ISACA®

Trust in, and value from, information systems

Risk Management at PridePoint Bank

Caselet #2:

IT Risk Assessment

Disclaimer

ISACA has designed and created the *Risk Management at PridePoint Bank* series (the ‘Work’) primarily as an educational resource for educational professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, security governance and assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

The example companies, organisations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious. No association with any real company, organisation, product, domain name, email address, logo, person, place or event is intended or should be inferred.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *info@isaca.org*
Web site: *www.isaca.org*

Trust in, and value from, information systems

Reservation of Rights

Provide Feedback: *www.isaca.org/risk-management*
Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Follow ISACA on Twitter: *https://twitter.com/ISACANews*
Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

Acknowledgements

Author
James C. Samans, CISA, CISM, CRISC, CISSP-ISSEP, CIPT, PMP, XENSHA LLC, USA

Board of Directors
Robert E Stroud, CGEIT, CRISC, CA, USA, International President
Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Vice President
Garry J. Barnes, CISA, CISM, CGEIT, CRISC, BAE Systems Detica, Australia, Vice President
Robert A. Clyde, CISM, Clyde Consulting LLC, USA, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President
Vittal R. Raj, CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past International President
Gregory T. Grocholski, CISA, SABIC, Saudi Arabia, Past International President
Debbie A. Lew, CISA, CRISC, Ernst & Young LLP, USA, Director
Frank K.M. Yam, CISA, CIA, FHKCS, FHKIoD, Focus Strategic Group Inc., Hong Kong, Director
Alexander Zapata Lenis, CISA, CGEIT, CRISC, ITIL, PMP, Grupo Cynthus S.A. de C.V., Mexico, Director

Knowledge Board
Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Chairman
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Neil Patrick Barlow, CISA, CISM, CRISC, CISSP, IntercontinentalExchange, Inc. NYSE, UK
Charlie Blanchard, CISA, CISM, CRISC, ACA, CIPP/E, CIPP/US, CISSP, FBCS, Amgen Inc., USA
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Anthony P. Noble, CISA, Viacom, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK
Ivan Sanchez Lopez, CISA, CISM, CISSP, ISO 27001 LA, DHL Global Forwarding & Freight, Germany

Academic Program Subcommittee
Matthew Liotine, Ph.D., CBCP, CHS-III, CSSBB, MBCI, University of Illinois at Chicago, USA, Chairman
Daniel Canoniero, Universidad de Montevideo, Uruguay
Tracey Choulat, CISM, CGEIT, CRISC, University of Florida, USA
Umesh Rao Hodeghatta, Xavier Institute of Management, India
Nabil Messabia, CPA, CGA, Université du Québec en Outaouais, Canada
Mark Lee Salamasick, CISA, CSP, CIA, CRMA, University of Texas, USA
Ype van Wijk, Ph.D., RE, RA, Rijksuniversiteit Groningen, The Netherlands
S. Vanderloot, CISA, CISM, CRISC, Ph.D., AST, CCNA, CCNA Security, CCSA, CEH, ECSA, ISO 27001 LA, NCSA, PCIP, UK
Nancy C. Wells, CISA, CRISC, USA

Student Book

This caselet was developed to support ***Risk Management Student Book***

www.isaca.org/risk-management

Introduction

What is risk management?

What is risk assessment?

How does it benefit a CIO?

- **Risk management** refers to the co-ordinated activities taken by an enterprise to direct and control activities pertaining to risk.
- Risk management is an active process, not simply a form of elaborate observation.
  - ‘Control’, when used as a verb in the context of risk management, is often used as a synonym for ‘measure’.
  - However, the results of measurement must be used as the basis for directing actions and activities.
- Comprehensive risk management includes four steps:
  1. Identification
  2. Assessment
  3. Mitigation (response)
  4. Ongoing monitoring and reporting

Introduction

What is risk management?

What is risk assessment?

How does it benefit a CIO?

- **Risk assessment** is a process used to evaluate risk on the basis of its probability and the impact of consequences upon operations.
- Probability is a function of two inputs:
  - Threat, which is anything that is capable of acting against an asset that can result in harm; and
  - Vulnerability, which is a weakness that allows effects upon a system exposed to a threat.
- Risk scenarios identify risk on the basis of threats.
- Risk assessment establishes difficulty of detection and whether a corresponding vulnerability may exist.

