ISACA*
With more than 86,000 constituents in more than 160 countries, ISACA (www.isaca.org) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the Information Systems Control Journal®, and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 60,000 professionals since 1978; the Certified Information Security Manager® (CISM®) designation, earned by more than 9,000 professionals since 2002; and the new Certified in the Governance of Enterprise IT™ (CGEIT™) designation.

Disclaimer
ISACA has designed and created Top Business/Technology Issues Survey Results (the “Work”), primarily as an informational resource for audit/assurance professionals, security management and information technology (IT) management. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, CIOs, senior management and IT management should apply their own professional judgment to the specific circumstances presented by the particular systems or IT environment.

Disclosure
© 2008 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use, and consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: info@isaca.org
Web site: www.isaca.org

Top Business/Technology Issues Survey Results
Printed in the United States of America.
Acknowledgments

ISACA wishes to recognize:

**Top Business/Technology Issues Task Force**
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA, Chair
Anthony Noble, CISA, CCP, Viacom Inc., USA
Manuel Aceves, CISA, CISM, CISSP, Mexico
Sushil Chatterji, Edutech, Singapore
Wim Van Grembergen, Ph.D., University of Antwerp Management School, and IT Alignment and Governance (ITAG) Research Institute, Belgium
Rolf von Roessing, CISA, CISM, CGEIT, KPMG, Germany
Paul Zonneveld, CISA, CA, Deloitte, Canada

**ISACA Board of Directors**
Lynn Lawton, CISA, FBCS, FCA, FIIA, KPMG LLP, UK, International President
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control sa-nv, Belgium, Vice President
Avinash Kadam, CISA, CISM, CBCP, CISSP, GCIH, GSEC, Miel e-Security Pvt. Ltd., India, Vice President
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Vice President
Jose Angel Pena Ibarra, CGEIT, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President
Robert E. Stroud, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President
Frank Yam, CISA, FHKCS, FHKIoD, CIA, CCP, CFE, CFSA, FFA, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President
Emil D’Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., USA, Director
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA, Director
# Table of Contents

## Executive Summary
- Project Objectives ..................................................................................................................... 5
- Survey Sample ................................................................................................................................. 5
- Global Reach .................................................................................................................................. 5
- How to Read This Report ................................................................................................................ 5
- Key Findings of the Survey ............................................................................................................. 5

## 1. Research Approach and Methodology
- Survey Approach ............................................................................................................................ 7
- Drill-down Approach ....................................................................................................................... 7
- The Respondents ............................................................................................................................. 7

## 2. Top Seven Business Issues
- Introduction ........................................................................................................................................ 10
- Issue 1: Regulatory Compliance ...................................................................................................... 11
- Issue 2: Enterprise-based IT Management and IT Governance ...................................................... 11
- Issue 3: Information Security Management .................................................................................... 12
- Issue 4: Disaster Recovery/Business Continuity ............................................................................. 12
- Issue 5: IT Value Management ...................................................................................................... 13
- Issue 6: Challenges of Managing IT Risks ..................................................................................... 13
- Issue 7: Compliance With Financial Reporting ............................................................................ 14

## 3. Top Five Business Issues—Audit/Assurance
- Introduction ........................................................................................................................................ 15
- Top Issues ....................................................................................................................................... 15

## 4. Top Five Business Issues—IT Management
- Introduction ........................................................................................................................................ 16
- Top Issues ....................................................................................................................................... 16

## 5. Top Five Business Issues—Security Management
- Introduction ........................................................................................................................................ 17
- Top Issues ....................................................................................................................................... 17

## Appendix
- About ISACA .................................................................................................................................... 18
- Questionnaire ................................................................................................................................. 18

## List of Figures
- ..................................................................................................................................................... 32

## Other Publications
- ..................................................................................................................................................... 33
Executive Summary

At the end of 2007, ISACA’s Board of Directors commissioned a project that involved a task force of volunteers from ISACA’s Assurance, IT Governance and Security Management committees. The top business/technology issues survey was conducted globally over three weeks in April and May 2008 with the assistance of audit/assurance, IT and information security managers across the globe, resulting in this report.

Project Objectives

ISACA recently established a business/technology issues task force that identified 21 current business issues that are impacted by technology and that face IT managers and executives. The list consisted of global issues that the task force felt were already affecting ISACA members and constituents, or would be in the next 12 to 18 months.

The 2008 ISACA top business/technology issues survey was conducted to assist the task force in validating and prioritizing these issues within ISACA. The ultimate purpose of the study was to obtain guidance that could readily be used by ISACA to direct resources for the creation of guidance, tools and techniques for addressing the key issues being faced by ISACA audit/assurance, security and IT management members. To facilitate ease of use, the structure of this report parallels that of the survey form, a copy of which can be found in the appendix.

Survey Sample

The total number of completed and usable responses to the survey was 3,173, representing a 6.9 percent response rate. The survey was distributed on 30 April 2008 to 46,101 ISACA members via an e-mail message containing a link to the online survey web site. Reminder e-mails were sent on 13 May 2008, and responses were accepted through 21 May.

Global Reach

The business/technology survey had robust worldwide participation, with respondents from 95 countries, representing all five ISACA regions. More detail on geographic distribution of respondents can be found in chapter 1 in the section titled “The Respondents.”

How to Read This Report

The report contains five chapters:
• Chapter 1 explains the methodology used to conduct the survey.
• Chapter 2 focuses on the survey results supporting the top seven business issues.
• Chapter 3 presents the top five business issues from an audit/assurance perspective.
• Chapter 4 highlights the top five business issues from an IT management perspective.
• Chapter 5 identifies the top five business issues from a security management perspective.

The appendix includes the questionnaire and provides additional information about ISACA. There is a list of figures at the end of the report.

Key Findings of the Survey

The top seven business issues identified by the survey are as follows:
1. Regulatory compliance—Organizations are faced with more challenges now than ever; they must grow and maximize market opportunities while at the same time complying with an ever-increasing number of regulations and standards. Keeping on top of legislative and regulatory requirements is a significant task, and regulatory compliance still operates in “project” mode and has not yet been embedded in business processes. IT must design and maintain systems to comply with these legislative and regulatory requirements, despite the lack of an integrated framework.
2. Enterprise-based IT management and IT governance—Managing efficient and effective IT departments requires IT governance—
the disciplines and capabilities that bring consistent and reliable delivery of IT services to the business. IT governance requires the alignment of IT operations with the goals and objectives of the business. In addition, delivery of IT services requires well-designed IT processes and coordination among the IT team members. However, while there is some recognition of the importance of IT governance at the executive level, further awareness is needed.

