



**CENTER FOR
INFORMATION
SYSTEMS
RESEARCH**

**Sloan School
of Management**

Massachusetts
Institute of
Technology

Cambridge
Massachusetts

**PFPC: Building an IT Risk
Management Competency**

**George Westerman and
Robert Walpole**

April 2005

CISR WP No. 352 and Sloan WP No. 4549-05

© 2005 Massachusetts Institute of Technology. All rights reserved.

- Research Article:** a completed research article drawing on one or more CISR research projects that presents management frameworks, findings and recommendations.
- Research Summary:** a summary of a research project with preliminary findings.
- Research Briefings:** a collection of short executive summaries of key findings from research projects.
- Case Study:** an in-depth description of a firm's approach to an IT management issue (intended for MBA and executive education).
- Technical Research Report:** a traditional academically rigorous research paper with detailed methodology, analysis, findings and references.

CISR MISSION

CISR was founded in 1974 and has a strong track record of practice based research on the management of information technology. As we enter the twenty-first century, CISR's mission is to perform practical empirical research on how firms generate business value from IT. CISR disseminates this research via electronic research briefings, working papers, research workshops and executive education. Recent and current research topics include:

2003 PROJECTS

- Business Models and IT Investments
- Governing IT for Different Performance Goals
- Assessing Architecture Outcomes
- Infrastructure as Variable Cost
- Managing IT Related Risks

2004 PROJECTS

- Assessing the Performance of Alternative Business Models
- Managing the Next Wave of Outsourcing
- Managing IT Architecture for Business Value
- Measuring IT-driven Risk
- Exploring the Role of the IT Unit in Leading IT-enabled Change

Since July 2000, CISR has been directed by Peter Weill, formerly of the Melbourne Business School. Drs. Jeanne Ross, George Westerman and Nils Fonstad are full time CISR researchers. CISR is co-located with MIT Sloan's Center for e-Business and Center for Coordination Science to facilitate collaboration between faculty and researchers.

CISR is funded in part by Research Patrons and Sponsors and we gratefully acknowledge the support and contributions of its current Research Patrons and Sponsors.

CONTACT INFORMATION

Center for Information Systems Research
MIT Sloan School of Management
3 Cambridge Center, NE20-336
Cambridge, MA 02142
Telephone: 617/253-2348
Facsimile: 617/253-4424
<http://web.mit.edu/cisr/www>

Peter Weill, Director	pweill@mit.edu
David Fitzgerald, Asst. to the Director	dfitz@mit.edu
Jeanne Ross, Principal Res. Scientist	jross@mit.edu
George Westerman, Res. Scientist	georgew@mit.edu
Nils Fonstad, Research Scientist	nilsfonstad@mit.edu
Jack Rockart, Sr. Lecturer Emeritus	jrockart@mit.edu
Chuck Gibson, Sr. Lecturer	cgibson@mit.edu
Chris Foglia, Center Manager	cfoglia@mit.edu
Julie Coiro, Admin. Assistant	julieh@mit.edu

CISR RESEARCH PATRONS

BT Group
The Boston Consulting Group, Inc.
DiamondCluster International, Inc.
Gartner
Hewlett-Packard Company
Microsoft Corporation
Tata Consultancy Services—America

CISR SPONSORS

Aetna Inc.
Allstate Insurance Co.
American Express Corp.
AstraZeneca Pharmaceuticals, LP
Banknorth, NA
Biogen Idec, Inc.
Campbell Soup Company
Care USA
Celanese
ChevronTexaco Corporation
Det Norske Veritas (Norway)
Direct Energy
eFunds Corporation
EMC Corporation
The Guardian Life Insurance Company of America
ING Group
Intel Corporation
International Finance Corp.
Merck and Company
Merrill Lynch & Co., Inc.
MetLife
Mohegan Sun
Motorola, Inc.
National Kidney Foundation, Singapore
Nomura Research Institute, Ltd.
Pasco County, Florida
Pfizer, Inc.
PFPC, Inc.
Raytheon Company
State Street Corporation
Telenor ASA
TRW Automotive, Inc.



Title: PFPC: Building an IT Risk Management Competency

Author: George Westerman and Robert Walpole

Date: April 2005

Abstract: IT Risk management is becoming increasingly important for CIOs and their executive counterparts. Educators and managers have materials they can use to discuss specific IT risks in project management, security and other risk-related topics, but they have few resources they can use to have a holistic discussion of enterprise-level IT risk management. This case is intended to address the gap. It describes the IT risks facing a large financial services firm, PFPC, as a result of rapid growth, a large merger and distributed management of the IT function. The firm's first enterprise-wide CIO, Martin Deere used risk management as a key pillar in a major revamp of the firm's applications and IT capabilities. The case is rich in detail on the firm's IT risks, the new risk management process, including examples of the firm's risk management tools. It also describes early lessons and outcomes in the implementation of risk management capabilities. The case has enough richness and potential controversy to engage students from the undergraduate through executive levels in an informative and interesting discussion of IT risk management.

