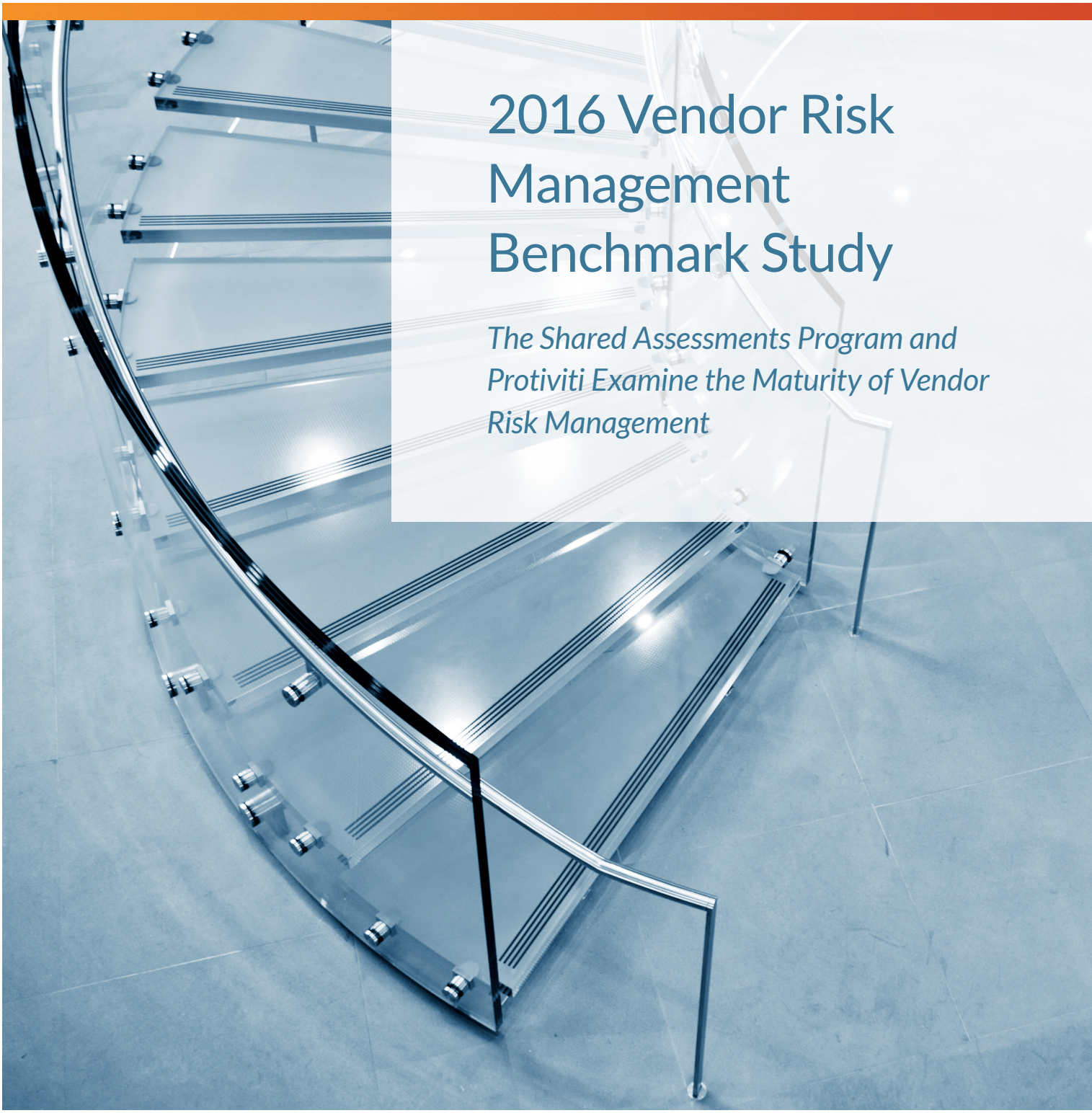
SHARED ASSESSMENTS

protiviti®

Face the Future with Confidence



2016 Vendor Risk Management Benchmark Study

The Shared Assessments Program and Protiviti Examine the Maturity of Vendor Risk Management

Executive Summary

Companies appear to have reached a positive turning point with regard to managing their vendor risks. The results of the latest **Vendor Risk Management Benchmark Study** indicate that:

- Organizations in all industries are increasing their focus on managing vendor and third party risks.
- Levels of maturity in different vendor risk management components have noticeably improved.

This is the third year that the Shared Assessments Program and Protiviti have partnered on this research, which is based on the comprehensive **Vendor Risk Management Maturity Model (VRMMM)** developed by the Shared Assessments Program. Shared Assessments is the trusted source in third party risk management and is a collaborative consortium of leading industry professionals from financial institutions, assessment firms, technology and GRC solution providers, insurance companies, brokerages, healthcare organizations, retail firms, academia, and telecommunications companies – dedicated to assisting organizations by helping them to understand, manage and monitor vendor risk effectively and efficiently.

Positive momentum is portrayed in this year's survey, which is a significant change over prior years. In 2015, respondents rated their overall maturity across the eight vendor risk management categories to be virtually identical to those reported in 2014. In financial services, the improvement seen this year could be motivated, in part, by significantly increasing regulatory scrutiny, especially in areas related to cybersecurity.

For example, in June 2015, the Federal Financial Institutions Examination Council (FFIEC) published its Cybersecurity Assessment Tool, which provided financial institutions with a methodology for assessing their own cybersecurity capabilities in terms of their unique risk profiles.[1] In November 2015, based on recent guidance, some regulators began using an updated *FFIEC Information Technology Examination Handbook* to examine the cybersecurity and third party risk management proficiencies of financial institutions.[2] Among the items that examiners now review regularly at the board of director level is an evaluation of whether a board appropriately oversees the risks involved in its outsourced relationships.[3] That's just one of many third party risk–related procedures that will increasingly be a focus of periodic regulator examinations.

[1] *FFIEC Cybersecurity Assessment Tool*, June 2015, www.occ.gov/news-issuances/bulletins/2015/bulletin-2015-31.html; www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf.

[2] *FFIEC Information Technology Examination Handbook:* Management Booklet, Appendix A, "Examination Procedures," Federal Financial Institutions Examination Council, November 2015, http://ithandbook.ffiec.gov/it-booklets/management/appendix-a-examination-procedures.aspx.

[3] Ibid.

Headlines regarding a series of healthcare-related data breaches may also have contributed to improvements in the third party risk management maturity of firms in that sector. In 2015, there were a record-breaking number of healthcare-related breaches, with more than 111 million records compromised in just the 10 largest incidents.[4] In one serious breach, more than 79 million records were compromised. In this particular instance, an external review two years earlier found vulnerabilities that had the potential to provide a "gateway for malicious virus and hacking activity that could lead to data breaches."[5] Events such as this one seemed to be a wake-up call to healthcare firms in general.

The results from this year's study also show a direct correlation between having the appropriate "tone at the top" and higher levels of third party risk management maturity. The study examined board engagement with cybersecurity risks relating to internal operations and vendor operations. Companies reporting low levels of board engagement with vendor-related cybersecurity risks had an average maturity level of 2.2 (slightly above the "Determine roadmap" maturity level), while companies with highly engaged boards boasted maturity levels, on average, of 3.6 (midway between the "Fully defined" and "Fully implemented" maturity levels on our 5-point scale). When vendor risk management maturity was assessed against low and high board engagement with cybersecurity risk issues inside the organization, there was a similar disparity in the results – 2.0 for firms with low engagement but 3.4 for companies with high levels of board engagement.

Our Key Findings

01 **Vendor risk management is garnering more attention and maturity levels are on the rise** – Compared to last year's survey, this year's results show significant improvement in vendor risk management capabilities, suggesting this has become more of a "front burner" issue for organizations. As a consequence, the maturity gap between financial services and organizations in other verticals is shrinking.

02 **Many boards have a high level of engagement regarding cybersecurity risks to the business, but less so for vendors** – There is a noticeable difference in the "high" engagement levels among board members with regard to cybersecurity risks to the business compared with those risks to the organization's vendors.

03 **Board engagement in cybersecurity risk is a key differentiator** – For organizations in which boards have high engagement levels in cybersecurity risks, vendor risk management maturity levels are noticeably higher.

04 **Metrics matter more** – Maturity levels have jumped significantly in a number of vendor risk components that relate to vendor assessments and performance metrics, including calculating and distributing vendor assessment metrics, and implementing metrics and reporting for compliance to required training and awareness of vendor risk policies.

05 **Despite higher maturity levels in most vendor risk components, there remain numerous areas for improvement** – While more areas are reported to be at or near the "Fully defined and established" level, few are close to the "Fully implemented and operational" or "Continuous improvement – benchmarking, moving to best practices" levels.

[4] "Data Breaches In Healthcare Totaled Over 112 Million Records In 2015," Dan Munro, *Forbes*, December 31, 2015. www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#670f45607fd5.

[5] "Anthem Was Warned About Hacking Weakness – US agency audited health insurer two years before data for 80m stolen," Gina Chon, Kara Scannell, *Financial Times*, March 2, 2015. www.ft.com/cms/s/2/3cb94550-bd26-11e4-b523-00144feab7de.html?siteedition=intl#axzz4Jc3eP7Br.

• • • *Vendor Risk Management – Overall Maturity by Area*

Category	2016 Index	2015 Index	2014 Index
Program Governance	3.0	2.8	2.9
Policies, Standards and Procedures	3.1	2.9	2.9
Contracts	3.1	2.9	3.0
Vendor Risk Identification and Analysis	2.9	2.7	2.7
Skills and Expertise	2.7	2.3	2.3
Communication and Information Sharing	2.9	2.5	2.6
Tools, Measurement and Analysis	2.8	2.4	2.4
Monitoring and Review	3.0	2.8	2.9

Vendor Risk Management Maturity Levels

5 = Continuous improvement – benchmarking, moving to best practices

4 = Fully implemented and operational

3 = Fully defined and established

2 = Determine roadmap to achieve goals

1 = Initial visioning

0 = Do not perform

"Risk managers at all levels, including the C-suite and board of directors, understand that the maturity of our risk management programs has a profound effect on our organization. This study documents in detail what many have believed to be true – that for organizations in which boards have high engagement in and knowledge of critical risk issues, vendor risk management maturity levels are noticeably higher."

– Cathy Allen, CEO, The Santa Fe Group

Assessing Results by Respondent Role

To identify notable trends in the data, we also tabulated our 2016, 2015 and 2014 survey results by the role of the respondent. There is an overall trend over the past three years that the higher the level of respondent in the organization, the lower the assessed score is for a vendor risk component or category. Notably, this year we do see a shift that suggests midlevel managers are detecting a higher level of maturity improvement than either respondent cohort above or below. As with the overall response, with few exceptions, average maturity levels are higher this year compared to 2015.

	C-Level			VP/Director Level			Manager Level		
Vendor Risk Management Category	2016	2015	2014	2016	2015	2014	2016	2015	2014
Program Governance	2.8	2.9	2.9	3.2	2.8	3.2	3.1	3.2	3.1
Policies, Standards and Procedures	2.8	2.8	2.4	3.2	2.8	2.9	3.2	3.0	3.0
Contracts	3.0	2.7	2.6	3.3	2.8	3.0	3.2	3.0	3.0
Vendor Risk Identification and Analysis	2.8	2.4	2.2	3.0	2.7	2.7	3.0	2.8	2.8
Skills and Expertise	2.5	1.9	1.8	2.8	2.1	2.3	2.7	2.5	2.3
Communication and Information Sharing	2.7	2.2	2.1	3.0	2.3	2.5	3.0	2.7	2.5
Tools, Measurement and Analysis	2.7	2.0	1.9	2.9	2.3	2.5	2.9	2.6	2.5
Monitoring and Review	3.0	2.6	2.5	3.1	2.7	2.9	3.1	2.9	3.0
Average	**2.8**	**2.4**	**2.3**	**3.1**	**2.6**	**2.8**	**3.0**	**2.8**	**2.8**

Management level

	2016	2015	2014
C-Level	2.8	2.4	2.3
VP/Director	3.1	2.6	2.8
Manager	3.0	2.8	2.8

Score

This year's survey shows improvement in incident reporting and focus on policy and standards related to communication. That said, on balance, the Communication and Information Sharing category lags others at a time when two-way internal communication (top-down and bottom-up) and external information sharing are more important than ever.

