www.pwc.com

Third Party Risk Management

ISACA Central
Maryland chapter
December 9, 2015

pwc

Here with you today

Ellen Ozderman
Director
Cybersecurity, Privacy
& IT Risk
M: 240.750.5669
E: ellen.ozderman@pwc.com

Stephanie Hardt
Manager
Cybersecurity, Privacy
& IT Risk
M: 202.365.0033
E: stephanie.l.hardt@pwc.com

Danny Wuckovich
Senior Associate
Cybersecurity, Privacy
& IT Risk
M: 571.213.8308
E: danny.w.wuckovich@ pwc.com

Agenda

Third Party Risk Management

- Questions to Consider
- Why is Third Party Risk Management important?
- What is Third Party Risk Management/Security and Privacy Considerations

Cloud Reliance

Common Challenges and Lessons Learned

Appendix

Learning objectives

A deep dive into Third Party Risk Management Programs and the information security and privacy over third parties

- Describe the Third Party Risk Management lifecycle and why it is important
- Highlight the importance of TPRM as demonstrated by current events and news headlines
- 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
- Identify how Third Party Risk Management programs work to mitigate security and privacy risks originating at our third party vendors
- Explain the process for identifying and monitoring third party vendors' security postures
- Share common information security and privacy challenges surrounding TPRM
- Explain the benefits of Third Party Risk Management
- Highlight the key TPRM, information security, and privacy considerations for cloud service providers

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?

Questions to consider *(continued)*

Due Diligence and Third Party Selection

- 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

Recent breaches involving third-party vendors

Cybersecurity

Home Depot Hackers Got in Via a Vendor, Took E-Mails, Too

By Dune Lawrence | November 06, 2014

SEND TO kindle

"Home Depot disclosed that hackers stole 53 million e-mail addresses, on top of the data for 56 million credit cards."

http://www.bloomberg.com/bw/articles/2014-11-06/home-depot-hackers-got-in-via-a-vendor-took-53-million-e-mails-too

"Home Depot said the crooks initially broke in using credentials stolen from a third-party vendor. The company said thieves used the vendor's user name and password to enter the perimeter of Home Depot's network, but that these stolen credentials alone did not provide direct access to the company's point-of-sale devices. For that, they had to turn to a vulnerability in Microsoft Windows that was patched only after the breach occurred…"

http://krebsonsecurity.com/tag/home-depot-breach/

Recent breaches involving third-party vendors (continued)

KrebsonSecurity
In-depth security news and investigation

05 Target Hackers Broke in Via HVAC Company

FEB 14

Last week, **Target** told reporters at *The Wall Street Journal* and *Reuters* that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor. Sources now tell KrebsOnSecurity that the vendor in question was a

"...the source of the Target intrusion traces back to network credentials that Target had issued to **Fazio Mechanical**, a heating, air conditioning and refrigeration firm in Sharpsburg, Pa. Multiple sources close to the investigation now tell this reporter that those credentials were stolen in an email malware attack at Fazio that began at least two months before thieves started stealing card data from thousands of Target cash registers."

- 40 million customer credit cards stolen
- 70 million customer records (name, address, email, phone)
- 46% decrease in Q4 2013 profits vs Q4 2012

http://krebsonsecurity.com/tag/target-data-breach/

Recent breaches involving third-party vendors *(continued)*

2 OCT 15

Experian Breach Affects 15 Million Consumers

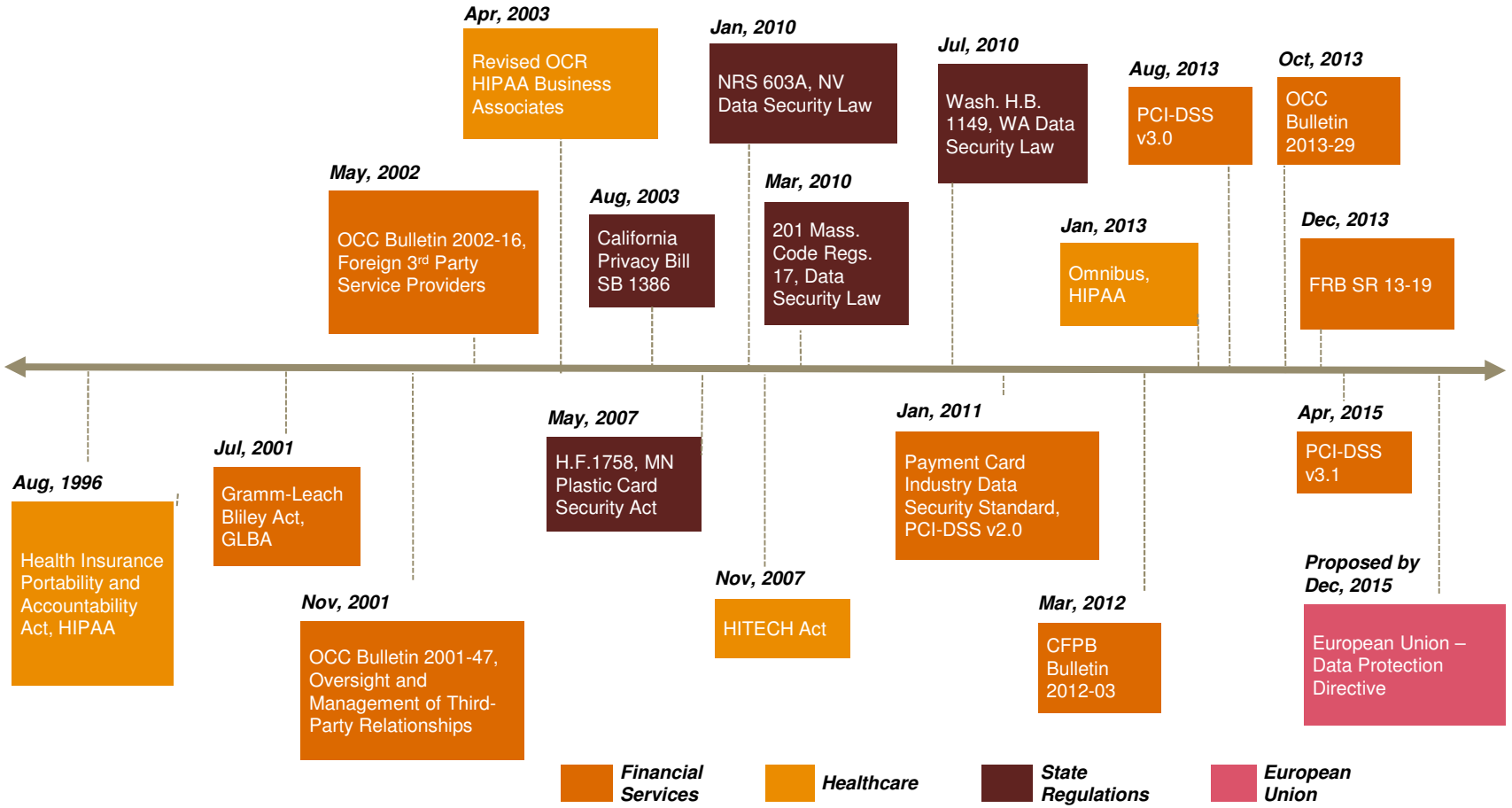
Kicking off National Cybersecurity Awareness Month with a bang, credit bureau and consumer data broker **Experian North America** disclosed Thursday that a breach of its computer systems exposed approximately 15 million Social Security numbers and other data on people who applied for financing from wireless provider **T-Mobile USA Inc**.

"Experian *said* the compromise of an internal server exposed names, dates of birth, addresses, Social Security numbers and/or drivers' license numbers, as well as additional information used in T-Mobile's own credit assessment."

"…the breach lasted for two years from Sept. 1, 2013 to Sept. 16, 2015…Experian detected the breach on Sept. 15, 2015, and confirmed the theft of a single file containing the T-Mobile data on Sept. 22, 2015."

