Third Party Risk Management

By pwc

craigc@clearstar.net

877-796-2559 x849

Here with you today

Garit Gemeinhardt

Director

Third Party Risk Management

M: 704.344.7757
E: garit.gemeinhardt@pwc.com

Brett Croker

Director

Cybersecurity, Privacy & IT Risk

M: 678.419.2107
E: brett.j.croker@pwc.com

Agenda

Third Party Risk Management

- Background & Contact Information
- Questions to Consider
- Why is Third Party Risk Management important?
- What is Third Party Risk Management?
- Insights and Lessons Learned

Understanding and Reviewing Attest Reports

- SOC Reporting
- SOC Evaluation Pitfalls
- SOC Reporting Alternatives

Third Party Risk Management

How can your organization help mitigate information security and privacy risk resulting from third party activities?

www.pwc.com

pwc

Learning Objectives

A deep dive into Information Security & Privacy Third Party Risk Management Programs

- Describe the lifecycle activities within Third Party Risk Management and why it is important
- Explain implications of recent developments and current events
- Identify where Third Party Risk Management typically impacts Vendor Management events
- Identify key stakeholders, how they interact, and their roles and responsibilities of typical Third Party Risk Management programs
- Identify the three lines of defense and how each apply to a Third Party Risk Management program
- Explain the benefits of Third Party Risk Management

Questions to Consider

Planning / Governance

- Do you have an inventory of Third Parties?
  - Is it by service?
  - Is it risk ranked?
  - Do you have current contracts related to the service being provided?
- Do Third Parties go beyond traditional vendors and suppliers (e.g., affiliates)?
- Are there standardized risk profiling methodologies with defined assessment frequencies and types in place?
- Who is accountable for overseeing your TPRM Program? and managing it?

Due Diligence and Third Party Selection

- Are due diligence assessments performed prior to contracting?
  - Are they around privacy?
  - Are they around security?
- Do you know which of your third parties have access to data?
- Do you know which subcontractors are used by your third parties, and what work they are performing for you?

Contract Negotiation

- Do contract clauses include the authority to audit the Third Parties processes over the service provided?
- Are contracts for similar services consistent and contain Service Level Agreement's?

Ongoing Monitoring

- Do monitoring processes include both risk AND performance concerns?

Termination

- Do you have exit strategies in place for significant Third Party relationships?

Reputational Drivers

Sample headlines involving third parties

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.

– ZDNet Asia on July 14, 2010

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

Vendor mistake causes breach of 32,000 patients' data. The vendor was hired to transcribe care notes on what was supposed to be a secure website. However, the information remained publicly accessible because the vendor **apparently failed to activate a firewall.**

– Healthcare Business & Technology, August 2013

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

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

–CNN, March 2012

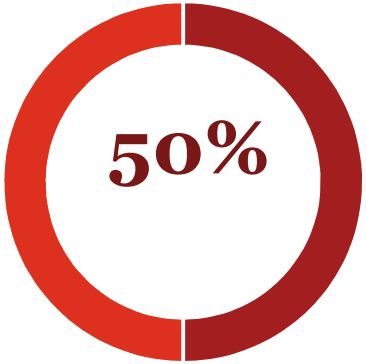
3.6 million personal income tax returns and 657,000 business filings exposed due to **third party data breach**.

– Washington Post, October 2012

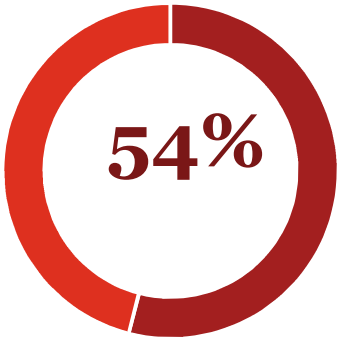
PwC's Global State of Information Security Survey results

Inventory of third parties that handle **personal data** of customers and employees