– Linnea Solem, Chief Privacy Officer, Vice President Risk and Compliance, Deluxe Corporation

Methodology

The Vendor Risk Management Benchmark Study was conducted online by the Shared Assessments Program and Protiviti in the second and third quarters of 2016, with 391 executives and managers participating in the study. Using governance as the foundational element, the survey was designed to comprehensively review the components of a robust third party risk management program.

Respondents were presented with different components of vendor risk under eight vendor risk management categories:

- Program Governance
- Policies, Standards and Procedures
- Contracts
- Vendor Risk Identification and Analysis
- Skills and Expertise
- Communication and Information Sharing
- Tools, Measurement and Analysis
- Monitoring and Review

For each component, respondents were asked to rate the maturity level as that component applies to their organization, based on the following scale:

5 = Continuous improvement – benchmarking, moving to best practices

4 = Fully implemented and operational

3 = Fully defined and established

2 = Determine roadmap to achieve goals

1 = Initial visioning

0 = Do not perform

Board Engagement, Cybersecurity and Incident Response

This year's survey contains a new section focusing on the cybersecurity and incident response capabilities of organizations. Although tone at the top has not been a component of the Vendor Risk Management Maturity Model, sharply increased regulatory focus on board risk management responsibilities and ongoing board-related research at both Protiviti and Shared Assessments suggested the time was right to explore at a more detailed level the relationship between board engagement and specific control maturity.

Incident response has also become a regulatory focus, but there has been little work to date to understand whether and how disruptive incidents might lead to more rapid maturity progress. In our results, we look not only at the overall findings, but also at how the views of respondents who report high levels of board engagement with cybersecurity risks to their own organizations as well as to their vendors compare with the views of other respondents (i.e., those who report lower levels of board engagement in these issues).

Key Observations

- In a high percentage of companies – although not a majority – the board has a high level of engagement and understanding with regard to cybersecurity risks to the business and internal operations.
- However, these numbers are noticeably lower when it comes to their vendors and the cybersecurity risks they face, suggesting boards and their companies are not as attuned to cybersecurity risks for their third parties as they are for their own businesses, even though such issues can create the same adverse, long-term effects.
- Organizations with high levels of board engagement and understanding with regard to cybersecurity risks also report higher maturity levels with all aspects of vendor risk management (see tables on the following pages).

Key Facts

Organizations that have an incident response plan in place to respond to events at vendors or third parties

Financial services organizations that have an incident response plan in place to respond to events at vendors or third parties

Organizations with an incident response plan in place that test the plan with vendors or third parties

• • • *How engaged is your board of directors with cybersecurity risks relating to your business and internal operations?*

High engagement and level of understanding by the board	39%
Medium engagement and level of understanding by the board	37%
Low engagement and level of understanding by the board	17%

	Cybersecurity Risks – Business and Internal Operations		
Vendor Risk Management Category	High engagement and level of understanding by the board	Medium engagement and level of understanding by the board	Low engagement and level of understanding by the board
Program Governance	3.5	3.0	2.0
Policies, Standards and Procedures	3.6	3.1	2.1
Contracts	3.6	3.1	2.2
Vendor Risk Identification and Analysis	3.4	2.9	1.9
Skills and Expertise	3.2	2.6	1.7
Communication and Information Sharing	3.4	2.9	2.0
Tools, Measurement and Analysis	3.3	2.8	1.8
Monitoring and Review	3.5	3.0	2.1
Average	**3.4**	**2.9**	**2.0**

We speak with many client board members who are highly engaged in their organization's cybersecurity risks. This high level of engagement is, at least in part, creating a strong tone at the top in their organizations to drive improvement in cybersecurity and privacy capabilities generally. We believe these efforts are translating into stronger vendor risk management processes as well. The key is to now build strong board engagement specifically in vendor risk management because it poses just as significant a risk to organizations as cybersecurity.

– Cal Slemp, Managing Director, Security Program and Strategy Services, Protiviti

- - - *How engaged is your board of directors with cybersecurity risks relating to your vendors?*

High engagement and level of understanding by the board	26%
Medium engagement and level of understanding by the board	37%
Low engagement and level of understanding by the board	27%

	Cybersecurity Risks – Vendors		
Vendor Risk Management Category	High engagement and level of understanding by the board	Medium engagement and level of understanding by the board	Low engagement and level of understanding by the board
Program Governance	3.7	3.2	2.2
Policies, Standards and Procedures	3.7	3.2	2.3
Contracts	3.7	3.3	2.4
Vendor Risk Identification and Analysis	3.6	3.1	2.1
Skills and Expertise	3.4	2.8	1.8
Communication and Information Sharing	3.5	3.0	2.2
Tools, Measurement and Analysis	3.5	2.9	2.1
Monitoring and Review	3.7	3.1	2.3
Average	**3.6**	**3.1**	**2.2**

- *Has your organization experienced a significant disruption within the past two years resulting from a cyberattack or hacking incident?*

Yes	16%
No	79%
Don't know	5%

- *If so, how soon after the cyberattack or incident occurred was your organization able to address the issue sufficiently and incorporate additional security measures to prevent a similar incident in the future?*

Within 1 month	38%
2-3 months	21%
3-6 months	24%
6 months to 1 year	6%
More than 1 year	3%
Don't know	8%

Program Governance

Overall level of maturity: 3.0

Key Observations

- Maturity levels are higher for a number of vendor risk components, including aligning specific vendor risk management objectives with strategic organizational objectives, communicating internally the requirements for risk-based vendor management, defining risk monitoring practices, and evaluating key risk and performance indicators.
- Certain vendor risk components have higher levels of maturity compared to last year's results, yet still score relatively low and may be areas for improvement, such as establishing an independent organizational structure for the vendor risk management program, and allocating sufficient resources to the program.
- One particularly noteworthy Program Governance result in this year's study is the performance of larger banks (with assets of $50 billion and above). In the vendor risk component focusing on maintaining vendor management policies that include risk management, security, privacy and other areas that are in alignment with existing organizational policies and objectives, banks boasted maturity scores of 4 (Fully implemented and operational) or greater, a very good result and a major improvement over previous years.

Program Governance – Overall Results

Vendor Risk Component	2016	2015	YOY Change
We define organizational structures that establish responsibility and accountability for overseeing our vendor relationships.	3.1	3.0	0.1
The organizational structure of our vendor risk management program operates independently of our business lines.	2.8	2.7	0.1
We articulate the goals and objectives of our organization.	3.3	3.1	0.2
We align specific vendor management objectives with our strategic organizational objectives.	2.9	2.6	0.3
We define vendor management policies that include risk management, security, privacy and other areas that are in alignment with our existing organizational policies and objectives.	3.1	3.0	0.1
We allocate sufficient resources for vendor risk management activities.	2.8	2.6	0.2
We communicate to our organization the requirements for risk-based vendor management.	3.1	2.8	0.3

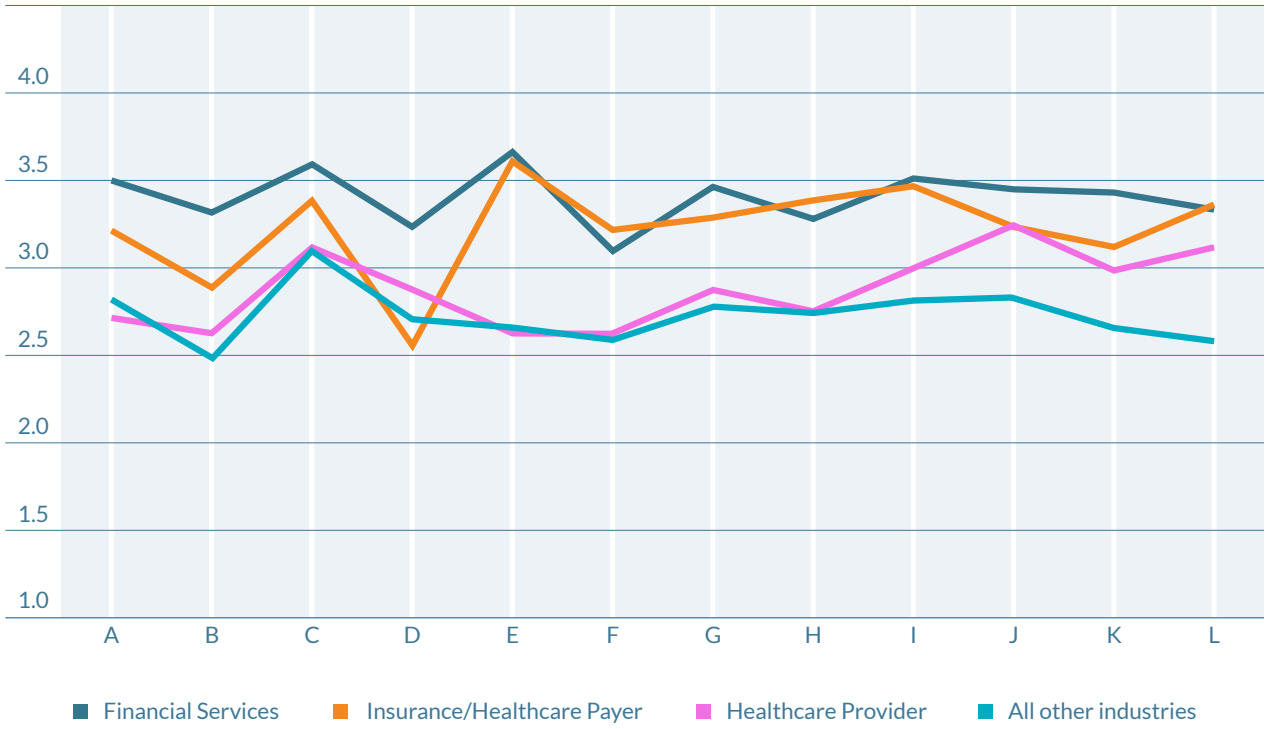
Vendor Risk Component	2016	2015	YOY Change
We determine the business value expected from our outsourced business relationships, we understand the acceptable range of business risks our organization is willing to assume in pursuing these benefits, and we determine that risks are in alignment with our vendor risk policy.	3.0	2.8	0.2
We define risk monitoring practices and establish an escalation process for exception conditions.	3.1	2.8	0.3
We evaluate key risk and performance indicators provided in management and board reporting.	3.1	2.8	0.3
We revise corporate vendor risk policy as needed to achieve strategic objectives.	3.0	2.8	0.2
We have established a formal program review schedule.*	2.9	NA	NA
Category Average	**3.0**	**2.8**	**0.2**

* Represents new vendor risk component added to this year's survey.

Commentary

Governance is a key foundational element in any vendor risk management program. Without the right resources, organizational structure and vendor risk management practices that align with a defined risk appetite, no program can succeed. Regulators have increasingly stressed the role of boards of directors in establishing, funding and periodically reexamining the effectiveness of vendor risk management programs, and with good reason. This year's study shows a 1.5-point maturity advantage overall when companies have boards that are highly engaged in cybersecurity risk management-related issues compared with those boards that have a low level of engagement in these issues.