Keywords: IT risk management, IT governance, IT architecture, IT transformation

13 Pages



Massachusetts Institute of Technology
Sloan School of Management

Center for Information Systems Research

PFPC: Building an IT Risk Management Competency

Introduction

Michael Harte, Chief Information Officer (CIO) of PFPC, was apprehensive. Starting tomorrow, the US Federal Reserve (“the Fed”) would begin a three-week on-site review of all information technology (IT) applications, infrastructure and management processes at his firm.

Previous external reviews done just after he joined as PFPC’s first corporate CIO had identified numerous issues in PFPC’s IT organization and portfolio. Harte had used these audit findings as a spur for taking action. He had initiated a wholesale restructuring of the firm’s IT organization and systems, which was underway.

Now that Harte had been CIO for 18 months, any audit findings would reflect on his management, and potentially jeopardize his change initiative or his credibility. While PFPC had made great progress, there was still a long way to go. As he drove home, Harte reflected on PFPC’s IT assets and his organization’s risk management capability.

Background

PFPC provided a wide range of processing services to the investment management industry (see Figure 1 for overview of PFPC and its parent, PNC, and Figure 2 for financial highlights). With US\$1.7 trillion in assets under management, PFPC was one of the largest full-service transfer agents and providers of mutual fund accounting services globally. PFPC provided a number of other financial services to corporate clients, including custody, sub-accounting, integrated banking transaction services, securities lending and alternative investment services. PFPC was a subsidiary of PNC Financial (PNC), a very large regional commercial and retail bank.

PFPC had grown rapidly over the past 30 years, moving quickly to launch new services and enter new regions as opportunities arose. To provide maximum focus and flexibility, each line-of-business (LOB) was organized under its own managing director (MD). The MD had control over all aspects of the business, including sales, back-end processing and IT functions.

This case was prepared by Dr. George Westerman of the Center for Information Systems Research at the MIT Sloan School of Management and Robert Walpole of the Sloan MBA Class of 2003. This case is for the purpose of management education, rather than illustrating or endorsing any particular management practice. This case may be reproduced free of charge for educational purposes provided the copyright statement appears on the copy.

The authors would like to thank Michael Harte, Kwafu Ofori-Boateng and all of the other PFPC employees who participated in the development of this case.

PFPC's growth in the 1990s was driven largely by a rapid increase in financial market activity. Increasing numbers of investors, providers and transactions increased the need for PFPC's services. Another driver of growth was the Y2K problem. Many financial services firms chose to outsource fund processing operations to PFPC rather than address Y2K issues in their own legacy systems and processes.

The recession of 2001, combined with the end of the Y2K era, reduced PFPC's growth from its high levels of the late 1990s. As a result, PFPC management refocused its strategy from high growth to intensive streamlining and cross-selling. Unfortunately, PFPC's legacy systems were not positioned to support these changes. They were dated, monolithic, not well documented, duplicated across silo applications and predominantly mainframe based. The applications were increasingly difficult to modify in response to new business or regulatory requirements.

One IT executive summarized the situation this way:

"In the late 90s, accounts were growing exponentially... We had no time to look internally at rationalization or architecture. We grew our customer base through acquisition. We'd do the barebones, integrate the general ledger, make sure the networks could talk to each other and then move on to the next thing.

In 2000 and beyond, market growth slowed down. All of a sudden, we're not acquiring, we're protecting current accounts. That's when we saw all these legacy problems, the problems of yesterday that we're dealing with today."

PFPC's new strategy had important implications for IT. The need to streamline meant that IT had to help the firm cut corporate costs while maintaining traditionally high levels of service quality. At the same time, the need to cross-sell meant that PFPC needed to extend its existing services, such as adding multi-currency features

to enable international expansion, and improving client self-service capabilities.

PFPC's senior executives recognized that the new focus on cost cutting and service quality would require radical changes in the way PFPC managed its information technology. One of their first steps was to hire Harte as the company's first corporate CIO.

Harte's mandates were to reduce IT spending (from 32% to 24% of total expenses) and resolve the jumble of monolithic legacy systems that had evolved during the company's period of rapid growth.

"When I got here, I saw the need to position information technology as a business center that would enable the company to move from being focused on back office processing to being a leader in solution integration and information products. The first stage in that transformation was to bring greater discipline to risk management and governance as the foundations for change."

PFPC rapidly restructured the IT organization so that all IT leaders reported in a 'dual solid line' arrangement. Harte had supervisory control, with input from each LOB unit head. LOBs kept their own IT budgets, with 33% of total enterprise IT budget allocated centrally.

A newly-created corporate IT organization had responsibility for management oversight and shared services. This organization, built mostly through internal promotions, rapidly implemented centralized management processes in seven key areas of IT: Architecture, Security, Service Delivery,¹ Strategy, Finance, Human Capital and Methodologies. Initial efforts included adopting a corporate risk management process, eliminating duplicative project methodologies across the organization and establishing a vendor management capability. Additionally, the firm moved to consolidate and outsource

¹ Service Delivery encompassed functions traditionally called IT Operations. The name change was intended to focus employees and customers on IT's role as a service provider.

helpdesk, network and data center functionality to the corporate parent.

