## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction and methodology</td>
<td>2</td>
</tr>
<tr>
<td>Executive summary</td>
<td>3</td>
</tr>
<tr>
<td>Section 1</td>
<td></td>
</tr>
<tr>
<td>ITRM survey results</td>
<td>5</td>
</tr>
<tr>
<td>Section 2</td>
<td></td>
</tr>
<tr>
<td>Organizational information</td>
<td>31</td>
</tr>
<tr>
<td>Appendices</td>
<td>36</td>
</tr>
</tbody>
</table>
Welcome to EY’s Financial Services IT Risk Management Survey 2014

IT Risk Management has quickly become a key issue for executive management, risk committees and boards. The purpose of this survey is to understand the maturity of IT Risk Management (ITRM) in financial services organizations, and to identify changes and trends by comparing this year’s results with previous surveys.

This year’s survey provides insights into leading practices where companies are investing in ITRM, and where IT Risk Management is making the greatest impact.

Methodology

The survey was conducted by EY during the May-June period in 2014 across a number of financial services companies.

Sixty-four senior executives from functions that include risk management and information technology participated in this survey. Of those, 42% were located in EMEIA, 36% in the Americas and 22% in Asia-Pacific and Japan. Fifty-two percent of the participants hold C-level or officer titles; 20% are information technology or information security executives; and 5% are internal audit directors, with the remaining 23% comprising of a variety of IT and Risk professionals.
This year’s survey is greater in geographic scope than previous surveys in 2008 and 2013, as we focus the attention on ITRM frameworks, risk processes and key drivers, and in particular the role ITRM plays in an organization's overall risk management process.

Emerging themes in IT Risk Management

The results of this survey identified three emerging themes in ITRM today:

1. Improved maturity in ITRM
2. Heightened interest from Regulators globally
3. Emergence of Governance, Risk and Compliance (GRC) technology solutions

Improved maturity in ITRM

The overall survey results reflect a noticeable improvement in organization's focus and commitment to establishing and sustaining an effective ITRM program. A greater awareness of IT risks now exists across the financial services sector, particularly at Board and senior management level. IT risk management practices for technology are showing greater signs of maturity with effective frameworks, control baselines, technology (GRC and data reporting tools) and skilled IT risk professionals.

Heightened interest from regulators globally

From this year's global survey, we see regulators showing a heightened interest in IT risk. Regulators have an expectation that IT risks are defined and managed, and that management should use IT risk metrics to improve investment strategies and to facilitate the continuity of services to customers, counterparties and markets. More than half of the survey respondents tell us that publicity surrounding systems outages, security breaches and loss of data has resulted in a modest or significant impact on their ITRM program in the last 12 months. We believe this is a key factor behind the increased attention from Regulators. As a result of the heightened regulatory interest globally, we are seeing an increasing maturity in the implementation of the three lines of defence, by clear roles and responsibilities being defined within IT, operational risk, and internal audit.

In addition to IT risk reporting and establishing a risk program framework, seventy-eight percent of our respondents say that their ITRM responsibilities includes interfacing with regulators and auditors. This is a trend which is fast becoming a sizeable part of the job role of an IT Risk professional.

Emergence of GRC technology solutions

As organizations now start to address legacy technology infrastructure, many have established the risk profiles of IT assets and can better identify associated threats and vulnerabilities. Several organizations have started to effectively capture this risk intelligence through using Governance, Risk and Compliance (GRC) tools and technologies.
We expect organizations to channel more investments toward the improvement of risk management reporting through the design of key risk indicators and relevant performance metrics. The increased demand for information from different stakeholders drives the need for risk tools, which can aid accurate information gathering, assist trend analysis, and help manage remediation activity. Fifty-two percent of our respondents are utilizing technology to address risk and control activities, with 27% adopting specific GRC solutions.

The way forward ...
Despite the improved maturity of ITRM, financial institutions must continue to invest in ITRM programs by enhancing ITRM frameworks as their risk profile will continue to change. There continues to be a focus from regulators on ITRM and particularly on IT resilience as a result of several high-profile system outages. Organizations now need to invest in specifically addressing IT infrastructure risks to provide an IT service that is resilient and that meets the growing expectations of customers and the many different stakeholders. As ITRM continues to mature, there will be a greater need to also provide more effective techniques to report on IT risk and display key metrics through the use of GRC tools and technologies.

We would like to thank the organizations who have participated in this comprehensive survey of ITRM.

We hope that you will all find the survey both informative and beneficial to your organization.
Section 1

ITRM survey results
Summary points
► Most of the organizations surveyed have invested in ITRM, with only 8% of respondents still without a formal ITRM function.
► Ninety-two percent represents a significant increase from our previous surveys, with data collected in both 2008 and 2013 showing three out of four respondents had a formal ITRM function (76% in 2013).

Our view
► There has been a noticeable shift in the proportion of our respondents with a formal ITRM function, up from 76% in 2013 to 92% in 2014.
► A formalization of ITRM functions is underway in the financial services industry, with many organizations defining roles and responsibilities, policies and procedures, formal charters, strategies and other foundational points. This is in part driven by regulators, who are showing an increased interest in IT and are pressing for more information. There is now an expectation that IT risk will be defined and managed to enhance IT Services.
► There is no correlation between the size of the company and the formalization of the ITRM function. Our sample found organizations with annual revenues in excess of US$10b without a formal ITRM function.
Summary points

► Most of the organizations surveyed have invested in ITRM, with only 8% of respondents still reporting that they have no dedicated resources. Of the 92% with defined ITRM operating models with dedicated resources, most maintain functions with fewer than six full-time employees (43%).

► Nearly one in five of our respondents (19%) has a formal ITRM function that employs more than 30 full-time employees. All of the companies in this group have revenues in excess of US$1b.