3. **Information security management**—After many spectacular breaches and losses, and enormous spending on “state-of-the-art” security technologies, enterprises are finally realizing that information security has more to do with managing people and process and less to do with implementation of technology. In so doing, enterprises can leverage international information security management standards (such as ISO/IEC 27001) that provide guidelines and common practices rather than reinventing the wheel each time.

4. **Disaster recovery/business continuity**—All business activity is subject to disruptions, such as technology failure, flooding, utility disruption and terrorism. In response, some enterprises implement business continuity management (BCM) programs to improve their resilience in the event of disaster. Unfortunately, these enterprises are in the minority and BCM still remains an elusive goal for most organizations.

5. **IT value management**—IT projects often lack alignment with business goals and objectives; as a result, they are unable to realize business benefits. In some cases, there is a lack of business involvement in IT projects, while in others, there is simply a breakdown in communication between what the business has asked for and what IT has delivered. Implementing processes to help bridge these gaps allows IT to service the needs of business and deliver value.

6. **Challenges of managing IT risks**—Risk management practices are poorly understood at the best of times so it is no surprise that IT risk management fares no better. Unfortunately, IT risks are pervasive across enterprises, so the impact of poor IT risk management can be disastrous.

7. **Compliance with financial reporting standards**—Global financial reporting standards, such as the US Sarbanes-Oxley Act, have been in place since 2004; however, they continue to be an area of focus for IT departments. While improvements have been made to the standards that help focus efforts on areas of higher risk, enterprises continue to experience challenges in complying in a cost-effective manner.
1. Research Approach and Methodology

Survey Approach

To conduct this study, ISACA retained the services of Industry Insights Inc., an independent research firm headquartered in Columbus, Ohio, USA.

The research instrument used for the study was a survey form that was designed by ISACA, working in close conjunction with Industry Insights. The survey was hosted online by Industry Insights. It was divided into four sections to ease the burden of completion on the part of the members. Respondents were asked basic demographic questions and questions related to ISACA membership on the first page. On the second page, the respondents were presented with the 21 current business issues facing IT managers and executives (as identified by the project task force) and were asked to indicate the level of importance and/or impact on their enterprise that these issues would have during the next 12 to 18 months. The third page listed those business issues that the respondents rated as “somewhat important” or “very important,” and asked the respondents to rank the five most important issues based on relative importance and/or impact on their enterprise.

Drill-down Approach

To perform further analysis on specific technology-based products and/or solutions for the top issues facing ISACA members, the survey included several possibilities of focus for each of the respondents’ top five issues. Respondents were asked to indicate the importance of each of the products and/or solutions in addressing the primary business issue. A sample of the survey instrument can be found in the appendix of this report.

The Respondents

The total number of completed and usable responses to the survey was 3,173, representing a 6.9 percent response rate. A more detailed analysis of the respondents is provided in the following paragraphs.

Geographic Reach

Figure 1 presents the regional breakdown of the survey respondents vs. the breakdown of ISACA members overall. The sample is, for the most part, reflective of the overall membership numbers.
**Figure 2** shows that a good global cross-section of ISACA members participated in the survey. The figure lists the countries with the highest level of participation in the ISACA survey.

### Figure 2—Country of Current Employment

- **USA**: 31.0%
- **India**: 6.2%
- **Canada**: 5.3%
- **United Kingdom**: 4.4%
- **Japan**: 3.1%
- **Australia**: 3.1%
- **Spain**: 3.0%
- **Hong Kong**: 2.0%
- **Italy**: 1.9%
- **Germany**: 1.8%

**Industry of Survey Respondents**

Survey respondents represent a wide variety of industries. **Figure 3** presents industries with the highest level of participation, broken down by audit/assurance, security management and IT management.

### Figure 3—Current Field of Employment

- **Technology Services/Consulting**: 31.2%
- **Financial/Banking**: 25.1%
- **Government/Military**: 28.2%
- **National/State/Local**: 25.1%
- **Manufacturing/Engineering**: 21.1%
- **Insurance**: 18.7%
- **Public Accounting**: 18.8%
- **Telecommunications/Communications**: 7.9%
- **Health Care/Medical**: 6.8%
- **Retail/Wholesale/Distribution**: 5.3%
- **Other**: 3.5%
- **Audit/Assurance**: 4.7%
- **Security Management**: 4.4%
- **IT Management**: 9.4%
Primary Job Responsibility

The survey results indicate an even spread of primary job responsibility. Thus, the results obtained for each of the three constituency areas are statistically significant, as shown in figure 4.

<table>
<thead>
<tr>
<th>Primary Job Responsibility</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Management</td>
<td>32.7%</td>
</tr>
<tr>
<td>Audit/Assurance</td>
<td>41.3%</td>
</tr>
<tr>
<td>Security Management</td>
<td>26%</td>
</tr>
</tbody>
</table>
2. Top Seven Business Issues

Introduction

The next section of the report details the key findings of the survey. The results are first reported in aggregate for all respondents. In subsequent sections, the results are broken down by the specific constituency area—audit/assurance, IT management or security management.

The top seven business issues affected by technology that will face IT managers and executives and impact their enterprises during the next 12 to 18 months are shown in figure 5.

<table>
<thead>
<tr>
<th>Business Issue</th>
<th>Number of Responses</th>
<th>Weighted Score$^1$</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory compliance</td>
<td>1,499</td>
<td>5,202</td>
<td>15.2%</td>
<td>10.6%</td>
<td>8.9%</td>
<td>6.6%</td>
<td>6.4%</td>
</tr>
<tr>
<td>Enterprise-based IT management and IT governance</td>
<td>1,462</td>
<td>5,088</td>
<td>16.5%</td>
<td>9.0%</td>
<td>7.6%</td>
<td>6.5%</td>
<td>6.9%</td>
</tr>
<tr>
<td>Information security management</td>
<td>1,592</td>
<td>4,887</td>
<td>11.3%</td>
<td>9.6%</td>
<td>9.9%</td>
<td>10.6%</td>
<td>9.5%</td>
</tr>
<tr>
<td>Disaster recovery/business continuity</td>
<td>1,482</td>
<td>4,283</td>
<td>7.4%</td>
<td>9.5%</td>
<td>10.3%</td>
<td>10.1%</td>
<td>10.0%</td>
</tr>
<tr>
<td>IT value management</td>
<td>982</td>
<td>3,142</td>
<td>6.9%</td>
<td>7.8%</td>
<td>5.8%</td>
<td>5.5%</td>
<td>5.3%</td>
</tr>
<tr>
<td>Challenges of managing IT risks</td>
<td>1,022</td>
<td>2,862</td>
<td>4.7%</td>
<td>5.7%</td>
<td>7.3%</td>
<td>7.8%</td>
<td>7.2%</td>
</tr>
<tr>
<td>Compliance with financial reporting standards</td>
<td>855</td>
<td>2,710</td>
<td>5.7%</td>
<td>6.7%</td>
<td>5.3%</td>
<td>5.2%</td>
<td>4.4%</td>
</tr>
</tbody>
</table>

