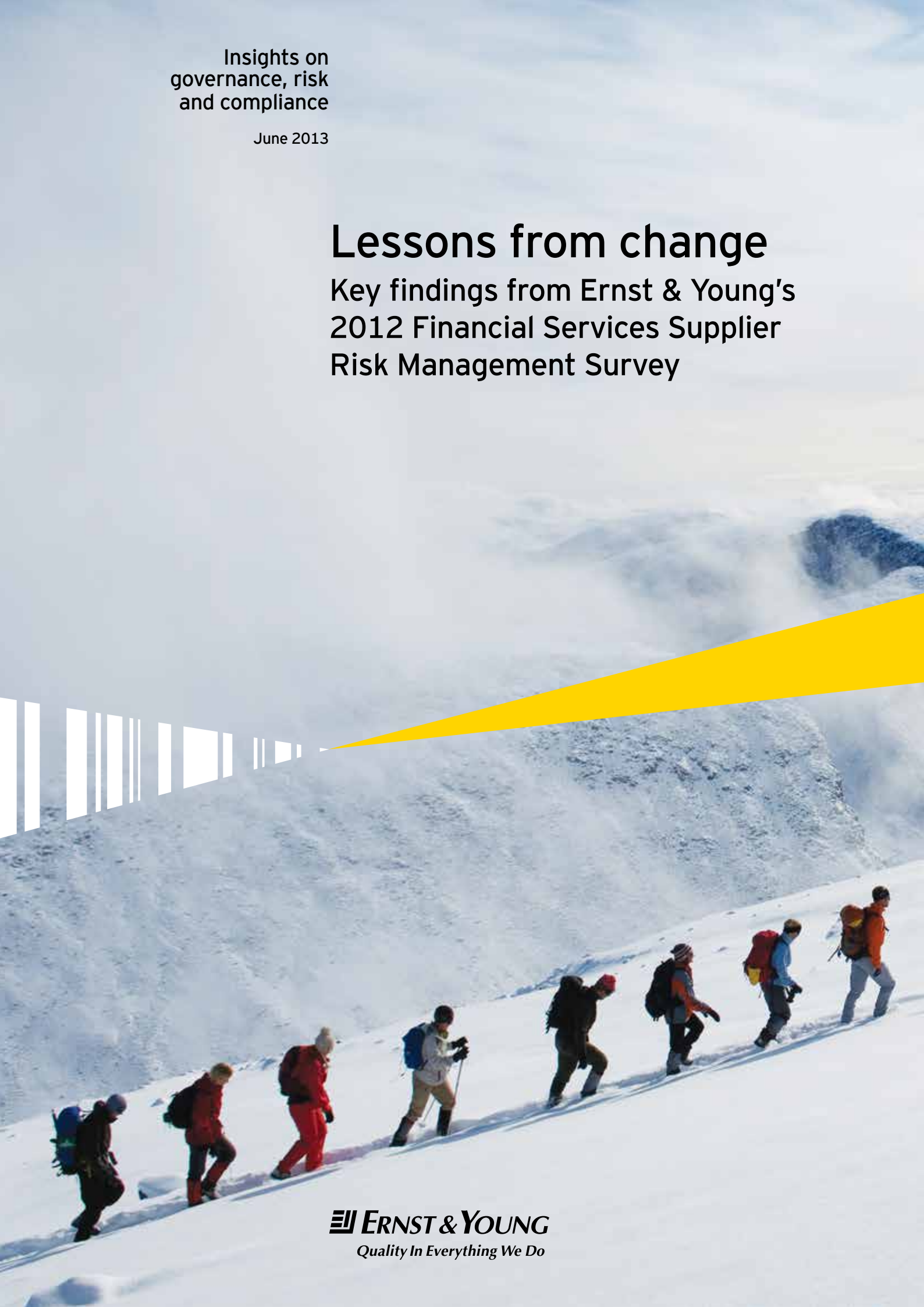
Insights on governance, risk and compliance

