Developing a Successful GRC Third Party Risk Management Program by Understanding Strategies and Industry Trends

ISACA Tokyo Chapter Seminar

February 17, 2017

EY
Building a better
working world

Harald deRopp

Executive Director
EY Advisory & Consulting Co., Ltd.

Harald has lived in Japan for over 20 years and has been with Ernst & Young (EY) in Japan for over 13 years performing IT audit and advisory engagements for financial institutions.

He is the eGRC solution leader for EY Financial Services Advisory in Tokyo providing IT GRC tool implementation and Third Party Risk Management services to financial services clients.

Prior to joining EY, Harald worked at the Japan branch of a US insurance company performing accounting and systems project management functions.

Agenda

Part I: Presentation

- Evolving regulatory expectations
- Third Party Risk Management (TPRM) industry perspective
  - 2016 EY TPRM Survey – only firm globally to produce an annual TPRM survey dedicated to financial services.
- EY Third Party Risk Management (TPRM) framework overview
- Cybersecurity and Enterprise Resilience and Recovery
- Protecting the enterprise – TPRM

Part II: Panel Discussion

Evolving regulatory expectations

Evolving regulatory expectations

Firms are facing a new regulatory environment

Regulatory landscape has changed significantly

- Firms face a wide range of regulatory change globally. This creates practical challenges in implementation, and mandated timescales can result in tactical or short-term solutions.
- Enhanced risk governance requirements are routinely cited in new regulations or supervisory examinations with significant focus on IT Security, Cyber, Enterprise resilience related to third party providers.
- The direction that many national regulators are taking has significantly increased the challenges and costs of operating a global or regional business and has a direct impact on risk governance.

Focus on remediation

- Regulatory fines and costly remediation. programs are at an unprecedented level.
- This is having a longer-term impact on business models.

Revenue and cost pressure

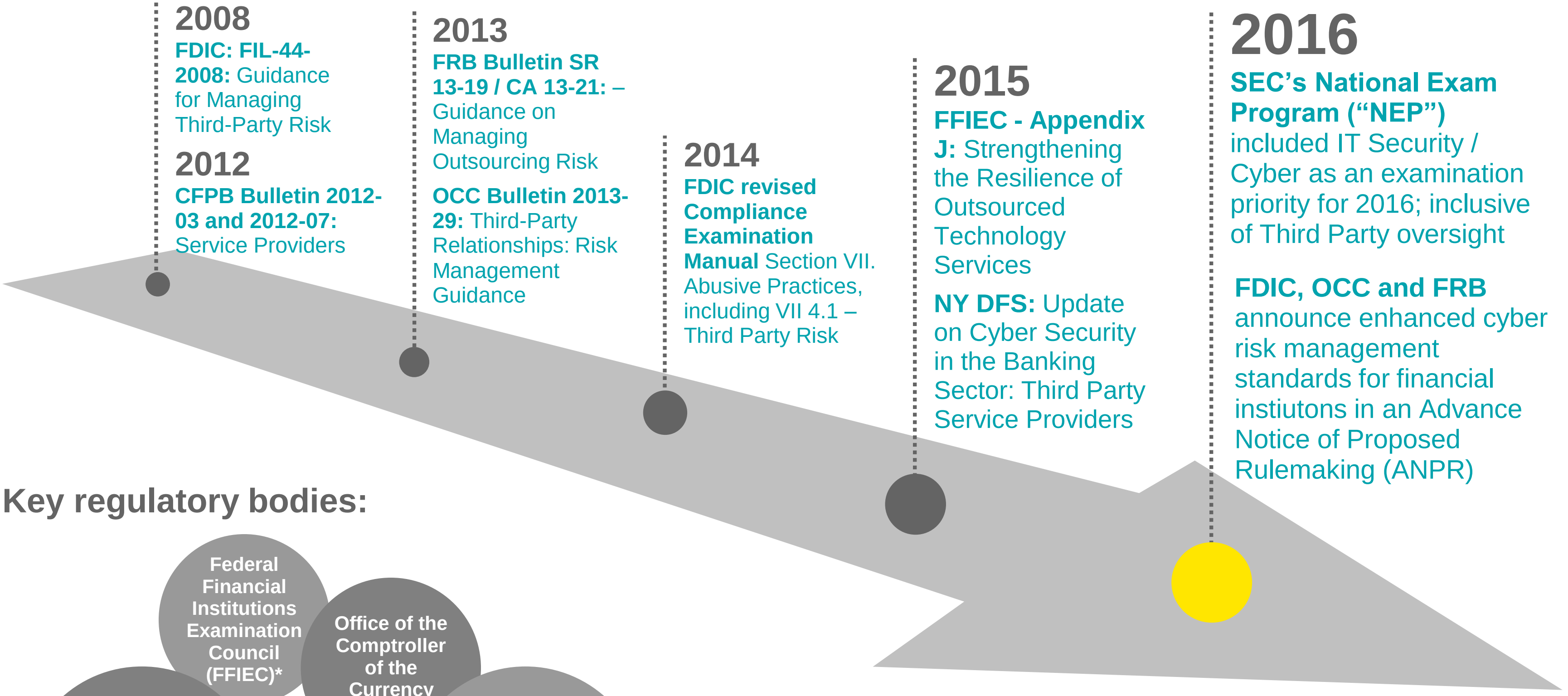
- There is a direct impact on revenues and business models, including exiting business lines.
- New regulation means operating to higher standards at significant cost.

New business models require a new approach to risk governance

- Firms will be operating in a new environment with a greater cost of regulation. As a result, many firms are transitioning to simpler and less global business models.
- Regulators are applying leading expectations regardless of relative size and scale.
- Investors are demanding sustainable returns and are applying pressure on costs.
- Risk governance needs to be forward-looking and influence strategic decisions and not just deal with the consequences of them.

Evolving regulatory expectations

Third Party Risk focus broadens



2008

FDIC: FIL-44-2008: Guidance for Managing Third-Party Risk

2012

CFPB Bulletin 2012-03 and 2012-07: Service Providers

2013

FRB Bulletin SR 13-19 / CA 13-21: – Guidance on Managing Outsourcing Risk

OCC Bulletin 2013-29: Third-Party Relationships: Risk Management Guidance

2014

FDIC revised Compliance Examination Manual Section VII. Abusive Practices, including VII 4.1 – Third Party Risk

2015

FFIEC - Appendix J: Strengthening the Resilience of Outsourced Technology Services

NY DFS: Update on Cyber Security in the Banking Sector: Third Party Service Providers

2016

SEC's National Exam Program ("NEP") included IT Security / Cyber as an examination priority for 2016; inclusive of Third Party oversight

FDIC, OCC and FRB announce enhanced cyber risk management standards for financial instituons in an Advance Notice of Proposed Rulemaking (ANPR)

Key regulatory bodies:

Federal Financial Institutions Examination Council (FFIEC)*

Office of the Comptroller of the Currency (OCC)

Federal Reserve Board (FRB)

Federal Deposit Insurance Company (FDIC)

Consumer Financial Protection Bureau (CFPB)

Security and Exchange Commision (SEC)

NY Department of Financial Services (NY DFS)

...

* The FFIEC is a formal U.S. government interagency body that includes five banking regulators – FRB, FDIC, OCC, CFPB and the National Credit Union Administration (NCUA).

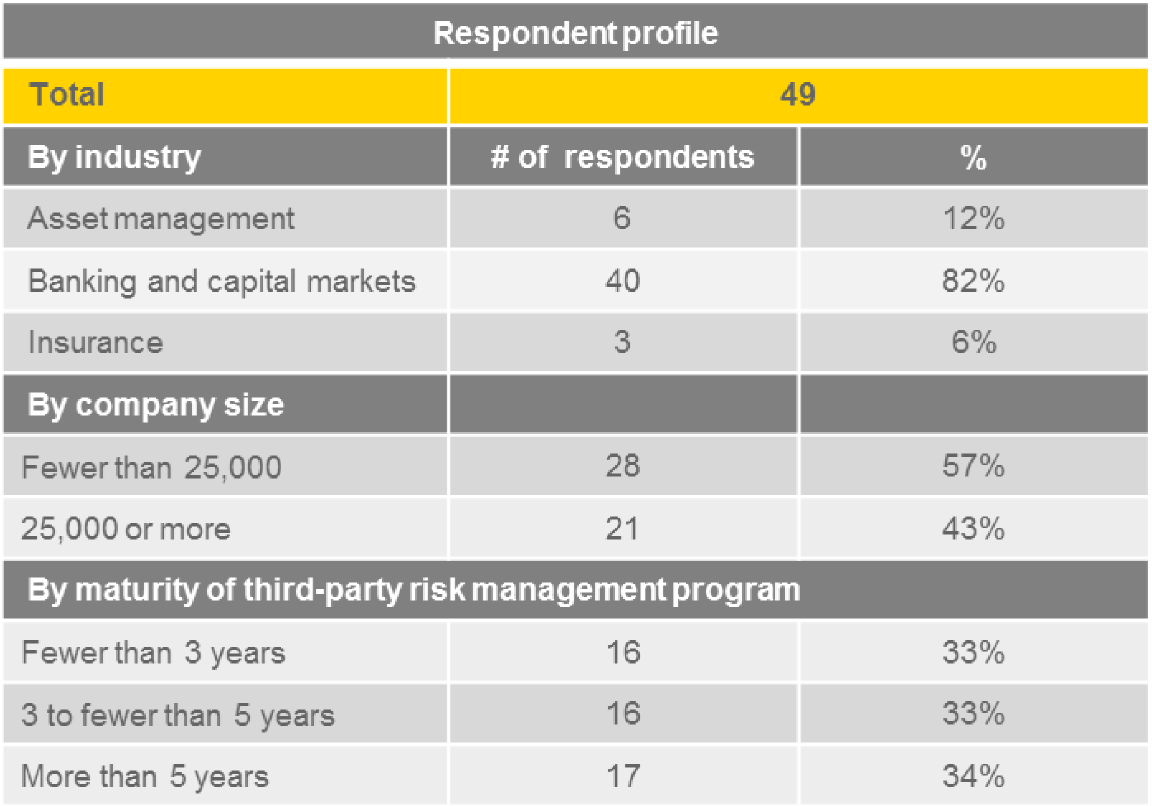
Increasing regulatory / industry focus on IT Security / Cyber and Resilience / Recovery in connection to third parties.

TPRM industry perspective

EY Third Party Risk Management survey – 2016

Overview

- EY's financial services industry survey of Third Party Risk Management (TPRM)
- 2016 was the 5th year of the survey and 49 global financial services organizations participated.
- Participants receive a breakdown of their survey results with a comparison to their peers for benchmarking purposes.
- 2017 survey is now underway. A new non-financial services industry survey has been added.



Respondent profile		
Total	**49**	
By industry	**# of respondents**	**%**
Asset management	6	12%
Banking and capital markets	40	82%
Insurance	3	6%
By company size		
Fewer than 25,000	28	57%
25,000 or more	21	43%
By maturity of third-party risk management program		
Fewer than 3 years	16	33%
3 to fewer than 5 years	16	33%
More than 5 years	17	34%

Survey Focus Areas

1. Third Party Population
2. Operating Model
3. Critical Third Parties
4. Assessment Framework
5. Termination / Exit Strategies
6. Oversight and Governance; Quality Assurance / Quality Control
7. Regulatory Exams
8. Technology
9. Inbound TPRM
10. Industry Outlook

EY Third Party Risk Management survey – 2016

Summary of Key Findings

39% ⇧ of organizations said **all of their third parties** fall within the scope of their TPRM program – up from 19% in ’14. 86% use 3 and 5 risk tiers.	**43%** ⇧ of organizations reported **critical third parties** to the board – up from 26% in ’14. Only 31% report third party breaches to the board.	**41%** ⇧ of organizations said primary ownership of the **TPRM function falls within procurement** (first line of defense) – up from 26% in ’14.	**Population and governance**
80% ⇔ of organizations reported they **spend two days or less on-site** when conducting information security and business resilience reviews.	**71%** ⇧ of firms **find SOC2 reports useful** in reducing the need to perform a review – up from 52% in ’14; while 74% conduct regulatory compliance reviews pre-contract.	**75%** ⇧ of organizations **rely on third parties to manage / evaluate fourth parties** through control assessments or contract terms – up from 36% in ’14.	**Assessment framework**
71% ⇔ of firms were either neutral or **face challenges with business unit support** in executing program requirements.	**90%** ⇩ of respondents **felt neutral / negative about TPRM tool integration** and ability to capture the overall risk for reporting – 49% require 1+ weeks to pull reports.	**44%** ⇔ of ranked **enterprise-critical third parties top regulatory review focus**, matched by oversight / governance 44%, and information security / enterprise resilience 38%.	**Industry / regulatory outlook**

Lack of knowledge across business functions and a pervasiveness of disintegration across third-party management tools were noted as significant barriers to greater progress…

A closer look at the Numbers

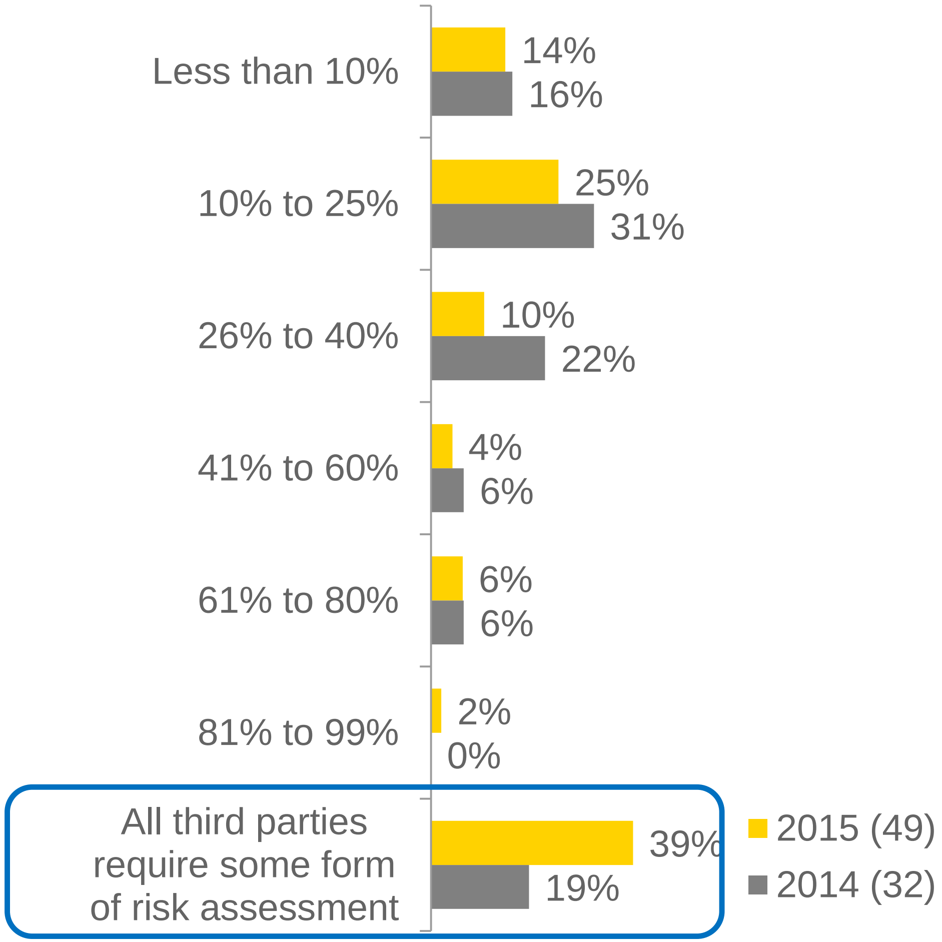
Population and governance

⇧ 39% of organizations said **all of their third parties** fall in scope of their TPRM program

Proportion of third parties in scope for risk

Q5. What percentage of third parties are in-scope for your organization's risk management program?

