The significance of security standards in Cloud Computing

V. Rajendran

http://venkrajen.in
venkrajen@yahoo.com

044-22473849: 9444073849

Contents

Cloud Computing – Meaning and significance
Data and Information Security
Pillars of Information Security: C.I.A., NR, Authentication
Handling of data in cloud
OS, other services in cloud
Cloud Security – how different from others
Role of standards in cloud
ISO 27001 – Certification standards
Other ISO standards
Benchmarks, Framework, Best Practices
The road ahead

Definition – Why cloud?

Local PCs need not have the computing resources

No storing of software or applications

Network of computers in the cloud (Internet) handles them

No huge hardware or related infrastructure in the PCs

Enough to have an interface browser

A simplified example of cloud computing:

Yahoo! mail and gmail already used by millions, since users do not have an email program in their systems nor are they storing the mails in their systems.

Simply in cloud..

No responsibility of procuring software licences

No follow-up on the use of resources – payment issues etc

A web-based service in the PCs would suffice

Remote machines owned by others will take care of all services like providing an email application, a word processing application, a spread-sheet or perhaps a database access too.

Pay for the amount used (like water, electricity?)

Cloud service providers: Microsoft, IBM, Amazon, AT & T etc offering cloud services like storage, application, interfaces etc

In the cloud…

Users in cloud may be a

PC user, a Mobile user, an iPad user

Whatever be the user, a web-based utility is kept

Cloud services:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

The cloud client or the user does not store the application software but only operates the same which is installed and maintained at the cloud provider's systems only

Advantages

- Low cost of ownership
- Adoption of high level computing
- Convenience of scalability and sustainability
- Locational independence
- 24 x 7 support (as offered by the cloud provider)
- Pay as per usage

Security concerns

- Vulnerabilities in the front-end affecting the provider ie cloud user impacting the cloud provider
- Cloud provider impacting the cloud user and not ensuring adequate security in the background, database, Access Control, OS and even network equipment

Security concerns of the user

Cloud provider has to ensure:

- Security controls are in place
- Access Privileges, Access Control etc
- Authentication, Authorization mechanisms
- Asset Classification, BC-DRP initiatives
- Compliance with regulatory procedures etc

ISO Standards

- Distributed application platform and services DPAS
- ISO 29361 Web Services Interoperability
- ISO 29362 and 29363 standards
- General standards
- ISO 90003 – Software standards
- ISO 27001 - Certification