June 2013

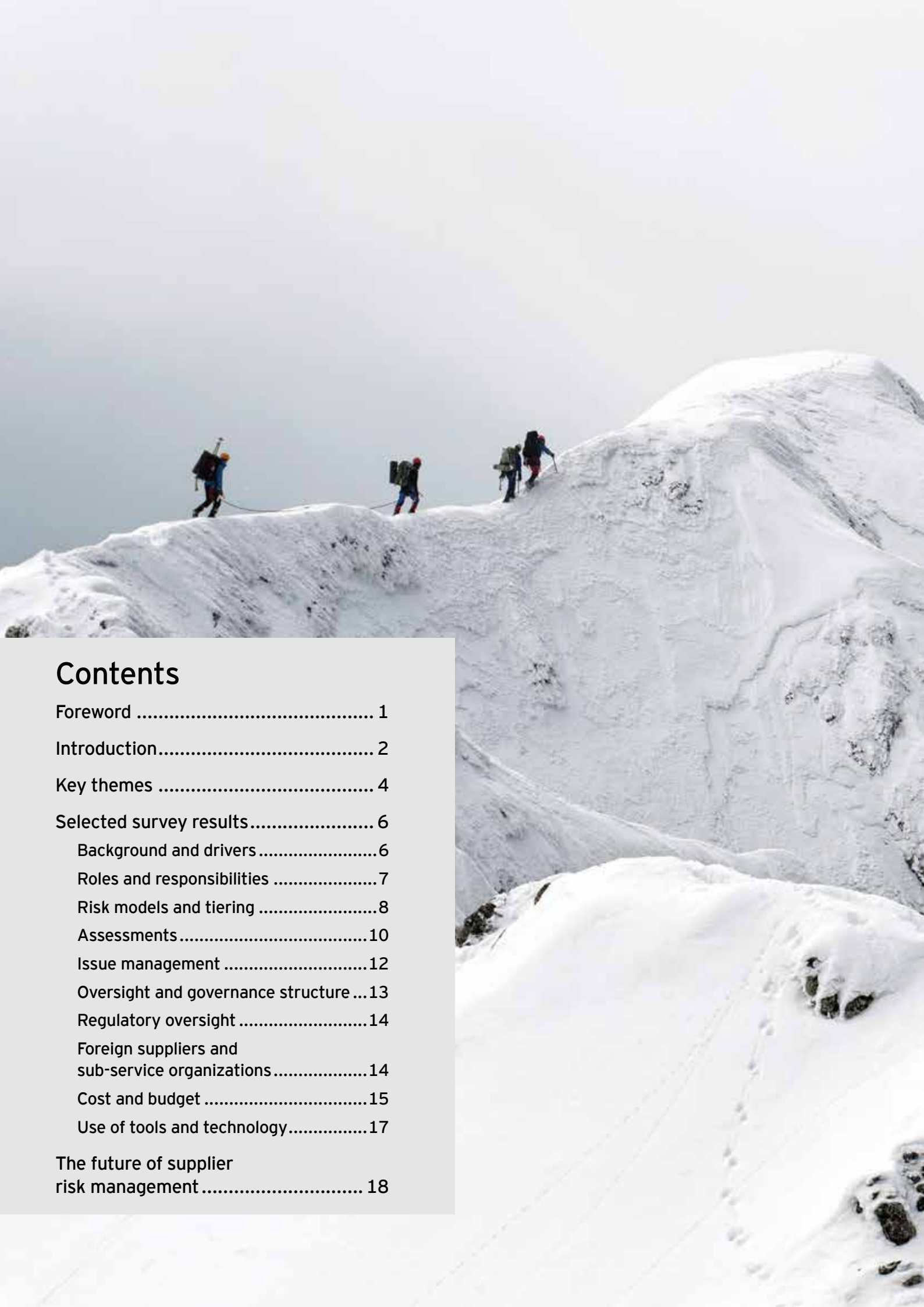
Lessons from change

Key findings from Ernst & Young's 2012 Financial Services Supplier Risk Management Survey



Ernst & Young

Quality In Everything We Do



Contents

Foreword

This report was previously published by the Ernst & Young Financial Services Office (FSO) based on survey results from the financial services sector.

However, as a global organization with a wide range of sector experience, we feel that it contains findings that are valuable for all businesses, not just those in financial services, and so it is republished here as part of our *Insights on governance, risk and compliance* series.

The survey results indicate that organizations in general need to focus on the following topics:

- Achieving clarity of roles and the interaction between lines of business; and matching program requirements to complementary skills
- Creating more transparent risk and segmentation models to adjust to the needs of the organization
- Concentrating on specific risks applicable to services provided by the suppliers; and introducing a baseline control environment
- Instilling consistency and compliance with internal policies via a quality assurance (QA) program
- Realizing regulatory compliance with consumer-based standards and laws
- Adjusting risk models and rationalizing supplier bases in order to effect change and reduce costs.

For more information on *Insights on governance, risk and compliance* and other publications on similar risk-related topics, please see page 20. You can also access our thought leadership at www.ey.com/GRCinsights.

About FSO

Amid sweeping regulatory change, today's financial services institutions must grapple with capital management, business risks and global growth — all while meeting greater demands for transparency.

We believe that the financial services industry deserves an integrated approach to managing its uncertainties and opportunities. Our reputation is built on assembling multidisciplinary teams from around the world to deliver a global perspective. Our 35,000 global asset management, banking and capital markets, and insurance industry professionals are located in major geographic hubs — a unique structure that allows us to rapidly mobilize and dedicate them to the right assurance, tax, transaction and advisory-related projects across the Americas, Asia-Pacific, EMEIA and Japan.

As a leading provider of integrated risk management and regulatory advisory services to the banking and capital markets, insurance, asset management, energy and corporate treasury sectors, our dedicated team helps clients tackle the numerous challenges of risk management.

Introduction

Supplier risk management (SRM) continues to be an important topic for many organizations. Negative publicity and fines for regulatory compliance infractions, security breaches and data thefts involving suppliers have required companies to continually improve their SRM functions. Increased regulatory attention to supplier risk within the consumer banking environment has also been an important driver for the continued enhancement of SRM programs across the financial services industry. During the third quarter of 2012, federal regulators, including the Consumer Financial Protection Bureau (CFPB), issued a number of Consent Orders, each of which had significant financial repercussions.

Each of the Consent Orders noted a lack of sufficient vendor compliance oversight. The message being delivered is that regulatory expectations regarding supplier management is increasing and scrutiny of these relationships will continue regardless of whether the activity is conducted in-house or by a supplier. Financial institutions no longer have the ability to transfer risk or regulatory compliance expectations fully onto their suppliers; accountability must remain with the financial institution. This message was also delivered by the Director of the CFPB (Richard Cordray), who recently commented that "[this action puts] all financial institutions on notice about these prohibited practices, and reinforces that they must make sure their service providers are complying with the law."[1]

The 2012 Ernst & Young Financial Services Supplier Risk Management Survey, our third annual survey focused on this topic, confirms that many of our clients are monitoring or increasing their already considerable investments in assessment and monitoring of various risks presented across their supplier base. As best practices for supplier risk management continue to evolve, companies are altering their functions to better ensure that supplier services are continually available and operating in line with risk, performance and regulatory compliance expectations, and to ensure that customer data is adequately handled and secured. This survey gathered benchmark information to assist companies in operating an efficient function that meets these risk management goals.

1. Prepared Remarks by Richard Cordray, Director of the Consumer Financial Protection Bureau (CFPB), Enforcement Action, Washington, DC, 18 July 2012.

We asked participants to answer 51 questions about significant components of their supplier risk management programs:

- Program drivers
- Roles and responsibilities
- Risk models and tiering
- Assessments
- Issue management
- Oversight and governance structure
- Regulatory oversight
- Foreign suppliers and sub-service organizations
- Cost and budget
- Use of tools and technology

We are pleased to share our 2012 survey results, as well as noteworthy year-over-year trends. We hope you find the information contained in this report valuable, and we welcome the opportunity to discuss with you the findings and our perspective on supplier risk management trends in the financial services industry and beyond.

About Ernst & Young's Supplier Risk Management Survey

In the third quarter of 2012, Ernst & Young surveyed 35 global institutions with a supplier risk function in the banking and capital markets, insurance and asset management sectors.

Collectively among the institutions, 71% were in the banking and capital markets industry, almost two-thirds had over 250,000 employees, and two-thirds had been operating a supplier risk management program for more than three years.

Tabulated responses for each question are contained in the sections that follow.

For further details about the survey and this report, please contact:

Americas

Chip Tsantes
Principal
Ernst & Young LLP
chip.tsantes@ey.com
+1 703 747 1309

Chris Ritterbush
Executive Director
Ernst & Young LLP
chris.ritterbush@ey.com
+1 212 773 4489

Matthew Moog
Senior Manager
Ernst & Young LLP
matthew.moog@ey.com
+1 212 773 2096

EMEIA

Steve Holt
Partner
Ernst & Young LLP (UK)
sholt2@uk.ey.com
+44 207 951 7874

Key themes

Program drivers

- Over 90% of respondents continue to cite the protection of reputation and brand, protection of customer and proprietary information, and complying with regulations as drivers for the assessment of supplier controls.
- Regulatory scrutiny has increased more than any other risk factor.

Roles and responsibilities

- The responsibility of supplier identification, which in the previous year's survey was shared evenly between procurement and the line of business, was more heavily attributed to the procurement function (57% vs. 37%).
- Ultimate supplier selection continues to be skewed toward the line of business (57% vs. 40%).
- Lines of business also continue to maintain ultimate ownership of issue remediation (69%).

