In This Issue:

- Report: COBIT Used by High Performance Organizations to Manage IT
- Steps for Incident Response
- Online COBIT Implementation Exam Available
- New Resource Available on XBRL
- Start Preparing for December CISA, CISM Exams With Practice Questions
- Book Review: System Forensics, Investigation, and Response

Report: COBIT Used by High Performance Organizations to Manage IT

The IT Policy Compliance Group, of which ISACA® and ITGI® are members, recently released a new research report, titled “How High Performance Organizations Manage IT,” that offers recommendations about IT to enterprises that are competing with the highest performers in their industry.

Read More

Steps for Incident Response

By Leighton Johnson, CISA, CISM, CIFI, CISSP

With current technological advances occurring at a rapid pace, it has become important to be prepared to respond to various types of computer incidents. The 6 major steps and considerations for preparing for incident response are...

Read More
Online COBIT Implementation Exam Available

The Implementing the Governance of Enterprise IT Using COBIT Online Exam is now available on the ISACA® eLearning Campus. This exam is applicable to IT professionals in all industries and all enterprises.

Read More

New Resource Available on XBRL

ISACA® has added a new white paper, Leveraging XBRL for Value in Organizations, to its library of resources. This white paper, developed jointly with IFAC, provides guidance on deriving value by implementing XBRL and identifies associated risks.

Read More

Start Preparing for December CISA, CISM Exams With Practice Questions

Among the review materials that ISACA offers for the CISA® and CISM® exams are the annually updated practice question databases, which bring practice questions together in an interactive format.

Read More

Book Review: System Forensics, Investigation, and Response

Reviewed by Jeimy J. Cano M., Ph.D., CFC, CFE, CMAS

The authors of System Forensics, Investigation, and Response, John Vacca and K. Rudolph, have written a book that lets us know, firsthand, the basics of incident response and how to advance digital forensic investigations.

Read More
Report: COBIT Used by High Performance Organizations to Manage IT

The IT Policy Compliance Group, of which ISACA® and the IT Governance Institute® (ITGI®) are members, recently released a new research report that offers recommendations about IT to enterprises that are competing with the highest performers in their industry. “How High Performance Organizations Manage IT” reveals the secrets that high-performance enterprises use to gain customers, retain customers, and reduce their capital and operating expenses, while minimizing business risk related to the use of IT.

ISACA was a resource for the report and COBIT® was cited as a value and risk framework that the best performers use to update changing conditions to their IT framework scorecards for value creation and risk management for different stakeholders in the enterprise.

Additionally, hundreds of interviews were conducted and findings from benchmarks covering more than 4,500 organizations were used to develop the report, which indicated a direct relationship between outcomes enterprises experience and how value and risk from IT are being managed. The research reveals that these high-performance enterprises are spending 70 percent more on IT to deliver higher yield and 100 percent more on information security to minimize business risk.

Other results from the research indicate that:
- Customer-focused strategies for financial and competitive advantage in IT are gaining unfair shares of customers, revenues and profits.
- Much higher spend on IT, information security and audit are driving significant market and financial advantages.
- Prioritized risk-reward practices are maximizing business value and minimizing risk.
- Contextual scorecards for different functions and business units are closing the business-IT alignment gap to drive higher value and less risk.

The findings in the report provide insight to any enterprise competing with the high-performance leaders in their industry. The practices of high-performance enterprises can be used by any firm seeking to regain its customers, avoid consolidation and avoid downside business risk related to the use of IT. The report is available as a free download from IT Policy Compliance.
Steps for Incident Response
By Leighton Johnson, CISA, CISM, CIFI, CISSP

With current technological advances occurring at a rapid pace, it has become important to be prepared to respond to various types of computer incidents. The 6 major steps and considerations for preparing for incident response are:

1. **Corporate response strategy**—Has your organizational leadership set up a corporate response strategy? Are leaders ready for working on the Internet? Have leaders addressed the risks and benefits of operating on the Internet?

2. **Corporate policy and procedure development**—What is the acceptable-use policy for users? Is there an Internet user’s guide or training system for the corporate user? Who is responsible for the corporate web site? Who is responsible for the corporate information on the Internet? Who is allowed to talk about the company on the various business forums, blogs, web sites, etc.? What are the parameters for incident response in the company? Who is the designated lead?

3. **Resonder training and development**—Who are the team responders? What are the team member backgrounds? What type of systems can they work on? What are the special training needs for team members in your environment? What operating systems are used? How is the team assembled? When was the response last tested?

4. **User awareness and training**—Who reported the incident? Did the person(s) who reported follow the corporate response mechanism? Did they stop their work immediately on the system? What is the current activity on the system?

5. **Predeployed assets for response**—What applications, network devices and servers are used? Where are these devices deployed in the network? Who is responsible for the logs? Where are the logs kept? Where is the last backup for the system maintained?

