About the survey

Between February and April of 2014, EY surveyed 36 global financial services firms with supplier risk management (SRM) functions in the retail and commercial banking, investment banking, insurance and asset management sectors.

The purpose of this year’s survey is to assist financial firms as they strive to achieve balance between regulatory expectations and operational effectiveness. Two-thirds of the firms surveyed have had SRM programs for more than three years, and half have had their programs in place for more than five years.

New for this year’s survey is the inclusion of respondent commentary during the survey process. We used this commentary to further reinforce and provide more context on the results.

This is the fourth SRM survey that EY has conducted since 2010. Three years have passed since a wave of mortgage-related consent orders changed the regulatory landscape in financial services, and we continue to see a heavy focus on regulatory change and its impact on how organizations define and deploy various aspects of SRM functions.

Over the past four years:

- We have seen fluctuations in operating model considerations and points of ownership across a variety of life cycle components – specifically between business units and central functions and control groups. This becomes more evident as the definition of a supplier expands and risk models grow to react to consumer protection oversight issues and publicly reported data breaches.

- We continue to see expansion (comparing to the 2012 survey), and now contraction this year, of the risk-managed supplier base as a percentage of total suppliers, all between 10% and 15%, with a broader focus on “critical” suppliers within that population.

- Regulatory pressure continues to impact spend on programs, which has shown that many organizations are spending the same or more on various functional components.

- There remains little consensus on what standard to use for assessment questionnaires, and the majority of firms are still not reporting suppliers’ breaches to their boards of directors.

- Changes to risk models, a focus on issue management and a widening of re-assessment timeframes – coupled with the increased leveraging of industry standard reports – contributes heavily to the market’s continued pursuit of “Achieving Balance” in the execution of SRM programs.
Introduction

Firms are currently enhancing programs, while seeking direction as to how they should handle risk posed by suppliers. Lines remain blurred as to who bears ultimate responsibility for various SRM functions. This has resulted in a balancing act for businesses, as they adapt to new standards and manage risk efficiently.

This survey is unique in that it was conducted shortly after the Office of the Comptroller of the Currency (OCC) and the Board of Governors of the Federal Reserve System (FRB) issued bulletins in October and December of 2013, respectively, that offered more prescriptive SRM guidance. We asked participants to respond to questions across the following key areas of their SRM programs:

- Roles and responsibilities
- Risk models and tiering
- Assessments
- Issue management
- Regulatory oversight
- Sub-service organizations
- Tracking and reporting
- Tools and technology
- Current and future investments

In the pages that follow, you will find the results of this survey in addition to evolving SRM trends. We look forward to discussing this report with you and sharing our outlook on SRM in the financial services industry.
Key themes

Roles and responsibilities
- Lines of business personnel own performance monitoring (74%) and issue remediation (67%). Ownership of the compliance assessment process continues to trend to Operational Risk/Compliance (47%).
- Information security and business continuity assessments are mostly owned by Information Security (78%).

Assessments
- In line with last year, approximately 90% of respondents complete control assessments pre-contract when risk is identified as “high.”
- Half of the organizations surveyed perform control assessments pre-contract when risk is identified as “medium,” down from 60% last year.
- Fewer firms reassessed their highest risk suppliers at least annually in 2014, as compared with 2013 (70% vs. 86%), indicating firms continue to apply more advanced residual risk models to adjust the frequency of effort year-over-year.
- Fifty-eight percent of respondents perform assessments pre-contract for customer-facing suppliers.
- Three-quarters of reviews are done remotely; on-site reviews typically last one to two full days.
- The number of organizations that use 250 or fewer questions on supplier review questionnaires increased over last year (57% in 2013 vs. 69% this year).
- Businesses are beginning to leverage industry standardized reports in assessing risk, specifically SOC2. Usefulness of SOC2 has increased from 31% to more than 50%.

Risk models and tiering
- The percentage of suppliers subject to risk monitoring continues to align with the historical average of between 10% and 11%. About 36% of the respondents have increased suppliers that are subject to monitoring, down from last year.
- Approximately 67% of businesses separate suppliers into three or four risk tiers.
- Consistent with prior surveys, about 70% of organizations indicated their highest-risk tier was about 10% of the overall population (excluding critical suppliers).
- More than 85% of respondents maintain a critical supplier list, and most (58%) keep 40 or fewer suppliers on the list. Sixty-eight percent keep 60 or fewer on their list. Interestingly, there is no correlation between the size of the firm and the size of its critical supplier list.