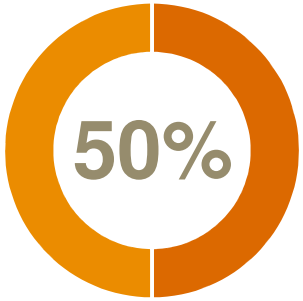
- Over 15 million customer records (name, dob, address, ssn, driver's license number)

Regulatory considerations

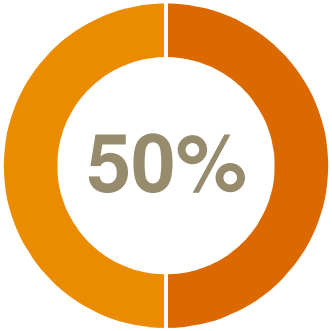


PwC's global state of information security survey results

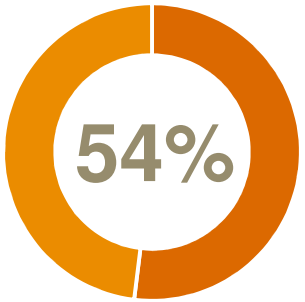
Inventory of third parties that handle personal data of customers and employees



Perform risk assessments



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



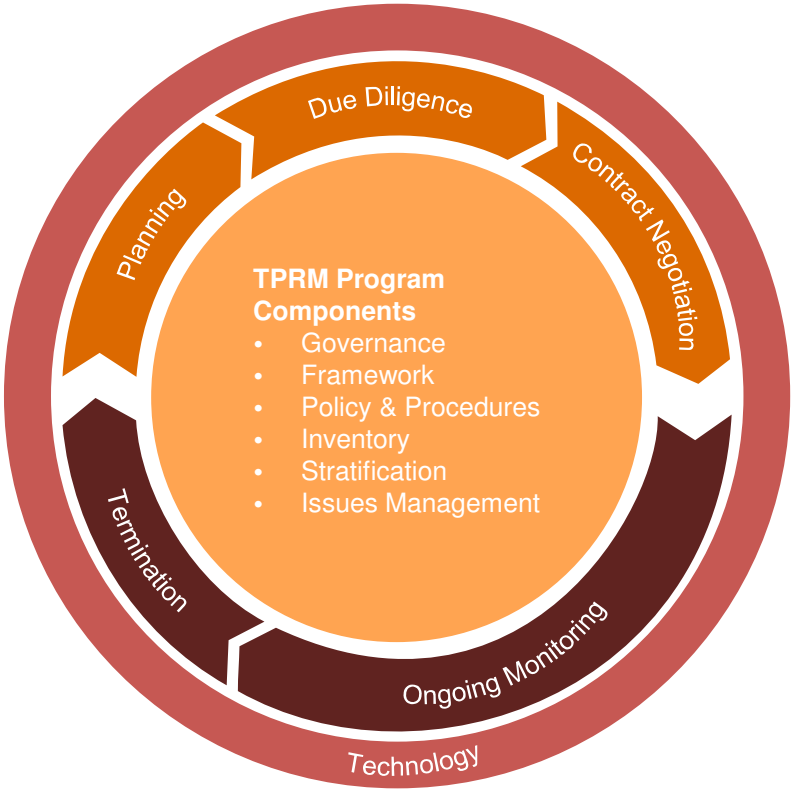
Third party risk management framework

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

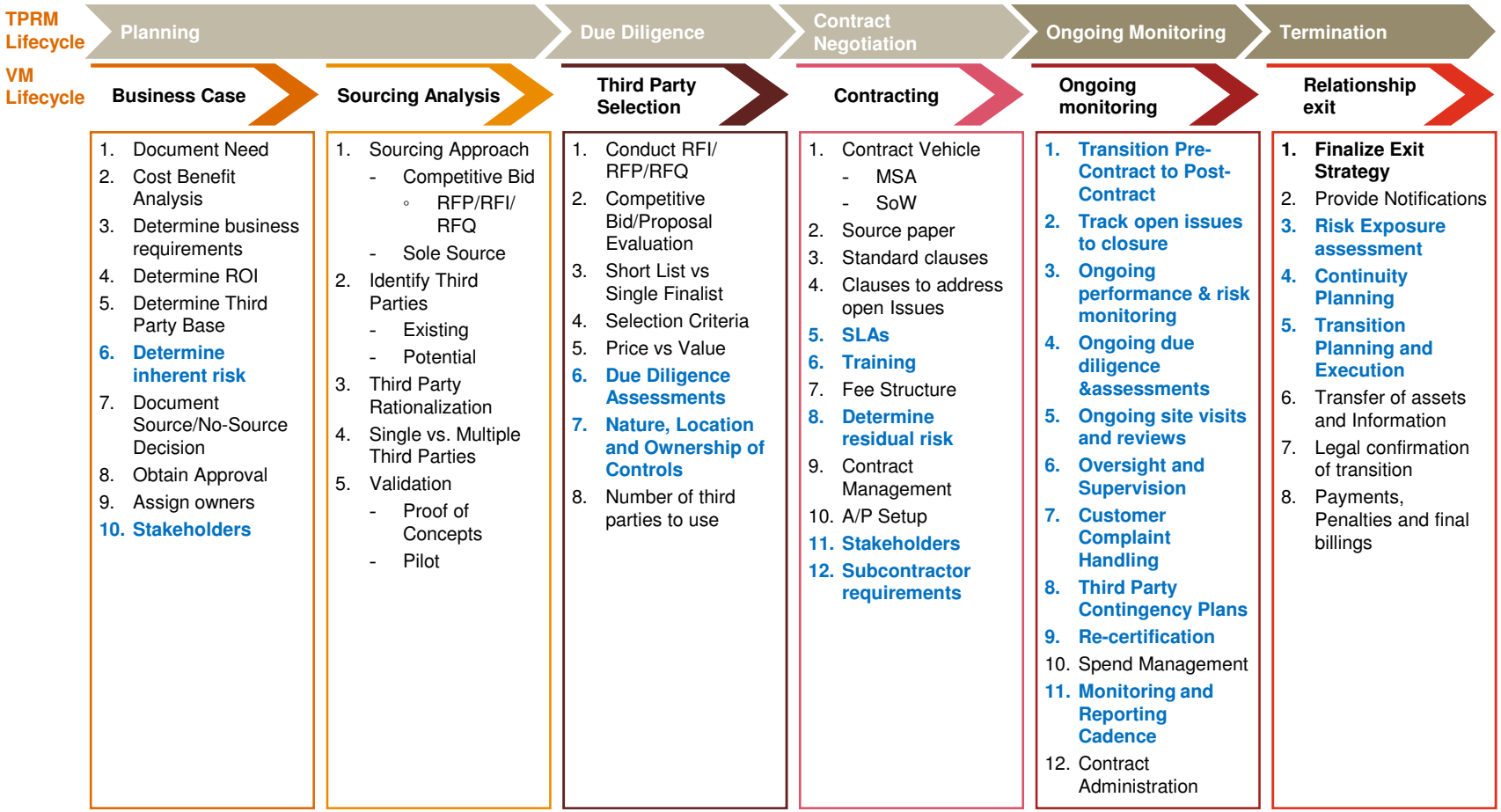
- Reputational
- Concentration
- Operational
- Regulatory/ Compliance
- Financial
- Termination
- Business Continuity
- Subcontractor
- Country
- Technology
- Information Security
- Privacy

TPRM – Security and privacy considerations

Third Party security lifecycle:

