



Information Security Governance  
in the Cloud

**JBW Group-LifeLine Data  
Centers**

**Tuesday, September 22, 2009**

**Patrick F. Sullivan**

Ph.D.  
Principal Consultant

**John B. Weaver**

CISSP, CISA, CISM, CPP  
Principal Consultants

# JBW Group International Inc.

- ❑ **Full Service Information Security Consultancy Founded in 2002, Specializing In**
  - ❑ ISO 27001 Information Security Management System Implementation, audit and training
  - ❑ ISO 20000 Information Technology Service Management implementation, audit and training
  - ❑ ISO 28000 Supply Chain Security Management System implementation, audit, and training
  - ❑ CISSP training
- ❑ **Clients in the United States, Canada, Japan, Mexico and Central America,**
  - ❑ Fortune 50 companies to small businesses; industry experience in
  - ❑ Healthcare, Pharmaceutical, Financial Services, Energy, Telecommunications, Software, BPO Application and Service Hosting
- ❑ **Methodology based on Internationally Recognized Standards**

Find more information at [www.jbwgroup.com](http://www.jbwgroup.com)



# Agenda

- What is Cloud Computing? NIST Working Definition of Cloud Computing
- What are the Concerns? Vulnerability as a Service
- Challenges: “It’s Just Vendor Management” (Right, and a Soufflé is Just Eggs)
  - User Perspective
  - Provider Perspective
- What to Do: Information Security Governance in the Cloud
  - Corporate Governance and the Duty of Due care
  - Objectives of Information Security Governance
  - Reasonable Information Security
  - Note on the Cloud Security Alliance

# Cloud Computing: Draft NIST Definition

## Business Characteristics

- On-Demand Self-Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

# NIST Definition

## Service Models

- Cloud Application as a Service
  - The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- Cloud Platform as a Service
  - The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- Cloud Infrastructure as a Service
  - The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

# NIST Definition

## Deployment Models

- *Private cloud*
  - The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- *Community cloud*
  - The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- *Public cloud*
  - The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- *Hybrid cloud*
  - The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

# Concerns- Vulnerability as a Service?

## General- Gartner's 7 Issues

- Managing privileged user access on the provider end
- Ensuring regulatory compliance on the provider end
- Potential vagueness of data location
- Data segregation in shared environments
- Business Continuity/Disaster Recovery across multiple sites
- Investigative support
- Long-term viability of vendor

# CSA Key Issues

- Compliance (cloud friendly legal framework)
- eDiscovery & Forensics
- Business Continuity (must have)
- Physical Security
- Authentication, IAM in-the-cloud
- Privacy
- Encryption & Key Management
- Data Governance
- Virtualization
- Web Security

*Cloud Computing providers must become information security specialists, or business is at risk*

# Things to Note

- Gartner's list focuses mainly on vendor management and capabilities-
  - Illustrates how cloud business features generate risk (vulnerabilities inherent in the features where threats aren't under direct control of the user)
- Risks generated by business features are amplified by service and deployment models
  - The key takeaway from a security architecture perspective in comparing these models is that the lower down the [application-platform-infrastructure] stack the Cloud service provider stops, the more security capabilities and management the consumer is responsible for implementing and managing themselves (Hoff, CSA Guidance version 1)
- CSA list and advisory statement, while directed largely to vendors, can apply to both users and providers of cloud services

