Audit Considerations for Outsourced Relationships

David Fong, SVP
Director of Professional Practices
Professional Strategies – S24

Key Points

- Reasons organizations outsource
- Understand outsourcing inherent risk
- Possible audit responses
- Useful references

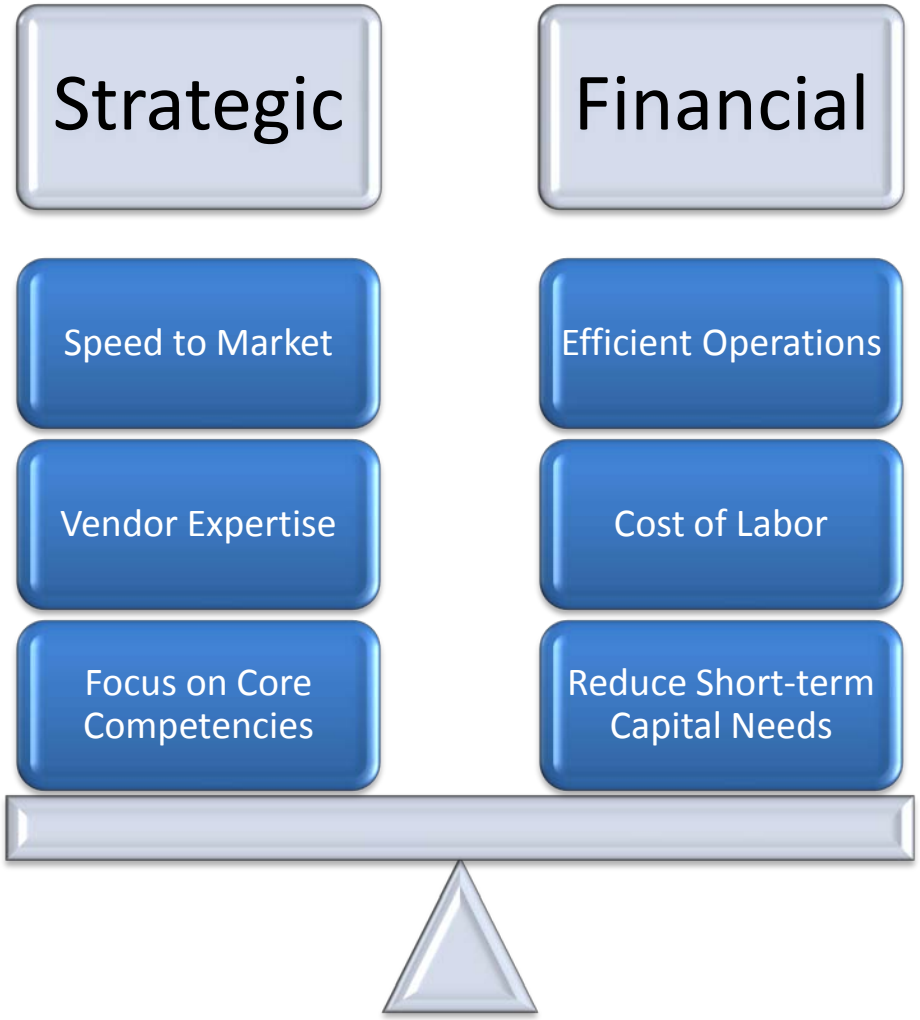
About Me

- Director of Professional Practices at Bank of the West (BNP Paribas Group)
- CPA and CISA
- Financial services experience (broker-dealer, asset management, banking, payment card, insurance)
- 16+ years external/internal audit experience
- 4+ years in vendor management

Your Outsourcing Experience

- Level of outsourcing at your organization
- Types of services being outsourced (technology, customer service, operations)
- Type of vendor management functions (none vs. centralized vs. decentralized vs. hybrid)
- Aspects of outsourcing that have been audited in your organization

Why Outsource?



