In This Issue:

- Tips for Successful Identity Access Management
- Top 5 Questions to Ask Cloud Providers About Information Risk Management and Security Before Engaging With Them
- Training Week Is Coming to Seattle
- Technical and Risk Management Reference Series Available
- North America CACS 2011—A Successful Delivery of Education, Networking Opportunities

Tips for Successful Identity Access Management

In describing information security management for governments, ISACA® Journal volume 4 author Krishna Raj Kumar, CISA, CISM, provided the following tips for successful identity access management (IAM).

Read More

Top 5 Questions to Ask Cloud Providers About Information Risk Management and Security Before Engaging With Them

By John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP

1. What level of visibility into your cloud environment are you willing to provide to me as a customer?

Read More

Training Week Is Coming to Seattle

Training Week is coming to Seattle, Washington, 8-12 August 2011. Training Week is an
intense, interactive program that offers training on IT audit and assurance, COBIT® strategies and governance of enterprise IT (GEIT). IT professionals attend to maintain, update and upgrade their skills and continue their professional development.

Technical and Risk Management Reference Series Available

ISACA® has developed the Technical and Risk Management Reference series for assurance, risk and security professionals. The series has been created to provide constituents with a security, audit and control focus on some of the most popular ERP systems. The series covers the three primary ERP systems: SAP, Oracle and PeopleSoft.

North America CACS 2011—A Successful Delivery of Education, Networking Opportunities

Nearly 800 participants gathered in Las Vegas, Nevada, this past May for North America CACSSM, a conference packed with information from the opening address to the closing keynote. Mark your calendar for next year’s North America CACS, which will be held 6-10 May 2012 in Orlando, Florida.


Reviewed by Sarathy BSP Emani, CISA, CISM

Empowering Green Initiatives With IT: A Strategy and Implementation Guide, by Carl H. Speshock, serves as a learning guide in integrating organizational green initiatives with green-related IT resources and offerings.
Tips for Successful Identity Access Management

In describing information security management for governments, ISACA® Journal volume 4 author Krishna Raj Kumar, CISA, CISM, provided the following tips for successful identity access management (IAM):

• All accounts should be uniquely identifiable and assigned to an individual.
• All default accounts should be removed and replaced by uniquely identifiable accounts with the same privileges as the default accounts.
• One account-naming convention should be maintained. For example, avoid using “jbrown” for AS/400 access, “joe_brown” for Windows access and “joe.brown” for UNIX access. An SSO system removes this problem.
• Privileged access activity (e.g., root, admin) should be regularly reviewed, and suspicious events should be investigated.
• Orphan accounts, i.e., accounts that belonged to employees who no longer work for the unit/department, should be closely monitored. These accounts should be disabled and removed as soon as the employee has been terminated.
• Exception reports for multiple password failures should be produced and reviewed daily.
• Audits and "clean-ups" of all user databases should be performed regularly.
• Contractors, auditors and remote system support should be granted only temporary access. If further access is required, the approval process should be followed and recorded.
• Adequate storage space and memory should be available for access logs, and all logs should record who, when, where and what for each instance of access.

Read Kumar’s full article, “Information Security Management for Governments," in the current issue of the ISACA Journal, in which you will also find additional coverage of timely and relevant security issues affecting the ISACA® professional communities.

Top 5 Questions to Ask Cloud Providers About Information Risk Management and Security Before Engaging With Them

By John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP

1. What level of visibility into your cloud environment are you willing to provide to
me as a customer? Visibility is one of the key concerns when engaging cloud providers with all flavors of their services. Often, cloud providers are willing to give you visibility into a set of logical containers they establish for you but limit your ability to peer under the hood to see how they design, implement and operate the supporting infrastructure. Unfortunately, this limits your ability to properly assess risk or enable controls to adequately secure your environment, since you can easily be impacted by operational activities or attacks that may be directed at the underlying infrastructure or carried out by an insider within the provider’s organization. If you are running in a private cloud configuration, I suggest requesting the ability to review a read-only mirror feed of all operational and system-management activities associated with the technical infrastructure supporting your services, including server, network and storage elements. You can then use this level of visibility to support a trust-but-verify approach to risk management and security with your provider, which is something that the provider should be able to support in this configuration.

2. **What are your availability guarantees and resiliency capabilities and how do you support them?** Recent outages, such as Amazon’s EC2 multiday outage, have brought to light the fact that many cloud providers do not have robust business resiliency capabilities (e.g., command and control, business continuity, disaster recovery, incident response) in place to effectively address broad-based disruptions to their capabilities and infrastructure. It is important to understand the existence and comprehensiveness of a provider’s capabilities as well as their level of maturity. It is also important to understand the requirements they have for you as a customer to be able to take advantage of these capabilities in advance of a business-impacting incident.