Some mention should be given to four areas that just missed the top seven this year and have the potential to be in the top seven next year:

1. **Continuous process improvement and business agility**—Modern enterprises now recognize that “business processes are the business” and that enterprise success is dependent on establishing the capabilities and infrastructures to continually improve business processes and rapidly implement change. This might prove very difficult and complex unless organizations foster business process-centric cultures, start thinking in terms of “processing business processes” (i.e., business process life cycle automation) and rethink/revamp their application software engineering practices and infrastructures. The promised land is now named business process management (BPM) and service-oriented architecture (SOA), but is fraught with challenges.

2. **Vulnerability management**—With the growth of the Internet and other communication methods, managing the threats of unauthorized access and data leakage is becoming a priority for almost all enterprises. Vulnerability management tools that help prevent and detect unauthorized access are essential in ensuring privacy, confidentiality, data integrity and availability.

3. **Collaborative/extended enterprises**—Many enterprises have tried to identify and achieve seamless integration of value chain components coming from a variety of enterprises, especially at the business process and technology tiers. Only a few enterprises have succeeded (e.g., Dell).

4. **Modernization and consolidation**—Replacing legacy applications and infrastructure while consolidating services, operations and resources is difficult to accomplish while reducing IT complexity and facing increasing storage demands and mobile device management. The costs and risks associated with complexity are causing management to focus more attention on this area.

For their top five issues, respondents were requested to indicate the level of importance of products, inhibitors and/or potential solutions associated with the respective issues for further analysis. Figures 6 through 12 show the survey results for the additional “drill-down” items for the top seven issues for all respondents.

---

$^1$ The weighted score in all figures is simply the average multiplied by the number of responses. This score gives weight to the issue receiving a ranking of most important. By doing this, the ranking or “score” for the top five business issues takes into account the frequency with which the issue was indicated as one of the top five business issues and also weights the importance each issue was given. For instance, each time a business issue was ranked as the most important business issue, it was scored 5 (second most important scored 4, third most important scored 3, fourth most important scored 2 and fifth most important scored 1).
Issue 1: Regulatory Compliance

Enterprises are faced with more business challenges now than ever; they must grow and maximize market opportunities while at the same time complying with an ever-increasing number of regulations and standards. Within the topic of regulatory compliance, the key technology areas that respondents felt will be the most important over the next 12 to 18 months (illustrated in figure 6) include the implementation of technology to support segregation of duties, privileged access monitoring and management of the compliance process. Two areas that were ranked nearly as high by ISACA members were the implementation of tools to support continuous transaction monitoring and systems to protect companies from the loss of personally identifiable information (PII).

![Figure 6—Regulatory Compliance Drill-down Importance (All Respondents)](image)

Issue 2: Enterprise-based IT Management and IT Governance

Managing efficient and effective IT departments requires IT governance—the disciplines and capabilities that bring consistent and reliable delivery of IT services to the business. IT governance requires the alignment of IT operations with the goals and objectives of the business. In addition, delivery of IT services requires well-designed IT processes and coordination among the IT team members. Within the topic of enterprise-based IT management, the key technology areas that the respondents believe will be the most important over the next 12 to 18 months (illustrated in figure 7) are the implementation of tools for the reporting of the business value generated by IT-driven change, tools to aid in performance management of IT and systems to aid enterprises in portfolio management of their IT-enabled investments to ensure that IT resources are deployed where the most business value can be derived.

![Figure 7—Enterprise-based IT Management Drill-down Importance (All Respondents)](image)
**Issue 3: Information Security Management**

The number of threats to an enterprise’s data that require management continues to grow at an exponential rate. Fortunately, a well-planned information security management approach can help make sense of the deluge. A proactive security management plan includes process, policy and technology. Within the topic of information security management, the key area that respondents believe will be the most important over the next 12 to 18 months (illustrated in figure 8) is an inhibitor to security where the effectiveness of controls is not properly monitored. The lack of senior management involvement in setting direction for information security was also highlighted as a key area, which ties to information security being viewed as only an IT issue. This may be the result of the lack of an enterprisewide information security awareness program.

### Figure 8—Information Security Management Drill-down Importance (All Respondents)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Somewhat Important</th>
<th>Very Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance and effectiveness of information security controls not regularly measured, monitored or improved</td>
<td>39%</td>
<td>43%</td>
</tr>
<tr>
<td>Information security risks either not known or only partially assessed</td>
<td>43%</td>
<td>38%</td>
</tr>
<tr>
<td>Lack of top management involvement in setting direction and objectives for information security</td>
<td>30%</td>
<td>49%</td>
</tr>
<tr>
<td>Lack of enterprisewide information security awareness and training</td>
<td>39%</td>
<td>38%</td>
</tr>
<tr>
<td>Information security perceived as belonging exclusively to the IT realm</td>
<td>40%</td>
<td>36%</td>
</tr>
</tbody>
</table>

**Issue 4: Disaster Recovery/Business Continuity**

Business continuity management proactively improves enterprise resilience against operational disruptions and provides the capability to react adequately. Notwithstanding the benefits, BCM remains an elusive goal for most enterprises. Within the topic of disaster recovery/business continuity, the key area that respondents felt will be the most important over the next 12 to 18 months (illustrated in figure 9) is business managers’ lack of awareness of their responsibility to be able to maintain critical functions in the event of a disaster, which leads to BCM not being a business-owned and business-driven process. Other areas that were highlighted include the lack of a formal BCM policy within the enterprise and BCM being treated as a “one-time” initiative that requires no maintenance.