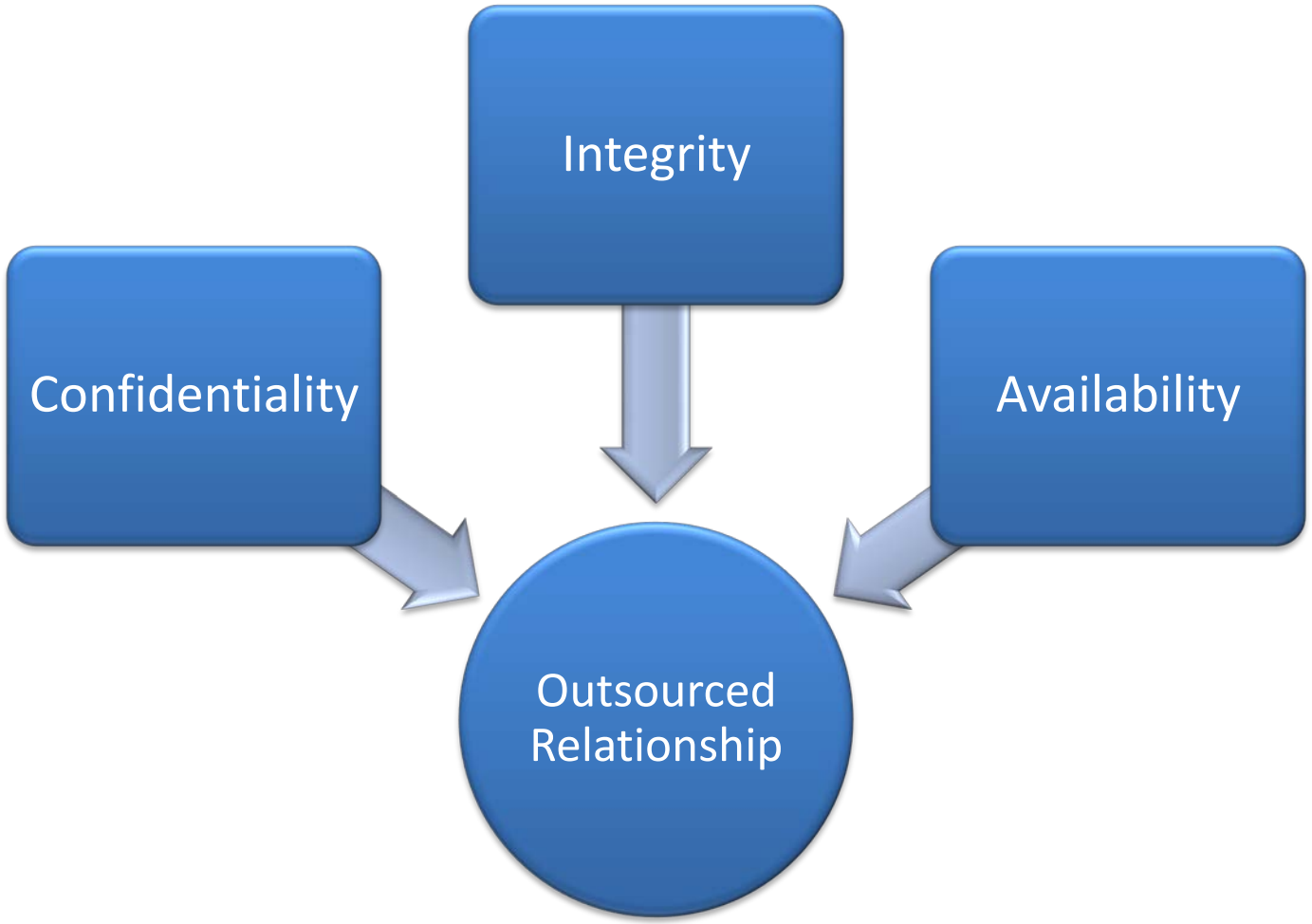
Strategic Reasons Organizations Outsource

- Speed-to-market
  - Migrate quickly using established vendor processes/infrastructure
- Leverage vendor expertise
  - Rely on subject-matter expertise in areas where your organization may not have expertise
- Focus on core competencies
  - Free-up internal resources to focus on mission-critical activities with potentially higher returns

Financial Reasons Organizations Outsource

- Leverage efficient operations
  - Gain economies of scales from a ‘provider’ of services
- Cost of labor
  - Lower labor costs
- Reduce short-term capital needs
  - Leverage established infrastructure and technologies without needing the initial capital outlay

What are the Primary Audit Concerns?



Audit Process

Starting the Audit Process

- During annual audit planning and regular audit plan refreshes:
  - Inventory the current and future outsourced relationships (audit universe)
  - Document the inherent risks from the various relationships (inherent risks)
  - Consider the organizational and departmental vendor management controls in place (control environment)

Audit Universe

- Inventory the outsourced relationships through
  - Process walkthroughs
  - Current contracts database(s)
  - Accounts payable/vendor lists
  - New products/initiatives
  - External connectivity diagrams
  - Data sharing

Detailed Risk Assessments

- Fully understand the risk of outsourcing your business operations
  - Risks from outsourced activities remain within the organization and NOT transferred to the vendor
- Determine the inherent risk (impact and likelihood) of a risk materializing
  - What could happen? How bad could it get?
  - How frequent could this happen?
- Assess the control environment to mitigate outsourcing risk within the organization

Understanding Inherent Risks

- Understand the inherent risks from the various relationships
  - Does management understand their risks?
  - What are the inherent risk factors used to measure risks?
    - Financial, reputational, regulatory/legal, client, etc. Remember to consider plausible impact instead of extreme outliers!
  - How does management account for risks from outsourced relationship?

