### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Methodology</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Executive summary</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Key findings</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Key success factors</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Conclusion</td>
<td>6</td>
</tr>
<tr>
<td>Section 1</td>
<td>ITRM Survey - results</td>
<td>7</td>
</tr>
<tr>
<td>Section 2</td>
<td>Organizational information</td>
<td>29</td>
</tr>
</tbody>
</table>

**Appendices**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ernst &amp; Young contacts</td>
<td>35</td>
</tr>
</tbody>
</table>
Welcome to Ernst & Young’s IT Risk Management Survey

The purpose of the IT Risk Management (ITRM) Survey is to understand the maturity of ITRM in organizations, gain insights of developments made in implementing and enhancing ITRM, and be able to see changes and trends by comparing the results with the Ernst & Young ITRM Survey conducted in 2008.

This year’s survey provides us with insight of where companies invest in ITRM, the alignment of ITRM with operational risk management (ORM), and insight on how ITRM is sponsored and governed by companies.

Methodology

Reports are used to provide competitive advantage

This survey was conducted by Ernst & Young. During November 2012 to January 2013, we performed the online survey on the topic of ITRM for Europe, Middle East, India and Africa (EMEIA)-based companies.

We polled 71 senior executives whose functions intersect risk management and IT. Of those, 47% are located in Switzerland, 18% in United Kingdom, 15% in Spain, 13% in Belgium and 7% in Germany.

Eighty-two percent hold C-level or officer titles, 16% are information technology executives or Information Security Executives, and 2% are Internal Audit Directors.

Eighteen percent of organizations have assets of between US$25 billion to US$250 billion, 43% of organizations have assets between US$1 billion and US$25 billion, and 23% between US$100 million and US$1 billion. Ten percent of all respondents’ firms have assets of less than US$100 million, and 6% of the firms are non-profit organizations.
Executive summary

Purpose of the survey
This survey provides insight into ITRM sponsorship and governance. It helps us (i) understand the maturity of and investment in ITRM, (ii) identify developments made in implementing and enhancing ITRM, and (iii) track changes and trends by comparing the results with the inaugural Ernst & Young ITRM Survey conducted in 2008.

Focus of the survey
The results of this survey represent findings from 70+ senior information technology and risk executives, from 62 diversified institutions in 5 countries within EMEIA. Following the 2008 inaugural survey, the questions we asked these senior executives were designed to focus their attention on the framework, processes and drivers of ITRM, in particular, their impact on decision-making and the role IT Risk Management plays in an organization’s overall risk management processes and posture.

Developing the ITRM framework
Over half of the organizations surveyed plan to increase spending in ITRM activities in the next 12 months, with investment being made in ITRM framework development and related processes to enhance risk management effectiveness. This approach will be vital in building an effective ITRM program that better aligns ITRM functions with ORM and builds consistency and standardization into the overall process-risk-control framework.

Formalizing and integrating ITRM within the enterprise risk management program
We have learnt from our latest survey that, while a predominant number of surveyed organizations have established ITRM functions, many continue to focus on the need to formalize and better integrate ITRM within their overall risk management program. The survey results indicate that, while some organizations are developing and aligning their frameworks with various standards and leading practices, such as ISO 27002:2005 and Information Systems Audit and Controls Association’s (ISACA) Risk IT Framework, only a third have a well-defined library of common controls. Establishing this critical component of the ITRM framework will help information technology functions to more effectively and efficiently manage risk, make better risk-aligned investment decisions and satisfy regulators, auditors (internal and external), and governance, risk and compliance function requirements and needs.

Reporting dashboards
As external and internal risk management requirements become increasingly complex, the demand for more comprehensive and actionable information continues to increase within many organizations. This is borne out in the survey, with reporting on IT risk assessments at the enterprise level being the number one reporting priority. In many cases, we expect organizations to channel investments toward the improvement of the risk management reporting dashboards and their integration with enterprise risk management activities, to help fully align ITRM with enterprise risk management strategies and frameworks.

Coping with challenges: regulatory compliance, emerging technologies and reporting
We continue to see the complexity and types of risk facing organizations expanding significantly. Cost-reduction activities, increased regulation, emerging technologies and deliberate acts of cybercrime all increase the exposure to risk and heighten the need to impose a new risk management regime.

Regulatory Compliance
Regulatory compliance is a key factor driving investment to enhance risk reporting and monitoring. From Basel III to Solvency II and Sarbanes-Oxley (SOX), IT Risk functions are required to guide and manage organizations through an increasingly complex regulatory landscape, driving an increased desire for compliance and simplification.
Emerging technologies

Many organizations are challenged with identifying and managing the risks associated with emerging technologies. We recently reported in our 15th annual Global Information Security Survey that organizations fighting to narrow the gap that mobile computing, social media, cloud, and cyber threats create need to fundamentally transform their approach to information security. The same is true for ITRM. As emerging technologies continue to put pressure on IT Risk functions, there needs to be a greater focus on proactively identifying, monitoring and managing these threats.

The way forward ...

Organizations are increasing their focus on standardizing the effectiveness of the three lines of defense, to ensure there is adequate oversight and control in place to manage IT risks. Issues with resilience and IT risk failures have significantly increased the impact on reputational risk. We would expect to see a more structured approach to risk appetite being used to reassess the IT risk landscape continually.

In addition to concentrating investment and effort around the alignment of the control library to the risk framework, we expect governance risk and compliance (GRC) tool implementation to be a main priority in the future. GRC technology is a key vehicle for creating value, reducing cost, integrating reporting and managing risk across the enterprise. It enables organizations to automate, standardize and streamline processes, create holistic views of risk and compliance, and analyse real-time business intelligence – allowing risk-related decision-making to really make a difference.

I would like to thank all 71 organizations who participated in the survey.

I hope that you will find this survey both informative and beneficial to your organization. We would be delighted to discuss the observations further with you and provide you with assistance on this very topical and fast-moving journey.

Pat Moran
IT Risk Management Leader, FSO EMEIA
Emerging themes

- Organizations are active in applying ITRM, but it is not yet fully effective.
- More than 50% of organizations are increasing their investment in IT risk.
- The trend to expect more results with fewer resources highlights the need to work smarter and to benefit from the implementation of frameworks and GRC solutions.
- The threat from IT risks are better understood, which is increasing the overall awareness of IT risk.