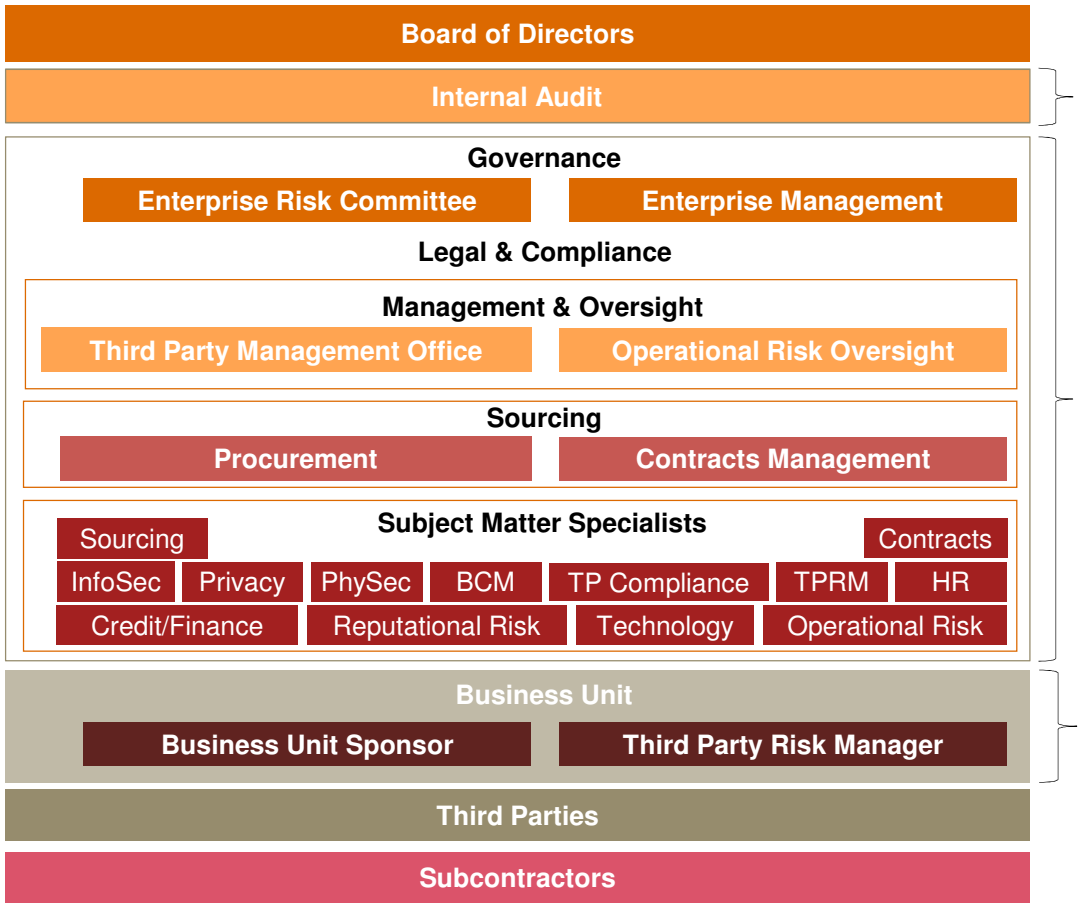
- **On-boarding, approval, and renewal –** Collaborating with Procurement, OGC, and Relationship Managers to obtain required documentation (e.g., Security & Confidentiality Agreement, Inherent Risk Questionnaires, etc.) and perform a precursory review of third parties' security postures during on-boarding and renewal of contractual services with third parties.
- **Risk assessments** – Performing TSP due diligence on third-parties to assess whether Company data and systems are safeguarded appropriately.
- **Monitoring and compliance** – TSP operational activities, including monitoring third party risk profile, remediation tracking, communication and awareness, and monitoring and reporting status.

Vendor Management (VM) vs. Third party risk management



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

Third party risk management – Program governance



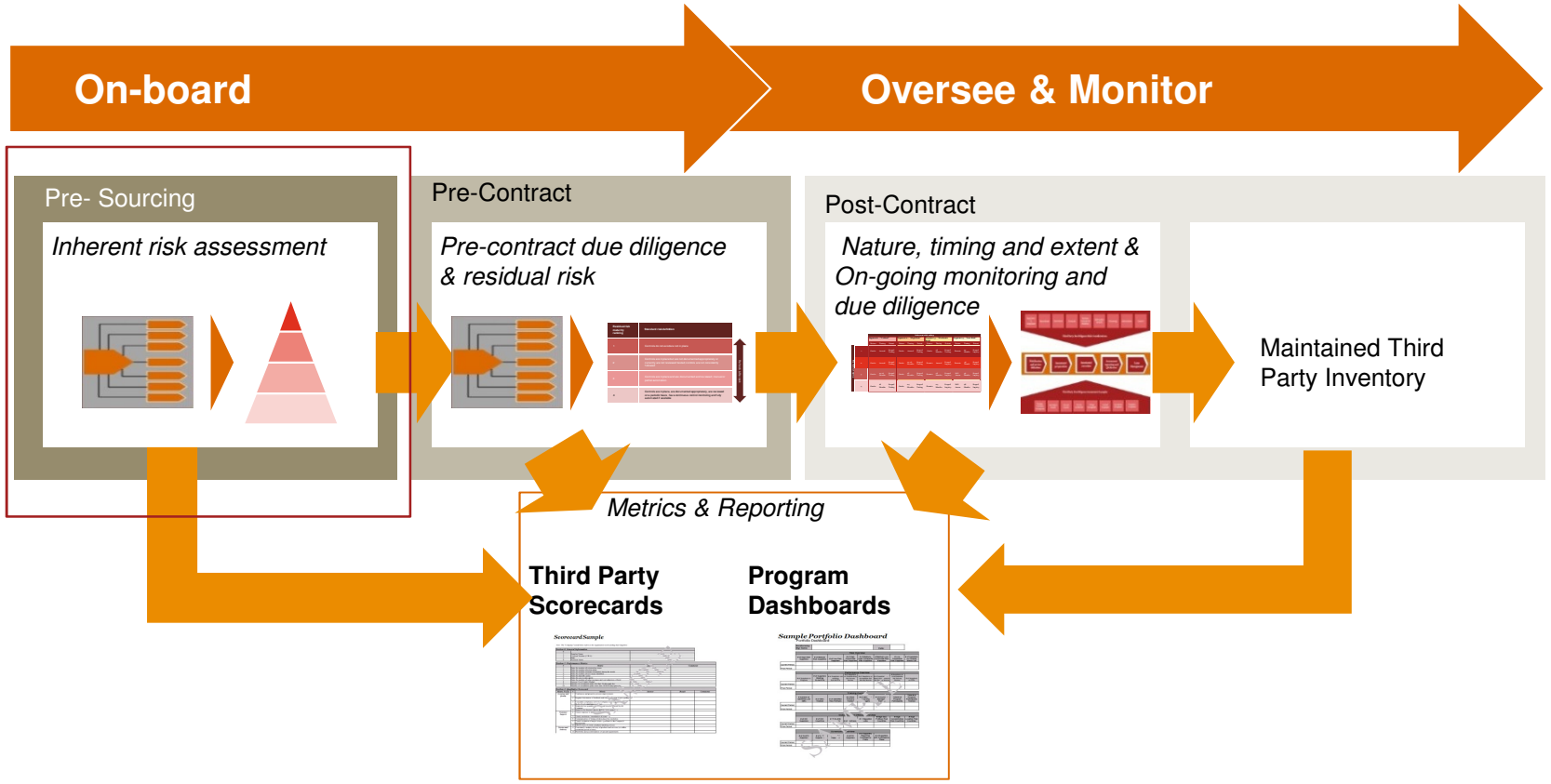
Third Line of Defense
- Independently test, verify and evaluate risk management controls against internal policies
- Report upon effectiveness of the program