Our view

► ITRM is gaining more visibility within organizations and there is a greater demand for informed knowledge, which may not have been the case a few years ago. However, staffing levels are still inadequate. This is a rapidly expanding area, as can be demonstrated by an increased awareness at the board level, a growing demand for IT-related management information, and the increased visibility in the recruitment market for individuals with IT risk skills.

► There is a low supply of talent in this area, which will need to be plugged by education and development investment.

Do you have a defined operating model with dedicated resources for IT risk?
Summary points

► 46% of the companies that we interviewed align their IT risk program framework to both the IT strategy and enterprise risk frameworks, whereas 8% do not align the IT risk program to either.
► Alignment is increasing – in 2013 just 23% told us that IT and enterprise risk management were fully aligned.

Our view

► Overall there is still some way to go before we see a common risk language implemented throughout the company so that programs are fully integrated. There is a need to align business and IT strategies for greater maturity.
► We see a greater need to build effective frameworks to enable effective reporting of risk in IT, which can enable senior management to make informed decisions and more effectively meet regulatory demands for information.
► Communication and alignment of functions within businesses could be improved to build consistency into the IT risk program framework.
The ITRM function needs to have a greater level of involvement and increased input at the board level if IT risk is to be properly incorporated into company strategy, and for the overall visibility of the program to improve.

With regulators increasingly interested in IT and pressing for more understanding and greater information, senior management needs better communication with the ITRM function in order to make more informed decisions.

Companies continue to have multiple teams performing IT risk assessments outside the ITRM function, which hampers their ability to form an entity view from a treatment and reporting perspective.

ITRM functions need to have more focus and carry more effort in vendor risk assessments.

The majority of the senior executives that we interviewed (63%) have a high involvement in the IT risk strategy for their organizations, our respondents all being in roles that intersect risk management and IT.

19% of our respondents say they have little or no involvement in technology enablement of the IT risk program, for example through the use of a Governance, Risk Management and Compliance tool.

22% of respondents say that the ITRM function has rare or non-existent involvement in third-party supplier assessments.
Summary points
► In all, 81% of respondents feel that their organization has formal and clear defined roles and responsibilities for the IT risk function.
► Only 8% disagree and believe their business is lacking in a formal and clearly defined mandate.
► These figures show an improvement on 2013, when 68% said they agreed with the statement, and the number that disagreed has dropped from 14%.

Our view
► The survey shows that roles and responsibilities appear clearly defined. Well-defined roles/responsibilities of an ITRM function could be the results of investment in ITRM frameworks.

Summary points
► Three out of four respondents say that their ITRM framework is aligned to a three lines of defense model, with a further 14% reporting that transition is in progress to such a model within their organization.
► 11% say that the framework in their organization does not align to a three lines of defense model.

Our view
► The three lines of defense model is now in place in most organizations, with a significant proportion currently transitioning to the model. This has improved in recent years.
Summary points

► The ITRM function is primarily responsible for IT risk reporting, alongside establishing the risk program framework for IT management and interfacing with regulators and auditors.
► The implementation of monitoring tools and technologies is considered to be a low priority for ITRM functions, as is the independent review of risk governance and management processes by internal and external auditors.
► IT risk reporting has overtaken identifying and evaluating risk response options in the order of priority since last year. In 2013, IT risk reporting was highlighted as a key responsibility by 78%, up to 94% this year.
► Interfacing with regulators and auditors has grown in importance for ITRM functions. It was seen as a key responsibility by 66% in 2013, and by 78% this year.

Our view

► Regulators are showing an increased interest in IT risk and seeking more information, particularly within the financial services industry. IT risk therefore needs to be defined and managed, and ITRM functions must increasingly take the lead in liaising with regulators and external auditors. We expect that this need for a greater interaction with regulators and auditors will grow significantly.
► The identification and evaluation of risks seems strong. There is a growing need to build effective frameworks to enable effective reporting of risk in IT. There is a need to understand any stress points and to apply adequate response to achieve resilience.
► It is clear that the ITRM function is a very diverse function with a wide set of responsibilities. With the increasing pressure on cost and efficiency and growing regulatory requirements the new ITRM function must be clearly defined, flexible and forward-looking.
To whom does the IT Risk Management function or oversight role report?

Summary points
► 37% report to the CRO and the same proportion to the CIO. The CRO has grown in influence in recent years - in our 2008 survey only 21% reported to a CRO, rising to 31% in 2013.
► Only 3% report to the CEO and just 3% report to the CFO, down from 9% and 6% respectively in 2013.
► Mature risk management functions report to either the CRO/CIRO or the COO.

Our view
► The survey shows that reporting lines appear clearly defined. Some have more than one reporting line. Compared to 2008, where 50% said that they report to the CIO, over the last five years more dedicated risk functions have been established resulting in more reporting lines.
► The reporting structure is primarily aligned to CIO or CRO, and trending toward the CRO is a positive trend as it shows more boards understanding the risks within IT and understanding IT from a business perspective.

<table>
<thead>
<tr>
<th>Role</th>
<th>2008</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief information officer</td>
<td>50%</td>
<td>34%</td>
<td>37%</td>
</tr>
<tr>
<td>Chief risk officer</td>
<td>21%</td>
<td>31%</td>
<td>37%</td>
</tr>
<tr>
<td>Chief executive officer</td>
<td>13%</td>
<td>9%</td>
<td>3%</td>
</tr>
<tr>
<td>Chief compliance officer</td>
<td>4%</td>
<td>12%</td>
<td>2%</td>
</tr>
<tr>
<td>Chief operation officer</td>
<td>-</td>
<td>26%</td>
<td>11%</td>
</tr>
<tr>
<td>Chief information security officer</td>
<td>-</td>
<td>14%</td>
<td>16%</td>
</tr>
<tr>
<td>Chief financial officer</td>
<td>-</td>
<td>6%</td>
<td>3%</td>
</tr>
<tr>
<td>IT chief risk officer</td>
<td>-</td>
<td>-</td>
<td>6%</td>
</tr>
<tr>
<td>Other</td>
<td>13%</td>
<td>14%</td>
<td>-</td>
</tr>
</tbody>
</table>
What impact has the following had on your ITRM program over the past 12 months?