- More firms are doing risk monitoring of **all** of their third parties.



Notes:

- 2016 survey was performed October - December 2015.
- 2015, 2014 and 2013 in the legends refer to the 2016 2015, and 2014 surveys respectively.

⇧ indicates upward trend from the Previous Year (PY)

⇩ indicates downward trend from the Previous Year (PY)

⇔ indicates no change in the trend from the Previous Year (PY)

A closer look at the Numbers

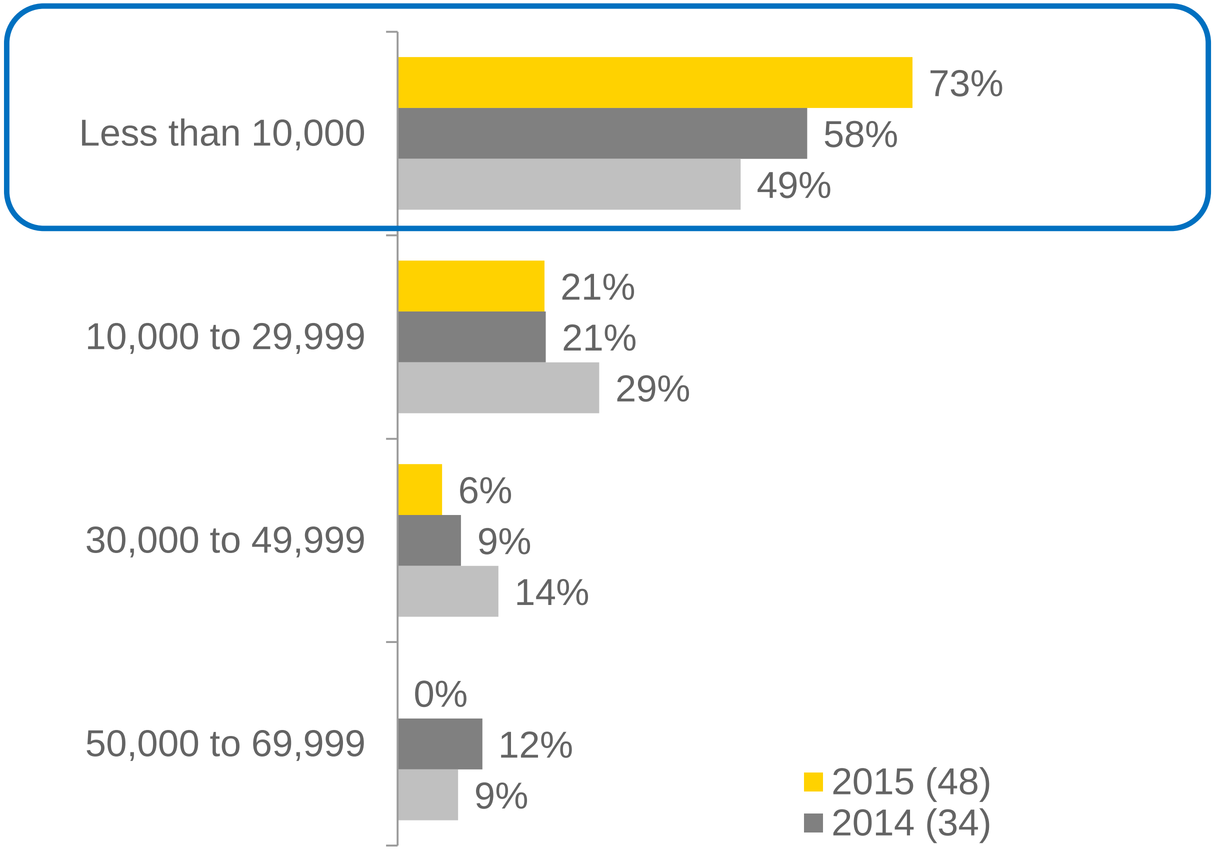
Population and governance

⇧ 73% of organizations have less than 10,000 vendors

Third-party inventory

Q4. Approximately how many third parties are within your organization's inventory/population?

- Firms are **reducing** the number of their third party vendors



A closer look at the Numbers

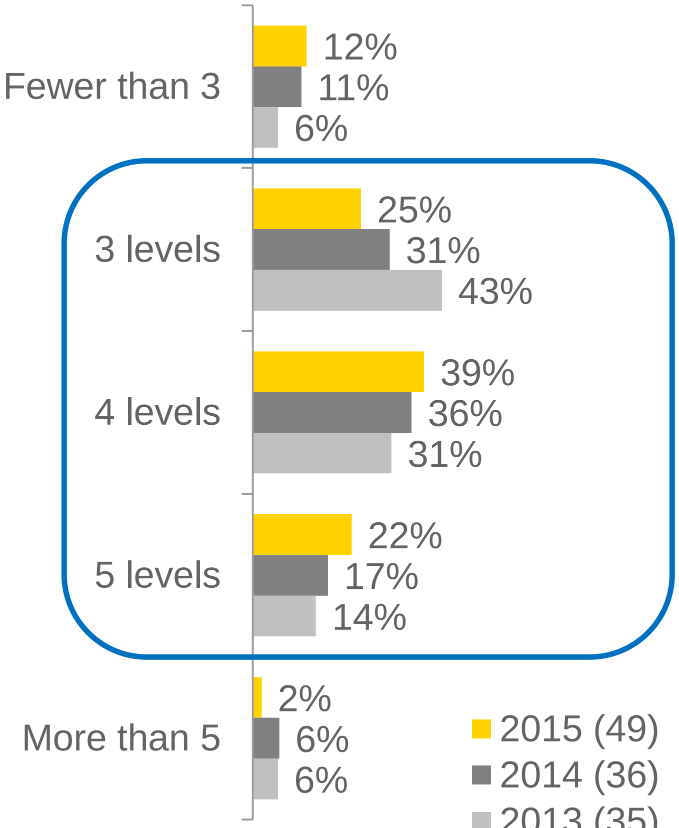
Population and governance

⇧ 86% of organizations use **3 to 5 risk tiers**

Levels of risk tiers to segment third parties

Q6. How many levels of risk or tiers are used to segment third parties within your organization’s program?

- Firms are going beyond the traditional “High” , “Medium”, “Low” risk tiers to segment their third parties.



A closer look at the Numbers

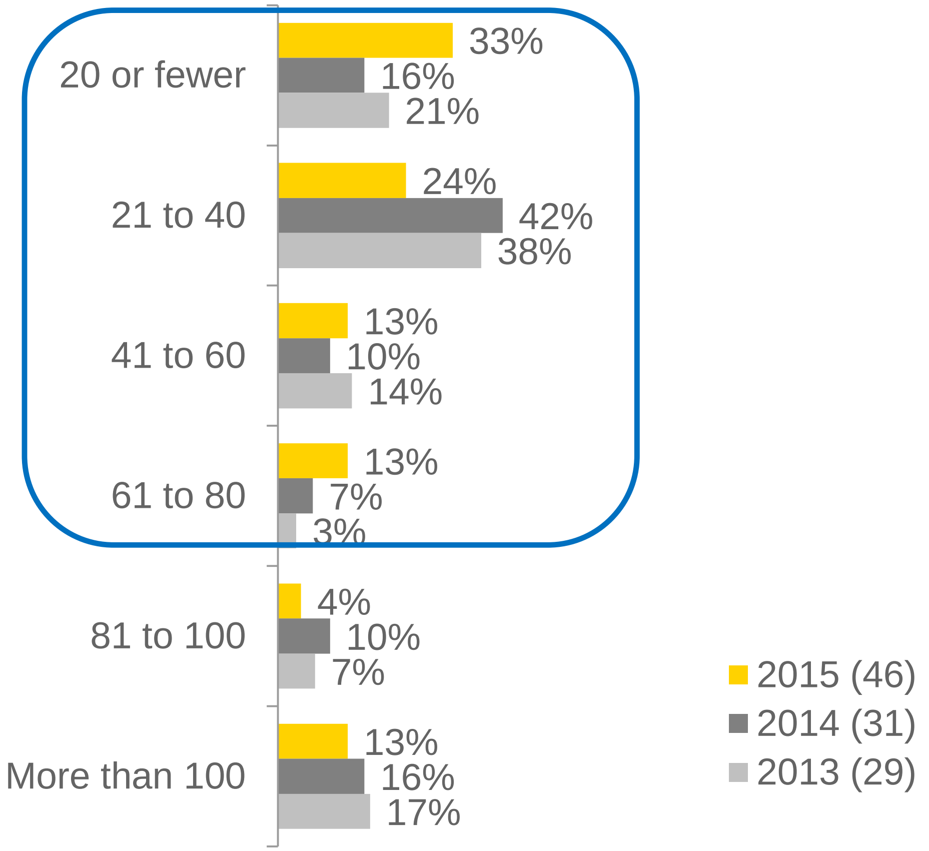
Population and governance

⇧ 33% of organizations have 20 or fewer **critical third parties**

Number of critical third parties

Q8. How many critical third parties are within the organization’s third-party inventory?

- Almost all firms (93%) keep an inventory of critical third parties.
- Firms are reducing the number of their critical third parties. 83% have 80 critical third parties or less.



A closer look at the Numbers

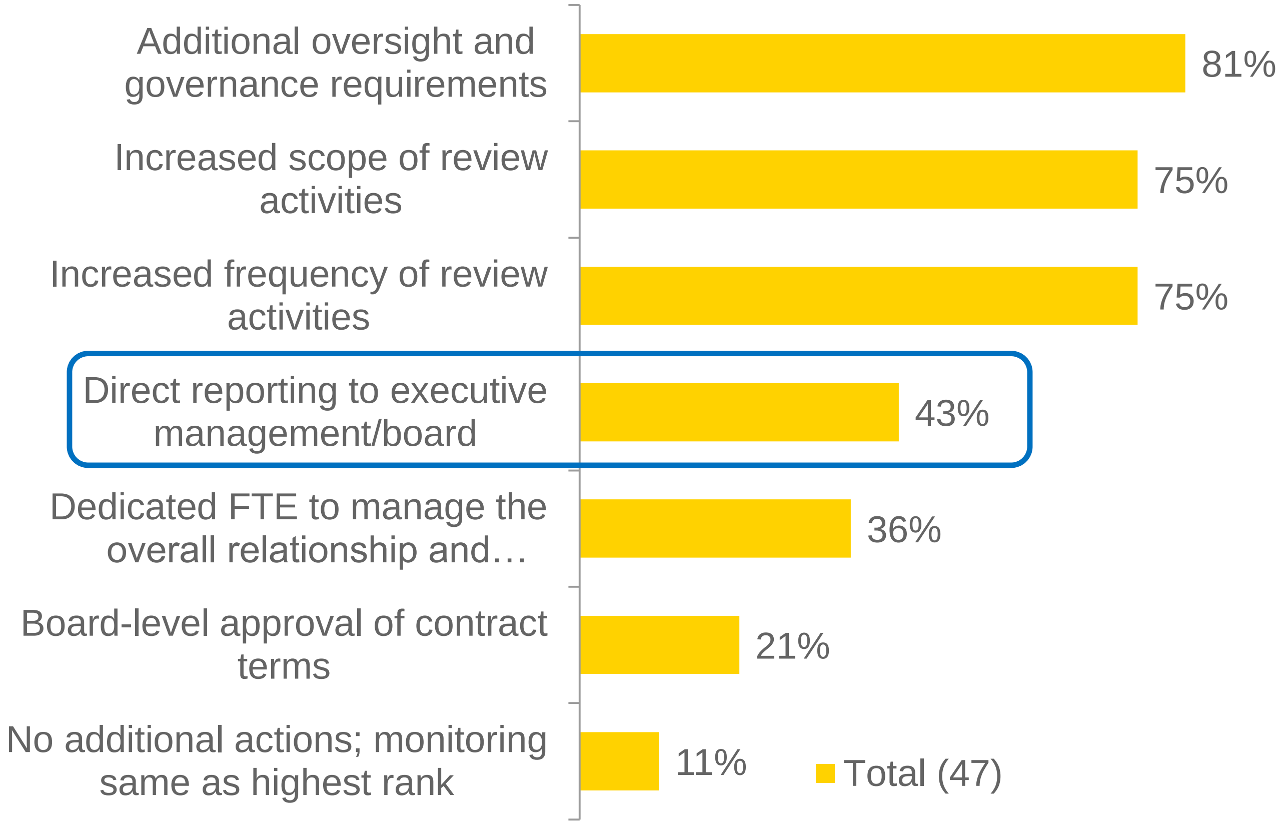
Population and governance

⇧ 43% of organizations reported **critical third parties** to the board

Additional actions applied for critical third parties

Q10. What additional actions are applied, outside of standard management activities, for your critical third parties? Please select all that apply.

- Direct reporting of critical third parties to Boards has increased from PY 26%
- Most firms apply additional oversight and governance, and increased scope and frequency of review for critical third parties.