# More Things to Note

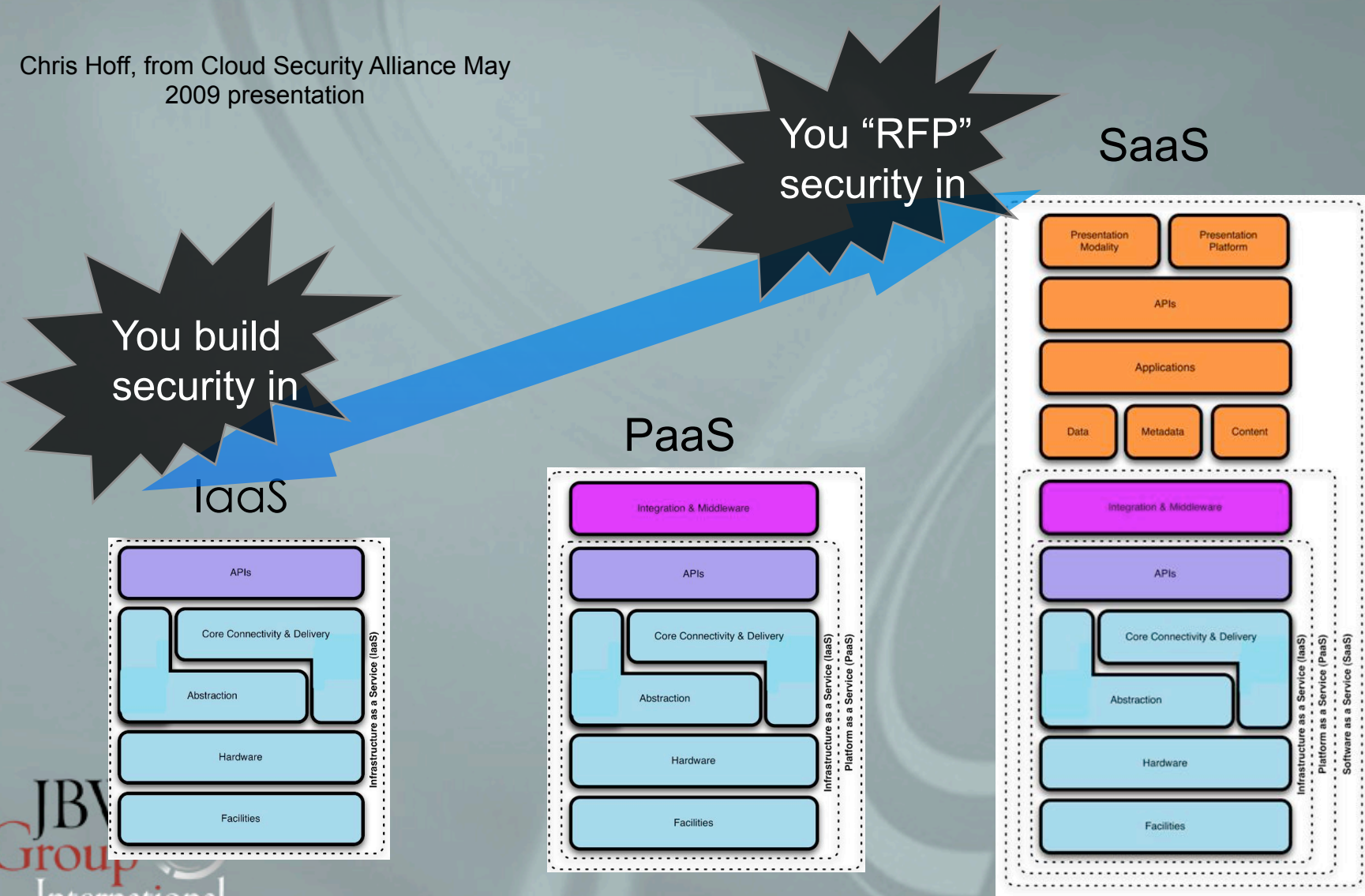
- Vendor management issues...
  - Risk assessment
  - Vendor compliance capabilities
  - Consistency of vendor security capabilities and control environment with yours
  - Ability to monitor and measure effectiveness of vendor's controls
- ...Are amplified by the service and deployment models used
- An organization's management of vendor information security risks is only as good as (the scope and maturity of) its own information security risk management
- *Cloud users must also be security specialists*

# Challenges

- Distributed scope of accountability and responsibility in governance, risk management and compliance:
- ...the notion of a well-demarcated perimeter separating the “outside” from the “inside” is an anachronistic concept...the impact of the re-perimeterization and the erosion of trust boundaries we have seen in the enterprise is amplified and accelerated due to Cloud.
  - Chris Hoff, CSA Guidance version 1, Domain 1, Cloud Architecture

# S-P-I Model

Chris Hoff, from Cloud Security Alliance May 2009 presentation



# Challenges

- The fundamental GRC problem:

*The fundamental issues of governance and enterprise risk management in cloud computing concern the identification and implementation of the appropriate organizational structures and processes required to maintain effective information security governance, risk management and compliance, and to assure **reasonable information security** for both providers and users of cloud computing services in any cloud deployment model within a defined business environment.*

