

Risk & Control Considerations for Outsourced IT Operations

Adnan Dakhwe, MS, CISA, CRISC, CRMA

Safeway Inc.

Core Competencies – C32



CRISC

CGEIT

CISM

CISA

2013 Fall Conference – “Sail to Success”


Introductions & Poll

Organization has outsourced some IT operations?

Organization has outsourced all of IT operations?

Organization is considering outsourcing some or all of IT operations?

Agenda

- 
- What is outsourcing/IT outsourcing?
 - Why do companies outsource IT?
 - Current trends in IT outsourcing
 - Benefits of IT outsourcing
 - IT outsourcing risks
 - Controls to be considered for IT outsourcing
 - Risk based approach to auditing outsourced IT operations

What is outsourcing?

A partnership between a client and an outside vendor, both sharing a common vision to effectively, efficiently, and accurately accomplish agreed-upon processes for the benefit of both parties.¹

1 – Outsourcing as defined in “Auditing Outsourced Functions” by Mark Salamasick (IIA Research Foundation)

What is IT Outsourcing?

Per Gartner¹: “IT Outsourcing is the use of external service providers to effectively deliver IT-enabled business process, application service and infrastructure solutions for business outcomes.

Outsourcing, which also includes utility services, software as a service and cloud-enabled outsourcing, helps clients to develop the right sourcing strategies and vision, select the right IT service providers, structure the best possible contracts, and govern deals for sustainable win-win relationships with external providers.”

1 - <http://www.gartner.com/it-glossary/it-outsourcing/>

Types of IT Outsourcing

- Application development and management
- Independent testing and validation services
- Innovation and R&D services
- Infrastructure management
- Help desk services
- Data center management
- Systems integration
- Managed security services, etc.

Why do Companies Outsource IT?

- Increased pressure to reduce costs
- Lack of technical knowledge about the particular area or process
- Lack of time, i.e. requirement to get things done more quickly
- Opportunities to increase focus on core competencies or value-added activities
- Lack of labor / Staff augmentation
- Lack of capital or resources
- Opportunities to expand market share and increase revenues

Current Trends in IT Outsourcing

Gartner¹:

- Worldwide IT Outsourcing (ITO) Market to Reach \$288 Billion in 2013
- The global ITO market will record a 5.4% compound annual growth rate (CAGR) from 2012 through 2017.

Dice²:

- U.S. Outsourcing Growth Outpaces Global Rate
- North America growth rate at 8 percent in 2013 and a 6 percent CAGR through 2017

1 – <http://www.gartner.com/newsroom/id/2550615>

2 - <http://news.dice.com/2013/08/12/u-s-outsourcing-growth-outpaces-global-rate/>

Current Trends in IT Outsourcing

KPMG Sourcing Advisory¹:

- 2Q13 Global Pulse Survey: ITO increase in demand of up to 36% in the next 1-2 quarters

HfS Research²:

- Growth in the IT Outsourcing (ITO) services market is expected to increase in 2013 to 3.5% and sustain a 4.7% CAGR through 2017

1 – <http://www.kpmginstitutes.com/shared-services-outsourcing-institute/insights/2013/pdf/2Q13-sourcing-advisory-global-pulse-report.pdf>

2 - <http://myemail.constantcontact.com/HfS-Market-Index-shows-4--growth-for-Global-IT-and-Business-Process-Outsourcing-in-2013.html?soid=1102861932005&aid=WRFwz7MgC4w>

Ponemon Institute's 2013 Report on "Securing Outsourced Consumer Data"

- 65% organizations have had a breach involving consumer data outsourced to a vendor
- 45% of the breaches were caused by negligence
- 40% of the breaches were due to lost or stolen devices
- 46% do not evaluate the security and privacy practices of vendors before sharing sensitive or confidential information

Source: <http://press.experian.com/United-States/Press-Release/experian-data-breach-resolution-and-ponemon-institute-survey-results.aspx>

2013 Trustwave Global Security Report

- A whopping 63% of data breaches were linked to a third-party.
- Unfortunately, almost all businesses provide these “trusted” outsiders with some degree of unfettered access.

Source: <https://www2.trustwave.com/2013GSR.html>

Benefits of IT Outsourcing

- Cost reduction
- Round-the-clock coverage
- Greater competency or specialized skills
- Accelerate time to market
- Take advantage of external expertise, assets and/or intellectual property
- Improvement of the organization's protection (managed security service providers)

IT Outsourcing Risks

- Reputation risk
- Service transition risk
- Strategic risk
- Data/Intellectual Property risk
- Service quality risk
- Business continuity risk
- Regulatory risk
- Security and Privacy
- Financial risk

IT Outsourcing Horror Stories!

[Fraud at Satyam, Indian Outsourcing Company](#) [- NYTimes.com](#)

www.nytimes.com/2009/01/08/business/worldbusiness/08satyam.html

Jan 7, 2009 - A top Indian outsourcing company massively inflated its earnings for years....

Controls to be Considered for IT Outsourcing

- Contract – terms and conditions
- Control environment
- Governance and monitoring
- Billing and time tracking
- Security considerations
 - Data protection risks
 - Security: network, physical, environment, personal, logical access and wireless access control

Controls to be Considered for IT Outsourcing

- Software/systems development controls
- Asset Management
 - Hardware
 - Software
- Change management controls
- HR policies and procedures
- Business continuity and disaster recovery

Key points to consider for contracts

Right to audit clause

Third party assurance of controls – SOC 1/2/3, ISO 27001, etc.