A closer look at the Numbers

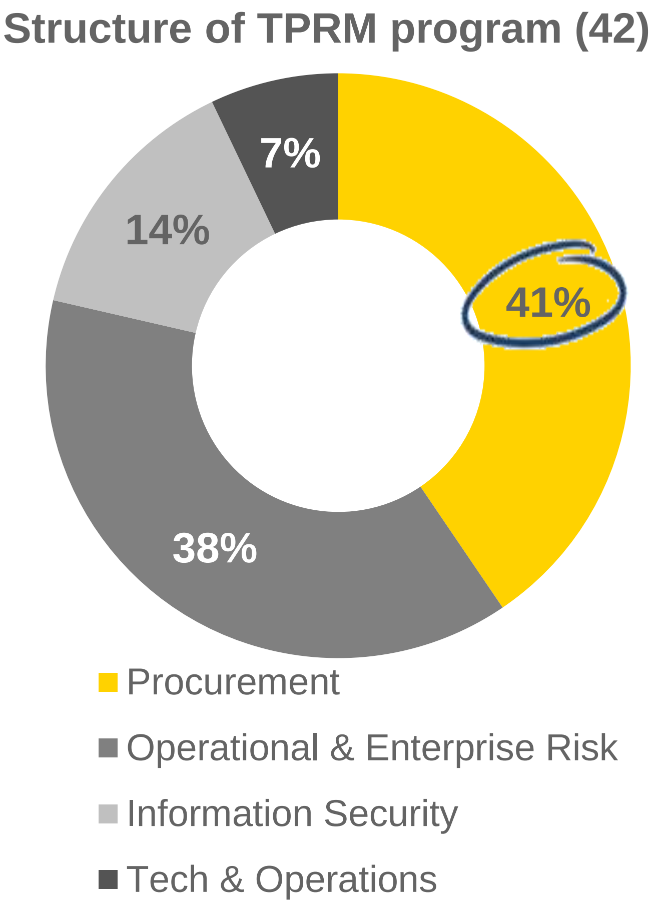
Population and governance

⇧ 41% of organizations said primary ownership of TPRM is with Procurement

Primary ownership of TPRM function

Q11. What area has primary ownership of the third-party risk management function?

- At most firms TPRM is primarily owned by either Procurement or Operational & Enterprise Risk.
- In PY, only 26% said Procurement was the primary owner.



A closer look at the Numbers

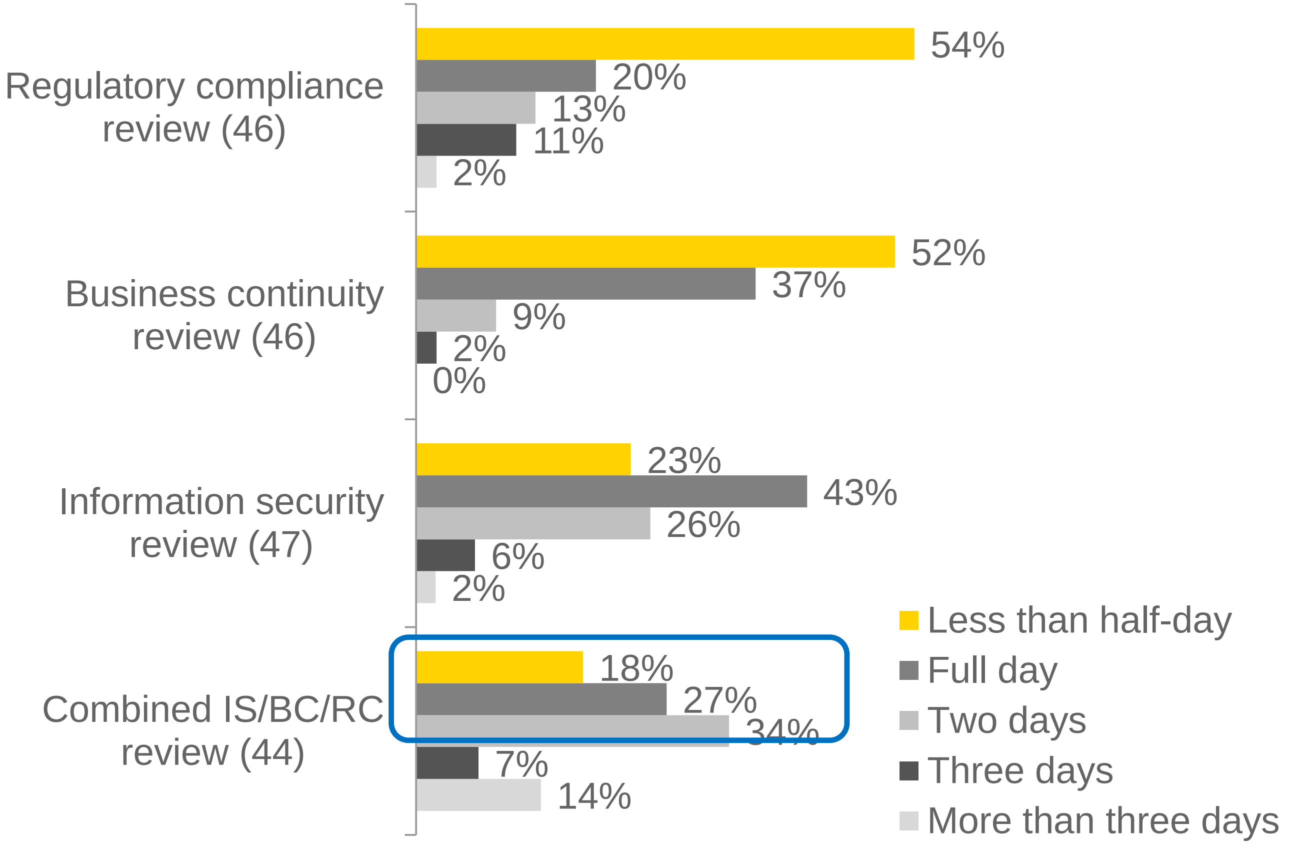
Assessment framework

⇔ 80% of organizations said they spend two days or less for on-site reviews

Duration of on-site reviews

Q21. When conducting an on-site review at a third-party site, what is the typical duration of the site visit for each of the following components of the review (excluding travel)?

- ► Most firms spend two days or less for on-site reviews of their vendors which is unchanged from the PY.
- ► However, full day or less than half day on-site visits are more common.



A closer look at the Numbers

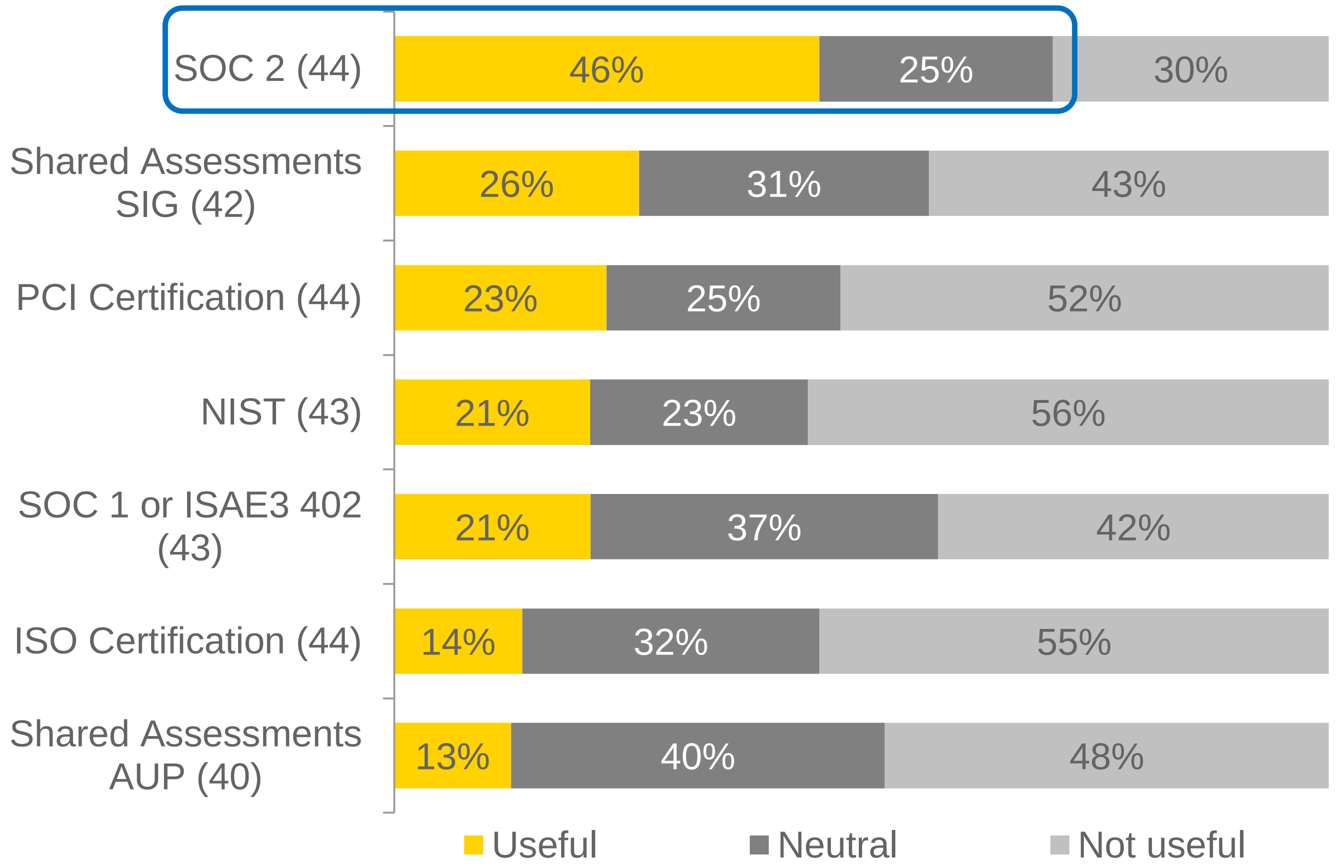
Assessment framework

⇧ 71% of organizations rely on SOC2 reports to reduce the need to perform reviews of controls

Usefulness of reports in reducing need for control assessment

Q24. On a 5 point scale, with 1 – not at all useful and 5 – extremely useful, when considering the need to perform a control review, which of the reports listed below are the most useful in reducing or removing the need to perform a review on a third party?

- ► Most firms (71%) see Service Organization Control 2 (SOC 2) Reports as a useful way to reduce the need for control self-assessments
- ► An increase from 52% of firms in PY..



A closer look at the Numbers

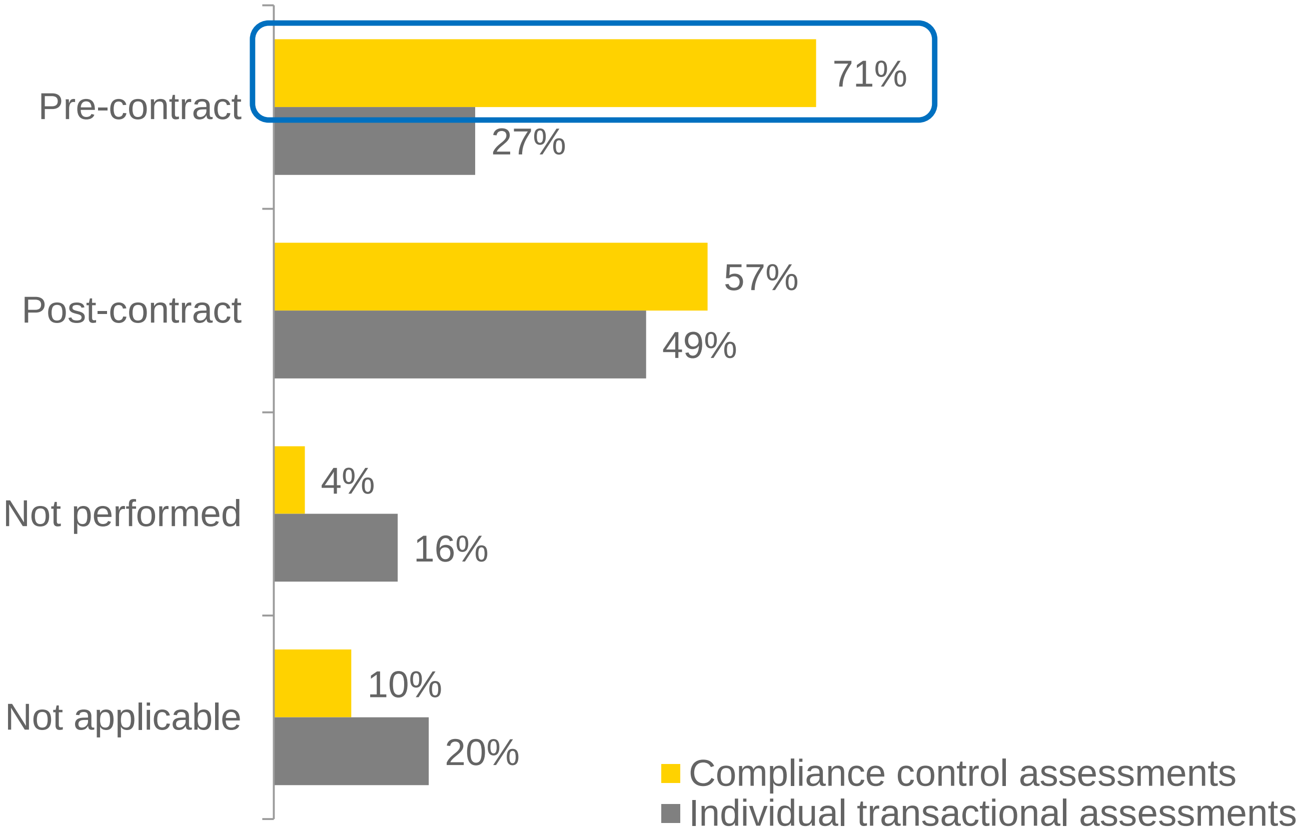
Assessment framework

⇧ 71% conduct regulatory compliance reviews pre-contract

Conducting regulatory compliance reviews

Q29. When are regulatory compliance reviews conducted? Please select all that apply.

- Most firms (71%) conduct regulatory contract reviews before contracting with third parties
- An increase from 47% of firms in PY.



