cloud security alliance℠

Cloud Security Alliance

Security Guidance for Critical Areas of Focus in Cloud Computing

April 27, 2009

Agenda

- About the Cloud Security Alliance
- Guidance 1.0
- Call to Action

Copyright © 2009 Cloud Security Alliance

About the Cloud Security Alliance

- Not-for-profit organization
- Inclusive membership, supporting broad spectrum of subject matter expertise
- Strong voice for the security practitioner
- We believe in Cloud Computing, we want to make it better
  - *"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."*

Copyright © 2009 Cloud Security Alliance

Contributors

Editor

Jim Reavis, Cloud Security Alliance

Industry Advisors

Jerry Archer, Intuit

Alan Boehme, ING

Larry Brock, DuPont

Dave Cullinane, eBay

Paul Kurtz, Good Harbor Consulting

Izak Mutlu, Salesforce.com

Nils Puhlmann, Qualys

Lynne Terwoerds, Barclays

Primary Authors

Jeff Bardin, Treadstone 71

Jon Callas, PGP

Shawn Chaput, Privity

Pam Fusco, UAT

Francoise Gilbert, IT Law Group

Christofer Hoff, Rational Survivability

Dennis Hurst, HP

Subra Kumaraswamy, Sun

Liam Lynch, eBay

Scott Matsumoto, Cigital

Brian O'Higgins, Third Brigade

Jean Pawluk, Visa

George Reese, enStratus

Jeff Reich, FUDless

Jeffrey Ritter, Waters Edge Consulting

Jeff Spivey, RiskIQ

John Viega, McAfee

Phil Agcaoili, Dell

Todd Barbee, New Dominion Bank

Girish Bhat, SAVVIS

Glenn Brunette, Sun

Jake Brunetto, Intuit

Sean Catlett, Barclays

Anton Chuvakin, Qualys

Joshua Davis, Qualcomm

Dr Ken Fauth, CPP

Jeff Forristal, Zscaler

Robert Fly, Salesforce.com

Edward Haletky, AstroArch Consulting

Jim Hietala, The Open Group

Michael Johnson, Security GRC2

Shail Khiyara, Cloud Computing

Mark Leary, Northrop Grumman

Tim Mather, RSA Security

Dave Morrow, Secure Business Operations

Josh Pennell, IOActive

Ben Rothke, BT

Stephen Sengam, Fox/Newscorp

Ward Spangenberg, IOActive

Michael Sutton, Zscaler

Dave Tyson, eBay

Dov Yoran, MetroSITE Group

Josh Zachry, Rackspace

Peter M. Mell, NIST

CSA cloud security alliance℠

Copyright © 2009 Cloud Security Alliance

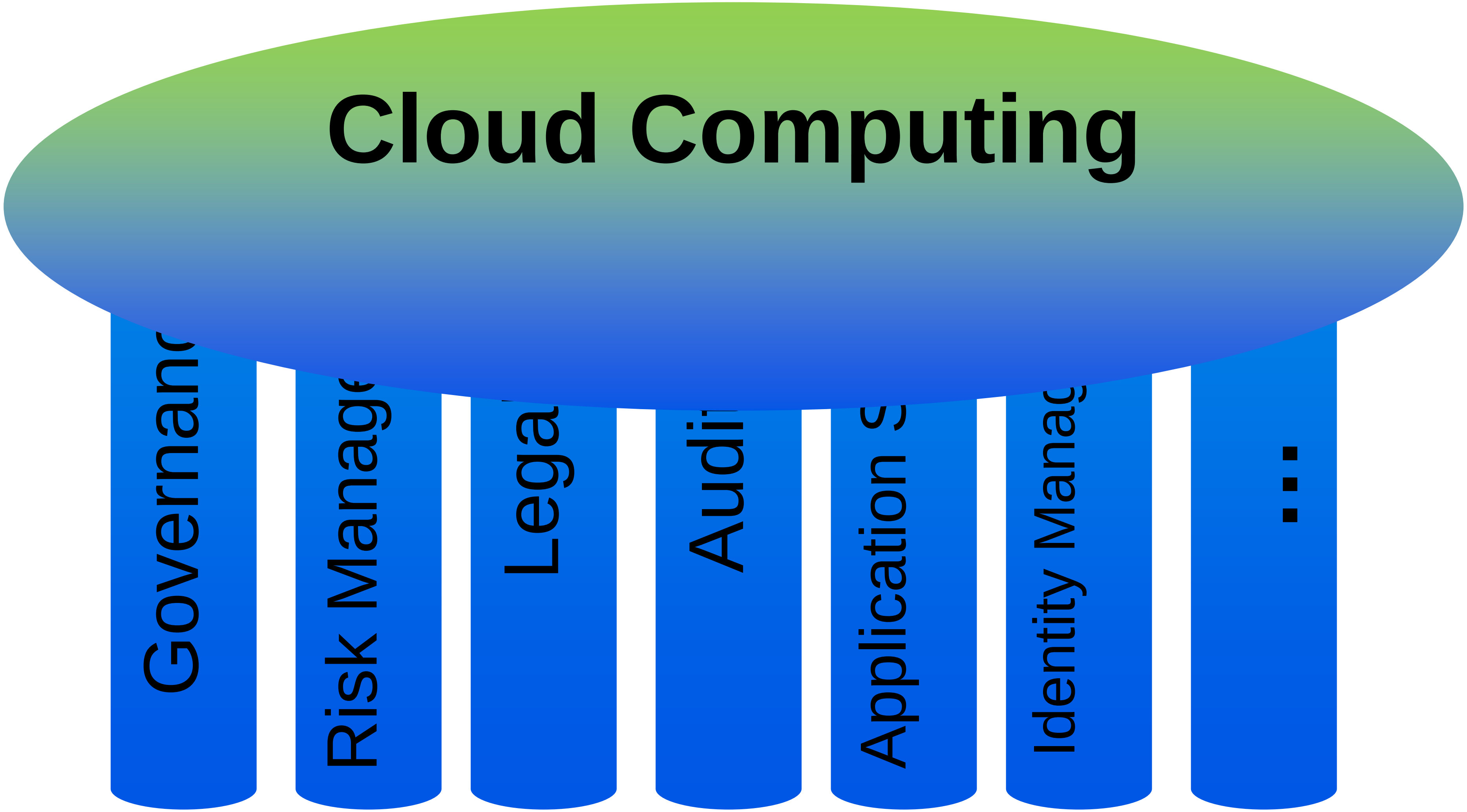
www.cloudsecurityalliance.org

Getting Involved

- Individual Membership (free)
  - Subject matter experts for research
  - Interested in learning about the topic
  - Administrative & organizational help
- Corporate Sponsorship
  - Help fund outreach, events, research
- Affiliated Organizations (free)
  - Joint projects in the community interest
- Contact information on website

Copyright © 2009 Cloud Security Alliance

Focus



Copyright © 2009 Cloud Security Alliance

Security Guidance for Critical Areas of Focus in Cloud Computing

Download at:

www.cloudsecurityalliance.org/guidance

Overview of Guidance

1. Architecture & Framework

Governing in the Cloud

2. Governance & Risk Mgt
3. Legal
4. Electronic Discovery
5. Compliance & Audit
6. Information Lifecycle Mgt
7. Portability & Interoperability

Operating in the Cloud

8. Traditional, BCM, DR
9. Data Center Operations
10. Incident Response
11. Application Security
12. Encryption & Key Mgt
13. Identity & Access Mgt
14. Storage
15. Virtualization

Copyright © 2009 Cloud Security Alliance

Assumptions & Objectives

- Selected domains based on both strategic and tactical pain points
