RULES FEST

Keynote Address

Semantic Technologies and the Cloud

Rules for the Next Generation

Said Tabet, Ph.D.

Research Scientist, Consultant
RuleML EMC CTO Office

JBoss® by Red Hat

FICO™

VisionArts communications
strategic thinking • creative action

How risky is the Cloud?

Is Cloud worth it? YES!

Cloud adds the concept of Supply Chain

Cloud Computing Definition

National Institute of Standards and Technology (NIST Special Publication 800-145 (Draft)

- Model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services)
- Rapidly provisioned and released with minimal management effort or service provider interaction
- Composed of 5 essential characteristics, 3 service models, and 4 deployment models.
- Source: http://www.nist.gov/itl/csd/cloud-020111.cfm

Cloud Computing
5 Essential Characteristics

- On-demand tenant self-service model for provisioning computing capabilities (server time, network storage, etc.)
- Broad network access with capabilities over the network accessible by standard mechanisms and mobile platforms
- Resource pooling through dynamically assigned physical and virtual capabilities delivered in a multi-tenant model and location independent
- Rapid elasticity of provisioned resources automatically or manually adjusted aligned with service level flexibility and needs
- Measured service to monitor, control and report on transparent resource optimization

Cloud Computing
3 Service Models

- **Software as a Service (SaaS)**
  - Capability made available to tenant (or consumer) to use provider's applications running on cloud infrastructure, accessible via web browser, mobile apps, and system interfaces.
  - Examples: Salesforce.com, Drop Box, Box.net, Google Docs, WebEx
- **Platform as a Service (PaaS)**
  - Capability made available to tenant to deploy tenant owned (created or acquired) applications using programming languages and tools supported by provider.
  - Examples: Microsoft Azure, Amazon Web Services, Bungee Connect
- **Infrastructure as a Service (IaaS) / Datacenter as a Service (DaaS)**
  - Capability made available to tenant to provision processing, storage, networks or other fundamental computing resources to host and run tenant's applications.
  - Examples: Rackspace, Terremark (Verizon), Savvis, AT&T

Cloud Computing
Deployment Models

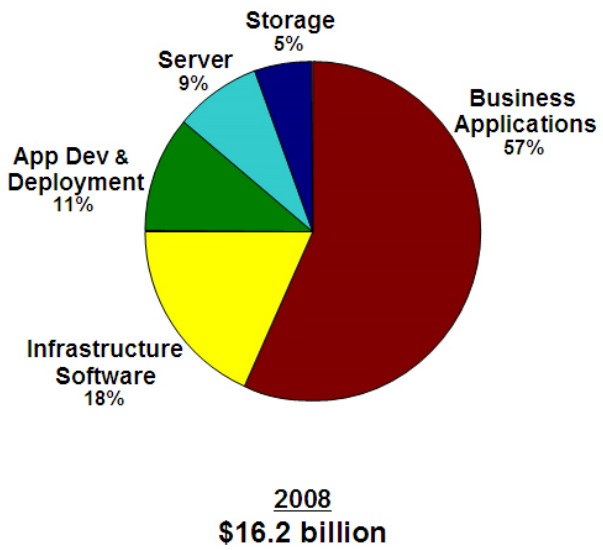
	(1) PRIVATE	(2) COMMUNITY	(3)PUBLIC
ACCESSIBILITY	Single Organization	Shared with Common Interests / Requirements	General Public / Large Industry Group
MANAGEMENT	Organization or Third Party	Organization or Third Party	Cloud Provider
HOST	On or Off Premise	On or Off Premise	On or Off Premise

(4) HYBRID

What should we do?