- Global regulatory requirements
- Operation between multiple regulatory regimes (cross-border activities)
- Compliance activities
- Business resilience - BCP
- Use of and extent of reliance upon third parties
- ERM integration/risk conversion
- Increased requirements for measuring and monitoring IT risk
- Greater awareness of ITRM
- IT risk analysis/management reporting
- IT risk analysis/management activities
- Technology changes due to merger and acquisition activities
- IT infrastructure availability - DRP
- Social media activities
- Publicity surrounding security breaches and loss of data
- Other IT security programs (IAM, data leakage, etc.)
- Use of emerging technology (e.g., cloud computing, virtualization and mobile computing)
Summary points

► Compliance activities – Compliance activities are taking up a considerable amount of resource for ITRM functions, and having a significant impact on their work. Thirty-eight percent of respondents tell us the impact is significant; a further 28% refer to a modest impact. Just 9% of respondents believe compliance activities have had no impact on their ITRM function in the last 12 months, in line with 11% in 2013.

► Business resilience/BCP – Thirty-nine percent of our respondents say that business resilience and Business Continuity Planning is of modest concern to their ITRM functions, while 25% add that this area is having a significant impact on their programs. Just 8% see no impact from BCP, compared to 18% who felt similarly isolated in 2013.

► Increased requirements for measuring and monitoring IT risk – In all, 86% of respondents to our survey tell us that the increased requirements for measuring and monitoring IT risk that are being imposed by regulators are having an impact on their ITRM function, with 37% saying that impact is significant. In 2013, only 45% of those that we asked were seeing an impact that was either modest or significant.

► IT risk analysis/management reporting – Forty-two percent of our respondents say that IT risk analysis and management reporting is having a modest impact on their ITRM programs, with a further 34% saying the impact has been significant. Only 9% say they have felt no impact from IT risk analysis and management reporting on their ITRM program.

► IT Infrastructure/DRP – Thirty percent of our respondents tell us that the availability of IT infrastructure and Disaster Response Planning has had a significant impact on their ITRM function in the last 12 months, highlighting this as an area of some concern. A further 31% say it is having a modest impact, with just 5% feeling no impact.

► Emerging Technologies – Thirty-eight percent say that the use of emerging technology has had a significant impact on their company’s ITRM program in the past 12 months, with 42% reporting a modest impact, overall resulting in 80% noting an impact from emerging technologies.

Our view

► Compliance activities – Compliance has a heavy impact and continues to drive the focus on risk within organizations. This will have a positive impact in the long run but the value to requirements ratio is still not balanced for the financial services industry.

The enterprise level of the compliance footprint still has an impact. An integrated baseline for requirements has still not matured or been addressed effectively, but has been contributing to the success of risk and compliance programs.

► Business resilience/BCP – Business resilience and BCP is moving up the agenda for ITRM functions in the financial services sector. While the focus has significantly improved, however, it is still behind DRP in terms of both focus and effort.

► Increased requirements for measuring and monitoring IT risk – The financial services respondents to our survey this year are clearly feeling a heavy impact from the increased regulatory pressure being put on their organizations around measuring and monitoring IT risk.

These institutions are increasingly looking for more IT risk information, so that senior management can make more informed decisions, and to utilize risk to improve investment strategies and continuous service improvement.

► IT risk analysis/management reporting – With regulators calling for a greater degree of information about IT risk, there is increased pressure on ITRM functions to provide management reporting in a way that allows the board to meet those demands. The impact of IT risk analysis and management reporting demands is growing in significance as a result. Reporting has improved significantly but is still not at the level of sophistication expected by CROs and boards.

► IT Infrastructure availability – DRP – IT infrastructure availability and DRP are rising up the agenda of ITRM teams. As programs have improved we see a re-base lining of risk in DRP, and this is a very positive trend in catastrophic risk scenarios. This combined with a heightened regulatory focus should result in enhanced coverage going forward.

► Use of emerging technologies – The use of emerging technology is having a growing impact on ITRM programs. Technology change, including social media, impacts traditional IT processes and therefore the IT risk frameworks. There is a new need to understand stress points, and react appropriately. For example, there is an expectation that IT systems are always on, because an App on an iPad is always accessible. Embedding risk practices in early adoption of new technologies will be essential.
10 Have the following challenged or contributed to ITRM success in the last 12 months?

- Define roles and responsibilities to align to lines of defense: 28% posed a challenge, 42% contributed to success, 27% had no effect, 3% don't know.
- Technology tools to support ITRM: 33% posed a challenge, 24% contributed to success, 35% had no effect, 8% don't know.
- Tools to monitor and report risk: 39% posed a challenge, 31% contributed to success, 27% had no effect, 3% don't know.
- Staff resources to support ITRM: 55% posed a challenge, 25% contributed to success, 19% had no effect, 1% don't know.
- Financial investment to support ITRM: 39% posed a challenge, 34% contributed to success, 20% had no effect, 7% don't know.
- Competing objectives e.g., cost vs. control, performance vs. cost: 65% posed a challenge, 6% contributed to success, 21% had no effect, 8% don't know.
- The alignment of risk appetite to organizational control culture: 48% posed a challenge, 25% contributed to success, 16% had no effect, 11% don't know.
- Level of risk tolerance/risk appetite: 34% posed a challenge, 30% contributed to success, 28% had no effect, 8% don't know.
- Multiple risk assessments: 37% posed a challenge, 27% contributed to success, 24% had no effect, 12% don't know.
- Control rationalization: 30% posed a challenge, 17% contributed to success, 39% had no effect, 14% don't know.
- Integrated approach to risk management: 33% posed a challenge, 48% contributed to success, 17% had no effect, 2% don't know.
- Documented ITRM strategy: 19% posed a challenge, 48% contributed to success, 27% had no effect, 6% don't know.
- Support from executive sponsors: 16% posed a challenge, 72% contributed to success, 27% had no effect, 11% don't know.
Summary points

► **Define roles and responsibilities to align to lines of defense** – Forty-two percent of those surveyed tell us that the definition of roles and responsibilities to align with lines of defense has been a positive for the ITRM function in the last year, contributing to success.