A closer look at the Numbers

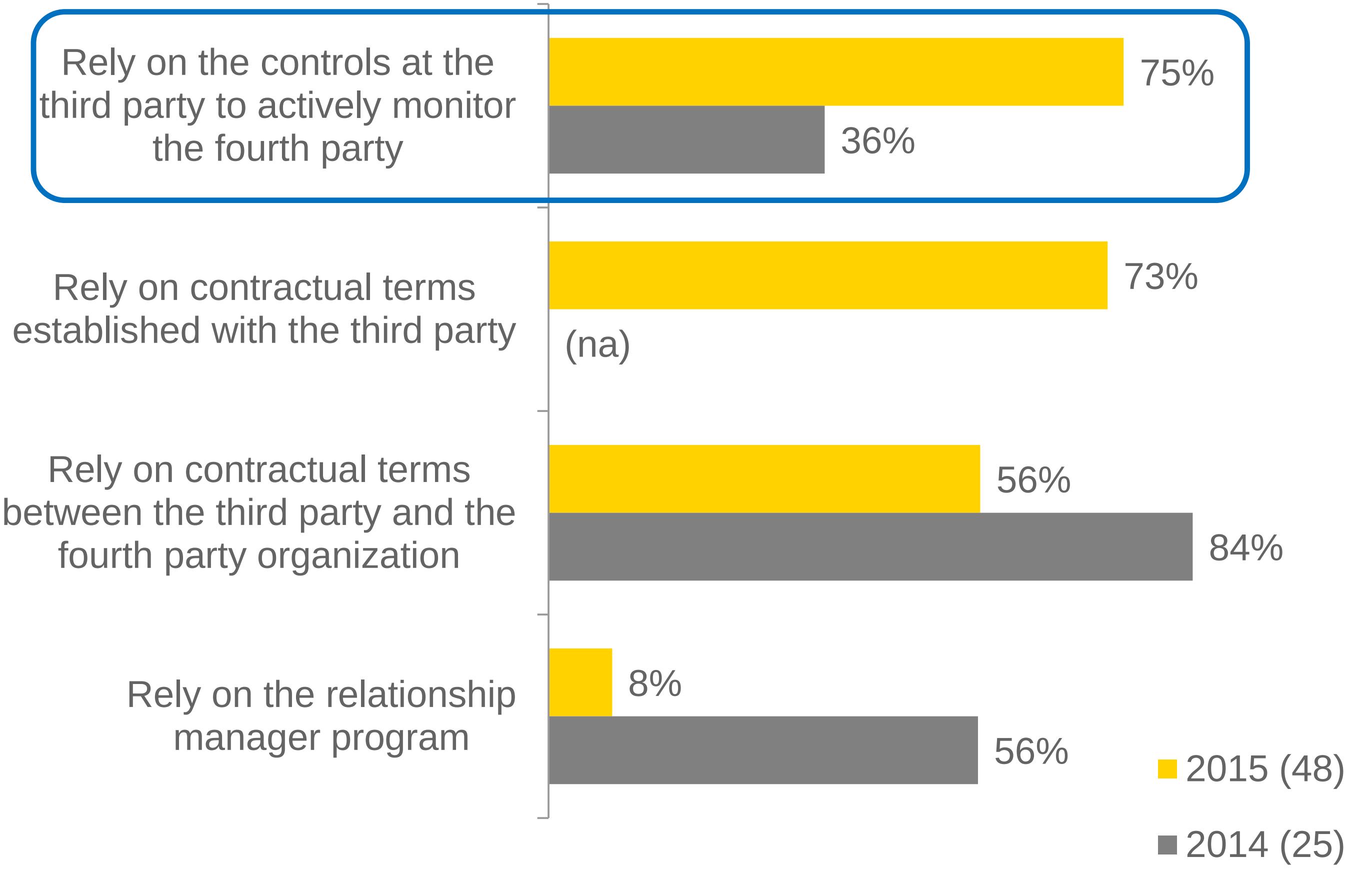
Assessment framework

⇧ 75% of organizations rely on third parties to manage / evaluate fourth parties

Assessing & monitoring fourth parties

Q31. How does your organization assess/monitor fourth parties? Please select all that apply.

- Most firms (75%) rely on the controls at the third party to monitor the fourth party
- It's less acceptable to rely on contractual terms between the 3rd and 4th parties or relationship manager programs



EY

A closer look at the Numbers

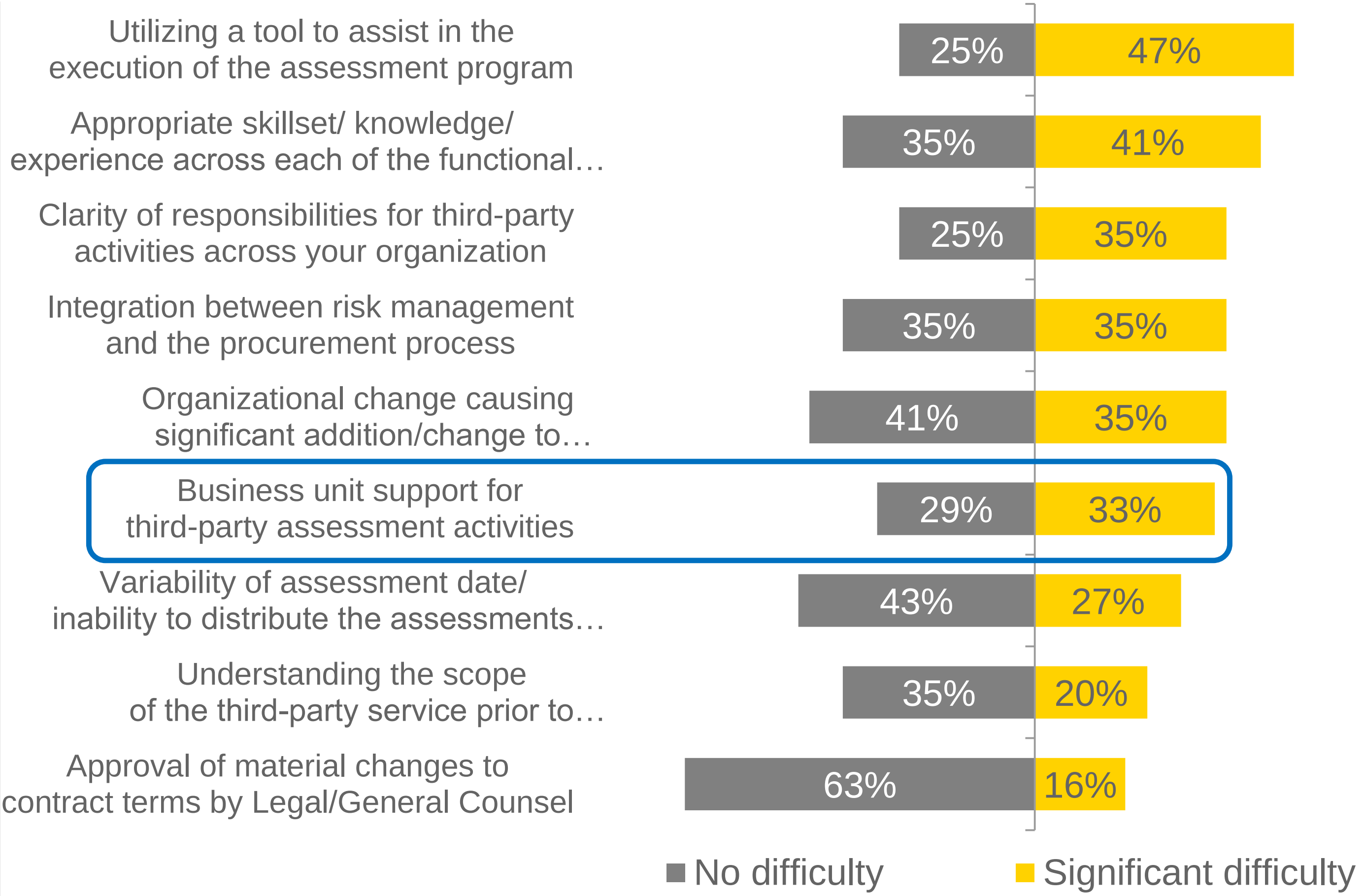
Industry / regulatory outlook

⇔ 71% of organizations were either neutral or faced challenges with business unit support

Challenges

Q20. On a 5-point scale, with 1 – no difficulty and 5 – significant difficulty, what degree of difficulty does your organization face in addressing each of these potential challenges to your third-party risk management program?

- Business unit support for third party assessment activities continues to be a challenge.
- Using a tool and having persons with the appropriate skillset / knowledge and experience for the activities is also a challenge.



A closer look at the Numbers

Industry / regulatory outlook

⇧ 22% of firms use proprietary tools for their TPPM activities

Use of tools

Q45. What technology/tool does your organization use for each of the following functions?

- Firms are using a variety of tools to manage TPPM activities.
- There is no one tool that significantly excels above the others at all TPRM activities.
- Use of proprietary tools grew from 9% of firms in PY.

Use of Tools (46)

	Archer	Bwise	Oracle	Ariba	SAP	Hyperos	Proprietary	Other
Sourcing activity	7%	2%	9%	**33%**	7%	7%	22%	22%
Inherent risk assessment	26%	2%	2%	2%	2%	13%	**33%**	17%
Contract repository	4%	2%	9%	**30%**	7%	0%	22%	26%
Primary third-party inventory	**26%**	2%	4%	4%	4%	11%	**26%**	**26%**
Control assessment facilitation tool	**30%**	2%	0%	0%	0%	13%	24%	20%
Issue management tool	26%	7%	2%	0%	0%	9%	**28%**	24%

A closer look at the Numbers

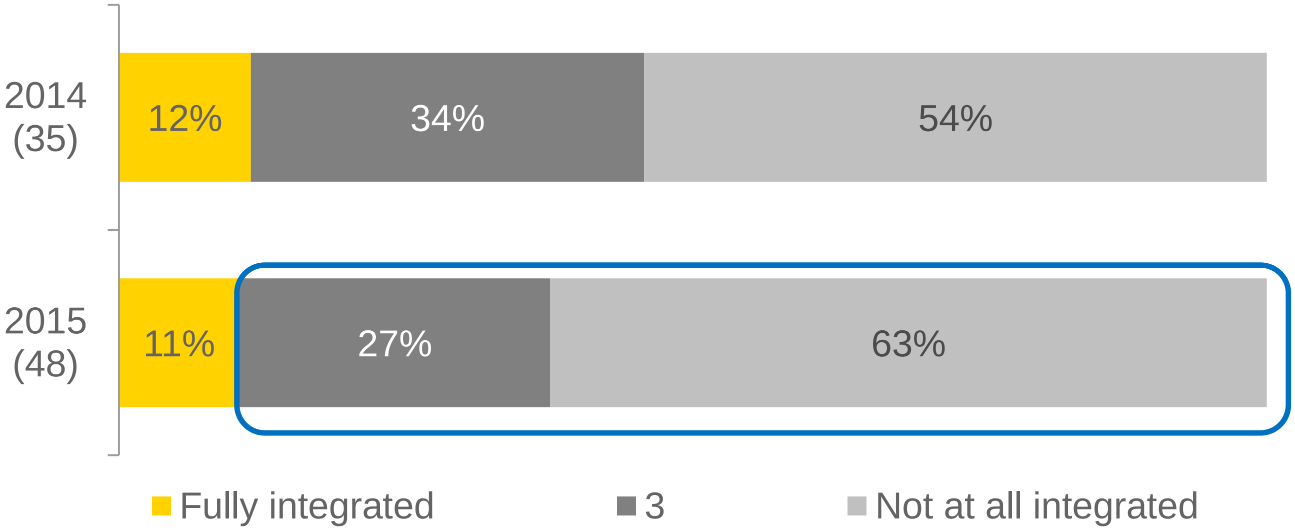
Industry / regulatory outlook

⇩ 90% of firms were neutral or negative about TPRM tool integration and reporting capabilities

Reporting tool integration

Q46. On a scale of 1 to 5, with 1- not at all integrated and 5 – fully integrated, how well do the above tools integrate and capture the overall risk for reporting purposes?

- Most firms are very dissatisfied with the lack of the integration of TPRM tools and the ability of the tools to capture the overall risk and report on it.
- In the PY firms were less dissatisfied.



A closer look at the Numbers

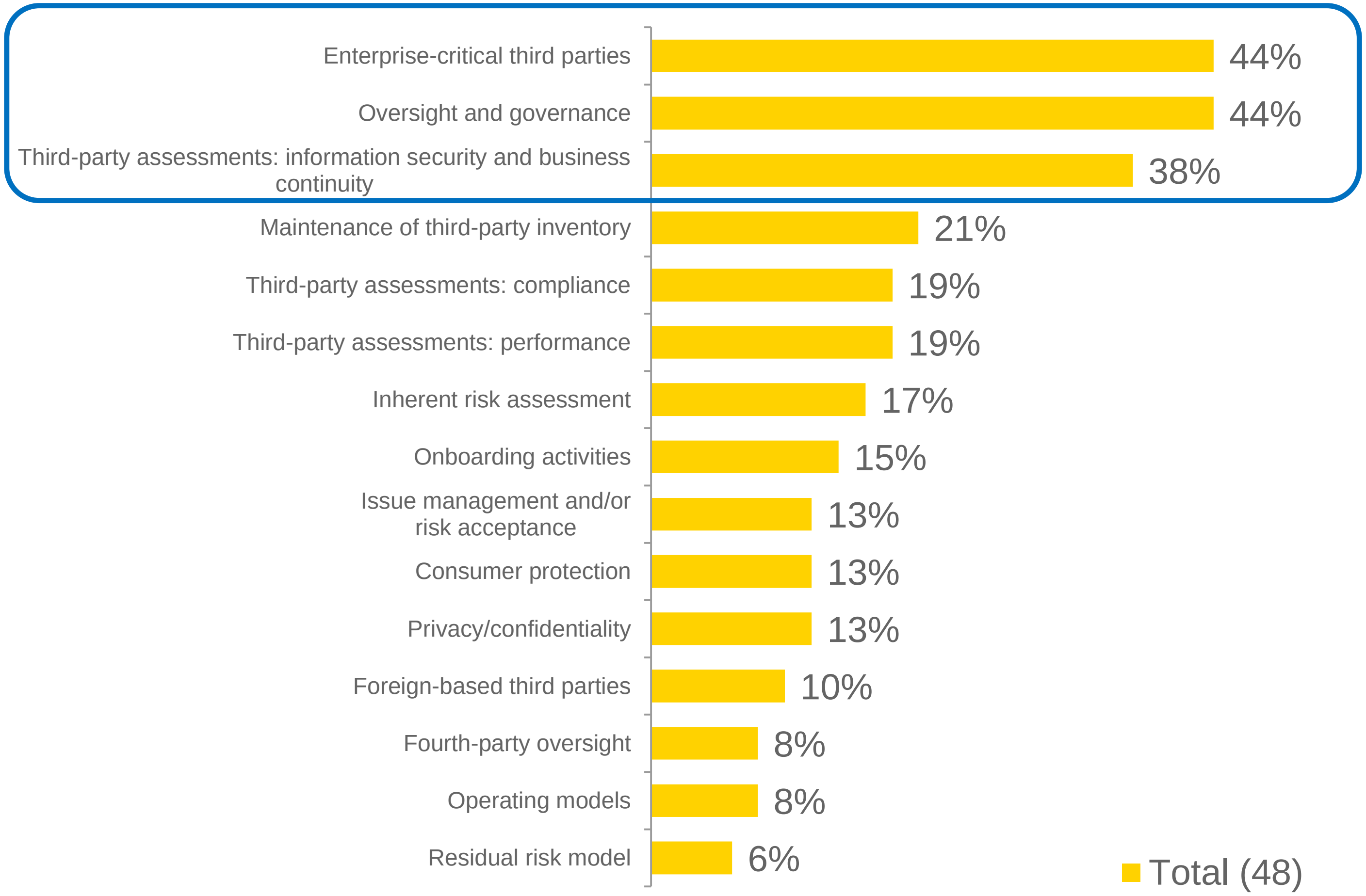
Industry / regulatory outlook

⇔ 44% of firms said regulators are most concerned with reviewing enterprise-critical third parties

Regulatory body review focus areas

Q41. During your organization's most recent regulatory body review, what were the 2 to 3 most important areas of focus?