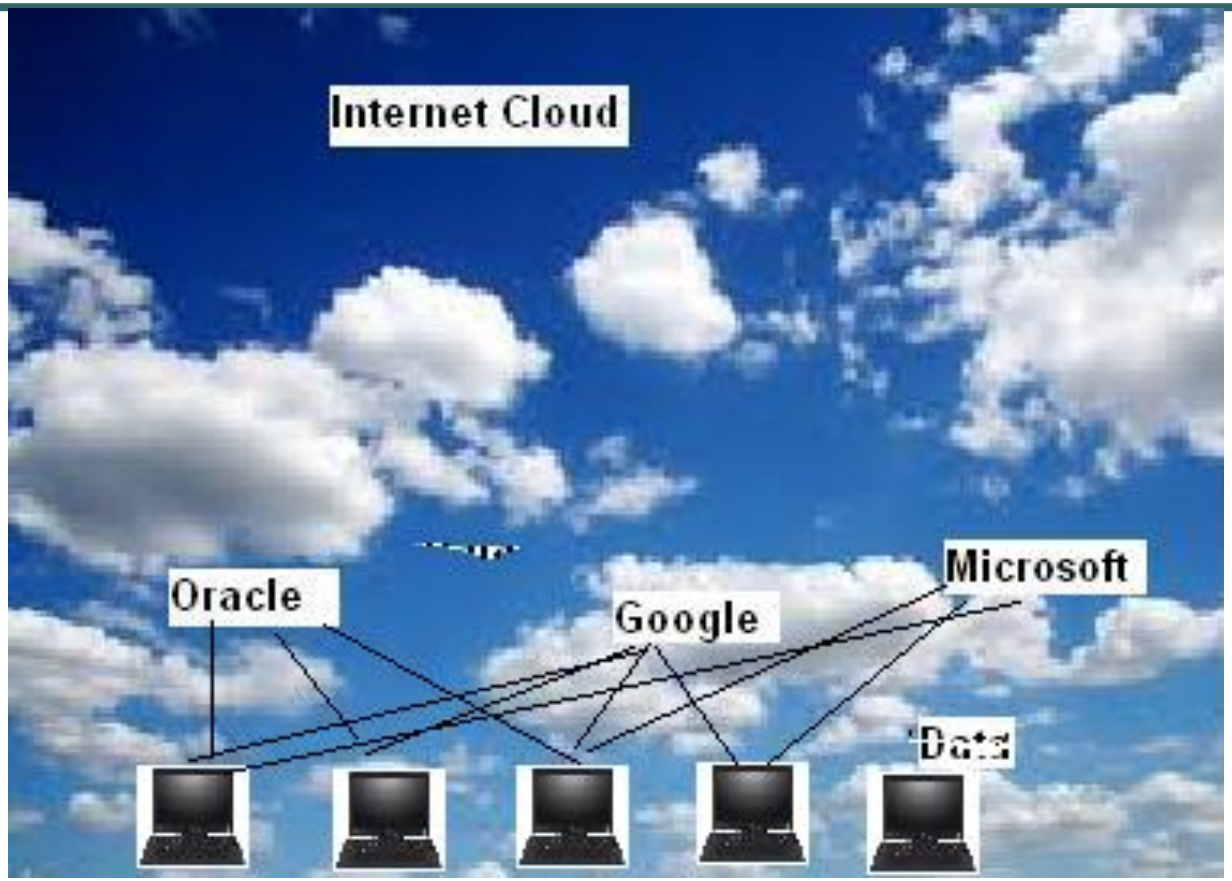
ISO 29361 to 29363

- **SOAP: Simple Object Access – for exchanging structured information in the implementation of web services**
- Uses XML for message format and other application layer protocols like HTTP, SMTP etc
- Considered to be protocol stack for web services
- Consists of three parts: an envelope, which defines what is in the message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing procedure calls and responses
- SOAP has three major characteristics: **Extensibility** (security and WS-routing) , **Neutrality** (over http, smtp, tcp) and **Independence** (any programming model)

ISO 29361 – 3 mainly includes

- The **Web Services Description Language** (now called definition) XML based used for describing the functionality offered by a web service.
- *WSDL* provides a machine-readable description of how the service can be called, what parameters it expects, and what data structures it returns
- It thus serves a roughly similar purpose as a method signature (ie input, output, function, subroutine, return type, argument etc) in a programming language.
- The current version of WSDL is WSDL 2.0.

