

## Risks and Controls in Cloud Computing

In Depth Seminars – T2

<p><b>Session I</b></p>	<p><b>Chad Woolf</b> Compliance Leader, Amazon Web Services</p> <p><b>Scott Gregory</b> Information Security Compliance Leader, Amazon Web Services</p>
<p><b>Session II</b></p>	<p><b>Robert Fly</b> Head of Product Security, salesforce.com</p> <p><b>Crispen Maung</b> Sr. Director of Technology Audit and Compliance, salesforce.com</p>
<p><b>Session III</b></p>	<p><b>Davi Ottenheimer</b> President, flyingpenguin</p>
<p><b>Session IV</b></p>	<p><b>Robert Zigweid</b> Principal Security Consultant, IO Active</p>

### Session Abstract

Do you want to know where data resides in the cloud? How data is protected and secured in the cloud? Who has access to your data? What happens when your cloud provider dissolves? Is there a disaster recovery plan. Find the answers to these questions and the latest risks, controls and audit guidelines in the Cloud Computing environment in a one day track that will be presented by leading cloud providers and control experts. Each presentation is interactive and will include a Q&A session. You will find yourself confident about your understanding of the risks and controls in Cloud Computing after this daylong session.

### Target Audience

- IT Security Officers
- IT Managers
- Management Systems Managers
- Chief Security Officers
- Information Security Consultants

- Professionals involved in cloud computing services

## COBIT Objectives

## Speaker Bio

### **Chad Woolf**

Chad leads the external and internal compliance program at Amazon Web Services. His efforts focus on enabling enterprise and government adoption of cloud computing by providing certifications and attestation reports required to integrate AWS into customers' risk and control frameworks. Chad's program includes the management of a suite of policies and controls applicable to a wide variety of control frameworks and the monitoring of control performance and effectiveness. He also focuses on working with AWS services to create tools for managing compliance in the AWS cloud. He supports the sales efforts of AWS and regularly interacts with customers' risk, compliance, and audit team members and their auditors. The scope of Chad's program includes an extensive SAS 70 Type II report, ISO 27001 certification, PCI compliance program, FISMA compliance program, and the annual Sarbanes-Oxley audit of Amazon's financial statements relevant to AWS.

Prior to joining AWS, Chad was a Senior Manager with Ernst & Young, a global accounting and consulting firm. In his 12 years with E&Y, Chad advised several Fortune 100 companies in a wide range of IT process improvement programs and was a recognized leader in IT server and ERP configuration and security practices. Today, Ernst & Young's globally-practiced security configuration assessment and technical audit methodology is based on Chad's work and leadership in this area.

Chad is a Certified Public Accountant (CPA), a Certified Information Systems Security Professional (CISSP), and a certified Project Management Professional (PMP). He holds a Master's degree in Accounting & Information Systems and a Bachelor's degree in Accounting

### **Scott Gregory**

Scott leads the Information Security Compliance and Security Intelligence program at Amazon. His primary responsibility is to globally manage information security risk and compliance throughout Amazon. The scope of Scott's program includes oversight of the PCI compliance program, Graham Leach Bliley (GLBA) program and Sarbanes-Oxley from an information security perspective. The scope also includes the active management of all information security risks and mitigations throughout the company. Before joining the Amazon Information Security team, Scott worked in the Internal IT Audit team. In that role Scott performed technical and compliance audits across all Amazon organizational units.

Prior to joining Amazon, Scott was a Vice President as an IT Audit Senior Manager with Washington Mutual, a financial institution, for 3 years. Scott led a team of technical auditors who conducted IT audits of the technology infrastructure and retail bank systems. Scott also worked in several external and internal IT Audit roles within the Washington State government and performed technical audits and forensic investigations. Scott also served four years in the United State Marine Corps.

Currently Scott holds both the Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA) credentials.

### **Robert Fly**

Robert Fly heads up the Product Security team at salesforce.com. Among other things, his team drives the security development life cycle effort, which helps assure the utmost attention is paid to keeping customers' data secure. Before joining salesforce.com, Robert spent eight years at Microsoft, most recently leading the software security team of what is now known as Microsoft Business Online Services. Prior to this, he spent time on the Office Security team, helping secure such products as Outlook and SharePoint. He is a co-author of the book Open Source Fuzzing, a founding member of the Cloud Security Alliance, a CISSP, and has several patents and patents pending in the areas of security and testing of software.

### **Crispen Maung**

Crispen Maung is the Sr. Director of Technology Audit and Compliance at Salesforce.com. Crispen is responsible for the salesforce.com global technology compliance strategy and maintaining all Salesforce.com security/compliance based certifications such as ISO 27001-2005, NiST 800-53, SAS70 type II, SOX, Japan privacy certification, SysTrust and PCI certification.

Crispen is a compliance executive with over 15 years of experience who has designed and implemented sustainable, value adding governance frameworks that meet legal and regulatory requirements within technology based companies such as Oracle, Apple and Excel Partnership.

Crispen holds a MBA degree from Nottingham University, England and a Bachelors Degree in Engineering Technology from DeMontford University Leicester, England. He is also a Certified Six Sigma Master Black Belt, IRCA Registered Lead Auditor, ISO 27001 Lead Auditor and holds the ITIL Foundation Certification.

### **Davi Ottenheimer**

Davi Ottenheimer has over seventeen years experience managing global security operations and assessments, including a decade of leading incident response and digital forensics. He is an expert in compliance, a qualified PCI DSS and PA-DSS assessor with K3DES, and former Board Member for the Payment Card Industry Security Alliance and the Silicon Valley chapters of ISACA and OWASP. Davi received his postgraduate academic Master of Science degree in International History from the London School of Economics.

He is an award-winning public speaker and has been quoted or written articles on security, risk management and compliance for publications including Bank Info Security, Network World, Red Herring, Chain Store Age and SC Magazine. He was formerly responsible for security at Barclays Global Investors (BGI), the world's largest investment fund manager (now BlackRock). Prior to BGI he was a "dedicated paranoid" at Yahoo! and responsible for managing security for hundreds of millions of mobile, broadband and digital home products. He has helped secure industry-leading organizations including Brady Corporation, Cisco, Cypress Semiconductor, Department of Defense University

Affiliated Research Center, IBM, Intel, M&I Data Services, Puget Sound Energy, State Farm, University of California Santa Cruz, University of Iowa Hospitals and Clinics, VMware and West Marine.

### **Robert Zigweid**

Robert Zigweid is an accomplished developer and application tester with advanced skills in the creation and analysis of systems architecture and threat modeling. As a Principal Compliance Consultant at IOActive, he works with clients to discover and solve network and application problems that threaten their business goals and assets. In addition to his direct efforts on penetration tests, security reviews, and network and application audits, Zigweid contributes to the advancement of more stable, secure systems through his research and development. He was a co-founder of OSJava, is working on a JDBC driver and more robust Java class loader, and has conducted groundbreaking research that will further the formal understanding of application and network security for audiences at varying levels of technical fluency.