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 and risk stratification

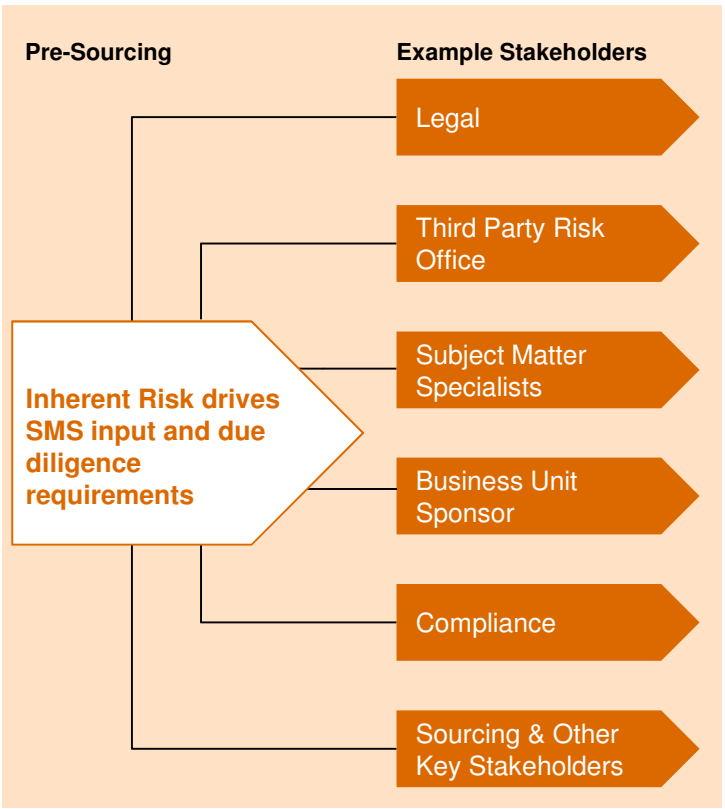
The Planning stage facilitates maintenance of the third party inventory, and enables management to focus resources and efforts on those services that present greater risk to the organization.



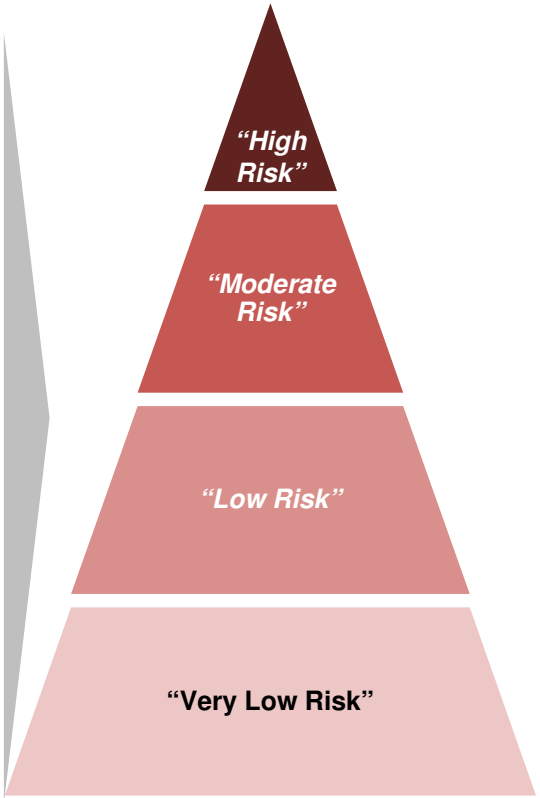
Inherent risk assessment – Service level stratification

The inherent risk assessment process allows for the sorting of third party services/products inherent risk scores and inherent risk ratings.

Inherent risk assessment



Risk stratification structure



1 – "High Risk" These third parties are handling high risk services, have a critical level of disruption, access to highly restricted types of data and are client facing.

2 – "Moderate Risk"
These third parties are handling high or medium risk services, have high level of disruption, access to restricted data and may be client facing.

3 – "Low Risk"
These third parties are handling medium risk services, have a moderate level of disruption, have access to restricted data and are not client facing.

4 –"Very Low Risk"
These third parties are handling low risk services, have a low level of disruption, do not have access to restricted data and are not client facing.

Planning – TPRM security and privacy

What Third Party risk factors qualify for security and privacy assessments by the TPRM program?

1 **2**

Third-parties that:

a. Store, process, or transmit organizational data on their own IT systems and network, or
b. Access the organization's internal IT infrastructure and systems (including network, applications, databases, etc.)

Sensitive data that is:

Shared with/collected by/accessible to the third party. Sensitive data may include:

a. Customer, customer spouse, and prospective customer information
b. Employee, Employee Family, Applicant, and Contractor Information
c. Organization's Intellectual Property, Proprietary Information, and Financial Data
d. Technology Information

*Note: should be aligned with organizational data classifications

Planning – TPRM security and privacy (continued)

Risk identification and prioritization of third parties:

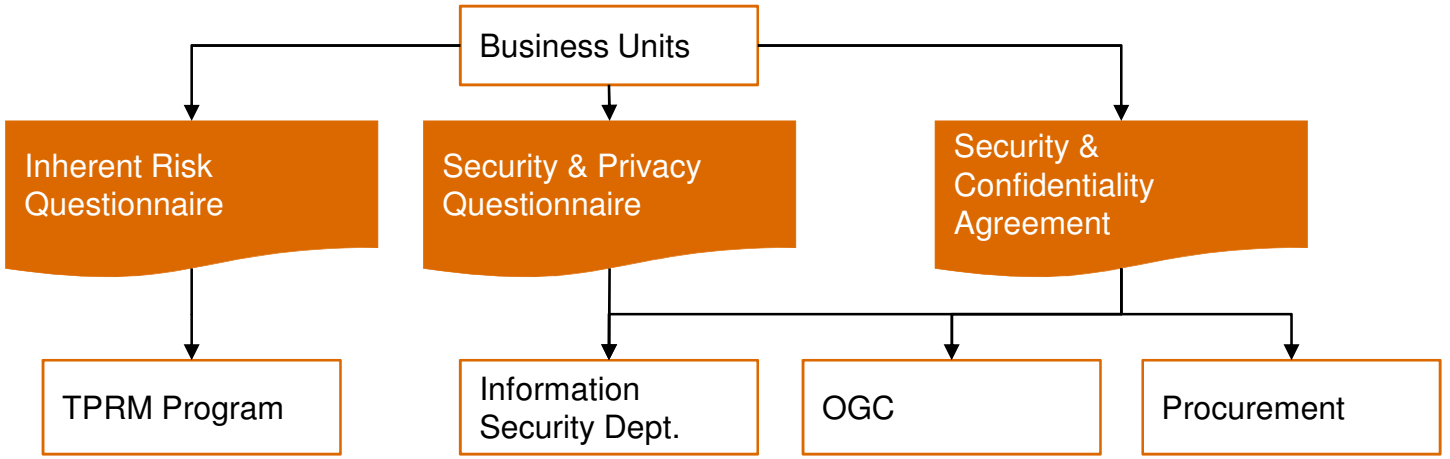
- An inherent risk questionnaire evaluates the third-party's inherent security and privacy risks against a primary set of qualitative and quantitative risk factors.
  1. **IT systems and data sensitivity** – Critical systems and sensitive data elements (based on the organization's data classifications) that are shared with, collected by, or accessible to the third-party organization.
  2. **Estimated record volume** – The maximum volume of sensitive data and information accessible to the third-party organization.
- Based on the inherent risk questionnaire, the third-party is risk rated against defined risk tiers.
- The risk tiers define the due diligence requirements to be completed for each third-party.