Issue management
- Similar to last year, 81% of respondents find an average of 10 or fewer issues per supplier control assessment.
- Approximately 70% of respondents said at least 40% of the issues were remediated after six months, a significant increase from the previous year’s survey.
Regulatory oversight

- Due diligence of suppliers, as well as oversight and governance, continue to top the list of focus areas during regulatory reviews.
- Regulators are becoming increasingly focused on critical suppliers, fourth parties and the assessment of security and business continuity, while focus on issue management and risk acceptance has dropped 33% from the prior year.
- The number of organizations that have a quality assurance function as part of the oversight and governance program increased to nearly 80%, up from 66% last year and 50% the year before.

Sub-service organizations

- Seventy-one percent of firms identify sub-service organizations, but fewer organizations identify sub-service providers within the contracting phase (60% this year vs. 83% in 2013), indicating this is being pushed further into the monitoring cycle.
- Most respondents (84%) said they rely on their suppliers’ and sub-service organizations’ contractual relationships to monitor fourth-party performance.

Tools and technology

- While there is no industry-wide consensus, more firms are shifting away from proprietary tools.
- Half of respondents indicated current tools used within SRM functions do not integrate into enterprise risk-reporting systems.
- Forty-seven percent of firms use spreadsheets to track issues.

Current and future investments

- Supplier risk management spending is increasing across the board: 63% of firms plan to boost spending on internal staffing for risk management and 57% will spend more to improve risk management.
- Most firms plan to increase the scope and depth of assessments within the next year.

Tracking and reporting

- At nearly 80% of firms, senior management only receives reports on suppliers that have had breaches or incidents. Only 40% of respondents report these suppliers to the board of directors.
Roles and responsibilities

Supplier oversight responsibility

As in past years, there is a lack of consensus as to who owns various aspects of SRM programs. Trends are starting to emerge, as businesses continue to determine the optimal organizational model. Typically, Procurement is responsible for contract negotiation, Information Security handles both information security and business continuity assessments and individual lines of business oversee performance monitoring and issue remediation. However, in other areas, such as oversight and accountability, there is variation among which functional area has primary responsibility for executing a specific portion of the SRM program.

For the second year in a row, the role of Operational Risk/Compliance grew significantly. Now, almost half of the respondents indicate the function oversees regulatory compliance assessments. Regulatory actions from Consent Orders and new regulatory guidance from the OCC and FRB have played a part in this change. The shift away from the line of business and procurement areas to the risk management and compliance areas also appears to be an effort to engage more skilled resources in execution of these regulatory compliance assessments. A similar evolution occurred in that the Information Security function now oversees both information security and business continuity assessments in 78% of firms.

Selected survey results

“We have risk partners identified through the whole corporation. So, it is the process not only of getting the [supplier] identified that we may be conducting business with, we have our own strategic sourcing department that does that. They are then vetted by our supplier risk management program in operational risk. Legal is involved in all of the contracts and all of what happens. We’re [Information Risk Management] brought on board to do the due diligence, which includes an onsite assessment, and an onsite assessment annually thereafter dependent upon a specific supplier, line of business and the regulations that would govern that particular line of business.”

— Executive, financial services firm
### Figure 1: Supplier risk management responsibility

Which functional area has primary responsibility for executing each of the following components of your organization's SRM program?