Outsourcing Risks

- Anticipated efficiencies and cost savings are not gained
- Vendor is not responsive to problems or changes
- Vendor expertise is limited
- Vendor solution has limited flexibility or does not conform to organization's requirements
- Insufficient internal expertise or resource to properly oversight vendor

Outsourcing Risks (continued…)

- Internal and external clients are impacted by service gap
- Vendor is acquired or not financially viable
- Inability of the organization to manage service levels from sub-contracted services
- Sensitive data is compromised by vendor

Specific Business Risks

- Assess risks from an internal perspective
  - Examples of internal risks that can exists through an outsourced provider:
    - Customer statements incorrect or sent to the wrong customer
    - Poor customer service
    - Interest calculations incorrect
    - Sensitive customer data disclosed/lost
    - Service organization cannot recover quickly after a disaster
    - Service organization suddenly closes down

Control Environment

- Consider the organizational or department vendor management controls in place
  - formal vendor management program
  - roles understood (e.g., vendor segmentation, monitoring requirements, due diligence)
  - senior management involved with outsourced relationships
  - sufficient number of ‘dedicated’ individuals managing the outsourced relationships?
  - reliable Key Risk Indicator

Possible Audit Responses

Possible Audit Responses

- Vendor management program audit
  - Examine the framework used to manage vendors within the organization
  - Understand the “lay of the land” in organizations with a formal program
- Outsourcing project audit
  - Examine the real-time selection and deployment with an outsourced provider
  - Pre- and post- implementation reviews

Possible Audit Responses (continued…)

- On-going monitoring audit
  - Examine how a business monitors key vendors in their operations
  - Part of “business as usual” audit
- Conversion project audit
  - Examine how a business moves an outsourced function back in-house or to another provider
  - Project-type review

Vendor Management Program Review Scope

- Breadth and depth of the vendor management program
- Vendor risk assessments
- Management and operational success indicator reporting
- Training and awareness

Vendor Management Program Key Attributes

Senior management sponsorship

Defined roles and responsibilities

Training and awareness

Robust procedures and policies

Risk-based oversight

On-going due diligence

Monitoring, reporting, and escalation

Vendor Management Program Review Scope

- Breadth and depth of the vendor management program (VMP)
  - Which outsourced relationships or business divisions are within scope of the VMP? Can the VMP be by-passed?
  - Where does the head of the VMP report into?
  - Are all vendors managed similarly, or is the approach risk-based?
  - Are there documented monitoring programs for each vendor?

Vendor Management Program Review Scope

- Vendor risk assessments
  - Are there formal risk assessments for each vendor or are the risk assessments embedded within the business?
  - How are vendor risks aggregated if used by more than one business area?
  - Are the risk assessments completed by ‘qualified’ individuals?

Vendor Management Program Review Scope

- Management and operational success indicator reporting
  - How are problems with the vendor collated and reported to the vendor manager?
  - How is performance against the contract and service levels monitored?
  - How are deviations escalated to the vendor and with senior management and the Board?
  - How does the VMP know that the information used to monitor the relationships are ‘accurate’?

Vendor Management Program Review Scope

- Training and awareness
  - Are employees aware that there is a vendor management program?
  - Do employees understand what their roles and responsibilities are in managing an outsourced relationship?

Outsourcing Project Review Scope

- Vendor selection and evaluation process
- Due diligence
- Issues tracking and resolution
- Contract negotiations
- Implementation and training plan
- Exit plan preparation

Outsourcing Project Key Attributes

Outsourcing Project Review Scope

- Vendor selection and evaluation process
  - How were prospective vendors identified and selected for a proposal?
  - Were submitted Request-for-Proposal (RFP) evaluated against a risk-based scorecard?
  - Were the due-diligence (DD) activities aligned to the organization's risk assessments?
    - If availability is important, perform DD activity over vendor recovery
    - If data security is important, perform DD activity over vendor information security program

Outsourcing Project Review Scope

- Due Diligence
  - Evaluate vendor ability and experience to perform services based on the organization's needs and perceived risks
  - Understand vendor processes/controls in place to mitigate inherent risks—validate the effectiveness of these controls
  - Identify the due diligence gaps and consider suitable risk mitigation
  - Outsourcer's business contingency planning

Outsourcing Project Review Scope

- Contract negotiations
  - A well-conceived contract is essential to protecting the interest of the organization
  - Legal counsel involved throughout contract negotiations and reviews
  - Risk acceptance for gaps communicated to and approved by senior management
  - Gaps, open issues, and other verbal understandings are incorporated into the contract

Key Contract Terms to Consider

- Limitations of liability
- Define services, SLAs (and measurement specifications) and penalties/rewards
- Confidentiality and records management
- Intellectual property (IP) ownership
- Incident/breach notification
- Costs and fees for start-up, on-going and transition
- Right to audit, even when a SAS 70/SSAE16 exists
  - Especially, regulatory!
- Rights to terminate and transition assistance