Risk Tier	Due diligence requirements	
	Nature	Timing
Tier 4 - High Risk	Onsite assessment	Annually
Tier 3 - Moderate Risk	Remote Assessment	Bi-Annually
Tier 2 - Low Risk	Self assessment	Tri-Annually
Tier 1 - Very Low Risk	Annual Recertification of TSP Profile	N/A

Planning – TPRM security and privacy (continued)

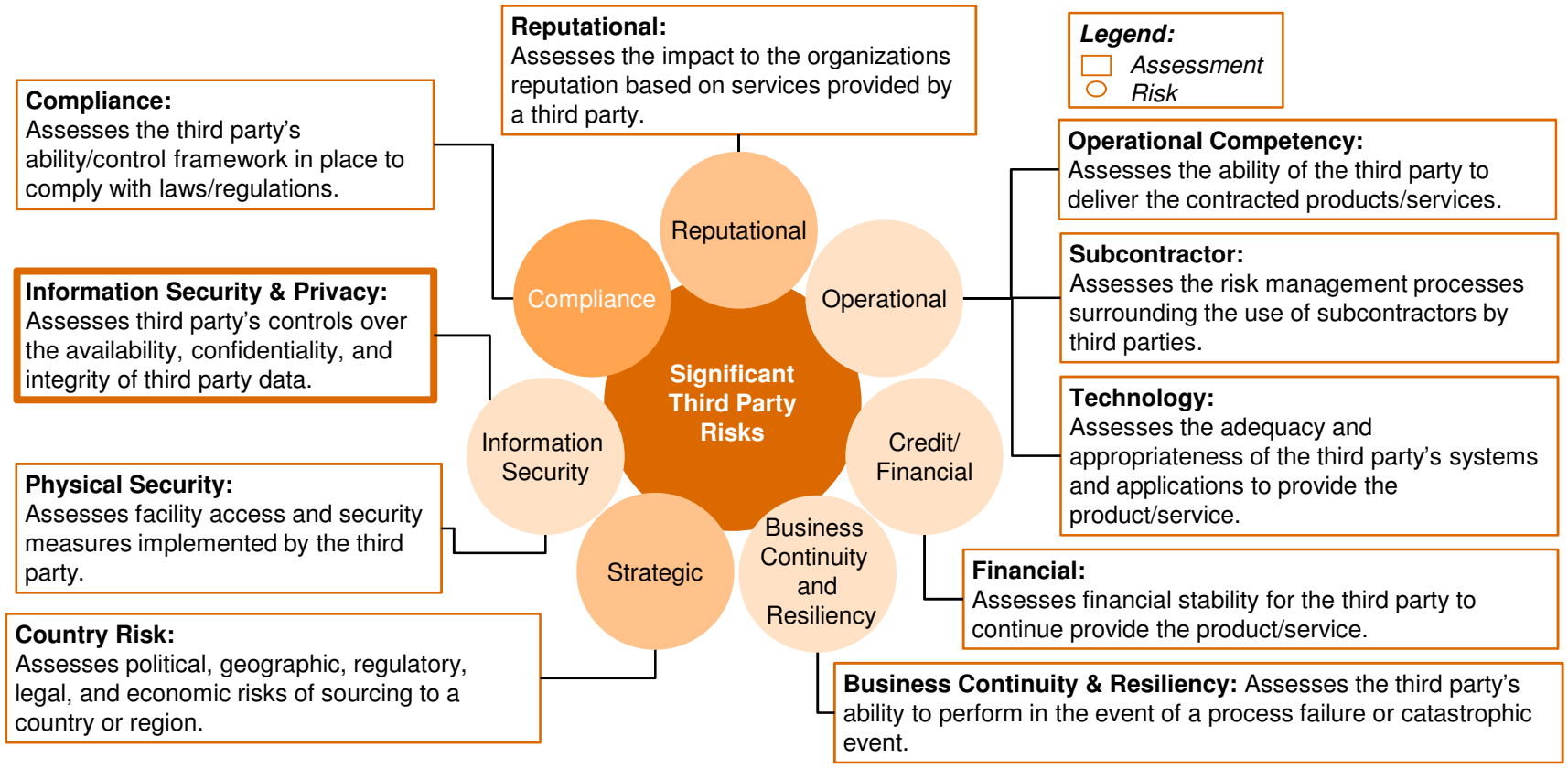
Review and approval of Third Party:

- A mature TPRM program requires approval from the Department of Information Security for all new contracts
- The Department of Information Security performs a precursory review of the Third Party's control assertions using a risks and controls questionnaire
- Approval typically requires completion of the following security and privacy documents:



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

Information Security & Privacy

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

Physical Security

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

Subcontractor

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

Country

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

Reputational

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

Financial

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

Bus Continuity & Resiliency*

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

Operational

- People
- Process
- Financial Reporting
- Subcontractors
- Concentration

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.

TPRM security and privacy

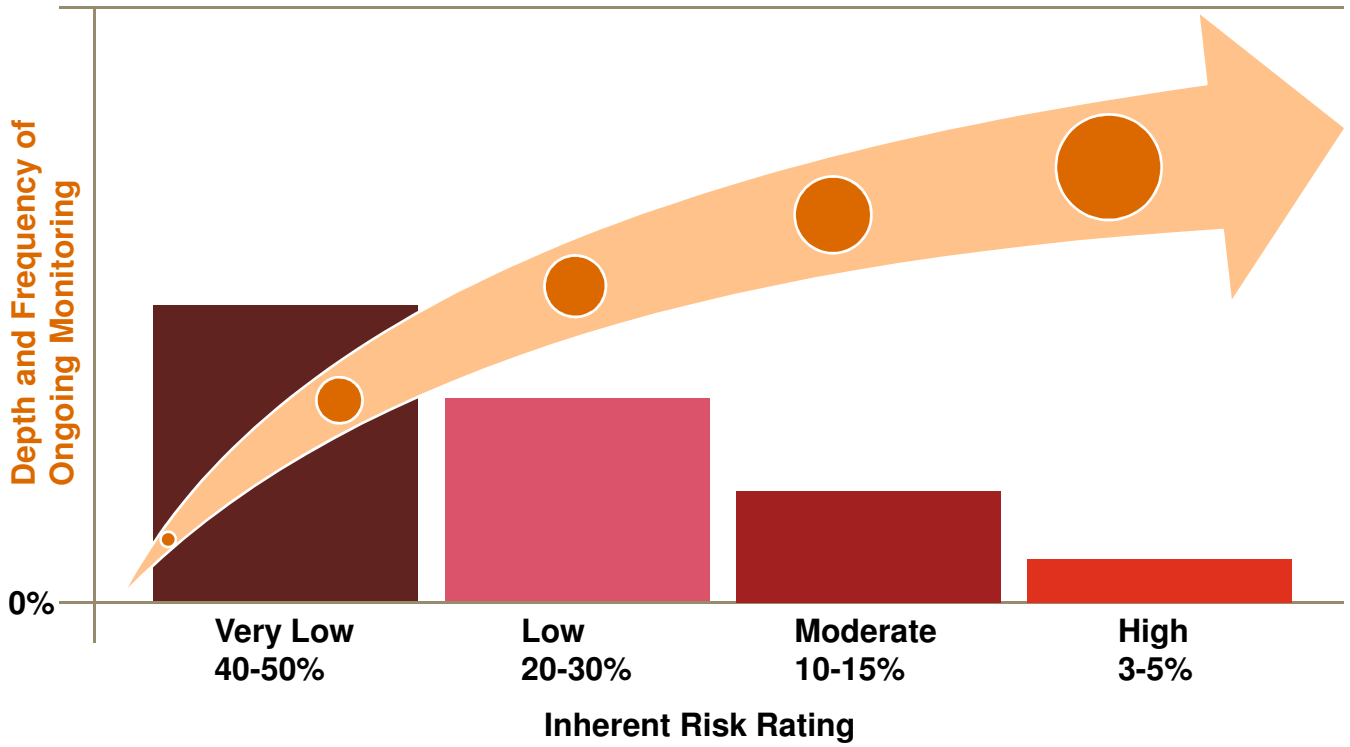
Security and privacy domains:

- The TSP identifies and monitors third-party risks through risks assessments, which provide assurance on whether third-parties are meeting the organization's security and privacy standards.
- The risk assessments assess security and privacy controls across the following domains:

Security Administration	Logical Security	Security Operations	Physical Security	Compliance Monitoring
Policies and procedures, security roles and responsibilities, HR personnel and subcontractor management and oversight (e.g., background checks, security awareness training, etc.)	Security administration, privileged access, authentication, workstation/application/database/platform security, network perimeter protection, remote/wireless access, network segmentation	Threat and vulnerability management, security monitoring, incident response, backup and recovery, encryption	Data center access controls, monitoring, environmental controls	Regulatory compliance management, policy and standards compliance