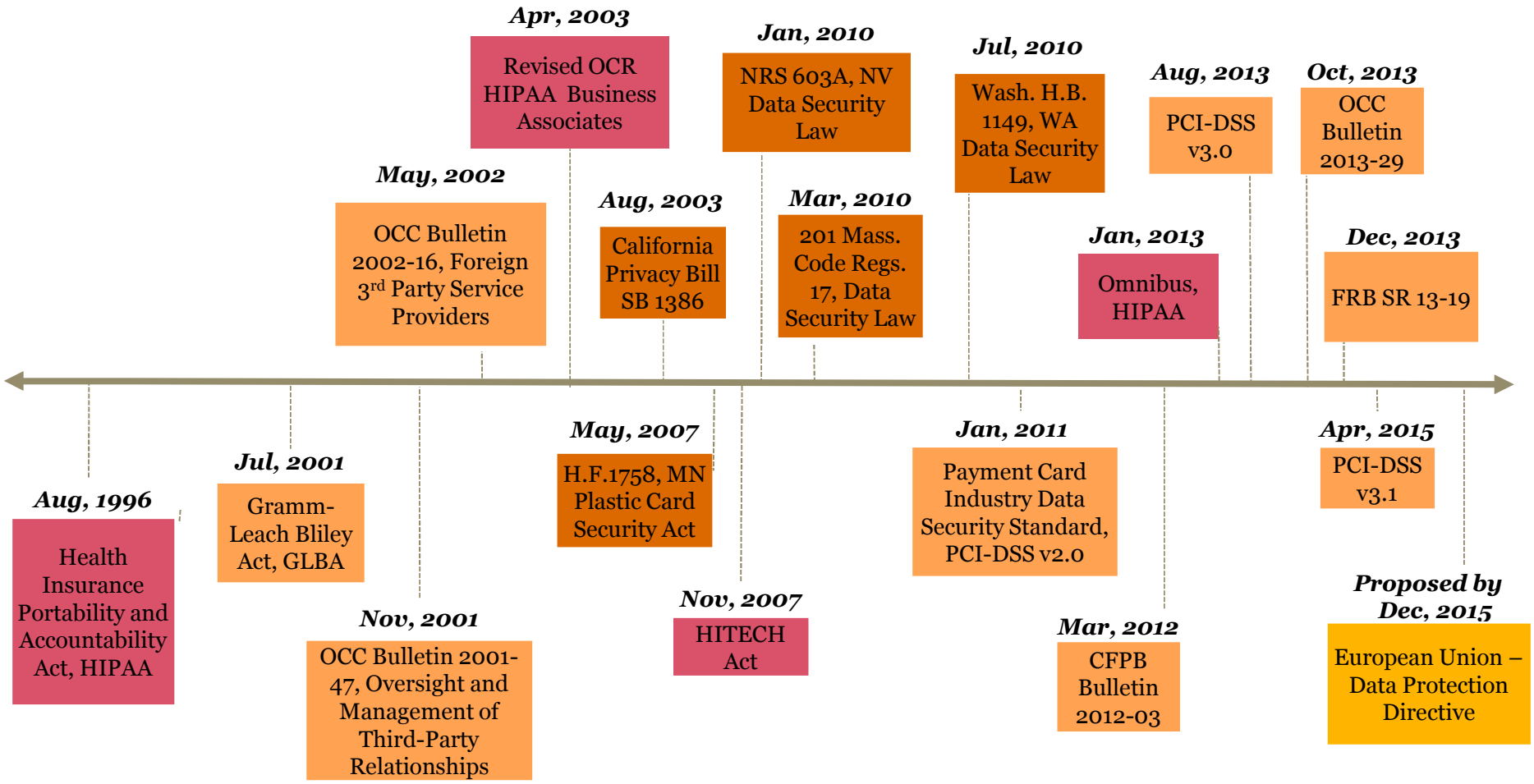
Perform risk assessments



Policy requiring third parties to comply with their privacy & security policies



Regulatory Considerations



Financial Services | Healthcare | State Regulations | European Union

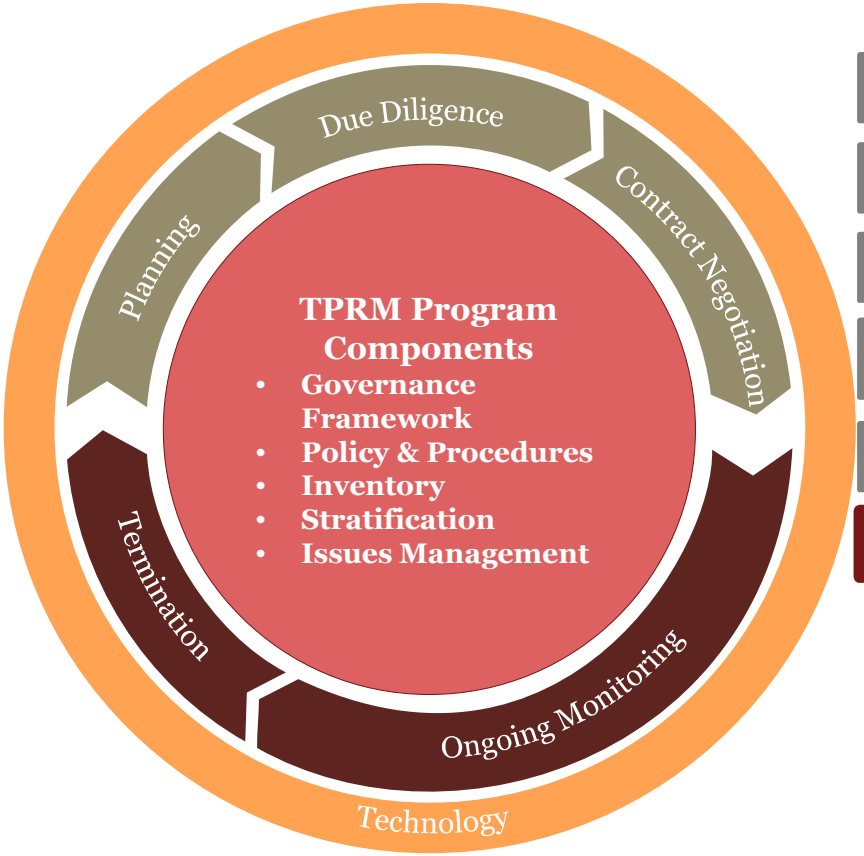
Third Party Risk Management Framework

Third Party risk management is focused on understanding and managing risks associated with third parties with which the company does business and/or shares data.

Third Parties

- Vendors
- Suppliers
- Joint Ventures
- Business Channels
- Marketing Partners
- Affiliates
- Broker Dealers
- Regulated Entities

