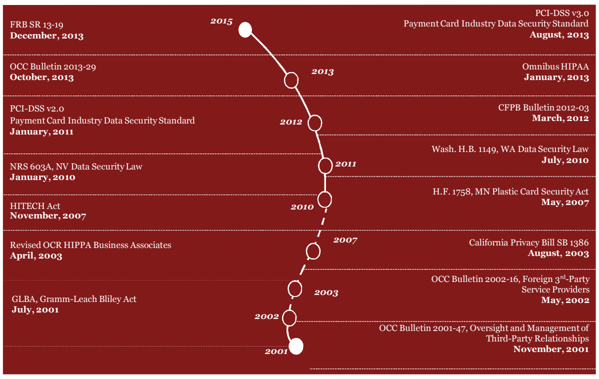
www.pwc.com

Third Party Risk Management:
What could go wrong?

April 7, 2016

pwc

Regulatory History



PwC

Office of the Comptroller of the Currency (OCC) focus:
What are the expectations of the OCC?

Comptroller of the Currency
Administrator of National Banks
US Department of the Treasury

The OCC expects financial firms to practice effective **Third Party Risk Management (TPRM)** regardless of whether the bank performs the activity internally or through a third party. A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner an in compliance with applicable laws.

Examinations may evaluate safety and soundness risks, the financial and operational viability of the third party to fulfill its contractual obligations, compliance with applicable laws and regulations, including consumer protection, fair lending, BSA/AML and OFAC laws, and whether the third party engages in unfair or deceptive acts or practices in violation of federal or applicable state law.

The OCC Bulletin 2013-29 set the expectations that supervised entities will:

- ***Plan and outline*** the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party.
- ***Perform proper due diligence*** in selecting a third party.
- Have written contracts that outline the ***rights and responsibilities of all parties***.
- ***Perform ongoing monitoring*** of the third party's activities and performance
- Prepare ***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.
- ***Conduct independent reviews*** that allow bank management to determine that the bank's process aligns with its strategy and effectively manages risks.

3

PwC

Consumer Financial Protection Bureau (CFPB) focus:
What are the expectations of the CFPB?

The CFPB was established to promote fairness and transparency for consumer financial products and services as a result of the Dodd-Frank Act, a law passed after the financial crisis in 2008.

Examinations are expected to focus on key **Third Party Risk Management** evaluation activities, such as how the firm monitors compliance management systems, customer complaints management, and compliance with certain consumer protection laws and regulations.

The CFPB bulletin of 2012-13 set the expectations that supervised entities will:

- ***Conduct thorough due diligence*** to verify that the supplier understands and is capable of complying with Federal consumer financial laws
- Request and ***review supplier policies, procedures, internal controls, and training materials*** to ensure that the supplier is conducting appropriate training and oversight of employees or agents that have consumer contact or compliance responsibilities
- Include in the contract with the supplier clear expectations about compliance, as well as ***appropriate and enforceable consequences for violating any compliance-related responsibilities***, including engaging in unfair, deceptive, or abusive acts or practices
- ***Establish internal controls and on-going monitoring*** to determine whether the supplier is complying with Federal consumer financial laws
- ***Take prompt actions to address fully any problems identified*** through the monitoring process, including terminating the relationship where appropriate

TPRM Business Drivers

Globalization continues and business partnerships are increasingly being leveraged as strategic enablers. This increases the need for Third Party Risk Management.

According to PwC's 14th Annual Global CEO Survey:
- Companies are reshaping strategies and operating models–focusing on **innovation, collaboration, and talent**–to find new sources of revenue growth and competitive advantage
- Roughly **a third of CEOs** indicated their companies plan to complete a **cross-border merger or acquisition**, or outsource a business process or function in the next year

Business drivers

Partnership will be key
- **40%** of CEOs expect the majority of innovations over the next three years to be **co-developed** with partners
- **50%** said their companies will enter into **a strategic alliance or JV** in the coming year
- As organizational models shift and risk profiles evolve, executives and Boards seek **greater transparency** and increased assurance that the company's most significant risks are appropriately mitigated

Reputational Drivers

Sample headiness involving third parties:

The hackers who stole 40 million credit and debit card numbers from a large discount retailer appear to have breached the discounter's system by using credentials stolen from a vendor.
– Wall Street Journal, January 2014