Transforming PFPC's Applications

PFPC's IT executives believed that incremental changes to the current architecture could not possibly deliver either the overall cost structure or the componentized web service-based innovation that PFPC needed to compete in a rapidly consolidating global financial services market. To meet business demands to streamline operations and provide a unified face to the customer, PFPC announced the Global Enterprise Platform (GEP) initiative.

GEP began with a three-pronged approach to establish a long-term strategic plan, set out the architecture for a unified technology platform, and cultivate a high performance staff culture. These initial steps set the stage to completely revamp PFPC's IT infrastructure and applications, including:

- Rationalizing the number of processing engines and applications;
- Restructuring the legacy application portfolio;
- Componentizing and creating open interfaces to legacy code;
- Unifying the architecture across a single platform;
- Designing new customer-facing applications;
- Creating a single portal through which customers could access PFPC services.

The multi-year GEP effort, begun in 2003, would be achieved through a staged series of implementations. New business initiatives would play double duty by both delivering new functionality and removing complex legacy applications. Simultaneously, IT would use an Enterprise Shared Services approach to create critical infrastructure and support components, such as a single sign-on capability, that other initiatives could build upon.

In the words of a senior IT manager,

"So, that's the new aim for the company. We're trying to get the company streamlined and aligned, with proper controls in place, so that when the market changes in six or 12 or 18 months, we're ready to pick up and run with it again."

IT-Related Risks at PFPC

Awareness of risk in the financial services industry had increased dramatically due to corporate failures (such as Enron and WorldCom), terrorist attacks and scandals among Wall Street firms. Legislation such as the USA Patriot Act and Sarbanes-Oxley increased the regulatory burden. Financial services firms felt even greater pressure as the success of the industry was highly dependent on the trust of the public.²

Increased awareness of risk was reflected in increased attention from regulators. PFPC was subject to regulatory scrutiny from many angles, including financial market regulators (US Securities and Exchange Commission), banking regulators (the Fed), and even customers and their auditors.³ Recent financial reporting corrections at PNC combined with recent regulatory audit findings at PFPC to intensify the scrutiny.

As a high-volume financial services firm, all aspects of PFPC's business were highly dependent on IT. Consequently, PFPC's ability to manage IT-related risks had an important influence over the enterprise risk of the business. Due to its role as a provider of critical services to other financial services firms, any operational or regulatory difficulties at PFPC could affect its clients' processes, its clients'

² Because the whole financial industry relies on trust, regulatory or other issues affected more than the offending party. For example, the repercussions of some mutual funds allowing after-hours trading impacted not only the guilty firms, but also the industry as a whole.

³ PFPC's business required a layer of risk management beyond managing its own risks. Since PFPC's activities were an integral part of its clients' processes, PFPC had to not only certify its own processes, but also help clients certify their own processes.

customers and even the whole financial services industry.

To manage both internal and external pressures, PFPC executives increasingly focused their attention on risk management. They wanted to understand the extent of each enterprise risk the firm faced. Furthermore they needed to clearly articulate how IT influenced PFPC's enterprise risks. Harte recognized this as an opportunity to make risk management an integral part of his efforts to restructure PFPC's IT assets and organization.

PFPC's IT risks in 2003 included the following:

Business Resiliency Risks

Events such as 9/11 made it apparent that business resiliency was an issue that permeated all of PFPC's activities. PFPC IT managers quickly came to the conclusion that their backup facility was too close to the main data center. Moving the backup center would reduce the risk of a single incident affecting both data centers.

PFPC was also charged by the Federal Reserve with identifying which of their processes were critical to the National Financial Infrastructure (NFI), meaning that they were essential to smooth functioning of the nation's monetary and banking system. Anything that was NFI critical required strong resiliency protection.

As part of its resiliency assessment, PFPC analyzed its IT relationship with the parent company. PFPC had recently outsourced most of its IT infrastructure (including Desktop, Network and Data Center Services) to the parent, and a number of risks had not yet been resolved. Using audit findings and internal analysis sessions, IT was able to identify 31 risks in this area. The IT organization obtained funding to address the most important risks in the latter half of 2003. Other risks would be resolved in the next two years or would be bundled into new business initiatives as the opportunity arose.

Strategic change risks

The GEP initiative was critical for the corporation but entailed numerous major risks.

New systems could be delivered late or customers could experience disruption during the transition to new applications. In addition, internal organizational or process changes could disrupt sales or increase staff turnover. Any of these could damage PFPC's reputation, reducing its ability to attract or retain customers. According to PFPC's Chief IT Architect Per Gyllstrom,

"GEP is about more than just cost savings. It also has to rapidly provide clients new capabilities to perform activities they could never do before. This transition must be seamless and smooth or the clients will go somewhere else.

What we were looking for was a gradual but complete modernization of our systems over time. That's a big deal. Our clients' core business solutions are on systems that we're now going to modernize. There has to be a huge incentive for the client to follow GEP, and we need to make this journey attractive and smooth. Otherwise a client might say, 'Oh, that's a good opportunity to check other alternatives out, too. If you're going to force me to change, maybe I should look for someone completely different from you.'"

PFPC took a holistic approach to reducing GEP risk by examining risk-management activities in all seven elements of IT. IT staff simultaneously began to improve project and program management capabilities, implement architectural standards and review processes, plan for future human capital requirements, and formalize financial management.

