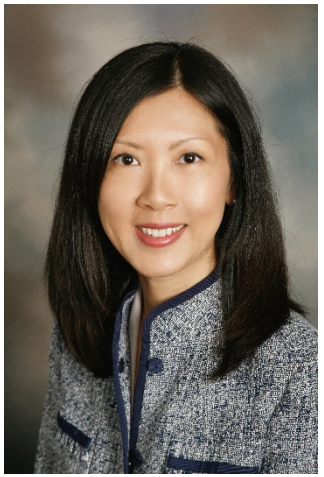
Best Practices on Managing Risks of Outsourced Services

Janis Parthun, Director, McGladrey, LLP

Governance, Risk & Compliance – G33

Introduction

- McGladrey LLP – San Francisco, CA
- Risk Advisory Services
  - 3rd Party/ Service Organization Reporting SME
  - 2013 COSO Framework SME
  - IT Risk Assessment, COBIT 5 SME
- Prior to joining McGladrey LLP
  - Division lead for Information Management and Technology Assurance (IMTA) services at AICPA
  - Consulting Manager for Grant Thornton LLP



Janis Parthun
CPA, CISA
Phone: 415-848-5318
Janis.parthun@mcgladrey.com

Agenda and Objectives

- Types of outsourcing
- Benefits of outsourcing
- Risk of outsourcing
- Due diligence and commitment considerations
- Monitoring performance and compliance
- Example scenario

Questions for the Audience

- Does your company or your department currently rely on a service provider to perform one of your business functions?

- Is this a significant or relevant function for your company or department?

TYPES OF OUTSOURCING SERVICES

Outsourcing Service Examples

- Procurement or payment function
- Other finance functions
- Payroll function
- HR (pension & benefits) function
- IT infrastructure support
- Document management
- Specialized/ advisory services
  - such as legal or accounting/ tax advice