Hackers successfully stole prepaid debit card information from the Indian and US-based third-party vendors of several large multi-national credit card institutions, **fraudulently withdrawing $45M from ATMs worldwide.**
– Wall Street Journal, May 2013

17,300 patients have their protected health information breached following a scam executed by a group posing as a vendor.
– Modern Healthcare, May 2013

What a vendor got wrong: The risky business of hiring from competitors
A vendor hiring the former CEO of its client's largest competitor, to lead its company. Despite a decades-long relationship, the client terminated its contract with the vendor due to this hiring decision.
– Modern Healthcare, May 2013

FTC Data Security Settlement Highlights Need for Third-Party Vendor Management and Oversight
Federal Trade Commission (FTC) announced a settlement with a translation services providers following the public exposure of thousands of medical transcript files containing personal medical information.
– HL Chronicle of Data Protection, January 2014

A bank points outage finger at its technology provider
A bank says a failure on its technology provider's part to correctly fix an identified instability within the bank's storage system led to the seven-hour service outage last week.
– By Eileen Yu, ZDNet Asia on July 14, 2010

'We Blew It': A world leader in consumer retail goods Admits to Mistakes Over Child Labor
A multi-billion dollar sportswear company admitted yesterday that it "blew it" by employing children in Third World countries but added that ending the practice might be difficult.
– Steve Boggan Independent/UK Oct 20, 2001

Breach at a large merchant processor cost approximately **$94 million** and removal from the global registry of a major card issuer.
–CNN, March 2012

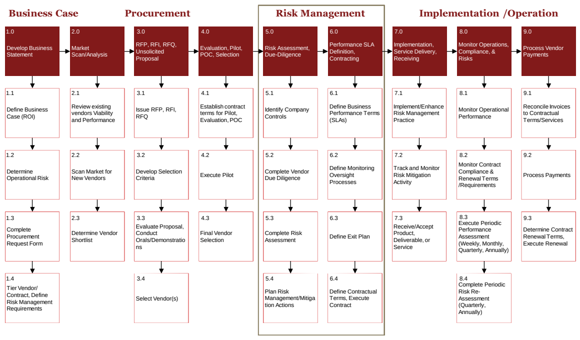
3.6 million personal income tax returns and 657,000 business filings exposed due to third party data breach.
– Washington Post, October 2012

Foreclosure defense lawyer is missing; his law partner **says at least $6M in firm money is gone**
A foreclosure defence lawyer in Florida has been reported missing as authorities investigate the reported disappearance of at least $6 million in funds held by his law firm in trust accounts.
– Criminal Justice Apr. 15, 2013

Investigators said that for years, high-ranking executives at the company's China operations used **travel agencies as money-laundering shops** to funnel bribes to government officials.
– New York Times, July 2013

Recent Ponemon Institute surveys reveal:
- Unsecure third parties including cloud providers are seen as one of the top three threats to an organization
- 41% of the companies surveyed experienced a data breach caused by a third party. And the consequent loss of brand value typically ranged from $184 million to more than $330 million

Taxonomy: Third Party Risk Management



PwC 7

TPRM Program Management Components

Governance and Organization

Accountability & Oversight | Documentation & Reporting | Organizational Coverage | Risk Management | Independent Reviews

Program Management

Board Approved Program | Completeness | Enterprise Coverage | Third Party Coverage

Planning
- Inherent Risks
- Complexity Assessment
- Cost/Benefit
- Other Initiatives
- Dual Employee
- Customer Impact
- Information Security
- Strategic Objectives
- Contingency Plans
- Laws & Regulations
- Diversity
- Selection & Contract Monitoring
- Critical Activities

Due Diligence
- Strategies & Goals
- Legal & Regulatory
- Financial Risk
- Experience & Reputation
- Fees & Incentives
- Qualification, Background, Reputation
- Risk Management
- Information Security
- Management Information Systems
- Resilience
- Incident Reporting & Management
- Physical Security
- Subcontractors
- Insurance Coverage
- Conflicting Arrangements
- Country Risk
- Reputational Risk
- Operational Competency
- Fraud
- FCPA
- BSA/AML
- PCI-DSS

Contract Negotiation
- Nature & Scope
- Performance
- Information Handling
- Right to Audit
- Compliance
- Cost & Compensation
- Ownership & License
- Confidentiality & Integrity
- Contingency
- Indemnification
- Insurance
- Dispute Resolution
- Limits on Liability
- Default and Termination
- Customer Complaints
- Subcontracting
- Foreign Based 3rd Parties
- OCC-CFPB Supervision
- Diversity
- Records Management
- Amendments