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

Ongoing monitoring – TPRM metrics

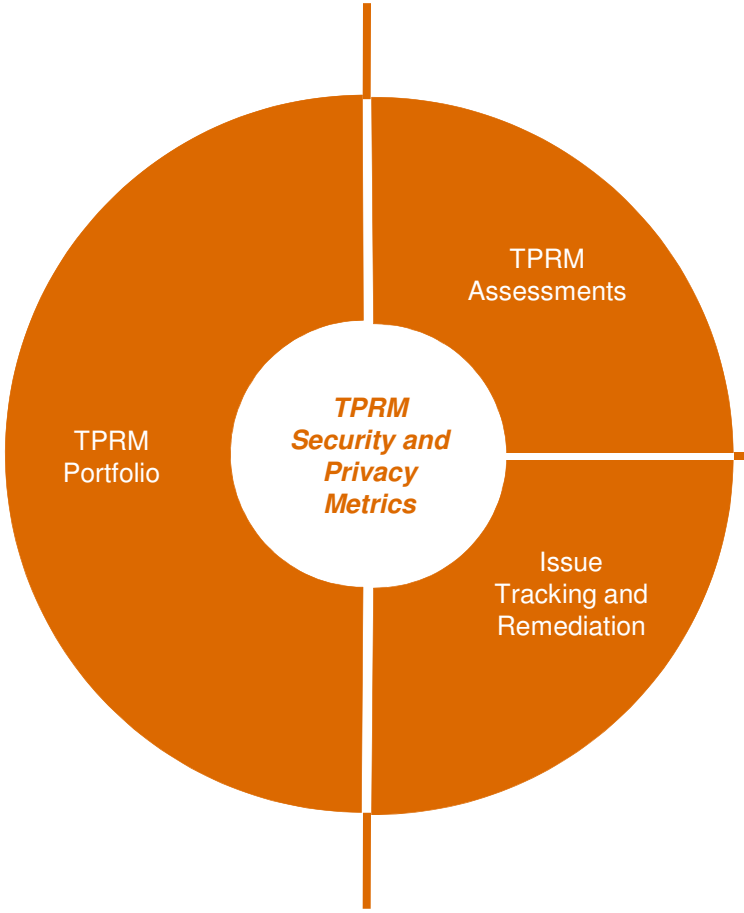
TPRM metrics:

What is the inherent risk distribution across the third-party population?

- Percentage count of third-parties at each security risk tier
- Change in inherent risk distribution over time

How often are third-parties on-boarded and renewed?

- Number of TPRM requests
- Count of third-parties that are approved, in-process, and expired for purposes of TPRM



How much assurance is provided by the TPRM Assessments?

- Number of TPRM assessments planned, in-progress, and completed
- Number of third-parties assessed in comparison to broader portfolio
- Average number of findings (high, medium, low) uncovered as part of the assessments

Issue Tracking and Remediation

- Total number of observations/risks
- Total number of risks outstanding and mitigated
- Estimated time to remediate

TPRM framework & benefits

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

TPRM challenges and trends

- Third party management efforts focus on high-spend Third Parties instead of taking risk based approach
- Organizations are unable to identify a complete inventory of Third Party relationships (contracts in desk drawers, etc.)
- Third-party management and security standards are not formalized and requirements are applied ad-hoc
- Beyond an organization's IT and Infosec Departments, there tends to be a:
  - Lack of training and awareness for Third Party security and privacy risks
  - Lack of understanding in what constitutes sensitive data and information
- Organizations often fail to identify 4th party subcontractors engaged by the Third Party who will have access to the organization's data and/or systems, and the third-party does not readily disclose them
- Ineffective coordination between stakeholders (Business Units, Procurement, OGC, Infosec Department, and IT) often results in weak contractual requirements (security, right to audit, etc.)

TPRM challenges and trends *(continued)*

- Lack of validation on the accuracy of the data and systems accessible to the third party; resulting in improper inherent risk classification
- Improper tone at the top leads to a lack of professional skepticism over third party security assertions
- Unauthorized use of organizational data not expressly prohibited by the contract
- Organizational belief that certain types of vendors are exempt (common to IT hosting and cloud service providers)
- Organizations often lack enough headcount to support comprehensive Third Party management activities

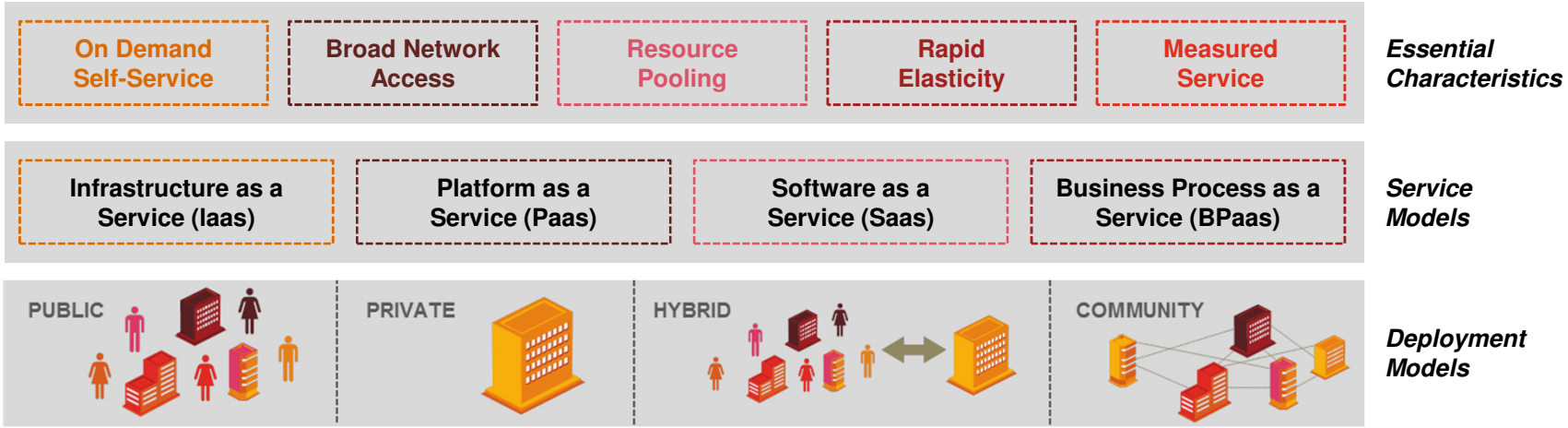
Reliance on cloud services

Reliance on cloud services

What is cloud computing?

- A game-changing technology model and paradigm
- Ubiquitous, convenient, on-demand, pay-as-you-go network access to a shared pool of configurable computing resources

- Major technology and business disrupter (cost reduction and innovation)
- ***Security impact:*** Driving new risks and security concerns that impacts all elements of the business ecosystem



** Source: "The National Institute of Standards and Technology (NIST) Definition of Cloud Computing (NIST Special Publication 800-145), Sept. 2011*

Reliance on cloud services (continued)

Cloud Rewards

- The role of IT is changing from building and deploying applications and infrastructure to providing a service catalog of Cloud services an organization can consume.
- Cloud leads to disruption of IT and innovation the LoBs demand.
- Cloud provides applications and infrastructure at a speed and scale that most Enterprise IT organizations can't replicate.
- Cloud allows you to trim the fat and right size your applications and infrastructure to what you really need.

Cloud Risks

- Cloud is a shared responsibility environment and requires a revised approach to manage risk and security.
- Cloud services often involve multiple third party providers, however, responsibility for security controls is often unclear.
- Lack of Cloud governance may lead to LoB Cloud consumption with little governance, oversight and unapproved usage.
- Cloud usage must have ownership and policies communicated from the top down.

