents feel their banks need flexible systems and processes for dealing with regulatory uncertainties. Since no bank can afford to be completely compliant to a shifting target, banks need guidance in leading practices and a deeper understanding of how vendor management impacts on the overall enterprise risk management function. Comments one participant, "Regulators look for a beginning-to-end view of the vendor, issues not dropping through cracks, definition of risk, high-to-low ranking, asking the right questions, categorization based on risk, [and] follow-up on action items in the vendor management plan."

Figure 2



(4)

***“Each year, the regulators have a new hot button. Now, it’s information security. There is still enough newness with information security and vendor management that folks are not sure what to do. What are the right things to do? What activities come first, second and third?”***

***“IT vendor management will be driven by internal audit and regulators. As CRO, it’s high on my list, especially in audit situations. You have to be able to say to regulators that you have a comprehensive list of vendors.”***

***“The part that fails is that whoever signed the contract has the most knowledge about it, especially around renewal. The owner leaves the organization (often due to reorganization) and the files go with him.”***

**IT Vendor Changes are not Easy.** Participants feel it can be difficult to switch out IT vendors in the “continuous operation” environment of banks. Changing vendors can entail retraining staff in IT, operations and lines of business within the bank. It can also impact on the customer experience. Since few qualified vendors meet the technical requirements and information privacy needs of the banking industry, there is a limit to the number of vendors with which banks can actually work.

Furthermore, IT vendors are more integrated into the business processes. They are highly tied to the bank infrastructure. Migrating does not simply mean terminating a contract. For example, 50% of all financial compliance, e.g., SOX controls, resides in IT. Ensuring controls requires passwords, official change management procedures and proof of separation of duties for checks and balances. Vendors are deeply integrated into the many steps of these processes. IT has direct responsibility for establishing and ensuring programmatic support for compliance controls. A vendor switch implies time-consuming, systemic changes.

Vendor power is also increasing, as companies like Oracle consolidate the industry. Banks that do not manage their vendors will lose negotiating power and the ability to hold vendors accountable to their commitments.

**(5) IT’s Participation is not at the Front of the Process.** Traditionally, business units at banks initiate a new vendor relationship and bring IT to the table after the purchase decision. This makes IT Vendor Management difficult, because IT managers don’t know what is owned and cannot help optimize the terms and conditions of the offerings.

Also, IT vendors are interdependent, e.g., some applications are built on a specific technology stack, such as Oracle, Webshpere, J2EE, MSWindows. Since IT has more vendors in total than any single line of business, it has the balcony view of how to create practical vendor solutions.

IT is beginning to press for early involvement and approval of new solution purchases, especially if IT will be responsible for the on-going operation, maintenance and support of the solution. “IT wants to help the business units ask better questions about quality, quantity, time, cost, etc., when our company is contracting with an external vendor,” mentions a participant. While proactive input can improve the quality of decisions, it does require time and better information management of vendors and the business users to evaluate options.

***“Tracking 400-600 vendors is very hard without an automated system. A lot of people in different groups deal with regulatory requirements.”***

***“We want a centralized repository that everyone can use. IT and the rest of vendor management should use the same system. One version of truth is very difficult today because we have manual processes with multiple versions of the truth.”***

***“Regulators look for a beginning-to-end view of the vendor, issues not dropping through cracks, definition of risk, high to low ranking, asking the right questions, categorization based on risk, follow-up on action items in the vendor management plan.”***

***“In labor efforts alone, our initiative saved 20 full-time equivalents, who can now be directed to higher-value activities.”***

## **A Payoff**

In the main, respondents believe they can save their banks money by better managing vendors. Half of those interviewed estimate a savings of 10-20%. One respondent cited a savings of \$350,000 in three months as a result of rationalizing its vendors. The majority, however, have not analyzed this potential and are unsure of what the amount could actually be.

Since vendor spending commonly accounts for more than half of a bank's IT budget, this is an opportunity awaiting a solution.

IT executives require more support to analyze and realize this potential. To take advantage of this opportunity, banks must centralize information and secure more adequate tools and resources.