On-going Monitoring
- Conflicting Interests
- Compliance
- Financial Condition
- Insurance
- Key Personnel
- Manage Risk Proactively
- Adaptable Process
- Technology
- Contingency Plans
- Subcontractors
- Confidentiality
- Customer Complaints
- Issues Management
- Credentials & Certifications
- Problem Management
- Monitoring Plan
- Testing/Quality Assurance

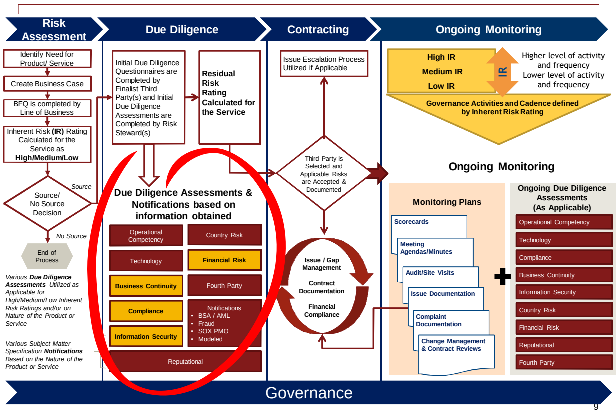
Termination
- Contingency Planning
- Transition
- Data
- Joint Intellectual Property
- Reputational Risk
- Written Exit Plan
- Identification of alternate sources
- Customer impact

Program Management

Program Support | Tactical Reporting | Tracking | Training | Tools and Technology | Continuous Improvement

PwC 8

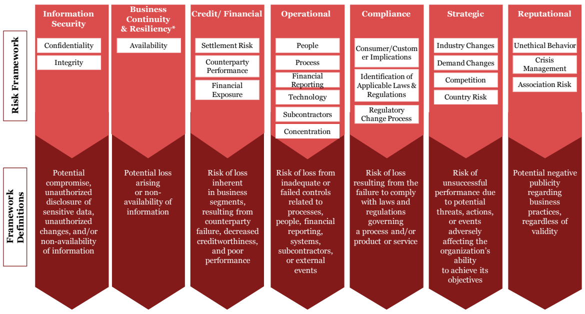
Third Party Risk Management Process Overview



PwC 9

Significant Enterprise Risk Dimensions

Significant enterprise risk dimensions must be identified and managed throughout the TPRM lifecycle.



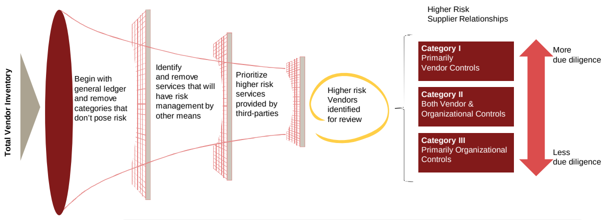
PwC

10

Vendor Stratification: Assessing Where Risk Exists

With hundreds up to tens of thousands of contracted vendors for many firms, assessments should only be accomplished for those suppliers that pose the highest inherent risk.

By designing an orderly risk ranking/rating system and screening for risk, firms can focus on contracts and suppliers that harbor the highest risk to the firm and its customers. Detailed assessments of controls are then performed at vendors with the highest risk, with less due diligence applied to vendors that hold lower risk.

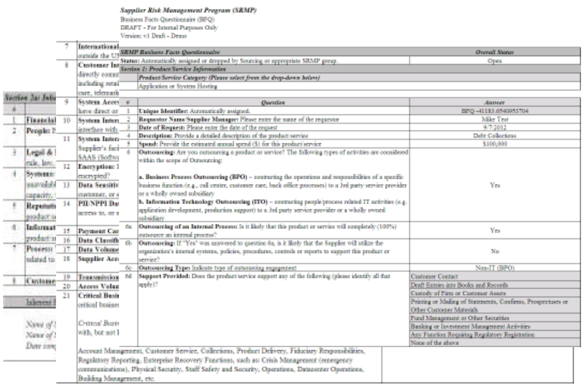


As the level of due diligence and the types of assessments required are ascertained, it will be important to check the allowances of the current contract with the vendor