Program Governance – Industry Results



A	We define organizational structures that establish responsibility and accountability for overseeing our vendor relationships.
B	The organizational structure of our vendor risk management program operates independently of our business lines.
C	We articulate the goals and objectives of our organization.
D	We align specific vendor management objectives with our strategic organizational objectives.
E	We define vendor management policies that include risk management, security, privacy and other areas that are in alignment with our existing organizational policies and objectives.
F	We allocate sufficient resources for vendor risk management activities.
G	We communicate to our organization the requirements for risk-based vendor management.
H	We determine the business value expected from our outsourced business relationships, we understand the acceptable range of business risks our organization is willing to assume in pursuing these benefits, and we determine that risks are in alignment with our vendor risk policy.
I	We define risk monitoring practices and establish an escalation process for exception conditions.
J	We evaluate key risk and performance indicators provided in management and board reporting.
K	We revise corporate vendor risk policy as needed to achieve strategic objectives.
L	We have established a formal program review schedule.

• • • *Program Governance – Focus on the Financial Services Industry*

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
We define organizational structures that establish responsibility and accountability for overseeing our vendor relationships.	3.2	3.4	3.8	3.6	3.6	3.6	3.9
The organizational structure of our vendor risk management program operates independently of our business lines.	2.8	3.3	3.5	3.7	3.6	3.2	3.7
We articulate the goals and objectives of our organization.	3.4	3.9	3.7	3.3	3.6	3.6	3.8
We align specific vendor management objectives with our strategic organizational objectives.	3.1	3.1	3.7	3.1	3.3	3.5	3.3
We define vendor management policies that include risk management, security, privacy and other areas that are in alignment with our existing organizational policies and objectives.	3.4	3.5	4.1	3.5	3.8	4.0	4.1
We allocate sufficient resources for vendor risk management activities.	3.0	3.0	3.1	3.0	3.6	3.3	2.9
We communicate to our organization the requirements for risk-based vendor management.	3.2	3.4	4.0	3.6	3.7	3.7	3.6
We determine the business value expected from our outsourced business relationships, we understand the acceptable range of business risks our organization is willing to assume in pursuing these benefits, and we determine that risks are in alignment with our vendor risk policy.	2.8	3.3	3.5	3.2	3.9	3.5	3.6

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
We define risk monitoring practices and establish an escalation process for exception conditions.	3.2	3.5	3.8	3.4	4.1	3.4	3.9
We evaluate key risk and performance indicators provided in management and board reporting.	3.0	3.7	3.5	3.5	3.8	3.5	3.9
We revise corporate vendor risk policy as needed to achieve strategic objectives.	3.2	3.4	3.7	3.4	3.3	3.8	3.7
We have established a formal program review schedule.	2.6	3.4	3.7	3.2	3.9	3.7	3.9
Category Average	**3.1**	**3.4**	**3.7**	**3.4**	**3.7**	**3.6**	**3.7**

Policies, Standards and Procedures

Overall level of maturity: 3.1

Key Observations

- Vendor risk components in this category show incremental improvements when compared to prior year results. Areas showing the greatest increases in maturity are defining risk categories for each classification in the vendor classification structure, and creating a process for managing contracts.
- Similar to last year, this vendor risk management category is highly correlated to having the overall highest level of maturity.
- Policies, Standards and Procedures is another category where financial services companies are beginning to show breakout performance levels. In seven of 13 vendor risk components, banks of various size had average scores of 4 (Fully implemented and operational) or greater. Larger financial services companies tended to have more risk components scoring at this level, but firms with assets under management of $5 billion to $10 billion showed markedly improved scores.

Policies, Standards and Procedures – Overall Results

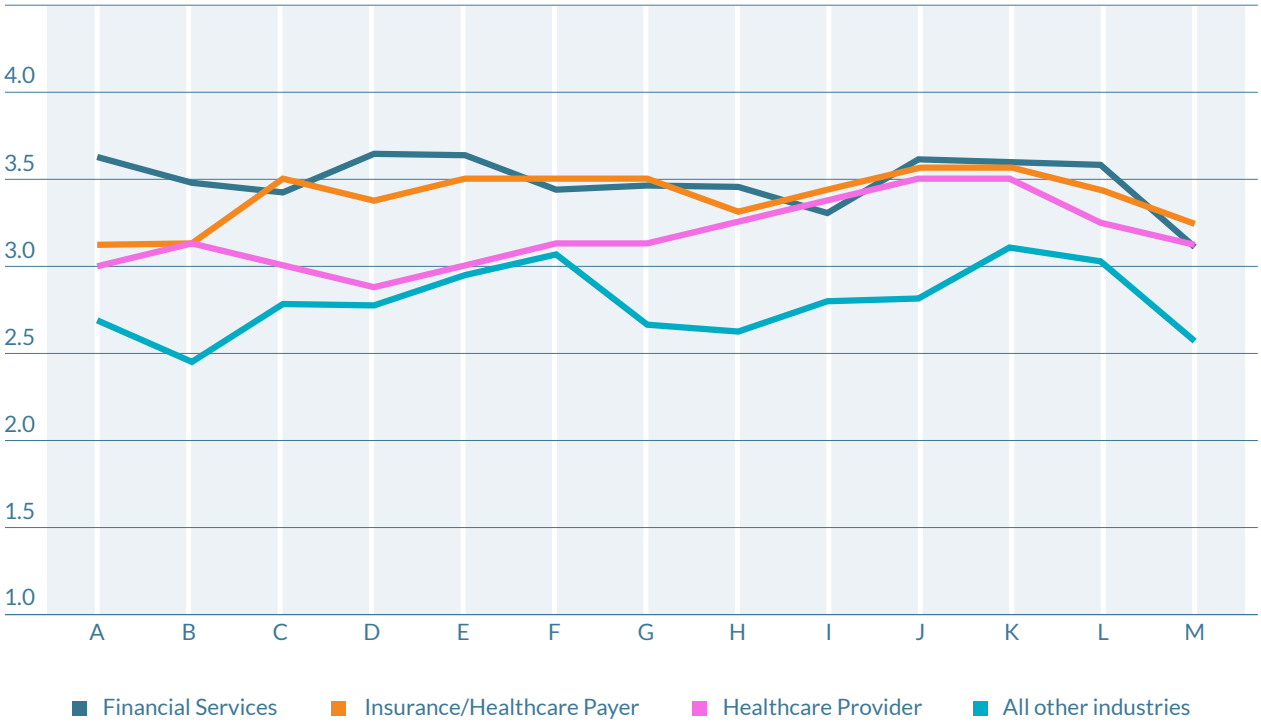
Vendor Risk Component	2016	2015	YOY Change
We have defined a vendor risk management policy.	3.1	3.0	0.1
We have defined vendor risk tier assignments.	2.9	2.8	0.1
We research and review all applicable regulatory updates and/or industry standards to ensure the overall program is meeting guidelines applicable to our organization.	3.1	3.0	0.1
We have obtained senior management approval of policy and risk tiers.	3.1	3.0	0.1
We have established standards for vendor selection and due diligence.	3.2	3.1	0.1
We have created a vendor selection process.	3.2	3.1	0.1
We have defined a vendor classification structure.	3.0	2.9	0.1
We have defined risk categories for each classification in our vendor classification structure.	3.0	2.7	0.3
We have identified existing company policies that may affect the contract process.	3.0	2.8	0.2

Vendor Risk Component	2016	2015	YOY Change
We have identified key stakeholders involved in each contract process.	3.2	3.0	0.2
We have created a process for managing contracts.	3.3	3.0	0.3
We have identified key positions involved in the contract management process.	3.3	3.1	0.2
We have established criteria and a process for vendor exit strategies.	**2.8**	**2.6**	**0.2**
Category Average	**3.1**	**2.9**	**0.2**

Commentary

Program governance is executed through policies, standards and procedures, which are essential elements of vendor risk management programs. Policies should generally be approved at the board level and should be reviewed periodically to ensure they are optimized for changing risk environments. Policies and procedures should be standardized across the enterprise to ensure that risks are evaluated uniformly. Experience has shown that larger firms operating across multiple jurisdictions and with more complex affiliate structures are at increased risk when policies and processes vary. Policies and procedures should incorporate the entire vendor lifecycle, from pre-selection due diligence, to ongoing management while a vendor is under contract, through lifecycle phases involving the termination of a relationship. Every component in this category improved this year, but we did not see the large leaps in scores for individual components experienced in some other categories.

• • • *Policies, Standards and Procedures – Industry Results*



A	We have defined a vendor risk management policy.
B	We have defined vendor risk tier assignments.
C	We research and review all applicable regulatory updates and/or industry standards to ensure the overall program is meeting guidelines applicable to our organization.
D	We have obtained senior management approval of policy and risk tiers.
E	We have established standards for vendor selection and due diligence.
F	We have created a vendor selection process.
G	We have defined a vendor classification structure.
H	We have defined risk categories for each classification in our vendor classification structure.
I	We have identified existing company policies that may affect the contract process.
J	We have identified key stakeholders involved in each contract process.
K	We have created a process for managing contracts.
L	We have identified key positions involved in the contract management process.
M	We have established criteria and a process for vendor exit strategies.

• • • *Policies, Standards and Procedures – Focus on the Financial Services Industry*

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
We have defined a vendor risk management policy.	3.2	3.7	3.9	3.5	3.9	3.9	4.0
We have defined vendor risk tier assignments.	2.9	3.4	3.4	3.5	3.9	4.0	4.0
We research and review all applicable regulatory updates and/or industry standards to ensure the overall program is meeting guidelines applicable to our organization.	3.2	3.4	3.4	3.3	3.6	3.8	3.5
We have obtained senior management approval of policy and risk tiers.	3.3	3.6	4.0	3.4	3.7	4.1	4.1
We have established standards for vendor selection and due diligence.	3.2	3.5	4.1	3.6	4.1	3.9	4.0
We have created a vendor selection process.	3.2	3.4	3.8	3.0	3.8	3.7	3.9
We have defined a vendor classification structure.	2.9	3.3	3.9	3.6	3.6	3.8	3.9
We have defined risk categories for each classification in our vendor classification structure.	3.1	3.5	3.8	3.4	3.4	3.8	4.1
We have identified existing company policies that may affect the contract process.	3.2	3.3	3.8	2.9	3.6	3.4	3.6
We have identified key stakeholders involved in each contract process.	3.2	3.6	3.9	3.6	4.0	4.0	3.7
We have created a process for managing contracts.	3.4	3.7	3.8	3.4	3.8	3.7	3.9

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
We have identified key positions involved in the contract management process.	3.1	3.8	3.8	3.5	4.0	3.7	3.8
We have established criteria and a process for vendor exit strategies.	2.7	3.1	3.7	2.8	3.4	3.4	3.5
Category Average	**3.1**	**3.5**	**3.8**	**3.3**	**3.8**	**3.8**	**3.8**

Contracts

Overall level of maturity: 3.1

Key Observations

- Several components in this category show significant jumps in maturity levels – namely, reviewing existing contracts for compliance with contract standards, ensuring inclusion of contract provisions consistent with each vendor risk classification/rating, and establishing criteria for the contract review cycle consistent with each vendor risk classification/rating.
- The Contracts vendor risk management category is tied with Policies, Standards and Procedures for having the overall highest level of maturity.
- There are two important additional components surveyed this year for the first time. The first component deals with the necessity for contract provisions that define the acceptability of vendor outsourcing to subcontractors, while the second focuses on the inclusion of contract provisions for terminating a vendor relationship.
- In this category, however, the maturity gap between financial services and some other sectors has diminished, or in the case of insurance and healthcare payers, completely vanished.