- Regulators' main focus continues to be on enterprise-critical parties but oversight and governance, and third party assessments for information security and business continuity are also key focus areas.



Key takeaways from the EY 2016 TPRM Survey

- Review your inventory of third parties.
  - ✓ Is it accurate and complete?
  - ✓ Are there some vendors that can be eliminated?
  - ✓ Do you have more than 80 critical third parties?.
- Review your third party risk tier segmentation.
  - ✓ Do you have a sufficient number of tiers?
- Review your risk monitoring coverage
  - ✓ Do you do risk assessments of all your vendors?
  - ✓ Can you do your on-site reviews more efficiently?
  - ✓ Do you do regulatory compliance reviews pre-contract?
- What TPRM reporting do you have?
  - ✓ Do your report critical third parties to the board?
- Do you know what regulations you must comply with for TPRM?
- Review your management of 4th party risk
  - ✓ Do you know who your 4th parties are?
  - ✓ Are there adequate controls at the 3rd party for them?

Key takeaways from the EY 2016 TPRM Survey

- How do you manage your TPRM program?
  - ✓ Consider implementing a tool to better manage the complexity
  - ✓ There is no one dominant tool that can “do it all” for you.
- Benchmark against your competitors
  - ✓ Consider to participate in the 2017 TPRM survey to be able to compare your firm to others in your industry.

TPRM framework

TPRM framework

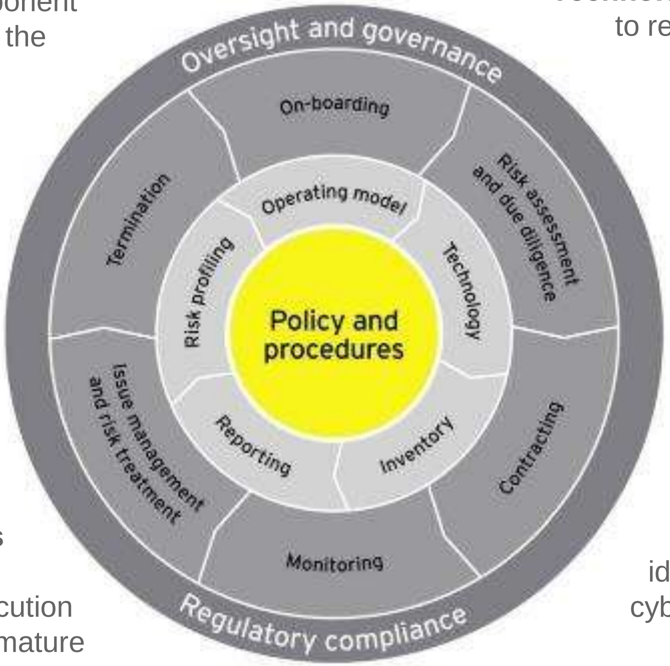
Functional components

A TPRM function is comprised of six functional components that enable efficient, consistent and enterprise-wide execution.

Oversight and governance is the component that oversees the function to ensure that the relationships and activities are managed effectively. This consists of the following sub-components: reporting, issue management and escalation, internal and external program liaison, quality assurance and policy adherence.

The **Operating Model** defines clear roles and relationships supportive of consistent, risk based application of all functional enterprise-wide TPRM process.

Enterprise-wide **Policy and Procedures** establish clear roles and responsibilities for all functional owners through the execution of the end-to-end TPRM lifecycle. More mature functions embed service / risk management within third party management policy / procedures for stream-lined integration and execution.



Technology and Data enable TPRM processes to reduce overall function cost. Additionally, the use of technology increases data integrity and drive seamless and reliable reporting.

Risk models help ensure monitoring activities are reflective of the inherent / residual risk associated with third parties and their services – essential in quantification and illustration of TPRM program value.

Risk assessment and due diligence are essential.to understand the third parties control environment around identified risks (e.g. enterprise resilience, cyber security, regulatory compliance etc.)

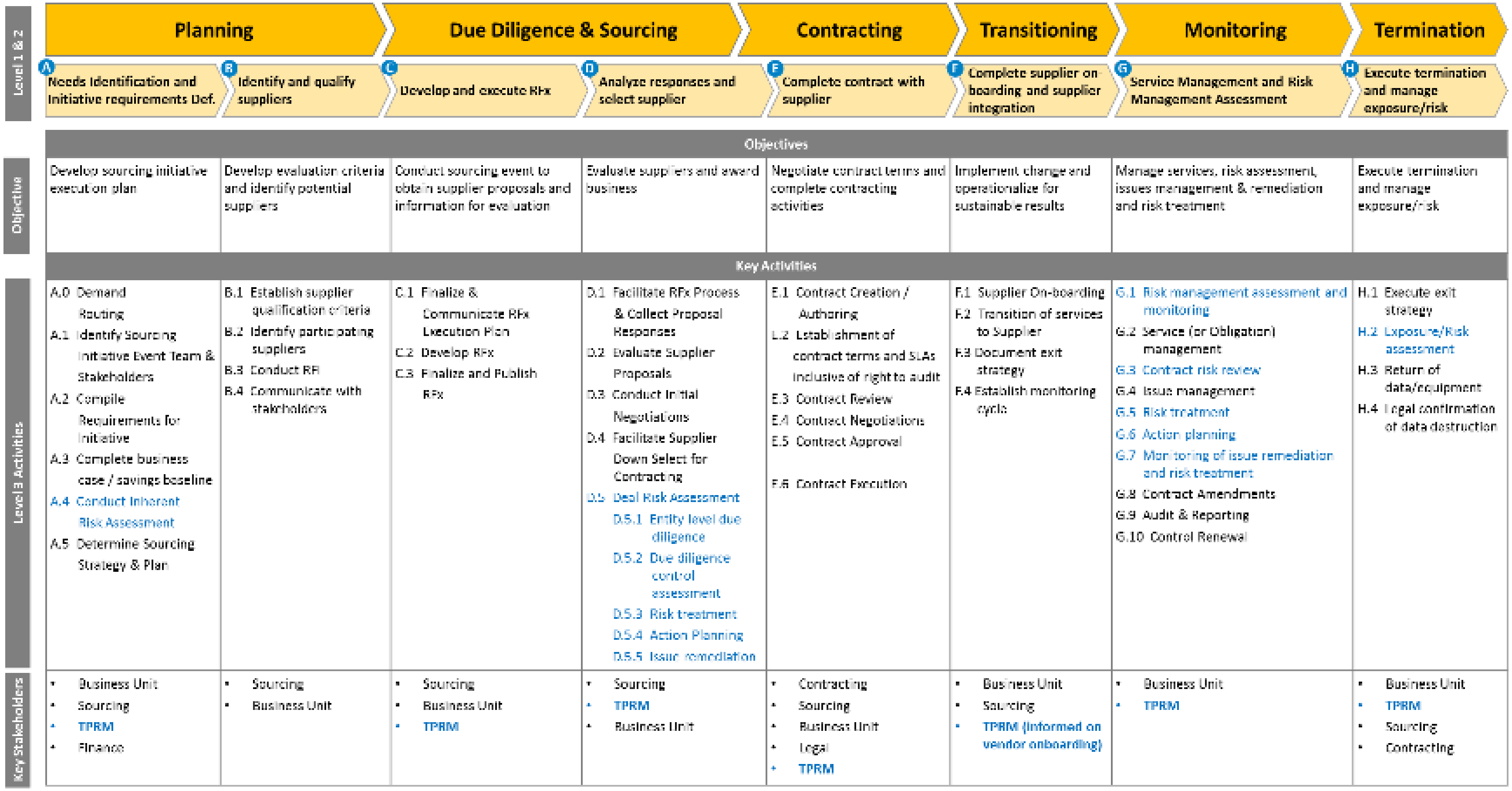
Monitoring is the periodic assessment and management of risk and service performance relative to a third party and the services provided once a contracted.

41% of firms said primary ownership of the TPRM function falls within procurement (1st line of defense)
– 2016 TPRM survey

TPRM framework

Workflow and stakeholders

A leading TPRM program is seamlessly integrated into the overall third-party management lifecycle, maintaining a balance between process, risk management and compliance.



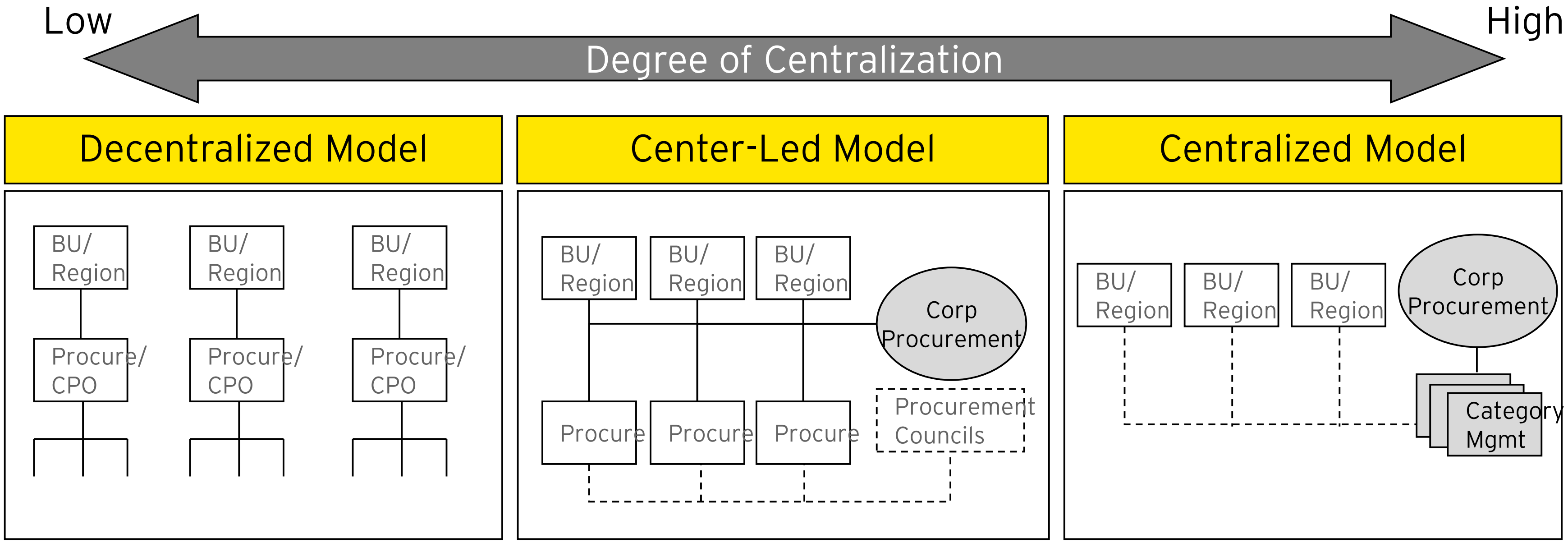
	Planning		Due Diligence & Sourcing		Contracting	Transitioning	Monitoring	Termination
Level 1 & 2	A Needs Identification and Initiative requirements Def.	B Identify and qualify suppliers	C Develop and execute RFx	D Analyze responses and select supplier	E Complete contract with supplier	F Complete supplier on-boarding and supplier integration	G Service Management and Risk Management Assessment	H Execute termination and manage exposure/risk
	Objectives							
Objective	Develop sourcing initiative execution plan	Develop evaluation criteria and identify potential suppliers	Conduct sourcing event to obtain supplier proposals and information for evaluation	Evaluate suppliers and award business	Negotiate contract terms and complete contracting activities	Implement change and operationalize for sustainable results	Manage services, risk assessment, issues management & remediation and risk treatment	Execute termination and manage exposure/risk
	Key Activities							
Level 3 Activities	A.0 Demand Routing A.1 Identify Sourcing Initiative Event Team & Stakeholders A.2 Compile Requirements for Initiative A.3 Complete business case / savings baseline A.4 Conduct Inherent Risk Assessment A.5 Determine Sourcing Strategy & Plan	B.1 Establish supplier qualification criteria B.2 Identify participating suppliers B.3 Conduct RFI B.4 Communicate with stakeholders	C.1 Finalize & Communicate RFx Execution Plan C.2 Develop RFx C.3 Finalize and Publish RFx	D.1 Facilitate RFx Process & Collect Proposal Responses D.2 Evaluate Supplier Proposals D.3 Conduct Initial Negotiations D.4 Facilitate Supplier Down Select for Contracting D.5 Deal Risk Assessment D.5.1 Entity level due diligence D.5.2 Due diligence control assessment D.5.3 Risk treatment D.5.4 Action Planning D.5.5 Issue remediation	E.1 Contract Creation / Authoring E.2 Establishment of contract terms and SLAs inclusive of right to audit E.3 Contract Review E.4 Contract Negotiations E.5 Contract Approval E.6 Contract Execution	F.1 Supplier On-boarding F.2 Transition of services to Supplier F.3 Document exit strategy F.4 Establish monitoring cycle	G.1 Risk management assessment and monitoring G.2 Service (or Obligation) management G.3 Contract risk review G.4 Issue management G.5 Risk treatment G.6 Action planning G.7 Monitoring of issue remediation and risk treatment G.8 Contract Amendments G.9 Audit & Reporting G.10 Control Renewal	H.1 Execute exit strategy H.2 Exposure/Risk assessment H.3 Return of data/equipment H.4 Legal confirmation of data destruction
Key Stakeholders	• Business Unit • Sourcing • TPRM • Finance	• Sourcing • Business Unit	• Sourcing • Business Unit • TPRM	• Sourcing • TPRM • Business Unit	• Contracting • Sourcing • Business Unit • Legal • TPRM	• Business Unit • Sourcing • TPRM (informed on vendor onboarding)	• Business Unit • TPRM	• Business Unit • TPRM • Sourcing • Contracting

Blue Text = Suggested Engagement Points for TPRM

Organizational model

Sourcing

Leading financial services organizations are aligning their vendor management operating model with enterprise-level strategy and culture. The center-led model is frequently deployed.



