SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

protiviti®
Face the Future with Confidence

2019 Vendor Risk Management Benchmark Study: Running Hard to Stay in Place

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

A company's reputation established and nurtured for 100 years can suffer severe and lasting damage following just one high-profile cyber attack. As a result, it can be difficult for boards to feel fully confident in how they are monitoring cybersecurity risk, both within the organization and especially among vendors.

— Scott Laliberte, Managing Director, Global Leader, Security and Privacy Practice, Protiviti

Executive Summary

Increasing pressures in the risk and regulatory environments continue to pose severe challenges to vendor risk management (VRM) programs, often offsetting incremental program improvements over the past 12 months, according to this latest **Vendor Risk Management Benchmark Study** from the Shared Assessments Program and Protiviti.

The results of our study indicate that:

- There is a strong correlation between high levels of board engagement with VRM issues and vendor risk management capabilities that are firing on all cylinders to reach and sustain superior levels of program maturity.
- To varying degrees across all industries, vendor risk management programs are barely able to keep up with the fast pace of change in the external environment.
- Four in 10 organizations have fully mature VRM programs, but just under a third have only ad hoc or no significant VRM processes.
- Resource constraints in the face of higher risk management costs represent one of the largest VRM challenges for organizations.

This marks the fifth 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. During the past year, Shared Assessments updated the VRMMM with 81 new detailed criteria probing more extensively into critical practice components such as continuous monitoring, data management and security, privacy, fourth party risk management, independent program review, and others. All of these items are covered in this year's survey.

Shared Assessments is the trusted source in third party risk assurance 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.

Our Key Findings

01 **The overall maturity of vendor risk management programs is virtually unchanged in the face of an increasingly challenging external risk and regulatory environment.** In aggregate, this year's findings show the overall maturity index for the eight VRMMM categories — as well as overall vendor risk management program maturity — hovers at or near a 3.0 out of 5.0 maturity level. This is despite the addition of new survey criteria and a shift in industry representation among survey participants. This suggests many organizations must work diligently to simply sustain the current performance and sophistication of their VRM programs.

02 **High levels of board engagement correlate with best-in-class VRM maturity.** This finding is critical: Organizations with high levels of board engagement with, and understanding of, vendor risk management issues are more than twice as likely to have VRM programs that are operating at or above target level, compared with organizations that have low levels of board engagement in these issues. Conversely, organizations with low levels of board engagement with VRM are three times as likely as those with high levels of board engagement to have vendor risk management programs that are ad hoc or non-existent. On a more positive note, the number of boards that are highly engaged with vendor risk issues has increased moderately but steadily in each of the past three years, from 26 percent two years ago to 29 percent last year to 32 percent this year. Organizations in the technology, healthcare and manufacturing industries are more likely to report high levels of board engagement. While board engagement is correlated with higher levels of vendor risk management maturity, it is important to keep in mind that a lack of board engagement does not necessarily doom a program. Organizations without VRM-engaged boards can build highly mature vendor risk management programs; doing so just takes more work.

03 **Cyber attack disruptions are increasing, and it is taking organizations longer to fix the underlying issues.** It comes as no surprise that nearly 67 percent more organizations reported that their organizations experienced a significant disruption from a cyber attack or hacking incident compared to respondents who reported similar disruptions in our previous survey. A more troubling cybersecurity issue has also emerged: The percentage of organizations that fixed the issues that led to a successful cyber attack within one month declined by 17 percent. Last year, only 28 percent of respondents reported that these fixes took from three months to one year; this year, 37 percent of respondents reported that fixing the issues that lead to a significant cyber attack required three months to one year.

04 **More organizations are moving away from high-risk vendor relationships.** A majority of organizations — 55 percent — are extremely or somewhat likely to move or exit risky vendor relationships this year, a 2 percent increase compared to last year's survey. This inclination likely represents an improved ability to identify risky vendor relationships as well as a resource constraint in terms of lacking the expertise, technology and funding needed to mitigate these risks in lieu of exiting the relationship altogether.

Our Key Findings (continued)

05 **High vendor risk management costs and a lack of VRM resources are significantly bigger factors among this year's responding organizations.** High costs and low resources represent a pervasive theme throughout the results of this year's study. When assessing their ability to both allocate resources to vendor risk management programs and to optimize those resources, more than one out of three organizations (36 percent) rate their capabilities "well below target level."

New survey measures and analyses

To help risk management professionals succeed in their roles and reflect a risk landscape that has changed significantly, this year's Vendor Risk Management Benchmark survey was revised in important ways. The purpose of the survey, its findings and the accompanying analysis remains the same: to help organizations better address the full vendor assessment relationship lifecycle, from planning a vendor risk management program, to building and capturing assessments, to benchmarking and ongoing evaluation of a program. Now in its fifth year, the survey is based on the comprehensive 2019 version of the Vendor Risk Management Maturity Model (VRMMM) developed by the Shared Assessments Program. The survey was fielded in the fourth quarter of 2018 (see Methodology and Demographics section on page 65 for details). Key changes to this year's survey and how the results were interpreted and presented include:

- **New practice measures:** This year's survey evaluated 81 new practice measures to reflect the updated 2019 VRMMM, which now contains 211 detailed criteria. Many of these new practice areas — including continuous monitoring, virtual assessments and geolocation risks — are part of leading vendor risk management capabilities.
- **New participants:** This year's surveying process was designed to generate feedback from a broader collection of industries and organizations.[1]
- **Additional analyses:** In addition to assessing the average maturity level (of overall respondents and by industry) of key vendor risk management processes according to the VRMMM's 5-point scale, this year's analysis includes an evaluation of responding organizations whose practice measures are *at or above target*, *transitional*, or *well below target*.

Detailed results and benchmarking tables for the eight high-level VRMMM categories can be found beginning on page 37.

[1] As a result of this industry realignment, this year's response from financial services industry organizations was lower than our surveys from prior years. Therefore, unlike in years past, we have not included a breakdown of results by organization size (assets under management) for the industry.

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

Category	2019 Index
Program Governance	2.97
Policies, Standards and Procedures	3.00
Contract Development, Adherence and Management	3.03
Vendor Risk Assessment Process	2.97
Skills and Expertise	2.89
Communication and Information Sharing	2.97
Tools, Measurement and Analysis	2.95
Monitoring and Review	2.93

Vendor Risk Management Maturity Levels, Fully Defined

In this year's Vendor Risk Management Benchmark Study, for each component from the VRMMM, respondents were asked to rate the maturity level as that component applies to their organization, based on the following scale:

5 = Continuous improvement: The organization is striving toward operational excellence, understands what are currently best-in-class performance levels and regularly implements program changes to achieve them.

4 = Fully implemented and operational: The vendor risk management activity is fully operational and all compliance measures are in place.

3 = Fully determined and established: The organization has fully defined, approved and established the vendor risk management activity, but it is not yet fully operational. Metrics and enforcement are not yet fully in place.

2 = Determining roadmap to achieve success: There is a management-approved plan to structure the activity as part of an effort to achieve full program implementation, but the vendor risk management activity is performed on an ad hoc basis.

1 = Initial visioning: The organization is considering how to best structure this activity as part of an effort to achieve full implementation. Vendor risk management activity is performed on an ad hoc basis.

0 = Non-existent: The vendor risk management activity is not performed within the organization.

• • • *Vendor Risk Management — Overall Maturity by Performance Category*

Vendor Risk Management Category	2018 survey year overall results — all VRM components	2018 survey year overall results — VRM components only included in 2017 study	2017 survey year overall results
Program Governance	2.97	2.95	3.01
Policies, Standards and Procedures	3.00	3.02	3.11
Contract Development, Adherence and Management	3.03	3.03	3.11
Vendor Risk Assessment Process	2.97	2.99	3.06
Skills and Expertise	2.89	2.88	2.85
Communication and Information Sharing	2.97	2.96	3.03
Tools, Measurement and Analysis	2.95	2.96	2.90
Monitoring and Review	2.93	3.00	3.12
Average	**2.96**	**2.97**	**3.03**

Note: The addition of 81 new VRM measures did not materially affect category-level scores.

• • • *Vendor Risk Management — Assessing Results by Respondent Role*

Vendor Risk Management Category	C-Level	VP/Director Level	Manager Level
Program Governance	2.97	3.04	2.93
Policies, Standards and Procedures	2.98	3.06	3.00
Contract Development, Adherence and Management	2.99	3.01	3.09
Vendor Risk Assessment Process	2.99	2.99	2.98
Skills and Expertise	3.02	2.95	2.81
Communication and Information Sharing	3.05	3.04	2.92
Tools, Measurement and Analysis	3.02	3.06	2.89
Monitoring and Review	3.02	2.99	2.91
Average	**3.00**	**3.02**	**2.94**

	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
Program Governance	2.97	3.19	3.13	3.29	2.96	3.26	2.76
Policies, Standards and Procedures	3.00	3.17	3.11	3.34	3.05	3.30	2.80
Contract Development, Adherence and Management	3.03	3.08	3.09	3.40	2.96	3.33	2.88
Vendor Risk Assessment Process	2.97	3.13	3.03	3.40	2.98	3.32	2.76
Skills and Expertise	2.89	3.03	3.03	3.23	2.92	3.23	2.68
Communication and Information Sharing	2.97	3.03	3.16	3.32	3.02	3.25	2.77
Tools, Measurement and Analysis	2.95	3.09	3.05	3.40	3.03	3.29	2.72
Monitoring and Review	2.93	2.98	3.03	3.34	3.03	3.25	2.72
Average	**2.96**	**3.09**	**3.08**	**3.34**	**2.99**	**3.28**	**2.76**

Introduction: Striving to Get Off the VRM Treadmill

Consider a silver medal-winning sprinter painstakingly shaving a *tenth* of a second from her personal best (quite an improvement), only to fail to reach the podium because a half-dozen of her competitors boosted their race times by *several tenths* of a second.

Executives responsible for vendor risk management programs will likely wince at this example of the vexing "running harder just to stay in place" dynamic that they increasingly must overcome. Although a vendor risk management strategy of standing pat is never optimal, notching even modest improvements to these crucial capabilities no longer suffices. That's because the speed and magnitude of external risk and regulatory changes continue to intensify, necessitating a robust vendor risk management program that is better resourced and/or better optimizes available resources.

The results of the 2019 Vendor Risk Management Benchmark Study make this vividly clear: The relative maturity level of vendor risk management programs has not changed over the past 12 months despite increased regulatory scrutiny; growing cyber threats at a global, national and state level; and a riskier business environment. At the same time, our findings also point to a number of effective and cost-efficient approaches to get off this treadmill and achieve more substantial VRM progress.

Of particular note, our results reveal two interrelated areas that boards and senior executives should consider when identifying improvement opportunities:

- Strong board of directors' engagement with, and understanding of, vendor risk management issues is critical to achieve and maintain effective risk management; and
- The increasing cost of risk management activities combined with the lack of resources often available to support increasing risk management demands make it essential to optimize those resources that are available.

Higher levels of board engagement with vendor risk management often lead to sufficient resource allocations to those programs: And, as might be expected, lower board engagement is often a characteristic of underperforming vendor risk management programs. A staggering 20 percent of organizations that describe a low level of VRM engagement and understanding at the board level also indicate that their vendor risk management programs are "non-existent."

Getting the most bang from your vendor risk management investments is vital given that risk management, regulatory compliance and an imposing set of external factors all create a higher hurdle than ever for organizations to clear.

Spotlight: Board Perspectives on Vendor Risk Management

There is a strong correlation between high levels of board engagement with cybersecurity issues, both internal and vendor-focused, and vendor risk management capabilities that are optimized to reach and sustain superior levels of program maturity.

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

	2018 survey year	2017 survey year	2016 survey year
High engagement and level of understanding by the board	35%	42%	39%
Medium engagement and level of understanding by the board	42%	38%	37%
Low engagement and level of understanding by the board	17%	14%	17%

Not shown: "Don't know" responses

	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	3.47	2.90	2.31
Policies, Standards and Procedures	3.50	2.91	2.39
Contract Development, Adherence and Management	3.50	3.00	2.28
Vendor Risk Assessment Process	3.47	2.91	2.29
Skills and Expertise	3.39	2.81	2.29
Communication and Information Sharing	3.48	2.87	2.31
Tools, Measurement and Analysis	3.48	2.87	2.27
Monitoring and Review	3.44	2.84	2.31
Average	**3.47**	**2.89**	**2.31**

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

	2018 survey year	2017 survey year	2016 survey year
High engagement and level of understanding by the board	32%	29%	26%
Medium engagement and level of understanding by the board	41%	39%	37%
Low engagement and level of understanding by the board	20%	25%	27%

Not shown: "Don't know" responses

	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	3.54	2.95	2.32
Policies, Standards and Procedures	3.55	2.97	2.39
Contract Development, Adherence and Management	3.55	3.05	2.31
Vendor Risk Assessment Process	3.54	2.95	2.27
Skills and Expertise	3.50	2.83	2.25
Communication and Information Sharing	3.57	2.91	2.27
Tools, Measurement and Analysis	3.55	2.93	2.22
Monitoring and Review	3.52	2.89	2.27
Average	**3.54**	**2.93**	**2.29**

Degree of board engagement with and understanding of vendor-related cybersecurity issues	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
Fully functional and advanced VRM programs (Levels 4 and 5)	57%	37%	25%
Transitional VRM programs (Level 3)	25%	30%	24%
Programs with ad hoc or no VRM activities (Levels 0, 1 and 2)	18%	33%	51%

"This year's findings provide an additional perspective on the compelling relationship between board engagement and third party risk management practice maturity. When board members have a clear understanding of the potential risks that can arise from interactions with physical and digital ecosystem partners, they enable environments where practitioners have the wind at their back."

— Catherine A. Allen, Chairman and President, Shared Assessments Program

External volatility matters

Vendor risk management capabilities must be governed in the context of an increasingly difficult threat environment. Cybersecurity, for example, is a moving target: As companies adopt new technologies, so do hackers.[2] Think back to early 2017 — an eternity ago in cybersecurity terms — when organizations struggled to address their, and their vendors', ransomware defenses in the wake of the NotPetya cyber attack. By December 2017, however, ransomware comprised only 10 percent of infections from external attackers because it was supplanted by *cryptomining* — the infection of organizational computing assets with bitcoin-mining software — which was responsible for as much as 90 percent of all remote code execution attacks by early 2018.[3] Yet, by the end of 2018, information security and vendor risk management professionals had shifted their focus once again, this time to the detection lag that helped make the massive attack of a major global hotel chain so damaging and expensive. The frequency of cyber attacks, the evolving risk of nation-state attacks, and the massive attack surface offered by the ever-expanding universe of Internet of Things devices, among other factors, contribute to a highly volatile external threat environment.

Bad actors are not the only factors that organizations must contend with. A broad range of regulatory bodies are also responding to the external risk environment with new requirements, such as the European Union's General Data Protection Requirement (GDPR) that took effect in May 2018 and the California Consumer Privacy Act that goes into effect in January 2020, as well as the growing focus by numerous regulators (most recently the European Banking Authority, or EBA) on fourth party risk management. And these demands barely scratch the surface of new compliance requirements vendor risk management groups must track and address. Organizations also must comply with the vendor risk management requirements and practices within an alphabet soup of recent and emerging regulatory guidance and rules, including but not limited to NIST 800-53r4, NIST CSF 1.1, FFIEC CAT Tool and PCI 3.2.1.