### **Creating an Effective Vendor Management System**

Participants note they would like to provide a unified system for recording and managing vendors across a vendor lifecycle. “We want a centralized repository that everyone can use. IT and the rest of vendor management should use the same system. One version of truth is very difficult today because we have manual processes with multiple versions of the truth!” exclaims a respondent.

### **Requirements for a Vendor Management Solution**

To help banks improve their vendor management, a sound solution includes five key elements:

(1) Institutionalize leading practices with a business process solution. This entails codified processes and a well-defined framework for a full vendor management lifecycle to manage the full maturity of vendor engagements.

(2) Provide a single version of the truth. Centralize the vendor repository and preserve knowledge and decision history in a master record system.

(3) Reduce risk of harm to reputation. Consistently assess vendors and ensure contract consistency to lower risk.

(4) Meet regulatory requirements at lower costs. Move Vendor Management from manual to automated workflows, e.g., distribute compliance testing, collect information and produce reports easily distributed to key executives and regulators.

(5) Create a portfolio view for vendor management, accountability and value. A holistic view of the overall use of vendors allows for better evaluation of vendor commitments, consistencies, internal effectiveness and efficiencies. It reduces redundancies and waste. Better visibility highlights opportunities for savings and better negotiations.

### **Early Adopters Are Making Strides**

To be sure, these steps can mean a dramatic cultural change within a bank. Shifting the focus from vendor management's value for compliance support to operational effectiveness and business performance improvement requires internal communication and understanding. Early adopters interviewed report the success of this shift is largely tied to a proactive communication process about culture change within their organizations.

Early adopters are making progress. “We were doing separate risk assessments. Now, we are able to combine them into a single risk assessment. Our information security and IT risk assessments are now combined,” notes a respondent. Another person offers, “We manage all vendor relationships, all contracts: IT and non-IT now. Everything gets documented in a single system. We

## Vendor Management in Banks

track vendor due dates, performance and notes of meeting with vendors.”

These early adopters report significant benefits from their efforts. One is a more efficient overview of regulatory compliance, which helps reduce compliance costs as workflows are automated. This produces faster, more effective responses to compliance requests. “Vendor management is easier because we now have a process. Regulators are now happy,” comments a respondent. A second benefit is overall improvement in

contracts management as redundant vendor contracts are eliminated.

Another benefit is greater visibility into vendor activities and processes. “We gained visibility and the ability to communicate IT priorities effectively and share accomplishments and challenges with various stakeholders. This improves IT’s credibility as a business partner,” notes a participant. This visibility creates more informed and empowered business and IT managers.

Another plus reported is better management of the project portfolio. “By leveraging an IT vendor management solution, our CIO and his team are eliminating silo-based compliance management and automating manual processes. More importantly, we have complete visibility into compliance status and can shift resources to the areas that need the most attention,” offers a manager.

Better financial management and costs savings are benefits, too. “In labor efforts alone, our initiative saved 20 full-time equivalents, who can now be directed to higher-value activities,” a respondent notes. Creating transparency about IT vendors empowers employees with the information to make smart investment decisions that improve operational performance.

A respondent notes his project selection and resource allocation are better aligned with the bank’s business objectives. “We are achieving our goal of IT management clarity, simplicity, stability and granularity. With these goals, we will have the agility and adaptability necessary in our fast-moving, constantly changing investment banking industry. We are making the important measurable, not the measurable important. We are commercializing IT.”

## Conclusion

While compliance requirements have elevated the importance of vendor management to banks today, its real value lies in understanding the role it plays in improving operational efficiency and effectiveness.

The early adopters show there is a strong reward for the pursuit of an enterprise-wide, well planned vendor management system.

CFOs, CROs, and IT executives who make it a priority to take full advantage of this opportunity will reap this significant payoff.

## About The FactPoint Group

*The FactPoint Group* is a Silicon Valley research and consulting firm that helps its clients improve their businesses by intelligently adopting new technology solutions. For more information, visit [www.factpoint.com](http://www.factpoint.com) or call Larry Gordon at 650.400-6818.

## Study Sponsor:

ITM Software  
2880 San Tomas Expy  
Suite 110  
Santa Clara, CA 95051  
Main: 408.764.7500  
[www.itm-software.com](http://www.itm-software.com)