- ***Embrace and accept this rapid change for Corporate IT and weigh the business benefits and risks.***
- ***Adopt and integrate guidance and toolkits for improved Governance, Risk & Compliance.***

Worldwide IT Cloud Services Spending* by Product/Service Type
2008, 2012



* Includes enterprise IT spending on Business Applications, Systems Infrastructure Software, Application Development & Deployment Software, Servers and Storage

Source: IDC, October 2008

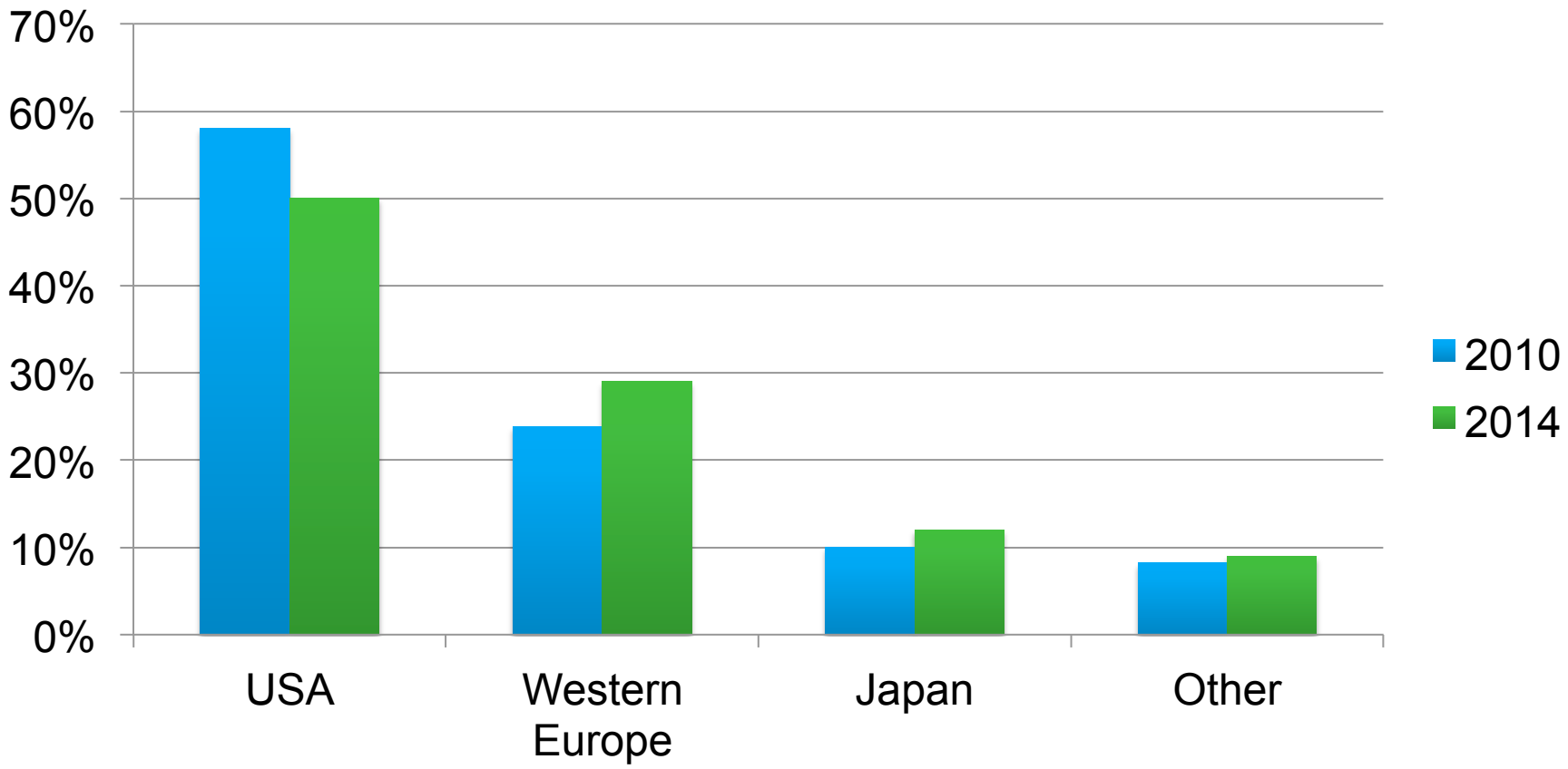
And some more Numbers

Source: Gartner

- Worldwide Cloud Services Market to reach $148.8 billions in 2014
  - $58.6 billion in 2009
  - $68.3 billion in 2010
- Spending to reach $112 billion within 5 years
- Sector by Sector adoption
  - Financial Services
  - Manufacturing
  - Communications and High Tech
  - Public Sector

