sifma

Internal Auditors Society

Internal Audit Guidelines

Leading Practices in Auditing Third-Party Risk Management

June 2016

The Audit Guidelines (the "guidelines") are intended to provide members of the Internal Auditors Society ("IAS"), a society of the Securities Industry and Financial Markets Association ("SIFMA"), with information for the purpose of developing or improving their approach towards auditing certain functions or products typically conducted by a registered broker-dealer. These guidelines do not represent a comprehensive list of all work steps or procedures that can be followed during the course of an audit and do not purport to be the official position or approach of any one group or organization, including SIFMA, or any of its affiliates or societies. Neither SIFMA, nor any of its societies or affiliates, assumes any liability for errors or omissions resulting from the execution of any work steps within these guidelines or any other procedures derived from the reader's interpretation of such guidelines. In using these guidelines, member firms should consider the nature and context of their business and related risks to their organization and tailor the work steps accordingly. Internal auditors should always utilize professional judgment in determining appropriate work steps when executing an audit. Nothing in these guidelines is intended to be legal, accounting, or other professional advice.

Leading Practices in Auditing Third-Party Risk Management

Third-party risk management is a persistent current regulatory focus in recent years, with US financial services regulators including FINRA, FDIC, FRB and the OCC issuing bulletins in recent years. In the US, the Comptroller of the Currency, Tom Curry, identified key risks as: (1) the extent to which service providers are consolidating and leaving financial institutions more dependent upon a single vendor; (2) increased reliance on outside vendors, including foreign-based subcontractors, to support critical activities and the legal and regulatory implications of where data is stored or transmitted; and (3) the access third parties have to large amounts of sensitive bank or customer data. This, coupled with the reputational impact of privacy and data breaches, mean that third parties are introducing ever more risk to financial institutions.

Outside the US, the Financial Conduct Authority in the UK, BaFin in Germany, and the Monetary Authority of Singapore have also been active in assessing the state of their supervised industries providing guidance on topics as current as outsourcing to the cloud.

Highlights of Regulatory Guidance

The OCC has provided the clearest and most comprehensive set of regulatory expectations that should be embedded in business practice and internal audit programs throughout the cycle of outsourcing. The following points come through from a review of the regulatory guidance:

- **Governance** – The program must have clear definition of roles and responsibilities, including at the board level, and escalation, including performance lapses and/or other instances of non-compliance with contractual provision.
- **A risk-based approach is crucial** – Given the breadth and depth of third-party relationships, a comprehensive risk assessment framework that allows for consistent treatment according to risk and criticality is needed.
- **The process must be formal** – The risk assessment process should be defined as mandatory. Key steps in the third-party management lifecycle – at a minimum vendor risk assessments, due diligence, contingency and termination – should be clearly documented and reviewed by senior management or the board, as appropriate.
- **The firm must manage the full lifecycle** – from qualification and selection through relationship maintenance, contingency planning, monitoring, and sunsetting/exiting.
- **The importance of a holistic view** – Third-party risk is derived from any outside relationship, including joint venture, affiliate, contractor, etc. Firms should maintain an inventory of key affiliates and vendors and continually asses the completeness of this inventory.
- **Third-party risk management should be integrated into enterprise risk** – Third-party risk management should be consistent with all other facets of risk management and integrated into the firm-wide risk appetite statement.
- **Your third-parties have third-party risk also** – Fourth party – and further – risk exists also. Firms will need to assess the impact that the vendors of your vendor could have on your control environment
- **Management processes and contracting should ensure transparency** – The firm must have visibility into services performed, pricing and risk management by its third-parties.

Regulatory References:

OCC Bulletin 2013-29: http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html, Office of Comptroller of the Currency, Third Party Relationships, Risk Management Guidance, October 30, 2013

FRB SR letter 13-19/CA letter 13-21: http://www.federalreserve.gov/bankinforeg/srletters/sr1319.htm, Board of Governors of the Federal Reserve System, Guidance on Managing Outsourcing Risk, December 5, 2013

FDIC FI Letter FIL-44-2008: https://www.fdic.gov/news/news/financial/2008/fil08044a.pdf, Federal Depository Insurance Corporation, Guidance for Managing Third-Party Risk, June 6, 2008

