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

Executive Summary

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 organisation 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 organisations 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 organisations.

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 organisations, retail firms, academia, and telecommunications companies — dedicated to assisting organisations by helping them to understand, manage and monitor vendor risk effectively and efficiently.

Our full report on this year's Vendor Risk Management Benchmark Study, available at www.protiviti.com/vendor-risk and www.sharedassessments.org, contains detailed results and more extensive analysis of our findings.

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 organisations 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: Organisations 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 organisations that have low levels of board engagement in these issues. Conversely, organisations 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. Organisations 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. Organisations 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 organisations longer to fix the underlying issues.** It comes as no surprise that nearly 67 percent more organisations reported that their organisations 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 organisations 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 organisations are moving away from high-risk vendor relationships.** A majority of organisations — 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 organisations. 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 optimise those resources, more than one out of three organisations (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 organisations 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 15 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 organisations.[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 organisations whose practice measures are *at or above target*, *transitional*, or *well below target*.

[1] As a result of this industry realignment, this year's response from financial services industry organisations was lower than our surveys from prior years. Therefore, unlike in years past, we have not included a breakdown of results by organisation 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 organisation, based on the following scale:

5 = Continuous improvement: The organisation 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 organisation 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 organisation 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 organisation.

• • • *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**

• • • *Vendor Risk Management — Assessing Results by Industry*

	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**

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 optimises 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 optimise 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 organisations 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 organisations 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 optimised 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 organisations struggled to address their, and their vendors', ransomware defences 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 organisational 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 organisations 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. Organisations 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 organisation's risk management changes and weak spots. "Untrained general (non-IT) staff represents the greatest cybersecurity danger organisational 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 organisations 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 organisation 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 organisation 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%

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 organisations 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. Optimising available resources by regularly honing current vendor risk management processes is an increasingly essential element in any successful program. Utilise 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 organisational stability and continuity.
>
> — Paul Kooney, Managing Director, Security and Privacy Practice, Protiviti

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 organisation, 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 Organisation (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 Organisation (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%

Organisation Type

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

ABOUT SHARED ASSESSMENTS

As the only organisation that has uniquely positioned and developed standardised 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 dialogue with peer companies and learn how you can optimise your compliance programs while building a better understanding of what it takes to create a more risk sensitive environment in your organisation.

ABOUT THE SANTA FE GROUP

The Santa Fe Group's risk management experts work collaboratively with organisations worldwide to identify valuable trends, risks, and vulnerabilities, and to advise, educate, and empower organisations 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 organisations 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.

PROTIVITI GLOBAL MARKET LEADERS

ARGENTINA

Pablo Giovannelli
+54.11.5278.6345
pablo.giovannelli@protivitiglobal.com.pe

AUSTRALIA

Garran Duncan
+61.3.9948.1200
garran.duncan@protiviti.com.au

BAHRAIN

Arvind Benani
+973.1.710.0050
arvind.benani@protivitiglobal.me

BRAZIL

Raul Silva
+55.11.2198.4200
raul.silva@protivitiglobal.com.br

CANADA

David Dawson
+1.647.288.4886
david.dawson@protiviti.com

CHILE

Soraya Boada
+56.22.573.8580
soraya.boada@protivitiglobal.cl

CHINA (HONG KONG)

Albert Lee
+852.2238.0499
albert.lee@protiviti.com

CHINA (MAINLAND)

David Cheung
+86.21.5153.6900
david.cheung@protiviti.com

EGYPT

Ashraf Fahmy
+202.25864560
ashraf.fahmy@protivitiglobal.me

FRANCE

Bernard Drui
+33.1.42.96.22.77
drui@protiviti.fr

GERMANY

Michael Klinger
+49.69.963.768.155
michael.klinger@protiviti.de

INDIA

Sanjeev Agarwal
+91.124.661.8600
sanjeev.agarwal1@protivitiglobal.in

ITALY

Alberto Carnevale
+39.02.6550.6301
alberto.carnevale@protiviti.it

JAPAN

Yasumi Taniguchi
+81.3.5219.6600
yasumi.taniguchi@protiviti.jp

KUWAIT

Sanjeev Agarwal
+965.2242.6444
kuwait@protivitiglobal.me

MEXICO

Roberto Abad
+52.55.5342.9100
roberto.abad@protivitiglobal.com.mx

NETHERLANDS

Anneke Wieling
+31.20.346.0400
anneke.wieling@protiviti.nl

OMAN

Shatha Al Maskiry
+968 24699402
shatha.maskiry@protivitiglobal.me

PERU

Marco Villacorta
+51.1.208.1070
marco.villacorta@protivitiglobal.com.pe

QATAR

Andrew North
+974.4421.5300
andrew.north@protivitiglobal.me

SAUDI ARABIA

Saad Al Sabti
+966.11.2930021
saad.alsabti@protivitiglobal.me

SINGAPORE

Nigel Robinson
+65.9169.2688
nigel.robinson@protiviti.com

UNITED ARAB EMIRATES

Arindam De
+9714.438.0660
arindam.de@protivitiglobal.me

UNITED KINGDOM

Peter Richardson
+44.20.7930.8808
peter.richardson@protiviti.co.uk

UNITED STATES

Scott Laliberte
+1.267.256.8825
scott.laliberte@protiviti.com

VENEZUELA

Gamal Perez
+58.212.418.46.46
gamal.perez@protivitiglobal.com.ve

www.sharedassessments.org

protiviti®

www.protiviti.com