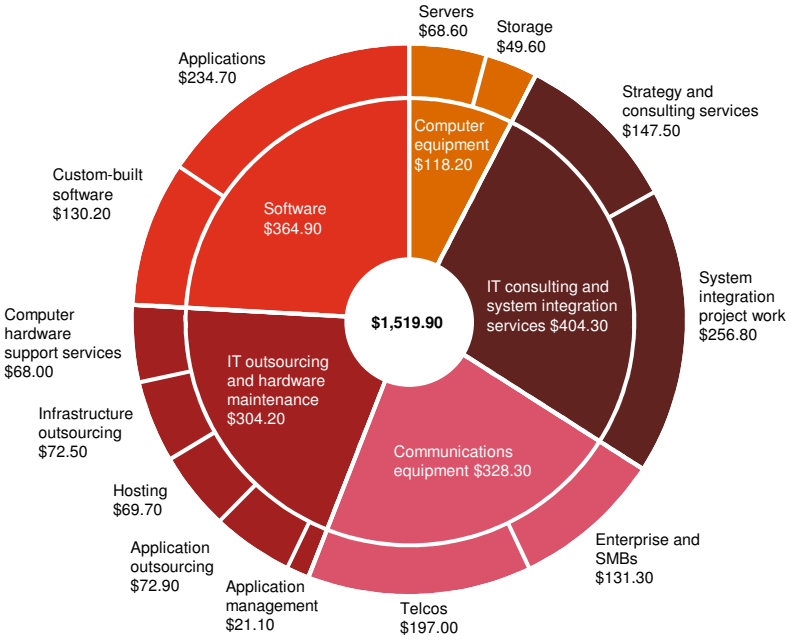
Reliance on cloud services *(continued)*

Analysts disagree on size of Cloud spending; but all agree it's large, here to stay, and growing

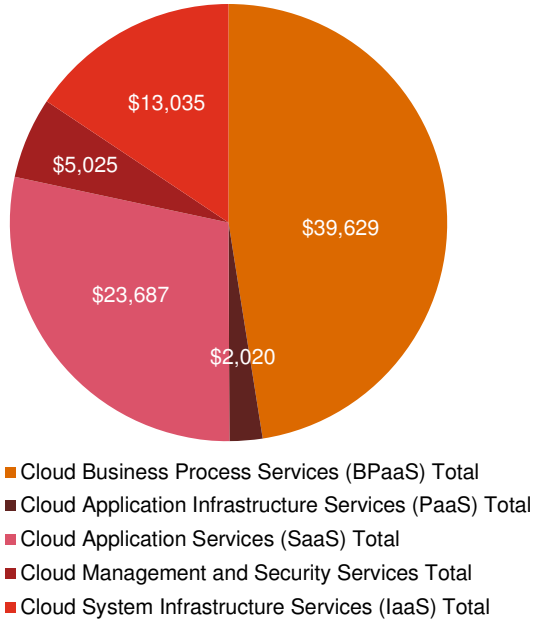
$1.5 Trillion *– Global IT spend Influenced by Cloud. Source: "Global Tech Market Outlook 2013 – 2014" Forrester*

$81 Billion *Global Cloud Spend in 2014 (not including marketing – which was single biggest cloud spend category!) Source: Gartner Cloud Forecast 2013*

Forrester's Global Tech Outlook – 2013 - 14

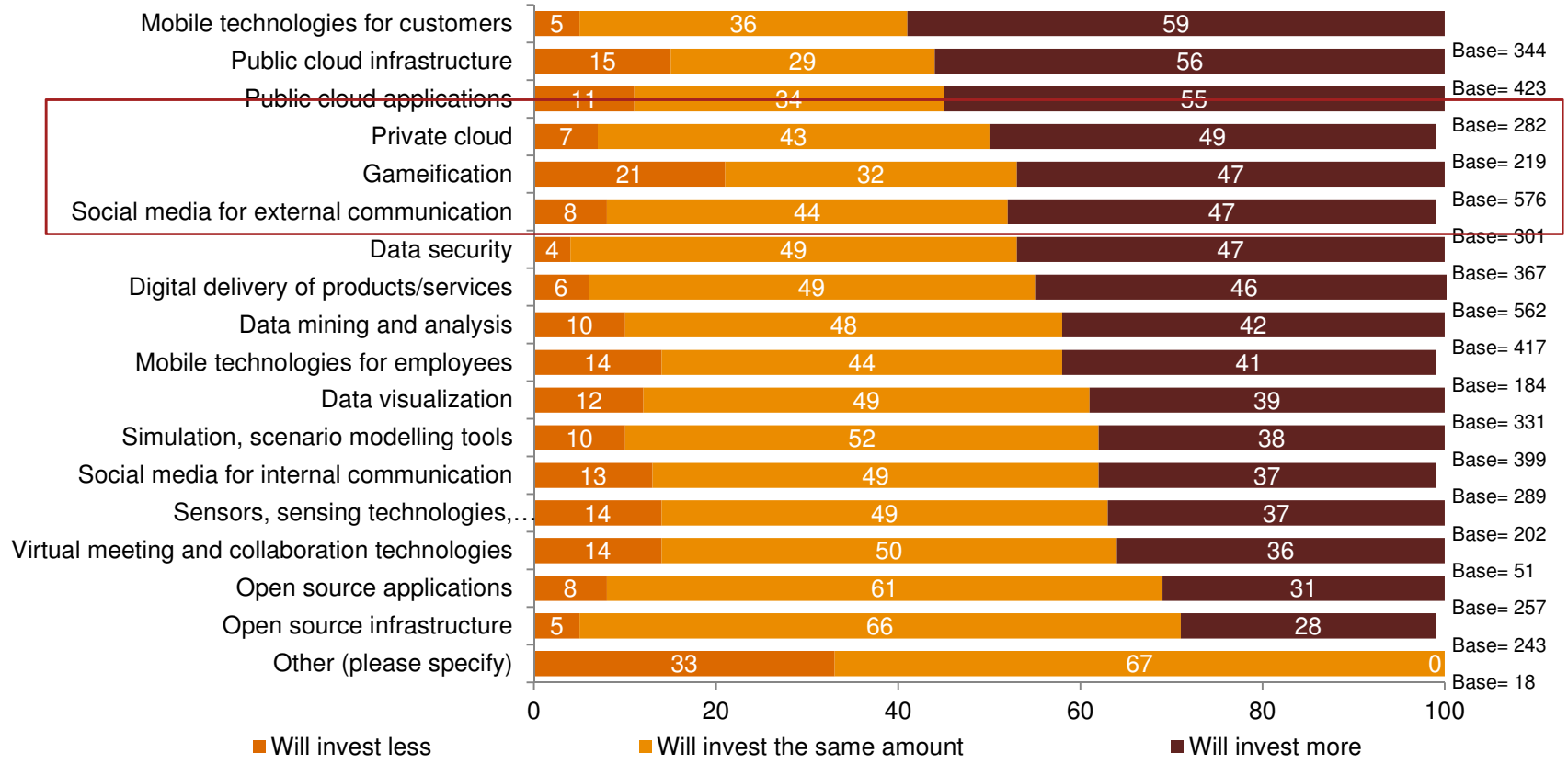


Gartner's Cloud Forecast - Yr 2014



Reliance on cloud services *(continued)*

PwC's Digital IQ survey finds 3 of 5 top planned tech spend categories include "Cloud"



**Source: PwC 4th Annual Digital IQ Survey report*

Reliance on cloud services *(continued)*

"A-B-C's of cloud security" succinctly identifies key risks that should be addressed across your cloud use cases

Secure cloud domain	Key risks, issues, and requirements
***A*ccess Control**	• Control access to sensitive data • Audit and report user access and data use • Provision and de-provision user access • Elevated access
***B*usiness continuity**	• Provider availability; contingency of the consumer's services • Provide business continuity and disaster recovery
***C*ompliance**	• Regulatory compliance overall and in face of shadow IT use of cloud • Maintain regulatory compliance across cloud ecosystems and migration models • Right to audit • Contract and SLA compliance
***D*ata protection and segregation**	• Data classification scheme and processes for handling sensitive data • Prevent unauthorized data exposure, loss or corruption • Maintain data segregation in multi-tenet environment • Data flows across jurisdictions and zones with various regulatory and data protection requirements • Securely dispose of data no longer required
***E*vents – threats, response and investigations**	• Ability to log, monitor, and communicate events; integration with consumer to turn data into actionable intelligence • Event signature creation across new infrastructure/services to drive security intelligence • Detect and correct security events • Cooperate during investigations and incident responses

Reliance on cloud services *(continued)*

What are the implications of cloud migration on security & risk strategy?