Adoption by Region

Source: Gartner



Chains are only as strong as the weakest link

GRC Insures the integrity of the chain

EU Concerns
Cloud Computing Strategy DIGIT-IPM

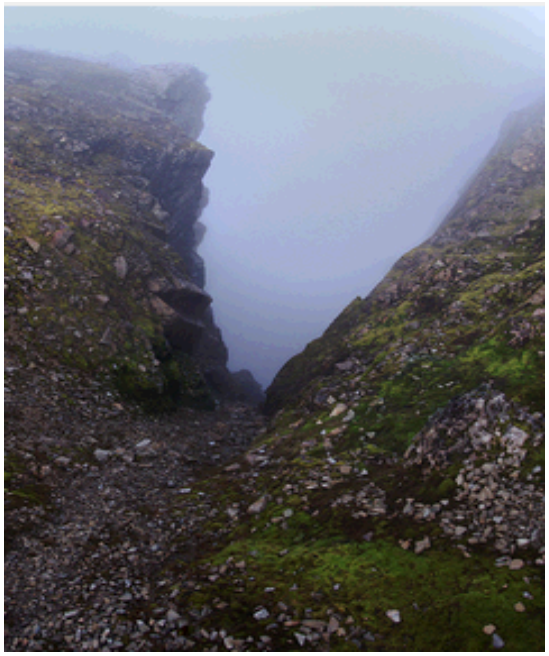
Questions to be answered:

- Legal Framework
- Technical and Commercial Fundamentals
- The Market

Top Five Barriers to Cloud Adoption

Source: CIO Magazine:

- ✓Security
- ✓Openness
- ✓Portability
- ✓Reliability
- ✓Integration



http://www.zdnet.co.uk/videos/view/online-business/experts-highlight-barriers-to-cloud-adoption-260682411/

Cloud Computing
Security: Largest Barrier to Adoption

Example: 2009 - U.K. Hosting provider compromise

- Hypervisor available on the Internet
- Attackers gained full-root access to the "datacenter"
- 100,000 hosted websites deleted

Lots of questions….

What happens if the provider's system goes down? How does my IT team interface with the providers?

What happens if data is comingled with other cloud data or data is introduced which damages the integrity of company data?

What happens if my provider goes out of business?

Security Role Clarity – What level of security can my provider supply? What are my company's responsibilities?

How do I know my provider's cloud architecture is safe?

Can I trust my provider?

How much "concentration" risk am I willing to accept?

Barriers Become Opportunity

Finance & Business Operations

- VP, Enterprise Risk Mgt
- Lines of Business VPs
- VP, Risk Mgt/Compliance
- CFO
- VP, Internal Audit

Management and audit needs dashboards and analytics that

→ Increase visibility, improve decision making, manage risk within appetites

→ Drive accountability into day to day operating fabric

→ Prioritize and scope risk assessments

Legal & Corporate Compliance

- VP, Legal and Compliance
- Chief Information Officer
- Chief Legal Counsel
- Chief Compliance Officer

Legal and compliance needs automated discovery, policy and risk analysis

→ Align policies with business and legal imperatives

→ Understand discoverable information risks, processes and assets in context

→ Leverage common, traceable system of record

Information Technology

- Chief Information Officer
- VP, IT Risk Mgt/Compliance
- VP, Applications
- VP, BCM/DR
- VP, Infrastructure