Contracts – Overall Results

Vendor Risk Component	2016	2015	YOY Change
We have defined an organizational structure for vendor contract drafting, negotiation and approval.	3.3	3.1	0.2
We have established procedures for contract exception review and approval.	3.3	3.0	0.3
We have corporate-required standards for mandatory contract language/provisions.	3.3	3.1	0.2
We have regulatory-required standards for mandatory contract language/provisions.	3.3	3.2	0.1
We have IT/security-required standards for mandatory contract language/provisions.	3.2	3.1	0.1
We have a procedure to review existing contracts for compliance with current contract standards.	3.2	2.8	0.4
We have a remediation process to correct contract deficiencies.	2.9	2.6	0.3
We have a process to ensure inclusion of appropriate performance-based contract provisions (SLAs, KPIs, KRIs, etc.).	2.9	2.7	0.2

Vendor Risk Component	2016	2015	YOY Change
We have a process to ensure inclusion of contract provisions consistent with each vendor risk classification/rating.	2.9	2.5	0.4
We have established criteria for the contract review cycle consistent with each vendor risk classification/rating.	3.0	2.6	0.4
We have a process to ensure inclusion of contract provisions terminating a vendor relationship.*	3.2	NA	NA
We have a process to ensure inclusion of contract provisions that define the acceptability of vendor outsourcing.*	3.0	NA	NA
Category Average	**3.1**	**2.9**	**0.2**

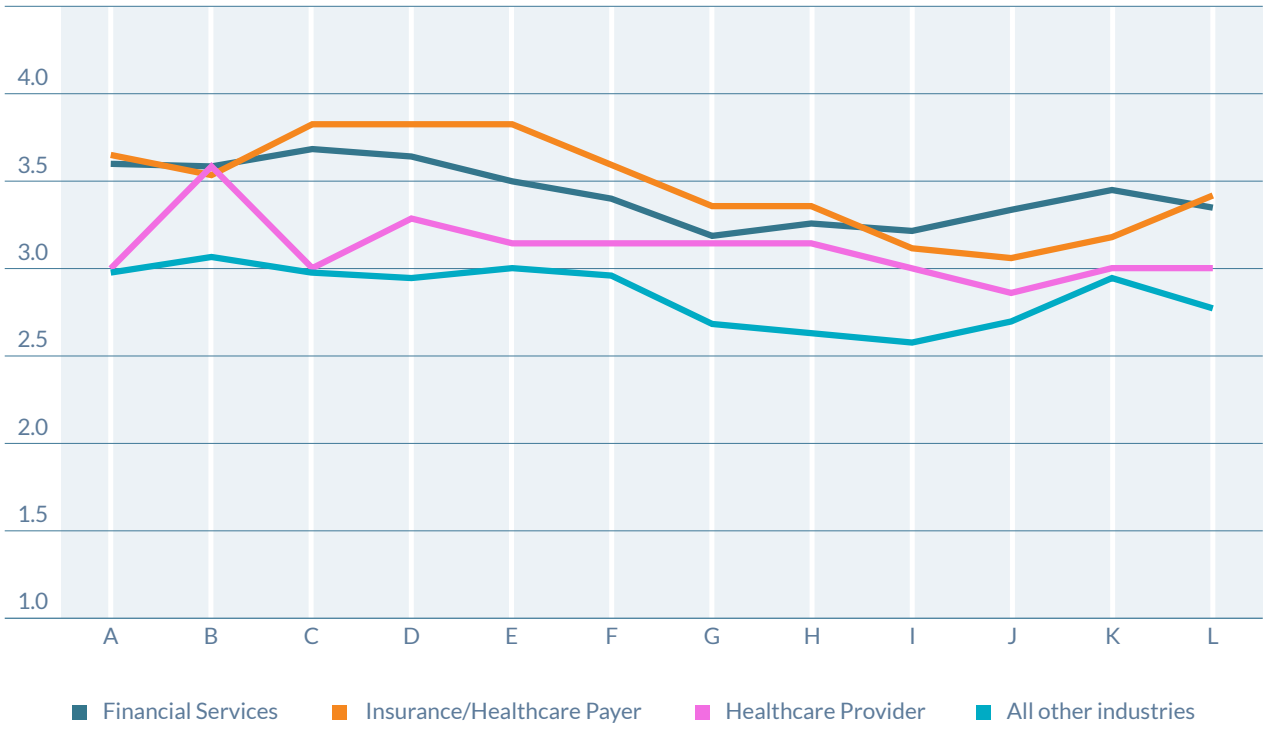
* Represents new vendor risk component added to this year's survey.

Commentary

Contracts describe the obligations for all aspects of vendor relationships, and often include items such as service-level agreements (SLAs) that define specific performance expectations, rights to audit, and the circumstances and terms under which a vendor can outsource work to subcontractors (note that subcontracting has become a recent regulatory focus point). Contracts should be written clearly, align with internal standards and reviewed regularly.

The final performance criteria of the contracts also should reflect the relative risk the specific vendor poses to the organization. In fact, two components in this category, maintaining a process to ensure inclusion of contract provisions consistent with each vendor risk classification/rating, and establishing criteria for the contract review cycle consistent with each vendor risk classification/rating, improved by healthy amounts.

Contracts – Industry Results



A	We have defined an organizational structure for vendor contract drafting, negotiation and approval.
B	We have established procedures for contract exception review and approval.
C	We have corporate-required standards for mandatory contract language/provisions.
D	We have regulatory-required standards for mandatory contract language/provisions.
E	We have IT/security-required standards for mandatory contract language/provisions.
F	We have a procedure to review existing contracts for compliance with current contract standards.
G	We have a remediation process to correct contract deficiencies.
H	We have a process to ensure inclusion of appropriate performance-based contract provisions (SLAs, KPIs, KRIs, etc.).
I	We have a process to ensure inclusion of contract provisions consistent with each vendor risk classification/rating.
J	We have established criteria for the contract review cycle consistent with each vendor risk classification/rating.
K	We have a process to ensure inclusion of contract provisions terminating a vendor relationship.
L	We have a process to ensure inclusion of contract provisions that define the acceptability of vendor outsourcing.

• • • *Contracts – Focus on the Financial Services Industry*

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
We have defined an organizational structure for vendor contract drafting, negotiation and approval.	3.3	3.5	3.7	3.4	4.2	4.4	3.8
We have established procedures for contract exception review and approval.	3.2	3.7	3.9	3.4	3.8	4.3	3.6
We have corporate-required standards for mandatory contract language/provisions.	3.4	3.8	3.8	3.6	4.1	4.1	3.7
We have regulatory-required standards for mandatory contract language/provisions.	3.2	3.8	4.0	3.5	3.8	4.4	3.8
We have IT/security-required standards for mandatory contract language/provisions.	3.1	3.6	3.8	3.4	3.5	4.1	3.8
We have a procedure to review existing contracts for compliance with current contract standards.	3.1	3.5	3.9	2.9	3.9	3.5	3.5
We have a remediation process to correct contract deficiencies.	3.1	3.1	4.1	2.6	3.4	3.8	3.1
We have a process to ensure inclusion of appropriate performance-based contract provisions (SLAs, KPIs, KRIs, etc.).	2.9	3.1	3.9	2.8	3.7	3.8	3.6
We have a process to ensure inclusion of contract provisions consistent with each vendor risk classification/rating.	2.9	3.2	3.9	3.0	3.4	3.8	3.4
We have established criteria for the contract review cycle consistent with each vendor risk classification/rating.	3.1	3.3	3.9	2.9	3.8	3.8	3.4

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
We have a process to ensure inclusion of contract provisions terminating a vendor relationship.	3.0	3.5	4.0	3.0	3.9	4.3	3.6
We have a process to ensure inclusion of contract provisions that define the acceptability of vendor outsourcing.	3.1	3.4	4.0	2.6	3.9	4.0	3.5
Category Average	**3.1**	**3.5**	**3.9**	**3.1**	**3.8**	**4.0**	**3.6**

Vendor Risk Identification and Analysis

Overall level of maturity: 2.9

Key Observations

- Vendor risk identification and analysis is one category where financial services firms are still consistently outpacing organizations outside the industry. We also see financial services firms with assets under management of more than $250 billion showing generally higher maturity levels than smaller financial services companies – often by significant margins.
- One component in particular, calculating and distributing vendor assessment metrics, jumped dramatically in maturity level this year. This suggests companies are paying significantly more attention to quantifying how they measure vendor performance and risk.
- There are six new vendor risk components being evaluated this year. One of these new components, maintaining a formal process for conducting onsite assessments, scored lower than any other item in this category.

• • • *Vendor Risk Identification and Analysis – Overall Results*

Vendor Risk Component	2016	2015	YOY Change
We have reviewed the defined business requirements for outsourcing.	2.8	2.6	0.2
We conduct a risk assessment for outsourcing the business function.	2.9	2.6	0.3
We consistently follow our process to collect and update vendor information.	3.1	2.8	0.3
We maintain a database of current vendor information.	3.3	3.0	0.3
We execute vendor risk tiering processes.	2.9	2.7	0.2
We determine vendor assessments to be performed based on risk, tiering and resources available.	2.9	2.8	0.1
We review vendor requirements with our Business, IT, Legal and Purchasing colleagues.	3.2	3.0	0.2
We send our vendors our self-assessment questionnaire and document request list.	2.9	2.7	0.2
We execute scheduling and coordinate assessment activities with vendors.	3.0	2.7	0.3
We assess compliance with vendor contracts.	3.1	2.7	0.4

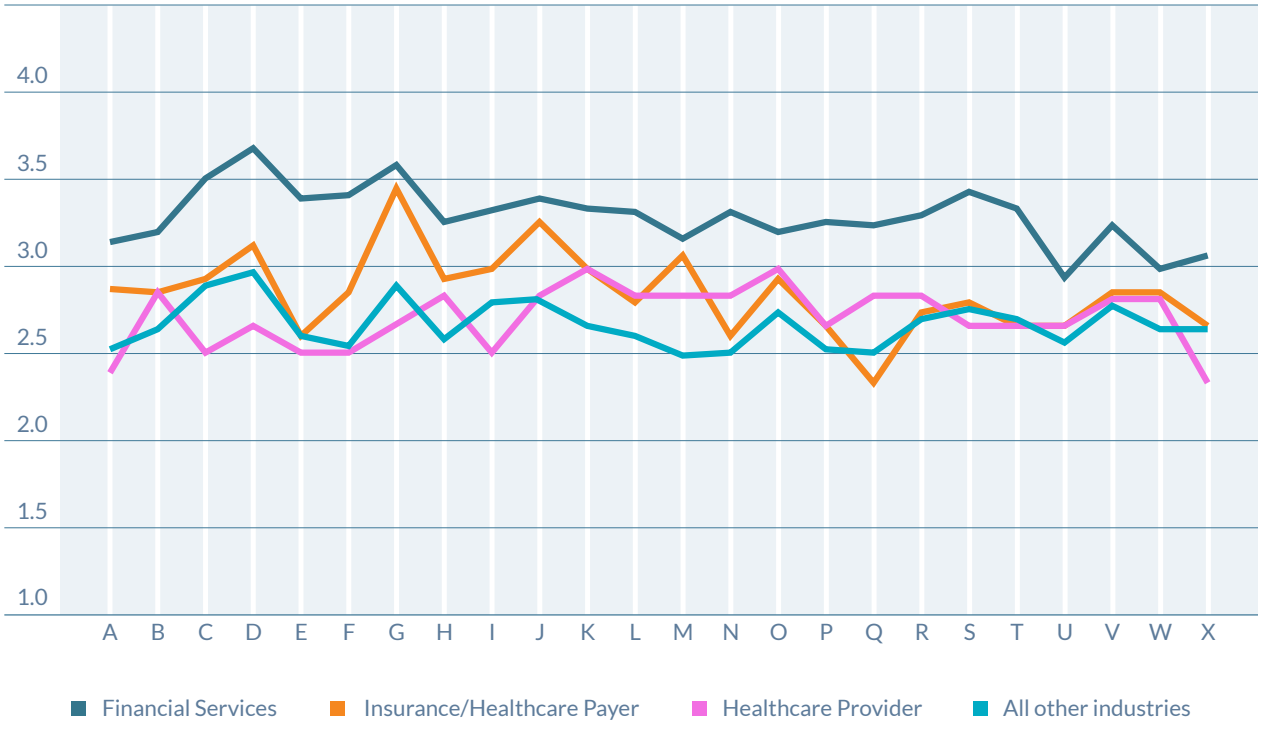
Vendor Risk Component	2016	2015	YOY Change
We identify findings and formulate recommendations.	3.0	2.8	0.2
We develop vendor assessment reports.	2.9	2.6	0.3
We establish a vendor remediation plan or termination/ exit strategy (as appropriate), validating this plan with our management and the vendor.	2.8	2.5	0.3
We establish/revise tiering of our vendors.	2.8	2.5	0.3
We perform remediation plan follow-up discussions with the vendor.	2.9	2.6	0.3
We consolidate the results of vendor assessments.	2.8	2.4	0.4
We calculate and distribute vendor assessment metrics.	2.8	2.2	0.6
We discuss results of vendor assessments and metrics with management.	2.9	2.6	0.3
We execute a formal vendor assessment process.*	3.0	NA	NA
We formally document assessment roles and responsibilities.*	2.9	NA	NA
We have a formal process for conducting onsite assessments.*	2.7	NA	NA
We assess compliance with business continuity contract terms.*	3.0	NA	NA
We assess compliance with outsourcing requirement contract terms.*	2.8	NA	NA
We have a process in place to determine if a vendor utilizes subcontractors whenever a vendor contract does not include vendor outsourcing requirements.*	2.8	NA	NA
Category Average	**2.9**	**2.7**	**0.2**