► **Staff resources** – Securing staff resources to support ITRM has posed a challenge to many of our respondents, with 55% responding negatively as regards investment. This compares to 42% who in our 2013 survey said that investment was a challenge for their department.

► **Competing objectives** – Competing objectives, between costs and controls, or between performance and costs, are seen as a negative for the ITRM function - 65% say that these conflicts have posed a challenge to their operations in the last year. This is up significantly from 43% in our 2013 survey.

► **Control rationalization** – Thirty percent say that control rationalization has posed a challenge in the last year for the ITRM function, while just 17% feel that it has contributed to the success of the ITRM program.

► **Integrated approach to risk management** – Thirty-three percent say that an integrated approach to risk management has posed a challenge in the last year, up quite significantly from the 20% that answered the same in our 2013 survey. Forty-eight percent of those surveyed say that such an integrated approach has contributed to the success of the ITRM function’s initiatives in the last 12 months, down from 52% in 2013.

► **Support from executive sponsors** – Seventy-two percent of those surveyed say that support from executive sponsors has contributed to the success of the ITRM function’s initiatives in the last 12 months, compared to 60% a year ago.

Our view

► **Define roles and responsibilities to align to lines of defense** – It is clear that the appreciation of three defined lines of defense is growing.

► **Staff resources to support ITRM** – Staff resources are increasing but still fall some way short of what our survey respondents are looking for. This is in part as a result of a shortage of supply, with IT risk expertise increasingly hard to come by in the recruitment market.

► **Competing objectives** – Competing objectives pose a big issue for ITRM functions, leading to costs and investments lagging behind risk intelligence, especially around control improvements.

► **Control rationalization** – Control rationalization is still not where it needs to be, being largely seen as a negative or as neutral in its impact, as most ITRM functions have yet to achieve success in completion of these projects.

► **Integrated approach to risk management** – Frameworks are in place at most organizations and they are now working toward alignment of IT risk and Enterprise Risk, to deliver an integrated approach to Risk Management. There is a need to align Business and IT strategies for greater maturity, but this is not achieved without its challenges.

► **Support from executive sponsors** – With more pressure from board members and regulators, there are signs that executive sponsors are being more supportive of ITRM functions and supporting their success, though there are certainly still those that pose a challenge.
Which of the following risks are managed or monitored in the scope of the ITRM function?

**Summary points**

- IT continuity and disaster recovery, cyber security and data leakage are the most well monitored risks within ITRM functions.
- Data quality, offshoring and end-user computing applications are the risks that are least well managed or monitored by the ITRM functions that responded.

**Our view**

- Business-type technology risks, like those associated with offshoring, data quality and end-user computing applications, are less of a focus or concern. This may be because awareness within the business community regarding the maturity of operational risk programs in addressing business risk has had an effect on incidents or lowering of residual risks in those areas.
- IT continuity and disaster recovery has moved significantly up the agenda, having been only moderately monitored according to respondents to our 2013 survey, and now the chief concern.
Summary points

 ► 74% of organizations surveyed plan to increase spending in ITRM activities over the next 12 months and the majority will increase their financial investment in ITRM by 5% to 25%. This compares to 54% in our 2013 survey, with most planning to increase investment then by less than 5%.

 ► There is a positive trend toward quite significant increases in ITRM investment. Most investment will be in the banking sector.

 ► Only 3% of organizations plan to decrease their spending in ITRM activities by 5% to 25%; this figure was 14% in our 2013 survey.

 ► Analysis of the results indicates that investment for ITRM is independent of the size and scale of the company.

Our view

 ► Most survey respondents will increase their investment, and with the current changes in technology and the ever-changing regulatory landscape. Organizations that are not increasing their investment by 5%-25% will struggle to keep up with the pace of change.

 ► IT risk functions are currently in growth mode, and can benefit from greater formalization of methods and supporting processes.

 ► Having no formal ITRM function may result in higher levels of unplanned investments.

 ► Spending does not depend on the type of business, but rather on the maturity of the ITRM framework and function.
How will investment in ITRM be distributed in the next 12 months?

- Infrastructure risk: 19% No investment, 22% Low investment, 38% Moderate investment, 13% Significant investment, 8% Don't know
- Third-party suppliers: 16% No investment, 32% Low investment, 35% Moderate investment, 13% Significant investment, 4% Don't know
- New technologies (e.g., investment in GRC tools): 21% No investment, 25% Low investment, 27% Moderate investment, 17% Significant investment, 10% Don't know
- Risk reporting and monitoring (e.g., risk dashboard, regulatory monitoring): 5% No investment, 27% Low investment, 44% Moderate investment, 21% Significant investment, 3% Don't know
- IT control self-assessment: 13% No investment, 28% Low investment, 36% Moderate investment, 20% Significant investment, 3% Don't know
- IT risk management framework development (e.g., process formalization and maturity enhancement): 11% No investment, 31% Low investment, 36% Moderate investment, 19% Significant investment, 3% Don't know
- Alignment with ERM: 19% No investment, 44% Low investment, 22% Moderate investment, 13% Significant investment, 2% Don't know
- Training and education: 11% No investment, 44% Low investment, 28% Moderate investment, 11% Significant investment, 6% Don't know
- Staffing: 14% No investment, 17% Low investment, 38% Moderate investment, 27% Significant investment, 4% Don't know
Summary points

► **Infrastructure risk** – Infrastructure risk continues to be a key point of the ITRM budget, but only 13% expect to make significant investment in addressing infrastructure risk in the coming year. 19% do not plan to spend any money on infrastructure risk in the next 12 months.