Business units or regions maintain their own procurement functions for most categories with some coordination and communication across units

Central procurement group defines strategy, tools, and processes and coordinates across BUs or regions by leveraging procurement councils; transactions and some categories managed at the BU or region level

Central procurement organization performs most functions–sourcing, SRM, category management, and transactions

Monitoring

Relationship, service and risk management

Effective relationship management accounts for the overall relationship across the enterprise and is inclusive of performance, compliance and risk management activities.

Vendor Relationship Management

Vendor relationship management refers to the process of managing the vendor relationship as a whole inclusive of all services provided to the company by the vendor across the enterprise. Effective relationship management accounts for any changes in the business or operating environment that may effect the relationship (i.e. market conditions, acquisitions, divestitures, personnel change or turnover) as well as the output of service, compliance and risk management activities.

Service Management

Service Management is commonly managed by the contract or relationship owner within the line of business. Common areas of assessment include:

- Client Satisfaction
- Contract Compliance
- Service Level Management
- Cost Management
- Exit Strategy

Regulatory Compliance

Regulatory Compliance overlaps with Service Management and Risk management expectations, but are also assessed qualitatively to effectively manage conduct risk. Common areas of assessment include:

- Policy File Reviews
- Call Monitoring
- Analytics

Risk Management

Risk Management may be managed by the risk organization, specific subject matter functions (i.e. Information Security), or the lines of business. Common areas of assessment include:

- Information Security
- Business Continuity
- Location/Country
- Financial Viability
- Business Reputational Risk

Risk dimensions

Common third party risks

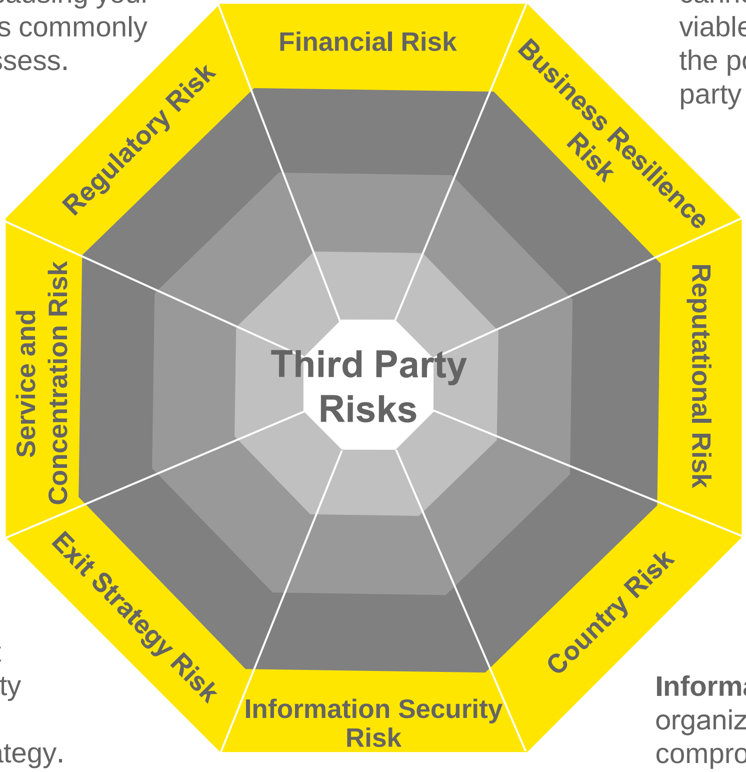
There are numerous aspects of risk to account for when making the decision to utilize a third party to perform a service for your company.

Regulatory Risk is the risk that a third party fails to comply with a required regulation, thus causing your company to be out of compliance. This is commonly the most complex risk to quantify and assess.

Service Risk is the risk that a third party fails to meet your needs as a company from a service delivery perspective. Common metrics include SLAs, scalability and overall performance reviews.

Concentration Risk is the risk created by a lack of diversification within an organizations third party base.

Exit Strategy Risk is the risk that the business would suffer a negative impact should the relationship with the third party need to be exited from and commonly internally controlled via a formal exit strategy.



Financial Risk is the risk that the third party cannot continue to operate as a financially viable entity. This may also be interpreted as the potential for financial loss due to third party failure or non-performance.

Business Resilience Risk assesses the risk of third party failure on the continuation of business as usual for the organization.

Reputational Risk assesses the impact to the organizations reputation should an event occur at your third party.

Country Risk assesses the risk of doing business in a specific country and includes legal/regulatory, geo-political and social-economic considerations.

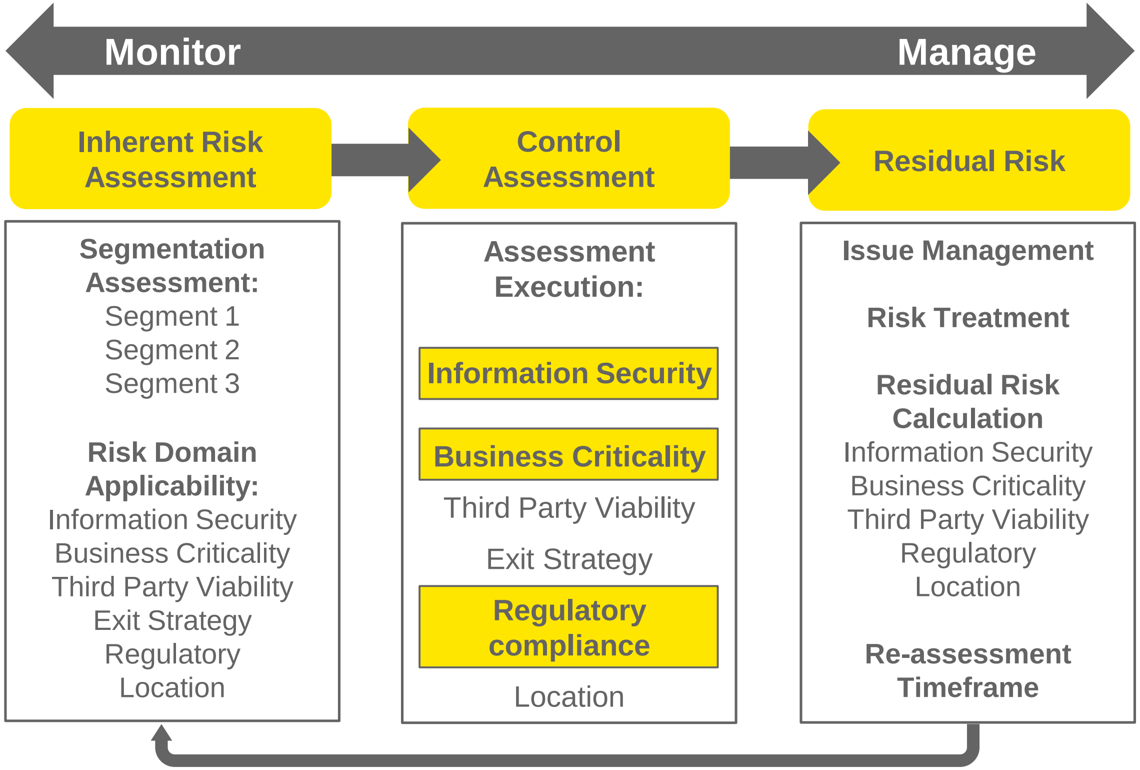
Information Security Risk is the risk that an organization’s data is lost or security is compromised.

Assess risk(s) at the third party level for Concentration, Financial, Reputational, etc. risk, where appropriate.

Risk models

Inherent, controls and residual risk

Risk models allow for the qualitative and quantitative assessment of risk; enabling an organization to focus efforts on monitoring higher levels of inherent risk and manage higher levels of residual risk.



Monitor

Manage

Inherent Risk Assessment

Segmentation Assessment:
Segment 1
Segment 2
Segment 3

Risk Domain Applicability:
Information Security
Business Criticality
Third Party Viability
Exit Strategy
Regulatory
Location

Control Assessment

Assessment Execution:

Information Security

Business Criticality

Third Party Viability

Exit Strategy

Regulatory compliance

Location

Residual Risk

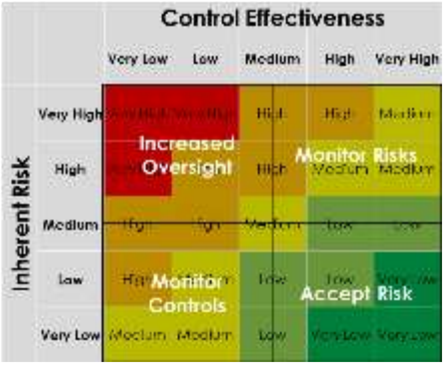
Issue Management

Risk Treatment

Residual Risk Calculation
Information Security
Business Criticality
Third Party Viability
Regulatory
Location

Re-assessment Timeframe

Mature organizations are moving towards real time management / monitoring of risks *while leveraging residual risk or control effectiveness ratings to determine frequency of reviews as opposed to inherent risk and transactional events (e.g. contracting, invoicing, etc.).*



Control Effectiveness

Inherent Risk

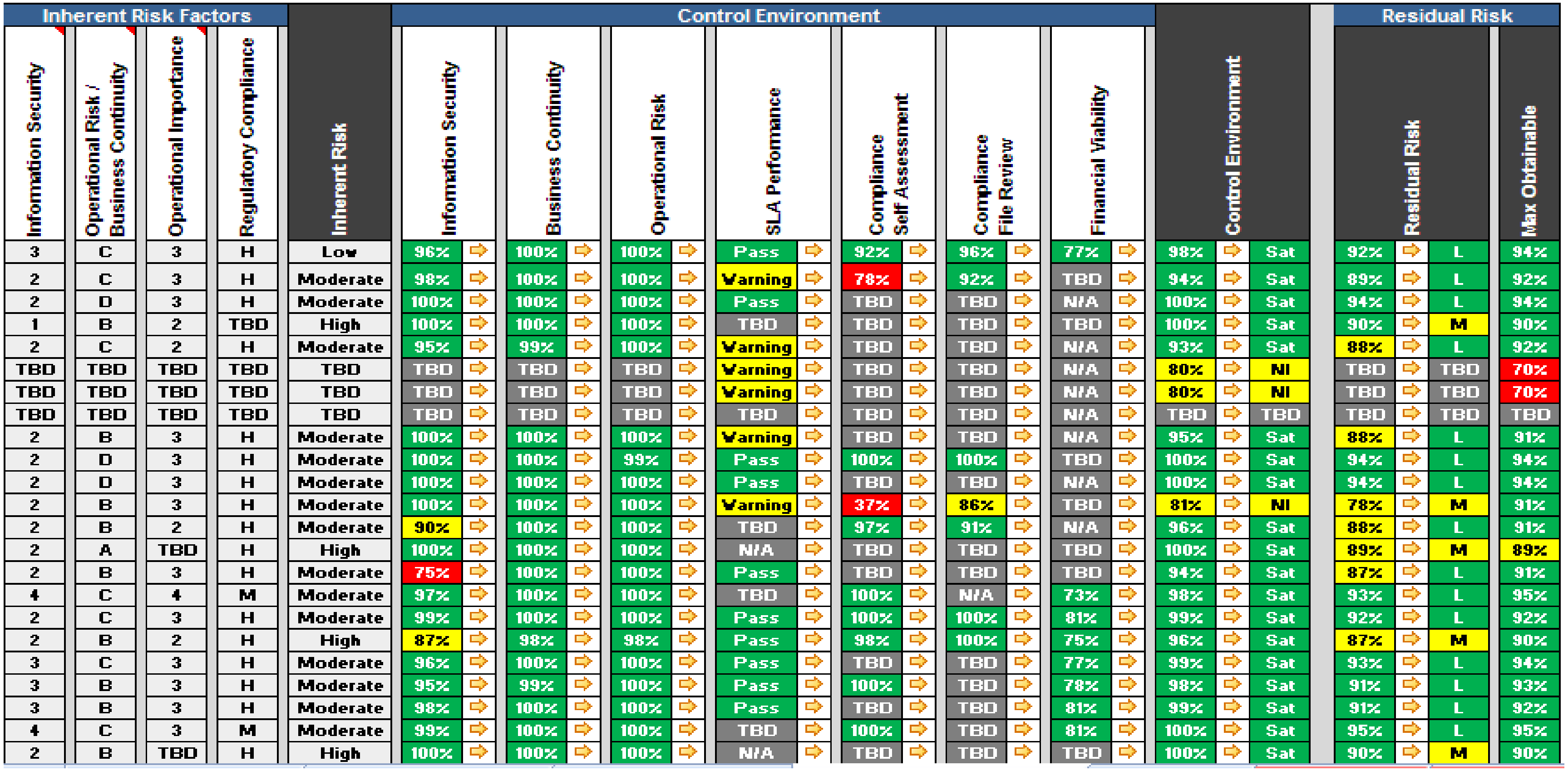
	Very Low	Low	Medium	High	Very High
Very High	Very High	Very High	High	High	Medium
High	[illegible]	[illegible]	High	Medium	Medium
Medium	High	High	Medium	Low	Low
Low	High	[illegible]	Low	Low	Very Low
Very Low	Medium	Medium	Low	Very Low	Very Low

71% of organizations said they conduct regulatory compliance reviews pre-contract, up from 47% in 2014
– 2016 TPRM survey

Reporting & metrics

Inherent vs. residual

Leading TPRM organizations have begun to look at the third party relationship holistically inclusive of risk, compliance and performance factors.



