This Training is Brought to you by ComplianceOnline.

Effective Vendor Risk Management

Presenter:

Mario A. Mosse

April 21, 2017

This training session is sponsored by ComplianceOnline
The Largest GRC Advisory Network

Agenda

- Background
- Major Risks
- Critical Activities
- Vendor Governance
- Risk Management Lifecycle
  - Planning
  - Due Diligence and Selection
  - Contract Negotiations
  - Ongoing Monitoring
  - Termination

This Presentation is based on and contains excerpts from OCC Bulletin 2013-29

Agenda

- Oversight and Accountability
  - Board of Directors
  - Senior Management
  - Employees
- Documentation and Reporting
- Independent Reviews
- Conclusion

This Presentation is based on and contains excerpts from OCC Bulletin 2013-29

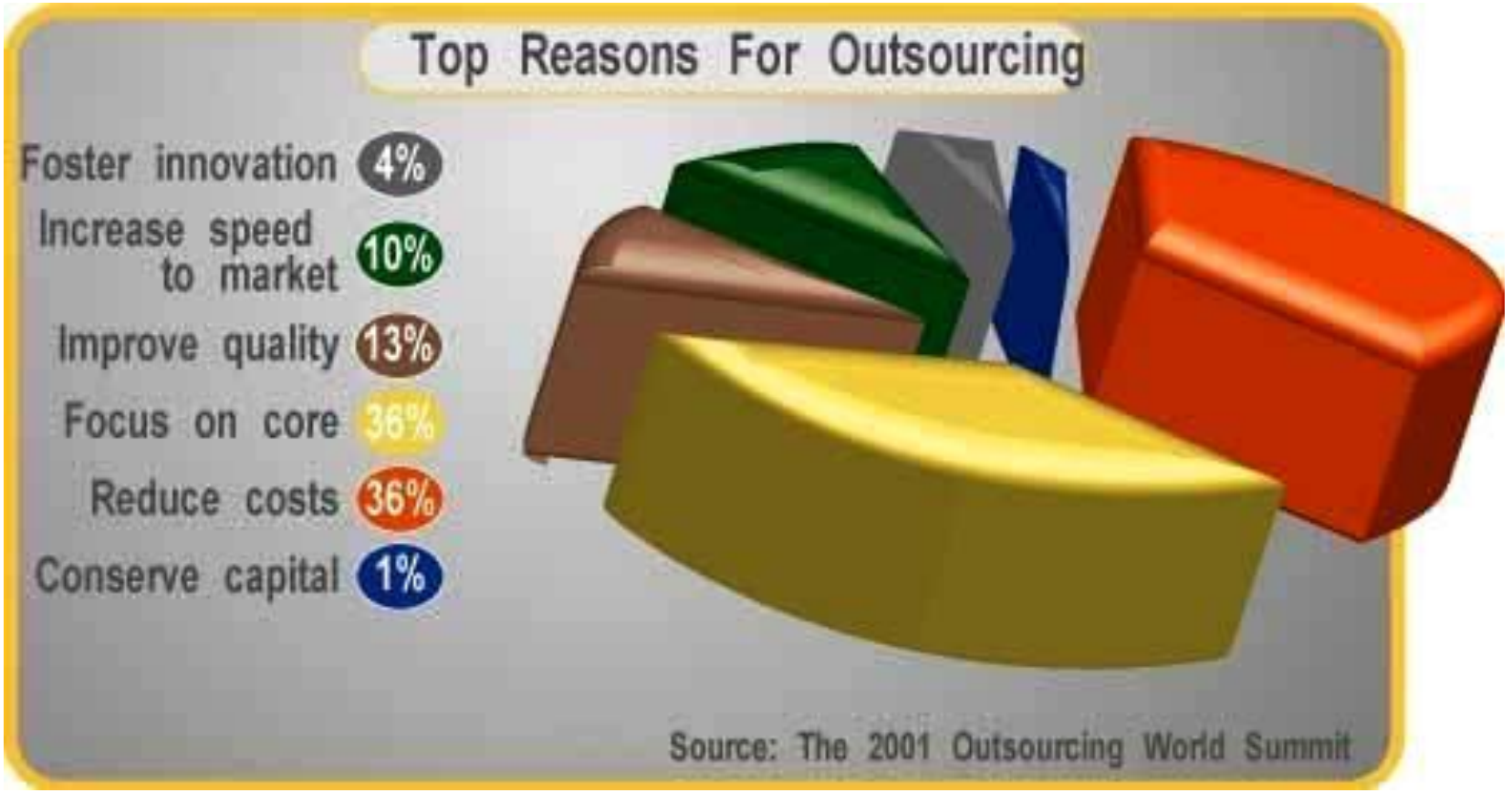
Background

Financial institutions continue to increase the number and complexity of relationships with both foreign and domestic third parties, such as:

- outsourcing entire functions to third parties, such as tax, legal, audit, or information technology operations
- outsourcing entire lines of business or products
- relying on a single third party to perform multiple activities
- working with third parties that engage directly with customers
- engaging vendors that subcontract activities to other foreign and domestic providers
- contracting with third parties whose employees, facilities, and subcontractors may be geographically concentrated
- working with a third party to address deficiencies in operations or compliance with laws or regulations

Background

Background



Major Risks

- Failure to properly assess and understand the risks and direct and indirect costs involved in third party relationships
- Failure to perform adequate due diligence and ongoing monitoring of third-party relationships
- Entering into contracts without assessing the adequacy of a third party's risk management practices
- Entering into contracts that incentivize a third party to take risks that are detrimental to the firm or its customers, in order to maximize the third party's revenues
- Engaging in informal third-party relationships without contracts in place

Critical Activities

Significant:

Functions	• Payments, Clearing, Settlements, custody)
Shared Services	• Information Technology, Payroll, Accounts Payable)
Risk	• Activities that could cause significant financial, legal or reputational risk if third party fails to meet expectations