Alignment and Integration with the business

- Recognized benefits in making better use of a common control library throughout the business.
- Many organizations could benefit from better integration of their ITRM programs, with their overall enterprise risk management (ERM) programs aligning business objectives and goals.
- There is an understanding and adoption of the language used in ITRM, which demonstrates the increased maturity of ITRM in many companies.

Key findings

- Organizations are active in applying ITRM, but it is not yet fully effective.
- More than 50% of organizations are increasing their investment in IT risk.
- The trend to expect more results with fewer resources highlights the need to work smarter and to benefit from the implementation of frameworks and GRC solutions.
- The threat from IT risks are better understood, which is increasing the overall awareness of IT risk.

Compliance

- 54% increase in investment in ITRM programs (tools to improve monitoring and reporting) driven by compliance needs.

Reporting

- 32% moderate and 15% significant investments are made in risk reporting, illustrating benefits and demand for good risk reporting.
- Lack of formal IT risk performance metrics in most companies potentially inhibits monitoring and reporting, and highlights a common need to measure IT risk.

IT Risk and Control Framework

- A well-defined common control library exists
- A loosely defined common control library exists
- No common control library exists, but various control libraries are available
- We have neither a common control library nor other control libraries

IT Risk Management Survey
Emerging technologies
► The expectation is that emerging technologies will continue to have a significant impact on the development of ITRM functions.

What impact has emerging technology (e.g., cloud computing, virtualization and mobile computing) had on your company's ITRM program over the past 12 months?

Our analysis shows that having a control library does not mean that a common risk framework is available. Also, companies that claim to have a common risk framework do not as a matter of course have formal risk assessment process in place.
► 66% stated that a common control library exists.
► 82% that a common risk framework exists.
► 72% say they have a formal IT risk framework and assessment process.

66% stated that a common control library exists.
82% that a common risk framework exists.
72% say they have a formal IT risk framework and assessment process.

Key success factors
Key success factors for an effective and efficient ITRM:
► Focus on your corporate strategy when assessing your IT Risk landscape
► Consider new IT risk scenarios driven by emerging technologies
► Consider regulatory requirements as a main driver for ITRM
► Think global - consider risk convergence, the integration of ITRM to ORM and alignment with ERM
► Define and monitor key risk indicators (KRI's) and consider your IT-sourcing strategy when doing so.
► Focus on efficient reporting

Questions for the C-level Executives
IT is a clear business enabler, but it also increases the risk to an organization. Be mindful of how new business models and new business strategies are leading to new IT risk scenarios.
► Do you adapt ITRM processes to align with business strategies and new business changes?
► Do you actively monitor regulatory changes for the impact of ITRM?
► Do you have enough focus on ITRM documentation to help formalize processes to increase communications and integration with ORM?
► Do you standardize ITRM processes and clearly defined roles and responsibilities to improve efficiency, quality and reporting?
► Do you have a good understanding of emerging technologies and business trends that are vital for the management of IT risks in a fast-changing environment?
Section 1
ITRM Survey - results
Does your company have a formal ITRM function?

Summary
► 76% of survey participants have a formal ITRM function. We also found out that having an ITRM function does not correlate to the size of a company.
► Compared with the inaugural pre-financial crisis survey conducted in 2008, we do not see a big change in this area. In 2008, 78% had a formal ITRM function.

Conclusion
► Many of the organizations surveyed do have an ITRM function, which could be a result of the heightened awareness of emerging threats that have an IT impact. For example, there is a greater awareness at board level of cyber attacks and the resilience of core services. Furthermore, with increasing global economic challenges, there is a greater regulatory focus and, in some cases, an increased insider threat as a result of cost-reduction activities.
► Despite growth in regulatory requirements and associated need for risk management in general, no increase or enlargement of the ITRM function can be detected over the last four years. Companies should question the existing ITRM function, not just in terms of size, but also in terms of effectiveness.
► 50% of companies who do not have an ITRM function do not follow an ITRM standard.
By what percentage do you estimate your company's financial investment in ITRM activities will change in the next 12 months?

<table>
<thead>
<tr>
<th>Percentage Change</th>
<th>Investment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase by less than 5%</td>
<td>31%</td>
</tr>
<tr>
<td>Increase by 5% to 25%</td>
<td>20%</td>
</tr>
<tr>
<td>Increase by more than 25%</td>
<td>3%</td>
</tr>
<tr>
<td>Decrease by less than 5%</td>
<td>(7%)</td>
</tr>
<tr>
<td>Decrease by 5% to 25%</td>
<td>(6%)</td>
</tr>
<tr>
<td>Decrease by more than 25%</td>
<td>(1%)</td>
</tr>
<tr>
<td>Don't know</td>
<td>(7%)</td>
</tr>
</tbody>
</table>

Summary

- 54% of organizations surveyed plan to increase spending in ITRM activities over the next 12 months, but the majority will not increase their financial investment in ITRM by more than 5%.
- There is a positive trend toward moderate increases in ITRM investment. Most investment will be in banks and insurance companies, and some technology firms.
- Only 14% of organizations plan to decrease their spending in ITRM activities.
- Analysis of the results indicates that investment for ITRM is independent of the size and scale of the company.

Conclusion

- IT risk functions can benefit from greater formalization of methods and supporting processes.
- Having no formal ITRM function does not result in higher levels of planned investments.
- Spending does not depend on the industry, rather on the maturity of the ITRM framework and function.
### How will your company’s investment in ITRM be distributed across the following initiatives in the next 12 months?

<table>
<thead>
<tr>
<th>Initiative</th>
<th>No investment</th>
<th>Low investment</th>
<th>Moderate investment</th>
<th>Significant investment</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>New technologies (e.g., investment in GRC tools)</td>
<td>31%</td>
<td>38%</td>
<td>15%</td>
<td>8%</td>
<td>8%</td>
</tr>
<tr>
<td>Risk reporting and monitoring (e.g., risk dashboard and regulatory monitoring)</td>
<td>11%</td>
<td>38%</td>
<td>32%</td>
<td>15%</td>
<td>4%</td>
</tr>
<tr>
<td>IT control self-assessment</td>
<td>14%</td>
<td>37%</td>
<td>34%</td>
<td>8%</td>
<td>7%</td>
</tr>
<tr>
<td>ITRM Framework development (e.g., process formalization and maturity...)</td>
<td>14%</td>
<td>23%</td>
<td>46%</td>
<td>8%</td>
<td>9%</td>
</tr>
<tr>
<td>Alignment with ERM</td>
<td>20%</td>
<td>39%</td>
<td>27%</td>
<td>4%</td>
<td>10%</td>
</tr>
<tr>
<td>Training and education</td>
<td>13%</td>
<td>38%</td>
<td>31%</td>
<td>11%</td>
<td>7%</td>
</tr>
<tr>
<td>Staffing</td>
<td>27%</td>
<td>38%</td>
<td>18%</td>
<td>8%</td>
<td>9%</td>
</tr>
</tbody>
</table>