Introduction

What is risk management?

What is risk assessment?

How does it benefit a CIO?

- Because resources are limited, chief information officers (CIOs) need to know which risk most urgently requires attention.
- Probability is quantitative.
- If the consequence of an event is quantifiable, the associated risk is therefore also quantitative.
- The results of risk assessment can be used to prioritise risk so that the most urgent risk is given attention before less urgent risk.
    - Time and other resources are always limited.

Agenda

- Company Profile – PridePoint Bank
- Background Information
- Your Role
- Interviews
- Your Tasks
- Discussion Questions

Profile of PridePoint Bank

Mid-sized regional bank

Taken public last month after an aggressive campaign of customer expansion and cost-cutting

2,150 employees and an additional **700 contractors**

ISACA®

Trust in, and value from, information systems

Background: Overview

- PridePoint is the dominant bank across three states with 92 branch locations.
  - Total assets of $3.6 billion
  - Non-interest income is 19.2% of total revenue
  - 84.1% loan-to-deposit ratio
  - Customers include both individual consumers and regionally established businesses.
  - Largest business customers average revenues in excess of $57 million per year.
- Most account holders have been with PridePoint since at least a year before it went public.

Background: Organisational Structure

Overview

Org. Structure

Operations

Competition

Business Goals

- PridePoint has a five-person board of directors with a non-executive chairman.
- The CEO has three direct reports:
    - Chief financial officer (CFO)
    - Chief operating officer (COO)
    - Senior vice president (SVP) of Administration
- Technology Operations and Information Security report to the COO through the CIO.
- Facilities and Physical Security report to the SVP, Administration through Human Resources.
- Procurement oversees contractors and reports to the CFO.
- Operational Risk and Internal Audit report to the CFO.