* Represents new vendor risk component added to this year's survey.

Commentary

Vendor risk identification and analysis is in some ways the mechanical heart of any vendor risk management program – it is here that execution of key processes is centered, from establishing and executing risk tiering processes, to developing, distributing and discussing vendor assessment reports, to assessing compliance with a wide range of contract terms. By their nature, these activities can be resource-intensive and inadequate funding can hinder otherwise promising programs. This category is one of three where organizations with low board engagement in internal cybersecurity risks report maturity scores of under 2.0.

Vendor Risk Identification and Analysis – Industry Results



A	We have reviewed the defined business requirements for outsourcing.
B	We conduct a risk assessment for outsourcing the business function.
C	We consistently follow our process to collect and update vendor information.
D	We maintain a database of current vendor information.
E	We execute vendor risk tiering processes.
F	We determine vendor assessments to be performed based on risk, tiering and resources available.

G	We review vendor requirements with our Business, IT, Legal and Purchasing colleagues.
H	We send our vendors our self-assessment questionnaire and document request list.
I	We execute scheduling and coordinate assessment activities with vendors.
J	We assess compliance with vendor contracts.
K	We identify findings and formulate recommendations.
L	We develop vendor assessment reports.
M	We establish a vendor remediation plan or termination/exit strategy (as appropriate), validating this plan with our management and the vendor.
N	We establish/revise tiering of our vendors.
O	We perform remediation plan follow-up discussions with the vendor.
P	We consolidate the results of vendor assessments.
Q	We calculate and distribute vendor assessment metrics.
R	We discuss results of vendor assessments and metrics with management.
S	We execute a formal vendor assessment process.
T	We formally document assessment roles and responsibilities.
U	We have a formal process for conducting onsite assessments.
V	We assess compliance with business continuity contract terms.
W	We assess compliance with outsourcing requirement contract terms.
X	We have a process in place to determine if a vendor utilizes subcontractors whenever a vendor contract does not include vendor outsourcing requirements.

• • • *Vendor Risk Identification and Analysis – Focus on the Financial Services Industry*

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
We have reviewed the defined business requirements for outsourcing.	2.6	3.4	3.9	2.1	3.4	3.9	3.9
We conduct a risk assessment for outsourcing the business function.	2.7	3.5	3.8	2.2	3.7	3.9	3.6
We consistently follow our process to collect and update vendor information.	3.1	3.6	3.8	3.1	3.9	4.1	3.8
We maintain a database of current vendor information.	3.5	3.5	4.0	3.5	4.0	4.2	3.9
We execute vendor risk tiering processes.	2.8	3.5	3.6	3.3	3.8	4.1	3.9
We determine vendor assessments to be performed based on risk, tiering and resources available.	2.8	3.4	3.8	3.3	3.9	4.2	3.8
We review vendor requirements with our Business, IT, Legal and Purchasing colleagues.	3.3	3.8	4.0	2.8	4.1	4.2	3.8
We send our vendors our self-assessment questionnaire and document request list.	3.1	3.2	3.8	3.1	2.9	3.9	3.5
We execute scheduling and coordinate assessment activities with vendors.	3.0	3.3	3.8	3.4	3.2	3.9	3.5
We assess compliance with vendor contracts.	3.4	3.4	3.7	2.9	3.2	3.5	3.7
We identify findings and formulate recommendations.	3.2	3.3	3.7	3.1	3.5	3.7	3.6
We develop vendor assessment reports.	2.9	3.4	3.7	3.2	3.6	3.5	3.9

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
We establish a vendor remediation plan or termination/exit strategy (as appropriate), validating this plan with our management and the vendor.	2.9	3.2	3.6	2.5	3.1	4.0	3.6
We establish/revise tiering of our vendors.	2.9	3.2	3.6	3.2	3.6	4.0	3.9
We perform remediation plan follow-up discussions with the vendor.	3.0	3.2	3.7	2.4	3.5	3.7	3.6
We consolidate the results of vendor assessments.	3.0	3.3	3.9	2.9	3.6	3.7	3.4
We calculate and distribute vendor assessment metrics.	2.8	3.3	3.9	2.9	3.4	4.2	3.7
We discuss results of vendor assessments and metrics with management.	2.8	3.4	3.8	3.1	3.6	4.1	3.7
We execute a formal vendor assessment process.	3.1	3.5	3.9	3.1	3.8	4.0	3.7
We formally document assessment roles and responsibilities.	3.1	3.4	3.7	2.6	3.8	4.0	3.6
We have a formal process for conducting onsite assessments.	2.4	3.1	3.9	2.4	3.1	3.6	3.3
We assess compliance with business continuity contract terms.	2.9	3.2	4.1	2.9	3.3	4.1	3.3
We assess compliance with outsourcing requirement contract terms.	2.4	3.0	4.0	2.6	3.4	3.9	3.2
We have a process in place to determine if a vendor utilizes subcontractors whenever a vendor contract does not include vendor outsourcing requirements.	2.6	3.1	3.9	2.5	3.4	3.5	3.4
Category Average	**2.9**	**3.3**	**3.8**	**2.9**	**3.5**	**2.9**	**3.3**

Skills and Expertise

Overall level of maturity: 2.7

Key Observations

- The Skills and Expertise category continues to have the lowest level of vendor risk management maturity in the benchmarking survey.
- Most components show significant progress in maturity levels this year – albeit from a very low base. Two training-related indicators improved by 0.6 and 0.7, among the largest increases in the survey.
- A new component measured this year focuses on having governance programs that can capture savings as programs are optimized to achieve maximum efficiency. Not surprisingly, scores in this area were modest, since meaningful optimization is typically a characteristic of more mature programs.

• • • *Skills and Expertise – Overall Results*

Vendor Risk Component	2016	2015	YOY Change
We have assigned vendor risk management accountability to an individual in our organization.	3.0	2.8	0.2
Roles and responsibilities (e.g., risk, sourcing, procurement, contracts) are defined clearly within our job descriptions.	3.1	2.8	0.3
We provide training for assigned vendor risk management resources to maintain appropriate certifications.	2.7	2.3	0.4
We have sufficient staff to manage vendor risk management activities effectively.	2.8	2.4	0.4
We have structures in place to define and measure the staffing levels required to meet vendor risk program objectives.	2.6	2.1	0.5
We have sufficient qualified staff to meet all vendor risk management objectives.	2.7	2.4	0.3
We have defined and communicated vendor risk management policies to our key stakeholders.	2.9	2.7	0.2
We periodically communicate our vendor risk management policies and procedures to all personnel.	2.7	2.4	0.3
At least annually, we provide training on vendor risk management policies and procedures to appropriate employee groups based on role.	2.7	2.1	0.6

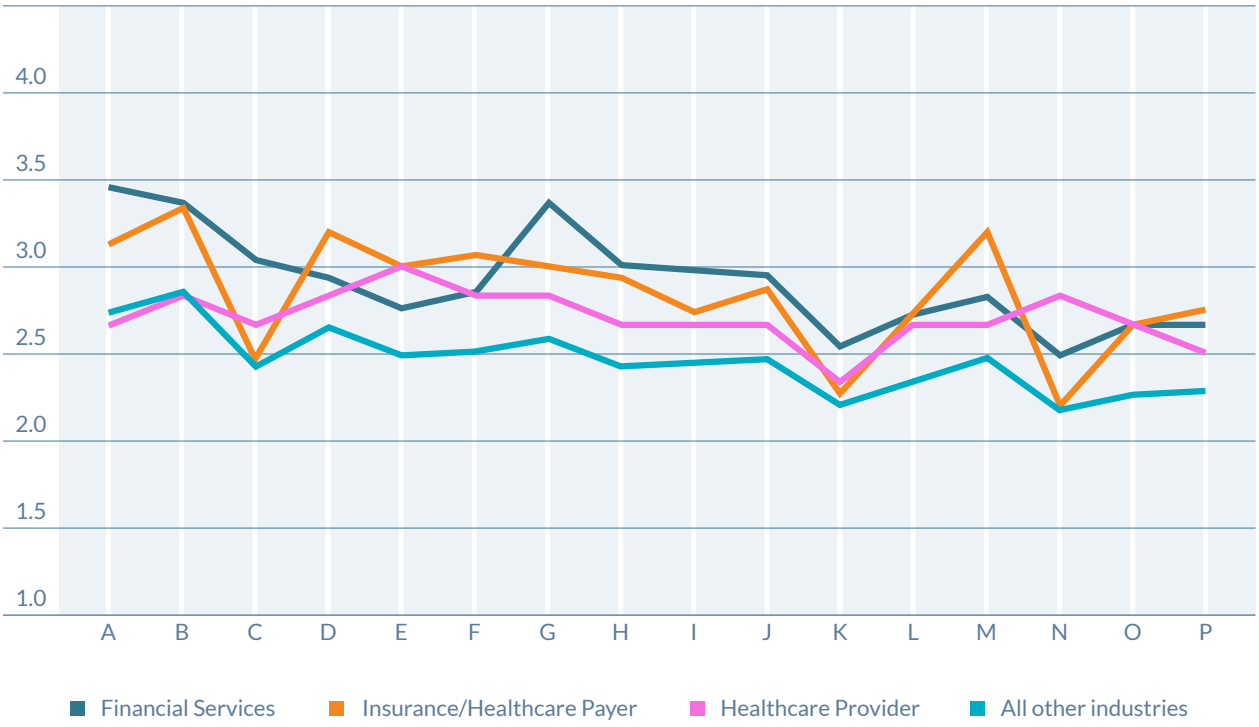
Vendor Risk Component	2016	2015	YOY Change
We have defined training and education for our vendor risk personnel to enable them to define, execute and manage our program.	2.7	2.2	0.5
On an annual basis, we measure employee understanding of vendor risk management accountabilities and report results to management.	2.3	1.8	0.5
We have implemented metrics and reporting for compliance to required training and awareness of our vendor risk policies.	2.5	1.8	0.7
We have allocated budget for vendor risk management functions, including basic travel, subscriptions, training and small projects.	2.6	2.3	0.3
We routinely measure or benchmark our vendor risk management budget with management reporting to demonstrate ROI.	2.3	1.9	0.4
We have integrated vendor risk management functions and tools sufficiently into our business lines so that overall costs and budget for dedicated risk management budgets are reduced.	2.4	2.1	0.3
We have formalized governance programs so that staffing levels can be reduced due to optimization.*	2.5	NA	NA
Category Average	**2.7**	**2.3**	**0.4**

* Represents new vendor risk component added to this year's survey.