**Summary**

- Over 50% of those surveyed want to invest more in ITRM.
- 54% of those surveyed will invest in IT risk framework development.
- 54% will be investing in the implementation of frameworks to enhance risk management effectiveness. 42% will be investing in increasing awareness of their IT control self-assessments.
- 15% of significant investment is driven by the need to enhance risk reporting and monitoring, which is likely to be driven by regulation (Basel III to Solvency II and SOX, etc.)
- 66% of those surveyed indicate there will be no investment or low investment in staffing. However, supporting methods show 11% are pushing significant investment in training and education – increasing efficiency of staff resources.

**Conclusion**

- Compliance with regulation seems to be a driver for investment in ITRM programs, with a focus on reporting and monitoring tools. Compliance and regulatory reporting activities may not yet be optimized, which could lead to additional cost.
- It seems that ITRM functions are established and, therefore, practically no further investment in the next 12 months is planned for more ITRM staff. Almost 50% report moderate to significant investment for IT control self-assessment.
- Three out of four participants will not invest or invest very little in GRC tools over the next 12 months. This could reflect a decision to adopt a phased approach: to first implement an ITRM Framework and then decide on the GRC solution.
- IT risk functions can benefit from greater formalization of methods and supporting processes.
- Staff resourcing is a challenge, and it is difficult to realize benefits from ITRM experts. Therefore, companies are focusing on training and education and improving the quality of staff resources already in place.
- There is a tendency to expect more with less resources, which highlights the need for risk officers to work smarter, be more streamlined and extract benefit from frameworks and GRC solutions.
Manage and monitor

Which of the following risks does your organization manage or monitor within the scope of the ITRM function?

- Offshoring
- Fraud, theft or loss of assets (e.g., mobile phone or intellectual property)
- Program and project risks
- Information technology compliance activities
- Data center operations
- Outsourcing and vendor risks
- Privacy and data protection
- Data quality
- IT continuity and disaster recovery
- IT infrastructure availability
- IT security (e.g., system patch level, system vulnerabilities and viruses)
- Information security (e.g., identity and access management)
- Data leakage

No or limited monitoring
Moderate monitoring priority
Well monitored

Summary
- According to the survey results, it can be seen that IT security, information security and data leakage are the most commonly monitored risks (priority 1 or 2).
- Fraud, theft or loss of assets such as mobile phones, as well as offshoring risks (average priority 5 out of 5) and program and project risks (average priority 4 out of 5) are lower priority when it comes to monitoring.

Conclusion
- It is clear that IT security, information security and data leakage related risks are the most highly monitored risks. Surprisingly, however, fraud, theft or loss of assets (e.g., mobile phone or intellectual property), which often contain sensitive information, are not monitored, despite the fact that monitoring tools and technology for remote data wiping exist.
- It is interesting to see that monitoring of Business Continuity Management (BCM) aspects, e.g., IT continuity and disaster recovery, along with IT infrastructure availability, is only moderately monitored, even in those countries where banks must be BCM compliant.
Please indicate the extent of your agreement with the following statement: “IT and project managers participate in and receive sufficient regular and robust information on risk from the company’s ITRM teams.”

Summary
- IT and project managers receive regular and robust information from the ITRM team (almost 60%), showing good involvement of IT and project managers.
- Most participants agreed (51%) or even strongly agreed (6%) with the following: “IT and project managers participate in and receive sufficient regular and robust information on risk from the company’s ITRM teams.”

Conclusion
- IT risk has a role to play in projects and programs (57%), but there is an opportunity to benefit from further improvement of such involvement.
- Investment in training in and development of associated frameworks can increase project-related communication and quality of ITRM Information within the business.
Impact on the ITRM program

What impact has each of the following had on your ITRM program over the past 12 months?

<table>
<thead>
<tr>
<th>Impact on the ITRM program</th>
<th>Significant impact</th>
<th>Modest impact</th>
<th>Low impact</th>
<th>No impact</th>
<th>Don't know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of emerging technology (e.g., cloud computing, virtualization and mobile computing)</td>
<td>32%</td>
<td>21%</td>
<td>26%</td>
<td>17%</td>
<td>4%</td>
</tr>
<tr>
<td>Other IT security programs (Identity and Access Management (IAM), data leakage, etc.)</td>
<td>26%</td>
<td>33%</td>
<td>30%</td>
<td>6%</td>
<td>5%</td>
</tr>
<tr>
<td>IT infrastructure availability - DRP</td>
<td>20%</td>
<td>38%</td>
<td>23%</td>
<td>14%</td>
<td>5%</td>
</tr>
<tr>
<td>IT risk analysis and management activities</td>
<td>18%</td>
<td>35%</td>
<td>32%</td>
<td>12%</td>
<td>3%</td>
</tr>
<tr>
<td>Business resilience - BCP</td>
<td>17%</td>
<td>29%</td>
<td>38%</td>
<td>12%</td>
<td>4%</td>
</tr>
<tr>
<td>Greater awareness of ITRM</td>
<td>15%</td>
<td>26%</td>
<td>35%</td>
<td>18%</td>
<td>6%</td>
</tr>
<tr>
<td>Operation between multiple regulatory regimes (cross-border activities)</td>
<td>14%</td>
<td>18%</td>
<td>24%</td>
<td>39%</td>
<td>5%</td>
</tr>
<tr>
<td>Compliance activities</td>
<td>14%</td>
<td>45%</td>
<td>26%</td>
<td>11%</td>
<td>4%</td>
</tr>
<tr>
<td>Technology changes due to merger and acquisition activities</td>
<td>14%</td>
<td>18%</td>
<td>18%</td>
<td>47%</td>
<td>3%</td>
</tr>
<tr>
<td>Use of and extend of reliance upon third parties</td>
<td>12%</td>
<td>26%</td>
<td>27%</td>
<td>29%</td>
<td>6%</td>
</tr>
<tr>
<td>Increased requirements for measuring and monitoring information technology risk</td>
<td>12%</td>
<td>33%</td>
<td>33%</td>
<td>17%</td>
<td>5%</td>
</tr>
<tr>
<td>IT risk analysis and management reporting</td>
<td>12%</td>
<td>35%</td>
<td>35%</td>
<td>15%</td>
<td>3%</td>
</tr>
<tr>
<td>Publicity surrounding security breaches and loss of data</td>
<td>12%</td>
<td>27%</td>
<td>36%</td>
<td>18%</td>
<td>7%</td>
</tr>
<tr>
<td>ERM integration and risk conversion</td>
<td>11%</td>
<td>18%</td>
<td>26%</td>
<td>35%</td>
<td>10%</td>
</tr>
<tr>
<td>Social media activities</td>
<td>9%</td>
<td>18%</td>
<td>36%</td>
<td>29%</td>
<td>8%</td>
</tr>
</tbody>
</table>