<table>
<thead>
<tr>
<th></th>
<th>Procurement/ Purchasing</th>
<th>Information Security</th>
<th>Internal Audit</th>
<th>Legal/General Counsel</th>
<th>Operational Risk/Compliance</th>
<th>Line of business</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pre-contract</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contract negotiation</td>
<td>61%</td>
<td>0%</td>
<td>0%</td>
<td>33%</td>
<td>3%</td>
<td>3%</td>
<td>0%</td>
</tr>
<tr>
<td>Planning</td>
<td>40%</td>
<td>6%</td>
<td>0%</td>
<td>0%</td>
<td>6%</td>
<td>49%</td>
<td>0%</td>
</tr>
<tr>
<td>Supplier selection</td>
<td>42%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>58%</td>
<td>0%</td>
</tr>
<tr>
<td>Financial viability</td>
<td>56%</td>
<td>3%</td>
<td>0%</td>
<td>0%</td>
<td>15%</td>
<td>21%</td>
<td>6%</td>
</tr>
<tr>
<td>Business reputation and qualification review</td>
<td>46%</td>
<td>6%</td>
<td>0%</td>
<td>6%</td>
<td>23%</td>
<td>17%</td>
<td>3%</td>
</tr>
<tr>
<td>Inherent risk assessment</td>
<td>29%</td>
<td>15%</td>
<td>3%</td>
<td>0%</td>
<td>18%</td>
<td>32%</td>
<td>3%</td>
</tr>
<tr>
<td><strong>Post-contract</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance monitoring</td>
<td>14%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>6%</td>
<td>74%</td>
<td>6%</td>
</tr>
<tr>
<td>Regulatory compliance assessment</td>
<td>14%</td>
<td>8%</td>
<td>0%</td>
<td>8%</td>
<td>47%</td>
<td>17%</td>
<td>6%</td>
</tr>
<tr>
<td>Information security and business continuity control assessment</td>
<td>8%</td>
<td>78%</td>
<td>0%</td>
<td>0%</td>
<td>3%</td>
<td>8%</td>
<td>3%</td>
</tr>
<tr>
<td>Issue remediation</td>
<td>8%</td>
<td>11%</td>
<td>0%</td>
<td>0%</td>
<td>6%</td>
<td>67%</td>
<td>8%</td>
</tr>
<tr>
<td>Customer complaint handling assessment</td>
<td>6%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>23%</td>
<td>57%</td>
<td>14%</td>
</tr>
<tr>
<td>Oversight and accountability</td>
<td>26%</td>
<td>0%</td>
<td>6%</td>
<td>0%</td>
<td>26%</td>
<td>31%</td>
<td>11%</td>
</tr>
</tbody>
</table>
Risk models and tiering

Risk monitoring and supplier oversight
Approximately 10% of suppliers are subject to risk monitoring, consistent with the similar “10% rule” of last year and previous years. However, this trend is not likely to continue. With regulators continuing to look at suppliers under the new guidelines, we expect to see an uptick in the number of suppliers subject to risk monitoring.

More than one-third of organizations increased their list of suppliers subject to monitoring. Those firms that are scaling back their supplier lists are doing so as part of a broader supply chain initiative to be more efficient and reduce risk.

Risk tiers
Most firms are now using three or even four risk tiers to categorize their suppliers. The number of organizations using two risk tiers fell to 11% from 43% a year ago, indicating an inherent flaw in a high-/low-risk profile model. Only 6% of firms have more than five tiers, which could make the program complex and difficult to manage.

Consistent with previous years, about 70% of organizations consider 10% of their suppliers to be in the highest-risk tier — not including critical suppliers. For larger businesses, the quantity is slightly higher: 35% have more than 10% of their suppliers in the highest-risk tier.

Most firms have fewer than 40 suppliers that they view as critical, and 68% keep 60 or fewer businesses on their critical supplier lists. As in years past, only 14% do not maintain a separate classification for these most critical parties. Businesses with newer programs tend to have shorter lists, but there does not appear to be any correlation between the size of the firm and the number of suppliers on its list.

“We’re in the process now of a vendor rationalization effort, reducing our high-spend, high-risk vendors by at least 25%. So, we’re starting it from the center. We’re identifying redundant services and seeing if we can consolidate our vendor population by moving some other services to existing vendors. That should reduce our number of high-risk, high-spend suppliers that we’re doing monitoring on.”

— Senior vice president, banking firm
Figure 2: Change in number of suppliers

Approximately how much has the number of third parties subject to risk monitoring increased or decreased in the past year?

- Increased 50%
- Decreased 36%
- Remained the same 14%

Average increase: 31%
Average decrease: 11%

- Increased
- Decreased
- Remained the same

Figure 3: Levels of risk used to segment suppliers

How many levels of risk are used to segment or tier your SRM program?

- Less than 3 36%
- 3 17%
- 4 11%
- 5 31%
- Greater than 5 6%

Figure 4: Number of most critical suppliers

How many critical suppliers are on your list?

- 20 or fewer 16%
- 20–40 42%
- 41–60 10%
- 61–80 7%
- 81–100 10%
- More than 100 16%

“In less than one month, we will be training our board of directors on their responsibilities and also, in less than one month, we will submit a revised policy for them to approve and, within six months, we will be reporting on all aspects of our critical supplier activities to our board ... The volume of content that the board will be aware of will be larger.”

— Senior vice president, banking firm
Assessments

Pre-contract assessments

Across the board, businesses are proactive about SRM. For the second consecutive year, approximately 90% of respondents completed pre-contract control assessments for high-risk suppliers, up from 60% two years ago. This shows an increased focus on understanding a supplier’s control environment prior to engaging contractually. However, fewer are completing assessments for medium-risk suppliers. The number of firms conducting pre-contract assessments for medium-risk suppliers fell to 50% from 60% last year, as businesses weighed the cost vs. benefit of conducting an analysis.