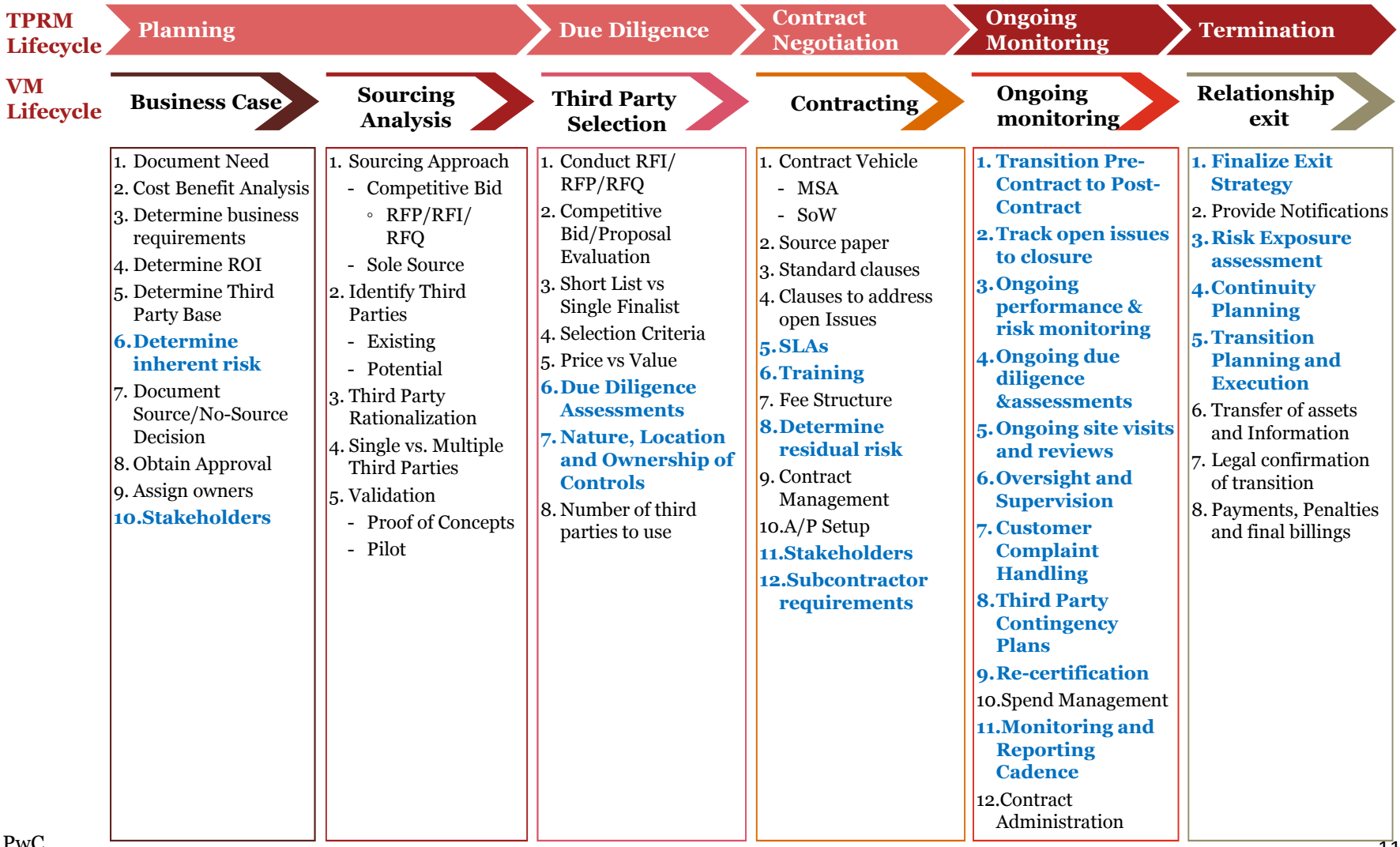
The PwC TPRM Framework



Risk Considerations

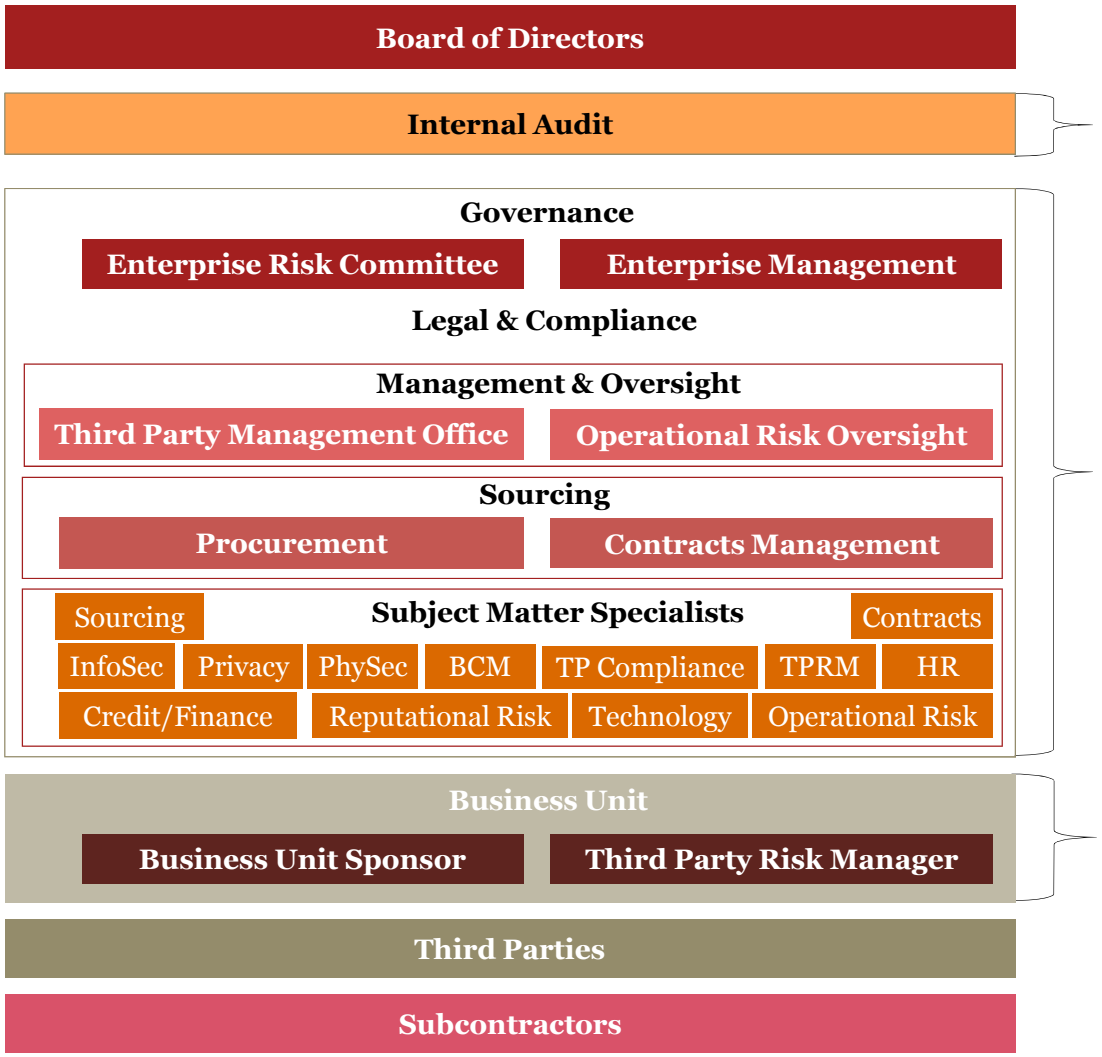
- Reputational
- Concentration
- Operational
- Regulatory / Compliance
- Financial
- Termination
- Business Continuity
- Subcontractor
- Country
- Technology
- Information Security
- Privacy