Risk models and tiering

- The percentage of suppliers subject to risk monitoring has grown year over year, and now averages between 13% and 17%.
- A strong majority of respondents, more than eight in ten, indicated they maintained a critical supplier list. Fifty-nine percent have 40 or fewer suppliers on that list; 73% have 60 or fewer.
- In the last 12 months, regulatory compliance scrutiny has increased more than any other risk factor as a driver of third-party supplier risk.
- Outside of critical suppliers, nearly three-quarters of those surveyed have less than 10% of their suppliers subject to monitoring in their highest risk tier.

Assessments

- In areas where inherent risk is identified as "high", 91% of respondents complete control assessments pre-contract, up from 60% in the previous year.
- Eighty-six percent of respondents reassess their highest risk suppliers at least annually.
- Sixty percent of respondents indicated they spent a day or less on site, up from 55% last year.
- Fifty-seven percent of respondents use 250 or fewer questions on their supplier review questionnaires.

Issue management

- Eighty percent of respondents find 10 or fewer issues, on average, per supplier control assessment.
- Two-thirds of respondents reported that only 40% of the issues had been remediated after six months.
- Only 11% of organizations terminated more than five suppliers in the past year due to a supplier issue or breach.

Oversight and governance structure

- Two-thirds of the organizations surveyed reported having a quality assurance (QA) function as part of the oversight and governance program, up from 50% last year.

Regulatory oversight

- Oversight and governance, along with due diligence activities and supplier assessments, top the list of focus areas during the most recent regulatory reviews.

Foreign suppliers and sub-service organizations

- About two-thirds (63%) of respondents actively identify and use sub-service organizations, and most organizations (82%) indicated the identification of sub-service providers within the contracting phase, up from 50% last year.

Cost and budget

- On average, respondents indicated that they intended to spend as much as or more than they did a year ago on many of the activities associated with supplier risk management.

Use of tools and technology

- The only notable variance between this year and last is a reduction in the use of automated tools to facilitate the execution of online assessments; 40% this year vs. 63% in the previous year.
- Two-thirds of respondents indicated that tools used within supplier risk management functions do not integrate into enterprise risk reporting systems.

Selected survey results

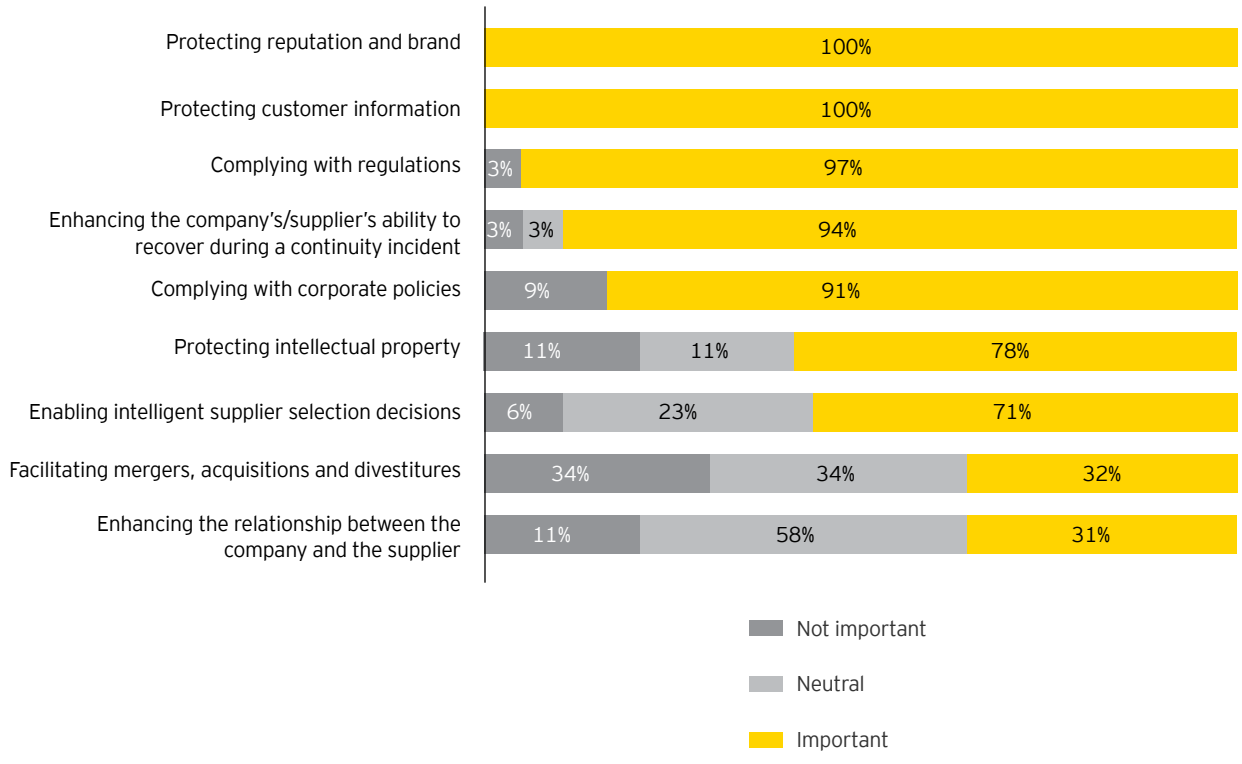
Background and drivers

SRM program drivers

As in previous years, over 90% of respondents continue to cite the protection of reputation and brand, protection of customer and proprietary information, complying with regulations and corporate policies and enhancing the supplier's ability to recover during an incident as drivers for the assessment of supplier controls.

Respondents also indicated that regulatory scrutiny has increased more than any other risk factor, with 100% of banking and insurance industry participants indicating this is an important consideration in their program execution.

Figure 1: How important is the assessment of third-party supplier controls in supporting the following activities for your organization?



Roles and responsibilities

In assessing organizational roles and responsibilities among various activities commonly conducted within an established supplier risk management function, the 2012 survey showed much more of a polarization of answers, indicating a greater emphasis on role clarity within most organizations. The responsibility of supplier identification, which in the previous year's survey was shared evenly between procurement and the line of business, was more heavily attributed to the procurement function (57% vs. 37%). This validates our industry observations that companies continue to focus significant effort on supplier identification and rationalization. Ultimate supplier selection continues to be skewed toward the line of business (57% vs. 40%), as they, in the end, own the risk and performance of the supplier. Lines of business also continue to maintain ultimate ownership of issue remediation (69%); however, we have noted that if this responsibility is placed solely on the line of business without support from a risk, compliance or control partner organization, failure in timely progression to remediation seems to be prevalent.