Summary
► The following elements have had the most significant impact on participant ITRM programs over the past 12 months:
► Use of emerging technologies
► IT security programs, e.g., IAM or DLP
► IT infrastructure availability - DRP
► Compliance activities
► 32% of survey participants indicate that the use of emerging technologies had a significant impact on their ITRM program over the last 12 months.
► 59% of participants noted that compliance activities had a modest or significant impact on their ITRM program over the last 12 months.
► ERM integration and risk conversion and cross-border activities had almost no to very low impact.

Conclusion
► There is a heightened awareness of regulatory pressures impacting IT, which need to be understood and applied by ITRM to avoid potential exposure from regulatory breaches.
► Emerging technologies are a drive (or trend) for ITRM. This leads to continuous enhancement of risk assessments, KRI and risk monitoring requirements. Annual risk reassessments are probably insufficient in this climate, especially as the assessment of emerging technology can be time-critical and must be well integrated into any in-flight programs.
► Emerging technology, e.g., Bring your own Device (BYOD) could be an upcoming focus area. New emerging risks and threats require dynamic solutions for ITRM to meet demands for change.
Factors for challenges or success

**Summary**

- **Factors contributing to the success of ITRM initiatives:**
  - Support from executive sponsors (60%)
  - Documented ITRM strategy (54%)
  - Integrated approach to risk management (52%)

- **Factors posing a challenge to ITRM initiatives:**
  - Competing objectives – cost vs. control, performance vs. cost (43%)
  - Staff resources to support ITRM (42%)
  - Tools to monitor and report risk (37%)
  - Financial investment to support ITRM (34%)

**Conclusion**

- The key success factors did not change from 2008 to 2013. Support from executive management continues to be fundamental. It seems that executive management is now more involved in RM and ITRM. This is also reflected in the way reporting is organized: 65% say that ITRM is reported at an enterprise level on a quarterly or annual basis; 12% say that they report to the Chief Compliance Officer; 9% state that they report to the CEO. The increasing demand on reporting and the stronger involvement of executive management will most probably increase the need for GRC tool integration and result in the need for associated increases in financial investment.

- Staff resources to support ITRM is a challenge but major investments are yet to be made. Gaps will probably be filled by external IT risk consultants.

- These trends reinforce the focus on formalized ITRM strategies, reporting tools and staff skills and knowledge.
Common control library

Which of the following statements best describes your company’s establishment of a common control library (not only for IT control)?

- A well-defined common control library exists: 35%
- A loosely defined common control library exists: 31%
- No common control library exists, but various control libraries are available: 28%
- Don’t know: 5%
- We have neither a common control library nor other control libraries: 2%

To what extent is the company’s common control library utilized in implementing or re-engineering processes to align risk with control?

- Moderate usage: 58%
- Extensive usage: 23%
- Rare usage: 12%
- Don’t know: 7%

Summary
- Around 60% of survey participants report that they have a well-defined (35%), or at least an elementary (31%), common control library.
- 23% of companies extensively use their common control library to align risk with control.
- One-third has no common control library.
- In the ITRM Survey in 2008, 35% said that they had a loosely defined common control library and 28% had a well-defined common control library.

Conclusion
- In comparison to 2008, some progress regarding the common control library is evident. However, considerable effort is required to ensure the common control library is part of an ITRM program. Interestingly, 66% of participants indicate that they have a well-defined common control library, yet a third of that number do not use their common control libraries.
- Two potential causes could be implied as to why a common control library exists, but the library is only moderately or rarely used: (i) the company does not have a useful control library, or (ii) the common control library may be outdated and no longer useful.
- Emerging technologies will be a clear driver to update existing common control libraries. The ITRM function would need to consider the effort required to review and enhance the common control library.
Please indicate the extent of your agreement with the following statement: “There is a common risk language that is broadly used and understood throughout my company.”

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neither agree nor disagree</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>2%</td>
<td>9%</td>
<td>28%</td>
<td>48%</td>
<td>14%</td>
</tr>
</tbody>
</table>

Does your company have a common risk and control framework or foundation that is used today across the company?

- Yes: 82%
- No: 15%
- Don't know: 3%

Does your company have a formal information and technology risk framework and assessment process in place?

- Yes: 72%
- No: 25%
- Don't know: 3%

Summary

- 65% of survey participants indicate that a common risk language exists.
- 82% of organizations have a formal risk management framework in the enterprise, with 72% having a formal IT risk framework and IT assessment process in place. However, only 23% are fully aligned with enterprise risk.
- Interestingly, while a high percentage indicate that they have an IT risk framework aligned with the ERM and assessment process in place, according to the investment question, there is still the biggest investment planned.
- 75% report that their companies’ approach to ITRM is aligned with the enterprise operational risk management strategies and frameworks.

Conclusion

- 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.
- Trends in IT risks may impact the entire enterprise.
- Overall, a common risk language, implemented throughout the company, is not fully integrated.
- Communication and alignment of functions within businesses could be improved to build consistency into the IT risk framework.
- Cost optimization potential, related to IT risk framework optimization, exists.
IT risk assessments

Who performs your company’s information and technology risk assessments?

- Internal audit: 55%
- Information security officers: 52%
- Information technology risk officers: 38%
- Operational risk and compliance function: 35%
- Management: 31%
- Third party: 25%
- Don't know: 3%
- Other, please specify: 2%

How often are information and technology risk assessments performed?

- Continuously: 26%
- Quarterly: 22%
- Annually: 18%
- Occasionally: 14%
- Monthly: 8%
- Every six months: 6%
- Don't know: 5%
- We do not perform risk assessments: 2%

Summary

► 55% of the survey participants report that internal audit performs IT risk assessments, either in combination with or in addition to the IT risk officer (38%) or the information security officer (52%), and operational risk and compliance functions (35%).