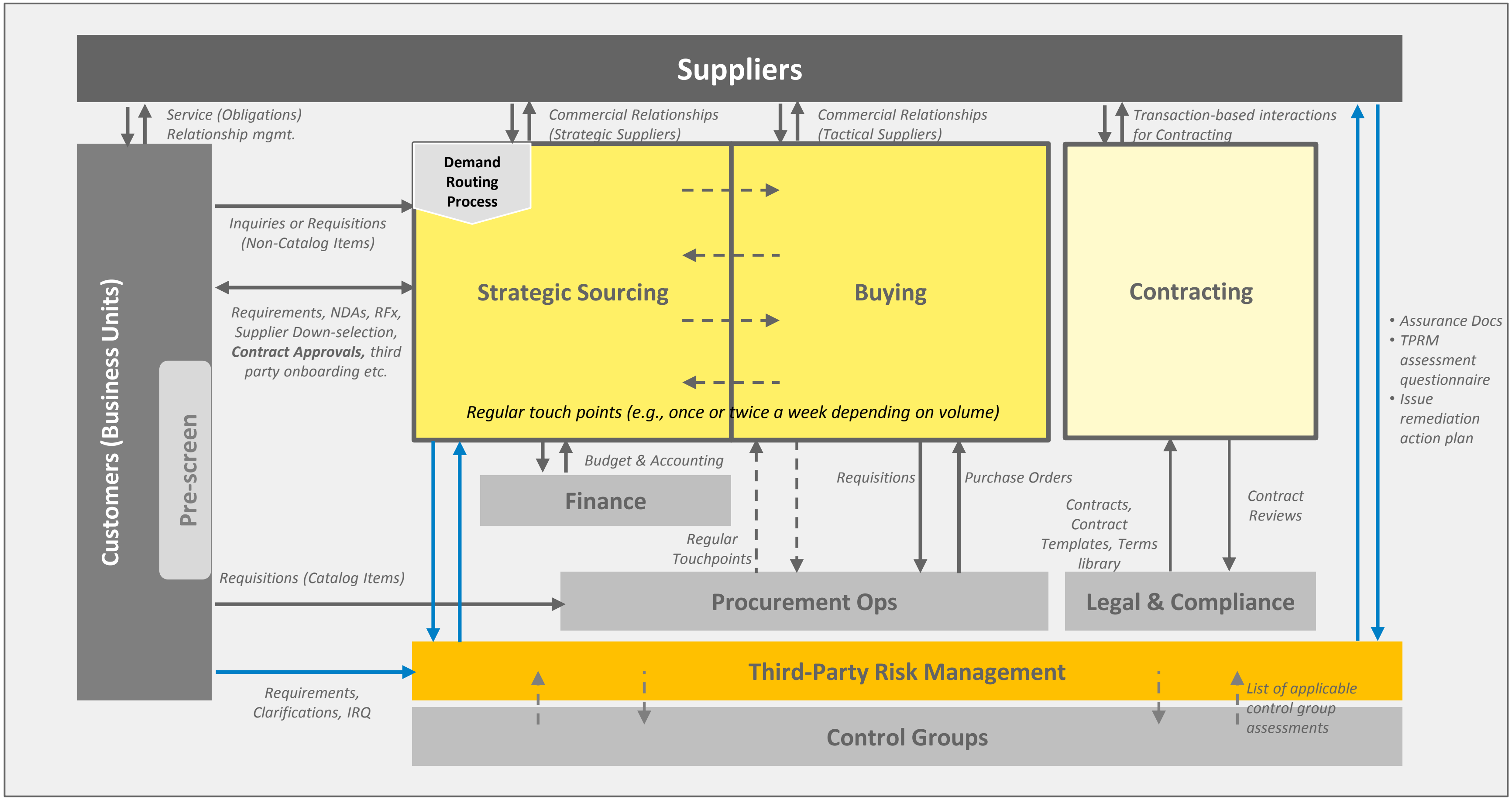
Inherent Risk Factors					Control Environment									Residual Risk		
Information Security	Operational Risk / Business Continuity	Operational Importance	Regulatory Compliance	Inherent Risk	Information Security	Business Continuity	Operational Risk	SLA Performance	Compliance Self Assessment	Compliance File Review	Financial Viability	Control Environment		Residual Risk		Max Obtainable
3	C	3	H	Low	96% ⇨	100% ⇨	100% ⇨	Pass ⇨	92% ⇨	96% ⇨	77% ⇨	98% ⇨	Sat	92% ⇨	L	94%
2	C	3	H	Moderate	98% ⇨	100% ⇨	100% ⇨	Warning ⇨	78% ⇨	92% ⇨	TBD ⇨	94% ⇨	Sat	89% ⇨	L	92%
2	D	3	H	Moderate	100% ⇨	100% ⇨	100% ⇨	Pass ⇨	TBD ⇨	TBD ⇨	N/A ⇨	100% ⇨	Sat	94% ⇨	L	94%
1	B	2	TBD	High	100% ⇨	100% ⇨	100% ⇨	TBD ⇨	TBD ⇨	TBD ⇨	TBD ⇨	100% ⇨	Sat	90% ⇨	M	90%
2	C	2	H	Moderate	95% ⇨	99% ⇨	100% ⇨	Warning ⇨	TBD ⇨	TBD ⇨	N/A ⇨	93% ⇨	Sat	88% ⇨	L	92%
TBD	TBD	TBD	TBD	TBD	TBD ⇨	TBD ⇨	TBD ⇨	Warning ⇨	TBD ⇨	TBD ⇨	N/A ⇨	80% ⇨	NI	TBD ⇨	TBD	70%
TBD	TBD	TBD	TBD	TBD	TBD ⇨	TBD ⇨	TBD ⇨	Warning ⇨	TBD ⇨	TBD ⇨	N/A ⇨	80% ⇨	NI	TBD ⇨	TBD	70%
TBD	TBD	TBD	TBD	TBD	TBD ⇨	TBD ⇨	TBD ⇨	TBD ⇨	TBD ⇨	TBD ⇨	N/A ⇨	TBD ⇨	TBD	TBD ⇨	TBD	TBD
2	B	3	H	Moderate	100% ⇨	100% ⇨	100% ⇨	Warning ⇨	TBD ⇨	TBD ⇨	N/A ⇨	95% ⇨	Sat	88% ⇨	L	91%
2	D	3	H	Moderate	100% ⇨	100% ⇨	99% ⇨	Pass ⇨	100% ⇨	100% ⇨	TBD ⇨	100% ⇨	Sat	94% ⇨	L	94%
2	D	3	H	Moderate	100% ⇨	100% ⇨	100% ⇨	Pass ⇨	TBD ⇨	TBD ⇨	N/A ⇨	100% ⇨	Sat	94% ⇨	L	94%
2	B	3	H	Moderate	100% ⇨	100% ⇨	100% ⇨	Warning ⇨	37% ⇨	86% ⇨	TBD ⇨	81% ⇨	NI	78% ⇨	M	91%
2	B	2	H	Moderate	90% ⇨	100% ⇨	100% ⇨	TBD ⇨	97% ⇨	91% ⇨	N/A ⇨	96% ⇨	Sat	88% ⇨	L	91%
2	A	TBD	H	High	100% ⇨	100% ⇨	100% ⇨	N/A ⇨	TBD ⇨	TBD ⇨	TBD ⇨	100% ⇨	Sat	89% ⇨	M	89%
2	B	3	H	Moderate	75% ⇨	100% ⇨	100% ⇨	Pass ⇨	TBD ⇨	TBD ⇨	TBD ⇨	94% ⇨	Sat	87% ⇨	L	91%
4	C	4	M	Moderate	97% ⇨	100% ⇨	100% ⇨	TBD ⇨	100% ⇨	N/A ⇨	73% ⇨	98% ⇨	Sat	93% ⇨	L	95%
2	C	3	H	Moderate	99% ⇨	100% ⇨	100% ⇨	Pass ⇨	100% ⇨	100% ⇨	81% ⇨	99% ⇨	Sat	92% ⇨	L	92%
2	B	2	H	High	87% ⇨	98% ⇨	98% ⇨	Pass ⇨	98% ⇨	100% ⇨	75% ⇨	96% ⇨	Sat	87% ⇨	M	90%
3	C	3	H	Moderate	96% ⇨	100% ⇨	100% ⇨	Pass ⇨	TBD ⇨	TBD ⇨	77% ⇨	99% ⇨	Sat	93% ⇨	L	94%
3	B	3	H	Moderate	95% ⇨	99% ⇨	100% ⇨	Pass ⇨	100% ⇨	TBD ⇨	78% ⇨	98% ⇨	Sat	91% ⇨	L	93%
3	B	3	H	Moderate	98% ⇨	100% ⇨	100% ⇨	Pass ⇨	TBD ⇨	TBD ⇨	81% ⇨	99% ⇨	Sat	91% ⇨	L	92%
4	C	3	M	Moderate	99% ⇨	100% ⇨	100% ⇨	TBD ⇨	100% ⇨	TBD ⇨	81% ⇨	100% ⇨	Sat	95% ⇨	L	95%
2	B	TBD	H	High	100% ⇨	100% ⇨	100% ⇨	N/A ⇨	TBD ⇨	TBD ⇨	TBD ⇨	100% ⇨	Sat	90% ⇨	M	90%

49% of organization require one week or more to pull reports on third parties using specific data.
– 2016 TPRM survey

Technology & data

Functional architecture

Functional integration of process is the first step in defining necessary technology enablement as multiple systematic solutions may be selected for portion(s) of the end-to-end function.



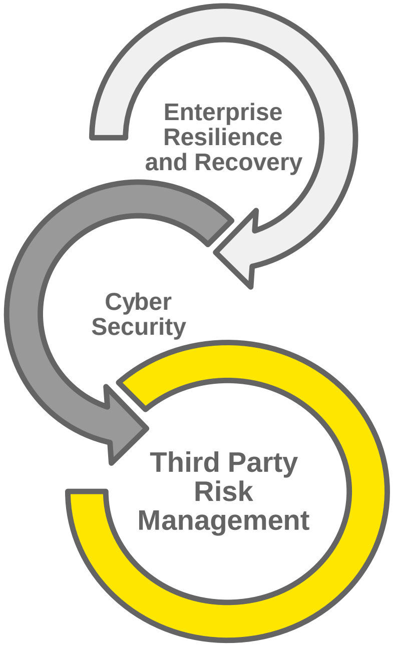
Suppliers
Service (Obligations)
Relationship mgmt.
Commercial Relationships
(Strategic Suppliers)
Commercial Relationships
(Tactical Suppliers)
Transaction-based interactions
for Contracting
Customers (Business Units)
Pre-screen
Demand Routing Process
Inquiries or Requisitions
(Non-Catalog Items)
Requirements, NDAs, RFx, Supplier Down-selection, Contract Approvals, third party onboarding etc.
Strategic Sourcing
Buying
Contracting
Regular touch points (e.g., once or twice a week depending on volume)
Assurance Docs
TPRM assessment questionnaire
Issue remediation action plan
Budget & Accounting
Finance
Requisitions
Purchase Orders
Contracts, Contract Templates, Terms library
Contract Reviews
Regular Touchpoints
Requisitions (Catalog Items)
Procurement Ops
Legal & Compliance
Third-Party Risk Management
Requirements, Clarifications, IRQ
List of applicable control group assessments
Control Groups

Cybersecurity and Enterprise Resilience trends

Cybersecurity and Enterprise Resilience

Overview and third party risks

Heightened regulatory / industry focus on Information (IT) / Cyber Security and Enterprise Resilience and Recovery in connection to third parties continues to drive the need for cross-functional integration.


Enterprise Resilience and Recovery
Cyber Security
Third Party Risk Management

Enterprise Resilience and Recovery

- ► Focuses on protecting the enterprise and business operations. Third-party breaches and outages continue to impact the marketplace.

Cyber Security

- ► Concentrates on shielding a company's cyber / IT vulnerabilities. Any single entity, including third parties, can be a potential threat entry point.

Third Party Risk Management (TPRM)

- ► Focuses on protecting the enterprise from potential threats / risks related to leveraging third parties to provide goods and / or services.
- ► Holistic approach to understanding, managing and mitigating third party risks across risk dimensions (e.g. Cyber, Resilience, Compliance, etc.) is key to meeting regulatory and industry expectations.

Cyber / IT Security and Enterprise Resilience third party risk assessments topped the list of focus areas of recent regulatory reviews, alongside enterprise-critical third parties, oversight and governance.
– 2016 TPRM survey

Enterprise Resilience and Recovery

Overview and third party risks

Focused on protecting the enterprise and business operations from internal and external incidents that could impact the organizations' ability to conduct business, meet regulatory expectations, react in a resilient manner and recover from a **third party outage or incident**.

Key issues / drivers

- Regulatory community is increasing scrutiny / pressure on FSO environments to enable operations for 30+ business days in an outage.
- Need to understand potential failure points and weaknesses in supporting business applications / technology landscape aligned to business recovery targets and sequencing.
- **Third-party breaches and outages continue to impact the marketplace** and expand the boundaries of the threat environment outside the walls of the bank itself.

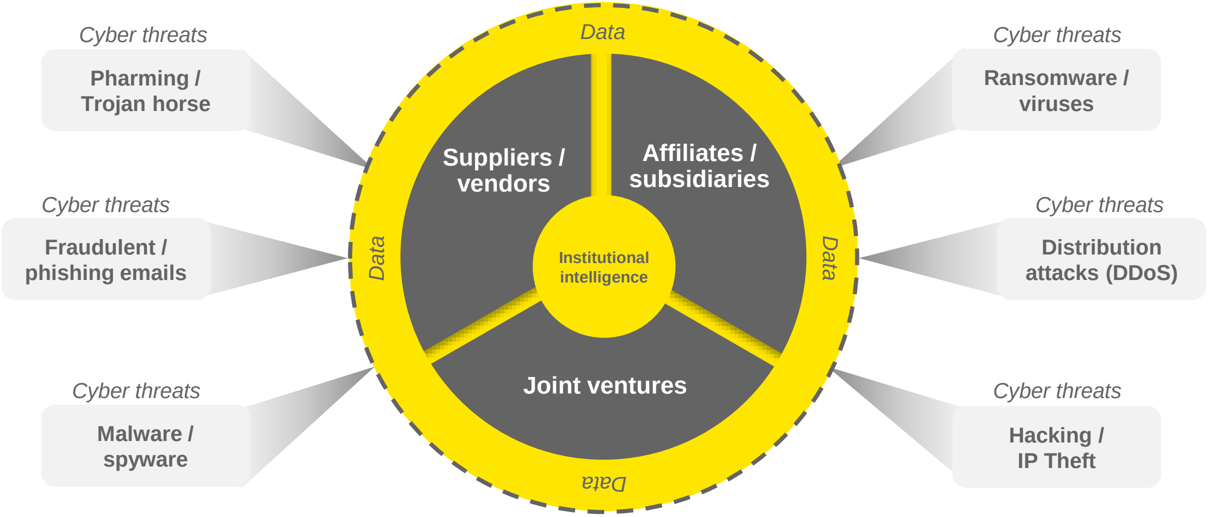
Key maturity indicators re:Third parties

- Does the organization have an understanding of "all" third-parties supporting the enterprise?
- Is there a clearly defined expectation for how to vet, select, engage and manage third-parties?
- Is the business (e.g. business lines, board, sr. leadership, etc.) aware of third-party risks and third-parties considered critical to the organization?
- Has technology been integrated across the end-to-end third-party management value chain?