Vendor Management (VM) vs. Third Party Risk Management



Third Party Risk Management (TPRM) activities in **BLUE BOLD**

Third Party Risk Management – Program Governance



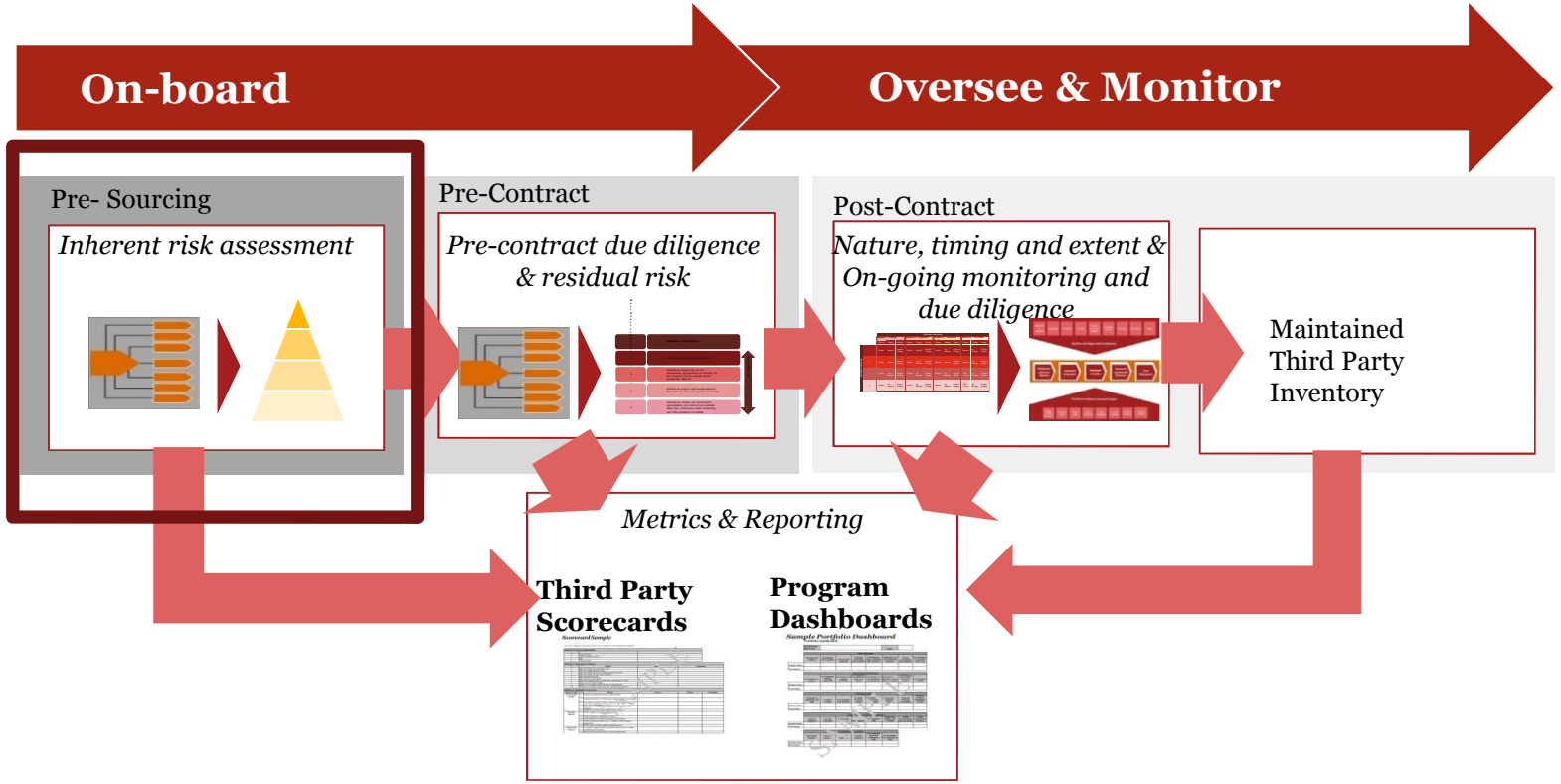
Third Line of Defense
- Independently test, verify and evaluate risk management controls against internal policies
- Report upon effectiveness of the program

Second Line of Defense
- Independent compliance framework, policy & oversight
- Design and assist in implementing company-wide risk framework and oversee enterprise risks
- Provide independent risk oversight across all risk types, business units and locations

First Line of Defense
- Primary responsibility for compliance and owner of risk
- BU managers and third party relationship owners are responsible for identifying, assessing and mitigating risk associated with their business
- Promote a strong risk culture and sustainable risk-return decision making