► **Third-party suppliers** – Most respondents have earmarked third-party suppliers for moderate investment in the next 12 months, with 35% anticipating this level of spending, and another 13% expecting a significant spend.

► **New technologies** – New technologies are a growing feature of the ITRM budget, with 45% expecting to make a moderate or significant investment in such advances in the coming year. This figure was 23% in our 2013 survey. The biggest proportion of respondents say they will make a moderate investment in new technologies, such as GRC tools.

► **Risk reporting and monitoring** – Only 5% do not anticipate making any investment in risk dashboard and regulatory monitoring in the next 12 months.

► **ITRM framework development** – While companies continue to invest in ITRM framework development, such as process formalization and maturity enhancement, 19% expect to make significant investment in the area in the coming year. This figure was 8% in our 2013 survey.

   Overall, 45% expect a moderate to significant investment in ITRM framework development.

► **Staffing** – Many respondents have earmarked staffing for moderate investment in the next 12 months, with 38% anticipating this level of spending.

   Only 14% do not anticipate making any investment in staffing in the next 12 months.

Our view

► **Infrastructure risk** – infrastructure investments have been overlooked in the financial services industry, where there has been a shortfall between 2008 and 2013. Investments in infrastructure risk now needs to be significantly increased.

► **Third-party suppliers** – Third-party supplier investments will need to address more evidence-based risks and controls. Funding should be invested wisely to automate service validation, and third parties that also outsource additional functions and support fourth- and fifth-party suppliers are still not being effectively addressed.

► **New technologies** – The appetite for new technologies such as GRC tools remains low, with more than 20% planning no investments in such advances this year. The number planning significant investment has increased, but still the majority plan only low or moderate spending.

   Tools and technologies have improved the value of programs but investment in them is still not at the pace of market expectations. This could be the result of a lack of broader systems engineering (SE) for risk overall, driven by the fact that SE takes a significant amount of time and money to demonstrate strategic value and impact. This in conjunction with low investments and cost has led to siro solutions.

► **Risk reporting and monitoring** – The number of ITRM functions making no investment at all in their risk reporting and monitoring processes has dropped off considerably since our 2013 survey, down from 11% to 5%. But still most are anticipating moderate investment rather than any significant spending.

   Significant investments in metrics will be challenging without mature frameworks and control assessment baselines not in place. In such cases, metrics will require tremendous amounts of time and will provide limited value. Therefore, other areas must be focused on first.

► **ITRM framework development** – Investment in framework development has moved up the agenda a little for ITRM teams, but is still not earmarked for major investment. Funds are being committed to frameworks however, as functions continue to mature.

► **Staffing** – As the financial services industry emerges from the financial crisis and returns to investment mode, staffing in ITRM functions is on the agenda for growth. While significant investment is only planned by 25% of respondents, growth is expected by the majority of organizations, and far fewer than last year will not invest in their team staffing.

   The recruitment market for individuals with IT risk skills is heating up as a result of growing demand for talent in expanding teams.
Is there a common risk language (taxonomy) that is used?

Summary points
► 51% of our respondents now believe there is common risk language being used throughout their company.
► This is down from the 62% that agreed with this statement in our 2013 survey.
► 22% disagree that there is any common taxonomy being used; a figure that has increased from 11% a year ago.

Our view
► Organizations can identify the benefits from aligning their IT risk to the broader organizational risk management to effectively and efficiently achieve IT and business objectives.
► Common risk languages represent a positive step forward, even though a growing number of respondents tell us these taxonomies are not broadly used or understood.
How effective is your company with the following risk management activities?

Summary points

► **Providing IT with concise and actionable risk intelligence and recommendations** – Most organizations score only an average endorsement from their ITRM functions when it comes to the provision of concise and actionable risk intelligence and recommendations to IT. Sixty-seven percent say this is neither effective nor ineffective; none describe it as a highly effective area in their business.

► **Apply remediation action following an incident/problem root cause assessment** – Fifty-eight percent consider the application of remediation action following an incident, and RCA, to be effective in their organization.

► **Alignment between IT and corporate risk management** – The alignment between IT and corporate risk management is strengthening, with 60% ranking it four out of five or above for effectiveness in their organization.

  In our last survey just 28% rated the alignment between IT and corporate risk management in the top two categories.

► **Use of technology to manage risk** – The effectiveness of technology use to manage risk is broadly positive, though a quarter of our respondents are less than satisfied with its application, with 66% considering it to be neither effective nor ineffective, or ineffective.

► **Optimization of controls** – Most respondents rate the effectiveness of optimization of controls as mediocre, with no one going so far as to say that it is highly effective in their organization.
Our view

► Providing IT with concise and actionable risk intelligence and recommendations - There is clear room for improvement in the provision to IT of concise and actionable risk intelligence and recommendations.

► Apply remediation action following an incident/problem RCA - Remediation action following an incident, and RCA of problems, is carried out effectively in most organizations.

► Alignment between IT and corporate risk management - Alignment seems to have improved considerably since our 2013 survey and is considered to be very strong among the ITRM functions at financial institutions.

► Use of technology to manage risk - Technology use needs to be more effective, as many are still skeptical about its usefulness.

► Optimization of controls - Only one in three organizations deem the optimization of controls to be effective.

---

16 Does your company have a formal IT risk framework and assessment process in place?

Summary points

► 79% of respondents say that their company has a formal IT risk framework and assessment process in place. This is up slightly from the 72% that responded positively in our 2013 survey.

Our view

► Most organizations have an effective framework. The next stage in enhancement is to improve the framework utilization through monitoring and reporting.
17 Do you have a common risk and control framework used across the company?

Summary points
► 81% of respondents say their organization now has a common risk and control framework in place that is used across the company.