The role of the operational risk and compliance function continues to evolve. Today, its responsibility in control assessments is now even with that of other functions, such as information security and business continuity. This is due to the increased scrutiny of the regulatory compliance of suppliers, which has led to a shift of oversight and governance from the procurement function to risk and compliance. These findings show a continuing overall maturity of these functions, and that companies are shifting roles to match them more appropriately to the skills required to effectively operate the function.

Figure 2: Which functional area has primary responsibility for the following components of your organization's third-party supplier risk management program?

	Procurement/ purchasing	Information security	Business continuity	Internal audit	Legal/general counsel	Operational risk/ compliance	Line of business
Inherent risk assessment	23%	23%	0%	0%	0%	20%	34%
Supplier identification	57%	0%	0%	0%	0%	6%	37%
Supplier selection	40%	3%	0%	0%	0%	0%	57%
Control assessment	17%	37%	0%	9%	0%	20%	17%
Issue remediation	11%	11%	0%	0%	0%	9%	69%
Oversight and governance	38%	11%	0%	0%	3%	34%	14%

Selected survey results

Risk models and tiering

Suppliers subject to monitoring

The percentage of suppliers subject to risk monitoring has grown year over year, and now averages between 13% and 17%, whereas in prior years this had been closer to 10%. This seems to be due to the inclusion of suppliers who previously had not been part of companies' SRM functions. For example, suppliers who support key mortgage banking processes are now subject to more formal monitoring routines, where previously they were exempt from most programs, or their oversight was managed elsewhere within the organization. Law firms, marketing firms, enhancement services, affiliate relationships and joint ventures are just a few of the supplier categories that are now incorporated into enterprise-wide SRM functions. This is also a reflection of the continued maturity of the supplier risk management functions, as risk models evolve and the inventory of suppliers is better defined.

The primary risk factors used to identify suppliers subject to risk monitoring is consistent with last year's results. These include business continuity, information security, regulatory compliance, strategic importance and delivery of customer-facing services.

Figure 3: What is the total number of suppliers that support your organization (including those with nominal or limited risk)?

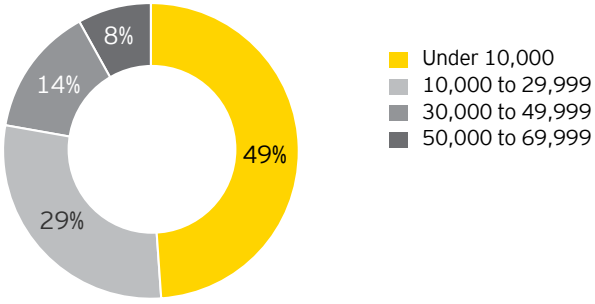
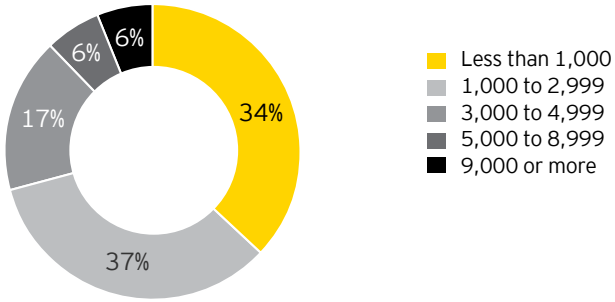


Figure 4: What is the total number of active suppliers subject to risk monitoring within your supplier risk management program?



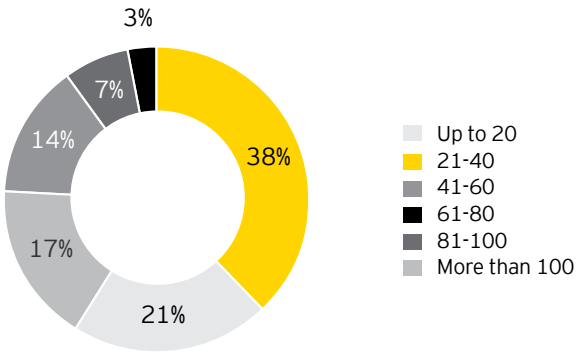
Critical suppliers

A strong majority of respondents, more than eight in 10, indicate they maintain a critical supplier list. Fifty-nine percent have 40 or fewer suppliers on that list; 73% have 60 or fewer. Our critical supplier results were consistent across the major breakouts of the respondents, regardless of size, industry or program maturity, indicating that this is a common theme with any SRM function. The criteria for these lists vary, but they seem to be aligned with:

- Business continuity risk (90%)
- Information security risk (83%)
- Regulatory risk (72%)
- Strategic importance (72%)
- Delivery of customer-facing services (72%)

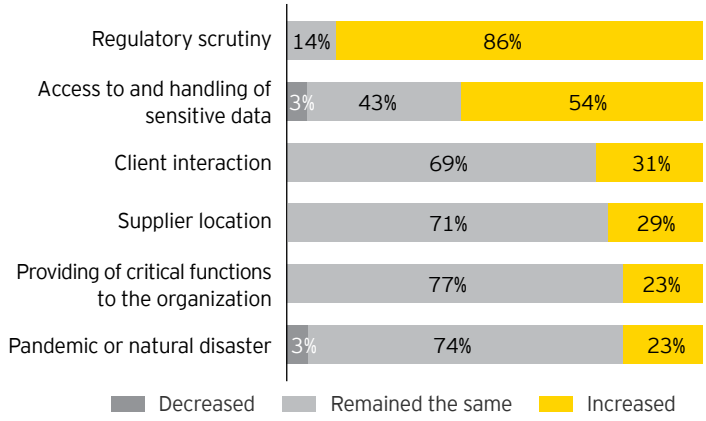
Figure 5: Does your organization maintain a separate listing for your most critical suppliers, ones that if unavailable would result in an immediate, significant operational impact or inability to service your customers?

Figure 5a: If so, how many critical suppliers are on that list?



In the last 12 months, regulatory compliance scrutiny has increased more than any other risk factor as a driver of third-party supplier risk.

Figure 6: Based on your observations, how has the overall risk associated with third-party suppliers changed in the last 12 months relative to the following factors?*

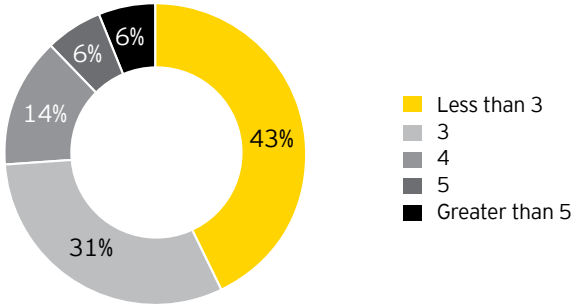


*Labels 2% or less not shown

Segmentation

As in prior years, more than nine in 10 respondents use five or fewer segments in their supplier risk management programs. Organizations using five or more segments have been almost cut in half from last year's finding of 27%, to 14%, which indicates a continued consolidation of the number of segments or tiers to three or four levels of risk.