Any proposed business initiative was formally reviewed for all types of IT risk. Then, if approved, the project was followed closely to ensure all technical and human capabilities were in place, change management risks were being addressed, and the project was on time and on budget. The combination of initial review and frequent revisiting aimed to catch problems

early and address them before they became large.

Human Capital Risks

PFPC needed to ensure that it would have the right skills on hand for GEP and for the future. The current IT staff's programming skills were geared more toward mainframe application maintenance than to application development using modern IT tools such as web services.

Meanwhile, PFPC also needed to keep a talented, motivated workforce focused on existing applications and infrastructure. It could not afford to lose vital functional capability and intellectual capital for systems that had not been well documented.

In consultation with each IT element owner, PFPC's Human Resources (HR) organization helped to define and implement a human capital risk management process. They began to regularly monitor the extent of turnover and the length of time job postings were open. They also used compensation surveys to keep employee compensation on par with peers in the industry and the region. The goal was to have some turnover to prevent complacency among employees, but not so much that it hurt morale.

PFPC's IT executives believed that succession planning was the next HR risk to address. The firm needed processes to proactively identify good candidates. They needed a way to ensure that high-potential employees were properly motivated and developed so that they could grow within the company. Additionally, they needed plans to mitigate the risk of key IT employees leaving the company.

Use of Outside Vendors

Another major risk the company faced was that of vendor management. In the past, PFPC had primarily relied on individual consultants to provide specific skills in IT. As a skill was needed, PFPC hired a talented individual to provide it. When the skill was no longer needed, the relationship could be ended easily. While this approach provided flexibility to PFPC's application development process, it entailed

risks. For example, one of PFPC's mission-critical applications was dependent on a component that was proprietary to a two-person consulting firm. If the consulting firm went out of business, or if the relationship soured, PFPC could be unable to maintain the code.

PFPC was considering larger outsourcing deals, including offshore development. However, until recently, IT did not have a formal vendor management process. PFPC did not negotiate firm-wide contracts with preferred vendors or monitor vendor performance firm-wide. As a result, different LOBs tended to negotiate different terms with the same vendor without IT involvement. Individual LOBs' experiences with a particular vendor were not shared across the company.

PFPC began to manage vendors more closely. By mid-2003, 250 independent contractors had been managed out of the organization and a list of 110 vendors had been pared to ten. A Vendor Management Office (VMO) was being built to pre-select and screen vendors, as well as monitor vendor costs and performance. It tracked the vendors being used across the organization so that people in one business unit could benefit from the experience of other business units. The VMO also initiated a reverse auction process to keep costs low: pre-qualified vendors would bid on contracts, with the lowest-priced vendor winning the business.

PFPC was not using offshore outsourcing because there was considerable internal debate over its benefits and risks. Contracting for services in low-wage countries could increase flexibility, since PFPC could redirect savings in application maintenance toward more strategic application development projects. On the other hand, it could be difficult to ensure tight-knit collaboration on service and system requirements across thousands of miles. In addition, sensitive information would potentially be located outside the borders of the United States, and PFPC could lose critical IT expertise to the outsourcer.

New Regulations

PFPC faced a substantial burden of new regulatory requirements. The USA Patriot Act, passed in the wake of September 11 terrorist incidents, required all financial institutions to track customer transactions and identify suspicious activity. In addition, Sarbanes-Oxley, passed following a wave of notable corporate failures, required PFPC to certify the accuracy of its financial data and the integrity of its processes and internal controls.

PFPC was affected by these regulations in two ways. First, it needed to ensure that it was in compliance for its own processes. Second, as a provider of services to other firms, PFPC was audited by its customers as part of their own certification processes.

Information technology was an important component of the firm's ability to comply with the new regulations. As one corporate executive noted,

"[We] do not have the ability today to gather the information that the regulatory guideline requires for us to be able to report to the Office of Thrift Supervision and the SEC about specific customers doing inappropriate things."

Sarbanes-Oxley's requirement that executives personally certify processes and controls was an important risk that PFPC felt it had not yet mitigated completely. Auditors and regulators were requiring firms to demonstrate consistent processes and solid documentation of process steps and outcomes. PFPC managers realized they needed a better understanding of current processes embedded in the IT portfolio. In addition, system development processes needed to change so that new applications met requirements for internal controls, audit trails and security. PFPC was addressing the issue as part of developing its management processes in all elements of IT.

Security Risks

Controlling and tracking user access to systems was a critical source of IT risk. As employees

changed jobs, it was very difficult to determine who should have access to the various parts of each system. The situation was exacerbated as PFPC began to grant customers access to the network. In addition, with a large number of applications, each user had many passwords to remember. Users changed their passwords infrequently and, in some cases, wrote them down on their desks or terminals. Finally, it was difficult to verify that IT managers were consistently enforcing security policies across applications and regions.

PFPC was considering the implementation of identity management. With this capability, frequently called "single sign-on," each person would have a single UserID that could access all information to which she was entitled. Implementing this capability would be a difficult task at PFPC, given the complexity of the firm's IT architecture.