There is also some indication that firms are applying more advanced residual risk models to eliminate the need for re-assessment of their highest-risk suppliers annually, with only 70% of this year’s respondents saying they perform reassessments annually, compared with 86% last year.

Surprisingly, with Consumer Financial Protection Bureau (CFPB) guidelines in place for certain suppliers, only slightly more than half of respondents complete assessments pre-contract for customer-facing suppliers.

Figure 5: Reasons for performing control assessments pre-contract

In what cases are control assessments completed pre-contract?

- Inherent risk is identified as high: 89%
- Supplier is considered critical: 81%
- Supplier is deemed to be customer-facing: 58%
- Inherent risk is identified as medium: 50%
- Inherent risk is identified as low: 19%
- Not required pre-contract: 6%

“One of the things we’ve implemented to speed up some of these [assessments] is during the onboarding process. If we’re identifying any major rated risks associated with the service, we’re actually writing those risks and action plan into the contract.”

— Senior vice president, banking firm
Regulatory uncertainty

Businesses are grappling with the pace of regulatory change surrounding expectations of supplier assessment activities, as well as the demand to conduct more assessments with the same amount of funding and resources. Smaller firms are struggling to find the resources to perform and manage assessments, and businesses are increasingly hiring external firms to address the problem. In fact, one respondent expressed the need to augment resources by as much as 50%.

On-site reviews

Firms are limiting on-site reviews to only their highest risk suppliers, as those reviews are typically more time-consuming and come with an increased cost. Instead of making regular site visits to all risk monitored third parties on a periodic basis, organizations are taking a “swat team” approach, where fewer resources are dedicated to only the most mission-critical reviews. Additionally, with resources continually strained, routine reviews are being conducted remotely. The decision of whether to conduct a review remotely or on-site is driven largely by inherent risk and, in some cases, by the previous year’s results.

Figure 6: Proportion of reviews, by type

In terms of total reviews being executed, approximately what percentage are:

- Remote reviews: 27%
- On-site reviews: 73%

“In order to understand and manage the vendors’ controls, to assess the vendors’ controls, you really need to be able to touch, feel and smell what they’re doing. And if you can’t get access to their documentation or their facilities to prove it, then it’s really a paper exercise.”

― Executive, insurance firm
“Our program is expanding to include other types of third parties that wouldn’t otherwise have been part of our formal testing and assessment program. So, we have the traditional vendors who we send data to or who host a web service for us, critical in that respect, but there’s a large part of our third party base that you wouldn’t necessarily classify as a vendor. For instance, we have affinity partners in our credit card business where we share data with them, but technically they’re not a vendor. We have groups of third parties who host trading servers and trading engines for us around the world for low latency trading with the exchanges. They, up until now, have not been included as part of our traditional vendor management program. But, following the OCC 2013-29 directive, which expanded the definition of a third party, this has now brought those sort of relationships into focus.”

— Executive, banking firm

Assessments

Assessment standards

There remains little consensus on what standard to use for assessment questionnaires. Organizations are evenly split as to whether to use proprietary guidelines or industry standards, such as BITS, ISO or COBIT. Additionally, organizations are shortening the volume of assessment criteria in their questionnaires. The number of respondents with 250 or fewer questions grew to 69% this year, up from 57% last year.

In previous years, independent assessments and opinions were not widely adopted and most respondents found marginal value in using standardized reports to limit the need for a control assessment. However, in 2014, about half of the firms found SOC 2 to be useful in reducing the need for control assessments – 31% more than last year. Additionally, 41% said PCI certification was useful in reducing the need for assessments and 41% found SSAE 16 and ISAE 3402 useful.

Figure 7: Baseline for control self-assessment questionnaire

What is the primary guidance used as a baseline for your control self-assessment questionnaire?

<table>
<thead>
<tr>
<th>Proprietary/Institutional</th>
<th>44%</th>
</tr>
</thead>
<tbody>
<tr>
<td>BITS Shared Assessments Program</td>
<td>24%</td>
</tr>
<tr>
<td>ISO</td>
<td>21%</td>
</tr>
<tr>
<td>COBIT</td>
<td>6%</td>
</tr>
<tr>
<td>Other</td>
<td>6%</td>
</tr>
</tbody>
</table>
Figure 8: Largest control self-assessment questionnaire

With respect to the largest control self-assessment questionnaire you use to assess your highest-risk third parties, what is the total number of questions asked?