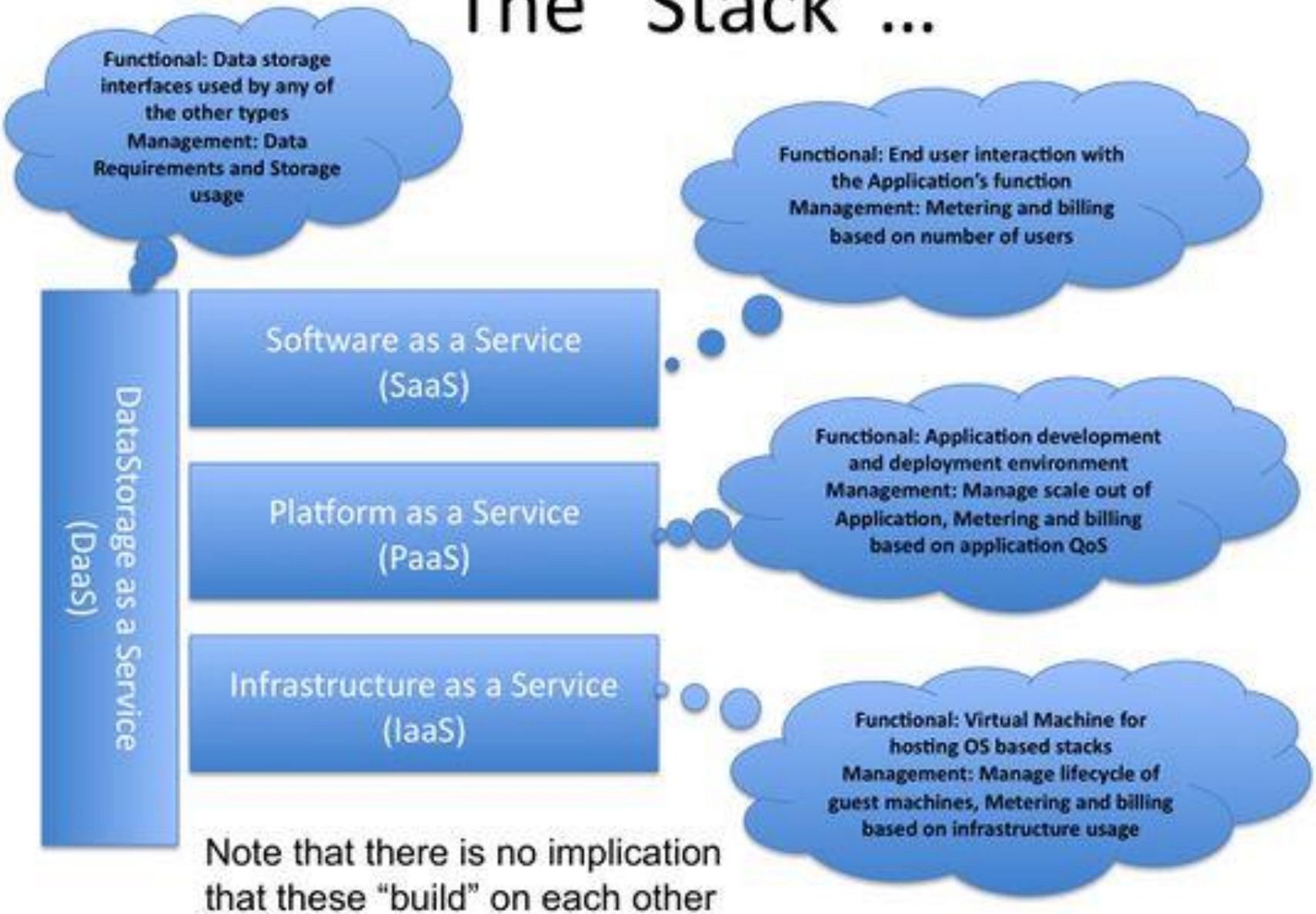
A Cloud(y) picture?



Security in cloud

- Requirements for security in cloud are varied: types of services, criticality etc
- VM – Virtual Machines and Open VM is now the emerging format for cloud
- Ensure that what is created in VM for one provider runs efficiently for the other provider, typically. ie ensuring compatibility, scalability, ‘standardised’

The "Stack"…



Note that there is no implication that these "build" on each other – and they rarely do.

Some Possible Standards

- Federated security (e.g. identity) across Clouds
- Metadata and data exchanges among Clouds
- Standards for moving applications between Cloud platforms
- Standards for describing resource/performance capabilities and requirements
- Standardized outputs for monitoring, auditing, billing, reports and notification for Cloud applications and services
- Common representations (abstract, APIs, protocols) for interfacing to Cloud resources
- Cloud-independent representation for policies and governance
- Portable tools for developing, deploying, and managing Cloud applications and services
- Orchestration and middleware tools for creating composite applications across Clouds
- Standards for machine-readable Service Level Agreements (SLAs)

Cloud Standards and practices

Cloud Security Alliance

Distributed Management Task Force

Open Grid Forum

Open Cloud Consortium

Internet Engineering Task Force

International Telecom Union

Acknowledgement

- http://cloud-standards.org/wiki/index.php?title=Cloud_standards_overview

- http://cloud-standards.org/wiki/index.php?title=File:Slide24.jpg

Information Asset in cloud

- Classification of Information Asset
- Hardware, software and other values
- Responsibility of classification
- Ownership of Information Asset
- Legal, regulatory compliance
- Responsibility to owners, stake-holders
- Preservation of Assets and retrieval