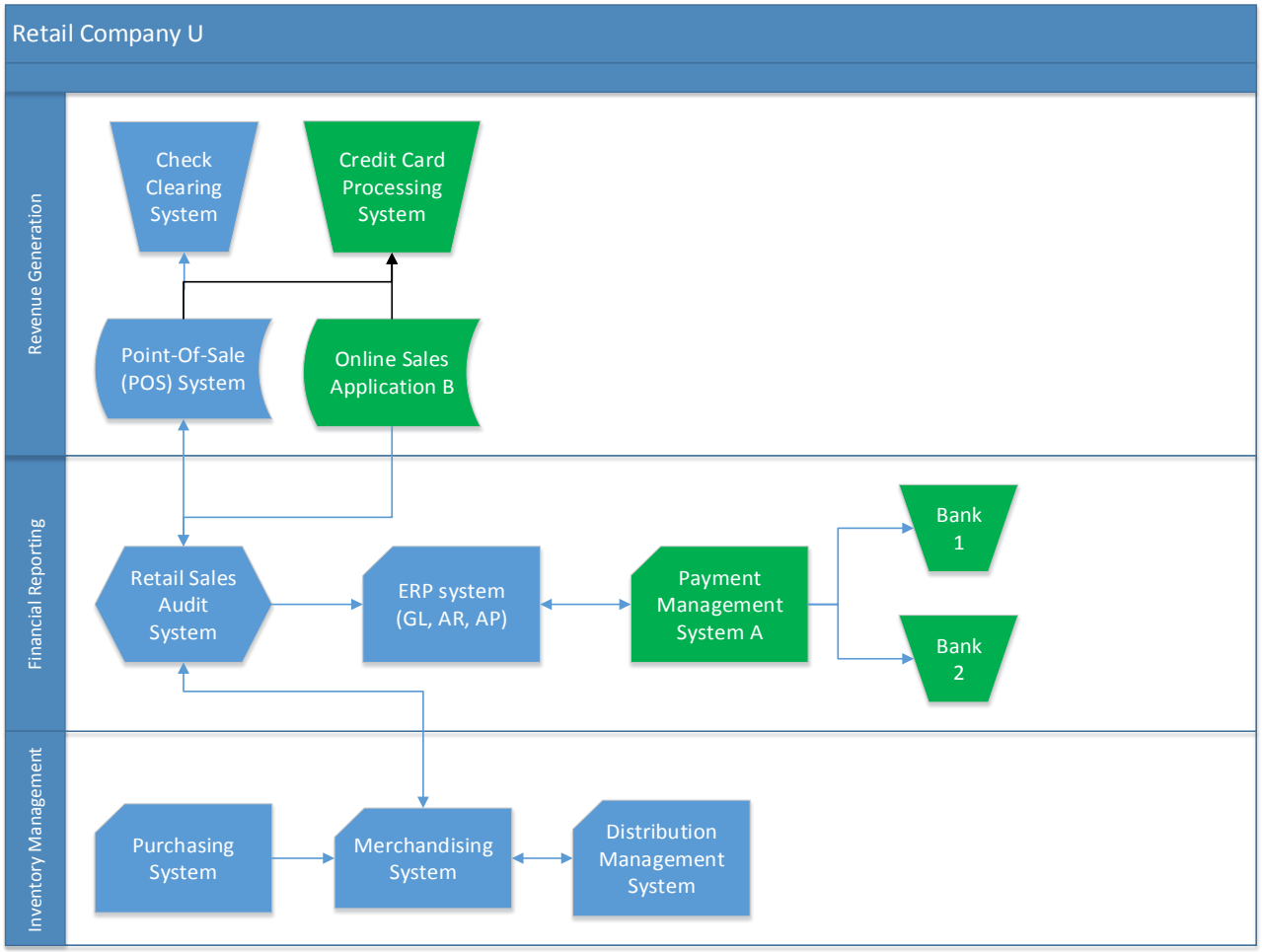
Cloud Computing Services

Type	Description*
Software as a Service (SaaS)	To utilize the service provider's applications running on a cloud infrastructure
Platform as a Service (PaaS)	To deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the service provider
Infrastructure as a Service (IaaS)	To provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software

** Source: National Institute of Standards and Technology (NIST)*
http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

Outsourcing Service Example

Illustration of a retail clothing company leveraging outsourcing services



BENEFITS OF OUTSOURCING BUSINESS FUNCTIONS

Market Indicators to Outsource

- Pressure to improve operational costs
- Leverage experts specialized in the outsourced service offering
- Potential availability of more sophisticated resources (such as the latest hardware or software)
- Availability of a virtual workforce
- Meet short term demands or needs
- Lack of resources to support a process or function

Benefits to Outsourcing

1. Speed
2. Efficiency
3. Cost savings

- Reasons for this economy of scale:
  - Provider has on-demand and scalable technology
  - Provider leverages advances in technology specifically for the function & skilled resources/ expertise
  - Provider may support more complex and changing business operations and may be cost prohibitive for management as an internal investment

RISK OF OUTSOURCING BUSINESS FUNCTIONS

Breaches Related to Service Providers

Company	The Breach	Reference
U.S. Department Of Veterans Affairs	Personal information for ~ 76 million veterans were possibly compromised when a defective hard drive was sent for repair and recycling to a vendor with unencrypted data	http://abcnews.go.com/Technology/Media/10-top-data-breaches-decade/story?id=10905634&page=2
Epsilon (Email Marketing Provider)	Intruders accessed one of its email servers and obtained names and email accounts of some of its 2,500 corporate customers	http://www.computerworld.com/s/article/9215527/FAQ_Epsilon_email_breach
Amazon Web Services (Provider)	Multi-day service outage slowed/ shut down a large number of prominent Internet businesses	http://www.informationweek.com/news/cloud-computing/infrastructure/229402520
Target	Source of the Target major intrusion attack traces back to network credentials that Target had issued to Fazio Mechanical (heating & air conditioning vendor) Target had also relied on its data security monitoring services to Trustwave (service provider) at the time	http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/ http://www.infoworld.com/d/security/security-vendor-trustwave-named-in-target-data-breach-suit-239119

Outsourcing Risks to Consider

Risks:

1. Handling and processing of data
2. Security and access
3. Availability of system
4. Retention of data
5. Other possible factors specific to your business

User Concerns Associated With Outsourcing Services

- When users/ customers of a service provider's services outsource certain tasks and functions, many of the risks of the service provider become risks of the users/ customers.