### Figure 9—Disaster Recovery/Business Continuity Drill-down Importance (All Respondents)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Somewhat Important</th>
<th>Very Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managers and owners not fully aware of their responsibility to maintain the ability of the enterprise to function without disruption</td>
<td>36%</td>
<td>44%</td>
</tr>
<tr>
<td>Organizations seldom formalizing and enforcing a BCM policy</td>
<td>39%</td>
<td>33%</td>
</tr>
<tr>
<td>BCM not a business-owned and business-driven process</td>
<td>32%</td>
<td>39%</td>
</tr>
<tr>
<td>BCM approached as a “one-time” initiative and not as a process</td>
<td>35%</td>
<td>35%</td>
</tr>
<tr>
<td>BCM regarded as a costly planning process and not as one that adds value to the enterprise</td>
<td>36%</td>
<td>29%</td>
</tr>
</tbody>
</table>
Issue 5: IT Value Management

IT projects often lack alignment with business goals and objectives; as a result, they are unable to realize business benefits. In some cases, there is a lack of business involvement in IT projects, while in others there is simply a breakdown in communication between what the business has asked for and what IT has delivered. Implementing processes to help bridge these gaps allows IT to service the needs of business and deliver value. Within the topic of IT value management, the key area that respondents felt will be the most important over the next 12 to 18 months (illustrated in figure 10) is the implementation of tools for project and knowledge management. Tools to keep track of the portfolio of IT systems and projects, tools for budgeting, and methods to communicate about projects more efficiently and effectively were also found to be important.

![Figure 10—IT Value Management Drill-down Importance (All Respondents)](image)

<table>
<thead>
<tr>
<th>Tool Type</th>
<th>Somewhat Important</th>
<th>Very Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project management tools</td>
<td>41%</td>
<td>36%</td>
</tr>
<tr>
<td>Knowledge management tools</td>
<td>39%</td>
<td>32%</td>
</tr>
<tr>
<td>Communication tools</td>
<td>44%</td>
<td>24%</td>
</tr>
<tr>
<td>Portfolio tools</td>
<td>40%</td>
<td>27%</td>
</tr>
<tr>
<td>Budgeting tools</td>
<td>39%</td>
<td>22%</td>
</tr>
</tbody>
</table>

Issue 6: Challenges of Managing IT Risks

Many enterprises do not understand that they are also in the business of managing their risks, from the boardroom to the network. IT risk variables can often interact in complex and subtle ways, making IT risk management a very difficult endeavor. Within the topic of managing IT risk, the key area that respondents felt will be the most important over the next 12 to 18 months (illustrated in figure 11) is the current lack of senior management commitment to and awareness of IT risk management, along with a lack of understanding of what IT risks are. Funding for IT risk management projects and the lack of IT risk management standards were also highlighted.

![Figure 11—Challenges of Managing IT Risk Drill-down Importance (All Respondents)](image)

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Somewhat Important</th>
<th>Very Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT risk illiteracy and lack of awareness</td>
<td>41%</td>
<td>41%</td>
</tr>
<tr>
<td>Lack of senior management commitment to IT risk management</td>
<td>31%</td>
<td>49%</td>
</tr>
<tr>
<td>Risk management processes, if any, not following generally accepted principles, practices and standards</td>
<td>41%</td>
<td>30%</td>
</tr>
<tr>
<td>Poor funding and staffing for risk management purposes</td>
<td>39%</td>
<td>32%</td>
</tr>
</tbody>
</table>
Issue 7: Compliance With Financial Reporting

Global financial reporting standards, such as the US Sarbanes-Oxley Act, have been in place since 2004, but they continue to be an area of focus for IT departments. While improvements have been made to the standards that help focus efforts on areas of higher risk, organizations continue to experience challenges in complying in a cost-effective manner. Within the topic of compliance with financial reporting, the key area that respondents felt will be the most important over the next 12 to 18 months (illustrated in figure 12) is the implementation of tools for managing access and changes to programs and data efficiently and effectively. Lack of a good “tone at the top” regarding compliance was also seen as a potential inhibitor to the tools being deployed. Additionally, managing the development of new systems was considered important.

Figure 12—Compliance With Financial Reporting Drill-down Importance (All Respondents)
3. Top Five Business Issues—Audit/Assurance

Introduction

The next section of the report details the key findings that were identified by analyzing the responses from participants who stated that their primary responsibilities were audit-assurance-related (41.3 percent of the total responses). The results are reported by the highest overall weighted score for the importance ranking. After the top five, there is a significant drop-off in score, which shows that these are the business issues with which ISACA audit/assurance members are most concerned.

Top Issues

The top five business issues impacted by technology, as ranked by the audit/assurance respondents, are shown in figure 13.

<table>
<thead>
<tr>
<th>Business Issue</th>
<th>Number of Responses</th>
<th>Weighted Score</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory compliance</td>
<td>696</td>
<td>2,464</td>
<td>18.4%</td>
<td>12.5%</td>
<td>8.9%</td>
<td>6.6%</td>
<td>7.4%</td>
</tr>
<tr>
<td>Enterprise-based IT management and IT governance</td>
<td>592</td>
<td>2,048</td>
<td>15.8%</td>
<td>8.0%</td>
<td>8.8%</td>
<td>6.7%</td>
<td>6.4%</td>
</tr>
<tr>
<td>Information security management</td>
<td>578</td>
<td>1,734</td>
<td>9.2%</td>
<td>8.3%</td>
<td>8.5%</td>
<td>9.9%</td>
<td>8.9%</td>
</tr>
<tr>
<td>Disaster recovery/business continuity</td>
<td>566</td>
<td>1,528</td>
<td>5.2%</td>
<td>8.0%</td>
<td>9.4%</td>
<td>10.3%</td>
<td>11.0%</td>
</tr>
<tr>
<td>Compliance with financial reporting</td>
<td>468</td>
<td>1,521</td>
<td>7.9%</td>
<td>10.0%</td>
<td>6.7%</td>
<td>5.9%</td>
<td>5.6%</td>
</tr>
</tbody>
</table>

The top issue facing the audit/assurance respondents is regulatory compliance, which is not a surprising result given the audience. Technology to aid in compliance with regulations is being deployed with the support of ISACA’s audit/assurance members because it is much more reliable and cost-effective than the manual business processes currently in place.

For the next issue, enterprise-based IT management and IT governance, technology is being implemented to facilitate the need for documented, justifiable and repeatable IT management processes, such as the system development life cycle.

The third ranked issue is information security management, which has always been, and probably always will be, a focus of audit/assurance professionals.