Background: Organisational Structure

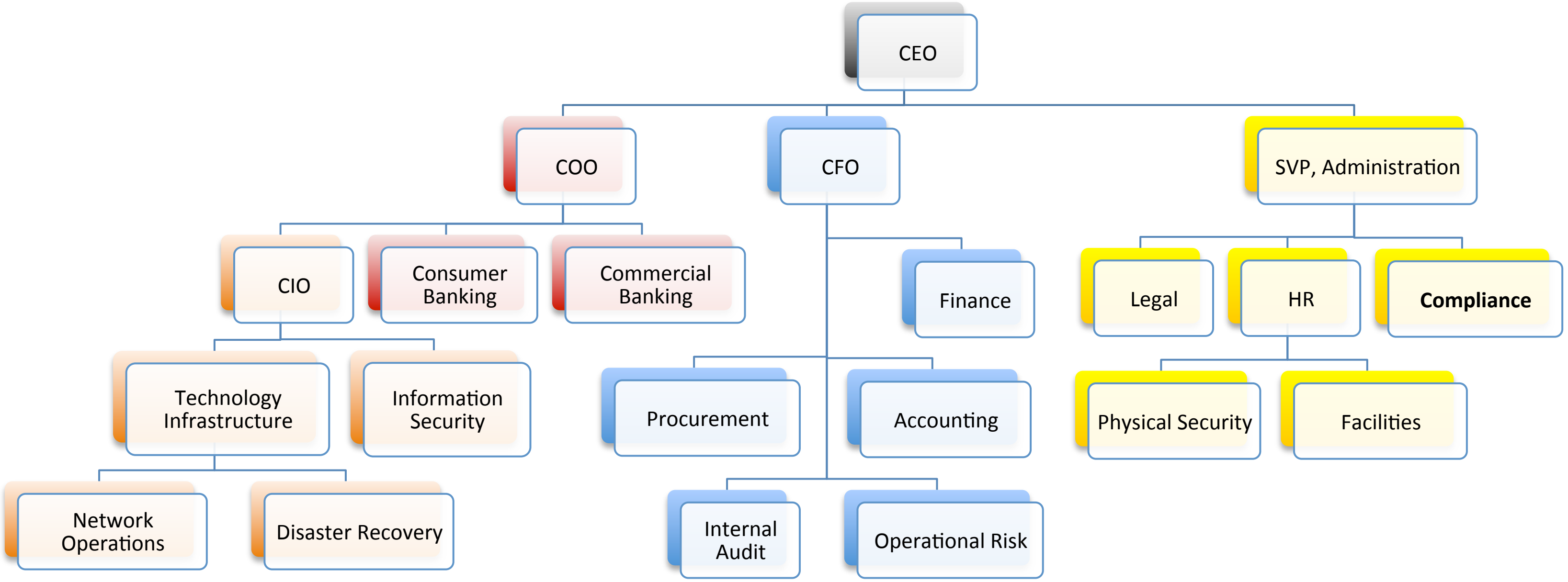
Overview

Org. Structure

Operations

Competition

Business Goals



Trust in, and value from, information systems

Background: Operations

Overview

Org. Structure

Operations

Competition

Business Goals

- The board of directors is pleased with profitability but concerned about controlling risk.
- To address this concern, the CEO has mandated that risk assessments be completed across the enterprise.
- The CFO has directed Operational Risk Management to lead the assessment of consumer and commercial banking.
- The SVP of Administration has tasked Physical Security with assessment of facility and workforce risk.
- The COO has directed the CIO to identify risk associated with information technology and systems.

Background: Competition

Overview

Org. Structure

Operations

Competition

Business Goals

- Miners Bank is PridePoint’s largest competitor:
  - Privately held
  - 57 branches
  - Total assets of $2.6 billion
- Up until six months ago, PridePoint had been steadily taking market share from Miners.
  - PridePoint focused on marketing the advantages of banking with a regional giant.
- Miners recently unveiled a marketing message that customers’ money is safer with a privately held bank.

Background: Business Goals

- The top business goal is to increase profitability in anticipation of an initial public offering (IPO) in five years.
- The strategy for meeting this goal is to:
  - Increase non-interest bearing deposits; and
  - Reduce operating costs.
- PridePoint has so far retained most of its pre-merger customers, and their continued retention is considered essential to the business strategy.

Your Role

Experience:

- Three years of experience in information assurance
- Joined XYZZY Consulting two months ago
- First independent customer engagement

Credentials:

- Bachelor's degree in Information Technology
- CRISC certification

- As an Information Systems Risk Analyst, you:
  - Represent XYZZY Consulting, which has been engaged by the CIO
  - Are responsible for the IT risk assessment
- You are not to access any PridePoint information systems; however, you may:
  - Ask questions of any employee or contractor within the CIO's organization
  - Review network diagrams and policies associated with all aspects of technology
- You will submit your report to the CIO.
- Your report should be well developed with clearly supported recommendations.

Interviews

- Your instructor’s Teacher Edition of this caselet includes the following interviews: (THESE ARE ATTACHED AS THE LAST SLIDES(21-26)
  - CIO
  - Network Operations
  - Disaster Recovery
  - Information Security
  - Technology Operations
- Check with your instructor to determine whether these will be used interactively in the classroom or distributed as handouts. (THESE ARE ATTACHED AS THE LAST SLIDES(21-26)

Identified Risk

Category	Threat Event	Targeted Asset or Resource	IT Risk Category
Architecture	Regional event affecting connectivity and/or power	Physical Infrastructure, IT Infrastructure	Operations/Service
Architecture	Consolidation into a single-zone network	Physical Infrastructure, IT Infrastructure	Benefit/Value, Project Delivery
Environmental	Loss of cooling capacity within a data centre	Physical or IT Infrastructure: Data centre 3	Operations/Service
Information	Customer data accessed without permission	Information	Operations/Service
IT Expertise & Skills	Key knowledge lost due to employee departures	Applications, IT Infrastructure	Operations/Service
Logical Attacks	External parties direct cyber attacks against the network	Applications, IT Infrastructure	Operations/Service
Program/Project Life Cycle Management	IT projects cost more or take longer than planned	People and Skills, Process	Project Delivery
Staff Operations	Data transaction processed on wrong system	Information, Applications	Operations/Service

Your Tasks

1. Prepare a network diagram based on your interviews, reflecting your understanding of the PridePoint network in its current state. Include:
   a. Zone boundaries
   b. Connection points and links
   c. Known security capabilities
2. Review the list of risk identified by the Director of Technology Operations. For each risk, based on your interviews:
   a. Estimate the difficulty in detecting the threat event given current capabilities.
   b. Identify a vulnerability that aligns with the threat event.
   c. Summarise a possible consequence associated with the risk.
3. Select the most serious risk based on your assessment and your understanding of the enterprise risk appetite (Prioritize Risks).