- Fewer than 50 questions: 22%
- 51–100 questions: 8%
- 101–250 questions: 39%
- 251–500 questions: 14%
- More than 500 questions: 17%

Figure 9: Usefulness of reports in reducing need for control assessment

When you received one of the reports listed below, how useful were they in reducing or removing your need to perform a control assessment in relation to a supplier?

- SOC 2 or similar independent service organization report: 52% useful, 27% neutral, 21% not useful
- SOC 1, SSAE 16 or ISAE 3402: 41% useful, 18% neutral, 41% not useful
- PCI certification: 41% useful, 15% neutral, 44% not useful
- Shared Assessment SIG: 26% useful, 10% neutral, 65% not useful
- ISO certification: 21% useful, 35% neutral, 44% not useful
- Shared Assessment AUP: 7% useful, 32% neutral, 61% not useful
Similar to last year, 81% of respondents found 10 or fewer issues per supplier control assessment. More issues are being resolved within six months, indicating that issue management processes have increased in maturity in the last 18 months. However, cost is the greatest determining factor in the length of the remediation process. For instance, high-cost items involving business process overhaul typically take more than six months to remediate.

Compared to last year, about half of the firms we surveyed have terminated a supplier as a result of a control issue or incident. Larger firms with more mature SRM programs are more likely to have terminated a supplier. Not doing so may leave companies reliant on suppliers with known risk exposures. In order to become more proactive on issues, businesses are looking to increase their due diligence pre-contract and identify and remediate risks earlier in the process.

**Issue management**

“It’s obviously the high-cost, technical implementations that require supplier solutions – data-leakage prevention, for example – requires a significant investment up-front to buy it and to implement and support it. Some of the quick wins can be implemented within a six month time frame, but other solutions, especially for mid-size or smaller organizations, of any size of investment have extended remediation time frames.”

– Executive, insurance firm

**Figure 10: Average number of issues identified per supplier control review**

On average, how many issues are identified per supplier control review?

<table>
<thead>
<tr>
<th>Number of Issues</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>No issues</td>
<td>6%</td>
</tr>
<tr>
<td>1–10 issues</td>
<td>75%</td>
</tr>
<tr>
<td>11–20 issues</td>
<td>14%</td>
</tr>
<tr>
<td>21 or more issues</td>
<td>6%</td>
</tr>
</tbody>
</table>
Regulatory oversight

Regulators continue to concentrate on due diligence activities and oversight and governance processes in their periodic reviews. These areas of focus have remained consistent and show the regulators’ aim on remediating risk prior to contracting, as well as the need for a stronger oversight function to confirm the program operates as designed in the future.

This year, the survey results indicated that regulators are beginning to look more at historic focal areas, such as security/business continuity and fourth parties, in addition to placing new focus on enterprise-critical suppliers, supplier compliance assessments and executive and board involvement. We would expect to see additional attention given to reporting, board involvement and supplier compliance assessments, since they were key parts of the OCC’s recent guidelines.

Based on the survey results, the most significant change in regulatory review was issue management and/or acceptance, a 33% decrease from the last year. The prior year’s focus drove improvement in this area, as evidenced by issues being remediated within six months.

The spotlight on the oversight and governance area has led to an increase in quality assurance efforts for many organizations. Seventy percent of businesses include quality assurance in their oversight and governance program, up from 66% last year and 50% the year before. Risk assessment and required documentation are most often subject to quality assurance, but one-third of firms subject all elements of their SRM programs to quality assurance.

“Implementing consumer safeguards is by far the greatest challenge. Number one, there’s a cost to it. Number two, some of the contract clauses — and it’s an issue for the industry — will not be attainable.”

— Senior vice president, banking firm

Figure 11: Regulatory body review focus areas

During your most recent regulatory body review, what were the most important areas of focus?
Sub-service organizations

Firms are still tracking their suppliers’ use of fourth parties: 71% identify the use of sub-service organizations by suppliers, up from 63% last year. Fewer businesses than last year are doing it pre-contract (60% vs. 82%), but regulatory observations lead us to believe this may change in the coming years. For now, this is being pushed further into the life cycle, largely because identifying fourth parties has become part of assessment questionnaires, and suppliers are often contractually required to notify customers of any fourth-party use.

Nearly all businesses are either directly or indirectly monitoring fourth-party performance, compared with three-quarters of firms a year ago. However, businesses are leaning heavily on contractual relationships between their suppliers and their sub-service organizations for this. Eighty-four percent of the firms we surveyed rely on contractual terms established between suppliers and their sub-service organizations to assess and monitor fourth parties. Only about a quarter of firms conduct independent fourth-party reviews.