Disaster recovery/business continuity management, which ranked fourth and has also been a traditional focus for IT audit/assurance, is the implementation of technology systems to aid in the efficiency and effectiveness of these efforts.

The fifth issue, compliance with financial reporting standards, is a more recent focus. As other regulations that may not be financial reporting-based are introduced, enterprises are seeking technology solutions that will enable them to comply with both financial reporting requirements and other applicable regulations.
4. Top Five Business Issues—IT Management

Introduction

The next section of the report details the key findings that were identified by analyzing the responses from respondents who stated that their primary responsibilities were IT management-related (32.7 percent of the total responses). The results are reported by the highest overall weighted score for the importance ranking. After the top five areas, there is one additional area—continuous process improvement and business agility (highlighted earlier in this report as one of the near misses for this year’s top seven business issues)—before the significant drop-off in score.

Top Issues

The top five business issues impacted by technology, as ranked by the IT management respondents, are shown in figure 14.

<table>
<thead>
<tr>
<th>Business Issue</th>
<th>Number of Responses</th>
<th>Weighted Score</th>
<th>Importance Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1st</td>
<td>2nd</td>
</tr>
<tr>
<td>Enterprise-based IT management and IT governance</td>
<td>531</td>
<td>1,917</td>
<td>20.1%</td>
</tr>
<tr>
<td>Disaster recovery/business continuity</td>
<td>518</td>
<td>1,533</td>
<td>9.2%</td>
</tr>
<tr>
<td>IT value management</td>
<td>436</td>
<td>1,500</td>
<td>11.4%</td>
</tr>
<tr>
<td>Information security management</td>
<td>467</td>
<td>1,354</td>
<td>7.9%</td>
</tr>
<tr>
<td>Regulatory compliance</td>
<td>381</td>
<td>1,288</td>
<td>10.0%</td>
</tr>
</tbody>
</table>

The top issue selected by the IT management membership is enterprise-based IT management and IT governance. Technology is being implemented by ISACA’s IT management members to facilitate the growing need for documented, justifiable and repeatable IT management processes, such as the system development life cycle. The use of a globally recognized framework such as Control Objectives for Information and related Technology (COBIT®) helps in this endeavor.

Disaster recovery/business continuity management, which was ranked as the second most important issue for IT management professionals, has been a traditional area of focus for IT professionals. Systems are being implemented to aid in the efficiency and effectiveness of these efforts.

IT value management was considered the third most important issue to IT managers. Frameworks such as Val IT™ support this level of importance.

Information security, which ranked fourth, has also been a conventional focus for IT managers as it has been for security managers and audit/assurance professionals. This supports the premise that information security and IT management are closely related.

The fifth issue for IT management professionals is regulatory compliance. Technology to aid in compliance with regulations is being deployed with the support of ISACA IT management members because it is much more reliable and cost-effective than the manual business processes that have traditionally been in place.
5. Top Five Business Issues—Security Management

Introduction

The next section of the report details the key findings that were identified by analyzing the responses from participants who stated that their primary responsibilities were security management-related (26 percent of the total responses). The results are reported by the highest overall score in aggregate for the overall importance ranking. After the top five, there is a significant drop-off in score, which shows that these are the business issues with which our security management professionals are most concerned.

Top Issues

The top five business issues impacted by technology, as ranked by security management respondents, are shown in figure 15.

<table>
<thead>
<tr>
<th>Business Issue</th>
<th>Number of Responses</th>
<th>Weighted Score¹</th>
<th>Importance Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>1ˢᵗ</td>
</tr>
<tr>
<td>Information security management</td>
<td>547</td>
<td>1,794</td>
<td>18.8%</td>
</tr>
<tr>
<td>Regulatory compliance</td>
<td>422</td>
<td>1,452</td>
<td>16.5%</td>
</tr>
<tr>
<td>Disaster recovery/business continuity</td>
<td>398</td>
<td>1,222</td>
<td>8.6%</td>
</tr>
<tr>
<td>Enterprise-based IT management and IT governance</td>
<td>339</td>
<td>1,122</td>
<td>12.8%</td>
</tr>
<tr>
<td>Challenges of managing IT risks</td>
<td>287</td>
<td>829</td>
<td>5.2%</td>
</tr>
</tbody>
</table>

The top issue facing ISACA’s security management membership is information security management—not surprising given the audience. Technology will always play a key role in securing enterprises’ internal networks and systems from unintended and deliberate attacks.

The second highest-ranked issue is regulatory compliance. Technology to aid in compliance with regulations is being deployed with the support of ISACA’s security management members because it is much more reliable and cost-effective than the manual business processes to secure systems that have traditionally been in place.

Disaster recovery/business continuity management, which was ranked third by security management professionals, has also been a traditional responsibility for them. Systems are being implemented to aid in the efficiency and effectiveness of these efforts.

For the next issue, enterprise-based IT management and IT governance, technology is being implemented by ISACA’s members to facilitate the growing need for documented, justifiable and repeatable IT management processes, such as the onboarding and offboarding of staff onto corporate systems. The use of a globally recognized framework such as COBIT helps in this endeavor.

The fifth issue for ISACA’s security managers is the challenge of managing IT risks. This is one of the key domains for security management professionals, and technology is being introduced to facilitate the growing need for documented and acceptable responses to identified IT-related risks as a part of a larger enterprise risk management program.
About ISACA

ISACA’s constituents—more than 86,000 worldwide—are characterized by their diversity. Members live and work in more than 160 countries and cover a variety of professional IT-related positions—to name just a few, information systems (IS) auditor, consultant, educator, IS security professional, regulator, CIO and internal auditor. Some are new to the field, others are at middle-management levels and still others are in the most senior ranks. They work in nearly all industry categories, including financial and banking, public accounting, government and the public sector, utilities, and manufacturing. This diversity enables members to learn from each other and exchange widely divergent viewpoints on a variety of professional topics. It has long been considered one of ISACA’s greatest strengths. Previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves.

Another of ISACA’s strengths is its chapter network. ISACA has more than 175 chapters established in more than 70 countries worldwide, and those chapters provide members with education, resource sharing, advocacy, professional networking and a host of other benefits on a local level. A list of all chapters is available at www.isaca.org/chapter.