Our view
► Communication and alignment of functions within businesses is often now in place but could be improved to build consistency into the IT risk framework.
► One of the core essential aspects of an effective ITRM framework and program is the effective use of risk and control framework or normalized framework that meets the organizations IT risk needs and requirements.

18 What best describes your establishment of a common process, risk and control library?

Summary points
► 43% described their companies as having a well-defined common process, risk and control library and hierarchy in place.
► In a third of businesses these are more loosely defined processes and hierarchies, but 20% say no common process exists.
► These figures show an improvement from our 2013 survey, when 30% talked of no common process.

Our view
► Common processes, risk and control hierarchies are increasingly being established by mature functions. Often, however, risks are still only being addressed at lower levels and not at a process level. This can lead to undervalued efforts and increased costs if process efficiencies are not achieved.
► Considerable effort is required to ensure the common control library is part of an ITRM program, and that it is used and kept up to date.
► Emerging technologies will be a clear driver to update existing common control libraries. The ITRM function would need to considerable effort to review and enhance the common control library.
19 Which standards or practices have you used for your IT risk program framework?

Summary points
► 70% of respondents have leveraged or aligned ISO standards to their IT risk program, compared to 50% who aligned to ISO standards in 2013.
► 22% have leveraged leading practices relating to NIST-SP 800s and NIST Cyber Security Framework.

Our view
► There is a growing trend toward the adoption of frameworks for ITRM.

Other includes
► COBIT 5
► COSO
► ITILv3
► ISO 31000
► OCTAVE
► PCOI
► PRC

20 Which types of assessments do you perform?

Summary points
► 81% of respondents perform risk and control self-assessments, while 70% also perform third-party assessments.
► Other popular assessments include IT process, application, information/data and compliance targeted assessments.

Our view
► There is a heightened regulatory focus on resiliency in infrastructure management. We would expect this to be reflected in the assessments being performed; however, this was not the case.
Who performs your company’s IT risk assessments?

Summary points
► In most companies, IT risk assessments are carried out by IT risk or information security.
► Management carries out IT risk assessments in 17% of cases, and 21% say that they are carried out by third parties.
► The role of Internal Audit in completing IT risk assessments has diminished considerably since our last survey. In 2013, 55% said IT risk assessments were carried out by Internal Audit, and it was the most popular answer with respondents. Today, the figure is reduced to 35%.
► In 2013, 38% of organizations had IT risk assessments completed by their Information Security teams. In 2014, this number increased to 68%.

Our view
► IT risk functions have started to complete risk assessments in a more prominent fashion than reported in our last survey. This is a clear articulation of the roles defined by the three lines of defense and will further strengthen the quality of IT risk assessments being completed.

<table>
<thead>
<tr>
<th>Category</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Audit</td>
<td>55%</td>
<td>35%</td>
</tr>
<tr>
<td>IT risk</td>
<td>52%</td>
<td>71%</td>
</tr>
<tr>
<td>Information Security</td>
<td>38%</td>
<td>68%</td>
</tr>
<tr>
<td>Operational risk and compliance function</td>
<td>35%</td>
<td>46%</td>
</tr>
<tr>
<td>Management</td>
<td>31%</td>
<td>17%</td>
</tr>
<tr>
<td>Third party</td>
<td>25%</td>
<td>21%</td>
</tr>
<tr>
<td>IT (first line of defense)</td>
<td>-</td>
<td>46%</td>
</tr>
<tr>
<td>Other, please specify</td>
<td>2%</td>
<td>3%</td>
</tr>
</tbody>
</table>
What drives the timing of your risk assessments?

Summary points
► 51% of our respondents tell us they have defined assessments schedules, with 38% conducting them on an annual basis and 13% on a bi-annual basis.
► In 2013, 18% told us they conducted assessments annually, and 6% did so every six months.
► A quarter of respondents carry out their risk assessments on an ad-hoc basis according to the current priorities or focus areas.

Our view
► There is now a growing trend in IT risk assessments being completed on a planned and scheduled basis.

Is there a clearly defined IT risk appetite that has been successfully implemented?

Summary points
► Only 16% of our respondents report that their organization has a clearly defined IT risk appetite statement that is fully implemented, while 44% do not.
► A third of the organizations covered by our survey are currently developing IT risk Appetite Statements and implementing them.

Our view
► There is a clear move within the financial services industry to implement clearly defined IT risk Appetite Statements, driven by regulatory pressures. A third of our respondents are in the process of developing and implementing these statements.
24 How does your company report on its IT risk?

Summary points
► 62% of the respondents to our survey tell us that their company reports on IT risks by aggregating into a risk management dashboard for the entity. This is up from 52% in our 2013 survey.
► 56% of respondents report at the enterprise level and 54% report by business line.
► Reporting at enterprise level was the most popular means of reporting in 2013, at 65%, and reporting by business line stood at 48%.

Our view
► Investment should be made to improve the risk management reporting dashboard and its integration with ERM activities, e.g., as part of risk convergence projects.
► There is a strong trend toward integrated reporting, with company and asset level reporting still lagging due to complexities and significance.
► Business reporting of IT risk is essential if business and funding are to be in alignment with expectations.

25 Have you defined IT risk performance metrics that are monitored and reported?

Summary points
► 35% of respondents have defined IT risk performance metrics that are monitored and reported to management on a regular basis, while a further 32% are in the process of specifying IT risk performance metrics.
► 6% tell us that metrics are specified but not reported to senior management, and 14% do not have defined metrics in place.

Our view
► The monitoring and reporting of IT risk performance metrics has made significant improvements, but as a result of complexities and resource availability factors, metrics generally take 12 to 24 months to mature and get to an effective state.
► Additional factors may be complexities in metrics while also trying to enable technology over program - two very complex and challenging strategic initiatives being executed at the same time is proving to be impossible to gain success on both fronts for many organizations.
Summary points
► Many companies now have defined KRI and KPIs for security management, IT resilience including IT contingency, and problem and incident management.
► Only 25% of companies have indicators for data governance and data management, 32% for regulatory compliance management and 37% for vendor management.