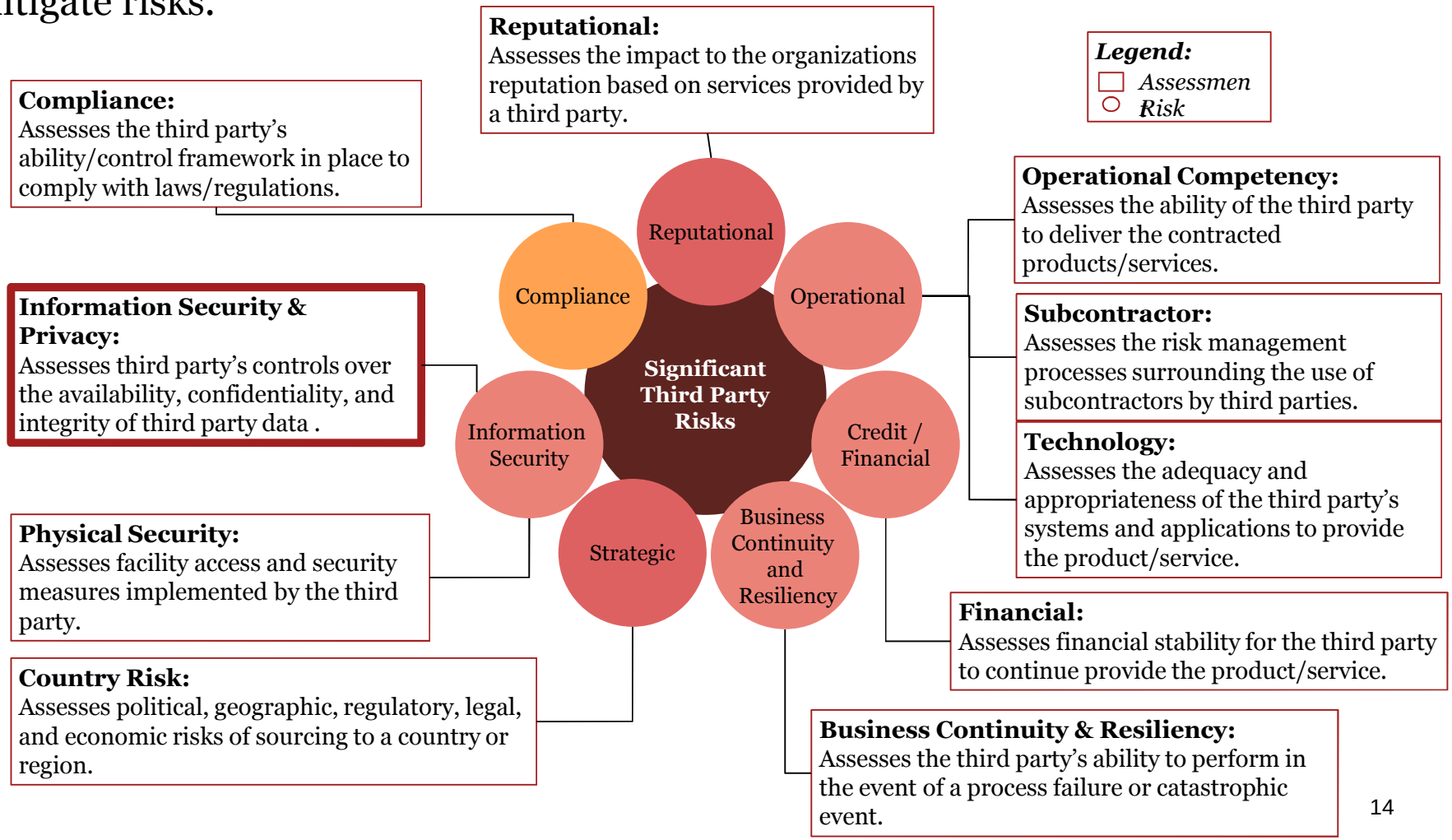
Planning

The Planning stage facilitates maintenance of the third party inventory, and enables management to focus resources and efforts on those services that present greater risk to the organization.



Due Diligence

The following correlates significant third party risks to the assessments utilized by organizations to evaluate the effectiveness of third party controls in place to mitigate risks.



Risk assessment types

The following are examples of Third Party due diligence assessments performed on potential and existing third parties to understand the existing control environment and capabilities.

Technology

- Technology Architecture
- Assets utilized
- Technology Roadmap
- Technological capabilities

Country

- Political
- Geographic
- Regulatory
- Legal
- Economic
- Travel Safety

Information Security & Privacy

- Security policies
- Change controls
- Encryption
- Logical access Control
- Monitoring, communication and connectivity
- Incident management
- Application management
- System development
- Customer contact

Reputational

- Litigation or ethical flags
- Media coverage
- OFAC or other factors
- Criminal and/or civil complaints

Operational

- People
- Process
- Financial Reporting
- Subcontractors
- Concentration

Physical Security

- Fire Suppression
- Server Security & Conditions
- Data Centers
- Backup Power Sources
- Asset management
- Key Card & Facility Access

Financial

- Going concern
- Liquidity
- Leverage
- Profitability
- Transaction Processing

Subcontractor

- Third Party Relationship Management
- Sub-Service Third Party Relationships
- Logical access Control
- Monitoring, communication and connectivity

Bus Continuity & Resiliency*

- Recovery
- Data Backup Management
- Offsite storage
- Media and vital records
- Data integrity

Compliance

- Regulatory requirements
- HIPAA
- CFPB
- GLBA
- Customer complaints handling
- PCI

**Business Continuity Management includes Business Contingency ("BC") planning and Disaster Recovery ("DR")*

Note: Regulation W requirements exist when a Financial Institution receives services from an Affiliate, which may have special due diligence assessment aspects to consider.

Risk assessment types

The following are examples of Third Party due diligence assessments performed on potential and existing third parties to understand the existing control environment and capabilities.

Information Security & Privacy

- Security policies
- Change controls
- Encryption
- Logical access control
- Monitoring, communication and connectivity
- Incident management
- Application management
- System development
- Customer contact

Contracting

The service risk profile should assist in driving the following internal actions:

- Inherent Risk should drive the required contract approval levels;
- Contracts should be reviewed periodically, particularly those involving critical activities, to ensure they continue to address pertinent risk controls and legal protections; and
- Where problems are identified, the organization should seek to renegotiate at the earliest opportunity.