Investment	• Activities requiring significant investment in resources to implement and manage the third-party relationship
Impact	• Activities that could have a major impact on operations if the vendor relationship had to be terminated

Vendor Governance

Major elements of a vendor governance framework:

Risk Management Lifecycle

Risk Management Lifecycle

Planning

Major steps in the planning process:

- **Discuss** risks inherent in the activity
- **Outline** strategic purposes
- **Assess** complexity of arrangement
- **Determine** if potential benefits outweigh estimated costs
- **Consider** how other strategic initiatives could be affected
- **Consider** impact on employees
- **Assess** customer impact

Planning

- **Consider** contingency plans if the firm needs to transition the activity to another third party or bring it in-house
- **Assess** need to comply with specific laws and regulations
- **Consider** impact on diversity policies and practices
- **Detail** selection, assessment, and oversight process, including monitoring vendor's compliance with contract
- **Obtain** approval from board of directors when critical activities are involved

Due Diligence and Selection

Major steps in the due diligence process:

- Strategies and Goals
- Legal and Regulatory Compliance
- Financial Condition
- Business Experience and Reputation
- Fee Structure and Incentives
- Qualifications, Backgrounds, and Reputations of Company Principals
- Risk Management
- Information Security
- Management of Information Systems

Due Diligence and Selection

- Resilience
- Incident-Reporting and Management Programs
- Physical Security
- Human Resources Management
- Reliance on Subcontractors
- Insurance Coverage

Contract Negotiation

Contracts should generally address the following:

- Nature and Scope of Arrangement
- Performance Measures or Benchmarks
- Responsibilities for Providing, Receiving, and Retaining Information
- The Right to Audit and Require Remediation
- Responsibility for Compliance With Applicable Laws and Regulations
- Cost and Compensation
- Ownership and License
- Confidentiality and Integrity

Contract Negotiation

- Business Resumption and Contingency Plans
- Indemnification
- Insurance
- Dispute Resolution
- Limits on Liability
- Default and Termination
- Customer Complaints
- Subcontracting
- Foreign-Based Third Parties
- Regulatory Supervision

Ongoing Monitoring

Major items that should be part of vendor monitoring:

- Changes to business strategy and reputation
- Compliance with legal and regulatory requirements
- Financial condition
- Insurance coverage
- Retention of key personnel
- Ability to effectively manage risk
- Process for adjusting policies and procedures when necessary

Ongoing Monitoring

- Information technology used
- Ability to recover from service disruptions or degradations
- Reliance on subcontractors, their location, and ongoing monitoring and control testing
- Agreements with other entities that may pose a conflict of interest or introduce reputation, operational, or other risks
- Ability to maintain the confidentiality and integrity of information and systems
- Volume, nature, and trends of complaints, specially those that indicate compliance or risk management problems
- Ability to appropriately remediate customer complaints

Termination

Items to consider in the event of contract termination:

- Consider legal, regulatory, customer, and other impacts that might arise
- Assess risks associated with data retention and destruction, information system connections and access control issues, or other control concerns
- Decide on handling of joint intellectual property developed during the course of the arrangement

- Assess reputation risks if the termination happens as a result of the third party's inability to meet expectations
- Consider extent and flexibility of termination rights

Oversight and Accountability

- The financial institution's board of directors (or a board committee) and senior management are responsible for overseeing the firm's overall risk management processes.
- The board, senior management, and employees within the lines of businesses who manage the third-party relationships have distinct but interrelated responsibilities to ensure that the relationships and activities are managed effectively and commensurate with their level of risk and complexity, particularly for relationships that involve critical activities.

Roles and Responsibilities

- Board of Directors
- Senior Management
- Business and Functional Units (First Line of Defense)
- Corporate Oversight Functions (Second Line of Defense)
- Internal Audit (Third Line of Defense)

Documentation and Reporting

A firm should properly document and report on its third-party risk management process and specific arrangements throughout their life cycle. Proper documentation and reporting facilitates the accountability, monitoring, and risk management associated with third parties and typically includes:

- A current inventory of all third-party relationships, which should clearly identify those relationships that involve critical activities and delineate the risks posed by those relationships across the firm
- Approved plans for the use of third-party relationships
- Due diligence results, findings, and recommendations
- Analysis of costs associated with each activity or third-party relationship, including any indirect costs assumed by the firm

Documentation and Reporting

- Executed contracts
- Regular risk management and performance reports required and received from the third party (e.g., audit reports, security reviews, and reports indicating compliance with service-level agreements)
- Regular reports to the board and senior management on the results of internal control testing and ongoing monitoring of third parties involved in critical activities
- Regular reports to the board and senior management on the results of independent reviews of the firm's overall risk management process

Independent Reviews

- Periodic independent reviews of the third-party risk management process should be conducted.
- Results of independent reviews should be analyzed to determine whether and how to adjust the firm's third-party risk management process, including policy, reporting, resources, expertise, and controls.
- Understanding of the effectiveness of the firm's third-party should inform decisions about commencing new or continuing existing third-party relationships, bringing activities in house, or discontinuing activities.
- Management should respond promptly and thoroughly to significant issues or concerns identified and escalate to the board if the risk posed is approaching the firm's risk appetite limits.

Conclusion

- Financial institutions should adopt risk management processes commensurate with the level of risk and complexity of their third-party relationships.
- They should ensure comprehensive risk management and oversight of third-party relationships involving critical activities.
- An effective risk management process throughout the life cycle of the relationship includes:
  - plans that outline the firm's strategy, identify the inherent risks of the activity, and detail how the firm selects, assesses, and oversees the third party.
  - proper due diligence in selecting a third party.
  - written contracts that outline the rights and responsibilities of all parties.

Conclusion

- ongoing monitoring of the third party's activities and performance.
- contingency plans for terminating the relationship in an effective manner.
- clear roles and responsibilities for overseeing and managing the relationship and risk management process.
- Documentation and reporting that facilitates oversight, accountability, monitoring, and risk management.
- Independent reviews that allow firm management to determine that the firm's process aligns with its strategy and effectively manages risks.

THANK YOU FOR YOUR ATTENTION

For more information on the seminar and questions contact us at :
webinarassist@complianceonline.com or call us at: **1- 650- 620 – 3937 / 3915**