Commentary

Although Skills and Expertise continues to be the lowest-rated category in the survey, the level of assessed maturity in this category improved as much as anywhere else throughout the survey. The vendor risk components in the Skills and Expertise category assess the organization's ability to respond quickly to properly targeted management investment, again highlighting the importance of having adequate resources to provide appropriate levels of risk management. However, demand for skilled third party risk management resources has often exceeded the supply of properly trained candidates, and this reality has become a cross-industry concern. Only if investments in third party risk management programs continue and enough skilled resources are appropriately trained will maturity-level gains in this area begin to outpace those in other categories.

• • • *Skills and Expertise – Industry Results*



A	We have assigned vendor risk management accountability to an individual in our organization.
B	Roles and responsibilities (e.g., risk, sourcing, procurement, contracts) are defined clearly within our job descriptions.
C	We provide training for assigned vendor risk management resources to maintain appropriate certifications.
D	We have sufficient staff to manage vendor risk management activities effectively.
E	We have structures in place to define and measure the staffing levels required to meet vendor risk program objectives.
F	We have sufficient qualified staff to meet all vendor risk management objectives.
G	We have defined and communicated vendor risk management policies to our key stakeholders.
H	We periodically communicate our vendor risk management policies and procedures to all personnel.
I	At least annually, we provide training on vendor risk management policies and procedures to appropriate employee groups based on role.
J	We have defined training and education for our vendor risk personnel to enable them to define, execute and manage our program.
K	On an annual basis, we measure employee understanding of vendor risk management accountabilities and report results to management.
L	We have implemented metrics and reporting for compliance to required training and awareness of our vendor risk policies.

M	We have allocated budget for vendor risk management functions, including basic travel, subscriptions, training and small projects.
N	We routinely measure or benchmark our vendor risk management budget with management reporting to demonstrate ROI.
O	We have integrated vendor risk management functions and tools sufficiently into our business lines so that overall costs and budget for dedicated risk management budgets are reduced.
P	We have formalized governance programs so that staffing levels can be reduced due to optimization.

• • • *Skills and Expertise – Focus on the Financial Services Industry*

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
We have assigned vendor risk management accountability to an individual in our organization.	3.2	3.3	3.7	3.4	3.5	4.3	3.7
Roles and responsibilities (e.g., risk, sourcing, procurement, contracts) are defined clearly within our job descriptions.	3.1	3.4	3.7	2.9	3.2	4.3	3.8
We provide training for assigned vendor risk management resources to maintain appropriate certifications.	2.6	3.2	3.1	2.5	3.4	3.7	3.5
We have sufficient staff to manage vendor risk management activities effectively.	2.6	3.0	3.7	2.5	3.1	3.5	3.2
We have structures in place to define and measure the staffing levels required to meet vendor risk program objectives.	2.5	2.9	3.6	1.9	2.9	3.5	2.8
We have sufficient qualified staff to meet all vendor risk management objectives.	2.6	3.0	3.2	2.4	3.3	3.2	3.0
We have defined and communicated vendor risk management policies to our key stakeholders.	3.0	3.5	3.4	2.9	3.5	4.0	3.8
We periodically communicate our vendor risk management policies and procedures to all personnel.	2.5	3.2	3.1	2.4	3.5	3.9	3.3

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
At least annually, we provide training on vendor risk management policies and procedures to appropriate employee groups based on role.	2.5	3.1	3.2	2.1	3.5	4.1	3.3
We have defined training and education for our vendor risk personnel to enable them to define, execute and manage our program.	2.6	2.8	3.3	2.6	3.5	3.6	3.3
On an annual basis, we measure employee understanding of vendor risk management accountabilities and report results to management.	1.9	2.8	3.3	1.9	2.7	3.1	3.1
We have implemented metrics and reporting for compliance to required training and awareness of our vendor risk policies.	2.0	3.0	3.3	2.4	3.0	3.5	3.2
We have allocated budget for vendor risk management functions, including basic travel, subscriptions, training and small projects.	2.3	2.6	3.8	2.2	3.2	3.5	3.6
We routinely measure or benchmark our vendor risk management budget with management reporting to demonstrate ROI.	1.9	3.0	3.4	1.6	3.1	2.8	2.6
We have integrated vendor risk management functions and tools sufficiently into our business lines so that overall costs and budget for dedicated risk management budgets are reduced.	2.0	2.8	3.3	2.2	3.1	3.6	3.1
We have formalized governance programs so that staffing levels can be reduced due to optimization.	2.0	2.9	3.8	2.2	3.0	3.7	2.7
Category Average	**2.5**	**3.0**	**3.4**	**2.4**	**3.2**	**3.6**	**3.3**

Communication and Information Sharing

Overall level of maturity: 2.9

Key Observations

- Significant jumps in maturity level for numerous components contributed to a notable increase in the overall average for the category. The greatest increase in maturity is in managing vendor inventory.
- Two key aspects of communications performance improved this year, the first relating to communicating and escalating incidents and the second focusing on the process to provide board and executive management responses to vendor assessment results.
- There is one new communication component in this year's study focusing on an organization's process to communicate policies and standards. That new item scored a maturity level of 3.1.

Communication and Information Sharing – Overall Results

Vendor Risk Component	2016	2015	YOY Change
We have a formal process in place for adoption of the program by executive management and adoption of the program as a standard practice (sourcing, procurement, contracts).	2.8	2.7	0.1
We have in place an ongoing education program for vendor management policies, procedures and updates.	2.6	2.2	0.4
We have a process in place to periodically assess vendor value (for example, service delivery, vendor security, control environment, operations, etc.).	2.8	2.5	0.3
We have a process in place to evaluate internal compliance with vendor management onboarding, periodic assessment and off-boarding.	2.8	2.4	0.4
We have a process in place to manage vendor inventory.	2.9	2.4	0.5
We have a process in place to report status of vendor assessments.	2.8	2.6	0.2
We have a process in place to evaluate compliance with vendor management processes and procedures.	2.8	2.5	0.3
We have a process in place to periodically evaluate vendor service delivery.	2.9	2.5	0.4
We have a process in place to track and communicate incidents.	3.1	2.7	0.4

Vendor Risk Component	2016	2015	YOY Change
We have a process in place to escalate and communicate incidents and issues.	3.1	2.8	0.3
We have a process in place to provide board and executive management response to vendor assessment results.	2.9	2.5	0.4
We have a process in place to communicate policies and standards.*	3.1	NA	NA
We have clearly defined roles and responsibilities in the areas that manage sourcing, procurement, contracts.*	3.1	NA	NA
Category Average	**2.9**	**2.5**	**0.4**

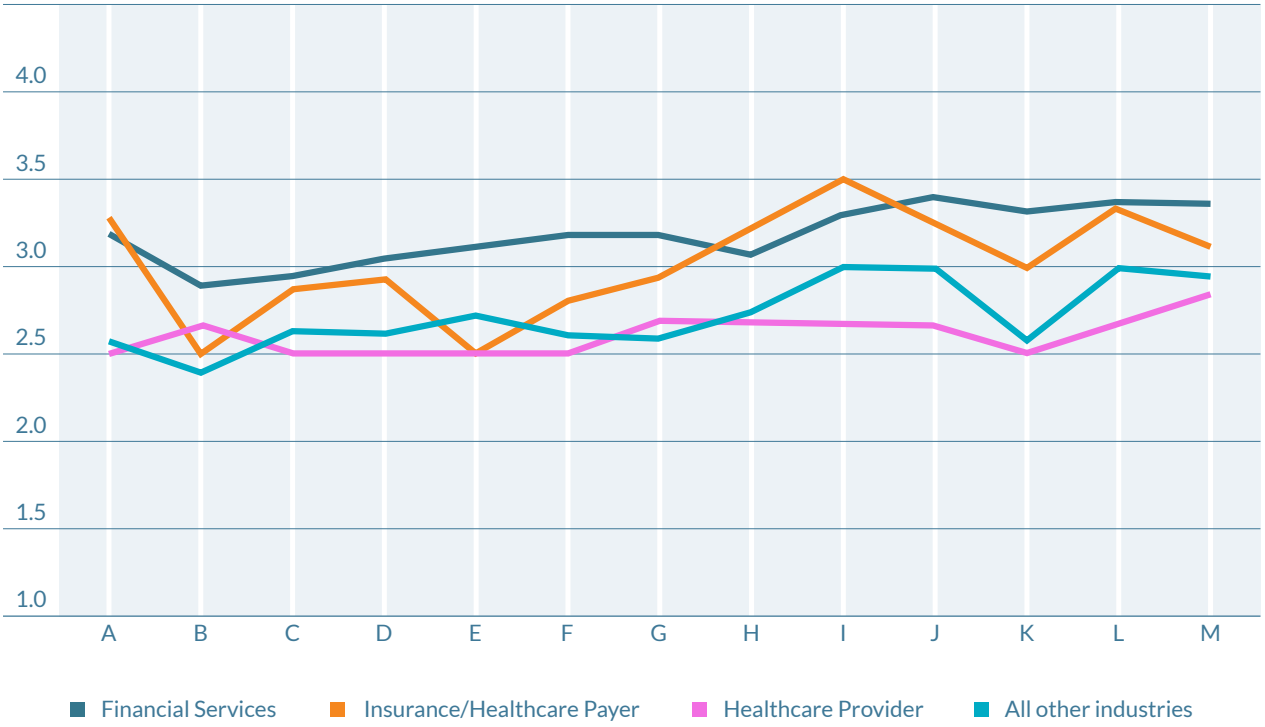
* Represents new vendor risk component added to this year's survey.

Commentary

Communications around the subject of third party risk management should be both top-down and bottom-up – anything less is suboptimal. Frameworks should be in place to establish how results of vendor risk assessments and risk-related incidents are shared with the board, senior management and key risk committees, and results in this year's study show significant improvement from 2015. Communication with board risk committees is particularly important, and communications should adopt styles (tailored dashboards, for example) that are comfortable for committee members.

Top-down communication from the board and executive management is critical to establishing the right risk culture and specific performance expectations. Widespread communications are essential to promote an understanding of the organization's risk appetite and how that perspective then translates to day-to-day risk management expectations.

Communication and Information Sharing – Industry Results



A	We have a formal process in place for adoption of the program by executive management and adoption of the program as a standard practice (sourcing, procurement, contracts).
B	We have in place an ongoing education program for vendor management policies, procedures and updates.
C	We have a process in place to periodically assess vendor value (for example, service delivery, vendor security, control environment, operations, etc.).
D	We have a process in place to evaluate internal compliance with vendor management onboarding, periodic assessment and off-boarding.
E	We have a process in place to manage vendor inventory.
F	We have a process in place to report status of vendor assessments.
G	We have a process in place to evaluate compliance with vendor management processes and procedures.
H	We have a process in place to periodically evaluate vendor service delivery.
I	We have a process in place to track and communicate incidents.
J	We have a process in place to escalate and communicate incidents and issues.
K	We have a process in place to provide board and executive management response to vendor assessment results.
L	We have a process in place to communicate policies and standards.
M	We have clearly defined roles and responsibilities in the areas that manage sourcing, procurement, contracts.