Our view
► KRI appears to be covering all the key topics by specific client risk needs. We may have expected data, resource management, vendor and regulatory/compliance areas for greater focus.

For which of the following IT activities has your company defined KRI or KPIs?

Summary points
► Although, 72% report that senior management in their business takes appropriate actions to address IT risk indicators that have been reported to them, we have seen a downward trend in this area. In 2008, 93% agreed that management took the right steps. In 2013, 78% backed management and only 5% felt they were not doing the right thing.

Our view
► Risk remediation from KRI shows strong support from senior management, though this does appear to be diminishing over time.
► We feel that this is because KRI are not always seen as relevant by management, because ITRM functions are not always providing the right data.
Summary points
► 52% of those surveyed say that their business has technology enabled the IT risk program, with 27% saying that has occurred through the use of GRC tools.

Our view
► More than half of the organizations have in place a GRC tool or other tools and technology, and 29% are in progress. This shows a strong improvement toward a holistic enterprise wide view.
► These types of initiatives often take longer than expected so the survey results are positive. We note that a focus on strong business functional requirements and a rigorous system development life cycle is essential for success of programs being enabled through technology.

Does your IT risk program have GRC tools or other tools and technology?
Section 2
Organizational information
### Summary of the participating companies

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>83%</strong></td>
<td>have less than 50,000 employees</td>
</tr>
<tr>
<td><strong>82%</strong></td>
<td>generate more than $1b annual revenue</td>
</tr>
<tr>
<td><strong>35%</strong></td>
<td>are global multinational companies</td>
</tr>
<tr>
<td><strong>37%</strong></td>
<td>are local companies (operate in one country)</td>
</tr>
<tr>
<td><strong>50%</strong></td>
<td>are operating in the financial services - banking sector</td>
</tr>
<tr>
<td><strong>31%</strong></td>
<td>are operating across the entire financial services sector</td>
</tr>
</tbody>
</table>
Financial figures:

<table>
<thead>
<tr>
<th>Financial Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>more than $250b</td>
<td>11%</td>
</tr>
<tr>
<td>$25b to $250b</td>
<td>28%</td>
</tr>
<tr>
<td>$10b to $24b</td>
<td>16%</td>
</tr>
<tr>
<td>$1b to $9b</td>
<td>26%</td>
</tr>
<tr>
<td>$500m to $999m</td>
<td>9%</td>
</tr>
<tr>
<td>$250m to $499m</td>
<td>8%</td>
</tr>
<tr>
<td>$100m to $249m</td>
<td>2%</td>
</tr>
</tbody>
</table>

Total number of employees:

<table>
<thead>
<tr>
<th>Employee Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 1,000</td>
<td>8%</td>
</tr>
<tr>
<td>1,000 to 9,999</td>
<td>48%</td>
</tr>
<tr>
<td>10,000 to 49,999</td>
<td>27%</td>
</tr>
<tr>
<td>50,000 to 99,999</td>
<td>14%</td>
</tr>
<tr>
<td>More than 100,000</td>
<td>3%</td>
</tr>
</tbody>
</table>
Industry

**Industry**

- Financial services - banking: 50%
- Financial services - all (ie asset management, banking & insurance): 31%
- Financial services - insurance: 8%
- Financial services - asset management: 8%
- Financial services - Other (trading, superannuation): 3%

**Entity operating areas**

- Americas: 63%
- EMEIA: 64%
- Japan: 20%
- Far East: 20%
- Asia-Pacific: 38%
- Oceania: 23%
Responses by location

- Americas: 23
- EMEIA: 27
- Asia-Pacific and Japan: 14

Responsibilities of respondents
Appendices
IT risk environment

Aligning ITRM to the business environment
Developing an ITRM framework

Corporate Risk Charter, Risk Governance structure, Strategy and Roadmap, risk tolerance guidance, expectations for risk management and integration of capabilities into operational competencies

Framework incorporating an IT process, risk and control framework (library) with associations to regulatory, leading practices and internal requirements

Business objectives, regulatory requirements and board directives that drive program requirements

IT risk dashboard: ongoing monitoring and reporting on program effectiveness and risk posture

Organization structure, roles and responsibilities, training and awareness and personnel to support and execute the ITRM program

Risk identification, risk domains, risk profiles, risk and controls library and ratings criteria that define IT risk for the organization

IT policies and standards that assist in achieving IT risk objectives and effective management of IT risk

Information and technology risk governance and strategy

Process, risk and control framework

Risk assessments

Risk processes and operational procedures

Tools and technology

Compliance monitoring and reporting

Managing risk, driving value, controlling costs, achieving compliance

Alignment with IT strategy for business and IT objectives and critical success factors

Design methodologies and procedures to enable a sustainable assessment of IT risk in support of ITRM goals

Processes, procedures and methods for executing the IT risk program (e.g., risk control self assessment, issues management)

Tools to facilitate IT risk program processes and reporting

Managing risk, driving value, controlling costs, achieving compliance
Key IT risk trends and challenges

EY has observed the following key IT risk trends and challenges the financial industry is currently experiencing:

<table>
<thead>
<tr>
<th>Emerging consumerization</th>
<th>Enhanced persistence of cyber crime</th>
<th>Increased exposure to internal threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>► Increased vulnerabilities due to anytime, anywhere accessibility</td>
<td>► Spread of malicious code causing outages</td>
<td>► Heightened exposure to fraud via toxic access combinations</td>
</tr>
<tr>
<td>► Risk of unintended sharing and disclosure of confidential data</td>
<td>► Data loss increase</td>
<td>► Data loss or theft increase through inappropriate access rights and monitoring controls</td>
</tr>
<tr>
<td>► Lack of knowledge of new technologies and appropriate management of risks</td>
<td>► Reputational loss due to poor publicity</td>
<td>► Key IT people with access to client identifying data</td>
</tr>
<tr>
<td>► Value leakage through poor application of new technologies</td>
<td>► Financial loss due to unauthorized transfers</td>
<td>► Lack of regulatory compliance and ability to respond</td>
</tr>
<tr>
<td>► Reputational damage through poor management of new channels (e.g., social media)</td>
<td>► Lack of regulatory compliance and ability to respond</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rise of cloud computing</th>
<th>Growing importance of resiliency</th>
<th>Continued challenge for skilled staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>► Lack of governance over IT Infrastructure applications and databases</td>
<td>► Failure of business continuity and disaster recovery plans causing financial and reputational loss</td>
<td>► Lack of appropriate knowledge transfer during off-shoring/outsourcing or redundancy processes</td>
</tr>
<tr>
<td>► Privacy and security risk exposure especially through cross-border data transfer</td>
<td>► Single points of failure unidentified in critical infrastructure</td>
<td>► Lack of appropriate business knowledge leading to poor quality IT solutions</td>
</tr>
<tr>
<td>► Increased likelihood of regulatory non-compliance (SOX, PCI-DSS, etc.)</td>
<td>► Poor incident management causing increased reputational and financial loss during an incident</td>
<td>► Inability to recruit key IT staff leading to a mismatch in IT skills</td>
</tr>
<tr>
<td>► Reduction in IT agility via platform or vendor lock-in</td>
<td>► Business change exceeding technology change</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accelerating change agenda</th>
<th>Increased use of outsource providers</th>
<th>Increased focus on true golden source data</th>
</tr>
</thead>
<tbody>
<tr>
<td>► Failure to deliver IT projects and programs within budget, timing, quality and scope causing value leakage</td>
<td>► Lack of supplier risk management leading to exposures (financial, reputational, regulatory, etc.)</td>
<td>► Inappropriate usage of data by business leading to operational risk exposure</td>
</tr>
<tr>
<td>► Increased complexity and volume of change leading to inappropriate control</td>
<td>► Lack of awareness of fourth parties and fourth-party risk</td>
<td>► Inappropriate data classification leading to poor data disclosure control</td>
</tr>
<tr>
<td>► Adoption of methodologies without due consideration of appropriate/minimal control requirements</td>
<td>► Poor management of regulatory risk in particular around data privacy and cross-border controls</td>
<td>► Inability to dispose of data securely due to multiple versions of the truth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Increased likelihood of data corruption</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Moves to acquire, divest or segregate businesses and IT</th>
<th>Increasing regulation</th>
<th>Increased reliance on future proof technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>► Inability to separate or segregate key systems and technologies</td>
<td>► Increased assurance through enhancement of three lines of defense</td>
<td>► Systems selection and integration agenda is increasingly complex</td>
</tr>
<tr>
<td>► Lack of ability to integrate and align core systems</td>
<td>► A heightened need to provide informative management information over IT</td>
<td>► Ability to maintain pace of technology change challenging</td>
</tr>
<tr>
<td>► Complex support environments with loss of legacy knowledge creating poorly supported IT environments</td>
<td>► Cross-border complexities in particular around data privacy and security leading to non-compliance</td>
<td>► Risk awareness of new technologies can be limited</td>
</tr>
<tr>
<td></td>
<td>► Increasing focus on cloud, mobile devices, outsourcing and new technologies adding to complexity and volume of regulation and regulators</td>
<td>► Staff training and awareness is often poor leading to poor selection or inappropriate requirements</td>
</tr>
</tbody>
</table>
EY's related insights and resources

Expecting more from risk management: drive business results through harnessing uncertainty

Accelerating high-growth companies’ climb to the top: strong risk management practices and Internal Audit capabilities as drivers for growth

Maximizing value from your lines of defense: a pragmatic approach to establishing and optimizing your LOD model

Maximizing the value of a data protection program


Bring your own device: Security and risk considerations for your mobile device program

Privacy trends 2014: Privacy protection in the age of technology

A New View on IT risk

Tim Purcell
# Contacts

## EMEIA

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Phone Number</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pat Moran</td>
<td>EMEIA FSO ITRM Leader</td>
<td>+353 1 221 2769</td>
<td><a href="mailto:pat.moran@ie.ey.com">pat.moran@ie.ey.com</a></td>
</tr>
<tr>
<td>James Turpie</td>
<td>EMEIA FSO</td>
<td>+44 131 777 2040</td>
<td><a href="mailto:jturpie@uk.ey.com">jturpie@uk.ey.com</a></td>
</tr>
</tbody>
</table>

## Americas

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Phone Number</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tim Purtell</td>
<td>Americas FSO ITRM Leader</td>
<td>+1 212 773 1232</td>
<td><a href="mailto:tim.purtell@ey.com">tim.purtell@ey.com</a></td>
</tr>
<tr>
<td>George Haggar</td>
<td>Americas FSO</td>
<td>+1 212 773 4425</td>
<td><a href="mailto:george.haggar@ey.com">george.haggar@ey.com</a></td>
</tr>
</tbody>
</table>

## Asia Pacific

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Phone Number</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faith Page</td>
<td>Asia-Pacific FSO ITRM Leader</td>
<td>+61 3 9288 8012</td>
<td><a href="mailto:faith.page@au.ey.com">faith.page@au.ey.com</a></td>
</tr>
<tr>
<td>Nitin Singh</td>
<td>Asia-Pacific FSO</td>
<td>+61 3 9655 2541</td>
<td><a href="mailto:nitin.singh@au.ey.com">nitin.singh@au.ey.com</a></td>
</tr>
</tbody>
</table>
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.

Ernst & Young LLP
The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.

Ernst & Young LLP, 1 More London Place, London, SE1 2AF.

© 2014 Ernst & Young LLP. Published in the UK.

All Rights Reserved.

ED 0115
EYG No. C00160

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

Information in this publication is intended to provide only a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice. Ernst & Young LLP accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.

ey.com/uk