- Due diligence is necessary in order to manage the risks and address any stakeholder concerns

DUE DILIGENCE AND COMMITMENT CONSIDERATIONS

Monitoring Performance and Compliance of Service Providers

- Evaluate knowledge and competencies of service provider
- Consider regulatory and operational compliance obligations of service provider
- Positive financial history

Commitment Considerations

- Return on investment (ROI) for leveraging a service provider
- Service offering address the business or functional needs of your organization

Commitment Considerations

- Adequate requirements within the Service Level Agreement (SLA) or contract
  - clear and concise contractual terms
  - include standard of conduct
  - flexibility within the agreement
  - problem resolution support / escalation procedures
- Designated point of contact within the organization to be accountable for the service provider

MONITORING PERFORMANCE AND COMPLIANCE OF SERVICE PROVIDERS

Monitoring Performance

- Establish periodic monitoring procedures against expectations or requirements
  - Extent may depend on the risk associated
  - Monitor services stated in a service level agreement (SLA) - such as reliability, performance and support

Obtain an Independent Assessment

How can you trust and have confidence in the 3rd party relationships you form or contract?

1. Monitor through obtaining an independent assessment over the service provider's internal controls
2. Attestation reports provide details to user management and with the information they need about the service organization's controls to help assess and address the risks associated with the outsourced service
3. Multiple options to consider and request for

3rd Party Reporting Options

Service Organization Control Reporting:

	SOC 1 Report	SOC 2 Report	SOC 3 Report
Purpose	Reports on controls for F/S audits	Reports on controls related to compliance or operations	Reports on controls related to compliance or operations
Objective	Processes with F/S impact	Trust Services Principles & Criteria	
Standard	SSAE16 – Service Auditor Guidance	AT 101	AT 101
Use	Restricted use report	Generally a restricted use report	General use report (with a public seal)
Extent of Report	Type I Report – Test of control design, or *(as of a specific date)* Type II Report – Test of Operating effectiveness *(throughout a specified period)*		

Trust Services Principles & Criteria

Security

- The system is protected against unauthorized access (both physical and logical).

Availability

- The system is available for operation and use as committed or agreed.

Processing integrity

- System processing is complete, accurate, timely and authorized.

Confidentiality

- Information designated as confidential is protected as committed or agreed.

Privacy

- Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity's privacy notice, and with criteria set forth in Generally Accepted Privacy Principles (GAPP) issued by the AICPA and Canadian Institute of Chartered Accountants.