Example Due Diligence Assessments

1. Operational Competency
2. Financial
3. Reputational
4. Compliance
5. **Information Security & Privacy**
6. Technology
7. Business Continuity & Resiliency
8. Physical Security
9. Subcontractor
10. Country Risk

Results

Findings

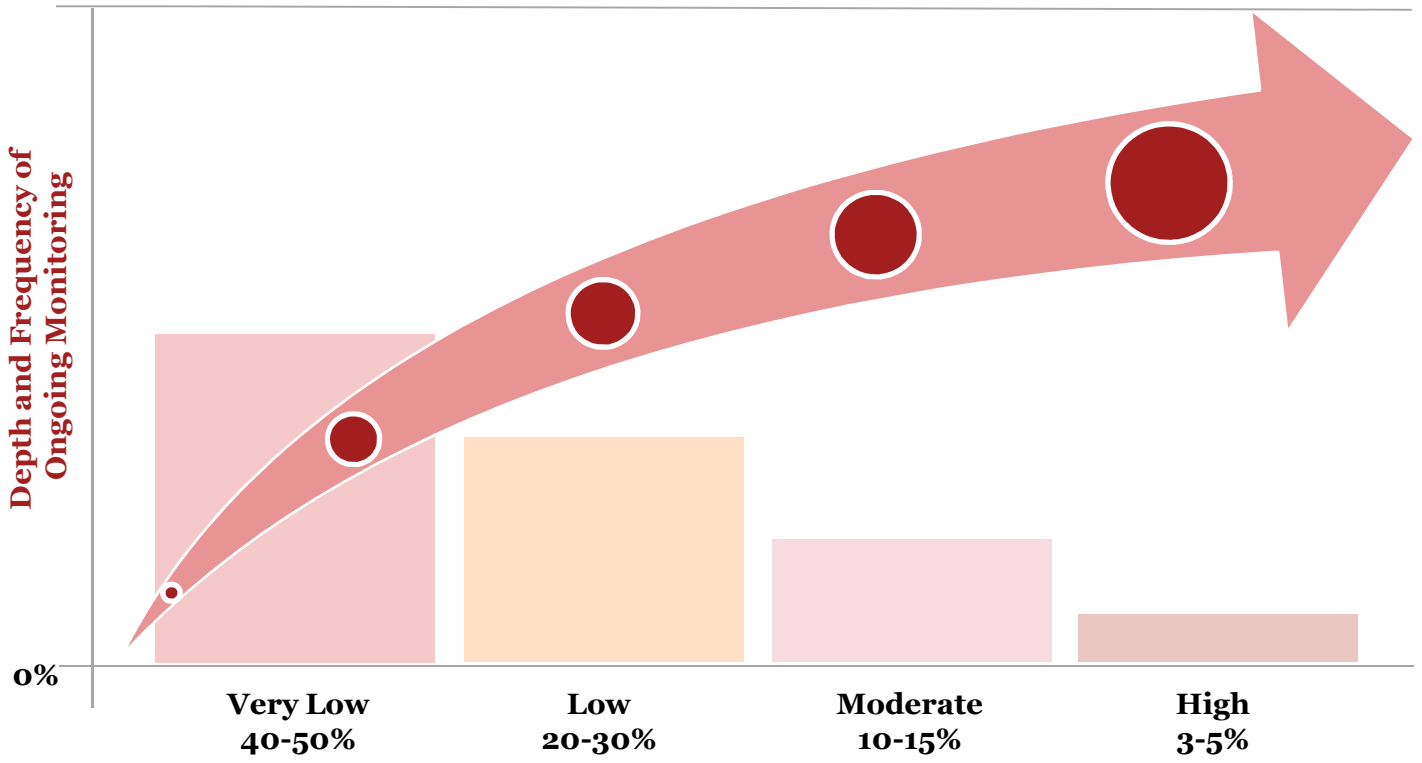
Issues

Example Contract Clauses

1. Nature and scope of service
2. Performance standards
3. Information Handling
4. Right to Audit and Require Remediation
5. Responsibility for Compliance with Laws and Regulations
6. Cost and Compensation
7. Ownership and License
8. Confidentiality and Integrity
9. Business Resumption and Contingency Plans
10. Indemnification
11. Insurance
12. Dispute Resolution
13. Limits in Liability
14. Default and Termination
15. Customer Complaints
16. Subcontracting
17. Foreign-Based Third Parties
18. Controls Verification
19. Notification and Escalation Procedures
20. Records Management
21. Pricing
22. Payment terms
23. Dispute Resolution

Ongoing Monitoring

Results of the inherent risk should drive the nature, timing and extent of activities used to monitor, oversee, and re-assess third party relationships. Due to the higher costs associated with more in-depth assessment activities, a risk based approach should be leveraged ensuring higher risk relationships receive more active risk management than lower risk relationships.



Termination

Each third party termination will be unique; however, there are common decisions, considerations, and results that should be addressed with key stakeholders and executed with a defined plan and checklist.

Termination decision

- Service Failure/Significant Customer Complaints
- Regulatory/Legislative
- End of Contract
- Business Decision
- Product/Service Discontinued

Termination considerations

- Product/Service Brought In-House
- Product/Service Transitioned to Alternate Third Party
- Customer Impact
- Contingency Procedures
- Oral & Implied Contracts
- Internal Employee Impact

Termination result

- Interim Processes
  - NDA
  - Transfer Process Knowledge
  - Migrate or Destroy
- Costs
  - Monetary
  - Non-monetary
- Migrate/Sell Assets
  - Software/Intellectual Property
  - Hardware
  - Facilities
- Notification to Customers and Internal Employees

TPRM Framework & Benefits

TPRM is focused on understanding and managing risks associated with third parties.