FINRA Notice to Members 05-48: https://www.finra.org/sites/default/files/NoticeDocument/p014735.pdf , FINRA, Outsourcing, July 2005

FINRA Notice to Members 11-14: https://www.finra.org/sites/default/files/NoticeDocument/p123398.pdf, FINRA, Third-Party Service Providers, March 2011, proposed Rule 3190)

FFIEC: http://ithandbook.ffiec.gov/it-booklets/e-banking/risk-management-of-e-banking-activities/managing-outsourcing-relationships.aspx, Federal Financial Institutions Examination Council, IT Booklet - Oversight and Monitoring of Third Parties

FCA (UK): https://www.fca.org.uk/news/tr15-7-delegated-authority-outsourcing-in-the-general-insurance-market, Financial Conduct Authority, TR15/7: Delegated authority: Outsourcing in the general insurance market

FCA (UK): https://www.fca.org.uk/news/guidance-consultations/gc15-06-proposed-guidance-firms-outsourcing-cloud, Financial Conduct Authority, GC15/6: Proposed guidance for firms outsourcing to the 'cloud' and other third-party IT services

BaFIN (Germany): http://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2013/fa_bj_2013_08_outsourcing_institute_en.html, Federal Financial Supervisory Authority, Outsourcing: BaFin compares outsourcing by institutions

MAS (Singapore): http://www.mas.gov.sg/news-and-publications/consultation-paper/2014/consultation-paper-on-notice-and-guidelines-on-outsourcing.aspx, Monetary Authority of Singapore, Guidelines on Outsourcing

Key Risks and Considerations

Consistent throughout the regulatory guidance is the framework of a four-step process for identifying and managing third-party risk:

I) Risk Assessment of Proposed Outsourced Function or Service
II) Due Diligence in Selecting a Third-Party
III) Contract Structuring and Review
IV) Oversight by Board of Directors, Senior Management and Ongoing Monitoring by Business Relationship Owners

The addition of governance of this program completes the framework. Key risks underlying these steps include:

Risk Assessment of Proposed Outsourced Function or Service:

1) Lack of a consistent and comprehensive risk assessment process, flexible enough to cover all third parties, and their subcontractors, with risk categories that drive appropriate controls through the lifecycle
2) Risk assessment omits risk inherent in the process and/or additional risk of outsourcing
3) Risk not assessed by qualified resources
4) Risk assessment does not include institution's ability to oversee outsourced relationship
5) Risk assessment omits strategic, operational and financial ramifications of depending on third parties for key functions
6) Risk assessment excludes analysis of whether third-party's activities could be viewed as predatory, discriminatory, abusive, unfair, or deceptive to consumers.

Due Diligence in Selecting a Third-Party:

Incomplete process for evaluating the third-party, omitting factors such as:

1) Financial strength and depth and quality of supporting documentation (e.g., financial statements, etc.)
2) Overall significance of the proposed revenue to the third-party, and investment needed to provide service
3) Business Reputation, including regulatory findings, customer complaints, litigation and OFAC/background checks
4) Experience, competence and maturity in providing the proposed service
5) Qualification and background of the third-party's principal management, including the tone at the top (i.e., ethics, established code of conduct and fraud risk assessments)
6) Strategies and goals, including service philosophies, quality initiatives, efficiency improvements, and employment policies
7) Ability to perform the proposed functions using current systems or the need to make additional investment
8) Use of subcontractors by the third-party and information about the third-party's risk assessment of the subcontractor
9) Scope and maturity of internal controls, systems, information security and privacy protections, and audit coverage (e.g., availability of Type 2 SOC 1, Type 2 SOC 2 Report, etc.)
10) Sufficiency, flexibility and ease of interface with management information systems

11) Ability to demonstrate compliance with regulatory and legal requirements
12) Business continuity and disaster recovery capabilities
13) Knowledge of relevant consumer protection laws and regulations
14) Adequacy of insurance coverage

Contract Structuring and Review:

1) Unclear definition of services, including performance standards, form, frequency, location, etc.
2) Missing definition of compensation, including terms, timing and amounts
3) Unclear definition of roles and responsibilities, including compliance with laws and regulations
4) Absence of comprehensive documented review and approval of contract by legal and board as determined by materiality/risk
5) Lack of clear, transparent reporting
6) Lack of right to audit
7) Lack of complaint or problem identification and escalation on the part of the third-party
8) Unclear compensation and payment terms, or inconsistent with market or value pricing
9) Omission of confidentiality and security of information
10) Foreign-based service providers are not identified, qualified and monitored for compliance with applicable US laws, regulations, and regulatory guidance
11) Unclear information regarding ethics and codes of conduct employed by the service provider
12) Omission of business continuity and disaster recovery
13) Unclear performance metrics and reporting
14) Lack of "look-through" to subcontractors
15) Missing key contract elements: Confidentiality and privacy breach notification; Ownership and licensing; Limits on liability; Indemnification; Dispute and resolution; Default and termination; Insurance

Oversight by Board of Directors, Senior Management and Ongoing Monitoring by Business Relationship Owners:

1) Lack of comprehensive oversight responsibilities to include finance, operational risk, information technology, and compliance functions as needed, with assessments of each area by internal audit as part of risk-based audit cycle
2) Lack of complete suite of oversight activities (performance and service level reporting; reporting and review of complaints; escalation of third-party issues; site visits; audits, etc.)
3) Policies and procedures are not comprehensive, authorized, maintained or communicated to relevant employees
4) Management does not set the appropriate tone in managing third-party risk
5) Lack of third-party oversight by appropriate business relationship owners, with appropriate frequency determined by risk ranking, to determine sufficiency of performance and consistency of risk factors
6) Lack of independent program oversight (e.g., by second or third line of defense) and/or onsite visits
7) Ineffective onboarding of third parties

Lack of ongoing monitoring, omitting factors such as:

8) Periodic risk-based due diligence during course of relationship or when considering a renewal of a contract
9) Risk mitigation plans for higher risk service providers that include processes such as additional reporting by service provider or heightened monitoring
10) Determining whether service provider is complying with Federal consumer financial law
11) Monitoring performance metrics and service level agreements linked to provisions in contract
12) Escalating oversight and monitoring when service providers are failing to meet performance, compliance, control, or viability expectations
13) Maintaining an exit strategy, including a pool of comparable service providers, in the event that a contracted service provider is unable to perform
14) Previously identified issues/recommendations are not resolved
15) Periodic training programs are not appropriate, relevant, or, not performed

Leading Practices in Auditing Third-Party Risk

In addition to assessing the risks identified above, the regulatory guidance suggests the following leading practices in auditing Third-Party Risk:

- **Audit Involvement** – Audit groups should be involved early in the development of third-party risk management programs and based on risk and materiality to the organization, early in the relationship with new third parties.
    - Planning – Programs should be structured to allow IA review of third-party needs in real-time
    - Selection – IA should be involved in reviewing the third-party selection process, based again on risk and materiality to the organization.
    - Contract Review - IA should verify that controls are being built into the process at the contract phase
- **Expect Maturity in a Third-Party** – Evaluate whether the third-party has experience in supporting client needs – and the flexibility to react when these needs evolve.
- **Criticality of Service Drives Closeness of Relationship** – The greater the need of the service provided, the greater the expectation of service levels and the transparency of delivery and risk management must be.
- **An Integrated Team** – A comprehensive management solution requires a comprehensive audit response. Evaluating a third-party risk management program is not just an IT role.

Call to Action

With the competing pressures of businesses expanding their reliance on third parties in order to manage costs and focus on core competences, and regulators heightening expectations regarding the risk this brings, the strength of third-party risk management has never been more important to the strength of the firm. Internal Audit can play a key role in developing the performance expected of the third-party function by integrating regulatory guidance with key risk management principals, thereby providing management, the board, and regulators the assurance they require that this key function is in alignment with their needs and is operating effectively.

Thought Leadership

Deloitte: http://www2.deloitte.com/us/en/pages/risk/articles/managing-third-party-risk-in-financial-services-key-considerations-for-the-extended-enterprise.html

EY: http://www.ey.com/Publication/vwLUAssets/ey-third-party-risk-management/$FILE/ey-third-party-risk-management.pdf

KPMG: http://advisory.kpmg.us/risk-consulting/forensics/third-party-risk-management.html

PwC: http://www.pwc.com/us/en/risk-assurance-services/vendor-risk-management.jhtml