Figure 12: Tracking of sub-service organization use by suppliers

Do you actively identify and track the use of sub-service organizations by your suppliers?

![Figure 12](image)

Figure 13: Methods for assessing and monitoring sub-service organizations

How does your organization assess/monitor sub-service organizations?

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rely on contractual terms established between your supplier and the sub-service organization</td>
<td>84%</td>
</tr>
<tr>
<td>Rely on a review of the sufficiency of the supplier's relationship management program</td>
<td>56%</td>
</tr>
<tr>
<td>Rely on a review of the fourth party performed by the supplier</td>
<td>36%</td>
</tr>
<tr>
<td>Perform your own independent review of the fourth party</td>
<td>28%</td>
</tr>
<tr>
<td>Identified, yet not assessed or monitored</td>
<td>4%</td>
</tr>
</tbody>
</table>
Tracking and reporting

New guidance from the OCC and the FRB will likely lead to more firms reporting on suppliers to their boards of directors. For now, however, firms report on suppliers to senior management, but not necessarily all the way up to the board of directors.

Most organizations currently do not report breaches or incidents, operational metrics, critical suppliers, suppliers with the highest inherent risk, suppliers with noted significant or past-due issues to their boards of directors. Approximately 60% do not report suppliers with breaches or incidents, 26% report critical suppliers and slightly less (23%) report suppliers with the highest inherent risk to their Boards.

Figure 14: Supplier reporting management

Please specify the level of management that you provide with the following types of reporting on suppliers.

<table>
<thead>
<tr>
<th>Suppliers with breaches or incidents</th>
<th>Board of directors</th>
<th>Senior management</th>
<th>Employees</th>
<th>No reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>40%</td>
<td>74%</td>
<td>63%</td>
<td>6%</td>
</tr>
<tr>
<td>Operational metrics of the program</td>
<td>26%</td>
<td>77%</td>
<td>54%</td>
<td>6%</td>
</tr>
<tr>
<td>Critical suppliers</td>
<td>26%</td>
<td>66%</td>
<td>51%</td>
<td>17%</td>
</tr>
<tr>
<td>Suppliers with highest inherent risk</td>
<td>23%</td>
<td>63%</td>
<td>63%</td>
<td>9%</td>
</tr>
<tr>
<td>Suppliers with noted significant or past-due issues</td>
<td>17%</td>
<td>77%</td>
<td>66%</td>
<td>9%</td>
</tr>
<tr>
<td>Suppliers with highest residual risk</td>
<td>17%</td>
<td>57%</td>
<td>54%</td>
<td>20%</td>
</tr>
<tr>
<td>Suppliers refusing to undergo assessment</td>
<td>9%</td>
<td>63%</td>
<td>60%</td>
<td>11%</td>
</tr>
<tr>
<td>Suppliers related to emerging risks</td>
<td>6%</td>
<td>46%</td>
<td>43%</td>
<td>31%</td>
</tr>
<tr>
<td>Suppliers in termination</td>
<td>9%</td>
<td>37%</td>
<td>46%</td>
<td>31%</td>
</tr>
<tr>
<td>All suppliers</td>
<td>6%</td>
<td>29%</td>
<td>60%</td>
<td>29%</td>
</tr>
<tr>
<td>New suppliers</td>
<td>3%</td>
<td>29%</td>
<td>66%</td>
<td>23%</td>
</tr>
</tbody>
</table>

“We're looking at our enterprise-critical vendors in a different perspective now with the new OCC guidance around board-level scrutiny of our critical activities ... We’ll roll up all the control-based assessments into a higher-level risk assessment document that we’ll take to the board on each of our critical activities. Any new critical activity coming on, we’ll give the board ample time to review and challenge due diligence, selection and the whole vendor end-to-end cycle prior to contract signing. We’ll also bring quarterly reporting to the board that will show inherent risk and residual risk of all our critical activities.”

— Executive, banking firm
Tools and technology

The lack of a “best-in-class” toolset is hindering integration of SRM tools into businesses’ overall reporting systems. Firms are moving away from proprietary tools, but there is little agreement as to what to adopt. The most-cited agreement is for an online control assessment facilitation tool: 40% use Archer, 37% use Archer for risk acceptance repository and 34% use Archer for an issue management tool.

With different tools being used across various functions, integration often requires manual processes and leads to widespread dissatisfaction with how well tools for SRM functions are integrated into risk reporting systems. Only 12% of businesses feel their risk management tools are well integrated into their overall risk management reporting systems.