In addition, vendor risk management teams must continually monitor their own organization's risk management changes and weak spots. "Untrained general (non-IT) staff represents the greatest cybersecurity danger organizational leaders identify, higher than unsophisticated hackers, cyber criminals and social engineers."[4] That explains why many information security and IT groups are devoting more effort to improving pivotal facets of internal cybersecurity — including permission and user access controls, employee security awareness, patch management, system configuration management and periodic penetration testing — that also affect vendor risk management activities. In sum, vendor risk management improvement is a never-ending job.

[2] *The Cybersecurity Imperative: Managing cyber risks in a world of rapid digital change*, ESI Thought Lab, www.protiviti.com/US-en/insights/cybersecurity-imperative.

[3] "Top Cybersecurity Facts, Figures and Statistics for 2018," Josh Fruhlinger, *CSO*, Oct. 10, 2018, www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html.

[4] *The Cybersecurity Imperative: Managing cyber risks in a world of rapid digital change.*

Spotlight: De-Risking

Our results suggest that a majority of organizations are likely to exit their riskiest vendor relationships within a year.

When queried about the reasons for terminating risky vendor relationships, participants in our research reported that difficulties associated with assessing fourth parties is the most important factor, though down from the prior year. One reason for the decline may be related to more outsourcers taking advantage of continuous monitoring's ability to help identify and track fourth parties. The other four measures are all related to cost, and those numbers are all higher than in the past. In fact, in our survey overall, it's clear that cost-related concerns associated with the steadily increasing vendor threat landscape are increasing.

- • • *Over the next 12 months, what is the likelihood that your organization will move to exit or "de-risk" vendor relationships that are determined to have the highest risk?*

	2018 survey year	2017 survey year
Extremely likely	16%	14%
Somewhat likely	39%	39%
Somewhat unlikely	25%	24%
Not at all likely	9%	13%
Don't know	11%	10%

- • • *Which of the following are reasons why your organization may be more inclined to exit or "de-risk" certain vendor relationships? (Multiple responses permitted)*

	2018 survey year	2017 survey year
It's become imperative from a risk and regulatory standpoint to also assess our vendors' subcontractors.	41%	48%
The cost associated to assess our vendors properly is becoming too high.	33%	29%
We lack the internal support and/or skills for the required sophisticated forensic control testing of our vendors.	27%	24%
We do not have the right technologies in place to assess vendor risk properly.	24%	15%
We will not receive sufficient internal support to "de-risk" our vendor relationships.	19%	18%

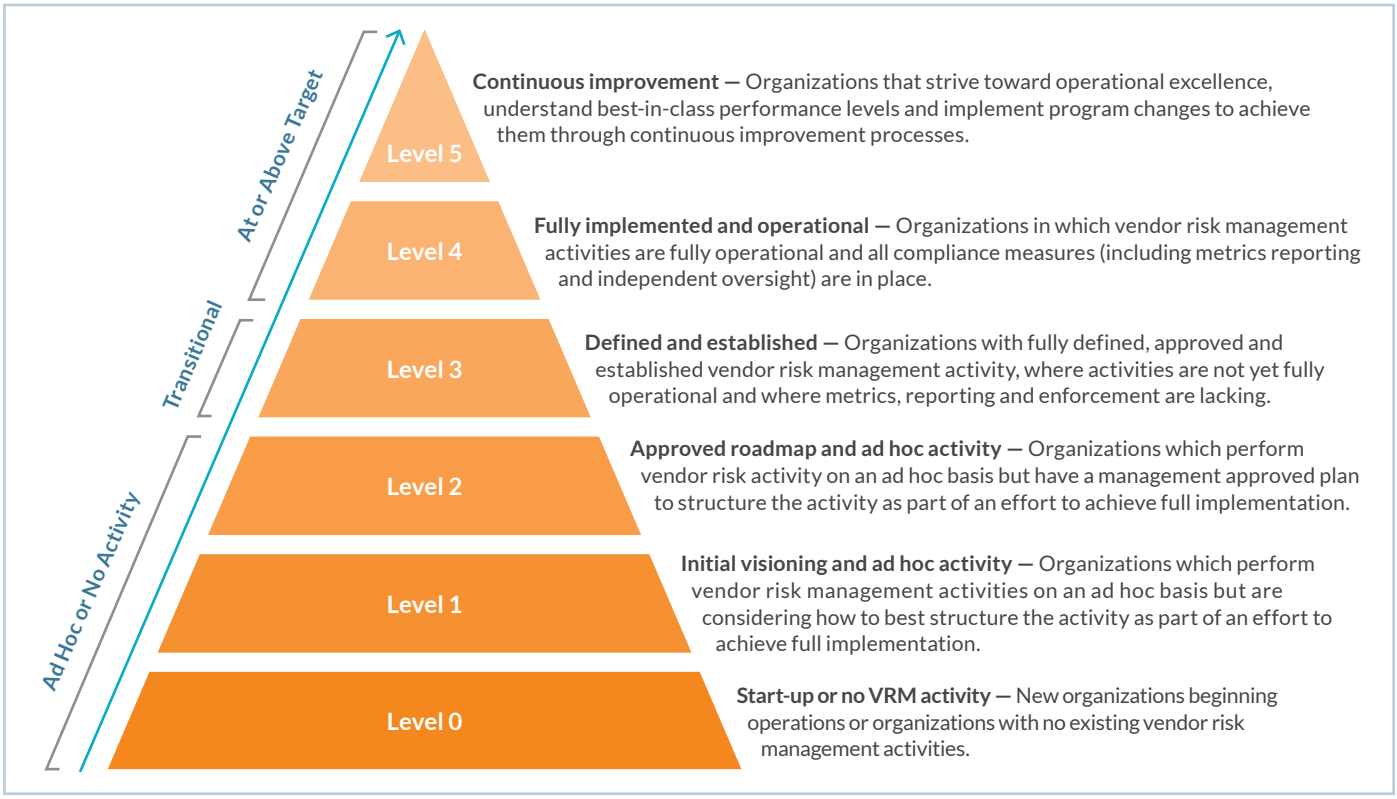
Focus Areas: Getting to Continuous Improvement

In addition to the maturity-level assessments of eight high-level vendor risk management categories (see section beginning on page 37), this year's report features an analysis of 11 new focus areas (see graphic below). Charts describing the individual VRMMM criteria that make up each focus area are included to enable benchmarking.

These areas include processes and approaches that, in the past 18 months or so, have grown increasingly pivotal to the effectiveness (continuous monitoring, fourth party risk management, privacy, resource availability, managing geolocation risk) and/or efficiency (resource optimization, virtual assessments) of VRM programs in most industries. For example, while fourth party risk has been a focal point of financial services industry regulators for years, it has more recently been embraced as a leading vendor risk management practice across many other industries. Continuous monitoring maturity levels, which also were measured for the first time in this year's survey, trail longer point-in-time risk management techniques.

Privacy marks another longstanding component of many vendor risk management programs, especially among healthcare organizations, whose importance has recently soared — in this case, thanks to a far-reaching boost from GDPR requirements that took effect last spring. The GDPR boost appears to have exerted a positive effect on many VRM programs. Privacy practices throughout the survey received the largest portions of "at or above target" maturity evaluations — that is, Level 5: Continuous improvement, or Level 4: Fully implemented and operational — among any of the other focus areas besides vendor criticality (the identification of critical processes and vendors), which 43 percent of all respondents rated at or above target.

• • • *Vendor Risk Management Model Maturity Levels*



At or above target	Level 5: Continuous improvement; or
	Level 4: Fully implemented and operational
Transitional	Level 3: Fully determined and established
Ad hoc or no activity	Level 2: Determine roadmap to achieve success;
	Level 1: Initial visioning; or
	Level 0: Non-existent

Identifying organizations that assigned different maturity levels to a specific practice criteria equips readers of this report with a more precise understanding of how their own capabilities compare to their industry peers. In addition to seeing that, for example, program governance received an average maturity level rating of 2.97 from all survey respondents, readers can also gain a more nuanced view of how many survey respondents rate their fourth party risk management practices (39 percent), continuous monitoring practices (38 percent) or ability to optimize VRM resources (38 percent) at or above target. To facilitate these comparisons, we grouped the five VRMMM maturity levels as follows:

Overall Vendor Risk Management Maturity Snapshot

Percentage of programs at each maturity level (all respondents)

Maturity Level	Percent of Programs		Maturity Group
Continuous improvement (5)	12%	40%	Fully functional and advanced programs/at or above target
Fully implemented and operational (4)	28%		
Fully determined and established (3)	28%	28%	Transitional programs
Determine roadmap to achieve success (2)	17%	32%	Programs with ad hoc or no VRM activity; substantially below target
Initial visioning (1)	7%		
Non-existent (0)	8%		

All organizations strive to avoid the lowest maturity levels and to achieve levels that are at or above target. For that reason, organizations with significant portions of vendor risk management programs at the transitional level often find themselves at a crossroads. In practice, we typically observe two types of VRM programs (or program components) in the transitional stage: those that are upwardly mobile and steadily progressing to Level 4 and Level 5, and those that are treading water. In these situations, program leaders can attempt to engage executive management and the board, demonstrate the extent and consequences of existing vendor risk management effectiveness gaps, and make the case for closing those deltas. If successful, with full management support and with adequate resources in place, program leaders can then close performance gaps to move their program's maturity forward to desired levels. In circumstances where executive management or the board is not immediately responsive, program managers might pursue other options to improve their vendor risk management capabilities (e.g., by hiring an outside expert to assess and recommend the most cost-effective improvements available with current resources, or by enlisting internal audit to weigh in with similar insights).

Regardless of which maturity level an organization's vendor risk management program currently occupies, an important step in elevating that program is benchmarking it against others. In addition to the eight broad VRMMM categories available for that purpose since the survey's inception, this year users can benchmark their programs against each of the following 11 focus areas. Detailed results for each focus area are provided later in this section.

Continuous Monitoring

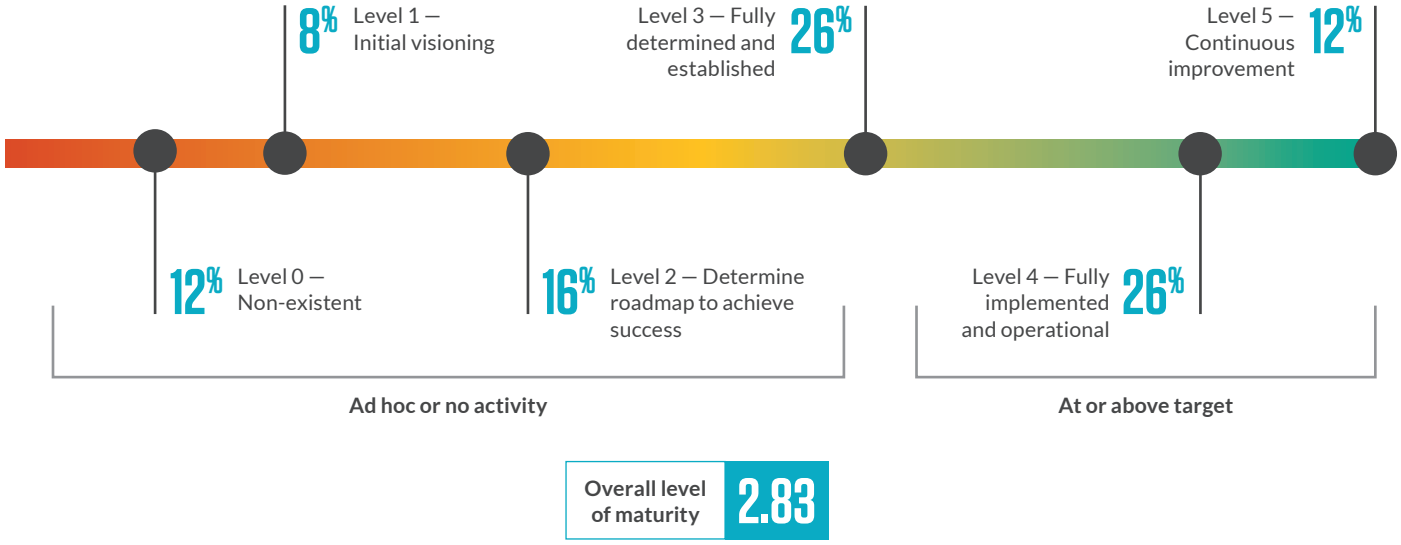
	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
We have established and documented a continuous monitoring program.	2.96	2.87	3.08	3.20	3.09	3.43	2.74
We have a process to monitor external data sources to identify risks resulting from potential litigation regarding our vendors.	2.83	2.84	2.98	3.30	2.90	3.24	2.59
We have a process to monitor external data sources to identify potential risks resulting from changes to the financial viability of our vendors.	2.82	2.87	3.10	3.30	2.87	3.13	2.58
We have a process to monitor external data sources to identify changes to our vendors' business models, strategies, or changes due to mergers and acquisitions.	2.84	2.62	3.02	3.13	3.01	3.27	2.64
We track the timeliness of responses to our vendor information requests as an indicator of potential risk.	2.82	2.65	3.00	3.10	3.10	3.23	2.58
We monitor and track external audit findings across multi-year assessments as an indicator of potential risk.	2.79	2.55	3.00	3.30	2.94	3.15	2.59

Continuous Monitoring (continued)

	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
We monitor and measure the timeliness of vendor response regarding notifications on patches, vulnerabilities and malware to identify potential risks.	2.83	2.82	2.98	3.30	3.07	3.26	2.55
We monitor external data sources to identify our vendor's vendor (fourth party/ subcontractor) relationships.	2.71	2.55	2.92	3.07	2.93	3.17	2.45
We monitor external data sources for reports of complaints to regulators and other industry organizations.	2.77	2.73	2.90	3.27	2.94	3.23	2.51
We have a process to regularly incorporate continuous monitoring outputs to update our vendor risk management program.	2.79	2.75	2.86	3.00	2.86	3.12	2.64
We have a process to respond to issues identified by continuous monitoring activities.	2.92	3.11	2.88	3.13	3.00	3.36	2.70
Average	**2.83**	**2.76**	**2.97**	**3.19**	**2.97**	**3.24**	**2.60**

Continuous Monitoring Maturity Snapshot

Percentage of programs at each maturity level



Overall level of maturity **2.83**

"While point-in-time assessments are still extremely valuable, the ever-changing threat landscape requires a rapid capability to understand your vendor ecosystem risks. The right continuous monitoring capability, tightly integrated into your vendor risk management program, provides valuable information that will allow you to focus on those triggers that indicate there may be trouble ahead."