PwC

11

Sample Vendor Stratification Questionnaire



Supplier Risk Management Program (SRMP)
Business Facts Questionnaire (BFQ)
DRAFT - For Internal Purposes Only
Version: v1 Draft - Demo

SRMP Business Facts Questionnaire		*Overall Status*
Status: Automatically assigned or dropped by Sourcing or appropriate SRMP group.		Open
Section 1: Product/Service Information		
	Product/Service Category (Please select from the drop-down below)	
	Application or System Hosting	

#	Question	Answer
1	**Unique Identifier:** Automatically assigned.	BFQ -41183.6540953704
2	**Requestor Name/Supplier Manager:** Please enter the name of the requestor	Mike Test
3	**Date of Request:** Please enter the date of the request	9/7/2012
4	**Description:** Provide a detailed description of the product/service	Debt Collections
5	**Spend:** Provide the estimated annual spend ($) for this product/service	$100,000
6	**Outsourcing:** Are you outsourcing a product or service? The following types of activities are considered within the scope of Outsourcing: **a. Business Process Outsourcing (BPO)** – contracting the operations and responsibilities of a specific business function (e.g., call center, customer care, back office processes) to a 3rd party service provider or a wholly owned subsidiary **b. Information Technology Outsourcing (ITO)** – contracting people/process related IT activities (e.g. application development, production support) to a 3rd party service provider or a wholly owned subsidiary	Yes
6a	**Outsourcing of an Internal Process:** Is it likely that this product or service will completely (100%) outsource an internal process?	Yes
6b	**Outsourcing:** If "Yes" was answered to question 6a, is it likely that the Supplier will utilize the organization's internal systems, policies, procedures, controls or reports to support this product or service?	No
6c	**Outsourcing Type:** Indicate type of outsourcing engagement	Non-IT (BPO)
6d	**Support Provided:** Does the product/service support any of the following (please identify all that apply)?	Customer Contact Draft Entries into Books and Records Custody of Firm or Customer Assets Printing or Mailing of Statements, Confirms, Prospectuses or Other Customer Materials Fund Management or Other Securities Banking or Investment Management Activities Any Function Requiring Regulatory Registration None of the above

Account Management, Customer Service, Collections, Product Delivery, Fiduciary Responsibilities, Regulatory Reporting, Enterprise Recovery Functions, such as: Crisis Management (emergency communications), Physical Security, Staff Safety and Security, Operations, Datacenter Operations, Building Management, etc.

PwC

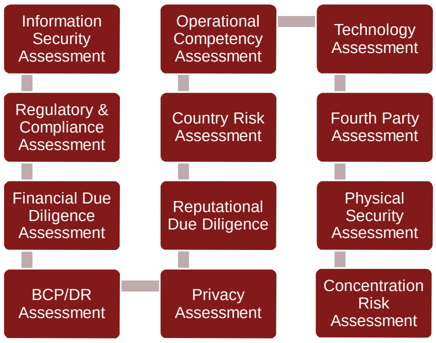
12

TPRM Risk Assessments

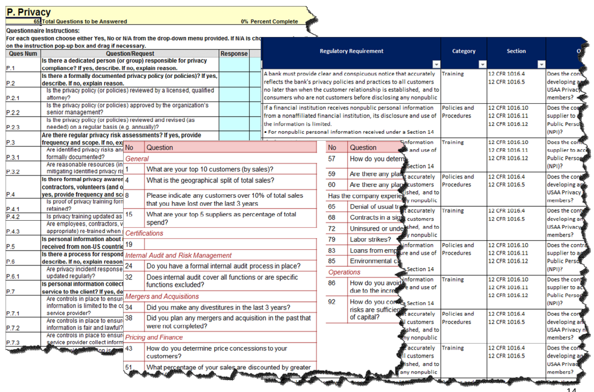
Establishing Controls; Setting Vendor Requirements

As the primary risks are identified for each supplier type or category, those third parties with key exposures can be proactively and continuously monitored. These take on the form of initial assessments, ongoing reporting, on-site monitoring, contractual provisions and transmittal of required audits and assessments (e.g. SOC2, SSEA, etc.)

Once completed, depending upon the third party risk and assessment results, suppliers are set up on an ongoing cycle to assure that risk is continuously minimized or mitigated.