Cost

- **Reduced cost** of managing third party risk through stratification, process simplification, and use of technology

Quality

- **Consistent approach** to assessing third parties and risks they present

Standardization

- **Improved quality, efficiency, timeliness and accuracy** of TPRM stemming from automated workflows and reporting tools

Risk

- **More effective monitoring** of due diligence activities and their frequency driven by both inherent and residual risks

Flexibility and efficiency

- **Tighter focus on specific controls** associated with those relationships found to pose the greatest risk

Shareholder value

- Improved compliance with laws and regulations, thereby **reducing or eliminating fines and penalties** that could prohibit services and impact the bottom line

Understanding and Reviewing Attest Reports

How can your organization use attest reporting to mitigate information security and privacy risk resulting from third party activities?

www.pwc.com

pwc

What are SOC reports?

In 2010, the AICPA introduced three new Service Organization Controls (SOC) examination reports, identified as SOC 1 (AT 801), SOC 2 (AT 101), and SOC 3 (AT 101).

- **SOC 1** reports cover controls mitigating financial reporting risks (i.e. completeness, accuracy and validity of transaction processing). Formerly known as "SAS 70" reports, and sometimes referred to as "SSAE 16" reports.

- **SOC 2** reports center more on operational data risks, and contemplate data security, data confidentiality, system availability, processing integrity and/or data privacy (i.e. the Trust Services Principles)

- **SOC 3** reports cover the same content as SOC 2, but disclose less information and are distributable to the general public primarily as marketing material.

SOC 2 / 3 Trust Services Principles

Security
The system is protected against unauthorized access (both physical and logical)

Availability
The system is available for operation and use as committed or agreed

Processing integrity
System processing is complete, accurate, timely, and authorized

Confidentiality
Information designated as confidential is protected as committed or agreed

Privacy
Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice and with criteria set forth in Generally Accepted Privacy Principles (GAPP)

2014 Trust Services Principles Change

Prior to AICPA Guidance Update	After AICPA Guidance Update
Separated into **5 principles:** • Security • Availability • Processing Integrity • Confidentiality • Privacy Each principle had separate criteria that **overlapped**, leading to redundancies There was no set of common criteria	**5 principles** have remained consistent Criteria organized into **common criteria** and **principle – specific criteria:** • The **security principle** is addressed by common criteria only • The **availability**, **processing integrity**, and **confidentiality** principles are fully addressed by combining the common and principle-specific criteria • The **privacy** criteria is under revision and is currently addressed by Generally Accepted Privacy Principles. Principles **no longer overlap**

Now that you have determined which report is most appropriate…

Does the report meet my needs?

- **Service auditor** (see auditor opinion)
  - Are they reputable? Competent?
- **Services covered** (see auditor opinion and management description)
  - Does the scope align to the services provided (e.g. what parts of the business process are covered, what applications are in scope, what control objectives or TSPs are in scope)?
  - Is any of the relevant subject matter performed by a subservice provider and excluded from scope? If so, does a subservicer SOC report exist and can I obtain it?
  - For a SOC 1, are all relevant classes of transaction covered? Are the control objectives relevant?
  - For a SOC 2, are all relevant TSPs covered?
- **Period covered** (see auditor opinion)
  - Does the report assess the operating effectiveness of controls over a period of time (i.e. Type II) that aligns to my assessment period?
  - If a gap, how long and what is available to bridge the gap?

Is that it? (No)

- **Controls and control deficiencies** (see testing section)
  - Which controls are relevant?
  - Any deficiencies?
  - What remediation is in place?
  - WARNING: Even though the opinion may be 'clean', the specific service most applicable to you/the user entity, which is likely buried in the report, can have lots of failures.
- **User control considerations** (see either description or testing sections)
  - Are there any?
  - Are they applicable to you/the user entity?
  - Do you/the user entity have a control in place to cover the consideration?

Common evaluation pitfalls

SOC 1 Considerations

- Important information technology controls might be scoped out
- Certain applications or interface programs used by some customers might not be included in the scope of the report
- The report might be directed at certain clients and you are not one of them (if only certain clients are in scope, this will be described in Section II along with client-specific controls), or the coverage is only for certain locations (may not be yours)

SOC 2 Considerations

- Inappropriate mapping / assumptions (Maturity of TPRM program)
- Appropriately adjust level of effort / reliance on the reports
- Scope of the report is not appropriate (i.e. in-scope systems, infrastructure, physical locations)
- Time frame coverage (within the period? 6, 9, or 12 month coverage)
- Complementary User Entity Controls
- SOC2 and Type II are not the same
- Inclusive method vs. carve-out
- Understand and evaluate exceptions

SOC2+ Why customers need greater transparency

- Vendor sourcing arrangements are increasingly complex and exposing companies to emerging risks
- Company management and in certain situations - regulators – are shifting their focus to look at the effectiveness of third party governance programs in place to address these emerging risks
- More vendors are being contractually obligated to provide independent assurance over their processes and controls to address their customer's risks
- Internal control areas where greater transparency may be required include:
  - Financial reporting
  - Information security and privacy
  - Business continuity and disaster recovery
  - Regulatory areas (i.e., FATCA, Electronic Health Records)

"Increasingly, we are moving away from looking at cost alone. People are going to put more emphasis on how well the risk is managed, and how well the outsourcing company cater to our needs or to the needs of the industry."
-Leading info-communications technology (ICT) service provider

SOC2+ Why customers need greater transparency

Traditional vendor assessment practices:	Challenges in meeting customer needs:
Vendor Questionnaires SIG/SIG Lite On-site assessments by customers Agreed Upon Procedure engagements SOC 1 reports SOC 2 reports SOC 3 reports	• Vendor Questionnaires and SIG/SIG Lite are often "self-assessments" completed by vendors with no validation • Questionnaires and on-site assessments can often be conducted by various personnel without defined standards for performance, resulting in inconsistencies and limited comfort • Conducting assessments can be time consuming and costly to both the vendor and the assessor • Agreed Upon Procedures require all parties to agree to procedures being performed and does not provide assurance • SOC1 reports are exclusively focused on risks related to internal controls over financial reporting and may not align to third party oversight risks • SOC2 and SOC3 reports provide assurance, but in many cases do not provide coverage over all areas of interest in managing third party risk

With significant costs associated with the questionnaire process and on-site audits, a more cost effective, reliable and efficient form of vendor assurance is needed.