3. **What guarantees of risk management and security are you willing to provide to me as a customer?** Unfortunately, if you look closely at many of the agreements and terms of service that are required for organizations or users to execute to use cloud services, you will find most providers offer little or no guarantee of appropriate risk management and security of either their or your environments. In fact, by default, many cloud providers typically make it the responsibility of the customer to properly protect the capabilities and services they utilize as well as their data. Without enhanced visibility into and control of the underlying information infrastructure that supports the capabilities and services you contract for, it is almost impossible for you as a user to effectively secure your environments and the data included within them. Often, cloud providers will offer you a series of security technologies that you can implement in your environment at your cost to help you enhance your own security, but this still does not solve the challenges associated with underlying information infrastructure, which can adversely impact you as well.
4. **How do you protect yourself and the solutions and services that I purchase from you from denial-of-service attacks?** From a risk management and security perspective, one of the Achilles' heels associated with cloud solutions is the denial-of-service attack. If users are unable to connect to or take advantage of the cloud environments, then they are essentially useless. In the case of cloud infrastructure, this is a bigger concern since an adversary may be attacking the provider or another customer of the provider that has no relationship to your organization, but it still can have a direct impact on you and other customers. Unfortunately, these attacks are relatively easy to carry out and can be very effective, if an adversary is motivated and capable. This has been seen recently by the attacks carried out by the group known as “Anonymous.” There are various ways cloud providers can attempt to defend themselves from these types of attacks, which can include having reserve network capacity available; implementing and operating technology specifically designed to capture and redistribute attack traffic; establishing, testing and maturing incident response procedures specific to this type of attack; and even having reserve data centers available that are connected to alternative networks and mirror your environment and associated data on a regular basis.

5. **How comprehensive and mature is your information risk management and security program and the capabilities it provides to your organization?** Information risk management and security are typically 75 percent people, process and procedure and 25 percent technology. It is important to understand how seriously and comprehensively a cloud provider recognizes this paradigm and also the maturity of its associated capabilities. If the cloud provider’s primary evidence of the comprehensive nature and maturity of its program and capabilities is to identify and demonstrate the technologies that it has in place or the certifications it has earned from third-party organizations, such as the Payment Card Industry (PCI) Security Standards Council or the Cloud Security Alliance (CSA), this could be a warning sign about its level of focus or ongoing support. Unfortunately, technology works only as well as the people, processes and procedures that are used to leverage and support it, and industry certifications tend to set the minimum acceptable level for risk management and security capabilities, not the ideal or appropriate ones. In fact, the use of third-party certifications as proof of capabilities often leads to the use of security-by-compliance as a risk management strategy instead of the operation and support of a properly funded comprehensive information risk management and security program. When evaluating capabilities of cloud providers in this area, ask to review the structure, mechanics and evidence of regular and consistent use of their programs for the services for which you are contracting. This can include a review of their approach and capabilities associated with threat and vulnerability management; integration of risk management and security capabilities in their business and operational
processes; a governance model that supports their program; and metrics and measures they use to monitor the effectiveness of their program and capabilities on a regular basis.

The following publications related to cloud computing are available from ISACA: *IT Control Objectives for Cloud Computing, Audit/Assurance Program: Cloud Computing Management* and *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*. In addition, ISACA offers the Cloud Computing Group in the Knowledge Center and further guidance on the Cloud Computing page of the ISACA web site.

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC.

---

**Training Week Is Coming to Seattle**

Training Week is coming to Seattle, Washington, 8-12 August 2011. Training Week is an intense, interactive program that offers training on IT audit and assurance, COBIT® strategies and governance of enterprise IT (GEIT). IT professionals attend to maintain, update and upgrade their skills and continue their professional development.

This local event provides an intimate learning environment for case study analysis, discussion and networking with IT professionals in various industries. In addition, courses include a combination of lectures, class discussions and group exercises. Up to 38 continuing professional education (CPE) hours can be earned by attending Training Week.

COBIT: Strategies for Implementing IT Governance is one of the courses that will be offered in Seattle. This course discusses how COBIT is used to promote effective alignment of IT with business goals in the management of value delivery and risk mitigation. This comprehensive COBIT training program highlights IT issues, governance concepts, risk management and control. The course uses the most current COBIT and *Val IT™: Based on COBIT®* information, as well as supporting components and related tools to provide guidance in implementing an IT governance process. Two other courses will be offered at Training Week in Seattle: IT Audit and Assurance Practices and Governance of Enterprise IT (GEIT).

To register for and participate in ISACA Training Week, visit the Training Week page of the ISACA web site.
ISACA® has developed the Technical and Risk Management Reference series for assurance, risk and security professionals. The series has been created to provide constituents with a security, audit and control focus on some of the most popular enterprise resource planning (ERP) systems. ERP systems are pervasive globally in medium-to-large enterprises and in the public sector. The series covers the three primary ERP systems: SAP, Oracle and PeopleSoft.