Figure 7: How many levels of risk are used to segment or tier your supplier risk management program?



Outside of critical suppliers, nearly three-quarters of those surveyed have less than 10% of their suppliers subject to monitoring in their highest risk tier, continuing to confirm the "10% rule" established in previous years' surveys. Fifty-two percent of organizations indicated their second-highest risk tier contained between 10% and 25% of managed suppliers.

Companies are continuing to recognize that not all suppliers can be treated and monitored equally. The limited percentages in the critical and higher-risk tiers displays an understanding of the need to identify and focus on the suppliers that present the highest amount of risk to the organization.

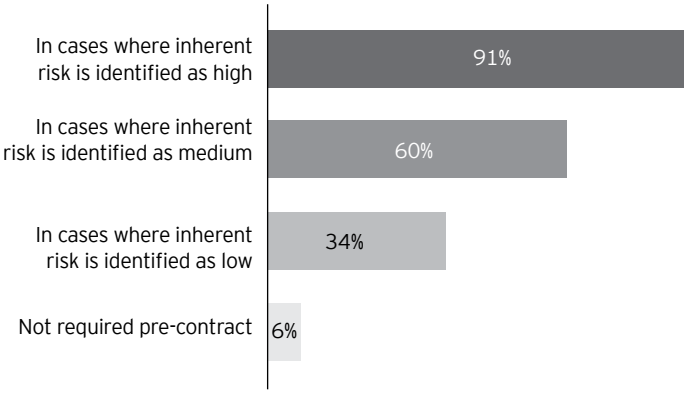
Selected survey results

Assessments

Pre-contract activities

Proactive supplier risk management practices have become more widespread. For suppliers where inherent risk is identified as "high," 91% of respondents complete control assessments pre-contract, up from 60% in the previous year. The movement to a function that performs more pre-contract assessments shows respondents are attempting to identify and make more informed, risk-based, on-boarding decisions to help mitigate unidentified risks that may appear after the relationship has been established.

Figure 8: Are control assessments completed pre-contract?*

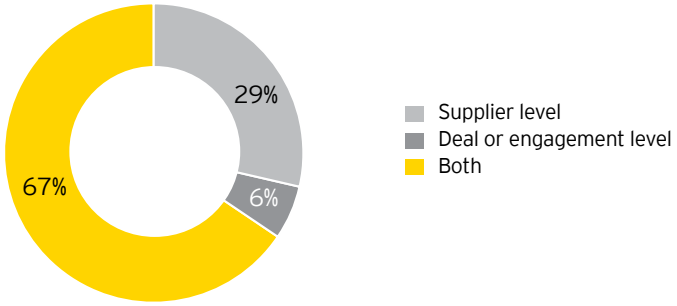


*Multiple responses allowed

Level of risk assessment

Companies are becoming more sophisticated in their assessments, with two-thirds of companies assessing risk at both the supplier and the service level, a 19% increase over last year. More specifically, with respect to assessment of risk at the service level, this percentage grew to 72%, from 56% last year, showing a continued focus on the identification of risk at the contract level, since this often varies greatly among suppliers that provide multiple services across a single organization.

Figure 9: At what level is your risk assessed and reported?



Frequency of reassessment

Eighty-six percent of respondents reassess their highest risk suppliers at least annually. Eight in 10 respondents reassess their second-highest risk suppliers less than every 18 months. Both of these ranges continue to be in line with the previous years' results, indicating a focus on the adjustment of risk model and segmentation criteria to manage the volume of effort, and not the frequency of review, assigned to each segment.

Figure 10: How often do you reassess your highest risk tier suppliers?

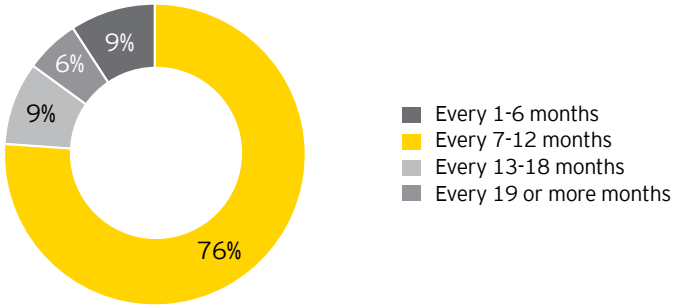
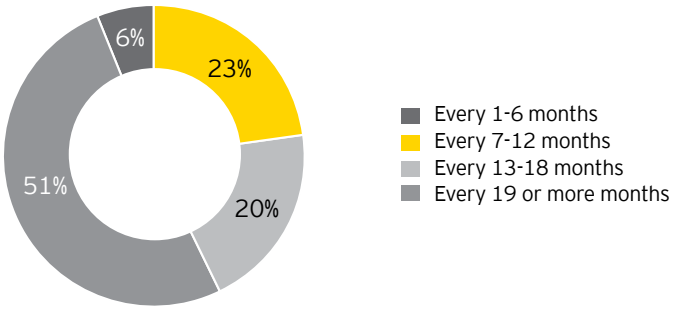


Figure 11: How often do you reassess your second-highest risk tier suppliers?



The overwhelming majority of respondents found minimal to marginal value in using the reports to reduce or remove the need to perform a control assessment.

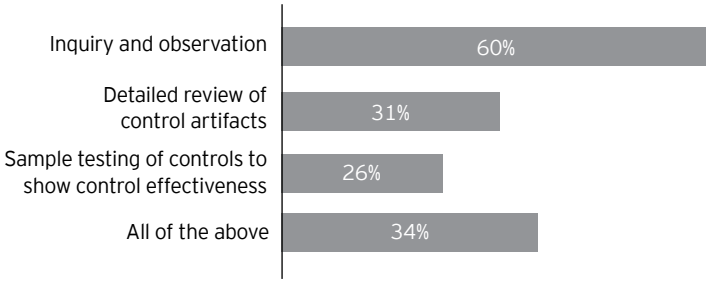
On-site reviews

We continue to see a trend toward shorter durations of on-site reviews, and a shrinking of the population where on-site reviews would be required through the usage of more advanced residual risk models. Sixty percent of respondents indicated they spent a day or less on site, up from 55% last year. With respect to the percentage of suppliers within the program that require an on-site review, 57% of US-based financial services organizations indicated it was less than 5%, while 59% of non-US-based financial services organizations indicated it was greater than 25%, showing a much larger propensity for on-site assessments within non-US-based organizations.

In addition to the time and depth of the assessments, the volume of assessment criteria has also decreased. Fifty-seven percent of respondents use 250 or fewer questions on their supplier review questionnaires, where in years past, the majority utilized more than 250 questions. For non-US-based organizations, this number is even more substantial, with 83% indicating they use 250 or fewer questions.