Aligning IT and Business

In PFPC's decentralized organizational culture, it was often difficult to ensure that systems simultaneously met the requirements of LOBs and Corporate IT. LOB chiefs demanded fast system implementation to meet a customer or market need. They often resisted enterprise thinking if it required a change to their preferred vendor or required additional work to utilize existing enterprise infrastructure or applications. In order to address this problem, Harte created a "dual solid line" reporting relationship structure for IT. Each Business Information Officer (BIO), as the head of each LOB's IT group, reported both to the LOB president and to the corporate CIO. This arrangement helped to ensure that the BIO considered both enterprise and LOB needs when implementing applications.

The IT Risk Management Process

IT risk management was part of the overall corporate risk management process. PFPC had implemented an enterprise risk management process for its LOBs about 18 months earlier. Enterprise level risk was the purview of the corporate Risk Management Committee (RMC),

which consisted of the firm's top executives in charge of each LOB. Sue Keller, the corporate risk officer reporting to the CEO, worked with the Managing Director of each LOB to identify and prioritize risks in his or her area. She produced an LOB risk report and also rolled up the LOB risks into a corporate-level risk report (see Figure 3 for an enterprise-level risk summary and Figure 4 for a summary-level listing of IT risks). Risks were discussed at RMC meetings before being forwarded to the PFPC board and the parent company's risk management committee.

While the RMC had responsibility to discuss and prioritize key risks, neither it nor Keller had responsibility for mitigating each risk. Instead, each risk was the responsibility of the LOB to which it applied. Keller's role was to create and coordinate the enterprise risk management process, but not to mitigate risks.

In late 2002, the RMC expanded to include IT. In response, Harte created the Technology Risk Management Committee (TRMC). This oversight forum met monthly to track IT-related risks, communicate risk-related issues and recommend investment to resolve risks. IT risks were summarized and submitted to the corporate RMC, where IT risks were discussed alongside risks from each LOB or major function.

PFPC leveraged the expertise of its parent company when implementing its IT risk management capability. Kwafo Ofori-Boateng, originally from PNC's IT group, became a deputy to Harte, with responsibility to implement and manage the risk management process.

Working with the element owners and other IT managers, he modified and extended the PNC framework and processes so that they worked in the PFPC context while still meeting the requirements of PNC's risk management process (see Figure 5 for an overview of PFPC's risk management governance structures).

"PNC had some good processes, but we couldn't use them directly. We're a financial services provider, not a bank. We integrate differently with our

customers, and our volumes and time frames are different. We even have different regulators. Plus we needed to make the processes work in the PFPC culture—it was a lot of work.

The PFPC IT risk management framework classified risks into categories that matched the seven IT elements. As a first step in the process, each element owner periodically identified element-related risks across LOBs. Some risks were identified from internal and external audit findings. Others were identified through brainstorming sessions in which element owners and their staffs examined failure modes for each process.

Additionally, the IT unit forged closer relations with existing corporate functions such as internal audit, compliance, and human resources. These relations helped to identify existing risks and see emerging ones on the horizon.

Risks were also identified at project initiation. Projects that exceeded a size threshold were required to complete the Key Business Initiative (KBI) process. In addition to describing the business case, the KBI documents contained a standard checklist of IT risk factors. Each proposed initiative was reviewed by IT elements to ensure that architecture, methodology and other guidelines were being followed (see Figure 6). Any issues or exceptions were recorded as risks to be managed over time. Chief IT Architect Gyllstrom described the process this way:

"As part of our reviews, we end up performing risk assessments of current projects. Identified risks are tracked and managed through the risk management program.

But we do more than just review projects. We proactively get involved with projects long before the review, providing architecture and design consulting. That's because I don't want to be one who just passively sits in a chair saying, 'No, that didn't work. Try something else.'"

The IT group took its risk identification duties seriously. Whereas some managers might have been nervous about documenting each risk, PFPC executives were of the opposite opinion:

“If we’re aware of risks, we can do something about them. It’s the ones I don’t know about that worry me.”

Every risk was recorded and tracked in a newly-developed Technology Risk Management (TRM) database (see Figure 7). For each risk, element owners assigned a status (red, yellow, green), mitigation plan, expected resolution date, and risk owner. The TRM database enabled centralized tracking, trending, and reporting for all of PFPC’s IT risks.

Issues in the IT Risk Management Process

PFPC recognized a number of areas for improvement in its risk management process and capabilities. As of mid-2003, nine months into the introduction of the TRM process, the level of detail was a major issue. PFPC’s TRM database had more than 300 open entries. There were more than 30 identified risks in the area of networks alone.

There was no process to identify what level of risk made it into the reports, or to consistently assess the potential impact of a risk. Some managers reported very detailed risks, while others reported risks at too high a level.

Each risk was assessed as high, medium or low (red, yellow, green) priority by its assigned owner, based on his/her own analysis. People with different perspectives or risk tolerances tended to rate risks very differently. Some element owners convened teams to ensure that risk assessment was done consistently within their elements, but it remained difficult to ensure consistency across the seven IT elements.

The inconsistencies made it difficult to report on or prioritize among risks. The periodic rollup of IT risks prior to RMC meetings required a great deal of manual intervention and judgment, but still did not effectively communicate IT’s risk status. One senior IT manager stated:

“There’s too much detail. Many of the items in the TRM database would be better classified as action items or task-level project issues rather than corporate IT risks.”