— Bob Maley, Chief Security Officer, NormShield CyberSecurity

Cybersecurity

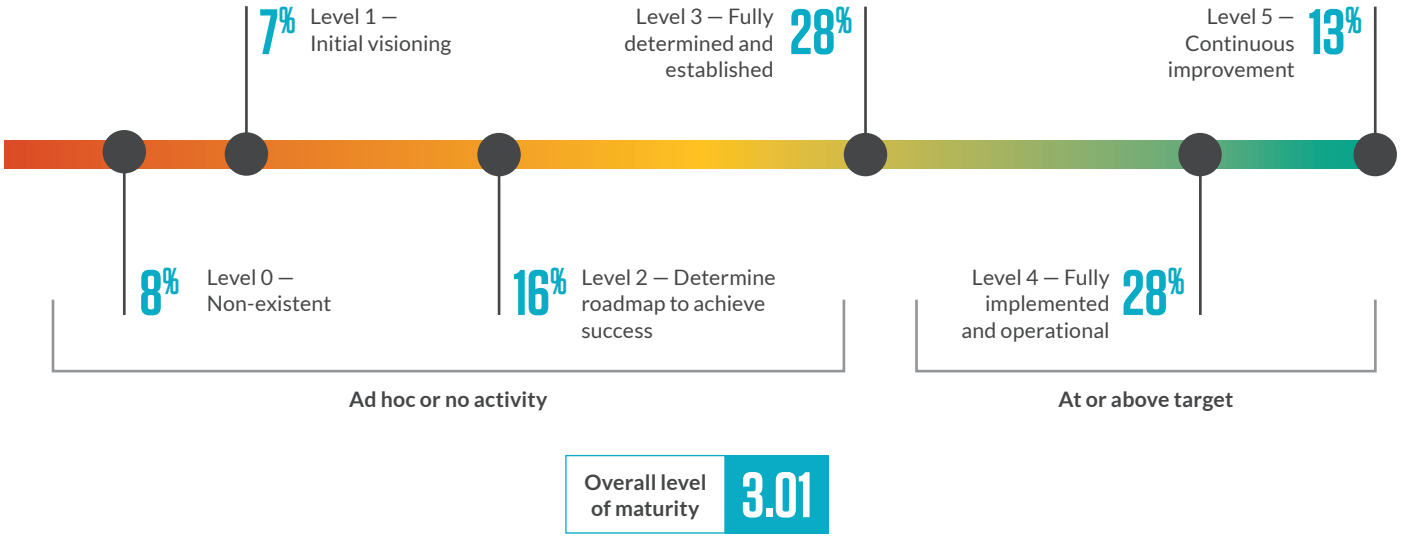
	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
We have developed standards to address minimum cybersecurity or data protection practices at our vendors.	3.08	3.44	3.29	3.23	3.16	3.35	2.83
We have standard contractual language for required security and IT provisions.	3.14	3.40	3.08	3.40	2.96	3.44	3.02
We have a process in place to track and communicate the status of incidents (identification tracking, resolution, consequences).	3.01	3.18	3.12	3.50	3.00	3.30	2.81
We have a process in place to escalate and communicate incidents and issues.	3.07	3.09	3.20	3.40	3.23	3.31	2.88
We establish relevant business risk measures and benchmarks (e.g., reputation, geopolitical, ethics, financial, physical environment, cybersecurity, resilience, compliance, etc.).	2.95	3.07	3.14	3.50	3.06	3.17	2.73
We have a process to respond to issues identified by continuous monitoring activities.	2.92	3.11	2.88	3.13	3.00	3.36	2.70
We have established and documented a process to respond to, escalate and inform key stakeholders of relevant data security breaches or other similar incidents.	3.02	3.33	3.04	3.30	2.89	3.31	2.85

Cybersecurity (continued)

	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
We collect information about IT controls, data protection controls and information security controls.	3.04	3.53	3.02	3.60	3.00	3.38	2.78
We monitor and measure the timeliness of vendor response regarding notifications on patches, vulnerabilities and malware to identify potential risks.	2.83	2.82	2.98	3.30	3.07	3.26	2.55
Average	**3.01**	**3.22**	**3.08**	**3.37**	**3.04**	**3.32**	**2.80**

Cybersecurity Maturity Snapshot

Percentage of programs at each maturity level



Overall level of maturity **3.01**

Fourth Party Risk Management

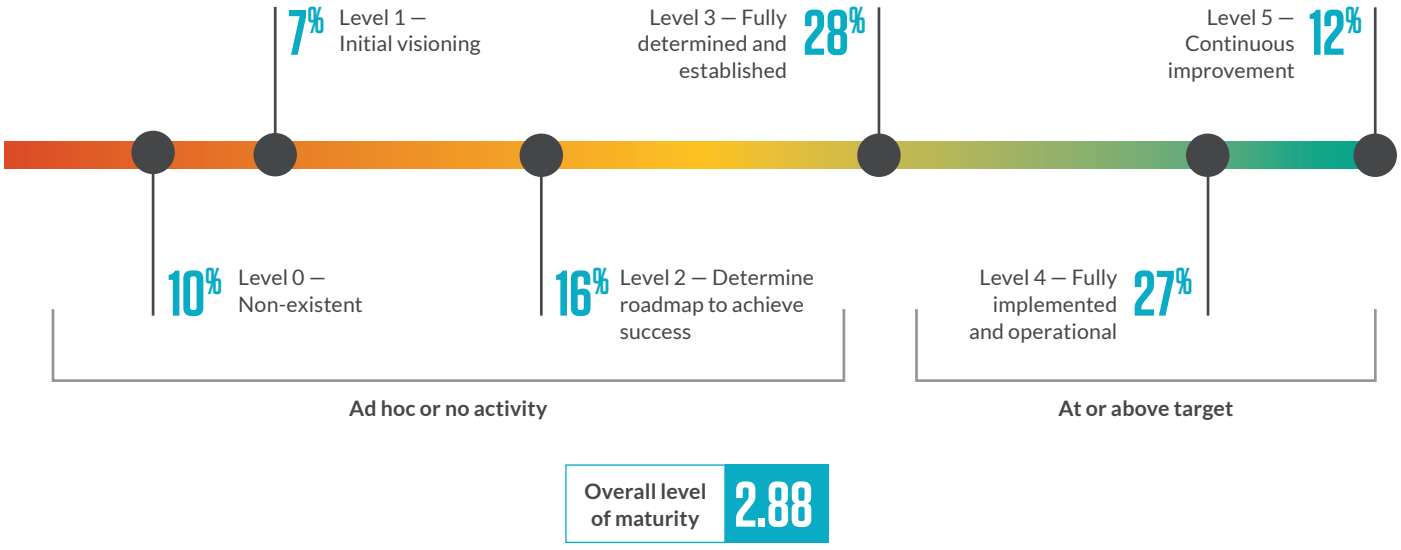
	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
We maintain an inventory of our vendors' vendors (fourth parties/subcontractors).	2.85	2.67	2.86	3.03	3.00	3.22	2.70
We have a process to define the terms, if any, under which vendor outsourcing to subcontractors/fourth parties is permissible.	3.01	3.13	2.82	3.33	2.81	3.40	2.91
We have included provisions to address notification of changes related to our vendor's vendors (fourth parties/subcontractors).	2.98	3.11	3.06	3.47	2.93	3.35	2.78
We have an established and documented procedure for extension of contract obligations to our vendor's vendors (subcontractors/ fourth parties).	2.92	2.78	3.12	3.30	2.81	3.34	2.75
We collect information about vendors' vendor relationships.	2.89	3.13	2.88	3.40	2.91	3.31	2.63
We have a process in place to determine if a vendor uses subcontractors/fourth parties if the vendor's contract does not include vendor outsourcing requirements.	2.84	3.02	2.96	3.17	2.81	3.22	2.63

Fourth Party Risk Management (continued)

	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
We monitor external data sources to identify our vendor's vendor (fourth party/ subcontractor) relationships.	2.71	2.55	2.92	3.07	2.93	3.17	2.45
Average	**2.88**	**2.91**	**2.94**	**3.25**	**2.89**	**3.29**	**2.69**

Fourth Party Risk Management Maturity Snapshot

Percentage of programs at each maturity level



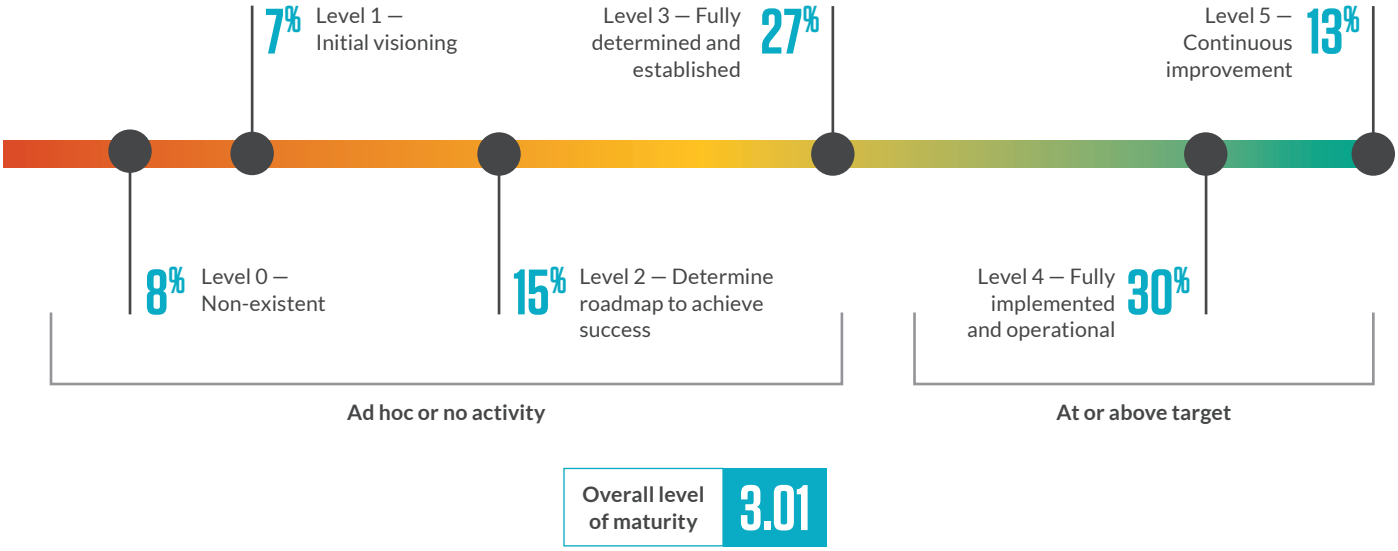
Overall level of maturity **2.88**

Vendor Risk Management Privacy Practices

	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
We have a process to require data destruction/secure disposal and/or the return of confidential data and other designated assets when a vendor agreement is terminated.	3.00	2.95	3.18	3.27	3.01	3.24	2.87
We have included provisions to address the authorized use, limitations, processing and retention of data based on its classification.	3.08	3.18	3.33	3.37	3.07	3.35	2.89
We collect information about data classifications and locations.	2.97	3.20	2.90	3.53	2.99	3.44	2.71
We collect information about IT controls, data protection controls and information security controls.	3.04	3.53	3.02	3.60	3.00	3.38	2.78
We have a process to obtain and assess confidentiality commitments, consistent with the organization's requirements, from vendors with access to confidential personal information.	2.99	3.38	2.98	3.47	3.00	3.24	2.76
We have a process to obtain and assess, on both a periodic and as-needed basis, privacy commitments of vendors with access to confidential personal information including corrective action if required.	3.01	3.42	3.12	3.40	2.86	3.33	2.79
Average	**3.01**	**3.28**	**3.09**	**3.44**	**2.99**	**3.33**	**2.80**

Vendor Risk Management Privacy Maturity Snapshot

Percentage of programs at each maturity level



Overall level of maturity **3.01**

"In our annual Internal Audit Capabilities and Needs Survey, we regularly see vendor risk management ranking among the top priorities to address in the organization's annual audit plan. Assessing vendors in numerous areas, including but not limited to regulatory compliance, data security and cyber risk practices, is a critical mandate for internal audit functions, underscoring the vital importance of a strong vendor risk management program."

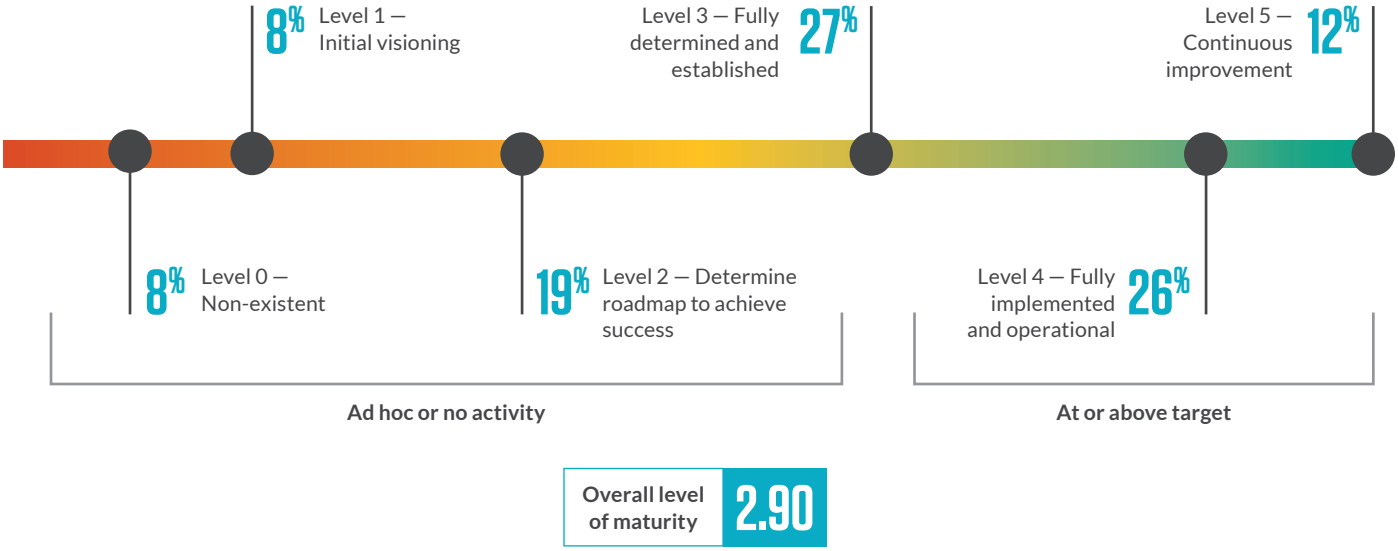
— Brian Christensen, Executive Vice President, Global Leader, Internal Audit and Financial Advisory

Resource Allocation Practices

	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
We have allocated enough resources for vendor risk management activities.	2.97	3.15	3.14	3.30	2.97	3.29	2.75
We have enough staff to manage vendor risk management activities effectively.	2.89	3.13	3.22	3.17	2.81	3.13	2.70
We have enough qualified staff to meet all vendor risk management objectives.	2.90	3.02	2.86	3.00	3.00	3.28	2.73
We have competent personnel with enough authority to perform vendor control assessments and interpret vendor responses.	3.05	3.29	3.00	3.30	3.24	3.34	2.83
We have sufficient funding for vendor management training and awareness as set by policy.	2.84	3.00	3.31	3.00	2.69	3.22	2.63
We have allocated budget for vendor risk management functions, including basic travel, subscriptions, training and small projects.	2.81	3.00	3.00	3.07	2.83	3.23	2.57
We allocate a specific vendor risk management budget for industry memberships and training/education to accomplish its objectives.	2.81	2.93	3.16	3.07	2.79	3.13	2.60
Average	**2.90**	**3.07**	**3.10**	**3.13**	**2.90**	**3.23**	**2.69**

Resource Allocation Maturity Snapshot

Percentage of programs at each maturity level



Overall level of maturity **2.90**

"While third-party monitoring is improving, serious risks continue due to location factors such as political unrest, weather, law changes and legislation. The World Economic Forum identified Location Risk as a top concern, and market analysis concludes that real-time, continuous location monitoring is a critical component of any third-party risk program."