► 56% of companies perform their IT risk assessments at least every quarter.

► Very positively, most of the participants perform IT risk assessments on a regular basis (quarterly or annually) and only 14% report that they perform IT risk assessments on occasion.

Conclusion

► It is apparent that IT risk assessments are performed frequently.

► Only 25% reporting that IT risk assessments are executed by a third party.

► The absence of a dedicated ITRM function does not mean that there is no formal ITRM function providing risk assessments.

► More than half of companies perform IT risk assessments at least every quarter and more than half of companies use internal audit to perform IT risk assessments. This highlights the growing importance of ITRM and how organizations are beginning to specialize their ITRM functions.

► Where internal audit performs IT risk assessments (55%), organizations should consider the need to address the implementation of the different lines of defense. Reliance on internal audit only may not be sufficient.
In your opinion, how effective is your company at conducting the following risk management activities?

<table>
<thead>
<tr>
<th>Activity</th>
<th>5-Highly effective</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1-Ineffective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alignment between IT and corporate risk</td>
<td>5%</td>
<td>23%</td>
<td>38%</td>
<td>26%</td>
<td>8%</td>
</tr>
<tr>
<td>management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optimization of controls</td>
<td>5%</td>
<td>15%</td>
<td>43%</td>
<td>34%</td>
<td>3%</td>
</tr>
<tr>
<td>Use of technology to manage risk</td>
<td>4%</td>
<td>18%</td>
<td>43%</td>
<td>29%</td>
<td>6%</td>
</tr>
<tr>
<td>Coordinated risk and compliance activities</td>
<td>3%</td>
<td>35%</td>
<td>40%</td>
<td>11%</td>
<td>11%</td>
</tr>
<tr>
<td>Risk reporting and disclosure</td>
<td>1%</td>
<td>31%</td>
<td>44%</td>
<td>16%</td>
<td>8%</td>
</tr>
</tbody>
</table>

Summary
► 75% of the participants state that they coordinate risk and compliance tasks. However, the coordination of risk and compliance tasks seems to be a task that is performed in a highly effective way, whereas the optimization of controls seems to be less effectively performed and presents opportunities for improvement.
► Areas for improvement of an ITRM function:
  ► Optimization of controls
  ► Use of technology to help govern risk
  ► An alignment of ITRM and corporate risk management
► 11% of companies believe they are ineffective at conducting coordinated risk and compliance activities.

Conclusion
► Companies could be more effective in defined ITRM frameworks, compliance activities and IT and business integration, highlighting the need for improvement.
► The optimization of controls will help to improve the common control library overall.
### How does your company report on its information and technology risk assessment?

<table>
<thead>
<tr>
<th>Report Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report at the enterprise level</td>
<td>65%</td>
</tr>
<tr>
<td>Aggregate into a risk management dashboard</td>
<td>52%</td>
</tr>
<tr>
<td>Report by line of business</td>
<td>48%</td>
</tr>
<tr>
<td>Report by geographic region</td>
<td>15%</td>
</tr>
<tr>
<td>Report by country</td>
<td>15%</td>
</tr>
<tr>
<td>Not applicable, we do not report on information technology risk</td>
<td>6%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>3%</td>
</tr>
<tr>
<td>Report by industry sector</td>
<td>3%</td>
</tr>
<tr>
<td>Other</td>
<td>0%</td>
</tr>
</tbody>
</table>
To what extent are you involved in ITRM at your company?

<table>
<thead>
<tr>
<th>Area</th>
<th>High Involvement</th>
<th>Medium Involvement</th>
<th>Low Involvement</th>
<th>Rare Involvement</th>
<th>No Involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition of the ITRM framework</td>
<td>57%</td>
<td>25%</td>
<td>6%</td>
<td>3%</td>
<td>9%</td>
</tr>
<tr>
<td>IT risk identification, assessment and evaluation</td>
<td>54%</td>
<td>37%</td>
<td>5%</td>
<td>4%</td>
<td></td>
</tr>
<tr>
<td>IT risk monitoring</td>
<td>46%</td>
<td>31%</td>
<td>12%</td>
<td>6%</td>
<td>5%</td>
</tr>
<tr>
<td>Development and implementation of the ITRM framework</td>
<td>46%</td>
<td>32%</td>
<td>8%</td>
<td>8%</td>
<td>6%</td>
</tr>
<tr>
<td>IT risk response</td>
<td>38%</td>
<td>38%</td>
<td>11%</td>
<td>3%</td>
<td>10%</td>
</tr>
<tr>
<td>Controls monitoring and maintenance</td>
<td>35%</td>
<td>35%</td>
<td>15%</td>
<td>8%</td>
<td>7%</td>
</tr>
<tr>
<td>IS control design and implementation</td>
<td>32%</td>
<td>31%</td>
<td>23%</td>
<td>5%</td>
<td>9%</td>
</tr>
</tbody>
</table>

Summary

► Reporting on IT risk assessments at the enterprise level is the number one reporting priority. Approximately 50% of survey participants reported that they aggregate results into a risk management dashboard for the entire company. Only 15% of the companies report either by country, geographic region or industry sector, which is, of course, dependent on the company’s geographical coverage, e.g., international or not.
► The analysis of the results show that almost a third of participants have more than two different reporting methods in place. Around 5% have more than five different reports in place.
► 6% of participants do not report on IT Risks.

Conclusion

► Almost 50% of those surveyed have no ITRM dashboard for the entire company. This factor could influence the alignment of ITRM with ERM strategies and frameworks.
► Participants with an existing risk reporting method also appear to have well-established risk reporting mechanisms. Nevertheless, the survey reveals that risk reporting is the area requiring most investment over the next 12 months. Therefore, it seems that the investment will either be made to further optimize or enhance reporting to obtain a more granular risk view.
► Investment should be made to improve the risk management reporting dashboard and in its integration with ERM activities, e.g., as part of risk convergence projects.
Please indicate the extent of your agreement with the following statement: “My company has formal and clear defined roles and responsibilities (mandate) for the IT risk function.”

- Strongly disagree: 2%
- Disagree: 12%
- Neither agree nor disagree: 18%
- Agree: 37%
- Strongly agree: 31%
To whom does the ITRM function or oversight role report?