- Broad “security program” view of the problem
- Primary audience is the cloud customer’s security practitioner
- Focused on differences caused by cloud models

Copyright © 2009 Cloud Security Alliance

Domain: Architecture

- Not possible to adequately summarize here
- But critical to understanding risks & mitigation
- 5 principal characteristics (abstraction, sharing, SOA, elasticity, consumption/allocation)
- 3 delivery models
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)
- 4 deployment models: Public, Private, Managed, Hybrid

Copyright © 2009 Cloud Security Alliance

Domains

- Governance & ERM
  - Invest cost savings/ 3rd Party transparency/ Financial viability
- Legal
  - Provider – Customer reg conflicts/ secondary uses of data/ Cross border data/ term relationship
- Electronic Discovery
  - Authentic data preservation/ roles & responsibilities

Copyright © 2009 Cloud Security Alliance

Domains

- Compliance & Audit
  - Audit on demand/ privacy impact assessment/ certification scoping
- Information Lifecycle Mgt
  - Breach cost recovery/ data destruction/ classify data
- Portability & Interoperability
  - Abstraction layers/ PaaS loose coupling/ open standards/ competitors

Copyright © 2009 Cloud Security Alliance

Domains

- Traditional, BCM/DR
  - Provider insider threat & job compartmentalization/ onsite inspection/ infrastructure
- Data Center Operations
  - System & data compartmentalization/ patch mgt/ resource sharing framework/ Failover
- Incident Response
  - Limit scope of incident through encryption/ application layer monitoring/ app registry

Domains

- Application Security
  - Trust boundaries for SDLC/ Trusted VM image/ Secure inter-host channels/ “DMZ” hardening
- Encryption & Key Mgt
  - Separation of cloud provider encryption & key mgt/ standards in contract language/ App developers
- Identity & Access Mgt
  - Federated strategy & arch & standards/ Strong auth & pw policies exceed internal standards/ Identity service providers

Copyright © 2009 Cloud Security Alliance

Domains

- Storage
  - Trust boundaries/ storage retirement/ seizure/ long term archiving/ multi-tenant encryption & key mgt
- Virtualization
  - 3rd party protection, hardening guidelines, provisioning/ traffic across VM backplane/ admin access

Copyright © 2009 Cloud Security Alliance

Summary

- Cloud Computing is real and transformational
- Cloud Computing can and will be secured
- Broad governance approach needed
- Tactical fixes needed
- Combination of updating existing best practices and creating completely new best practices
- Common sense not optional

Copyright © 2009 Cloud Security Alliance

Call to Action

- Shared responsibility with users, providers, associations, governments
- Seek to improve our guidance
- Seek to improve our domains of knowledge
- Partner to accomplish all of above

Next Steps

- Hold regional CSA Meetups in conjunction with other associations
- Participate in discussions & announcements on LinkedIn
- CSA organizing global meetup for Version 2.0 of Guidance first week of June
- Other research initiatives and events being planned

Copyright © 2009 Cloud Security Alliance

Thank You!

cloud security alliance

www.cloudsecurityalliance.org