Unlike prior years, we have seen a decrease in the extent of testing conducted during on-site reviews. Only a third of respondents indicated that they conducted sample testing of controls to assess control effectiveness. This shift may indicate that respondents understand the costs associated with the execution of on-site reviews, and the value of taking a risk-based approach to assess the risks most prevalent based on the services provided by their supplier populations. The more focused and risk-based approach brings cost savings by performing risk assessments only on in-scope criteria or in areas designated as higher risk.

Figure 12: Where on-site reviews are performed at supplier sites, what level of assessment is performed?



Selected survey results

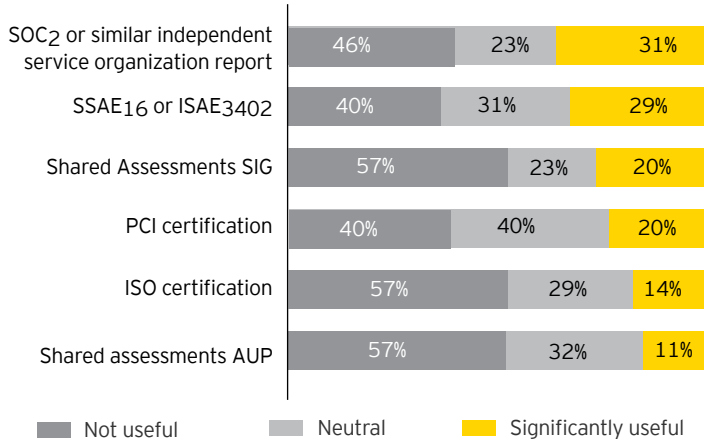
Evaluation criteria

Continuing with trends of previous years, 75% of institutions with more than 50,000 employees utilized proprietary frameworks for the execution of their assessment programs, while two-thirds of smaller organizations relied on industry-accepted frameworks.

Use of independent reporting

Throughout the history of supplier risk management, several reporting standards have been developed in an attempt to reduce the need for company-specific assessments of suppliers. To date, these reporting standards have not been widely adopted by firms that operate SRM functions. The overwhelming majority of respondents found minimal to marginal value in using the reports to reduce or remove the need to perform a control assessment. This is in part due to the proprietary nature of many organizations' assessment approaches, as each is designed to meet individual risk appetites and internal policy standards. In addition, organizations seem to struggle to be more efficient when mapping various standards to their own internal frameworks, only to come to a result where additional assessment activities are necessary to address the identified gaps. In parallel, many companies have been scrutinized for putting undue reliance on such reports and are now resistant to using them.

Figure 13: When you receive one of the reports listed below, how useful is it for reducing or removing your need to perform a control assessment in relation to a supplier?



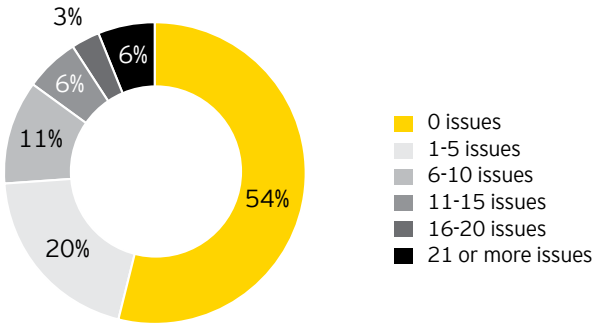
Issue management

Issue identification

A new area of focus in this year's survey was the identification and management of issues that are produced by assessment activities. We have observed that across our client base, issue management continues to be a challenge, with higher unresolved volumes than we have seen in past years.

Eighty percent of respondents find 10 or fewer issues, on average, per supplier control assessment. While that is encouraging, two-thirds of respondents reported that only 40% of the issues have been remediated after six months. Although supplier risk assessments may be adequately identifying issues, reducing the issue remediation lifecycle, the lack of remediation presents a significant risk and is an opportunity area for operational savings.

Figure 14: On average, how many issues are identified per supplier control self-assessment?



Consequences of issues and incidents

In addition to the rising volume of unresolved issues, only 11% of organizations terminated more than five suppliers in the past year due to a supplier issue or breach. The majority (57%) have not terminated a single supplier for either reason.

The fact that issues are not being remediated on a timely basis and these issues and breaches are not leading to a termination signals a significant risk exposure. It could also indicate that some SRM functions are not mature enough to manage supplier terminations and transitions without significant costs and impacts to the business, leaving them heavily dependent on suppliers even when they are not delivering services at expected levels or with known risk exposures.

Oversight and governance structure

Oversight and governance continues to be a critical element of a mature supplier risk management function and is increasingly more of a focus during regulatory reviews (see "Regulatory oversight" section).

Quality assurance

Two-thirds of the organizations surveyed reported having a quality assurance (QA) function as part of the oversight and governance program, up from 50% last year. This is a positive trend that points to an increased focus on the operational efficiencies of the function. More than 50% of respondents indicating the existence of a QA program also noted that QA is conducted in the following areas:

- Control assessments and related evidence (74%)
- Issues and action plans (74%)
- Inherent risk assessments (70%)
- Supplier selection and competitive due diligence (57%)
- Supplier record information (52%)

We expect continued progress in this area as participants continue to face pressure to self-assess the health of the supplier risk management program and report to executive management.

Policy exceptions

More than three-fourths (77%) of respondents formally track policy exceptions as part of their SRM function. Of those that do, almost all (89%) reassess exceptions at least annually. The fact that the majority of our respondents are tracking and reassessing policy exceptions shows a high level of maturity in this area across all organizations and industries.

Figure 15: Is quality assurance (i.e., testing of internal compliance with program requirements) part of your oversight and governance program?

Figure 15a: If so, which of the following elements are subject to quality assurance?*

*Multiple responses allowed

Selected survey results

Regulatory oversight

At the beginning of the survey, 97% of participants indicated that regulatory compliance was a significant driver in the design and execution of their supplier risk management programs. Oversight and governance, along with due diligence activities and supplier assessments, topped the list of focus areas during the most recent regulatory reviews. Less focus has been placed on supplier selection and fourth parties.

Figure 16: During your most recent regulatory body review, which of the following were the areas of focus?*

*Multiple responses allowed

Foreign suppliers and sub-service organizations

Foreign suppliers

As expected, there is a wide variation in the use of foreign suppliers among both US-based and non-US-based participants. Only 13% of US firms reported that more than 15% of their suppliers were foreign-based, compared to 42% of non-US firms.