Since its inception, ISACA has become a pace-setting global organization for information governance, control, security and audit professionals. Its IS auditing and IS control standards are followed by practitioners worldwide, and its research pinpoints professional issues challenging its constituents. Its CISA certification is recognized globally and has been earned by more than 60,000 professionals since inception. The CISM certification uniquely targets the information security management audience and has been earned by more than 9,000 professionals. The CGEIT designation promotes the advancement of professionals who wish to be recognized for their IT governance-related experience and knowledge and has been earned by more than 200 professionals since it was introduced in 2007.

ISACA publishes the Information Systems Control Journal and hosts a series of international conferences focusing on both technical and managerial topics pertinent to the IS audit/assurance, control, security and IT management professions. Together, ISACA and its affiliated IT Governance Institute lead the IT governance community and serve its practitioners by providing the elements needed by IT professionals in an ever-changing global environment.

Questionnaire

The following pages reproduce the survey that produced the results that formed the basis of this publication.
Thank You for Participating in ISACA’s Top Business/Technology Issues Survey

ISACA recently established a Business /Technology Issues Task Force that identified twenty-one (21) current business issues facing IT managers and executives that are supported by technology based products and/or solutions. The list consists of global issues that the task force felt were already affecting ISACA members and constituents, or would be in the next twelve to eighteen months.

In order to assist the task force to validate and prioritize these issues, please complete this survey. The survey will collect detailed data on the impact and importance of each issue and the related technologies. Survey results will be shared with ISACA members and constituents and will be used to create guidance, tools and techniques for addressing these issues from an assurance, security and governance perspective. The survey should take between ten and fifteen minutes.

Please answer each question honestly and completely based on your own experience. Your individual responses to the survey questions will be entirely confidential. Please note that the survey is written in American English.

To begin the survey, click on the button below. Please be sure to answer each question and submit your responses to the survey by 21 May 2008.

Thank you in advance for your participation in this important project. We look forward to sharing with you the results of the study, after the findings have been tabulated and evaluated.

Click here to begin

© ISACA and Industry Insights, Inc.
If you are experiencing technical issues, please contact ISACA@industryinsights.com
Demographics
An answer to each question is required to continue with this survey.

1. Which of the following most closely describes your primary job responsibility?
   - Audit/Assurance Management
   - Security Management
   - IT Management

2. Current Professional Activity:
   Please select the job title that best describes your position. [ ] Other (Please specify.)

3. How many years of management experience do you have?
   - No management experience
   - 1-2
   - 3-5
   - 6-10
   - 11 or greater

4. What is the size of your organization?
   (Indicate total number of employees)
   - 1-99
   - 100-499
   - 500-1,499
   - 1,500-9,999
   - 10,000-49,999
   - 50,000 or more

5. In what country are you currently employed? (Choose from the drop-down menu.)
   Select country employed in [ ] Other (Please specify.)

6. Current field of employment? (Choose from the drop-down menu.)
   Select current field of employment [ ] Other (Please specify.)
ISACA Top Business Issues Impacted by Technology

For each of the business issues below, please indicate its level of importance and/or impact on your organization during the next 12 to 18 months. For those business issues that you rate as “somewhat important” or “very important” you will be asked for additional input on questions that follow.

We realize your time is limited, and we would like to thank you in advance for sharing your views. Your submission must be completed and submitted no later than Wednesday, 21 May 2008.

BUSINESS ISSUES

**Collaborative/Extended Enterprises**
The notion of business ecosystems where value chain components from different enterprises integrate and collaborate seamlessly to deliver enhanced products and/or services to end-customers and other recipients seems to be the ultimate goal for many business leaders. Value delivery through business collaboration and integration will remain a theoretical aspiration for the vast majority of enterprises unless they genuinely, deliberately and responsibly open their frontiers, cultures, mindsets, business models, processes and technology infrastructures.

**Enterprise-Based IT Management and IT Governance**
Considerations for security, shared services, IT resource maximization and governance concerns have contributed to a growing focus on enterprise-based IT management and IT governance. Included are issues surrounding IT strategic alignment with business mission, state and federal regulatory compliance, and adherence to generally accepted security and control practices. However, while there is some increase in recognition of the need for IT governance at the C suite level, progress is still slow. Is the IT governance community missing something?

**IT Value Management**
Business does not always have adequate engagement in IT-related projects from the perspective of maximizing value. This means being able to deliver and demonstrate recognized business value including alignment, innovation and affordability. Doing so will help the corporation achieve its goals while adding value and balancing risk versus return over IT and its enablement of change. Of importance here is managing and monitoring the business value of IT-enabled change, i.e., how to optimize the portfolio of technology investments to maximize returns.

**Regulatory Compliance**
Companies are faced with more challenges now than ever; they must grow and maximize market opportunities while at the same time stay in compliance with ever increasing regulations and standards. Keeping on top of legislative and regulatory requirements is a huge burden and regulatory compliance still operates in “project” mode and has not yet been embedded in business processes. IT must design and maintain systems to comply with these legislative and regulatory requirements despite the lack of an integrated framework for regulatory compliance.
BUSINESS ISSUES

Modernization and Consolidation
Replacing legacy applications and infrastructure while consolidating services, operations and resources is difficult to accomplish while reducing IT complexity and facing increasing storage demands and mobile device management. The costs associated with complexity, as well as the risks are pushing management towards focusing on this area.

Inventory/Asset Tracking RFID
Inadequate global RFID standards and solutions are available to support RFID usage in critical applications across locations in different countries. Issues include traceability and cryptographic controls that ensure data privacy by preventing interception and protection against cloning of RFID tags.

Vulnerability Management
With the growth of Internet and other communication methods, managing the threats of unauthorized access and data leakage is becoming a priority for almost all companies. Vulnerability management tools that help prevent and detect unauthorized access are essential in ensuring privacy, confidentiality, data integrity and availability.

Business Intelligence
Executives widely acknowledge the value of business intelligence (BI), but report problems with inconsistent or poor quality data and an ad hoc approach to installing BI systems. Organization's performance would improve if BI data were disseminated to employees other than senior and middle managers, and others report that workers often make poor decisions because of inadequate data. Other problems include BI tools confined to individual departments or groups, too many BI platforms and incompatible systems.

Business and Social Networks
Allowing such networks to be used within a corporate computing environment can present serious risks to personal privacy and corporate confidentiality but can help marketing and improve employee productivity so an appropriate balance of control and usability must be achieved.

Electronic Records Management
Rapidly changing regulations, poor management support and privacy issues are all slowing the progress of managing electronic records and limiting the amount of benefit obtained in supporting knowledge management, collaboration and overall data retention.