Privacy, Compliance and Financial Risk Assessments



Risk Assessment Execution Approach

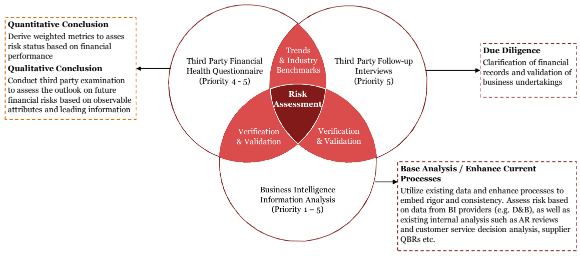
The approach below is utilized for both initial due diligence and on-going assessments. An effective tool may assist in the automation of workflow of the due diligence assessment process and standardize the reporting of results.

	Mobilization and service definition	Assessment preparation	Assessment execution	Assessment reporting and QA Review	Issue Management
Activities	• Determine required nature, timing and extent of assessment procedures • Inform third party of intent to review	• Confirm third party acceptance and understanding of scope • Determine assessment date • Confirm assessment resource • Obtain and review initial documentation from third party	• Conduct assessment (Self-assessment, Remote, On-site) • Gather supporting documentation • Document results • Coordinate assessment execution with third party, as required	• Finalize report and supporting evidence • Discuss and confirm identified issues with internal stakeholders and third party contacts • Perform internal QA of assessment report • Finalize compensating controls	• Determine issue management steps • Define remediation plans and closure timing • Determine risk acceptance plan, if required • Validate remediation plans and closure
Stake-holders	• Relationship Manager • Third Party • Risk Manager and/ or Assessor	• Relationship Manager • Third Party • Assessor • Risk Manager	• Third Party • Assessor • Risk Manager • Relationship Manager	• Assessor • Internal stakeholders • Third Party (as needed) • QA Reviewer	• Risk Manager • Relationship Manager • Third Party, as required
Outputs	• Scope Determination • Announcement Letter	• Assessment scope • Assessment date and time • Resourcing • Initial Evidence Request	• Draft assessment report and supporting evidence • Draft issues and compensating controls	• Finalize documentation • Issue/compensating controls summary	• Issue management steps • Remediation Plans • Risk Acceptance documentation • Metrics, reporting and scorecards

Oversight, monitoring, reviews tracking, service/status reporting

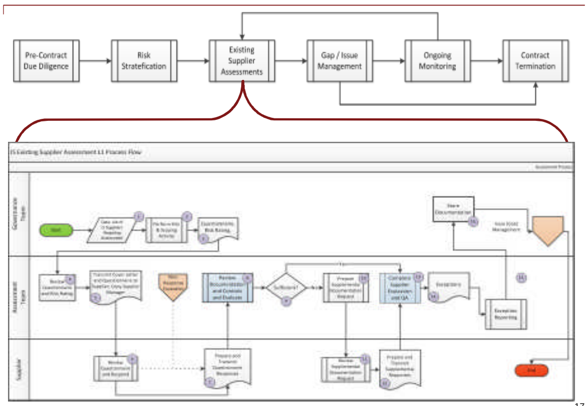
Financial Risk Assessment Approach

In conducting third party financial risk assessments, a tiered approach is constructed and typically occurs as follows. As priority of the third party increases, questionnaires and interviews are used to assess and determine the 'real' financial risk



PwC 16

High Level Processes for TPRM



PwC 17

Summary

Implementation of a Third Party Risk Management program is a complex process. But it is a necessary step in understanding the risks inherent when contracting with third parties and effectively managing enterprise risk.

PwC conducted a cross sector survey of third party risk in 2014 and found 35% of the firms surveyed had third party incidents that led to financial losses. 10% had an incident that had a reputational impact and 17% had incidents that had a client or customer impact. While a third party management program cannot eliminate those losses, it can help organizations improve the performance of their vendors and better manage third party risk.

The process is not without its rewards. The same survey indicated a majority of the respondents noted an improvement in third party performance/value. Significant numbers reported third party savings and cost avoidance in other parts of their organizations.

These increased benefits may include not only cost savings and performance benefits, but improvements in quality of service, performance improvements from standardization, better allocation of internal talent, and an improved organizational risk posture.

PwC 18

Questions and Discussion

PwC

19

www.pwc.com

Third Party Risk Management:

What could go wrong?

April 7, 2016

Scott Margolis, Director
Financial Services Cybersecurity & Privacy
scott.margolis@pwc.com
303.885.7728

David Miles, Director
Financial Services Cybersecurity & Privacy
david.miles@pwc.com
602.327.3049

pwc