Risk function reporting

Other:
- Chief internal control officer
- Internal audit director
- Staff and HR director
- Head of technology, new technology director
- Privacy and global continuity manager
- Group risk committee
- Joint line to CIO and head of operational risk
- There is no dedicated function
Roles and responsibilities and Risk function reporting

Summary
► 68% of survey participants agree that they have formal and clearly defined roles and responsibilities (mandate) for the IT risk functions.
► 10% of participants stated that the ITRM function reports to the CEO. Mature risk management functions reports to either the chief risk officer or chief information risk officer or the chief operation officer.
► 65% of organizations report their IT risk assessments at the enterprise level.

<table>
<thead>
<tr>
<th>Role</th>
<th>2008</th>
<th>2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief information officer</td>
<td>50%</td>
<td>34%</td>
</tr>
<tr>
<td>Chief risk officer</td>
<td>21%</td>
<td>31%</td>
</tr>
<tr>
<td>Chief executive officer</td>
<td>13%</td>
<td>9%</td>
</tr>
<tr>
<td>Chief compliance officer</td>
<td>4%</td>
<td>12%</td>
</tr>
<tr>
<td>Chief operation officer</td>
<td>-</td>
<td>26%</td>
</tr>
<tr>
<td>Chief information security officer</td>
<td>-</td>
<td>14%</td>
</tr>
<tr>
<td>Chief financial officer</td>
<td>-</td>
<td>6%</td>
</tr>
<tr>
<td>Other</td>
<td>13%</td>
<td>14%</td>
</tr>
</tbody>
</table>

Conclusion
► In summary, the survey shows that roles and responsibilities, as well as the reporting line, appear clearly defined. Some have more than one reporting line. Compared with 2008, where 50% said that they report to the CIO, over the last four years, more dedicated risk functions have been established, resulting in more reporting lines.
► We can see that, in cases where a common risk and control framework exists, most roles and responsibilities for the ITRM function are well defined. Conversely, there is no relation between clearly defined roles and responsibilities and the size of the company.
► Well-defined roles and responsibilities of an ITRM function could be the results of investment in ITRM frameworks.
Select from the list below the responsibilities that the ITRM function is – or is considered to be – responsible for.

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify and evaluate risk response options and initiate the decision-making process</td>
<td>84%</td>
</tr>
<tr>
<td>Information Technology Risk reporting (e.g., dashboard)</td>
<td>78%</td>
</tr>
<tr>
<td>Education about information technology policies, guidelines and regulatory requirements</td>
<td>69%</td>
</tr>
<tr>
<td>Establishing the risk framework for information technology management</td>
<td>67%</td>
</tr>
<tr>
<td>Interfacing with regulators or auditors</td>
<td>66%</td>
</tr>
<tr>
<td>Implementation of risk assessment tools and technologies</td>
<td>61%</td>
</tr>
<tr>
<td>Implementation of monitoring tools and technologies</td>
<td>45%</td>
</tr>
<tr>
<td>Independent review of risk governance and management processes by internal or external auditors</td>
<td>34%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
</tbody>
</table>

Summary
- Approximately 80% of survey participants reported that the ITRM function is responsible for:
  - Identifying and evaluating risk response options and initiating the decision-making process
  - IT risk reporting
  - Only 45% of ITRM functions are currently responsible for the implementation of monitoring tools and technologies.
- 37% of those surveyed considered tools to monitor and report risk to be a challenge to their ITRM function.
- Implementation of monitoring tools and technology is rated as the lowest priority in global environments.

Conclusion
- It is clear that the ITRM function is very diverse, 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 on one hand, but as flexible as possible and forward looking on the other hand.
- We assume that the need for a greater interfacing with regulators and auditors will grow significantly, especially in the financial service industry.
Which of the following standards or leading practices have you used in developing your information technology risk framework and assessment processes?

<table>
<thead>
<tr>
<th>Standard/Practices</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27005:2008</td>
<td>50%</td>
</tr>
<tr>
<td>Risk IT Framework - ISACA</td>
<td>39%</td>
</tr>
<tr>
<td>Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)</td>
<td>30%</td>
</tr>
<tr>
<td>NIST-SP 800</td>
<td>30%</td>
</tr>
<tr>
<td>Information Risk Analysis Methodologies (IRAM)</td>
<td>30%</td>
</tr>
<tr>
<td>Other</td>
<td>22%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>19%</td>
</tr>
<tr>
<td>Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management (COSO ERM)</td>
<td>17%</td>
</tr>
<tr>
<td>British Standard BS-6079-3:2000</td>
<td>8%</td>
</tr>
<tr>
<td>AS/NZS 4360 Risk Management Standard - Australia and New Zealand Standard</td>
<td>3%</td>
</tr>
<tr>
<td>CCTA Risk Analysis and Management Method (CRAMM)</td>
<td>0%</td>
</tr>
<tr>
<td>Canadian risk management guideline CAN/CSA-Q850-97</td>
<td>0%</td>
</tr>
<tr>
<td>Consultative, Objective, and Bi-functional Risk Analysis (COBRA)</td>
<td>0%</td>
</tr>
</tbody>
</table>

Other: ISO 31000:2009, ITIL, COBIT, M_o_R®, Schweizerische Treuhandkammer, historically developed and mapped to industry standards such as COBIT, ISO or PCI-DSS, etc.,

Summary
- 50% of companies have used ISO standards in the development of their ITRM framework.
- 39% of companies have used ISACA standards in the development of their ITRM framework.
- Independent of the company size, key standards or leading practices used in developing an information technology risk framework and assessment processes are:
  - ISO 27005:2008 - information security risk management (50%)
  - ISACA - risk IT framework (39%)
  - OCTAVE, NIST-SP 800, IRAM (30% each)

Conclusion
- The results indicate ITRM is an Information security risk management topic and often driven by security from the outset.
- It also shows that Risk IT from ISACA is well accepted and is the leading standards used by the companies surveyed. Scenario-based risk management seems to be preferred approach.

The importance of Risk IT by ISACA and the related Certification Certified in Risk and Information Systems Control (CRISC) is incessantly growing. ISACA has won the Best Professional Certification Program Award from SC Magazine for the Certified in Risk and Information Systems Control (CRISC) credential. The 2013 SC Awards were presented in conjunction with the RSA Conference 2013 in San Francisco.

*Source: http://www.sfisaca.org
http://awards.scmagazine.com/best-professional-certification-program-1*
Does your company have defined information technology risk performance metrics that are monitored and reported to management on a regular basis?