Billing provisions

Financial performance monitoring (needs to be negotiated in the contract for private service providers)

Quality assurance

Regulatory compliance

Asset ownership

Software licensing

Dispute resolution and termination

Security and nondisclosure

Key points to consider for contracts (continued)

Employee allocation

Confidentiality/Intellectual Property

Additional services

Delineation of responsibilities

Term of contract

Recourse and remediation of unsatisfactory performance

Data breach liability

Service level agreements and reporting procedures

Assignment and sub-contracting

Insurance

Disaster recovery and business continuity

Risk Based Approach to Auditing Outsourced IT Operations

- Perform an engagement level risk assessment
 - Interview key stakeholders within the company and the service provider
 - Determine the key objectives, risks and controls
 - Check to see if the service provider has any third party assessments or reports available
 - SOC 1 or SSAE 16 (formerly known as SAS 70)
 - SOC 2 or SOC 3
 - ISO 2700X
 - ISAE 3402, etc.
 - HIPAA, PCI, etc.

Risk Based Approach to Auditing Outsourced IT Operations

- Adjust the scope of the audit based on controls you could rely on in the above reports.
- Develop the risk and controls matrix
- Develop the audit program
- Consider leveraging subject matter experts, in case your department may not have expertise in certain areas, such as local laws and regulations.

Risk Based Approach to Auditing Outsourced IT Operations

- Fieldwork
 - Onsite/offshore
 - Travel & other logistics
 - Onsite presentation after the conclusion of fieldwork
 - Offsite/onshore
 - Offsite closing meeting
- Reporting
- Follow-up

Case Study:

Safeway Inc. (SWY) Quick Facts

- One of the largest food and drug retailers in North America operating under the Safeway, Vons, Dominick's, Carrs, Pavilions, Randall's, and Tom Thumb banners.
- Over 1400 stores in Western, Southwestern, Rocky Mountain, Midwestern, and Mid-Atlantic Regions of the U.S.
- Over 1100 in-store pharmacies.
- In June 2013, Safeway announced the sale of its Canadian operations for C\$5.8 billion.
- Owns GroceryWorks.com, an Internet grocer doing business under the names Safeway.com and Vons.com
- Safeway also owns 73% of Blackhawk Network Holdings Inc. (NASDAQ: HAWK), which completed its IPO in April 2013. Provides third-party gift cards, prepaid cards, telecom cards, and sports and entertainment cards to retailers in North America, Europe, Asia, and Australia.
- Holds 49% interest in Casa Ley, S.A. de C.V., which operates 195 food and general merchandise stores in Western Mexico.
- Headquartered in Pleasanton, CA in the San Francisco Bay Area.
- 171,000 employees.
- US\$44.2B in 2012 revenue (Fortune #62).

Case Study:

3rd Party Service Provider

- A key strategic offshore/onshore partner of Safeway Inc.
- Service Provider has global operations.
- Development centers are in Asia
- Services provided to Safeway: Application development, IT infrastructure, and innovation

Case Study

- Performed engagement level risk assessment
 - Interviewed key stakeholders at Safeway
 - Interviewed key 3rd party personnel
 - Determined the key objectives, risks and controls
 - Checked to see if the service provider had any third party assessments or reports available
 - Adjusted the scope of the audit based on controls you could rely on in the above reports.
 - Developed the Risk and Controls Matrix
 - Developed the audit program

Key Objectives

- Contract compliance
- Delivery model review (personnel, training, succession planning, etc.)
- Quality of work
- Relationship management
- Time tracking and billing
- Adherence to Safeway standards and best practices: software development, change management, information security and privacy, user access (adding, deleting, changing), physical security, desktop security, wireless access control, etc.
- Asset management (hardware and software)
- Business continuity and disaster recovery
- Compliance with local laws
- Benchmarking Safeway's relationship with the vendor and other companies' relationship with IT service providers in that country

Audit Team

- Team included
 - IT Audit Director
 - IT Audit Lead/Manager
 - Staff from a Big 4 office in Asia
 - Provided expertise in the area of local laws and regulations and emerging trends
 - One of the resource was a contributor to the previous version of the IIA GTAG – assisted in benchmarking for this review
 - We were onsite in Asia for a couple weeks with the Big 4 staff from an office in Asia.

Fieldwork

- Provided a presentation after the conclusion of onsite/offshore fieldwork
 - Included potential observations and next steps
- Performed offsite/onshore fieldwork
 - Review of controls at Safeway with regards to the relationship with this service provider
- Vetting of observations
- Obtained Management Action Plans/responses to the observations
- Closing Meeting

Reporting & Follow-up

- Draft Report – distributed to stakeholders at SWY
- Final Report – distributed to stakeholders at SWY
- Next step: Follow-up on observations

Common Observations Areas: Audit of Outsourced IT Operations

Contract (MSA and SOWs) terms and conditions are not adequate

Billing and time tracking procedures

Data security and physical security controls

Governance and monitoring processes

Software licensing

Business continuity and disaster recovery plan

Compliance with local laws and regulations

Resources

HfS Research

- <http://www.hfsresearch.com/>

IIA GTAG 7: Information Technology Outsourcing, 2nd Edition

- <https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG7.aspx>

ISACA: Outsourced IT Environments Audit/Assurance Program

- <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Outsourced-IT-Environments-Audit-Assurance-Program.aspx>

Resources

SANS: Outsourced
Information
Technology
Environment Audit

- http://it-audit.sans.org/community/papers/outsourced-information-technology-environment-audit_2514

“Auditing Outsourced
Functions” by Mark
Salamasick (IIA
Research
Foundation) –

- <http://www.theiia.org/bookstore/product/auditing-outsourced-functions-risk-management-in-an-outsourced-world-1632.cfm>

Questions?



Contact Information



Adnan Dakhwe, MS, CISA, CRISC, CRMA

adnan.dakhwe@safeway.com

adnandakhwe@gmail.com

<https://www.linkedin.com/in/adnandakhwe>

Thank you !