# Emerging Legal Standard

- ❑ Reasonable security is a risk-based, fact-specific process characterized by:
  - ❑ Defined governance structures & processes
  - ❑ Identification, inventory and valuation of information assets
  - ❑ Periodic risk assessment (threats, vulnerabilities, impacts)
  - ❑ Controls appropriate to identified risks and adaptable to changes in the business/technical/threat environments
  - ❑ Management of risks associated with third parties
  - ❑ Training and awareness
  - ❑ Monitoring of controls performance and effectiveness
  - ❑ Appropriate management review of processes, policies and controls
  - ❑ Continual improvement
- ❑ And should be business-driven, scalable, defensible, sustainable



See: "Where We're Headed: New Trends in the Law of Information Security," Thomas J. Smedinghoff, *Privacy and Data Security Law Journal*, January 2007

# GRC Problem- Provider's View

- Reasonable information security for its own operations
- Risk management objectives driven by business need to reliably deliver service while meeting customer's security expectations & requirements
  - Must understand the risk profile of its service and deployment approach with respect to customer's risk and compliance environment
  - Must deliver service in a way that supports the customer's information security risk management objectives that support their business
  - Metrics capable of consistency with customer's metrics for measuring effectiveness of information security (no, not just another SAS 70...)

# GRC Problem- User's View

Yeah, vendor management, but...

- User is not just outsourcing service, but also outsourcing (transferring/distributing) risk
- Utilization of cloud services must be consistent with user's own risk management objectives and risk tolerances
  - Risk assessment can't just focus on vendor controls, but also on risk management relative to user's own information security objectives to protect assets that support its delivery of services or products
  - User must understand the cloud option with respect to its own business and information security risk management strategies and objectives
  - Management must objectively understand and accept the risk

# How to Address the Issues

- The hard way- reasonable information security isn't achieved by fulfilling a compliance requirements checklist. It's a continually improving management process.
- Assurance isn't realistic without well developed information security governance and risk management structures and processes
- Reasonable security in the cloud will be collaboratively constructed in some way (and not just by contracts)

# Information Security Governance

- A subset of corporate governance fiduciary duty of due care.
- Characteristic processes and objectives:
  - An information security risk management methodology
  - A comprehensive security strategy explicitly linked with business and IT objectives
  - An effective security organisational structure
  - A security strategy that talks about the value of information protected—and delivered Security policies that address each aspect of strategy, control and regulation
  - A complete set of security standards for each policy to ensure that procedures and guidelines comply with policy
  - Institutionalised monitoring processes to ensure compliance and provide feedback on effectiveness and mitigation of risk
  - A process to ensure continued evaluation and update of security policies, standards, procedures and risks

# Risk Management

- Information security risk management is (well, should be) a subset of Enterprise Risk Management
  - Ties information security risk management to overall business objectives and strategy
  - Information security risk management will probably cut across all categories of enterprise risk, based on the role of information flow in the related business processes
  - Always related to business analysis and all reporting
  - Information security risk management in the cloud is also an instance of **supply chain** security management

# What is Risk?

## Information Assets

Technology

Customer Data

IP & Trade Secrets

Key Contributors

Threats

“Hackers”  
Malware  
Dishonest  
Employees  
New Services  
Competitors  
Legal & Regulatory  
Requirements