• • • *Communication and Information Sharing – Focus on the Financial Services Industry*

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
We have a formal process in place for adoption of the program by executive management and adoption of the program as a standard practice (sourcing, procurement, contracts).	2.7	3.3	3.3	2.9	3.5	4.1	3.4
We have in place an ongoing education program for vendor management policies, procedures and updates.	2.3	3.0	3.4	2.6	3.4	3.5	2.9
We have a process in place to periodically assess vendor value (for example, service delivery, vendor security, control environment, operations, etc.).	2.6	3.0	3.5	2.4	3.2	3.5	3.4
We have a process in place to evaluate internal compliance with vendor management onboarding, periodic assessment and off-boarding.	2.6	3.0	3.6	3.0	3.2	3.6	3.4
We have a process in place to manage vendor inventory.	2.4	3.3	3.5	3.0	3.5	3.7	3.7
We have a process in place to report status of vendor assessments.	2.6	3.2	3.5	3.1	3.7	3.6	3.8
We have a process in place to evaluate compliance with vendor management processes and procedures.	2.7	3.2	3.4	3.1	3.5	3.8	3.7
We have a process in place to periodically evaluate vendor service delivery.	2.8	3.0	3.6	2.8	3.2	3.5	3.6
We have a process in place to track and communicate incidents.	3.0	3.0	3.6	3.3	3.5	3.5	3.9
We have a process in place to escalate and communicate incidents and issues.	3.3	3.1	3.6	3.1	3.6	3.6	4.0

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
We have a process in place to provide board and executive management response to vendor assessment results.	3.1	3.1	3.9	2.9	3.6	3.8	3.6
We have a process in place to communicate policies and standards.	3.0	3.5	3.8	3.0	3.6	3.8	3.6
We have clearly defined roles and responsibilities in the areas that manage sourcing, procurement, contracts.	3.0	3.5	3.6	2.8	3.8	4.0	3.8
Category Average	**2.8**	**3.2**	**3.6**	**2.9**	**3.5**	**3.7**	**3.6**

Tools, Measurement and Analysis

Overall level of maturity: 2.8

Key Observations

- Scores in this category improved significantly this year.
- More organizations are providing periodic monitoring, reporting on reviews, and establishing relevant financial measures and benchmarks.
- Relatively low (but improved) scores focusing on the use of automated risk scoring suggest that many organizations can achieve step function improvements and efficiencies in vendor evaluation by investing in targeted process automation.

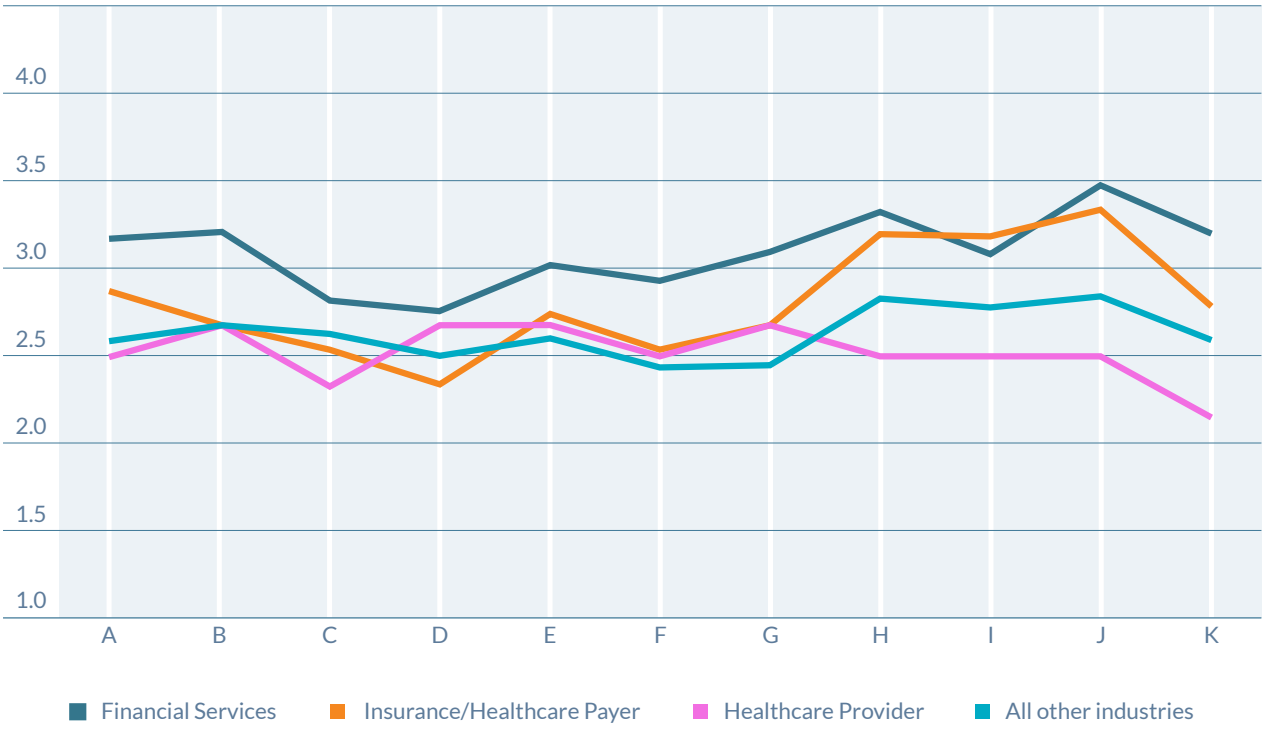
Tools, Measurement and Analysis – Overall Results

Vendor Risk Component	2016	2015	YOY Change
We establish vendor review schedules for all vendor assessments (onsite, remote, etc.).	2.8	2.5	0.3
We assign resources to accomplish reviews as scheduled.	2.9	2.5	0.4
We capture and report on vendor review costs, budget to actual, etc.	2.7	2.2	0.5
We monitor variances between scheduled reviews and actual reviews performed.	2.6	2.1	0.5
We provide periodic reporting on review monitoring.	2.8	2.2	0.6
We process information obtained during the vendor selection or review process into a risk scoring tool based on our risk scoring methodology.	2.6	2.3	0.3
We report risk scoring results to relevant stakeholders.	2.7	2.4	0.3
We engage finance and procurement partners.	3.0	2.6	0.4
We establish relevant financial measures and benchmarks.	2.9	2.3	0.6
We determine the financial viability of key vendors.	3.1	2.7	0.4
We report financial results from our vendors to relevant stakeholders.	2.8	2.4	0.4
Category Average	**2.8**	**2.4**	**0.4**

Commentary

Improved results in this category suggest that more organizations have realized the importance of conducting regular onsite assessments of critical vendors. These assessments are especially important when firms outsource activities that are central to their operations. Today's marketplace is generating an expanded set of options for firms to achieve efficiencies in verifying vendor performance, and the development of continuous monitoring solutions will be very important moving forward.

• • • *Tools, Measurement and Analysis – Industry Results*



A	We establish vendor review schedules for all vendor assessments (onsite, remote, etc.).
B	We assign resources to accomplish reviews as scheduled.
C	We capture and report on vendor review costs, budget to actual, etc.
D	We monitor variances between scheduled reviews and actual reviews performed.
E	We provide periodic reporting on review monitoring.
F	We process information obtained during the vendor selection or review process into a risk scoring tool based on our risk scoring methodology.
G	We report risk scoring results to relevant stakeholders.
H	We engage finance and procurement partners.
I	We establish relevant financial measures and benchmarks.
J	We determine the financial viability of key vendors.
K	We report financial results from our vendors to relevant stakeholders.

• • • *Tools, Measurement and Analysis – Focus on the Financial Services Industry*

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
We establish vendor review schedules for all vendor assessments (onsite, remote, etc.).	2.6	3.5	3.5	3.0	3.6	3.6	3.5
We assign resources to accomplish reviews as scheduled.	2.8	3.4	3.6	2.9	3.7	3.7	3.2
We capture and report on vendor review costs, budget to actual, etc.	2.6	3.3	3.9	1.6	3.1	3.1	3.0
We monitor variances between scheduled reviews and actual reviews performed.	2.2	3.0	3.8	2.1	3.3	3.2	2.9
We provide periodic reporting on review monitoring.	2.4	3.0	3.6	2.9	3.8	3.6	3.2
We process information obtained during the vendor selection or review process into a risk scoring tool based on our risk scoring methodology.	2.4	2.9	3.4	2.4	3.5	3.9	3.4
We report risk scoring results to relevant stakeholders.	2.6	3.2	3.1	3.0	3.6	3.9	3.3
We engage finance and procurement partners.	2.8	3.8	3.6	2.9	3.4	4.1	3.7
We establish relevant financial measures and benchmarks.	2.8	3.6	3.5	2.5	3.1	3.6	3.0
We determine the financial viability of key vendors.	2.9	3.8	3.6	3.4	3.8	4.1	3.7
We report financial results from our vendors to relevant stakeholders.	2.9	3.3	3.6	2.9	3.5	3.9	3.5
Category Average	**2.6**	**3.3**	**3.6**	**2.7**	**3.5**	**3.7**	**3.3**

Monitoring and Review

Overall level of maturity: 3.0

Key Observations

- External feedback stands out as an area of maturity growth, with more organizations periodically conducting customer satisfaction surveys.
- There were four new components included in the survey for the first time this year, relating to having processes in place to regularly assess providers' financial conditions, to determine if additional control validation is necessary, and to determine if an onsite assessment is necessary and should be performed. Scores in all these areas fell just below the category average.

Monitoring and Review – Overall Results

Vendor Risk Component	2016	2015	YOY Change
We have standard contract terms in place.	3.5	3.2	0.3
We have a process in place to facilitate approval of final contract terms by our Legal department and an appropriate level of management.	3.5	3.4	0.1
We have a process in place to modify contracts and approve modifications by our Legal department, and an appropriate level of management.	3.4	3.4	0.0
We have policies and procedures in place over the process to store, retain and make available contract terms.	3.3	3.1	0.2
We have a process in place to address expired or canceled contracts.	3.2	2.8	0.4
We have a process in place to periodically require SLA reporting.	2.7	2.5	0.2
We have a process in place to track and analyze customer complaints.	3.1	2.7	0.4
We have a process in place to periodically conduct customer satisfaction surveys.	2.9	2.3	0.6
We have a process in place to respond to, escalate and inform key stakeholders of relevant data security, breaches or other similar incidents.	3.1	3.1	0.0
We have a process in place to monitor industry and market trends that may negatively impact our vendors.	2.8	2.5	0.3
We have a process in place to respond to and inform our key stakeholders of regulatory requirements and trends.	3.0	2.8	0.2
We have a process in place to review applicable audit reports periodically.	3.1	2.9	0.2

Vendor Risk Component	2016	2015	YOY Change
We have a process in place to test our vendors' business continuity and disaster recovery measures periodically, and review the test results.	2.7	2.4	0.3
We have a process in place to periodically conduct vendor onsite visits and testing.	2.8	2.5	0.3
We obtain independent assurance or third party testing of key vendors.	2.8	2.6	0.2
We have a process in place to regularly assess providers' financial conditions.*	2.9	NA	NA
We have a process in place to determine if additional control validation is necessary.*	2.8	NA	NA
We have a process in place to determine if an onsite assessment is necessary.*	2.8	NA	NA
We have a process in place to determine if an onsite inspection should be performed.*	2.8	NA	NA
Category Average	**3.0**	**2.8**	**0.2**

* Represents new vendor risk component added to this year's survey.