Process Risk Control Matrix (PRCM)- Vendor Evaluation

Process	Risk	Control	Test Strategy
Vendor Evaluation	Vendor does not have the capability or capacity to provide the needed service	Due diligence is performed based on results the internal risk assessment Reference checks for current and terminated relationships are performed to understand the vendor capabilities For Tier 1 and 2 vendors, on-site reviews are conducted	Select # vendors from the approved contracts and the accounts payable database Review due diligence documentation to assess the quality and depth of the activities
	Vendor is not financially viable	For Tier 1 & 2 vendors, audited financial statements and key financial ratios are reviewed by credit risk group for financial health and continued viability before the contract is executed	From the new contracts selected above: Determine that the financial review was performed prior to contract execution

Note: This PRCM is not intended to be complete and is used for illustration purposes only.

On-going Monitoring Review Scope

- Key Operational Success Indicators (OSIs)
- On-going due diligence
- Continuous vendor oversight

On-going Vendor Monitoring Key Attributes

Documented Vendor Management Plan

Oversight

- Due diligence visits
- Service level meetings

Review

- SLA reports
- SAS70/SSAE 16
- Exit Plan

On-going Monitoring Review Scope

- Key Operational Success Indicators (OSIs)
  - Have OSIs been established for the vendor relationships?
  - What indicators do management use to assess whether the vendor is operating properly?
  - Are these the right indicators produced at the right frequency?
  - How are exceptions flagged and escalated?

On-going Monitoring Review Scope

- On-going due diligence
  - Are key, relevant vendor controls mitigating the organization's key risks validated during due diligence visits?
  - Who is involved with the due diligence reviews?
  - How are exceptions flagged and monitored?
  - Are key aspects of management reporting validated?

On-going Monitoring Review Scope

- Continuous vendor oversight requires a documented vendor management plan
  - Review the accuracy of service level reporting
  - Review the continued viability of the vendor
  - Risk-based review of SAS 70/SSAE 16 report
    - What vendor controls are relied upon? Have those controls been reviewed? If not, have they been included into the due diligence visits.
  - Annual exit plan reviews

Process Risk Control Matrix- Vendor Monitoring

Process	Risk	Control	Test Strategy
Vendor Monitoring	Vendor does not perform in accordance with the defined service levels	Performance issues are reported to the vendor manager for discussion with the vendor.	Based on inquiry understand the nature of some of the performance issues. Review supporting documentation for escalation to vendor manager or the vendor
		Monthly SLA reports are reviewed by the vendor manager and validated for accuracy. Where penalties payment are due, work with vendor to receive such payments	For a sample number of months, determine if SLA reports are reviewed against the contract. Where issues were identified, confirm that the correct escalation was taken
	Vendor can no longer provide services due to bankruptcy	Vendor financial health is regularly reviewed through news	Determine if relevant vednor news is monitored and escalated to appropriate individuals for consideration and action
		On an annual basis a formal finanical healthcheck is conducted to determine ongoing viability	On a sample basis, determine whether financial healthchecks are performed annually on key vendor relationships

Note: This PRCM is not intended to be complete and is used for illustration purposes only.

Conversion Project Review Scope

- Conversion and reconciliation of records
- Protection and destruction of records at the outsourcer
- Interim processing during migration
- Training and awareness

Conversion Project Key Attributes

Interim processing

- Migration
- Training and awareness

Historical records

- Handling and destruction of confidential records
- Access (e.g., tools, reports, etc.)

Conversion Project Review Scope

- Conversion and reconciliation of records
  - How are records being converted and mapped into the new environment?
  - How to access historical records not converted?
  - How does management gain assurance that the conversion was successful?
- Protection and destruction of records
  - How are records destroyed/removed from the vendor systems?

42

Conversion Project Review Scope

- Interim processing during migration
  - What are the plans for cutover of services?
  - How is transition services being monitored?
- Training and awareness
  - How are the new providers prepared to continue uninterrupted services?
  - How are organization personnel prepared to use the new services?

Useful References

- OCC Bulletin 2001-47: Third-Party Relationships
- FDIC FIL-50-2001: Bank Technology Bulletin on Outsourcing
- FFIEC “Outsourcing Technology Services”
- FFIEC “Supervision of Technology Service Providers”

Summary

- Organizations will continue to outsource
- Outsourcing has both benefits and risks
- Outsourcing left unmonitored may lead to more risks than benefits
- Robust monitoring will lead to outsourced relationships that maximize benefits with mitigated risks
- Regular audit of the monitoring and risk mitigation strategies for key relationships are essential to achievement of organizational objectives

Questions?

Thank You!