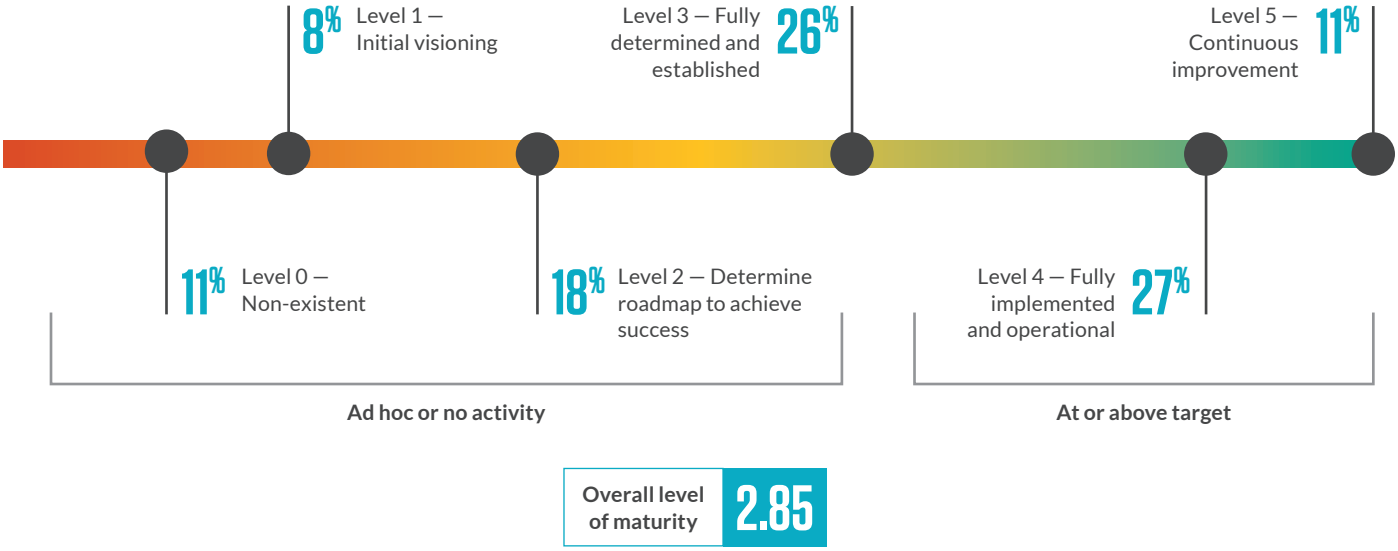
— John Bree, SVP and Partner, NEO Group

Resource Optimization Practices

	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
We have structures in place to define and measure the staffing levels required to meet vendor risk program requirements.	2.85	2.91	3.02	3.07	2.84	3.09	2.71
We have established and documented our governance programs so that staffing levels can be adjusted due to optimization.	2.81	2.64	2.67	3.03	2.83	3.34	2.67
We routinely measure or benchmark our vendor risk management budget with management reporting to demonstrate the return on investment.	2.76	2.44	3.08	2.90	2.84	3.23	2.58
We have sufficiently integrated our vendor risk management functions and tools into business lines so that overall costs and budget for dedicated risk management budgets are reduced.	2.82	2.80	3.20	2.93	2.91	3.21	2.59
We assign resources to accomplish reviews as scheduled.	3.00	3.25	3.08	3.57	3.03	3.37	2.75
Average	**2.85**	**2.81**	**3.01**	**3.10**	**2.89**	**3.25**	**2.66**

Resource Optimization Maturity Snapshot

Percentage of programs at each maturity level



Overall level of maturity **2.85**

"Keeping pace with regulatory change has become an essential vendor risk management skill as even regulations outside of financial services have become more prescriptive. The GDPR and California Consumer Privacy Act are two recent examples. Organizations that anticipate new regulations can eliminate last-minute compliance issues and enjoy more thoughtful business system integration."

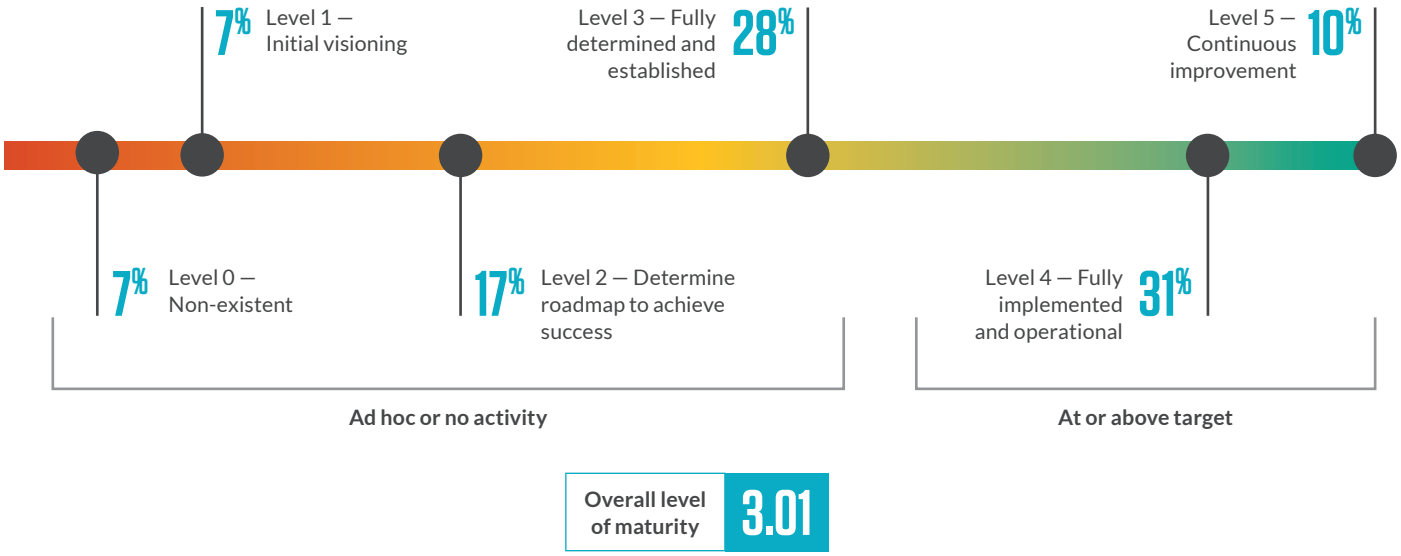
— Gary Roboff, Senior Advisor, The Shared Assessments Program

Assessing Vendor Criticality

	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
We have identified critical processes and vendors.	3.12	3.40	3.00	3.73	3.20	3.41	2.89
We have established exception criteria based on vendor criticality.	2.90	3.04	2.98	3.17	3.00	3.30	2.66
Average	**3.01**	**3.22**	**2.99**	**3.45**	**3.10**	**3.35**	**2.78**

Assessing Vendor Criticality Maturity Snapshot

Percentage of programs at each maturity level



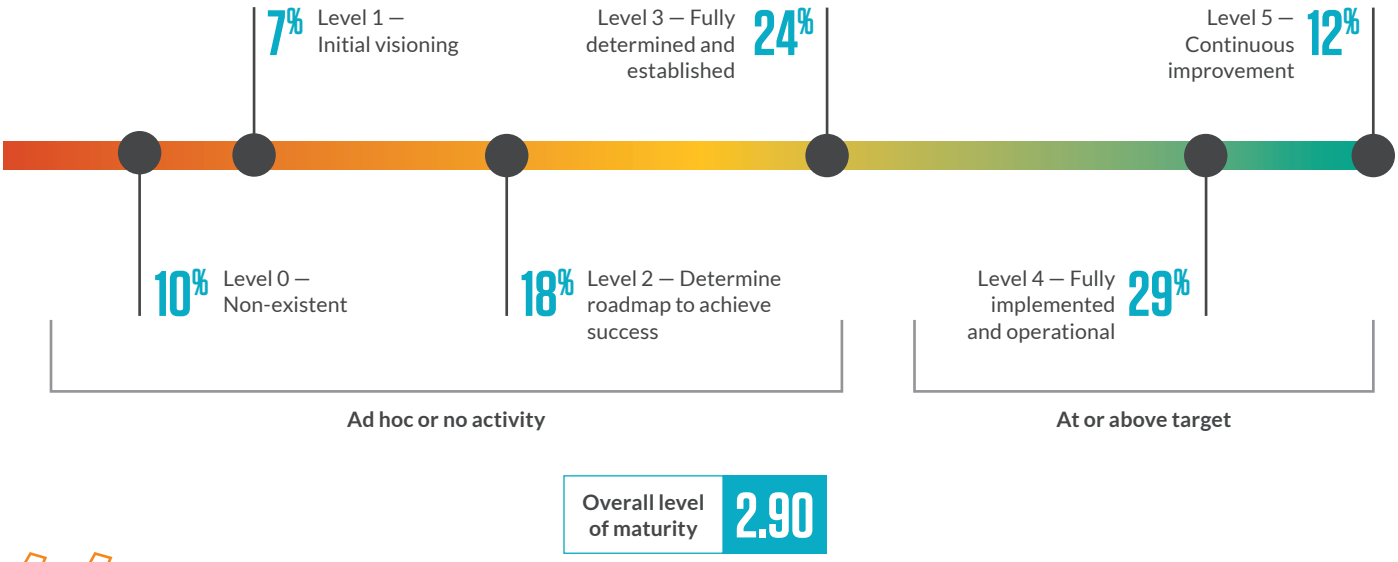
Overall level of maturity **3.01**

Performing Virtual Assessments

	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
We have established and documented a formalized process for conducting virtual assessments.	2.90	2.73	3.02	3.20	3.06	3.38	2.67

Performing Virtual Assessments Maturity Snapshot

Percentage of programs at each maturity level



Overall level of maturity **2.90**

"Virtual assessments enable rigorous evaluations following standardized control and test procedures to provide testing assurance with evidence in a way that is efficient for both service providers and outsourcers."

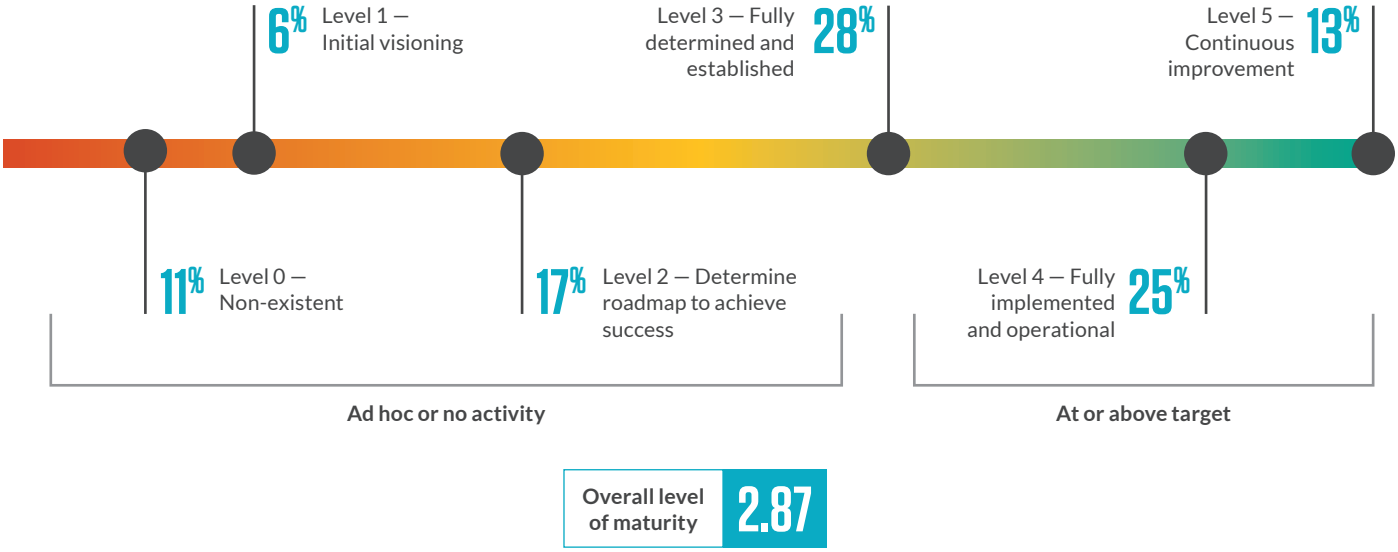
— Linnea Solem, CEO and Founder, Solem Risk Partners LLC

Assessing Geolocation Risk

	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
We have developed standards to address cross-border or geolocation risks at our vendors.	2.77	2.75	2.90	3.13	2.94	3.29	2.50
We collect information about data classifications and locations.	2.97	3.20	2.90	3.53	2.99	3.44	2.71
Average	**2.87**	**2.97**	**2.90**	**3.33**	**2.96**	**3.37**	**2.60**

Assessing Geolocation Risk Maturity Snapshot

Percentage of programs at each maturity level



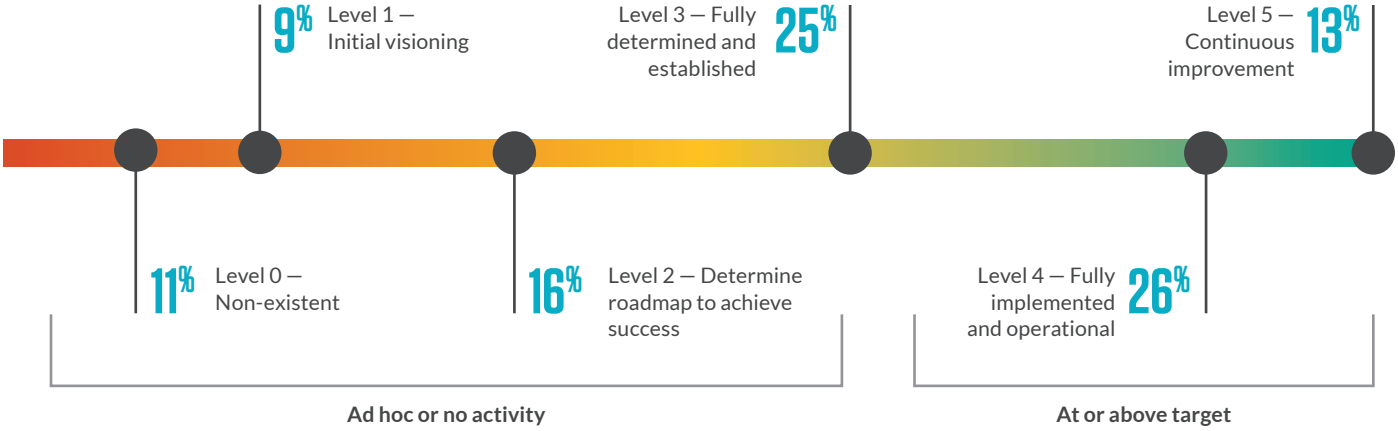
Overall level of maturity **2.87**

Resiliency

	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
We have established and documented a process to periodically review our program's effectiveness in reviewing and testing our vendors' business continuity and disaster recovery measures, and our use of those test results.	2.85	3.05	2.98	3.07	3.09	3.16	2.59

