2011 ISACA IT Risk/Reward Barometer—US Edition
www.isaca.org
*n=712 unless otherwise indicated

Respondents are US business and IT professionals and are members of ISACA.
Due to rounding, responses may not add up to 100%.

Media Inquiries:
Kristen Kessinger, ISACA, +1.847.660.5512, *news@isaca.org*
Marv Gellman, Ketchum, +1.646.935.3907, *marv.gellman@ketchum.com*

1. How well does your enterprise integrate IT risk management with its overall approach to risk management?
   a. Very effectively—Management of IT risks is fully integrated into our business risk management approach.   23%
   b. **Somewhat effectively—Management of IT risks is somewhat addressed in our business risk management approach.**   **58%**
   c. Not effectively—Management of IT risks is rarely, if ever, included in our business risk management approach.   14%
   d. We do not have a formal approach to business risk management.   5%

2. Which of the following do you believe about cloud computing (including software as a service)? (n=710)
   a. The benefits of cloud computing outweigh the risks.   20%
   b. **The risks of cloud computing outweigh the benefits.**   **41%**
   c. The risks and benefits of cloud computing are appropriately balanced.   39%

3. Which of the following best describes your enterprise's 2011 cloud computing plan (including software as a service)?
   a. **We limit cloud computing to low-risk, non-mission-critical IT services.**   **25%**
   b. We use cloud computing for mission-critical IT services.   14%
   c. We do not currently use cloud computing for any IT services.   21%
   d. We have not finalized our plans with regard to cloud computing at this time.   20%
   e. I do not know the details of our cloud computing plan.   20%

3a. IF C: What is your enterprise's biggest concern about implementing cloud computing? (Please enter your response below.) (n=127)

Frequently cited responses include: less control over data, security concerns, privacy concerns, potential for data leakage, compliance concerns

3b. IF A or B: What was the primary driver behind your enterprise's decision to use cloud computing? (Please enter your response below.) (n=267)

Frequently cited responses include: cost savings, efficiency, ease of use, flexibility

4. Of the following, which is the most important driver for your enterprise's IT-related risk management activities? (n=711)
   a. Avoid negative incidents (e.g., security breaches).   22%
   b. Manage costs.   11%
   c. Ensure that current functionality is aligned with business needs.   18%
   d. Support changes in the business.   7%
   e. Improve the balance of risk-taking with risk-avoidance to improve return on investment.   16%
   f. **Comply with industry and/or governmental regulations.**   **26%**

5. Which one of the following is your enterprise's greatest hurdle when addressing IT-related business risk? (n=707)
   a. Not sure how to tailor best practices to the environment   16%
   b. Lack of management support   13%
   c. **Budget limits**   **37%**
   d. Lack of cooperation across risk management silos   15%
   e. Business lines not willing to fully engage in risk management   19%

6. Of the following, what do you feel is the most important action your enterprise can take to improve IT risk management? (n=702)
   a. **Increase risk awareness among employees**   **31%**
   b. Increase the use of best practices   18%
   c. **Improve coordination between IT risk management and overall enterprise risk management**   **31%**
   d. Provide executive management with a "single view of risk" as opposed to risk silos   21%

7. Which of the following do you believe is the most accurate statement about employees using personal mobile devices for work activities? (n=711)
   a. The benefits outweigh the risks.   27%
   b. **The risks outweigh the benefits.**   **37%**

      c.   The risks and benefits are appropriately balanced.   36%

8. Which of the following mobile devices do you believe represents the greatest risk to your enterprise? (n=711)
   - a. Work-supplied smart phones   7%
   - b. Work-supplied laptops/netbooks   13%
   - c. Work-supplied tablet computers   2%
   - d. Work-supplied broadband cards   1%
   - e. Work-supplied flash drives   10%
   - f. **Any employee-owned mobile device**   **58%**
   - g. None of these pose significant risk.   6%
   - h. Other (please specify)   4%

9. Does your enterprise have a security policy in place for mobile computing?
   - a. **Yes, and it is kept up to date and/or well communicated to staff.**   **49%**
   - b. Yes, but it is in need of updating and/or most staff are not aware of it.   32%
   - c. No, but we are planning to implement one soon.   9%
   - d. No, and there are no plans for one.   4%
   - e. I am unsure.   5%

10. Does your enterprise prohibit employees from installing applications on their mobile devices that are used for work activities? (n=711)
    - a. **Yes**   **46%**
    - b. No   42%
    - c. I am unsure.   12%

11. If your organization allows personal smart devices (e.g., employee-owned smart phones or tablet computers) to connect to its networks and applications, what is its current security stance? (n=710)
    - a. We have a policy and systems to control all features on personal smart devices (including application installation and the ability to wipe all data).   13%
    - b. We have a policy and limited controls (such as encryption, password requirements and remote wipe capabilities).   22%
    - c. We have a policy and controls that allow for encryption, password requirements and management of organizational (non-personal) data on the smart devices.   15%
    - d. We have a policy, but do not control or modify personal smart devices that connect to internal systems.   14%
    - e. We do not have a policy or controls for personal smart devices that connect to internal systems.   10%
    - f. **Not applicable**   **26%**

12. What is the riskiest behavior you are aware of an employee doing with a mobile device that has access to the corporate network? (n=705)

a. Lose the device 27%
b. Disable the lock feature 4%
c. Keep passwords stored in a file or as a contact on the device 7%
d. **Store company data in an unsecured manner** **44%**
e. Access dangerous or risky web sites 8%
f. Leave Bluetooth or WiFi access on and unsecured 7%
g. Other (please specify) 3%

13. Over the next 12 months, you expect your enterprise's staffing requirements related to information security and risk management to: (n=709)

	Increase	Decrease	Remain at current levels
Information security	40%	5%	**55%**
Risk management	34%	5%	**61%**

14. In which industry sector do you work? (n=710)

- **Finance/banking/insurance** **24%**
- Public accounting 6%
- Transportation/aerospace 2%
- Retail/wholesale/distribution 5%
- Government/military 17%
- Technology services/consulting 12%
- Manufacturing/engineering 6%
- Telecommunications/communications 2%
- Mining/construction/petroleum/agriculture 2%
- Utilities 4%
- Legal/law/real estate 0%
- Health care/medical/pharmaceutical 7%
- Advertising/marketing/media 1%
- Education/nonprofit 6%
- Other 7%

15. Which of the following is closest to your job title? (n=703)

- External consultant 11%
- Professor/teacher 1%
- **Professional** **39%**
- Supervisor 5%

- Manager   25%
- Director   13%
- Vice President   7%
- President/CEO   1%

About the 2011 IT Risk/Reward Barometer
The IT Risk/Reward Barometer is based on March 2011 online polling of 2,765 ISACA members from 62 countries, including 712 members from the US. The study, now in its second year, helps gauge current attitudes and organizational behaviors related to the risks and rewards associated with IT projects and emerging trends. To see the full results, visit *www.isaca.org/risk-reward-barometer*.