INTERVIEWS

The subsequent slides summarize the ‘interview’ feedback from the bank employees.

Interview: CIO

‘PridePoint used to be two different banks. When they merged, I was tasked with two different goals: first, keep the customer experience consistent and always available; and second, cut costs as much as possible. The first goal took priority.

That pretty much tied my hands. We had two sets of customers, and each set was used to a different way of doing things. To keep meeting everyone’s expectations—because we had promised that there would be no big changes—we had to keep both models. That meant two, totally different network infrastructures. It means all of their applications, even when the same application was used on both networks, and all of the staff who maintained those systems. Basically, anything customer-facing had to be kept.

On the flip side, anything non-customer facing got hit hard. I had to eliminate half of the InfoSec staff. A year ago, I had the Director of Technology Operations identify our risks, but I had to reject any project that was proposed, no matter how good of an idea it was. I’m sure glad that the IPO is over’.

Interview: Network Operations

‘So what we have is basically one big network divided into two sub-networks, which we are calling ‘Zones.’ Zone A used to be one bank, Zone B the other.

Zone A is based on physical servers. It has two data centres, and it’s where we have the Internet perimeter – one circuit into each data centre, redundant so that we don’t lose connectivity if we lost one of those data centres.

Zone B uses a virtual server architecture within one big data centre, about 80 miles away from the other two. We’ve got all three data centres connected by high-speed fibre, but our branches and ATMs connect over Internet VPNs. Any Internet traffic reaching Zone B comes by way of the Zone A perimeter.

At this point, all of our new user accounts are being created in Zone A, but there are still some Zone B accounts from before the merger. Users can log into either zone, but admin privileges only work within their native zones. We also have some applications that exist in both zones, not redundant but totally separate instances from before the merger’.

Interview: Disaster Recovery

‘You’ve already heard about how we have two different Zones, right? Well, the zones have totally different architectures, so each has its own disaster recover plan.

Zone A is set up on a hot-site model, active-passive. Data centre 1 is primary, data centre 2 gets copies of every transaction so the data is up to date. If data centre 1 goes down, the servers in data centre 2 notice and come online.

The technical failover takes less than 15 minutes, but everyone from data centre 1 has to get out to data centre 2 to really have sustainable continuity. It’s 20 miles away, so it can take up to an hour with traffic.

Zone B is totally different. Virtual servers. If data centre 3 goes does, we need to activate host systems, restore backups of the virtual servers and then restore data. There’s no hot site, but there’s leased capacity at a contractor site 100 miles away. They pull the backups, recover everything and set up a VPN back to Zone A. Start to finish, it takes about 12 hours’.

Interview: Information Security

‘We really got hammered over the past year. Not at the perimeter, of course. We’ve got standard security suites in place for both circuits, firewalls scaled to 130% of typical traffic and proxies, AV suite for the mail—the usual stuff. Robust configurations recommended by US CERT.

Actually, our perimeter is probably stronger than most of our competitors’ networks. Inside is a different story. Staff cuts, postponed projects—we used to do security awareness training across the workforce, but that got cut. Last month, we did a test to see who would click on a phishing email? 67% of people here did it. We’re really vulnerable.

And the thing is, I can’t tell what the threat is. We’ve got those IDS sensors going off all of the time, alarm, alarm—all hours. But we check and it’s nothing. False positives. I don’t have the staff to try and tune them. Policy says that every alarm gets checked, but it’s probably closer to half of them. Maybe less. It’s hard to run things to ground with no internal monitoring. At least we have client antivirus’.

Interview: Technology Operations

‘I got here just after the merger. First time working in banking. The InfoSec layoffs had just finished, and I was told right away about the two priorities: guarantee the customer experience, and cut anything that didn’t contribute to that experience.

It’s been rough, because I came from a place where we were always looking for ways to improve. Sure, keep an eye on cost, but when you see an opportunity to do things better, do it. My last company was all about ‘resiliency’—make sure that we can survive whatever gets thrown at us.

I started off doing a project on risk identification. My folks put together a whole list using scenarios, then we sent it over to InfoSec to get their buy-in. Sent it to the CIO and he called me in for a meeting. Great stuff, he told me. Things he knew that we needed to deal with, but not for a year. The next year was all about keeping things the same. So we did.

I’m glad you’re here. I’ll be happy to share with you what we identified’.