Even with all of the tools and technology available today, nearly 50% of firms still use spreadsheets to track issues and exceptions. As SRM programs mature, this will likely change: 77% of businesses with SRM programs less than three years old rely on spreadsheets, compared with 30-40% of companies with more mature programs.

Figure 15: Use of tools

What tool do you use for each of the following functions?

<table>
<thead>
<tr>
<th>Function</th>
<th>Archer</th>
<th>SharePoint</th>
<th>Oracle</th>
<th>Ariba</th>
<th>SAP</th>
<th>Proprietary</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract repository</td>
<td>14%</td>
<td>11%</td>
<td>3%</td>
<td>29%</td>
<td>3%</td>
<td>9%</td>
<td>37%</td>
</tr>
<tr>
<td>Primary supplier inventory</td>
<td>34%</td>
<td>11%</td>
<td>9%</td>
<td>11%</td>
<td>6%</td>
<td>14%</td>
<td>37%</td>
</tr>
<tr>
<td>Online control assessment tool</td>
<td>40%</td>
<td>14%</td>
<td>0%</td>
<td>6%</td>
<td>0%</td>
<td>20%</td>
<td>34%</td>
</tr>
<tr>
<td>Issue management tool</td>
<td>34%</td>
<td>14%</td>
<td>0%</td>
<td>6%</td>
<td>0%</td>
<td>11%</td>
<td>43%</td>
</tr>
<tr>
<td>Policy exception repository</td>
<td>29%</td>
<td>11%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>20%</td>
<td>37%</td>
</tr>
<tr>
<td>Risk acceptance repository</td>
<td>37%</td>
<td>11%</td>
<td>0%</td>
<td>6%</td>
<td>0%</td>
<td>23%</td>
<td>29%</td>
</tr>
<tr>
<td>Documentation and reporting</td>
<td>31%</td>
<td>11%</td>
<td>6%</td>
<td>14%</td>
<td>3%</td>
<td>14%</td>
<td>40%</td>
</tr>
</tbody>
</table>
Current and future investments

SRM spending is on the rise. Technical solutions are fragmented and sub-scale, so businesses are increasing headcount rather than investing in automation. This year, 63% of respondents said they plan to increase staffing for risk management, while only 40% plan to invest more in technology.

Businesses are also more likely to increase spending for on-site assessments versus remote assessments, indicating a greater depth required for assessments done in person. Routine reviews are done remotely to preserve resources. However, for on-site reviews, firms are shifting to a “swat team” approach that allows them to dedicate a smaller group of resources to only the most mission-critical reviews, resulting in a longer on-site visit.

Moving forward, nearly all businesses will increase the scope and depth of assessments. Three-quarters of the largest firms will make changes within the next six months, as government pressure continues to mount and financial services organizations learn to adapt.

“We went from just performing traditional information security and business continuity physical security reviews to encompassing 14 different policies like anti-money laundering, anti-bribery corruption, and increased scrutiny around financial monitoring. So, I think the scope has increased exponentially. Resources have increased by 50%.”

— Executive, banking firm

**Figure 16: Methods for issue and exception tracking**

How are issues and exceptions stored and tracked?

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spreadsheets</td>
<td>47%</td>
</tr>
<tr>
<td>Enterprise-level issue management system (inclusive of all issues)</td>
<td>41%</td>
</tr>
<tr>
<td>Centralized supplier program-specific tool</td>
<td>41%</td>
</tr>
<tr>
<td>Various repositories by the line of business or business unit</td>
<td>35%</td>
</tr>
<tr>
<td>Various repositories by the assessment execution group</td>
<td>15%</td>
</tr>
<tr>
<td>Within the assessments themselves</td>
<td>15%</td>
</tr>
</tbody>
</table>

**Figure 17: Change in risk management spending**

Compared to the prior year, do you plan to spend more or less for the following activities?

- **Procurement process**: Spend more (32%), Spend less (3%)
- **Internal staffing – risk management**: Spend more (63%), Spend less (3%)
- **Oversight and governance**: Spend more (46%), Spend less (3%)
- **Internal staffing – relationship management**: Spend more (46%), Spend less (3%)
- **Technology enablement**: Spend more (40%), Spend less (3%)
- **Improving risk management**: Spend more (57%), Spend less (3%)
- **Outsourcing**: Spend more (37%), Spend less (3%)
- **On-site assessments**: Spend more (43%), Spend less (6%)
- **Audit or regulatory remediation requirements**: Spend more (37%), Spend less (6%)
- **Remote assessments**: Spend more (29%), Spend less (9%)

**Figure 18: Changes to SRM program**

In what time frame do you anticipate significant changes to your SRM program?