- Yes: 36%
- We are in the process of specifying Information Technology Risk performance metrics: 22%
- No: 20%
- We will specify Information Technology Risk performance metrics within the next 12 months: 11%
- Don't know: 5%
- Metrics are specified and monitored, but not reported to senior management: 3%
- Metrics are specified, but not monitored or reported to senior management: 3%
For which of the following information technology activities has your company defined KRIs or KPIs?

<table>
<thead>
<tr>
<th>Activity</th>
<th>2012</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem and incident management</td>
<td>60%</td>
<td></td>
</tr>
<tr>
<td>Continuity of business, e.g., availability and capacity</td>
<td></td>
<td>80%</td>
</tr>
<tr>
<td>Security management</td>
<td></td>
<td>83%</td>
</tr>
<tr>
<td>Change management</td>
<td></td>
<td>63%</td>
</tr>
<tr>
<td>Regulatory and compliance management</td>
<td></td>
<td>63%</td>
</tr>
<tr>
<td>Vendor management</td>
<td></td>
<td>49%</td>
</tr>
<tr>
<td>Third party</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project and benefits management</td>
<td></td>
<td>59%</td>
</tr>
<tr>
<td>Performance management</td>
<td></td>
<td>61%</td>
</tr>
<tr>
<td>Data governance and data management</td>
<td></td>
<td>54%</td>
</tr>
<tr>
<td>Information technology financial management</td>
<td></td>
<td>64%</td>
</tr>
<tr>
<td>Resource management</td>
<td></td>
<td>50%</td>
</tr>
<tr>
<td>Not applicable – we do not develop KRIs or KPIs for Information Technology Risk</td>
<td>10%</td>
<td></td>
</tr>
<tr>
<td>Don’t know</td>
<td></td>
<td>19%</td>
</tr>
</tbody>
</table>

Summary

- Only 36% of companies currently have defined IT risk performance metrics that are regularly monitored and reported to management.
- 33% are either in the process of specifying IT risk performance metrics or will specify metrics within the next 12 months.
- 20% said that they do not have defined information technology risk performance metrics that are monitored and reported to management on a regular basis.
- 11% will not develop ITRM KRIs or KPIs.
- KRIs and KPIs for vendor management and third-party management are not well defined (approximately 0%).
- According to the survey results, the most defined KRIs or KPIs are:
  - Problem and incident management (66%)
  - Continuity of business, e.g., availability and capacity (64%)
  - Security management (56%)
  - Change management (53%)

Conclusion

- Only a third of organizations surveyed have information technology risk performance metrics that are monitored and reported in place. Such measurements are only useful if controls are well defined. On the other hand, having defined metrics and monitoring controls should lead into proper IT risk reporting, which is not presently the case.
- Defining proper KRIs and KPIs seems to pose a challenge, in particular, where outsourcing is involved.
Please indicate the extent of your agreement with the following statement: “Senior management takes appropriate action in a timely manner to address information technology risk indicators that have been identified and reported to them.”

Summary
- Almost 80% agree that senior management takes appropriate action in a timely manner to address information technology risk indicators that have been identified and reported to them.
- 78% of organizations agree that IT risk indicators reported to them are actioned in a timely manner.
- Strongly agree: 2013 = 19%, down from 34% in 2008.

Conclusion
- Overall, actions are taken in a timely manner and are independent of those to whom the ITRM function or oversight role reports.
- Actions taken by senior management are not dependent on the reporting line.
Section 2
Organizational information
## Summary

Of the participating companies ... 

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>80%</td>
<td>Have less than 10,000 employees</td>
</tr>
<tr>
<td>61%</td>
<td>Generate more than US$1b annual revenue</td>
</tr>
<tr>
<td>25%</td>
<td>Are global multinational companies</td>
</tr>
<tr>
<td>45%</td>
<td>Are local companies (operate in one country)</td>
</tr>
<tr>
<td>45%</td>
<td>Are publicly owned</td>
</tr>
<tr>
<td>65%</td>
<td>Are operating in financial services industries (56% in the banking sector)</td>
</tr>
</tbody>
</table>

- 85% operate within EMEIA
- 29% operate within UK
Financial figures: annual revenue and assets under management

Annual revenue (US$)

- More than $250 billion: 8%
- $25 billion to $250 billion: 10%
- $10 billion to $24 billion: 16%
- $1 billion to $9 billion: 27%
- $500 million to $999 million: 11%
- $250 million to $499 million: 6%
- $100 million to $249 million: 6%
- Less than $100 million: 10%
- Not applicable (e.g., government or non-...): 6%

Assets under management

- 59%
- 41%
Total number of employees

<table>
<thead>
<tr>
<th>Total Number of Employees</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 1,000</td>
<td>38%</td>
</tr>
<tr>
<td>1,000 to 9,999</td>
<td>42%</td>
</tr>
<tr>
<td>10,000 to 49,999</td>
<td>15%</td>
</tr>
<tr>
<td>50,000 to 99,999</td>
<td>2%</td>
</tr>
<tr>
<td>More than 100,000</td>
<td>4%</td>
</tr>
</tbody>
</table>

Operation location

- **Global**
  - Present in multiple continents
  - 25%

- **Regional**
  - Located in several different countries
  - 29%

- **Local**
  - Centralized in one location or country
  - 45%
Form of ownership

- **Public**
  - Present in multiple continents
  - 45%

- **Private**
  - Located in several different countries
  - 42%

- **Government**
  - Centralized in one location or country
  - 13%

Industry

- Financial services - banking: 58%
- Insurance: 13%
- Financial services - asset management: 7%
- Technology: 5%
- Public sector (government or military): 4%
- Other: 16%

Other
- Energy and utilities
- Health care
- Manufacturing - consumer products
- Telecommunications
- Wholesale and distribution
- Airlines
Entity operating areas

EMEIA 85%
Japan 18%
Asia Pacific 27%
Oceania 16%
Far East 18%
Other 15%
Americas 31%

Country

UK 18%
France 13%
Spain 15%
Belgium 13%
Switzerland 47%
Germany 7%
IT risk environment

Aligning ITRM to the business environment
Ernst & Young ITRM framework overview

Developing an ITRM framework

- Corporate risk charter, risk governance structure, strategy and road map, risk tolerance guidance, expectations for risk management and integration of capabilities into operational competencies
- Framework incorporating an IT process, and a risk and control framework (library), with associations to leading regulatory 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