Resiliency Maturity Snapshot

Percentage of programs at each maturity level



Overall level of maturity **2.85**

Regulatory Change and Compliance

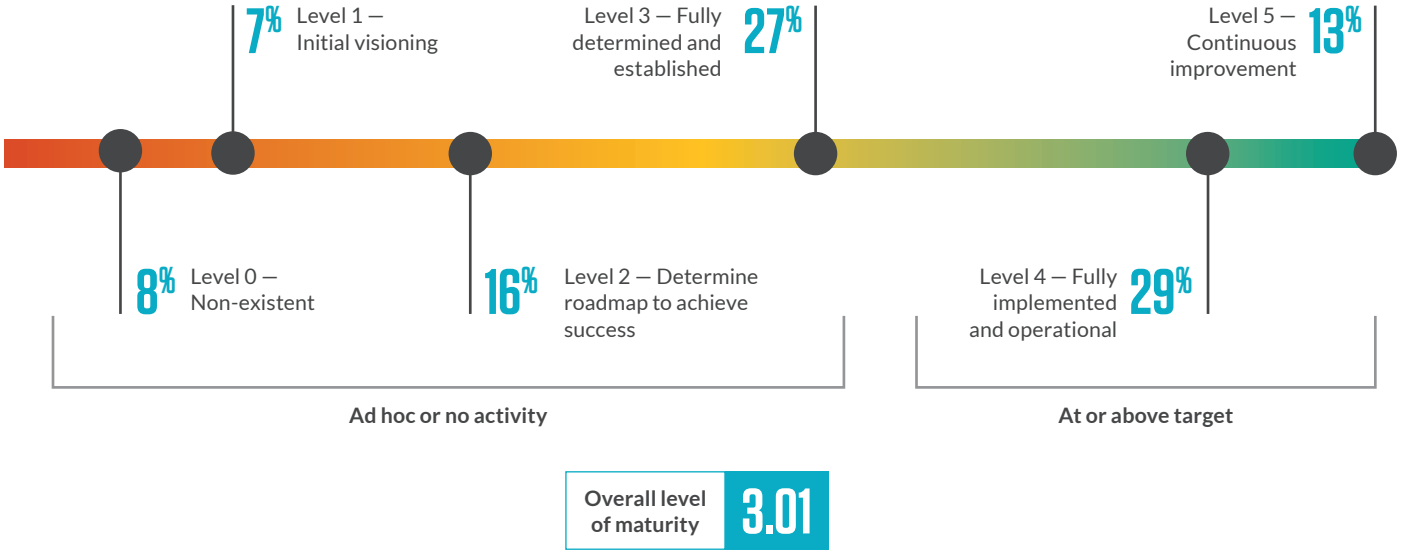
	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
We have established and documented a process to monitor industry and external changes to the regulatory, economic and physical environment that may negatively impact our vendors.	2.97	3.18	2.90	3.60	2.97	3.20	2.80
There is a process in place to periodically monitor regulatory changes applicable to our business, products and services.	3.06	3.25	3.14	3.43	3.07	3.30	2.88
We have established and documented a process to respond to and inform our key stakeholders of regulatory requirements, trends and changes.	3.00	3.20	2.98	3.53	3.01	3.45	2.75
We have defined and documented the roles to monitor changes to the regulatory landscape and to identify and recommend updates to our vendor risk management program.	2.97	3.25	3.04	3.63	3.06	3.44	2.65
We have standard contractual language for provisions required by regulators.	3.04	3.36	3.02	3.40	3.10	3.27	2.85

Regulatory Change and Compliance (continued)

	Overall	Financial Services	Healthcare Provider	Insurance/ Healthcare Payer	Manufacturing	Technology	All other industries
We have a process to monitor and review required changes in regulatory compliance or industry standards to update our third party risk oversight program.	3.02	3.09	3.18	3.33	2.97	3.36	2.84
We have defined vendor management policies that include risk management, security, privacy, regulatory compliance and other areas that are in alignment with our existing organizational policies and objectives.	3.03	3.35	3.33	3.30	2.94	3.26	2.83
Average	**3.01**	**3.24**	**3.08**	**3.46**	**3.02**	**3.33**	**2.80**

Regulatory Change and Compliance Maturity Snapshot

Percentage of programs at each maturity level



Overall level of maturity **3.01**

Final Thoughts: Working Smarter

Sprinting just to stay in place is extremely frustrating. Evading that trap is becoming more difficult for leaders of vendor risk management programs because of rapidly changing risk and regulatory environments. The challenge is formidable, but it can be overcome: 40 percent of organizations that participated in this year's Vendor Risk Management Benchmarking Study boast maturity performance at or above a target level of 4. This benchmark study and the Vendor Risk Management Maturity Model on which it is based provide an ideal overview of the key practice components that should be part of any fully implemented VRM program. Optimizing available resources by regularly honing current vendor risk management processes is an increasingly essential element in any successful program. Utilize the VRMMM to focus your review on individual program components, and put it to good use.

> The threat landscape is evolving daily, and new risk vectors — from nation state bad actors, data thefts and high-impact cyber attacks to business model viability and regulatory non-compliance — are making comprehensive vendor risk management programs all the more crucial to organizational stability and continuity.
>
> — Paul Kooney, Managing Director, Security and Privacy Practice, Protiviti

Benchmarking Detail: VRM Study Results

Program Governance

Overall level of maturity: 2.97

• • • *Program Governance — Overall Results*

	Vendor Risk Component	2018
	Formalized Vendor Risk Governance Model/Structure	
1	We define organizational structures that establish responsibility and accountability for overseeing our vendor relationships.	2.88
2	The organizational structure of our vendor risk management program operates independently of our business lines.	2.80
3	We have established a formal program review schedule.	2.93
4	We have defined specific requirements for vendor engagements based on the scope of service and product specifications.	3.01
4.1	We have defined specific requirements for vendor and business partner engagements.	3.04
4.2	We have defined service level agreements as required for vendor and business partner engagements.	2.99
5	We have defined specific requirements for roles and responsibilities for functions that perform vendor risk management activities.	2.99
6	We have defined the criteria to ensure the independence of our program components.	2.98
7	We have defined the criteria for program certification requirements.	2.81
	Defined Program Objectives and Goals	
8	We have articulated the goals and objectives of our organization.	3.10
9	We have aligned specific vendor management objectives with our strategic organizational objectives.	2.92
10	We have defined vendor management policies that include risk management, security, privacy, regulatory compliance and other areas that are in alignment with our existing organizational policies and objectives.	3.03

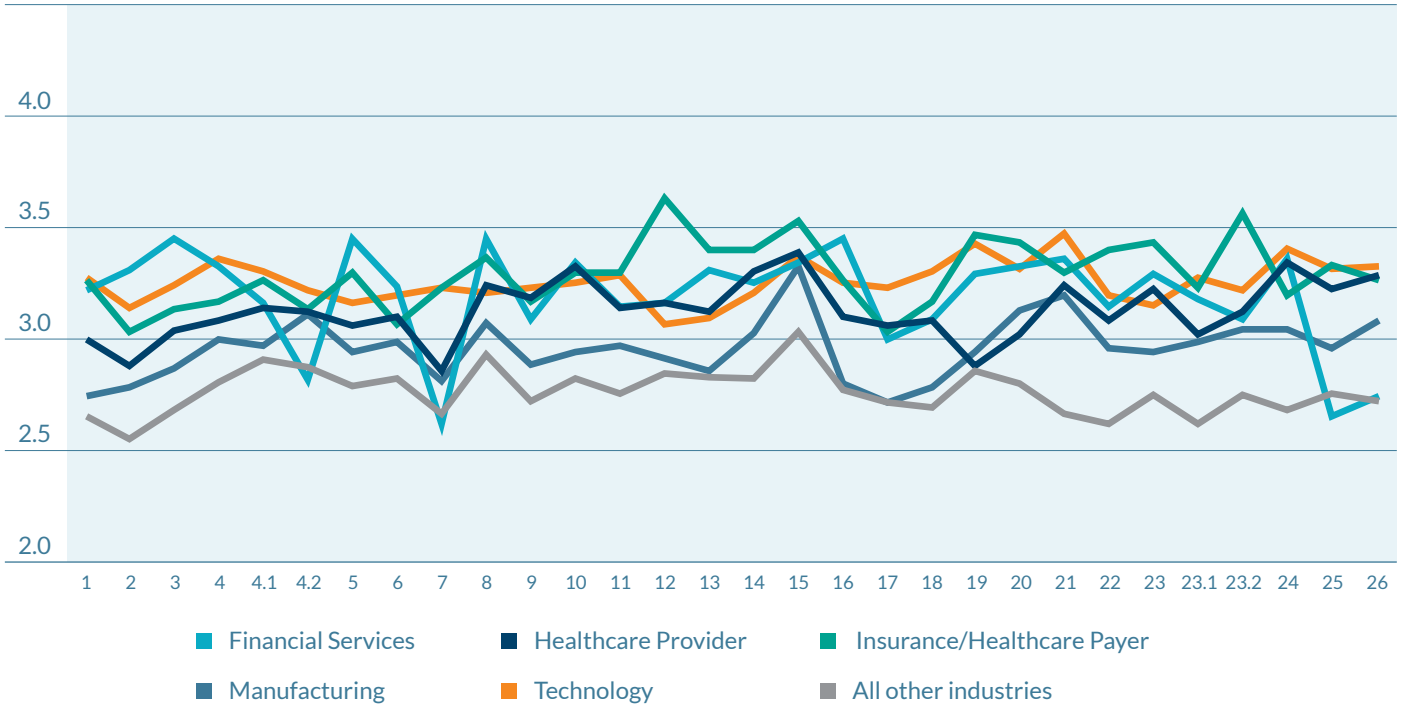
	Vendor Risk Component	2018
11	We have allocated enough resources for vendor risk management activities.	2.97
12	We have established compliance requirements and service levels for vendor and business partner engagements.	2.99
13	We have established specific requirements for vendor engagements based on the scope of service and product specifications.	2.98
14	We have defined requirements for addressing issue management within vendor engagement.	3.03
15	We maintain a complete inventory of new and existing vendors.	3.21
	Established Risk Posture	
16	We have communicated the requirements for risk-based vendor management to our organization.	2.97
17	We have determined the business value expected from our outsourced business relationships, based on understanding the range of business risks our organization is willing to assume.	2.87
18	We have a process to determine that accepted risks in outsourced business relationships are aligned with our vendor risk management policy.	2.90
19	We have defined risk monitoring practices and established an escalation process for exception conditions.	3.04
20	We maintain a documented risk management methodology for third party risk.	3.03
21	We have assigned responsibility and accountability for ongoing management of risks associated with vendors.	3.09
	Board Reporting and Management Oversight	
22	We evaluate key risk and performance indicators provided in management and board reporting.	2.92
23	We have established a formalized schedule for management and board reporting.	2.93
23.1	We have defined processes for reporting material changes in vendor risk to our board and executive management.	2.89
23.2	We have established and maintain processes for periodic risk updates of issues based on corrective actions.	2.97
24	We revise our organization's vendor risk management policy as needed to achieve strategic objectives.	2.99

	Vendor Risk Component	2018
	Standards of Conduct	
25	We have established standards of conduct applicable to vendors which have been provided to, and are understood by, outsourcing partners.	2.93
26	Our management has considered the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing exceptions in a timely manner.	2.94
	Category Average	**2.97**

• • • *Program Governance — Maturity and Board Engagement*

Degree of board engagement with and understanding of vendor-related cybersecurity issues	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
Fully functional and advanced VRM programs (Levels 4 and 5)	56%	35%	24%
Transitional VRM programs (Level 3)	26%	32%	24%
Programs with ad hoc or no VRM activities (Levels 0, 1 and 2)	18%	33%	52%

• • • *Program Governance — Industry Results*



Policies, Standards and Procedures

Overall level of maturity: 3.00

• • • *Policies, Standards and Procedures — Overall Results*

	Vendor Risk Component	2018
	Vendor Risk Management Policy and Risk Categorization	
1	We have a defined vendor risk management policy.	3.04
2	We have defined vendor risk management categories.	2.99
3	We have defined criteria for vendor criticality.	3.08
4	We have obtained senior management and/or board approval of our policies and risk categories.	3.05
	Vendor Inventory Requirements	
5	We have established and maintain complete vendor inventory requirements.	3.04
5.1	We maintain an inventory of vendors based on scope of service and product specification.	3.12
5.2	We maintain an inventory of our vendors' vendors (fourth parties/subcontractors).	2.85
5.3	We have identified critical processes and vendors.	3.12
5.4	We have defined data classification and data flow requirements.	3.08
	Vendor Due Diligence Standards	
6	We have established vendor due diligence standards.	3.01
6.1	We have developed standards to address reputation and strategic risk at our vendors.	2.91
6.2	We have developed standards to address financial or credit risk at our vendors.	3.06
6.3	We have developed standards to address cross-border or geolocation risks at our vendors.	2.77