Vulnerabilities

Poorly Managed  
Technology  
Inconsistent  
Policies  
Informal  
Processes

Impact

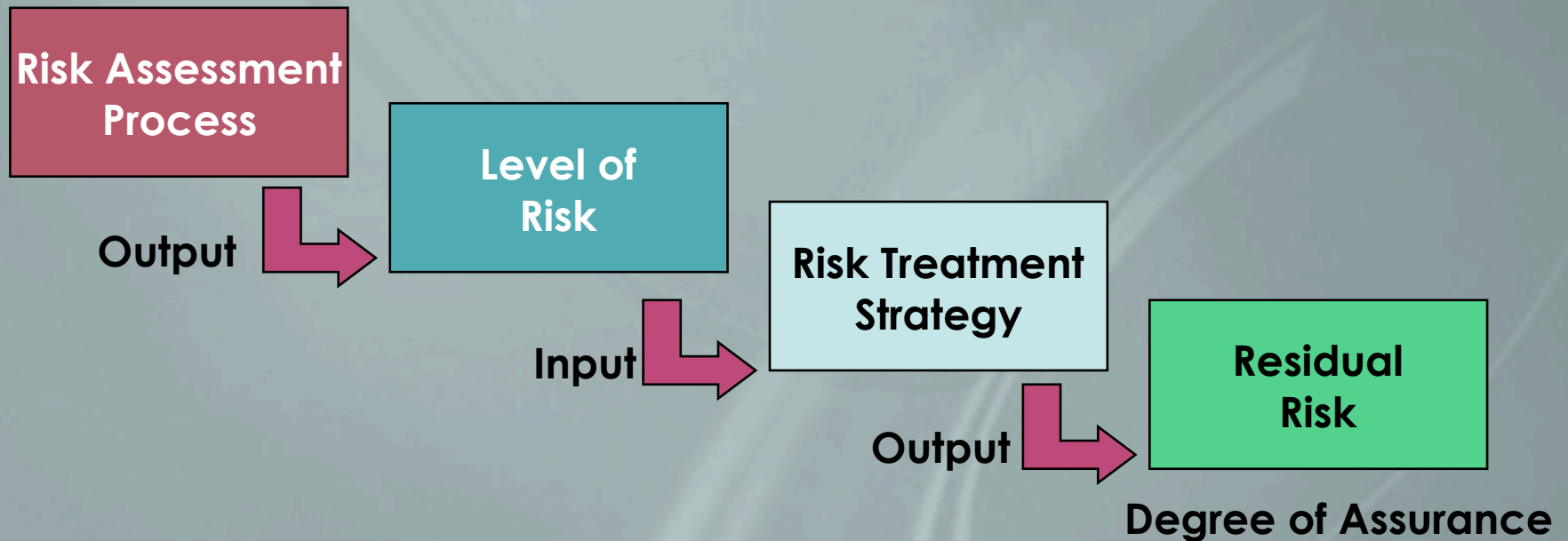
Lost  
Productivity  
Lost  
Market Share  
Brand  
Deterioration  
Penalties  
Litigation  
Jail Time  
(H, M, L)

Likelihood

Daily  
Weekly  
Monthly  
Annually  
(H, M, L)

# Risk Management (View from ISO 27001)

**Key element of ISO 27001 is the Degree of Assurance determined by:**



**Risk = Vulnerabilities + Threats + Probability + Impact**

# What to Look For

- Well-defined information security governance structure and processes in both user and provider
  - Service model may adjust roles and responsibilities (distributed scope of control for user & provider)
  - Deployment model may define accountabilities and expectations (based on risk assessments for user and provider)
- User organizations should include review of specific information security governance structure and processes as part of their due diligence of prospective provider organizations.
- Provider's processes should be assessed for capability maturity as well as presence, and for consistency with the user's information security management processes.

# What to Look For

- The *use* and proposed architecture of cloud services should be subject to risk assessment- not just the vendor
  - Impact of cloud services on user's risk management objectives should be assessed
  - Objectives of cloud use, business features, service & deployment models should be consistent with user's risk management approach and within tolerances (may even support them)

# What to Look For

- Where a provider cannot demonstrate comprehensive and effective information security governance in association with its services, users should carefully evaluate the use of the vendor and the user's own abilities to compensate for the potential risk management gaps.
- Where a (potential) user cannot demonstrate comprehensive and effective information security governance in association with its business objectives and services, it should probably leave the cloud alone.

# What to Look For

- When conducting due diligence on prospective service providers, users should assess the potential vendor not only for the presence of relevant information security controls (i.e., relevant to managing risk per a risk treatment plan for the potential service), but also for the presence and maturity of the elements of reasonable information security
- Users should view cloud services and security as supply chain security issues. This means examining and assessing the provider's supply chain (downstream service providers and, potentially, providers of equipment and other tangibles related to the cloud services), as well as assessing the current state of a prospective provider's security controls. This also means examining the provider's own third party management.

**JBW**  
**Group**  
International  
Information Assurance

A graphic element consisting of three concentric circles with a central dot, rendered in a light gray color, positioned to the right of the company name.

**John B. Weaver**  
CISSP, CISA, CISM, CPP  
President/CEO  
Principal Consultant

**JBW Group International**  
PO Box 19393  
Minneapolis, MN 55419 USA

**+1.877.97.27001**  
[www.JBWGroup.com](http://www.JBWGroup.com)