6. **Response requirements**—In addition to fixing the problem, always keep in mind the response requirements for reporting incidents. Does the company have to report the event to the authorities or other outside agencies? Look at the full effect of the event when preparing to respond to the incident.

Leighton Johnson, CISA, CISM, CIFI, CISSP, is a senior security consultant for the Information Security & Forensics Management Team (ISFMT) of Bath, South Carolina, USA.

Editor’s Note: Additional resources on this topic include *Security Incident Management Audit/Assurance Program, Business Model for Information Security (BMIS)* and *COBIT Security Baseline: An Information Security Survival Kit, 2nd Edition.*
Online COBIT Implementation Exam Available

The Implementing the Governance of Enterprise IT Using COBIT Online Exam is now available on the ISACA® eLearning Campus. This exam is applicable to IT professionals in all industries and all enterprises.

The scope of the exam includes the following subjects:

- Positioning IT governance
- Taking the first steps toward IT governance
- Challenges and success factors
- Enabling change
- Implementing a continual improvement life cycle
- Using COBIT®, Val IT: Based on COBIT®, and Risk IT: Based on COBIT® components

Passing the Implementing the Governance of Enterprise IT Using COBIT Online Exam recognizes that the candidate understands the core elements of the implementation of the COBIT framework for supporting governance of enterprise IT (GEIT).

Visit the Online COBIT Foundation Education page of the ISACA web site for more information.

New Resource Available on XBRL

ISACA® has added a new white paper, Leveraging XBRL for Value in Organizations, to its library of resources. This paper, developed jointly with the Professional Accountants in Business Committee of the International Federation of Accountants (IFAC), provides guidance on deriving value by implementing eXtensible Business Reporting Language (XBRL) and identifies associated risks. Understanding how to embed XBRL in information processes helps enhance management communication and assurance, which can increase the value of the information used in an organization. Leveraging XBRL is available as a complimentary PDF on the White Papers page of the ISACA web site.

Learn more about the ongoing ISACA research projects and upcoming deliverables by visiting the Current Projects page of the ISACA web site.
Start Preparing for December CISA, CISM Exams With Practice Questions

Among the review materials that ISACA® offers for the Certified Information Systems Auditor® (CISA®) and Certified Information Security Manager® (CISM®) exams are the annually updated practice question databases, which bring practice questions together in an interactive format. For the December CISA and CISM exams, candidates can prepare with:

- CISA Practice Question Database v11 CD-ROM
- CISA Practice Question Database v11 Download
- CISM Practice Question Database v11 CD-ROM
- CISM Practice Question Database v11 Download
- CISA Practice Question Database v11 CD-ROM Spanish
- CISA Practice Question Database v11 Download Spanish

Past purchasers of the CISA Practice Question Database and CISM Practice Question Database, in either the CD-ROM or download format, have expressed appreciation for the interactive format of the software, citing valuable benefits including:

- The ability to tailor study sessions to help candidates determine what domains should be the focus of their study
- Progress reports and reference reports to help determine performance levels
- Customization of study sessions to the candidate’s liking
- An opportunity for practice with a 200-question, 4-hour simulated exam

All ISACA certification exam preparation resources can be found in the ISACA Bookstore. For more information about and to register for the December exams, visit the Certification page of the ISACA web site.

Book Review: System Forensics, Investigation, and Response
Reviewed by Jeimy J. Cano M., Ph.D., CFC, CFE, CMAS

Talking about computer forensics and digital investigations means talking about how the information security hacker walks among us, hoping that our best models of prevention and reaction fail, leaving lessons we must learn to continue improving our understanding of the discipline of information protection.
Discovering details about information security incidents is a journey through records, logs, interviews, assurance procedures and strategies to find the truth about the facts interwoven with the relationships among technology, individuals and organizational processes. The demanding task of a digital forensic investigation involves recognizing the minds of intruders, their methods, their movements, and the technical and procedural skills of forensic investigators in IT.

In this context, the authors of *System Forensics, Investigation, and Response*, John Vacca and K. Rudolph, have written a book that lets you know, firsthand, the basics of incident response and how to advance digital forensic investigations, as well as essential elements of computer crime, to enable computer forensic researchers who are new to the field to know the key elements needed to deliver consistent results and to be clear when third parties and justice authorities are required.

The book is divided into three parts: fundamentals of forensic systems, techniques and methods; forensic tools; and incident response and future directions. The concepts are presented clearly and pedagogically. A summary and additional resources are provided at the end, and test questions are included to assess your knowledge of the content.

This publication is particularly relevant for professionals in information security, information systems and IT auditing and those thinking of a career in computer forensics. Additionally, it is useful for IT managers who want to update and understand the scope and risks of digital forensic investigations.

*System Forensics, Investigation, and Response* is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in the latest issue of the ISACA Journal, visit the ISACA Bookstore online or e-mail bookstore@isaca.org.

Jeimy J. Cano M., Ph.D., CFC, CFE, CMAS, is chief information security officer for Ecopetrol.