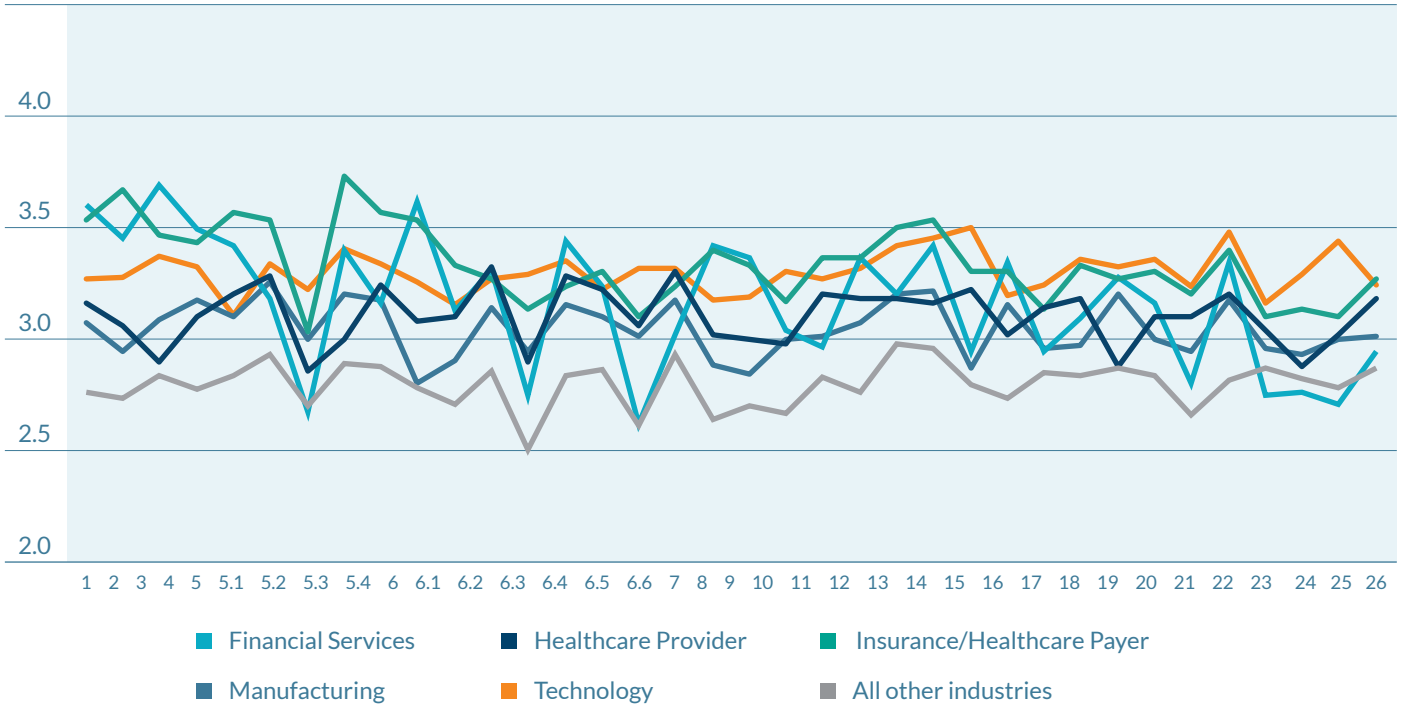
	Vendor Risk Component	2018
6.4	We have developed standards to address minimum cybersecurity or data protection practices at our vendors.	3.08
6.5	We have developed standards based on service, activity and/or product specifications.	3.04
6.6	We have developed standards to address concentration risk.	2.84
7	We have created a vendor selection process.	3.08
	Vendor Classification Operational Procedures	
8	We have defined a vendor classification structure based on risk categories.	2.90
9	We have defined risk categories for each classification in our vendor classification structure.	2.92
10	We have established exception criteria based on vendor criticality.	2.90
	Contract Management Governance	
11	We have identified existing company policies that may affect our contracting process.	3.00
12	We have identified the key stakeholder functions engaged in structuring our contracting process.	3.01
13	We have created a process for managing contracts.	3.14
14	We have identified the key positions involved in our contract management process.	3.16
15	We have established criteria for vendor exit strategies.	2.99
	Vendor Management Procedures	
16	We have implemented procedures for addressing issues found in vendor assessments.	2.97
17	We have established procedures for data destruction, portability and/or retention during the contract lifecycle.	2.97
18	We have a process to monitor and review required changes in regulatory compliance or industry standards to update our third party risk oversight program.	3.02
19	We have an escalation process for issues identified at our vendors.	3.04

	Vendor Risk Component	2018
20	We have a procedure for vendor incident notification and reporting that is periodically revised to achieve our strategic objectives.	3.02
21	We have established requirements for exit strategies based on our vendor risk classifications.	2.87
22	We have defined and documented criteria for ongoing monitoring activities.	3.08
	Vendor Termination or Exit Procedures	
23	We have defined criteria for the termination of vendor relationships, including exception processes.	2.94
24	We have defined termination and exiting procedures including timelines for vendor notification of termination.	2.92
25	We have a process to define a vendor's transitional service obligations when an agreement terminates.	2.94
26	We have a process to require data destruction/secure disposal and/or the return of confidential data and other designated assets when a vendor agreement is terminated.	3.00
	Category Average	**3.00**

• • • *Policies, Standards and Procedures — Maturity and Board Engagement*

Degree of board engagement with and understanding of vendor-related cybersecurity issues	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
Fully functional and advanced VRM programs (Levels 4 and 5)	57%	37%	26%
Transitional VRM programs (Level 3)	26%	32%	26%
Programs with ad hoc or no VRM activities (Levels 0, 1 and 2)	17%	31%	48%

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



Contract Development, Adherence and Management

Overall level of maturity: 3.03

• • • *Contract Development, Adherence and Management — Overall Results*

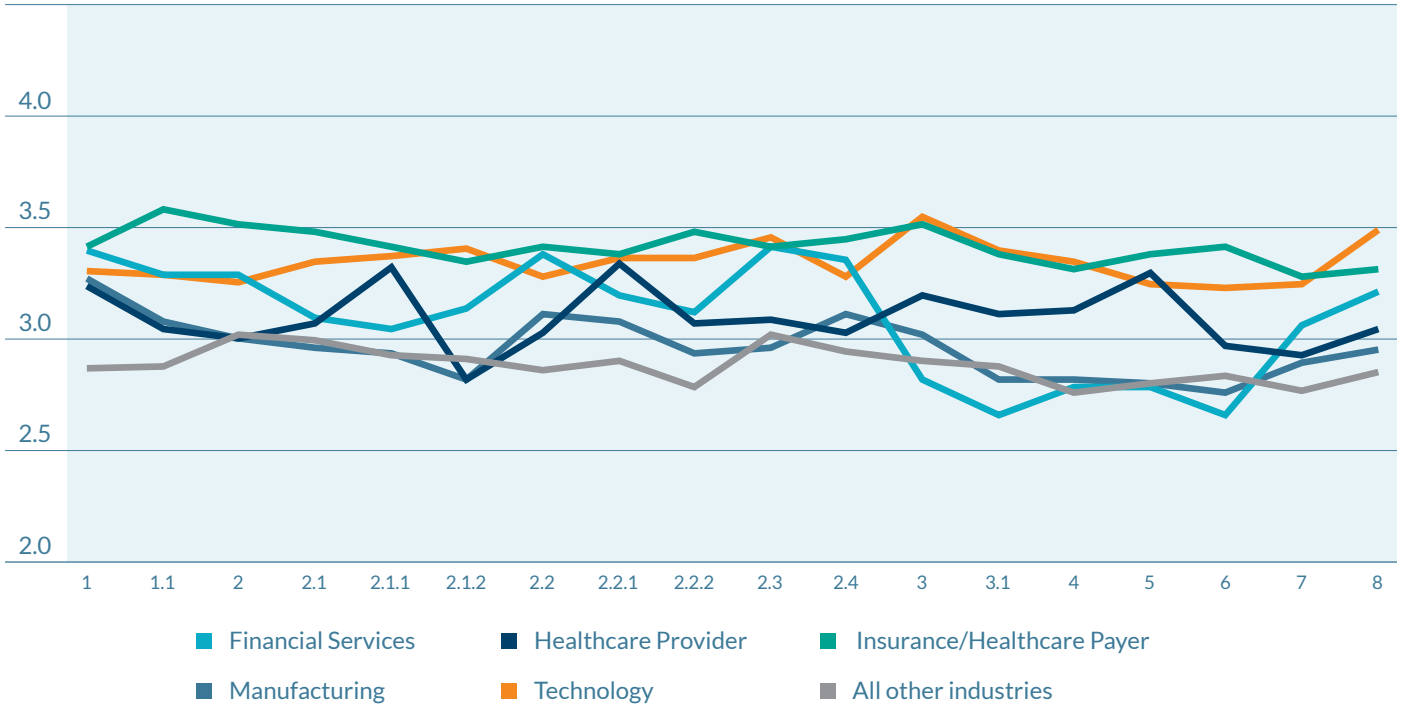
	Vendor Risk Component	2018
	Vendor Contract Management Operational Procedures	
1	We have defined an organizational structure for vendor contract drafting, negotiation and approval.	3.09
1.1	We have established and documented procedures for contract exception review and approval.	3.05
2	We have established and documented standards for mandatory contract language/provisions.	3.10
2.1	We have organizational requirements for mandatory contract language/provisions.	3.08
2.1.1	We have a process to ensure inclusion of contract provisions terminating a vendor relationship.	3.06
2.1.2	We have a process to define the terms, if any, under which vendor outsourcing to subcontractors/fourth parties is permissible.	3.01
2.2	We have standard contractual language for provisions required by regulators.	3.04
2.2.1	We have included provisions to address the authorized use, limitations, processing and retention of data based on its classification.	3.08
2.2.2	We have included provisions to address notification of changes related to our vendor's vendors (fourth parties/subcontractors).	2.98
2.3	We have standard contractual language for required security and IT provisions.	3.14
2.4	We have standard contractual language for required audit/inspection provisions.	3.08
3	We have an established and documented procedure to review existing contracts for compliance with our current contract standards.	3.06
3.1	We have an established and documented remediation process to correct contract deficiencies.	2.97
4	We have an established and documented procedure for extension of contract obligations to our vendor's vendors (subcontractors/fourth parties).	2.92

	Vendor Risk Component	2018
	Criteria/Guidelines for Standard Contract Provisions	
5	We have an established and documented process to ensure inclusion of appropriate performance-based contract provisions (service level agreements, key performance indicators, key risk indicators, etc.).	2.94
6	We have an established and documented process to ensure inclusion of contract provisions consistent with each vendor risk classification/rating.	2.91
7	We have established and documented criteria for the contract review cycle consistent with each vendor risk classification/rating.	2.92
8	We have an established and documented process, including designated authority levels, to approve contract exceptions based on risk.	3.03
	Category Average	**3.03**

• • • *Contract Development, Adherence and Management — Maturity and Board Engagement*

Degree of board engagement with and understanding of vendor-related cybersecurity issues	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
Fully functional and advanced VRM programs (Levels 4 and 5)	57%	40%	26%
Transitional VRM programs (Level 3)	26%	31%	24%
Programs with ad hoc or no VRM activities (Levels 0, 1 and 2)	17%	29%	50%

• • • *Contract Development, Adherence and Management — Industry Results*



Vendor Risk Assessment Process

Overall level of maturity: 2.97

• • • *Vendor Risk Assessment Process — Overall Results*

	Vendor Risk Component	2018
	Vendor Risk Assessment Approach	
1	We have reviewed the defined business requirements for outsourcing.	2.95
2	We conduct a risk assessment for outsourcing any business function.	2.97
3	We have established and documented a process to evaluate concentration risk in our vendor relationships.	2.91
4	We identify specific risks to be tracked or monitored.	3.04
	Vendor Assessment and Classification	
5	We maintain a database of vendor information.	3.28
6	We maintain a process to collect and update vendor information.	3.32
7	We execute vendor risk tiering and classification processes.	3.06
8	We determine vendor assessments to be performed based on risk categories or tiers, and resource availability.	3.05
9	We have identified compliance obligations that extend to each vendor.	3.12
	Vendor Assessment Operational Processes	
10	We have executed a defined and structured vendor risk management process throughout the complete vendor lifecycle.	2.97
10.1	We formally document specific assessment roles and responsibilities.	3.05
10.2	We have established and documented a formalized process for conducting onsite assessments.	2.94

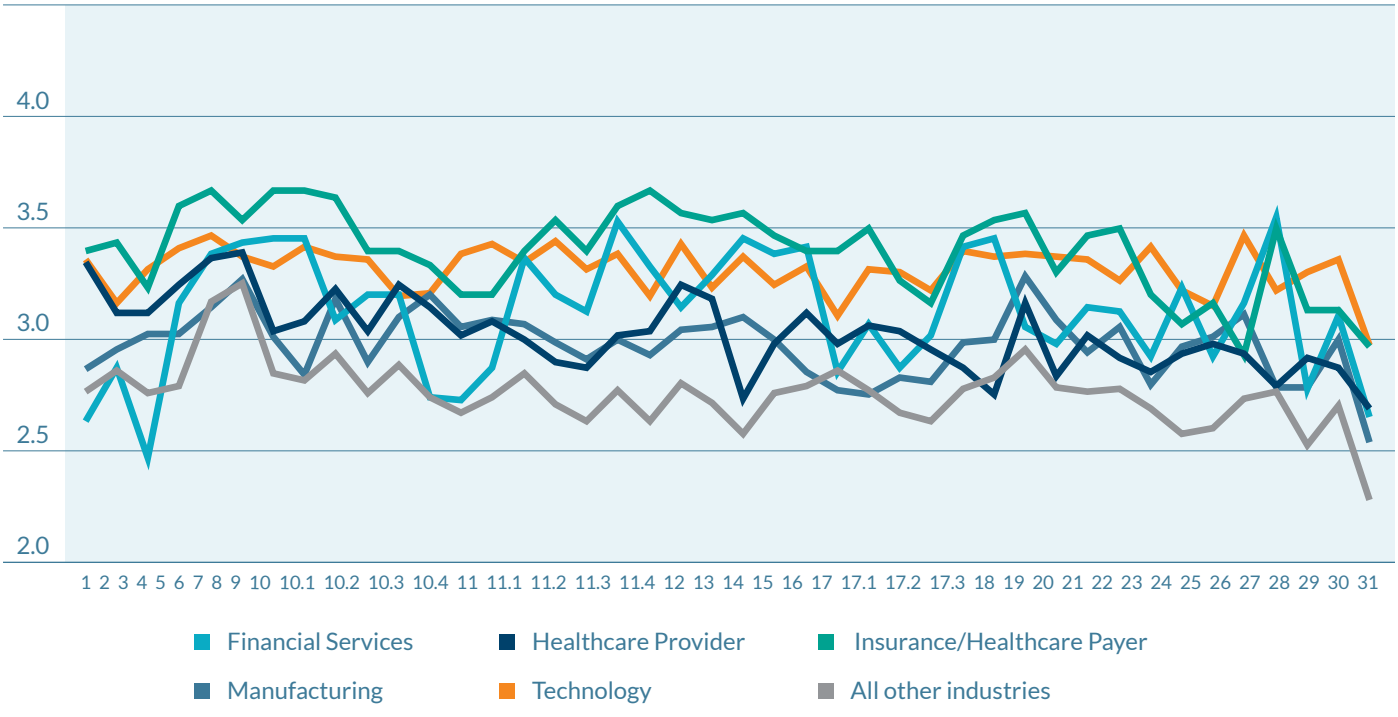
	Vendor Risk Component	2018
10.3	We have established and documented a formalized process for conducting virtual assessments.	2.90
10.4	We have established and documented a continuous monitoring program.	2.96
11	We have established and documented a formalized process for information gathering in vendor reviews.	3.05
11.1	We collect information about data classifications and locations.	2.97
11.2	We collect information about vendors' vendor relationships.	2.89
11.3	We collect information about IT controls, data protection controls and information security controls.	3.04
11.4	We collect information from external data sources in our vendor reviews.	2.92
12	We review vendor requirements with business, IT, legal and purchasing colleagues.	3.05
13	We execute scheduling and coordinate assessment activities with our vendors.	2.98
14	We send vendors a self-assessment questionnaire and documentation request list.	2.92
15	We have a process to obtain and assess confidentiality commitments, consistent with the organization's requirements, from vendors with access to confidential personal information.	2.99
16	We have a process to obtain and assess, on both a periodic and as-needed basis, privacy commitments of vendors with access to confidential personal information including corrective action if required.	3.01
17	We assess compliance with vendor contracts.	2.93
17.1	We assess compliance with business continuity contract provisions.	2.95
17.2	We assess compliance with outsourcing contract provisions.	2.87
17.3	We have a process in place to determine if a vendor uses subcontractors/fourth parties if the vendor's contract does not include vendor outsourcing requirements.	2.84
18	We identify control issues and formulate recommendations.	3.01

