



## 2010 ISACA IT Risk/Reward Barometer—US Edition

March 2010

[www.isaca.org](http://www.isaca.org)

\*n=1,809 unless otherwise indicated

Respondents are US business and IT professionals and are members of ISACA.

### Media Inquiries:

Kristen Kessinger, ISACA, +1.847.660.5512, [news@isaca.org](mailto:news@isaca.org)

Marv Gellman, Ketchum, +1.646.935.3907, [marv.gellman@ketchum.com](mailto:marv.gellman@ketchum.com)

1. Which of the following best describes your enterprise's overall attitude toward IT-related business risk? (n=1,804)
  - a. Risk aggressive (takes large risks to maximize business return) **11%**
  - b. **Risk accepting (takes carefully assessed risks, weighed against anticipated business return, in pursuit of balanced business objectives)** **69%**
  - c. Risk averse (seeks to avoid risks, even at the expense of limited return) **20%**
  
2. How well does your enterprise integrate IT risk management with its overall approach to risk management? (n=1,804)
  - a. Very effectively—Management of IT risks is fully integrated into our business risk management approach. **22%**
  - b. **Somewhat effectively—Management of IT risks is somewhat addressed into our business risk management approach.** **55%**
  - c. Not effectively—Management of IT risks is rarely, if ever, included into our business risk management approach. **15%**
  - d. We do not have a formal approach to business risk management. **8%**

3. When developing new products or business processes, at what point does your organization engage risk management staff or consultants to evaluate risks? (n=1,803)
- |  |            |
|--|------------|
| a. <b>At the beginning of the project</b>  | <b>49%</b> |
| b. In the middle of the project  | <b>21%</b> |
| c. At the end of the project   | <b>9%</b>  |
| d. My organization does not engage risk management staff members or consultants. | <b>22%</b> |
4. Based on continued economic uncertainty in 2010, do you believe your enterprise should initiate IT-related business projects that entail: (n=1,789)
- |  |            |
|--|------------|
| a. <b>Same level of risk as in 2009 (which offers the potential for the same return)</b> | <b>61%</b> |
| b. Higher risk than in 2009 (which offers the potential for a higher return)             | <b>22%</b> |
| c. Lower risk than in 2009 (which offers the potential for a lower return)               | <b>17%</b> |
5. Please rate the amount of resources (time and money) your organization will invest in risk management and compliance in 2010 compared to what was invested in 2009. (n=1,800)
- |                                 |            |
|---------------------------------|------------|
| a. Significantly more           | <b>8%</b>  |
| b. Slightly more                | <b>29%</b> |
| c. <b>About the same amount</b> | <b>50%</b> |
| d. Slightly fewer               | <b>10%</b> |
| e. Significantly fewer          | <b>3%</b>  |
6. Which of the following do you believe about cloud computing (including software as a service)? (Please select one.) (n=1,767)
- |  |            |
|--|------------|
| a. The benefits achieved with cloud computing outweigh the risks.        | <b>17%</b> |
| b. <b>The risks of cloud computing outweigh the benefits.</b>            | <b>45%</b> |
| c. The risks and benefits of cloud computing are appropriately balanced. | <b>38%</b> |
7. Which of the following best describes your organization's 2010 cloud computing plan (including software as a service)? (n=1,799)
- |  |            |
|--|------------|
| a. We plan to limit cloud computing to low-risk, non-mission-critical IT services. | <b>15%</b> |
| b. We plan to use cloud computing for mission-critical IT services.                | <b>10%</b> |
| c. We do not currently plan to use cloud computing for any IT services.            | <b>26%</b> |
| d. We have not finalized our plans with regard to cloud computing at this time.    | <b>18%</b> |
| e. <b>I do not know the details of our cloud computing plan.</b>                   | <b>30%</b> |

8. Of the following, which is the most important driver for your enterprise's IT-related risk management activities? (Please select one.) (n=1,807)
- a. Avoid negative incidents. **18%**
  - b. Manage costs. **16%**
  - c. Ensure that current functionality is aligned with business needs. **21%**
  - d. Support changes in the business. **9%**
  - e. Improve the balance of risk taking with risk avoidance to improve return. **8%**
  - f. **Comply with industry and/or governmental regulations.** **28%**
9. Which one of the following is your enterprise's greatest hurdle when addressing IT-related business risk? (n=1,794)
- a. Not sure how to tailor best practices to the environment **11%**
  - b. Lack of management support **14%**
  - c. **Budget limits** **44%**
  - d. Lack of cooperation across risk management silos **14%**
  - e. Business lines not willing to fully engage in risk management **17%**
10. Of the following, what do you feel is the most important action your enterprise can take to improve IT risk management? (Please select one.) (n=1,802)
- a. Increase risk awareness among employees. **27%**
  - b. Increase the use of best practices. **22%**
  - c. **Improve coordination between IT risk management and overall enterprise risk management.** **30%**
  - d. Provide executive management with a "single view of risk" as opposed to risk silos. **21%**
11. Please rate the following IT-related risk factors as low, medium or high, in terms of the risk they pose to your enterprise.

|   | Low Risk   | Medium Risk | High Risk |
|---|------------|-------------|-----------|
| Employees don't fully understand IT policies                          | 16%        | <b>51%</b>  | 33%       |
| Employees use non-approved software or online services for their work | <b>36%</b> | 33%         | 32%       |

|   |            |            |            |
|---|------------|------------|------------|
| Employees check personal e-mail or visit social networking sites from a work device | 39%        | <b>42%</b> | 20%        |
| Employees use peer-to-peer filesharing with a work device                           | <b>41%</b> | 29%        | 30%        |
| Employees do not protect confidential work data appropriately                       | 16%        | 35%        | <b>50%</b> |
| IT project does not align with business need  | 32%        | <b>43%</b> | 25%        |
| IT project does not provide an appropriate return on investment                     | 31%        | <b>48%</b> | 21%        |
| Investments in IT services are not utilized to their full benefit                   | 21%        | <b>54%</b> | 25%        |

12. In which industry sector do you work? (n=1,804)

|   |            |
|---|------------|
| • <b>Finance/banking/insurance</b>          | <b>28%</b> |
| • Public accounting                         | <b>6%</b>  |
| • Transportation/aerospace                  | <b>2%</b>  |
| • Retail/wholesale/distribution             | <b>4%</b>  |
| • Government/military                       | <b>14%</b> |
| • Technology services/consulting            | <b>12%</b> |
| • Manufacturing/engineering                 | <b>7%</b>  |
| • Telecommunications/communications         | <b>3%</b>  |
| • Mining/construction/petroleum/agriculture | <b>1%</b>  |
| • Utilities                                 | <b>3%</b>  |
| • Legal/law/real estate                     | <b>1%</b>  |
| • Health care/medical/pharmaceutical        | <b>9%</b>  |
| • Advertising/marketing/media               | <b>1%</b>  |
| • Education/nonprofit                       | <b>5%</b>  |
| • Other                                     | <b>5%</b>  |

13. Which of the following is closest to your job title? (n=1,800)

|                       |            |
|-----------------------|------------|
| • External consultant | <b>12%</b> |
| • Professor/teacher   | <b>1%</b>  |
| • <b>Professional</b> | <b>36%</b> |
| • Manager             | <b>26%</b> |
| • Supervisor          | <b>5%</b>  |

- Director **13%**
- Vice President **5%**
- President/CEO **1%**