Information and technology risk governance and strategy

- Organization (People, program and function)
- Risk identification and profiling
- Policies and standards

Process, risk and control framework

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

Policies and standards

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

Managing risk, driving value, controlling costs and 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 and issues management)

Tools to facilitate IT risk program processes and reporting
Ernst & Yong have observed some key IT risk trends and challenges that the financial industry is currently experiencing:

### Emerging consumerization
- Increased vulnerabilities due to anytime, anywhere accessibility
- Risk of un-intended sharing and disclosure of confidential data
- Lack of knowledge of new technologies and appropriate management of risks
- Value leakage through poor application of new technologies
- Reputational damage through poor management of new channels (e.g., social media)

### Enhanced persistence of cybercrime
- Spread of malicious code, causing outages
- Data loss increase
- Reputational loss due to poor publicity
- Financial loss due to unauthorized transfers
- Lack of regulatory compliance and ability to respond

### Increased exposure to internal threats
- Heightened exposure to fraud via toxic access combinations
- Data loss or theft increase through inappropriate access rights and monitoring controls

### Rise of cloud computing
- Lack of governance over IT infrastructure applications and databases
- Privacy and security risk exposure, especially through cross-border data transfer
- Increased likelihood of regulatory non-compliance (SOX, Payment Card Industry Data Security Standard (PCI-DSS), etc.,)
- Reduction in IT agility via platform or vendor lock-in

### Growing importance of resiliency
- Failure of business continuity and disaster recovery plans, causing financial and reputational loss
- Single points of failure unidentified in critical infrastructure
- Poor incident management, causing increased reputational and financial loss during an incident

### Continued challenge for skilled staff
- Lack of appropriate knowledge transfer during offshoring and outsourcing or redundancy processes
- Lack of appropriate business knowledge, leading to poor-quality IT solutions
- Inability to recruit key IT staff, leading to a mismatch in IT skills

### Accelerating change agenda
- Failure to deliver IT projects and programs within budget, timing, quality and scope, causing value leakage
- Increased complexity and volume of change, leading to inappropriate control
- Adoption of agile methodologies or similar without due consideration of appropriate and minimal control requirements

### Increased use of outsource providers
- Lack of supplier risk management, leading to exposures (financial, reputational, regulatory, etc.,)
- Lack of awareness of fourth parties and fourth-party risk
- Poor management of regulatory risk, in particular, around data privacy and cross-border controls

### Increased focus on true golden-source data
- Inappropriate usage of data by businesses leading to operational risk exposure
- Inappropriate data classification, leading to poor data disclosure control
- Inability to dispose of data securely due to multiple versions of the truth
- Increased likelihood of data corruption

### Moves to acquire, divest or segregate businesses and IT
- Inability to separate or segregate key systems and technologies
- Lack of ability to integrate and align core systems
- Complex support environments, with loss of legacy knowledge creating poorly supported IT environments

### Increasing regulation
- Cross-border complexities, in particular around data privacy and security, leading to non-compliance
- Increasing focus on cloud, mobile devices, outsourcing and new technologies, adding to complexity and volume of regulation and regulators

### Increasing reliance on future-proof technologies
- Systems selection and integration agenda is increasingly complex
- Ability to maintain the pace of technology change is challenging
- Risk awareness of new technologies can be limited
- Staff training and awareness is often poor, leading to inappropriate selection or requirements
Ernst & Young’s related insights and resources

The evolving IT risk landscape
The why and how of IT Risk Management today

Privacy trends 2013

Lessons from change
Key findings from Ernst & Young 2012 financial services supplier risk management survey

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

Unlocking the power of SAP’s governance, risk and compliance technology

Insights on IT risk:
Countering cyber attacks

Cloud computing issues and impacts

Insights on IT risk:
Data Loss Prevention
Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM</td>
<td>Business continuity management</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring your own device</td>
</tr>
<tr>
<td>DLP</td>
<td>Data leakage prevention</td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster recovery planning</td>
</tr>
<tr>
<td>EMEIA</td>
<td>Europe, Middle East, India and Africa</td>
</tr>
<tr>
<td>ERM</td>
<td>Enterprise risk management</td>
</tr>
<tr>
<td>GRC</td>
<td>Governance, risk and compliance</td>
</tr>
<tr>
<td>IAM</td>
<td>Identity and access management</td>
</tr>
<tr>
<td>ISO</td>
<td>International standards organization</td>
</tr>
<tr>
<td>ITRM</td>
<td>IT risk management</td>
</tr>
<tr>
<td>KPI</td>
<td>Key performance indicator</td>
</tr>
<tr>
<td>KRI</td>
<td>Key risk indicator</td>
</tr>
<tr>
<td>ORM</td>
<td>Operational risk management</td>
</tr>
</tbody>
</table>

Contacts

**Ernst & Young ITRM contacts**

<table>
<thead>
<tr>
<th>Name</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pat Moran</td>
<td>+ 353 1 221 2769 <a href="mailto:pat.moran@au.ey.com">pat.moran@au.ey.com</a></td>
</tr>
<tr>
<td>Reto Aeberhardt</td>
<td>+ 41 58 286 6740 <a href="mailto:reto.aeberhardt@ch.ey.com">reto.aeberhardt@ch.ey.com</a></td>
</tr>
<tr>
<td>James Turpie</td>
<td>+ 44 131 777 2040 <a href="mailto:jturpie@uk.ey.com">jturpie@uk.ey.com</a></td>
</tr>
<tr>
<td>David F. Santiago</td>
<td>+ 34 915 727 253 <a href="mailto:david.fernandezsantiago@es.ey.com">david.fernandezsantiago@es.ey.com</a></td>
</tr>
<tr>
<td>Stefano Ciminelli</td>
<td>+ 32 2 774 60 02 <a href="mailto:stefano.ciminelli@ey.be.com">stefano.ciminelli@ey.be.com</a></td>
</tr>
<tr>
<td>Daniel Jenth</td>
<td>+ 49 6196 996 20325 <a href="mailto:daniel.jenth@de.ey.com">daniel.jenth@de.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.

About EY’s Advisory Services
The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 25,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience.

We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that, to achieve your potential as an organization, you require services that respond to your specific issues, so we bring our broad sector experience and deep subject-matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It’s how Ernst & Young makes a difference.

© 2013 EYGM Limited.
All Rights Reserved.
EYG no. AU1712
ED None

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.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

ey.com