	Vendor Risk Component	2018
19	We develop vendor assessment reports.	3.03
20	We select, renew, or recommend termination of vendors when necessary.	3.13
21	We establish vendor remediation plans and termination/exit strategies (as appropriate) and validate these plans with the appropriate level of management and with our vendor.	2.97
22	We establish and revise the risk tiers of vendors based on assessment results.	2.98
23	We perform remediation plan follow-up discussions with the vendor.	2.98
24	We have a process to manage known un-remediated vendor issues.	2.88
	Vendor Assessment Metrics Reporting	
25	We consolidate the results of vendor assessments.	2.85
26	We calculate and distribute vendor assessment metrics.	2.84
27	We discuss the results of vendor assessments and metrics with management and/or the board of directors.	2.97
	Ongoing Vendor Risk Assessments	
28	We determine the frequency and scope of ongoing vendor risk assessment processes.	2.96
29	We determine the frequency and scope of ongoing subcontractor/fourth party risk assessment processes.	2.77
30	We have a process to respond to issues identified by continuous monitoring activities.	2.92
	Process Automation	
31	We have automated the scheduling/request process for conducting vendor risk assessments including the collection of compliance artifacts.	2.53
	Category Average	**2.97**

• • • *Vendor Risk Assessment Process — Maturity and Board Engagement*

Degree of board engagement with and understanding of vendor-related cybersecurity issues	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
Fully functional and advanced VRM programs (Levels 4 and 5)	57%	38%	25%
Transitional VRM programs (Level 3)	26%	30%	24%
Programs with ad hoc or no VRM activities (Levels 0, 1 and 2)	17%	32%	51%

• • • *Vendor Risk Assessment Process — Industry Results*



Skills and Expertise

Overall level of maturity: 2.89

• • • *Skills and Expertise — Overall Results*

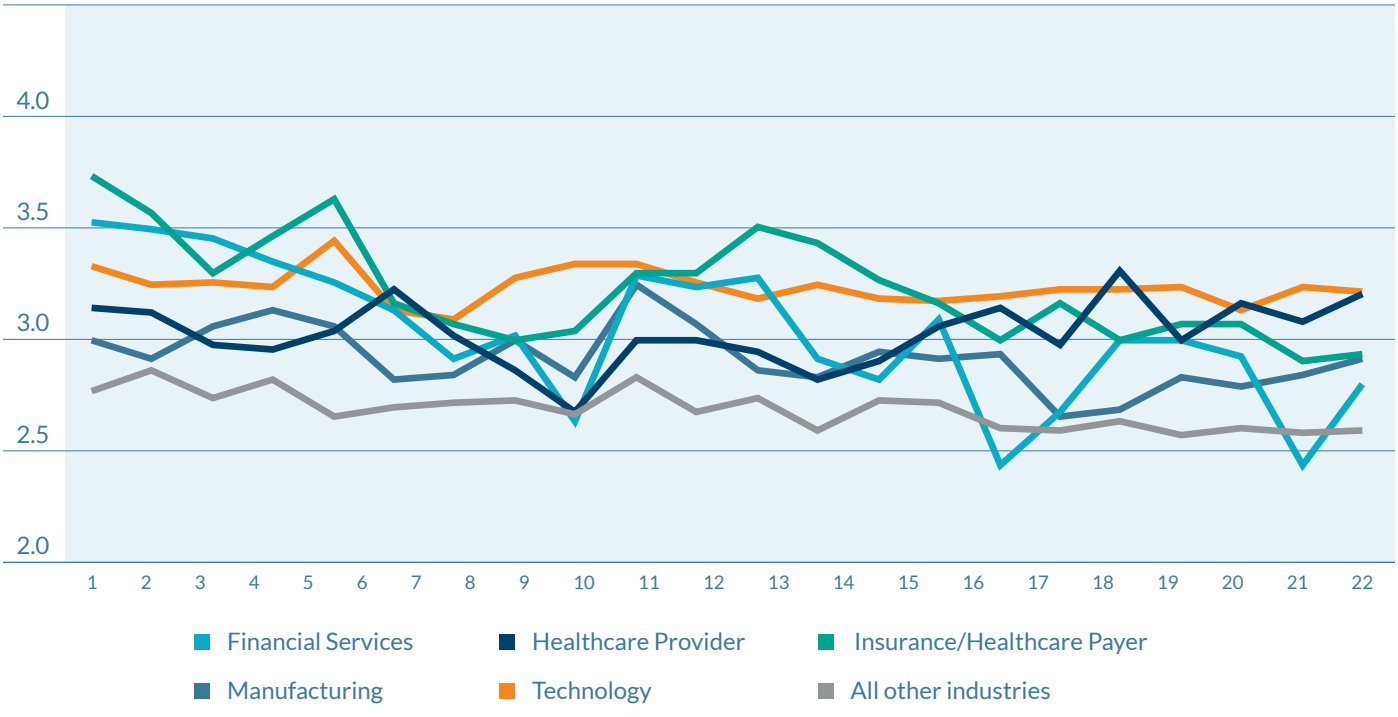
	Vendor Risk Component	2018
	Roles and Responsibilities	
1	We have established and documented the roles and responsibilities for vendor risk management.	3.04
2	We have assigned vendor risk management program ownership to an individual in our organization.	3.05
3	We have defined accountability for vendor risk within the organization and identified support staff for vendor risk management.	2.98
4	We have clearly defined roles and responsibilities (e.g., risk, sourcing, procurement and contracts) within our job descriptions.	3.02
5	We have defined and documented the roles to monitor changes to the regulatory landscape and to identify and recommend updates to our vendor risk management program.	2.97
	Staffing Levels and Competencies	
6	We have enough staff to manage vendor risk management activities effectively.	2.89
7	We have structures in place to define and measure the staffing levels required to meet vendor risk program requirements.	2.85
8	We have enough qualified staff to meet all vendor risk management objectives.	2.90
9	We have established and documented our governance programs so that staffing levels can be adjusted due to optimization.	2.81
10	We have competent personnel with enough authority to perform vendor control assessments and interpret vendor responses.	3.05
11	We provide training for assigned vendor risk management resources to maintain appropriate knowledge and certifications.	2.93

	Vendor Risk Component	2018
	Training and Awareness	
12	We have defined and communicated vendor risk management policies to our key stakeholders.	2.93
13	We periodically communicate our vendor risk management policies and procedures to all personnel.	2.82
14	At least annually, we communicate our vendor risk management policies and procedures and we provide training on vendor risk management policies and procedures to appropriate employee groups based on role.	2.88
15	We have defined training and education for our vendor risk personnel to enable them to define, execute and manage our program.	2.90
16	We measure employee understanding of our vendor risk management responsibilities and report results to management on an annual basis.	2.79
17	We have implemented metrics and reporting for compliance to vendor risk policies into the mandatory employee training and awareness program.	2.77
	Budget and Resources	
18	We have sufficient funding for vendor management training and awareness as set by policy.	2.84
19	We have allocated budget for vendor risk management functions, including basic travel, subscriptions, training and small projects.	2.81
20	We allocate a specific vendor risk management budget for industry memberships and training/education to accomplish its objectives.	2.81
21	We routinely measure or benchmark our vendor risk management budget with management reporting to demonstrate the return on investment (ROI).	2.76
22	We have sufficiently integrated our vendor risk management functions and tools into business lines so that overall costs and budget for dedicated risk management budgets are reduced.	2.82
	Category Average	**2.89**

• • • *Skills and Expertise — Maturity and Board Engagement*

Degree of board engagement with and understanding of vendor-related cybersecurity issues	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
Fully functional and advanced VRM programs (Levels 4 and 5)	56%	36%	24%
Transitional VRM programs (Level 3)	25%	28%	24%
Programs with ad hoc or no VRM activities (Levels 0, 1 and 2)	19%	36%	52%

• • • *Skills and Expertise — Industry Results*



Communication and Information Sharing

Overall level of maturity: 2.97

• • • *Communication and Information Sharing — Overall Results*

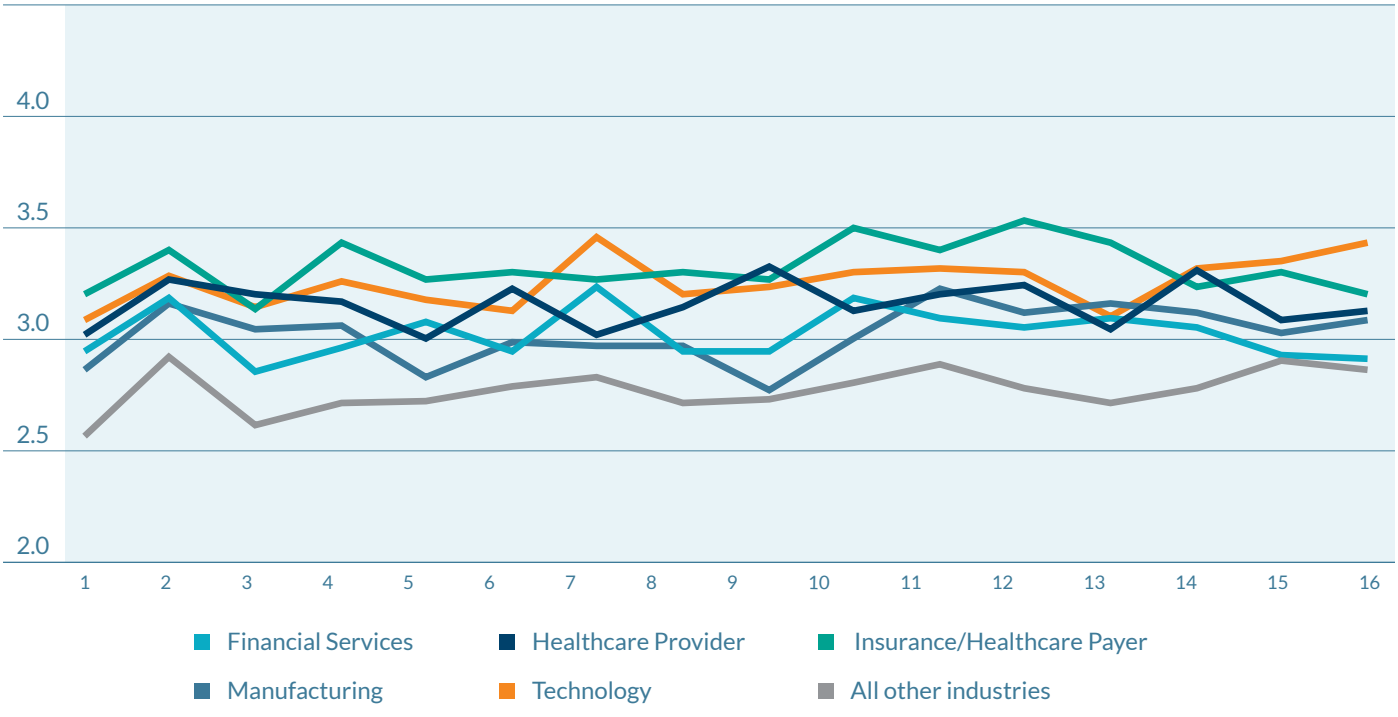
	Vendor Risk Component	2018
	Vendor Risk Program Integration	
1	We have implemented and communicated a Vendor Risk Governance program, approved by executive management, which includes integration into enterprise functions (e.g., sourcing, procurement, legal, risk).	2.79
2	We have a process in place to communicate policies and standards.	3.09
3	We have an ongoing education program for vendor management policies, standards, procedures and updates in place.	2.85
4	We have clearly defined, documented and communicated the roles and responsibilities for vendor risk management within the organizational areas that manage sourcing, procurement, legal and risk.	2.95
	Dashboards/Scoreboards	
5	We have defined a process to maintain and communicate periodic reporting for vendor management metrics that convey performance status, vendor value, service delivery, security, control environment, operations and regulatory compliance.	2.89
6	We have a process in place to communicate internal compliance with vendor management onboarding, periodic assessment and termination.	2.95
7	We have a process in place to communicate the status of vendor assessments and escalate concerns, as appropriate.	3.02

	Vendor Risk Component	2018
	Operational Management Reporting	
8	We have a process in place to communicate our compliance with vendor management processes and procedures.	2.92
9	We have a process in place to periodically communicate the effectiveness of vendor service delivery.	2.92
10	We have a process in place to track and communicate the status of incidents (identification tracking, resolution, consequences).	3.01
11	We have a process in place to escalate and communicate incidents and issues.	3.07
12	We have policies in place that define the roles and responsibilities for workflow tasks in the vendor risk assessment process including reporting on task completion.	3.01
	Board and Executive Reporting	
13	We have a process in place to periodically communicate the results of vendor assessments to executive management and the board.	2.94
14	We have a process in place to provide board and executive management responses to vendor assessment results.	3.00
	Communication Protocols	
15	We have established and documented a process for communicating and resolving service or product issues related to vendors.	3.03
16	The organization has established, documented and communicated exception handling procedures to resolve service or product issues related to vendors and business partners.	3.03
	Average	**2.97**

• • • *Communication and Information Sharing — Maturity and Board Engagement*

Degree of board engagement with and understanding of vendor-related cybersecurity issues	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
Fully functional and advanced VRM programs (Levels 4 and 5)	59%	37%	25%
Transitional VRM programs (Level 3)	25%	31%	25%
Programs with ad hoc or no VRM activities (Levels 0, 1 and 2)	16%	32%	50%