Process Control Security
Process control systems and networks help manage the critical infrastructure that we all depend on to live; including power, oil and gas, pipelines, and telecommunications. Historically, process control systems and networks used proprietary communication methods, but more recently these systems have adopted open communication standards such as the Internet Protocol (IP). While this has improved the interoperability of systems, it has also exposed our critical infrastructure to a new world of threats and vulnerabilities.
Transitional or e-Government
There have been management issues related to service integration, Internet governance and financial considerations, such as the cost of implementation/effect on existing budgets, effect on government procurement, and funding. In addition, legal implications including freedom of information and privacy (e.g., UK Data Protection Act) have caused security concerns.

BUSINESS ISSUES

Security Convergence
Security risks and incidents cross organizational lines for the management of risk. When incidents occur expertise contained within the IT department, in information security, and in traditional security organizations need to be brought together in a coordinated response. Identifying risk and developing approaches to managing risk requires coordinate between departments that have traditionally been isolated within siloed infrastructures.

Compliance with Payment Card Industry Data Security Standards (PCI DSS)
Theft and exploitation of credit card information is becoming a regular occurrence and the threat is no longer isolated to casual criminals – organized crime have made this a focus area. In response, the payment card industry has implemented security standards for any organization that processes, stores or transmits credit card information. The purpose of these standards is to enhance the protection of credit card information and reduce the likelihood of theft. The PCI DSS is comprised of six (6) main objectives which are comprised of several controls per objective.

Compliance with Financial Reporting Standards
Global financial reporting standards, such as the Sarbanes-Oxley act have been in place since 2004, however they continue to be an area of focus for IS departments. While improvements have been made to the standards that help focus efforts on areas of higher risk, organizations continue to experience challenges in complying in a cost effective manner.

Challenges of Managing IT Risks
The majority of businesses do not understand that they are also in the business of managing their risks, from the boardroom to the network. IT’s pervasiveness and ubiquity also bring about (sometimes inconspicuously) significant risks that, if realized, might jeopardize the viability and success of the organization. Unfortunately, IT risk variables often interact in complex and subtle ways, making IT risk management a very difficult endeavor.

BUSINESS ISSUES

Disaster Recovery/Business Continuity
All business activity is subject to disruptions, such as technology failure, flooding, utility disruption and terrorism. Business continuity management (BCM) proactively improves the organization’s resilience against operational disruptions and provides the capability to adequately react to these. Notwithstanding the benefits, BCM still remains an elusive goal for most organizations.
### Continuous Process Improvement and Business Agility
Modern enterprises now recognize that “business processes are the business” and that enterprise success is dependant on establishing the capabilities and infrastructures to continually improve business processes and rapidly implement change. This might prove very difficult and complex unless organizations foster business process-centric cultures, start thinking in terms of “processing business processes” (i.e., business process lifecycle automation) and rethink/revamp their application software engineering practices and infrastructures. The promised land is now named Business Process Management (BPM) and Services Oriented Architecture (SOA), but is fraught with challenges.

### Information Security Management
After many spectacular breaches and losses, and enormous spending in "state of the art" security technologies, enterprises are finally realizing that information security is all about being able to manage it adequately. Corporations do not need to reinvent the wheel and can expedite efforts through the adoption of international information security management standards such as ISO/IEC 27001.

### BUSINESS ISSUES

<table>
<thead>
<tr>
<th>Contrasted Services</th>
<th>Not at All Important</th>
<th>Not Very Important</th>
<th>Somewhat Important</th>
<th>Very Important</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Not at All Important</th>
<th>Not Very Important</th>
<th>Somewhat Important</th>
<th>Very Important</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Other

Other

Other
Listed below are those business issues that you rated as "somewhat important" or "very important." Please select and rank only the top five of relative importance and/or impact on your organization. If you have less than five, please rank only those on the list.

If you have erroneously selected a column you intended to have no ranking for, please press the Reset button below to reset this form and start over.

<table>
<thead>
<tr>
<th>BUSINESS ISSUES</th>
<th>First Most Important</th>
<th>Second Most Important</th>
<th>Third Most Important</th>
<th>Fourth Most Important</th>
<th>Fifth Most Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collaborative/Extended Enterprises</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise-Based IT Management and IT Governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Value Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modernization and Consolidation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inventory/Asset Tracking RFID</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Intelligence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business and Social Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Records Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Control Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transitional or e-Government</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Convergence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance with Payment Card Industry Data Security Standards (PCI DSS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance with Financial Reporting Standards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Challenges of Managing IT Risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster Recovery/Business Continuity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continuous Process Improvement and Business Agility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contracted Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© ISACA and Industry Insights, Inc.
If you are experiencing technical issues, please contact ISACA@industryinsights.com
Further Analysis of Top Business Issues

Listed below are the business issues that you rated as the top 5 (or less) business issues affecting your organization in the next 12 to 18 months. For each of these issues, technology based products and/or solutions associated with that business issue are listed. For each business issue, please indicate the level of importance of each of the products and/or solutions in addressing it.

<table>
<thead>
<tr>
<th>BUSINESS ISSUES</th>
<th>Not at All Important</th>
<th>Not Very Important</th>
<th>Neutral</th>
<th>Somewhat Important</th>
<th>Very Important</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Collaborative/Extended Enterprises</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration at the technological level might prove to be too complex and expensive</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Unwillingness to innovate, implement new business models and deal with uncertainty</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>How and where do I find the right business partners?</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Other</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td><strong>Enterprise-Based IT Management and IT Governance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portfolio management tools and better visibility/management of the different categories of IT-enabled investments</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Performance management tools and pursuit of outcomes/benefits of IT-driven change</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Communication and reporting tools and focus on the business value of IT-driven change</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Other</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td><strong>IT Value Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Budgeting tools</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Knowledge management tools</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Communication tools</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Portfolio tools</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Project management tools</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Other</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td><strong>Regulatory Compliance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy of data crossing borders</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Retention of personal information</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Compliance process management</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Category</td>
<td>Options</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forensic IT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continuous compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(transaction/fraud monitoring)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Segregation of duty and privileged access monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Modernization and Consolidation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legacy application modernization and upgrade to ERPs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtualization of servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collaboration platforms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice/Data networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensuring interoperability of infrastructure and data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Inventory/Asset Tracking RFID</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of global standards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Illicit tracking of tags</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Viruses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection against RFID interception</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tag cloning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Vulnerability Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrusion detection and prevention</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security event monitoring (SEM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability scanning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virus management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logging, monitoring and reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Managed security services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Business Intelligence</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data warehouses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital dashboards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online Analytical Processing (OLAP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data reporting or mining software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise information management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Business and Social Networks</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal networking sites</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(MySpace, Facebook)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media networking sites (YouTube)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Real-time networking (chat, messaging)</td>
<td>File networking (file sharing, torrent)</td>
<td>Voice networking (Skype, conference calling)</td>
<td>Other</td>
<td>Electronic Records Management</td>
</tr>
</tbody>
</table>
The cost of protection is increased when responsibility for protection is isolated between different reporting relationships.