We’re overwhelming Michael Harte and, as a result, he goes into the corporate risk meetings feeling like he’s not adequately prepared to fight for a few key risks.”

Accordingly, Ofori-Boateng worked with the element owners to develop consistent definitions of task, project, and program. The group also created a regular process of review and escalation. Every two weeks, element owners went through all risks in the database and rolled them up to their respective risk element category. These issues were then filtered through the TRM committee process to produce summary status reports that Harte could use in meetings with his staff and the RMC (see Figure 8).

Another issue was the focus of risk identification activities and communicating the purpose of risk management. Reviews of new initiatives tended to focus on implementation-related risks, rather than the effect of the initiative on the firm’s overall risk profile. In addition, although risks in several IT elements, such as architecture and methodology, had enterprise-level implications, these implications were not made clear. Consequently, some business unit leaders saw the reviews as a way of forcing compliance to subjective rules rather than as a way to improve the enterprise’s risk profile.

Another area for improvement was to embed risk analysis into all of the firm’s IT management processes. Risk management was already embedded into many points of the project demand management process (see red circles in Figure 6). However, the IT unit wanted to extend this into all other IT management processes.

In addition, IT executives saw the need to improve compliance with existing IT risk policies. They wanted to ensure that every

project went through the same assessment and mitigation process and was regularly monitored, so that IT could view project-related risks holistically.

Finally, PFPC realized a need to create an open dialogue about risk between the IT group and the rest of the decision makers within the company. Risk reporting needed to move from a defensive listing of risks to a more proactive use of risk information in managing the business. The IT management team felt this was an important goal, but one which would be difficult to reach until the company developed more comfort with risk management. In the words of one IT executive, this was an ongoing process:

“Processes such as internal audit and the implementation of a TRM process raise the awareness level. I don’t think we’re there today, but I think we’re headed in the right direction. Michael’s driving that process by creating the culture and educating people so that they’re thinking about risk and making sure it’s being included in decisions.”

Conclusion

Harte had much to think about as he traveled home for the evening. The Federal Reserve review of IT, which would begin tomorrow, was an unfamiliar exercise. The Fed was an outside

agency concerned with today’s reality, not tomorrow’s promise. Its findings had important implications for PFPC’s ability to gain and keep customers.

In the past 18 months, PFPC had changed its IT processes significantly. The IT group had worked hard to build a risk management competency in IT, seeing it as a lens for improving IT management in general.

PFPC’s senior executives were fully behind Harte’s efforts to change IT capabilities. However, while Harte and his team had made great progress in establishing IT risk management, real changes in the application portfolio would take longer to achieve. The future of the company depended on an effective and uneventful GEP transformation.

In thinking about the Fed review, Harte was cautiously optimistic, but he couldn’t help wondering: Had he and his staff missed anything important? Would the Fed focus on PFPC’s existing IT risks, or on its risk management capability? Would they believe that the Global Enterprise Platform transformation was a manageable risk? What else should PFPC be doing to improve its IT risk management capability?

He would find out starting tomorrow.

Figure 1: PFPC / PNC Overview

PNC Financial	PFPC
With \$14B Market Cap and \$70B in assets, PNC Financial Services Group is one of the nation's largest diversified financial services organizations.	PFPC provides Investor and Securities Services to many of the world's leading financial services firms. The firm has approximately \$1.7 Trillion in assets under administration.
It provides a full range of financial services including: <ul style="list-style-type: none"> ▪ Consumer banking; ▪ Wholesale banking, including corporate banking, real estate finance and asset-based lending; ▪ Wealth management; ▪ Asset management; and ▪ Global fund services. 	Major business lines include: <ul style="list-style-type: none"> ▪ Mutual Fund accounting and subaccounting; ▪ Transfer agency; ▪ Custody; and ▪ Securities lending.
2003 revenue was \$5.3 Billion.	IT spends approximately \$200M annually, and has 1050 staff.
	IT management is complicated by: <ul style="list-style-type: none"> ▪ Integration of \$1.3B acquisition of First Data ISG; ▪ 12 lines of business; ▪ Significant reorganization underway; and ▪ Simultaneous transformation of legacy IT applications and infrastructure.

Figure 2: Selected Operational and Financial Performance Highlights for PFPC

	<u>2003</u>	<u>2002</u>	<u>2001</u>	<u>2000</u>	<u>1999</u>
INCOME STATEMENT					
Operating revenue	762	817	846	674	264
Operating expense	618	650	644	501	184
Earnings	61	65	36	47	45
PFPC earnings as a % of total parent earnings	6.1%	5.5%	9.5%	3.7%	3.6%
BALANCE SHEET					
Average Assets	1909	1888	1771	1578	308
PERFORMANCE RATIOS					
Return on assigned capital	29%	31%	17%	22%	40%
Operating margin	21%	23%	17%	21%	30%
OTHER INFORMATION					
Average Number of Employees (Full-time-Equivalent persons)	5081	5834	5737	NA	NA
SERVICING STATISTICS (as of Dec. 31)					
Accounting / Administration assets (\$Billions)					
<i>Domestic</i>	622	481	514	454	NA
<i>Foreign</i>	45	29	21	9	NA
<i>Total</i>	667	510	535	463	412
Custody assets (\$Billions)	401	336	357	437	388
Shareholder accounts (millions)	53	51	49	43	34

These figures were excerpted and summarized by the authors from PNC annual reports. All numbers are in US\$Millions, except where noted otherwise.