• • • *Communication and Information Sharing — Industry Results*



Tools, Measurement and Analysis

Overall level of maturity: 2.95

• • • *Tools, Measurement and Analysis — Overall Results*

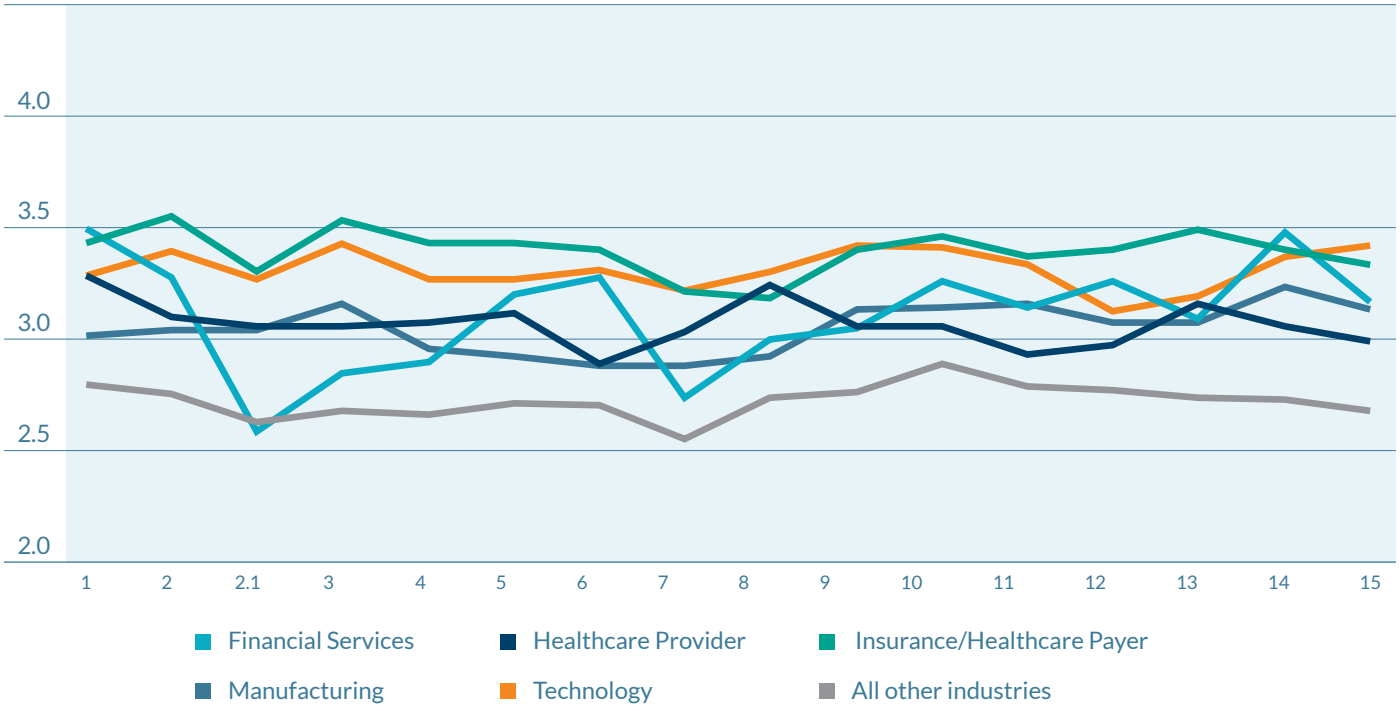
	Vendor Risk Component	2018
	Workflow Management	
1	We establish vendor review schedules for all types of vendor assessments (onsite, remote, etc.).	3.04
2	We assign resources to accomplish reviews as scheduled.	3.00
2.1	We capture and report on vendor risk management expenses (e.g., budget to actual, variances, etc.).	2.84
3	We monitor variances between scheduled reviews and actual reviews performed.	2.94
	Vendor Risk Scoring Tools	
4	We process information obtained during the vendor selection or review process into a risk scoring tool.	2.88
5	We process information according to an established risk scoring methodology.	2.94
6	We report risk scoring results to relevant stakeholders.	2.92
7	We leverage outside industry data in our risk scoring.	2.79
	Vendor Financial Analysis	
8	We engage finance and procurement partners to identify financial metrics.	2.93
9	We establish relevant business risk measures and benchmarks.	2.99
10	We determine financial viability of our vendors.	3.07
11	We report vendor financial results to relevant stakeholders.	2.99

	Vendor Risk Component	2018
	Vendor Business Risk	
12	We engage business, risk or legal partners to quantify risk.	2.95
13	We establish relevant business risk measures and benchmarks (e.g., reputation, geopolitical, ethics, financial, physical environment, cybersecurity, resilience, compliance, etc.).	2.95
14	We determine the risk posture or viability of our vendors.	3.02
15	We report vendor risk posture results to relevant stakeholders.	2.95
	Average	**2.95**

• • • *Tools, Measurement and Analysis — Maturity and Board Engagement*

Degree of board engagement with and understanding of vendor-related cybersecurity issues	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
Fully functional and advanced VRM programs (Levels 4 and 5)	59%	39%	23%
Transitional VRM programs (Level 3)	24%	28%	24%
Programs with ad hoc or no VRM activities (Levels 0, 1 and 2)	17%	33%	53%

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



Monitoring and Review

Overall level of maturity: 2.93

• • • *Monitoring and Review — Overall Results*

	Vendor Risk Component	2018
	Contract Provision Tracking and Maintenance	
1	We have established and documented a process to determine if standard contract terms are in place.	3.11
2	We have established and documented a process to modify the contract and approve modifications by legal and an appropriate level of management.	3.12
3	We have established and documented a process to facilitate approval of final contract terms by our legal department and the appropriate level of management.	3.20
4	We have established and documented policies and procedures for the storage, retention and retrieval of contract terms.	3.16
5	We have established and documented a process to address expired, canceled or terminated contracts.	3.12
	Monitoring Service Level Agreements and Performance	
6	We have established and documented a process to periodically require service level agreement reporting.	2.98
7	We have established and documented a process to track and analyze customer complaints.	3.02
8	We have established and documented a process to periodically conduct customer satisfaction surveys.	2.97
9	We have established and documented a process to periodically assess the performance of our vendors and business partners against our defined requirements.	3.00
	Potential Changes Due to Internal and External Environment	
10	We have established and documented a process to respond to, escalate and inform key stakeholders of relevant data security breaches or other similar incidents.	3.02
11	We have established and documented a process to monitor industry and external changes to the regulatory, economic and physical environment that may negatively impact our vendors.	2.97
12	There is a process in place to periodically monitor regulatory changes applicable to our business, products and services.	3.06

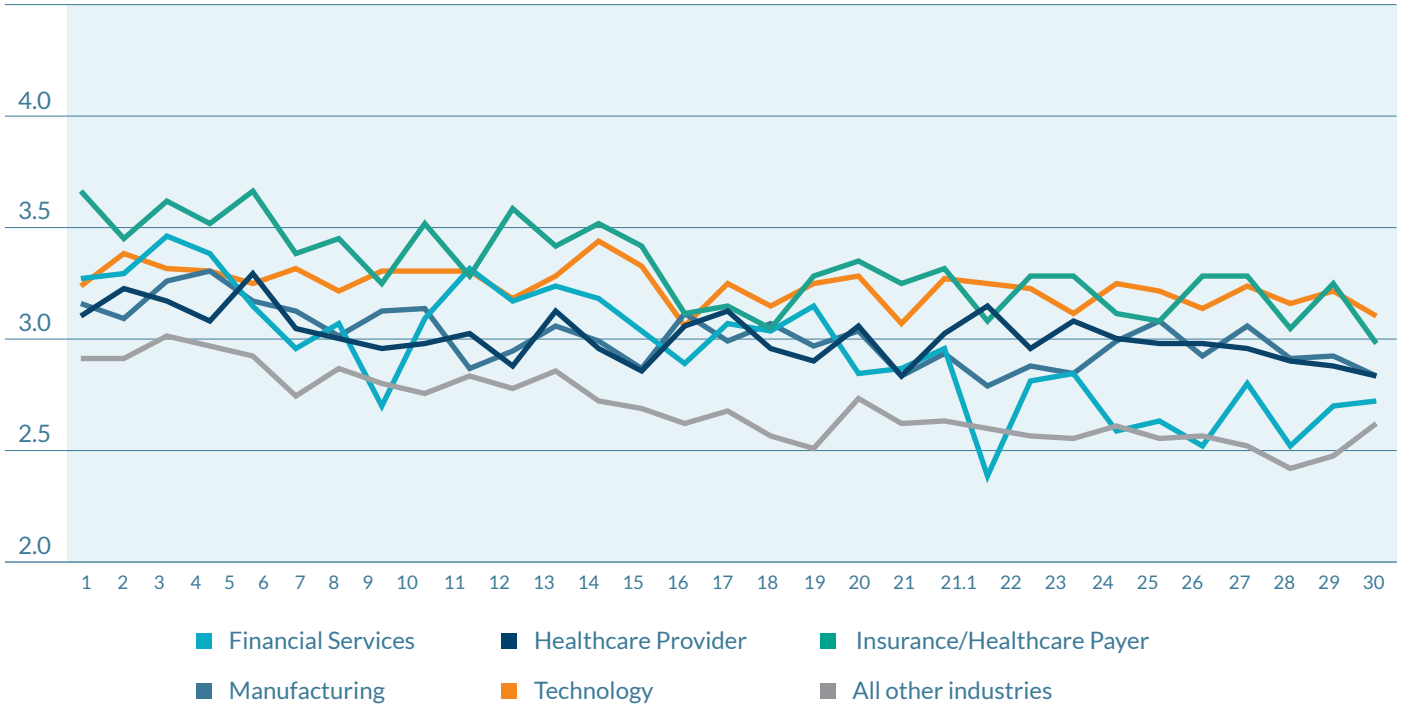
	Vendor Risk Component	2018
13	We have established and documented a process to respond to and inform our key stakeholders of regulatory requirements, trends and changes.	3.00
14	We have established and documented a process to consider the impact of changes to vendor operations (e.g., new business lines, technology changes, business models, acquired or divested operations) that have the potential to impact our vendor and business partner relationships.	2.92
	Self-Assessment/Audit Readiness and Assurance	
15	We have established and documented a process to periodically assess our program's effectiveness in evaluating our vendors' financial conditions.	2.86
16	We have established and documented a process to periodically review the scope of and our reliance on external audit reports.	2.93
17	We have established and documented a process to periodically review our program's effectiveness in reviewing and testing our vendors' business continuity and disaster recovery measures, and our use of those test results.	2.85
18	We have established and documented a process to conduct periodic independent reviews of our third party risk management program.	2.84
19	We have established and documented a process to address applicable filings or certifications of compliance.	2.95
	Controls Validation and/or Testing	
20	We have established and documented a process to determine if additional control validation is necessary.	2.82
21	We have established and documented a process to determine if an onsite assessment is necessary.	2.90
21.1	We have a process to determine if the onsite assessment should be performed by an independent third party.	2.80
	Continuous Monitoring Program	
22	We have a process to monitor external data sources to identify risks resulting from potential litigation regarding our vendors.	2.83
23	We have a process to monitor external data sources to identify potential risks resulting from changes to the financial viability of our vendors.	2.82
24	We have a process to monitor external data sources to identify changes to our vendors' business models, strategies, or changes due to mergers and acquisitions.	2.84
25	We track the timeliness of responses to our vendor information requests as an indicator of potential risk.	2.82

	Vendor Risk Component	2018
26	We monitor and track external audit findings across multi-year assessments as an indicator of potential risk.	2.79
27	We monitor and measure the timeliness of vendor response regarding notifications on patches, vulnerabilities and malware to identify potential risks.	2.83
28	We monitor external data sources to identify our vendor's vendor (fourth party/subcontractor) relationships.	2.71
29	We monitor external data sources for reports of complaints to regulators and other industry organizations.	2.77
30	We have a process to regularly incorporate continuous monitoring outputs to update our vendor risk management program.	2.79
	Average	**2.93**

• • • *Monitoring and Review — Maturity and Board Engagement*

Degree of board engagement with and understanding of vendor-related cybersecurity issues	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
Fully functional and advanced VRM programs (Levels 4 and 5)	58%	37%	26%
Transitional VRM programs (Level 3)	24%	30%	23%
Programs with ad hoc or no VRM activities (Levels 0, 1 and 2)	18%	33%	51%

• • • *Monitoring and Review — Industry Results*



Survey Methodology and Demographics

The Vendor Risk Management Benchmark Study was conducted online by the Shared Assessments Program and Protiviti in the fourth quarter of 2018, with 554 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 vendor risk management program.

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

- Program Governance
- Policies, Standards and Procedures
- Contract Development, Adherence and Management
- Vendor Risk Assessment Process
- 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

4 = Fully implemented and operational

3 = Fully determined and established

2 = Determining roadmap to achieve success

1 = Initial visioning

0 = Non-existent

The survey also included a special section on board engagement, cybersecurity and de-risking.

• • • *Position*

IT VP/Director	19%
IT Manager	15%
Chief Information Officer	11%
Chief Financial Officer	9%
Finance Manager	7%
Procurement/Purchasing/Supply Chain	7%
Finance Director	6%
Chief Technology Officer	4%
Operational Risk Management	3%
Chief Risk Officer	2%
Chief Security Officer	1%
IT Audit Manager	1%
Chief Audit Executive	1%
Chief Information Security Officer	1%
Chief Compliance Officer	1%
IT Audit VP/Director	1%
Internal Audit Manager	1%
Other	10%

• • • *Industry*

Technology (Software/High-Tech/Electronics)	15%
Manufacturing (other than Technology)	13%
Healthcare Provider	9%
Retail	6%
Government	6%
Professional Services	5%
Insurance	5%
Financial Services — Banking	4%
Financial Services — Other	3%
Higher Education	3%
Construction	3%
Financial Services — Asset Management	3%
Not-for-Profit	2%
Real Estate	2%
Pharmaceuticals and Life Sciences	2%
Consumer Packaged Goods	2%
Automotive	2%
Power and Utilities	2%
Transportation and Logistics	2%

• • • *Industry (continued)*

Agriculture, Forestry, Fishing	1%
Wholesale/Distribution	1%
Hospitality, Leisure and Travel	1%
Media and Communications	1%
Oil and Gas	1%
Biotechnology, Life Sciences and Pharmaceuticals	1%
Chemicals	1%
Healthcare Payer	1%
Other	3%

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

$20 billion or more	7%
$10 billion — $19.99 billion	8%
$5 billion — $9.99 billion	9%
$1 billion — $4.99 billion	18%
$500 million — $999.99 million	15%
$100 million — $499.99 million	13%
Less than $100 million	30%

Financial Services Industry — Size of Organization (by assets under management)

Greater than $250 billion	12%
$50 billion — $250 billion	7%
$25 billion — $49.99 billion	15%
$10 billion — $24.99 billion	15%
$5 billion — $9.99 billion	15%
$1 billion — $4.99 billion	20%
Less than $1 billion	16%

Headquarters

United States	97%
Canada	1%
United Kingdom	1%
Other	1%

Organization Type

Private	52%
Public	36%
Government	7%
Not-for-profit	4%
Other	1%

ABOUT SHARED ASSESSMENTS

As the only organization that has uniquely positioned and developed standardized resources to bring efficiencies to the market for more than a decade, the Shared Assessments Program has become the trusted source in third party risk assurance. Shared Assessments offers opportunities for members to address global risk management challenges through committees, awareness groups, interest groups and special projects. Join the dialog with peer companies and learn how you can optimize your compliance programs while building a better understanding of what it takes to create a more risk sensitive environment in your organization.

ABOUT THE SANTA FE GROUP

The Santa Fe Group's risk management experts work collaboratively with organizations worldwide to identify valuable trends, risks, and vulnerabilities, and to advise, educate, and empower organizations in the areas of cybersecurity, third party risk, emerging technologies, and program management. The Santa Fe Group is the managing agent of the membership-based Shared Assessments Program, which helps many of the world's leading organizations manage and protect against third party IT security risks.

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 75 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