Pillars of Information Security

- Meaning and definition
- Value: monetary, criticality etc
- Confidentiality: Volatility, permanent
- Integrity: a permanent feature
- Availability: when, to whom, how and negatively, prevent to whom, when, how
- Non Repudiation

Information Security - Essence

- Implementation aspects
- Information Systems Security Policy including procedures and guidelines
- Standards like ISO
- Framework: COBIT
- Info Sec and IS Audit – inseparable cousins
- Analysis of Information Security
- Risks, Threats, Vulnerabilities in systems
- Risk Management and Information Security

Information Security: Standards

- BS-7799 ISO 17799 and ISO 27001 certification
- Information Security: preservation of C.I.A. and other properties such as authenticity, accountability, non-repudiation, reliability
- I.S.M.S.: overall management system based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve info security … includes organisational structure, policies, planning activities, responsibilities, procedures, processes and resources
- Risk Management

ISO 27001

- Establish and manage ISMS
- Documentation requirement
- Management responsibility
- Training, awareness, competence
- Internal ISMS audits
- Management review: input, output
- ISMS improvement: C.A.P.A.

Threat and Vulnerability

Threat: A circumstance or event with potential to cause harm to a system (either physical or a computer system);

Includes destruction, unauthorised disclosure or modification of data and/or denial of service;

An external factor or an event which may or may not occur;

A potentiality to harm or destroy the system resources.

Vulnerability: A weakness that could be exploited to cause damage to the system or the assets it contains;

A situation inside the system which may be (should be?) improved;

A weakness inside the system which may be plugged or attended to;

Requires top management's attention to plug the loophole;

May be inherent and has to be put up with but with knowledge.

Threat types and perceptions

- Identify various threats like
- Force majeure
- Organizational shortcoming
- Human error: behaviour (internal or external)
- Technical failure
- Deliberate acts
- host threats
- application threats
- Systemic failure: inherent or sudden
- External event: forecast or feared already

Vulnerability

- Sometimes inherent in the system itself
- Weakness: May or may not be eliminated
- Study the level of exposure and the threat impact
- Impact Analysis to be done to ensure how serious the vulnerability is
- Sometimes dynamic and may increase over time
- When does a vulnerability become critical?
- Vulnerability Analysis and elimination
- Gap Analysis and best practices: Conformance

Impact Analysis

Done as a part of and as a supplementary to threat analysis to study the effect a threat has

A management level analysis to identify the effect of losing the organisation's resources.

BIA measures the effect of resource loss and escalating losses over time, in order to provide senior management with reliable data to enable the management in decision making on risk mitigation and continuity planning

A formal analysis of the effect on the business if a specific set of Information System services are not available

