Cloud Computing and the Regulatory Compliance Labyrinth
About ERM

mission

To protect individuals, organizations and society through comprehensive risk management.

vision

Worldwide leader and trusted advisor in Enterprise Risk Management.

values

Ethics. Do the right thing.
Trust. Provide transparency and protection.
Excellence. Provide the highest quality.
Service. Help clients, employees and society.
Can-Do Attitude. Face and overcome challenges.
Passion. Love what we do.
About The Speaker

Nick Shuman –

- Information Security Consultant

- Bachelor of Science in Computer Science and Psychology - University of Miami

Core Experience:
- Regulatory Compliance and Standards
- Risk and Vulnerability Management
- Technical Security Assessment
- Ethical Hacking
The Cloud

- What is “The Cloud”?  
  - Foggy about the Cloud

- Public, Private, and Hybrid Clouds  
  - What is the difference?

- Cloud-based services  
  - Software as a service (Saas)  
  - Platform as a service (PaaS)  
  - Infrastructure as a service (IaaS)  
  - Anything as a service (XaaS)
Why the Cloud?

Pros

- Cost Management
- Efficiency
- Time to Market
- Scalability
- Customer Demand
- Technical Resources

Cons

- Information Security
- Data Ownership Responsibilities
- Legal/Contractual Issues
- Performance Standards
- REGULATORY COMPLIANCE
Regulatory Compliance Issues

- Distinction between data owners and data processors
- Lack of knowledge about geographical location of data centers
- Physical controls being replaced by virtual controls
- Non-standard Private and Public Clouds
Questions Regarding Compliance in the Cloud

- Can I remain compliant after moving to the cloud?
  - How do I do that?

- How will I know where my data is?

- Will my cloud provider be forthcoming about potential compliance issues?

- Will my data be more secure in the cloud?
What is PCI DSS?

Set of regulations that are responsible for ensuring that companies are handling users’ credit card data in a secure and responsible manner.

Not all cloud providers are equal

PCI compliant only in certain areas.

PCI DSS Cloud Computing Guidelines
Health Insurance Portability and Accountability Act (HIPAA)

What is HIPAA?
- Strict rules set in place in the healthcare field in order to protect patient privacy
- Pertain to how medical information is collected, handled, protected, used, and disclosed

Compliance is a two way street
- Burden falls on you and the cloud computing provider

Where is data being physically stored?

© 2013 Enterprise Risk Management, Inc.
Federal Risk and Authorization Management Program (FedRAMP)

- **What is FedRAMP?**
  - Authorization, not certification
  - NIST-based
  - Standardized requirements

- Needed for any cloud service provider that intends to provide cloud computing services to Federal government agencies

- Contractors to hire third-party assessment organizations that will verify whether they meet the basic security requirements.
Gramm-Leach-Bliley Act (GLBA)

What is GLBA?
- Requires that financial institutions establish appropriate standards for protecting the security and confidentiality of their customers' non-public personal information
- Security and confidentiality of customer records and information
- Protect against any anticipated threats or hazards to the security or integrity
- Protect against unauthorized access which could result in harm or inconvenience to any customer

Financial Privacy Rule
Safeguards Rule
Cloud Compliance Conclusions and Suggestions

- Not sufficient to rely solely on claims of cloud providers
  - Due diligence
  - Thorough discussions with cloud providers

- Make a checklist
  - Enumerate all compliance requirements
  - Who manages/is responsible for which?

- “100% compliant” cloud providers is usually a warning sign

- Compliance DOES NOT EQUAL Security

- Do you fully understand all requirements?

© 2013 Enterprise Risk Management, Inc.
Questions and Inquiries

For further information please contact:

**Nick Shuman**  
*Information Security Consultant*

305-447-6750 (o)  
305-588-5103 (m)  

[nshuman@emrisk.com](mailto:nshuman@emrisk.com)  
[www.emrisk.com](http://www.emrisk.com)
Your go to advisors for all matters in information security.

Upcoming Webinars

June 2013: Business Continuity Planning
July 2013: Information Security for Law Firms

www.emrisk.com