- **Security, Audit and Control Features Oracle Database, 3rd Edition**—The third edition focuses on the attributes and incremental functionality in Oracle relational database management system (RDBMS) software releases 10g and 11g (with focus on 11g). The book covers other “soft” topics that an assessor needs to be familiar with, such as developing a strategy to plan the audit, understanding the IT environment, and reviewing policies and standards.

- **Security, Audit and Control Features PeopleSoft, 2nd Edition**—The second edition updates the human resources and payroll components for PeopleSoft since version 8 and has been written with the business manager as well as the IT and assurance professional in mind.

- **Security, Audit and Control Features SAP ERP, 3rd Edition**—The third edition enables assurance, security and risk professionals (both IT and non-IT) to evaluate risks and controls in existing ERP implementations and facilitates the design and building of better practice controls into system upgrades and enhancements. While many of the features and testing techniques described are also applicable to the earlier versions of SAP R/3, namely 4.6c and 4.7, this publication is designed to be a practical guide based on SAP ECC versions 5.0 and 6.0.

- **Security, Audit and Control Features Oracle E-Business Suite, 3rd Edition**—In response to customer needs and an increased market awareness of governance, risk and compliance (GRC), Oracle Corporation has continued to boost its GRC offerings and released the updated and improved Oracle E-Business Suite (EBS) R12.1 in 2009. The third edition provides an update on current industry standards and identifies future trends in Oracle EBS risk and control.

These and other valuable ISACA resources can be found in the ISACA Bookstore.
North America CACS 2011—A Successful Delivery of Education, Networking Opportunities

Nearly 800 participants gathered in Las Vegas, Nevada, this past May for North America Computer Audit, Control and Security (CACS™), a conference packed with information from the opening address to the closing keynote. The conference opened with a welcome by Las Vegas Mayor Oscar Goodman and continued with a contemporary presentation by Cheryl Shavers, Ph.D., chief executive officer (CEO) of Global Smarts Inc., an advisory services and strategy firm, on the impact of emerging technology.

Seventy-seven concurrent sessions over seven tracks covered topics ranging from IT audit, cloud, the payment card industry, governance and compliance, risk and exposure management, and human factors. Industry leaders from around the world served as presenters for this event. The conference concluded with David Foote’s presentation on people driving technology and the human/IT interaction.

Mark your calendar for next year’s event, which will be held 6-10 May 2012 in Orlando, Florida. Watch the North America CACS 2012 page of the ISACA web site for more information.

ISACA offers a variety of educational opportunities. Learn more about in-person and online events on the Education page of the ISACA web site.

Reviewed by Sarathy BSP Emani, CISA, CISM

The entire world is concerned about global warming, carbon footprints and soaring energy costs. Organizations in business, consumer and government sectors are expected to factor green initiatives into their portfolios. IT, being the backbone of any business, is challenging chief information officers, chief technology officers, IT managers and IT consultants as they look toward lowering energy costs, increasing social responsibility and becoming more eco-friendly.

For those in these roles, Empowering Green Initiatives With IT: A Strategy and Implementation Guide, by Carl H. Speshock, serves as a learning guide in integrating organizational green initiatives with green-related IT resources and offerings, such as business intelligence dashboards and balanced scorecards with green initiative performance metrics.
Early chapters address the internal and external drivers that lead organizations to pursue green initiatives and the mutual benefits derived by aligning IT with green initiatives.

The book goes on to provide strategy mapping and strategy framework components, emphasizing that green initiatives must be aligned with strategic goals. Building on this, it provides guidance on planning concepts and processes. The Planning Stage Overview chapter gives insight into the relationship among IT departments, the environmental management system (EMS) and organizational strategic goals. EMS is broadly termed as a set of management tools and principles to integrate environmental concerns into daily business practices. The chapter titled Planning Stage Process Flow highlights the contribution of IT departments at various stages. Later, the book provides planning-stage tips to address different levels of complexity within the processes.

As the book moves into the implementation of a green initiative with IT, it depicts the IT department as a contributor and participant. The implementation-stage tips section has comments and strong recommendations, too.

Finally, the book covers how to assess an organization’s green initiatives with the aid of IT, depicting an IT department’s integration during the assessment stage and emphasizing that the IT tools and offerings that relate to surveying, tracking, auditing and reporting are of great value. Overall, this book addresses current and potential green initiatives and integration of IT at different stages, both at general and specific levels and as a contributor and participant.

_Empowering Green Initiatives With IT: A Strategy and Implementation Guide_ 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 or e-mail bookstore@isaca.org.

Sarathy BSP Emani, CISA, CISM, has more than 25 years of experience and is the proprietor of MEQPRIMA Advisory Services, an organization doing research in software process and quality improvement. He is a member of the ISACA Publications Subcommittee.