A new approach to providing assurance on third party operations

PwC has developed a framework to help vendors respond to multiple requests from customers as well as save them, and their customers, time and money.

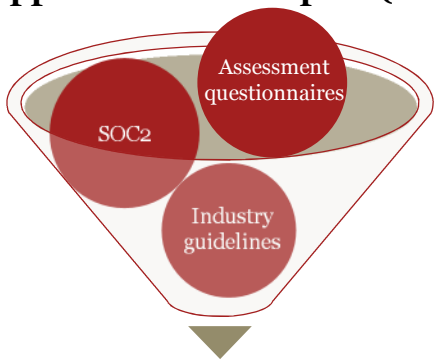
The SOC 2+ report covers most of the material normally covered in client questionnaires, with only minimal, typically non-critical material not covered by the SOC2+.

What is SOC 2+?

- A new Vendor Controls Attestation Report, developed and led by PwC, in collaboration with SIFMA
- Built upon AICPA SOC 2 reporting principles, allows an independent, standardized assessment to be performed over vendor operations and eliminates the need for costly vendor questionnaires
- The report format is similar to SOC 1 and SOC 2 reports, making it easy for both vendors and customers to digest
- In addition to the principles covered in SOC 2 reports (security, availability and confidentiality), the SOC 2+ report includes additional customized principles that meet the unique assurance needs of a vendor's customers

Traditional vendor assessment practices
Vendor Questionnaires
SIG/SIG Lite
On-site assessments by customers
Agreed Upon Procedure engagements
SOC 1 reports
SOC 2 /SOC 3 reports
ISO Certifications

New Approach – VCA report (SOC 2+)



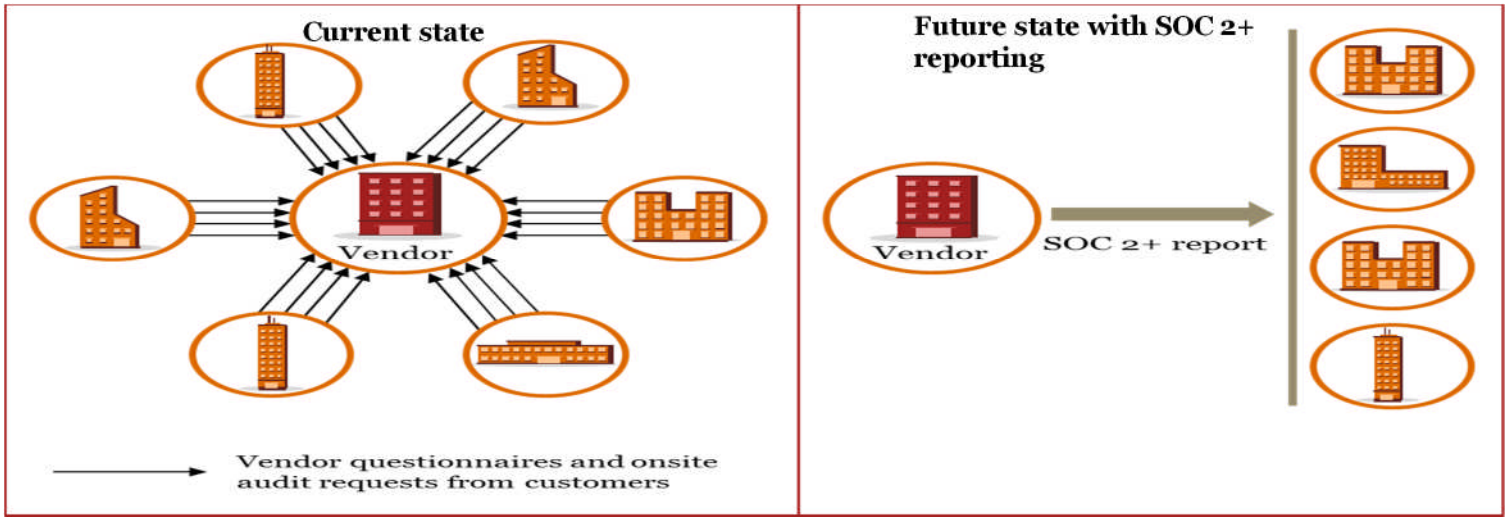
Benefits of SOC2+ reporting in TPRM/VRM

Vendor Benefits

- ✓ A SOC 2+ report can be customized to ensure most (if not all) of the information needs of customers are met
- ✓ Curb excessive spend on overseeing and responding to customer requests (e.g., questionnaires, on-site audits) and in providing comfort over vendor control processes
- ✓ A SOC 2+ report can be utilized as a differentiator from peers.

Customer Benefits

- ✓ Internal controls opinion from an independent third-party, covering most of the information requirements of the customer
- ✓ Eliminates the need for on-site audits and the questionnaire process, saving your customers time and money
- ✓ Prospective customers can obtain SOC2+ report (reduces time spent during the due diligence phase)
- ✓ Improved level of information being reported on the state of the control environment.



Contacts

Garit Gemeinhardt
PwC Director
Garit.gemeinhardt@pwc.com
(704) 344-7757

Brett Croker
PwC Director
brett.j.croker@pwc.com
(678) 409-3216

Thank You!

Contact: craigc@clearstar.net