Figure 3: Enterprise Level Risk Summary⁴

2004 Risk Assessment Matrix						
	Credit	Market	Liquidity	Operational	Comp/Legal	Strategic/Rep
High				<input type="checkbox"/> ✓ <input checked="" type="checkbox"/>		
Moderately High						<input type="checkbox"/> ✓
Moderate					<input type="checkbox"/>	<input checked="" type="checkbox"/>
Moderately Low					<input checked="" type="checkbox"/> ✓	
Low						
Inherent Risk Trend				Stable	Stable	Stable
Risk Management Assessment				Satisfactory	Satisfactory	Satisfactory

2003 Risk Assessment Matrix						
	Credit	Market	Liquidity	Operational	Comp/Legal	Strategic/Rep
High						<input type="checkbox"/> ✓
Moderately High				<input type="checkbox"/> ✓		<input checked="" type="checkbox"/>
Moderate				<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Moderately Low					<input checked="" type="checkbox"/> ✓	
Low						
Inherent Risk Trend				Stable	Stable	Stable
Risk Management Assessment				Satisfactory	Satisfactory	Satisfactory

<input checked="" type="checkbox"/>	Desired Inherent Risk
<input checked="" type="checkbox"/>	Risk Management Structure
<input type="checkbox"/>	Inherent Risk

Figure 4: Summary-level Listing of IT Risks

Technology	Business Specific Technology Risk
Vendor management	Legacy technology migration & innovation management in an uneven economy
Crisis management/Business continuity	Conversions
Technology risk management maturity—regulatory compliance	24x7x365 availability; reliability; keeping it all running in the face of infrastructure, vendor variables and changes in applications software
Migration of critical technology infrastructure	Compliance with standard architecture, getting modern skills, meeting deadlines, and managing risk in a time of rapid regulatory and market change

⁴ This enterprise-level summary was compiled by the Chief Risk Officer of the firm and presented to the RMC along with more detailed analysis of important risks in each LOB and function. For purposes of the case, it has been modified to show only IT-related risks.