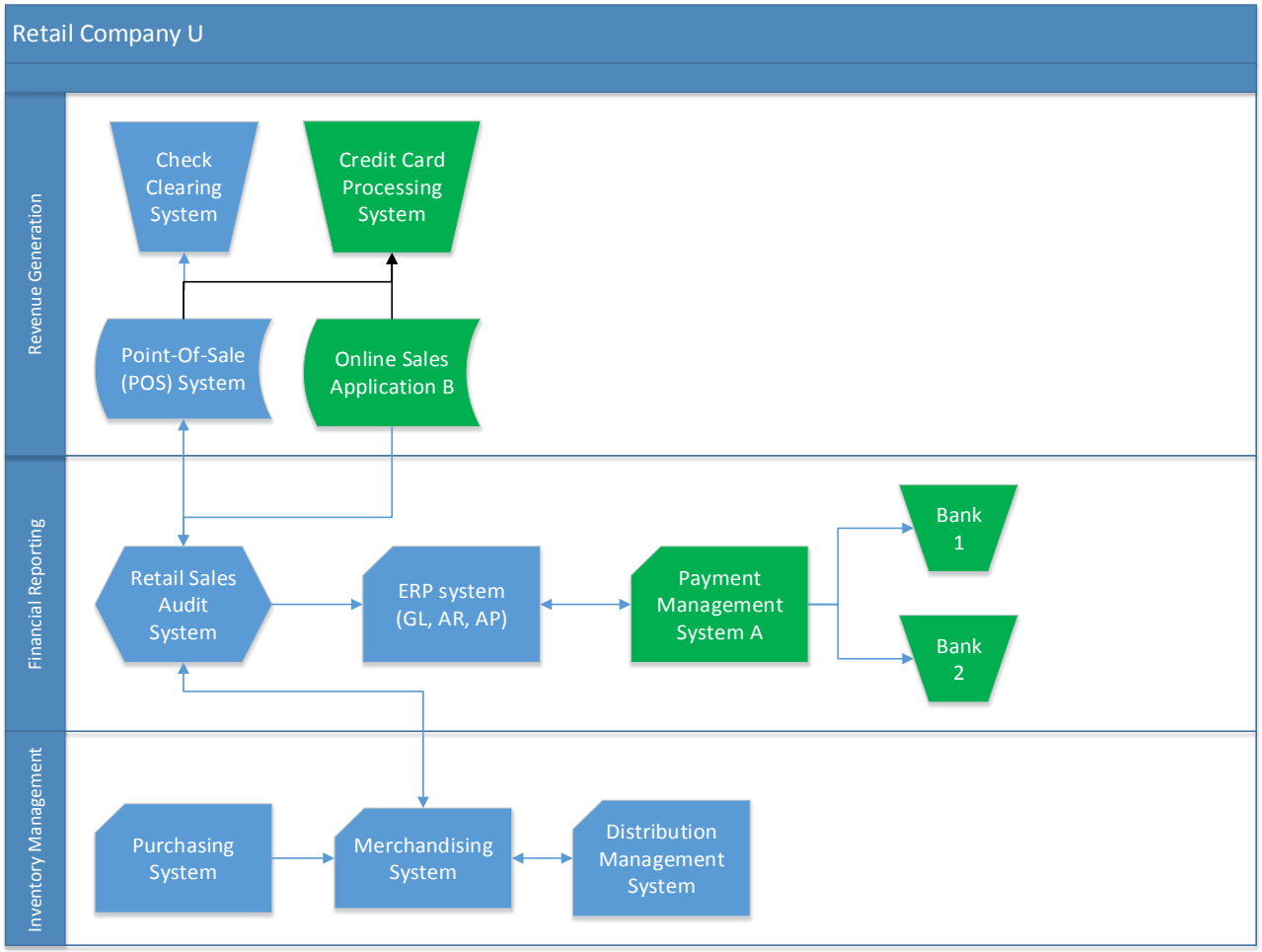
EXAMPLE SCENARIO

Retail Company U

- **Company U** (user) is a retail clothing company with retail stores all over the country. The company leverages a service provider to allow on-line purchasing for customers. Inventory is purchased from various vendors, and a warehouse is available to receive and ship the inventory. Accounting is performed using an in-house system, but the company leverages a service provider to manage vendor payments.

Outsourcing Service Example

Illustration of a retail clothing company leveraging outsourcing services



Resources

1. COSO: 2013 Internal Control–Integrated Framework
   - www.coso.org
2. AICPA Brochure: Service Organization Controls – Managing Risks by Obtaining a Service Auditor's Report
   - www.aicpa.org/SOC

THANK YOU!


ISACA
Trust in, and value from, information systems
San Francisco Chapter
CyberSizeIT
SF ISACA FALL CONFERENCE
NOVEMBER 9-11, 2015
HOTEL NIKKO-SAN FRANCISCO