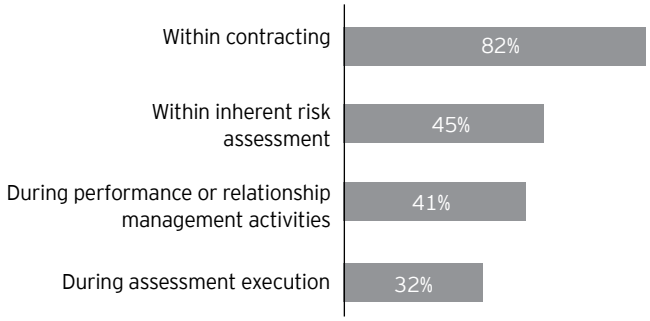
Sub-service organizations (fourth parties)

About two-thirds (63%) of respondents actively identify and use sub-service organizations, and most organizations (82%) identify sub-service providers within the contracting phase, up from 50% last year. This trend shows a movement from identification of fourth parties post-contract to pre-contract, allowing organizations to identify additional risks earlier in the process.

Figure 17: Do you actively identify and maintain the use of sub-service organizations by your suppliers?

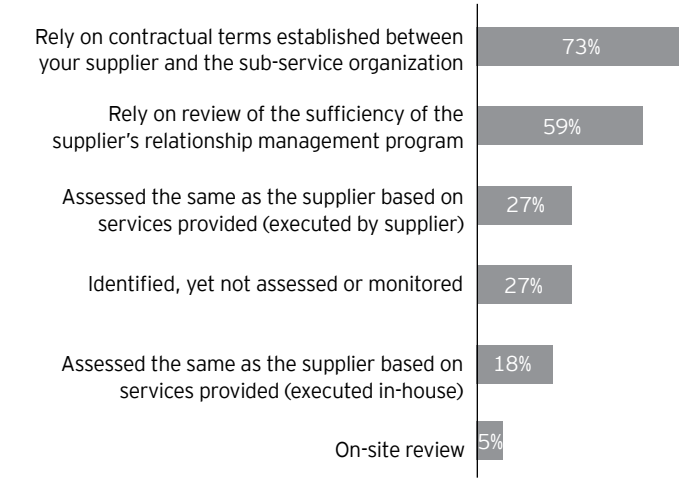
One-quarter (27%) of respondents noted they have identified, but not yet assessed or monitored, sub-service organizations. One-fifth of respondents review sub-service organizations the same way they review their suppliers.

Figure 17a: If so, how are sub-service organizations identified?



One-quarter (27%) of respondents noted they have identified, but not yet assessed or monitored, sub-service organizations. One-fifth of respondents review sub-service organizations the same way they review their suppliers.

Figure 17b: How does your organization assess/monitor sub-service-line organizations?



Cost and budget

On average, respondents indicated that they intended to spend as much as or more than they did a year ago on many of the activities associated with supplier risk management. Larger companies show a higher propensity to spend more in specific areas, most notably:

- On-site assessments (88%)
- Oversight and governance (75%)
- Audit or regulatory remediation requirements (63%)
- Improving the program as a whole (63%)

The focus on oversight and governance is understandable considering the regulatory focus and lack of maturity overall in this area. With the increased regulatory scrutiny, particularly for those vendors that are customer-facing, remediation of regulatory findings will continue throughout the year. As in past years, overall program improvement is also an area of focus.

As noted earlier, the scope and depth of on-site reviews for critical and high-risk suppliers have decreased in the past year. However, the fact that the spend on on-site reviews has not decreased in line with this shows that respondents are moving toward assessing a larger population of suppliers and possibly including medium- and lower-risk suppliers.

Selected survey results

Figure 18: Compared to the previous year, does your organization plan to spend more, less or relatively the same amount this year for the following activities within supplier risk management?*

	All respondents			Companies with 100,000+ employees			Companies with < 25,000 employees		
	Spend less	Spend the same	Spend more	Spend less	Spend the same	Spend more	Spend less	Spend the same	Spend more
Internal staffing (relationship management)	3%	**83%**	14%	0%	**75%**	25%	7%	**93%**	0%
Internal staffing (risk management)	6%	**63%**	31%	13%	50%	38%	7%	**79%**	14%
Outsourcing	3%	**60%**	37%	0%	50%	50%	7%	**71%**	21%
Improving third-party risk management	3%	49%	49%	0%	38%	**63%**	0%	57%	43%
Audit or regulatory remediation requirements	0%	**66%**	34%	0%	38%	**63%**	0%	**86%**	14%
Oversight and governance	3%	57%	40%	0%	25%	**75%**	0%	**79%**	21%
On-site assessments	6%	49%	46%	0%	13%	**88%**	7%	**71%**	21%
Remote assessments	6%	**63%**	31%	0%	**63%**	38%	7%	**79%**	14%
Technology enablement	6%	51%	43%	0%	50%	50%	14%	43%	43%
Procurement process	6%	**71%**	23%	0%	**75%**	25%	0%	**86%**	14%

*Figures above 60% noted in bold

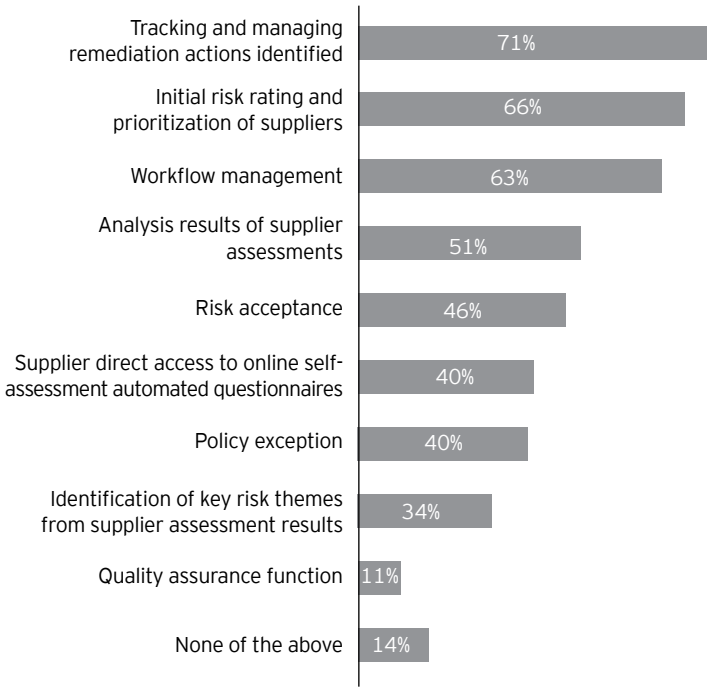
Use of tools and technology

Automated tools

The majority of organizations surveyed utilize automated tools to:

- Track and manage remediation actions (71%)
- Conduct inherent risk assessments (66%)
- Manage program workflow (63%)
- Analyze the results of supplier assessments (51%)

Figure 19: In which areas do you use automated tools?