Figure 5: PFPC Technology Risk Governance Structures

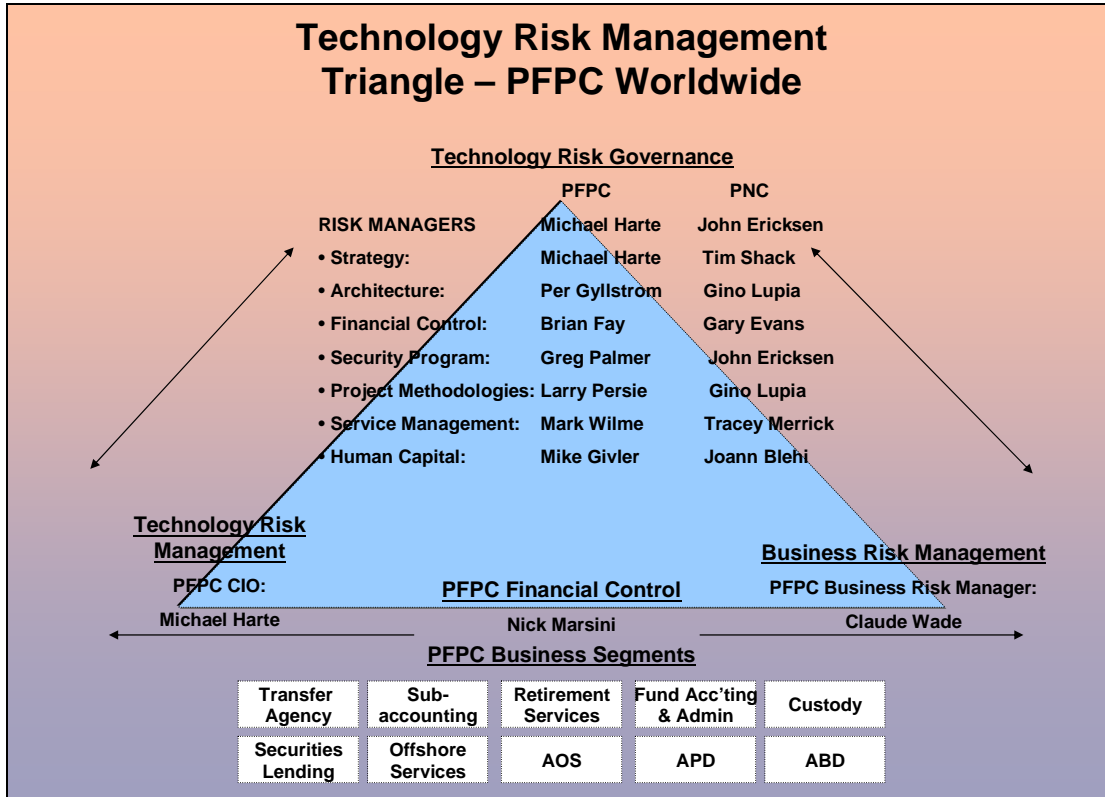


Figure 6: Risk-related Reviews in the project initiation and funding process

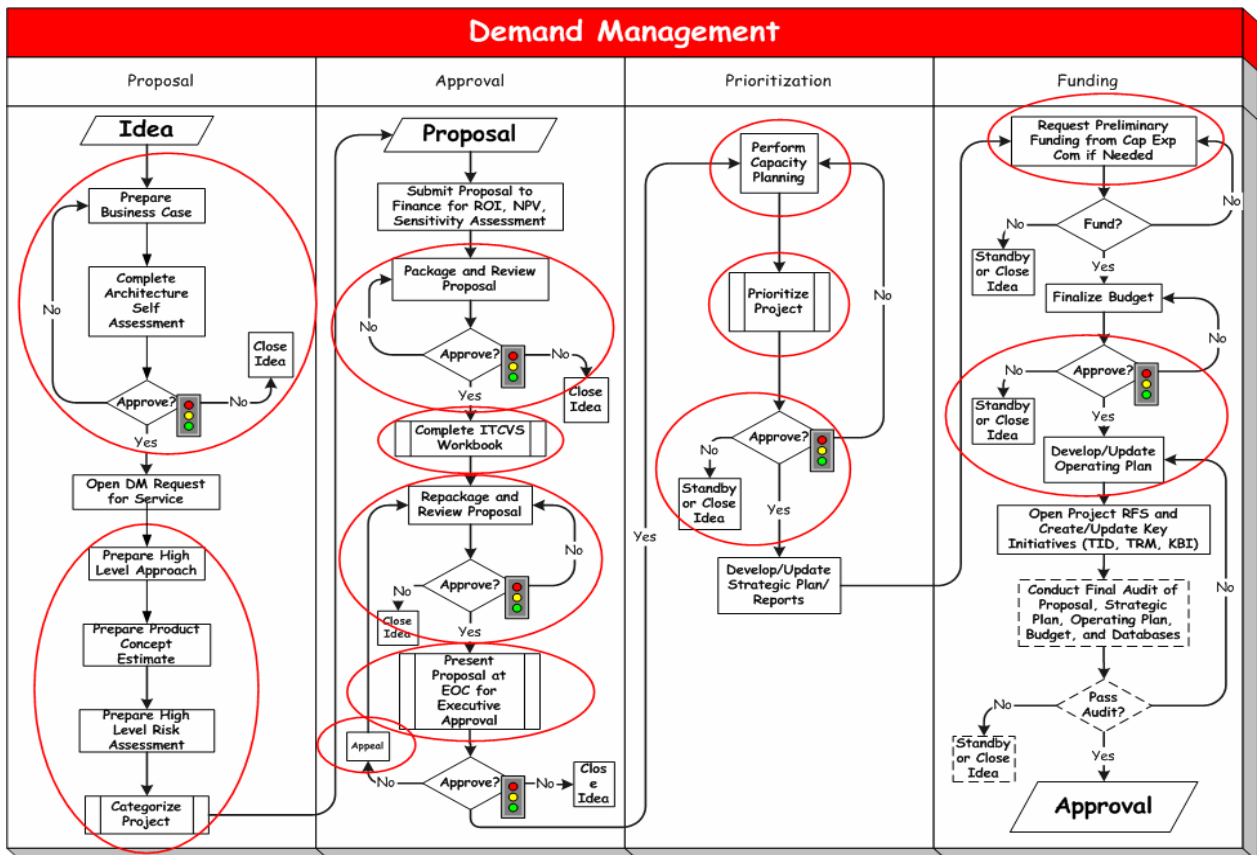


Figure 7: Excerpt from Technology Risk Management database

Project Status Report						Week Ending: 04/30/2004			
EXECUTIVE SUMMARY									
Risk Ranking	Total Number of Risks	Total Number of Projects	Projects Completed / Declined	Projects Approved / Active	Projects Pending Decision				
High:	13	13	8	0	5				
Medium:	10	10	1	5	4				
Low:	13	13	8	2	3				
Totals:	36	36	17	7	12				
RISK ITEM SUMMARY									
Risk Issue	Risk Description	Risk Type	Risk Owner	Risk Rank	Project Status	Target Date	Project Number	Project Manager	Comments
Call Recorder Performance Issues at 103 and 400 Bellevue	Performance issues with current Verint and NiceLogger systems affecting 2 LOBs (i.e. lost recordings).	Performance	Boyle	High	Not Started	TBD	TBD	TBD	NWS has submitted proposals for system upgrades to the (2) LOBs. Waiting for LOB decision.
Encryption on WAN Circuits at Lynnfield	Current encryption on Lynnfield to Summit WAN circuits does not meet PNC standards for 3DES.	Security	Dell'anno	High	Not Started	TBD	TBD	TBD	Related to risk item #3 - EOL Networking Equipment at Lynnfield. Waiting for LOB decision to remediate.

Figure 8: Technology Risk Management Dashboard