- Increased scope of the assessments: 54% (0–6 months), 23% (7–12 months), 20% (13–18 months), 3% (No changes expected)
- Increased depth of the assessments: 51% (0–6 months), 26% (7–12 months), 11% (13–18 months), 11% (No changes expected)
- Program requirements: 46% (0–6 months), 26% (7–12 months), 4% (13–18 months), 14% (No changes expected)
- Closer integration between risk management and procurement: 51% (0–6 months), 20% (7–12 months), 11% (13–18 months), 17% (No changes expected)
- Implement a tool to help perform and manage the assessment program: 26% (0–6 months), 31% (7–12 months), 26% (13–18 months), 17% (No changes expected)
- Significant changes in the operating or organizational model: 37% (0–6 months), 9% (7–12 months), 20% (13–18 months), 34% (No changes expected)
- Significant increase in size of internal team involved in assessment program: 23% (0–6 months), 11% (7–12 months), 20% (13–18 months), 46% (No changes expected)
Supplier risk programs will need to continually adapt in order to respond and adhere to new and existing regulatory initiatives and further maturity in internal risk management functions. Additionally, attention needs to be given to enhancing technology-based tools to enable the process and the definition of enterprise level operating models, so that these programs can become more efficient, effective and sustainable.

EY provides practical regulatory and technology advisory services to its clients worldwide. Our cross-functional team can assist financial service organizations in achieving balance, as they work to manage supplier risk management in this new regulatory environment. For more mature firms, our experienced team has augmented its existing risk management and assessment activities, and we are helping to redeploy the structure of the SRM function from a process and procedure perspective in less mature firms.

Following are some key steps that should be considered to help your business better prepare your SRM program for impending change:

- Program benchmarking by an independent third party to provide an occasional external perspective of your program with respect to the industry and your peers
- Challenge assessment frameworks and execution models to align efforts to guiding principles and objectives
- Leverage low or fixed cost support models with external partners to enhance global reach and speed to market
- Engage relevant stakeholders in open discussions around supplier performance and risk management
- Continually engage executive management and the board or board sub-committees in key decisions around critical suppliers, supporting alignment with the organizations objectives and risk appetite
- Leverage committee and governance structures in providing “effective challenge” of risk and supplier decisions, as well as structural and operational aspects of your program in an effort to achieve balance within your organization

To learn more about how regulation and changing business trends might affect your organization and the specific actions you should take, contact one of the following EY professionals:

**EY contacts**

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chris Ritterbush</td>
<td>Executive Director</td>
<td>+1 212 773 4489 <a href="mailto:chris.ritterbush@ey.com">chris.ritterbush@ey.com</a></td>
</tr>
<tr>
<td>Rich Alber</td>
<td>Senior Manager</td>
<td>+1 212 773 6199 <a href="mailto:rich.alber@ey.com">rich.alber@ey.com</a></td>
</tr>
<tr>
<td>Matthew Moog</td>
<td>Senior Manager</td>
<td>+1 212 773 2096 <a href="mailto:matthew.moog@ey.com">matthew.moog@ey.com</a></td>
</tr>
</tbody>
</table>
Want to learn more?

Centralized operations: the future of operating models for Risk, Control and Compliance functions
This paper discusses which risk, control and compliance capabilities are being shifted into new, centralized operating models (and which are not); and the challenges in making this transition.

Managing third-party relationships in the new regulatory environment
This alert discusses the recent formal guidance related to how banks manage the risks associated with their supplier relationships.

Turning risk into results: how leading companies use risk management to fuel better performance
This study explores EY’s experience with clients that shows turning risk into results requires a multifaceted approach.

In our 2014 survey, we discovered that organizations are making progress on building the foundations of cybersecurity—and this progress is important—however, most respondents report having only a “moderate” level of maturity in their foundations. There is still a lot to do.

Partnering for performance: part 1: the CFO and the supply chain
Partnering for performance is a series within the Master CFO Collection that explores the contribution CFOs can make by working in a business-partnering relationship with different functional areas of the business.

Maximizing value from your lines of defense: a pragmatic approach to establishing and optimizing your LOD model
The current economic environment and significant risk events over the last few years have caused companies to have a renewed focus on the effectiveness of risk management.

Please visit us at www.ey.com
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the 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 ey.com.

EY is a leader in serving the global financial services marketplace
Nearly 35,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Office today includes more than 6,500 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2014 Ernst & Young LLP.
All Rights Reserved.

SCORE No. CK0873
1408-1301999 NY
ED none

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

ey.com