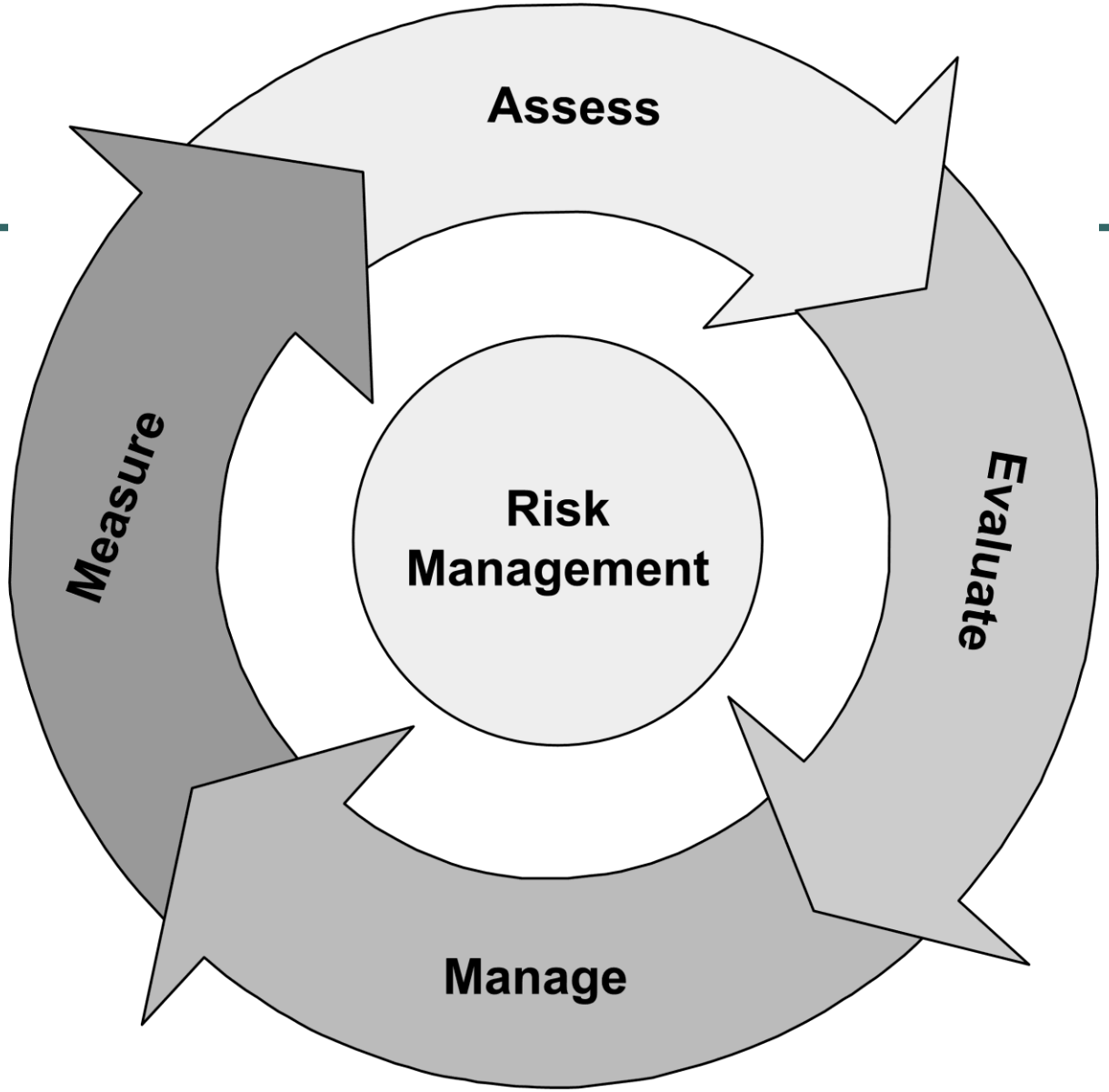
Identifies the minimum set of services that an organisation will require to continue operating

What is risk?

- Risk is probability of unfavorable condition; in financial sector it is the probability of actual return being less than expected return
- a source of danger; a possibility of incurring loss or misfortune
- Risks defined in ISO 31000 as *the effect of uncertainty on objectives*, whether positive or negative

Other concepts in risks

- Foreseen and never foreseen
- Risk appetite
- Risk Tolerance
- Risk Mitigation
- Risk Elimination
- Levels of risk
- Risk Communication


Assess
Evaluate
Manage
Measure
Risk
Management

Authentication factors in cloud

- Authentication: verify the identity of a person or entity requesting access under secure conditions
- Where what is followed?
- Need for a 2-factor, 3-factor in system?
- Meaning of three factor
- What is used in credit cards, ATMs, e-banking
- Private corporate usage
- Usage in secret government communication

Information (in)security

Information (in)security

Cyber Forensics and Digital evidence

- Reports and logs in the application
- Logs and trails in the O/S
- Audit logs and reports generated daily
- Info Security in the audit trails and logs and their access, preservation etc
- Use of tools like EnCase as digital evidence and their admissibility in courts
- Volatility of digital evidence, forensic value

Information Security - Future

- Mobile phone: one-point convergence of all technologies. Centralised security?
- Bandwidth will no longer be the constraint
- BlackBerry, SAT Phones,WiFi (Wireless LAN)
- Security in communication: Internet
- Corporate espionage - Information espionage
- ‘Cloudy’ scenario in Security?
- International espionage (national e-borders), illegal racket of AML, cyber terrorism, arms, narcotics..

Thank you ..... Best wishes

V. Rajendran

Cyber Law Consultant
http://venkrajen.in
Ph: 22473849; 9444073849
venkrajen@yahoo.com
rajcyberlaw@gmail.com