Executive management does not have the information required to make risk management decisions.

Other: ____________

**Compliance with Payment Card Industry Data Security Standards (PCI DSS)**

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security program

Other: ____________

**Compliance with Financial Reporting Standards**

- Overall IT control environment (tone at the top)
- Managing access to programs and data
- Managing changes to programs and data
- Managing development or implementation of new systems
- Managing computer operations (job scheduling, interfaces)

Other: ____________

**Challenges of managing IT Risks**

- IT risk illiteracy and lack of awareness
- Lack of senior management commitment to IT risk management
- Risk management processes, if any, do not follow generally accepted principles, practices and standards
- Poor funding and staffing for risk management purposes

Other: ____________

**Disaster Recovery/Business Continuity**

- BCM is not a business-owned and business-driven process
Organizations seldom formalize and enforce a BCM policy

BCM is regarded as a costly planning process and not as one that adds value to the organization

Managers and owners are not fully aware of their responsibility to maintain the ability of the organization to function without disruption

BCM approached as a “one time” initiative and not as a process

Other

**Continuous Process Improvement and Business Agility**

Instilling a business process-centric culture based on continuous improvement

Implementing SOA and exposing application services through standard interfaces might become a “technical nightmare”

BPM perceived as the new euphemism for process reengineering

BPM/SOA technology market needs to consolidate and mature

Lack of business architects capable of orchestrating application services through BPM systems.

Other

**Information Security Management**

Information security is perceived as belonging exclusively to the IT realm

Lack of top management involvement in setting direction and objectives for information security

Information security risks are either not known or are only partially assessed

Lack of enterprise wide information security awareness and training

Performance and effectiveness of information security controls are not regularly measured, monitored or improved

Other

**Contracted Services**

Off-shoring or on-shoring

Managed services

Network security
<table>
<thead>
<tr>
<th>Trojan horses</th>
<th>Trojan horses</th>
<th>Trojan horses</th>
<th>Trojan horses</th>
<th>Trojan horses</th>
<th>Trojan horses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other</td>
<td>Other</td>
<td>Other</td>
<td>Other</td>
<td>Other</td>
<td>Other</td>
</tr>
</tbody>
</table>

**Privacy**

- The cost of protecting sensitive and private information from public access
- The problem of preventing data leakage
- Employee use of company resources for personal use
- Loss of employee productivity due to personal use of company IT resources
- Loss of reputation resulting from security incidents
- Other [ ]

**Other**

[ ]

[ ]

[ ]

[ ]
List of Figures

Figure 1—Survey Sample vs. ISACA Membership by Region .....................................................................................................................7
Figure 2—Country of Current Employment ...................................................................................................................................................8
Figure 3—Current Field of Employment ........................................................................................................................................................8
Figure 4—Primary Job Responsibility ............................................................................................................................................................9
Figure 5—Top Seven Business Issues Overall ..............................................................................................................................................10
Figure 6—Regulatory Compliance Drill-down Importance (All Respondents) ..........................................................................................11
Figure 7—Enterprise-based IT Management Drill-down Importance (All Respondents) ........................................................................11
Figure 8—Information Security Management Drill-down Importance (All Respondents) ........................................................................12
Figure 9—Disaster Recovery/Business Continuity Drill-down Importance (All Respondents) .................................................................12
Figure 10—IT Value Management Drill-down Importance (All Respondents) ...........................................................................................13
Figure 11—Challenges of Managing IT Risk Drill-down Importance (All Respondents) ........................................................................13
Figure 12—Compliance With Financial Reporting Drill-down Importance (All Respondents) .................................................................14
Figure 13—Top Five Business Issues—Audit/Assurance ...........................................................................................................................15
Figure 14—Top Five Business Issues—IT Management .............................................................................................................................16
Figure 15—Top Five Business Issues—IT Security Management...............................................................................................................17
Other Publications

Many publications issued by ISACA and ITGI contain detailed assessment questionnaires and work programs. For further information, please visit www.isaca.org/bookstore or e-mail bookstore@isaca.org.

- Aligning COBIT®, ITIL® and ISO/IEC 17799 for Business Benefit, 2005
- COBIT® 4.1, 2007
- COBIT® Mapping: Mapping of CMM® for Development V1.2 With COBIT® 4.0, 2007
- COBIT® Mapping: Mapping of ITIL With COBIT® 4.0, 2007
- COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0, 2006
- COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0, 2007
- COBIT® Mapping: Mapping of SEI’s CMM for Software With COBIT® 4.0, 2006
- COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0, 2007
- Cybercrime: Incident Response and Digital Forensics, 2005
- Electronic and Digital Signatures: A Global Status Report, 2002
- Enterprise Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment, 2004
- Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0, 2008
- Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0 Extract, 2008
- Enterprise Value: Governance of IT Investments, Getting Started With Value Management, 2008
- Enterprise Value: Governance of IT Investments, The Business Case, 2006
- Enterprise Value: Governance of IT Investments, The ING Case Study, 2006
- Information Security Harmonisation—Classification of Global Guidance, 2005
- IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance, 2007
- IT Governance Domain Practices and Competencies:
  - Information Risks: Whose Business Are They?, 2005
  - Optimising Value Creation From IT Investments, 2005
  - Measuring and Demonstrating the Value of IT, 2005
  - Governance of Outsourcing, 2005
  - IT Alignment: Who Is in Charge?, 2005
- IT Governance Global Status Report—2008
- Linux: Security, Audit and Control Features, 2005
- Managing Enterprise Information Integrity: Security, Control and Audit Issues, 2004
- Oracle® Database Security, Audit and Control Features, 2004
- OS/390—z/OS: Security, Control and Audit Features, 2003
- Security Awareness: Best Practices to Serve Your Enterprise, 2005
- Stepping Through the InfoSec Program, 2007
- Stepping Through the IS Audit, 2nd Edition, 2004