Technical solutions continue to be focused on reducing manual processes within supplier risk assessment processes, and the extent of usage of these technologies continues to be consistent year over year. The only notable variance between this year and last is a reduction in the use of automated tools to facilitate the execution of online assessments: 40% this year vs. 63% in the previous year. This reflects that organizations have struggled in past years with pricey implementation of tools for solving execution issues only to find their processes more complicated and costly to maintain. In several organizations, we have seen significant expenditures related to access management, both on the internal and vendor side, as well as additional outlay in system configurations to meet internal process needs. Organizations are now reassessing whether and how these tools are actually enabling processes or making them more efficient.

Tool integration

Two-thirds of respondents indicated that tools used within supplier risk management functions do not integrate into enterprise risk reporting systems. Of the third that do, less than half (42%) are fully integrated, which demonstrates that many organizations continue to struggle with fragmented technology solutions.

The use of tools and technology to enable and drive the supplier risk management program is a significant item our respondents are factoring into their future state. Integration with enterprise risk models is a key step in ensuring standardized management of all risk types across the enterprise. We also believe that this integration would reduce the issue management cycle time, which was previously discussed as a significant risk. While easily agreed to in theory, a major obstacle is that the technologies used often vary greatly between different risk functions, leading to intensively manual integration processes to achieve a common or standardized tracking system.

The future of supplier risk management

As we think about the coming years, it is clear that the demands for sound risk management practices and continued regulatory scrutiny will further drive the focus on and development of supplier risk management. Within the US during the third quarter of 2012, federal regulators, including the CFPB, issued multiple Consent Orders to two of the top five credit card issuers. Each had significant financial repercussions, which included fees to be remediated to customers and civil money penalties. We expect this focus to continue throughout the UK, Europe, Australia and Asia as other regulators learn from the lessons of the US.

A call for action

Continuous regulatory scrutiny and increased corporate governance requirements by shareholders require organizations to monitor and manage their supplier risk more efficiently. Oversight and governance continues to be a critical element of a mature supplier risk management function and is increasingly more of a focus during regulatory reviews. This means that organizations need to:

1. Start involving their operational risk and compliance function even further in their supplier risk management program
2. Conduct pre-contract assessments for high risk suppliers to help identify potential issues and make more informed, risk-based, on-boarding decisions to help mitigate unidentified risks
3. Include foreign suppliers and sub service organizations in their supplier risk management program from the pre-contract stage
4. Finally, continue using tools and technology to enable and drive the supplier risk management program and work towards integrating these with enterprise risk reporting systems.

Ernst & Young would like to express its appreciation to those who took the time to participate in the survey. We suggest companies use these survey results as a starting point when considering ways to increase operational efficiency and better meet growing regulatory demands.

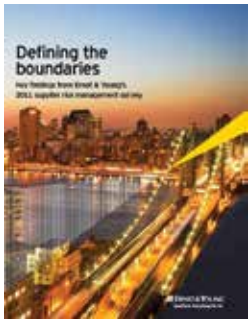
Key takeaways

- **Role clarity:** We continue to see a mature progression of role clarity within several key aspects of supplier risk management programs. As organizations change to adapt to the pressures of today's regulatory environment, a clear designation of the interaction between the line of business and respective specialist groups (e.g., procurement, risk, information security) is critical to the sustainability of the function. Over the past few years, we have also seen compliance and operational risk functions play a bigger role in an effort to match program requirements to complementary skills.
- **Risk model fluctuation:** Risk and segmentation models continue to fluctuate to adjust to the needs of each organization. There is no one right model; however, organizations are attempting to create more transparent models in an effort to provide more insight on specific risk attributes. Classifications such as High, Moderate and Low, or Tier 1, 2 or 3, are being replaced with designations such as Client Facing and Enterprise Critical. This also allows for monitoring routines to be standard within each classification.
- **Issue management:** This part of the assessment process continues to be the most challenging. While automation helps to reduce a certain amount of effort, exhaustive and large assessment questionnaires continue to build a significant backlog of issues. Since our previous survey, the amount of questions per questionnaire has decreased, but we continue to see a significant issue backlog and few vendors being terminated. Assessments must be focused on the specific risks applicable to the services provided by the supplier and the existence of a baseline control environment, all under consideration for a residual risk model.
- **Quality assurance (QA):** Quality assurance programs increased from 50% last year to 66% this year. This is a very positive development. A critical aspect of any oversight and governance function, QA procedures assist in attesting to the health of the overall function and are foundational in instilling consistency and compliance with internal policies. This is typically a foundational focus of any regulatory examination, and a formal QA role is essential to the continuous measurement of a program.
- **Regulatory compliance:** As regulatory bodies around the globe continue to mature in their focus on vendor management, regulatory compliance with consumer-based standards and laws will continue to be a primary focus. As stated in our findings, we have seen in the US significant attention given to identifying consumer conduct infractions that may be pervasive across the market. We expect this trend to continue through non-US regulatory bodies in the coming years.
- **Spend:** As long as the expectations for risk management continue to increase and the definition of suppliers continues to expand, reduction in spend does not seem likely for 2013. Organizations will need to continue to adjust risk models and rationalize supplier bases in order to effect change and reduce costs.

Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our *Insights on governance, risk and compliance* series at **www.ey.com/GRCinsights**



Defining the boundaries: key findings from Ernst & Young's 2011 Supplier Risk Management Survey

www.ey.com/DefiningTheBoundaries

Don't let your supplier take you down

www.ey.com/ProcurementRisk

Progress in financial services risk management: a survey of major financial institutions

www.ey.com/FS_risk_management

Fighting to close the gap: Ernst & Young's 2012 Global Information Security Survey

www.ey.com/giss2012

Driving improved supply chain results: adapting to a changing global marketplace

www.ey.com/ImprovingSupplyChain

Supply chain segmentation

www.ey.com/SupplyChainSegmentation

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 167,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

About Ernst & Young's Advisory Services
The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 25,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization you require services that respond to your specific issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

EYG no. AU1664

In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ED none

How Ernst & Young makes a difference

At Ernst & Young, our services focus on our clients' specific business needs and issues because we recognize that these are unique to that business.

Effective risk management is critical to helping modern organizations achieve their goals and it offers the opportunity to accelerate performance while protecting against the uncertainties, barriers and pitfalls inherent in any business. Integrating sound risk management principles and practices throughout operational, financial and even cultural aspects of the organization can provide a competitive advantage in the market and drive cost-effective risk processes internally.

Our 6,000 Risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective support – wherever you are in the world. We work with you to develop an integrated, holistic approach to managing risk and can provide resources to address specific risk issues. We understand that to achieve your potential, you need tailored services as much as consistent methodologies. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or a member of our team listed below.

Contact details of our Risk leaders

Global RISK Leader		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Area RISK Leaders		
Americas		
Jay Layman	+1 312 879 5071	jay.layman@ey.com
EMEIA		
Jonathan Blackmore	+44 20 795 11616	jblackmore@uk.ey.com
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.ey.com
Japan		
Shohei Harada	+81 3 3503 1100	harada-shh@shinnihon.or.jp