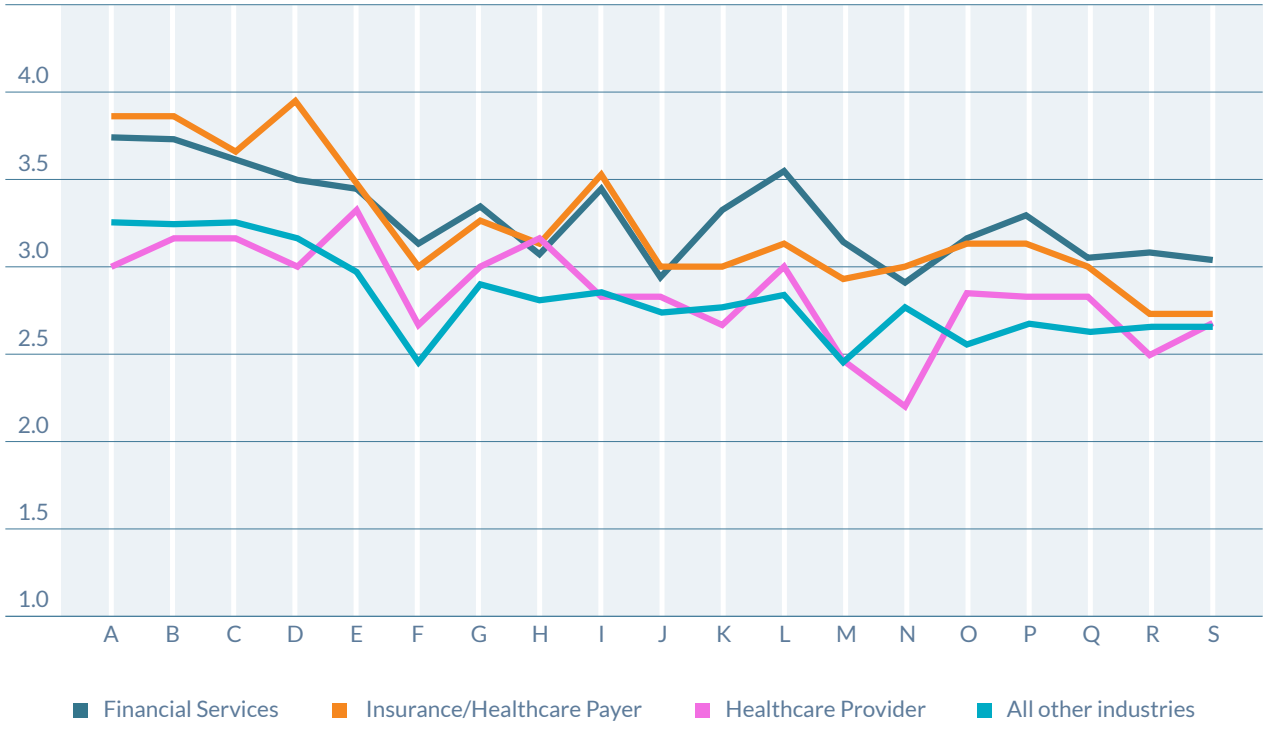
Commentary

Monitoring and review capabilities are important and have become a subject of regulatory interest since the Office of the Comptroller of the Currency (OCC) issued updated third party risk guidance in 2013, in which financial institutions are now required to conduct "periodic independent reviews" of their own third party risk management programs and report results to their board of directors.[6] Especially in heavily regulated environments, it is very important to have a process in place to monitor and communicate changes in regulatory requirements, not just internally, but also to external stakeholders. Evolving regulatory requirements, not to mention changes to the threat environment, may necessitate changes to existing vendor contracts and other aspects of the third party risk management process. Monitoring and testing third party business continuity and disaster recovery plans is also critically important and increasingly is a regulatory focus.[7] Periodic testing and evaluation of policies and processes allows management to make well-informed decisions about how to allocate resources to manage vendor risk. One component in this category, maintaining a process in place to periodically conduct customer satisfaction surveys, improved by 0.6 this year, one of the largest gains in the survey.

[6] OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," October 30, 2013. www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

[7] *FFIEC Information Technology Examination Handbook*, Appendix J: "Strengthening the Resilience of Outsourced Technology Services," FFIEC. February 2015. http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-j-strengthening-the-resilience-of-outsourced-technology-services.aspx.

• • • *Monitoring and Review – Industry Results*



A	We have standard contract terms in place.
B	We have a process in place to facilitate approval of final contract terms by our Legal department and an appropriate level of management.
C	We have a process in place to modify contracts and approve modifications by our Legal department, and an appropriate level of management.
D	We have policies and procedures in place over the process to store, retain and make available contract terms.
E	We have a process in place to address expired or canceled contracts.
F	We have a process in place to periodically require SLA reporting.
G	We have a process in place to track and analyze customer complaints.
H	We have a process in place to periodically conduct customer satisfaction surveys.
I	We have a process in place to respond to, escalate and inform key stakeholders of relevant data security, breaches or other similar incidents.
J	We have a process in place to monitor industry and market trends that may negatively impact our vendors.
K	We have a process in place to respond to and inform our key stakeholders of regulatory requirements and trends.

L	We have a process in place to review applicable audit reports periodically.
M	We have a process in place to test our vendors' business continuity and disaster recovery measures periodically, and review the test results.
N	We have a process in place to periodically conduct vendor onsite visits and testing.
O	We obtain independent assurance or third party testing of key vendors.
P	We have a process in place to regularly assess providers' financial conditions.
Q	We have a process in place to determine if additional control validation is necessary.
R	We have a process in place to determine if an onsite assessment is necessary.
S	We have a process in place to determine if an onsite inspection should be performed.

• • • *Monitoring and Review – Focus on the Financial Services Industry*

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
We have standard contract terms in place.	3.5	3.7	3.9	3.5	4.3	4.3	3.7
We have a process in place to facilitate approval of final contract terms by our Legal department and an appropriate level of management.	3.4	3.9	3.8	3.4	4.2	4.1	3.8
We have a process in place to modify contracts and approve modifications by our Legal department, and an appropriate level of management.	3.4	3.7	3.9	2.7	4.2	4.1	3.8
We have policies and procedures in place over the process to store, retain and make available contract terms.	3.2	3.5	3.9	3.1	3.5	4.2	3.8
We have a process in place to address expired or canceled contracts.	3.2	3.6	3.9	3.3	3.3	3.8	3.6

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
We have a process in place to periodically require SLA reporting.	2.7	3.6	3.8	2.3	3.2	3.5	3.3
We have a process in place to track and analyze customer complaints.	3.2	3.6	3.6	2.8	3.3	3.4	3.7
We have a process in place to periodically conduct customer satisfaction surveys.	3.0	3.6	3.9	1.7	2.8	3.4	3.2
We have a process in place to respond to, escalate and inform key stakeholders of relevant data security, breaches or other similar incidents.	3.3	3.3	3.4	3.3	3.5	4.1	3.8
We have a process in place to monitor industry and market trends that may negatively impact our vendors.	2.9	2.8	3.5	2.1	3.2	3.5	3.0
We have a process in place to respond to and inform our key stakeholders of regulatory requirements and trends.	3.2	3.7	3.5	2.8	3.2	3.8	3.2
We have a process in place to review applicable audit reports periodically.	3.4	3.8	3.6	3.2	3.5	3.8	3.7
We have a process in place to test our vendors' business continuity and disaster recovery measures periodically, and review the test results.	3.1	3.2	3.3	2.8	2.9	3.6	3.4
We have a process in place to periodically conduct vendor onsite visits and testing.	2.5	3.0	3.3	2.2	3.2	3.6	3.5
We obtain independent assurance or third party testing of key vendors.	2.9	3.6	3.0	3.3	3.5	3.4	2.8

	Assets Under Management						
	< $1B	$1B to $5B	$5B to $10B	$10B to $25B	$25B to $50B	$50B to $250B	> $250B
We have a process in place to regularly assess providers' financial conditions.	2.8	3.5	3.3	3.1	3.6	4.2	3.5
We have a process in place to determine if additional control validation is necessary.	2.6	3.2	3.3	3.0	3.3	3.3	3.4
We have a process in place to determine if an onsite assessment is necessary.	2.8	3.0	3.3	2.6	3.4	3.6	3.6
We have a process in place to determine if an onsite inspection should be performed.	2.6	3.1	3.1	2.6	3.3	3.7	3.5
Category Average	**3.0**	**3.4**	**3.5**	**2.8**	**3.4**	**3.8**	**3.5**

Demographics

Position

Chief Financial Officer	15%
Operational Risk Management	12%
IT Vice President/Director	11%
IT Manager	9%
Procurement/Purchasing/Supply Chain	7%
Chief Audit Executive	6%
Chief Information Officer	5%
Internal Audit Vice President/Director	5%
Internal Audit Manager	4%
IT Audit Manager	3%
Chief Information Security Officer	2%
Chief Risk Officer	2%
Chief Technology Officer	2%
Chief Security Officer	1%
Other	16%

Industry

Financial Services – Banking	21%
Technology (Software/High-Tech/Electronics)	10%
Financial Services – Other	8%
Professional Services	8%
Government	6%
Financial Services – Asset Management	6%

Manufacturing (other than Technology)	5%
Insurance	4%
Retail	3%
Construction	3%
Energy and Utilities	3%
Financial Services – Broker-Dealer	3%
Biotechnology, Life Sciences and Pharmaceuticals	2%
Healthcare Provider	2%
Higher Education	2%
Hospitality, Leisure and Travel	2%
Not-for-Profit	1%
Media and Communications	1%
Agriculture, Forestry, Fishing	1%
Automotive	1%
Healthcare Payer	1%
Real Estate	1%
Consumer Packaged Goods	1%
Transportation and Logistics	1%
Other	4%

- *Size of Organization (outside of Financial Services) – by gross annual revenue in U.S. dollars*

Greater than $20 billion	11%
$10 billion to $19.99 billion	3%
$5 billion to $9.99 billion	11%
$1 billion to $4.99 billion	18%
$500 million to $999.99 million	9%
$100 million to $499.99 million	14%
Less than $100 million	34%

- *Financial Services Industry – Size of Organization (by assets under management)*

Greater than $250 billion	13%
$50 billion to $250 billion	10%
$25 billion to $50 billion	10%
$10 billion to $25 billion	16%
$5 billion to $10 billion	7%
$1 billion to $5 billion	18%
Less than $1 billion	26%

- *Type of Organization*

Public	43%
Private	41%
Government	9%
Not-for-profit	5%
Other	2%

ABOUT SHARED ASSESSMENTS

The Shared Assessments Program is the trusted source in third party risk management, with resources to effectively manage the critical components of the third party risk management lifecycle that are: creating efficiencies and lowering costs for all participants; kept current with regulations, industry standards and guidelines and the current threat environment; and adopted globally across a broad range of industries both by service providers and their customers. Shared Assessments membership and use of the Shared Assessments Program Tools: The Agreed Upon Procedures (AUP); Standardized Information Gathering (SIG) questionnaire and Vendor Risk Management Maturity Model (VRMMM), offers companies and their service providers a standardized, more efficient and less costly means of conducting rigorous assessments for cybersecurity, IT, privacy, data security, and business resiliency controls. The Shared Assessments Program is managed by The Santa Fe Group (www.santa-fe-group.com), a strategic advisory company providing unparalleled expertise to leading financial institutions, healthcare payers and providers, law firms, educational institutions, retailers, utilities and other critical infrastructure organizations. The core of The Santa Fe Group's belief system is that, despite how complicated the world of commerce might be, business can – and should – be a good citizen. Corporations should be built on a foundation to provide greater good to society. We help organizations determine core values, make meaningful connections, facilitate collaboration and affect change. For more information on Shared Assessments, please visit www.sharedassessments.org.

ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

www.sharedassessments.org

protiviti®

www.protiviti.com