1. ***Migration readiness framework:*** You need an integrated security and risk assessment framework to determine the "readiness" of applications to move to cloud; readiness should be determined based on risk and architecture/operational fit for various cloud platforms
2. ***You're responsible for securing the gaps***: Outsourced/cloud providers do not solve all your risk and security problems (though they take on some of them); many technology, operations, contracting, and process controls are needed to operate securely. You must design, implement, operate, and manage these controls. These should not come as an afterthought to your cloud adoption.
3. ***Third-party Risk Management***: Perform a TPRM risk analysis to understand the security capabilities of the third party, control integration points, and gaps as you work to migrate to a cloud service.

Reliance on cloud services *(continued)*

Common challenges and lessons learned:

- Risk of un-authorized data exposure to the cloud from internal users is a critical threat to your organization.
- Your organization is already using cloud environments and applications whether you know it or not; you can't protect data if you don't know where it is and how it moves.
- Most likely your existing data discovery and protection capabilities don't natively scale to cloud; cloud-specific services and products exist to help identify and remediate sensitive data in your cloud environments.
- Existing data discovery and protection policies may be applicable, but may need to be revised/tuned.
- What you do with data once it's discovered is as important as discovery in the first place. Organizations need to refresh their data protection and response procedures and governance to address.

Questions

Appendix A – Bios

Placeholder for text

Ellen Ozderman, Director – PwC Cybersecurity, Privacy and IT Risk

Phone: (240) 750 -5669
Email: ellen.Ozderman@pwc.com

Mrs. Ellen Ozderman has over 12 years of cross-functional IT experience including information security program management, vendor risk management, data privacy/protection, IT strategic planning, IT controls assurance, regulatory readiness and reporting, and IT risk and compliance management. She provides a wide range of risk advisory services to a number of clients in the Federal Government and Fortune 500 companies across industries.

In her previous role, she was responsible for standing up and leading the Information Security & ITRM practice (a 3-million dollar practice after 18 months). She led engagements and provide subject matter advisory for Fortune 500 clients in the areas of Compliance Management, Information Security Management, Data Privacy/Protection, and Risk Governance.

Mrs. Ozderman is an active member of the local ISACA chapter and servers as a regular exam writer for the ISACA CGEIT certification. She has a Master of Science degree in Systems Engineering from Johns Hopkins University. She is also a Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC), Certified Information Privacy Professional (CIPP), and Certified in the Governance of Enterprise IT (CGEIT).

Select Client Engagements:

- Launched and led the assessment of a global commercial bank's governance framework and risk management practices for managing its India-based Outsourcing Service Providers (OSPs) and successfully assisted with preparation of a regulatory examination on Third Party Supplier Management.
- Led the rollout of a Vendor Management Framework and implementation of the framework, policy, and supporting procedures to achieve a robust and comprehensive Vendor Management Program for an FX settlement bank to meet federal regulators' expectations.
- Established an information security management framework based on SANS 20 Critical Controls for a global credit union.
- Led an enterprise-wide security controls gap assessment and remediation project for a leading financial services organization.
- Established an enterprise information protection program for a global logistics company and supported the Safe Harbor compliance filing.
- Developed a Payment Card Information (PCI) compliance program office, remediation framework and roadmap for a Fortune 100 financial services company.
- Led an Applications Development & Maintenance (ADM) Fed Readiness program implementation at an international insurance company, including developing action plans, establishing ADM governance models, and coordinating FFIEC controls implementation across 10 functions/regions.

Placeholder for text

Stephanie Hardt, Manager – PwC Cybersecurity, Privacy and IT Risk

Phone: 202-730-4232
Email: stephanie.l.hardt@pwc.com

Background:

Stephanie is a Third Party Risk Management Senior Associate within the Governance, Risk and Compliance practice based out of Washington, DC. She has seven years of experience in supply chain management with significant emphasis on third party risk and performance management. She has experience in three distinctive industries; national defense, financial services, and global pharmaceuticals. Over the last several years, Stephanie has been dedicated to assisting her employers with third party risk program implementations as well as serving as a third party relationship manager for large outsourcing providers. With PwC, Stephanie has executed third party internal audits and the redesign and execution of a large third party assurance program. She also holds a Masters of Business Administration from the University of Pittsburgh where she focused her studies on global supply chain management and accounting.

Certification and Memberships

- NCMA
- ISACA
- Certified Risk and Information Systems Control (CRISC)

Relevant Projects and Experience:

- Transformed the enterprise third party risk management program for one the largest U.S. financial services providers to comply with OCC and CFPB regulatory requirements. Elements of the transformed program included development of risk assessments, due diligence, on-going monitoring, performance management processes, organizational structures, policies and procedures, training programs, segmentation strategies, and a large third party management technology implementation.
- Led IT and BPO third party relationship management activities for a global pharmaceuticals provider including onsite controls and performance audits at offshore delivery centers in India.
- Executed an internal audit of the largest international development bank's IT third party management practices resulting in monetary recovery to the organization
- Redesigned elements of a large British banking and insurance corporation Third Party Assurance program and facilitated the execution of the organizations Third Party Assurance program on their behalf

Placeholder for text

Danny Wuckovich, Senior Associate – PwC Cybersecurity, Privacy and IT Risk

Phone: (571) 213 -8308
Email: danny.w.wuckovich@pwc.com

Danny is a Senior Associate in the Cybersecurity & Privacy Services practice based out of the Washington metro region. Danny has specialized in the area of information security and third party risk management, and has been actively involved in assisting clients in managing the security risks stemming from their third-party relationships across the world. Danny is currently leading one of PwC's largest third-party risk engagements in the Washington Metro region whereby the client has fully outsourced our capabilities to manage a portfolio of 300+ third-parties. Danny is responsible for coordinating and interfacing on a daily basis with client personnel, providing technical guidance and direction to teams of assessors and third-party relationship managers, and executing operations and continuous improvement of the overall third-party risk management program. With his background in cybersecurity and privacy, he is able to understand the key risks as it relates to his client's third-parties and the scope of their services. In doing so, Danny is able to deliver efficiencies and cost savings to our client, and ensure third-party risks are being effectively across the entire portfolio of vendors, suppliers, service providers, joint ventures, etc.

Select Client Engagements:

- Global Third Party Risk Management Program Design, Implementation, and Execution for Fortune 500 companies and 501(c)(4) Nonprofit organizations.
- Domestic and global Third Party Risk Assessments for Financial Services, Healthcare, and Power and Utilities clients.
- Currently leads the Third Party Security Program as part of an outsourcing agreement for a portfolio of over 300 vendors with security assessments being performed on a rolling 12 month basis
- Executed and led Third Party Assessments – Desk-top reviews and global/domestic on-site assessments
- Assessed Third Party Risk Management capabilities in support of Internal Audit
- Cybersecurity Program design, implementation, and assessments for Financial Services clients
- Cybersecurity Program Maturity Assessments – reviewing cybersecurity program design, implementation, and effectiveness of the programmatic, procedural, and technical controls supporting the overall program
- Technical security audits (e.g., database management audits, operating system audits, etc.)
- Development of organizational security structures, including defining security strategy and objectives, supporting functional security roles, business and IT risks, and tactical activities required for Fortune 500 organizations.