Cybersecurity and Third Party Risk

Multiple threat entry points

Traditionally, organizations thought of Cybersecurity as a function to protect their own vulnerabilities, stopping short of considering the data third parties access. Any single entity can be a potential threat entry point – causing a ripple effect across the enterprise.



Operating in a digital world invites new challenges and threats…

- ► Smart devices / services connect more networks; increasing attack surface area.
- ► Social media is ‘always on’ and information widely shared, without a full appreciation of privacy and security.
- ► Customers’ demand quicker updates and regulators increase security control focus.
- ► Information is increasingly stored in the cloud or with third parties, resulting in less control, increased risk and a more complex cyber ecosystem.

High-profile breaches:

- ► ***2013 Target breach involved*** *HVAC company with access to internal systems. Estimated financial impact of >$250m.*
- ► ***2013 and 2015 T-Mobile customer data breaches*** *involved Experian lacking adequate controls to protect consumer information of 15 million customers.*

Protecting the enterprise – TPRM

Protecting the enterprise

Third Party Risk Management (TPRM) approach – the three A’s

We suggest that organizations adopt a 3-stage improvement process to get ahead of third party risks across the enterprise – integrating Resilience / Recovery and Cyber / IT Security.

3) Anticipate – proactive approach

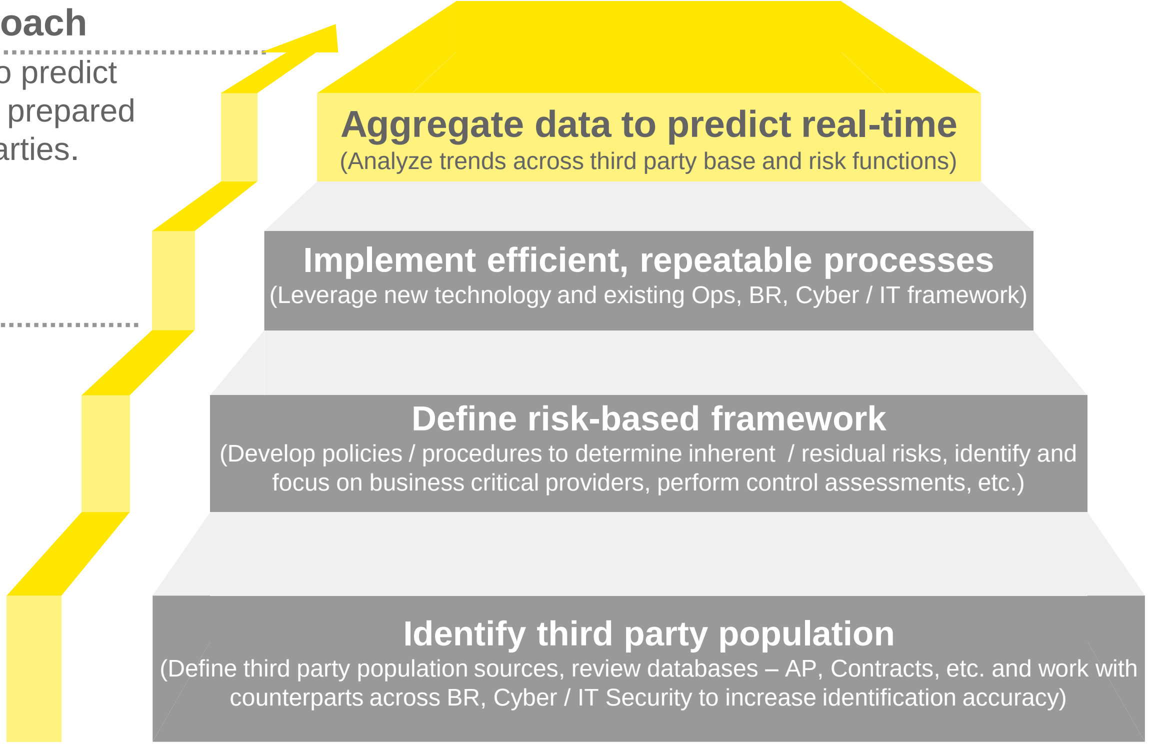
Organizations need to make efforts to predict what is coming so they can be better prepared for impacts on them and their third parties.

2) Adapt – build a better baseline

Organizations are constantly changing and cyber threats / resiliency issues are evolving: third party risk programs need to adapt to changing requirements by building a better baseline.

1) Activate – strong foundation

Organizations need to establish and improve the solid foundations of their third party risk program.



Aggregate data to predict real-time
(Analyze trends across third party base and risk functions)

Implement efficient, repeatable processes
(Leverage new technology and existing Ops, BR, Cyber / IT framework)

Define risk-based framework
(Develop policies / procedures to determine inherent / residual risks, identify and focus on business critical providers, perform control assessments, etc.)

Identify third party population
(Define third party population sources, review databases – AP, Contracts, etc. and work with counterparts across BR, Cyber / IT Security to increase identification accuracy)

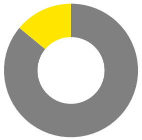
Two greatest challenges facing clients are Technology and Knowledge across business functions
– 2016 TPRM survey

Protecting the enterprise

*TPRM approach and **Cyber Security** – the three A's defined*

Activate
– strong foundation

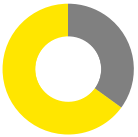
- **Set the expectation**
  - Review / update security policies, standards and procedures – including internal data classifications.
- **Create your ecosystem inventory**
  - Identify data classification / flows and who accesses (e.g. third parties).
  - Create risk tiers and classify third parties based on the risk posed to your organization.
- **Assess IT security controls**
  - Critical suppliers should safeguard your data within the same risk thresholds you maintain.



86% of organizations use between 3 and 5 segments / tiers of third parties*

Adapt
– build a better baseline

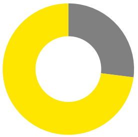
- **Know yourself**
  - Define TPRM RACI.
- **Enhance assessment criteria**
  - Just as threats evolve for your systems, they evolve for your third party's systems.
  - Use risk based approach to determine assessment type and depth (e.g. onsite vs remote).
- **Develop metrics**
  - Report on critical third party's performance and security to senior management and board.
  - Draw the line – how much risk is too much?



31% of organizations report third parties with breaches to the board*

Anticipate
– proactive approach

- **Know yourself and third parties**
  - Cyber threats are evolving constantly; in-direct threats may impact your third parties.
- **Define response to third party breaches** and understand how they'll involve you in incident response.
- **Volume of devices with access to your data will only increase.**
  - Assess third parties based on critical threats as they emerge.
- **Examine risk posed by 4th parties.**
  - Assess third party's TPRM program.
  - Assess the fourth party directly[1].



27% of organizations do not report on third parties related to emerging risk*

** - Results based on 2016 EY TPRM Survey; [1] – if contractually permissible*

Protecting the enterprise

TPRM approach and ***Enterprise Resilience*** *– the three A's defined*

Activate
– strong foundation

- **Identify framework**
  - Review / update resilience / recovery policies, standards and procedures.
- **Understand critical inventory**
  - Determine criticality of processes and third parties providing services related to those processes.
  - Create risk tiers and classify third parties based on the risk posed to your organization – incorporating criticality of processes supported by the third party.
- **Assess Enterprise Resilience controls**
  - Critical third parties should be held to the same resilience thresholds (e.g. 1 hr, 24 hrs, etc.) you maintain for the services they provide to support your processes.

Adapt
– build a better baseline

- **Enhance risk inventory criteria**
  - Enhance procedures to determine criticality of processes and related third parties.
  - Use a Business Continuity Analysis Template (BCAT) to determine if the process / service is:
    - Systemic
    - Required / obligatory
    - Business critical
    - Business important
- **Apply risk based approach to determine assessment type and depth (e.g. onsite vs. remote).**
- **Develop metrics**
  - Report on Business Critical third party's performance and resilience to senior management and board.
  - Develop a risk-appetite for your critical processes / third parties.

Anticipate
– proactive approach

- **Potential impacts from your third parties resiliency change constantly;** in-direct threats may impact your third parties and the critical services they provide.
- **Define response to Business Critical third party failures** and understand how they'll involve you in incident response.
- **Examine risk posed by 4th parties.**
  - Assess third party's TPRM program; specifically their focus on resilience of their third parties.
  - Assess the fourth party directly, if contractually permissible.
- **Increase governance and oversight of third parties providing Business Critical services** – understand their blind-spots / issues.

Enterprise Resiliency of your third parties continues to be a regulatory focus, driving the need for a proactive approach to manage / mitigate risk of potential third party failures.

Appendix

EY Third Party Risk Management survey

Market trends and survey details

In the winter of 2015, Ernst & Young surveyed 49 global institutions with a vendor risk function in the retail and commercial banking, investment banking, insurance and asset management sectors.

Key findings from Ernst & Young’s 2016 Supplier Risk Management Survey	
Third-Party Population	• 39% of organizations communicated that less than 25% of the organizations third-party population are in scope for the organization’s risk management program, which is a significant increase from the 10-15% of the population that has been a staple data point over the last 3 years. ➢ 39% said **all** which is a strong indication that organizations are continuing to revisit the third party population to re-profile. • **86% of organizations use between 3 and 5 segments/tiers** • **83% of organizations have a critical third-party list that is 80 third-parties or less; this has been observed regardless of the size of the organization or third-party population.** • 85% of organizations indicated that less than 25% of their risk assessed population posed consumer protection risk to the organization.
Operating Model	• **41% of organizations indicated that primary ownership of their third-party risk management function is within Procurement, up from 26% the year before; 26% house this within a risk function (enterprise or operational risk).** • Only 14% of organizations indicated that their program is fully decentralized, showing a strong push towards hybrid (41%) and centralized (45%) models. • 53% of organizations indicated that primary ownership of inherent risk assessments are owned within the Line of Business (up from 32% last year), however we did see strong coordination with risk groups to support in conducting this activity. • In looking at third-party entity level assessments such as AML, Sanctions, Reputation and Anti-bribery/corruption we see a wide distribution between the Line of Business, TPRM and Compliance. Ownership by Compliance for a first line activity could cause concern relative to the 3 Lines of Defense model. • **71% of organizations were either neutral or believed they faced challenges with business unit support in the execution of program requirements showing a continued challenge in business risk culture for third party management.**

EY Third Party Risk Management survey

Market trends and survey details (cont…)

Key findings from Ernst & Young's 2016 Supplier Risk Management Survey	
Reporting	• 31% of organizations noted that they communicate third-party data breaches to the board; 71% report this to Senior Management. • **43% of organizations report critical third-parties to the board level up from 26% last year.**
Assessment Framework	• 80% of organizations indicated they spend two or less days on-site in conducting Information Security and Business Resilience reviews. Even more interesting was 74% spend a day or less onsite when conducting regulatory compliance reviews. • Adoption of the Shared Assessments program as a framework went up from 24% to 28% but still trails proprietary frameworks which are in use at 46% of organizations. We did see a strong correlation between those who use Shared Assessments and accept a SIG or an AUP to reduce or replace assessment efforts. • **71% of organizations feel the SSAE16 SOC 2 is useful in reducing or removing the need to perform a review on a third party, up from 52% last year.** • 71% of organizations indicated they conducted compliance control assessments pre-contract up from last year's 58%. • The top three most important considerations when assessing third-party controls are protecting customer information (84%), complying with regulations (63%), and protecting reputation and brand (43%).
Fourth Parties	• **78% of organizations indicated that they identify fourth parties within the contracting phase; 75% also indicated they identify this within control assessment activities.** • In evaluating fourth parties, we saw an increase from 36% to 75% of organizations that rely on the third party's ability to manage the third party (this would include evaluating the third-parties' TPRM program).

EY Third Party Risk Management survey

Market trends and survey details (cont…)

Key findings from Ernst & Young's 2016 Supplier Risk Management Survey	
Termination / Exit Strategy	• 74% of organizations place responsibility for the creation of exit strategies within the line of business; Almost half of all organizations surveyed indicated they document this prior to contract execution. • 8% of organizations do not have exit strategies as a formal part of their program, however this was highly concentrated in organizations with less than 25k employees.
Oversight and Governance + Quality Assurance / Quality Control	• All of the organizations surveyed consider testing of internal compliance with program requirements, development of program policy and procedures and reporting to senior management as a core part of their Oversight and Governance program responsibilities. • The ability to pull reporting within these functions, however, seemed to be a challenge with 49% of organizations indicating it would take a week or more to pull a report of suppliers with specific criteria and 73% indicating it would take a week or more to forecast contract expiration, showing a strong data disconnect between Procurement and TPRM systems. • Only 26% of organizations indicated they could run on-demand risk scorecards. • We continue to see minimal action around termination of suppliers for breach or failure across the marketplace.
Regulatory Exams	• **In line with last year's results, we saw the top 3 focus points (in order) for regulatory reviews to be Enterprise critical third-parties, Oversight and governance, and Information Security/Business Resilience assessments.** • We did however, see a much wider tail on focal points across the full data set indicating that regulators are continuing to go wide as well as deep in their oversight activities.

For any questions related to

Third Party Risk Management services or

EY's 2017 Third-Party Risk Management Survey

Please contact :

Harald deRopp, Executive Director

EY Advisory and Consulting Co., Ltd.

Mobile: **080-2083-0056**

Email: **harald.deropp@jp.ey.com:**

EY | Assurance | Tax | Transactions | Advisory

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com