IT operations needs continuous, automated, consolidated assessments

→ Translate business appetite for risk into IT thresholds

→ Streamline policy and assessments across all IT assets

→ Drive down costs, improve accuracy and improve efficiencies

Security

- Chief Information Security Officer (CISO)
- Director, Security Ops

Security needs to integrate information risk analysis with IT and the business

→ Leverage security metrics and assessment for IT and enterprise risk

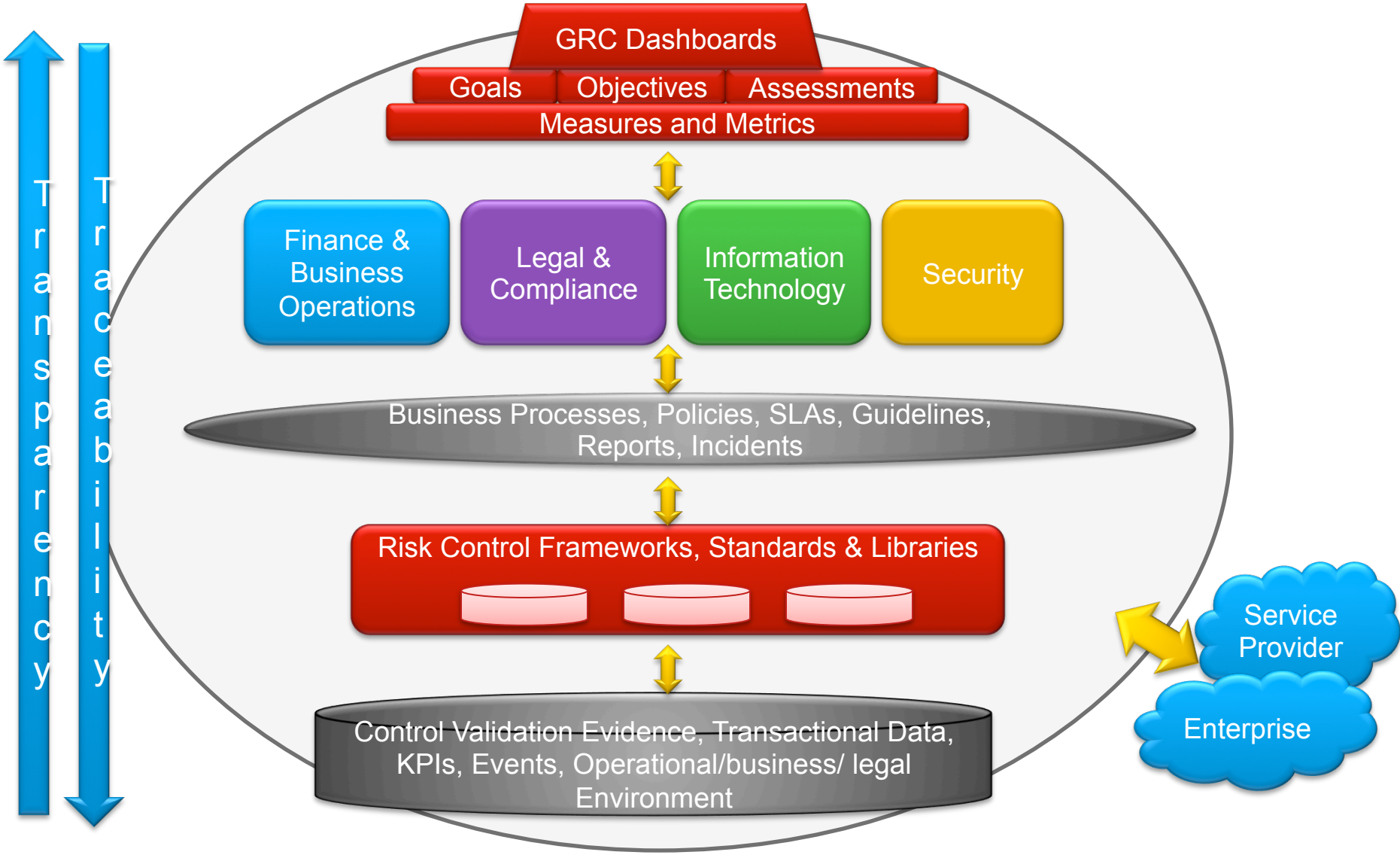
→ Protect information according to its importance and criticality to the business

→ Drive down costs, improve accuracy and improve efficiencies

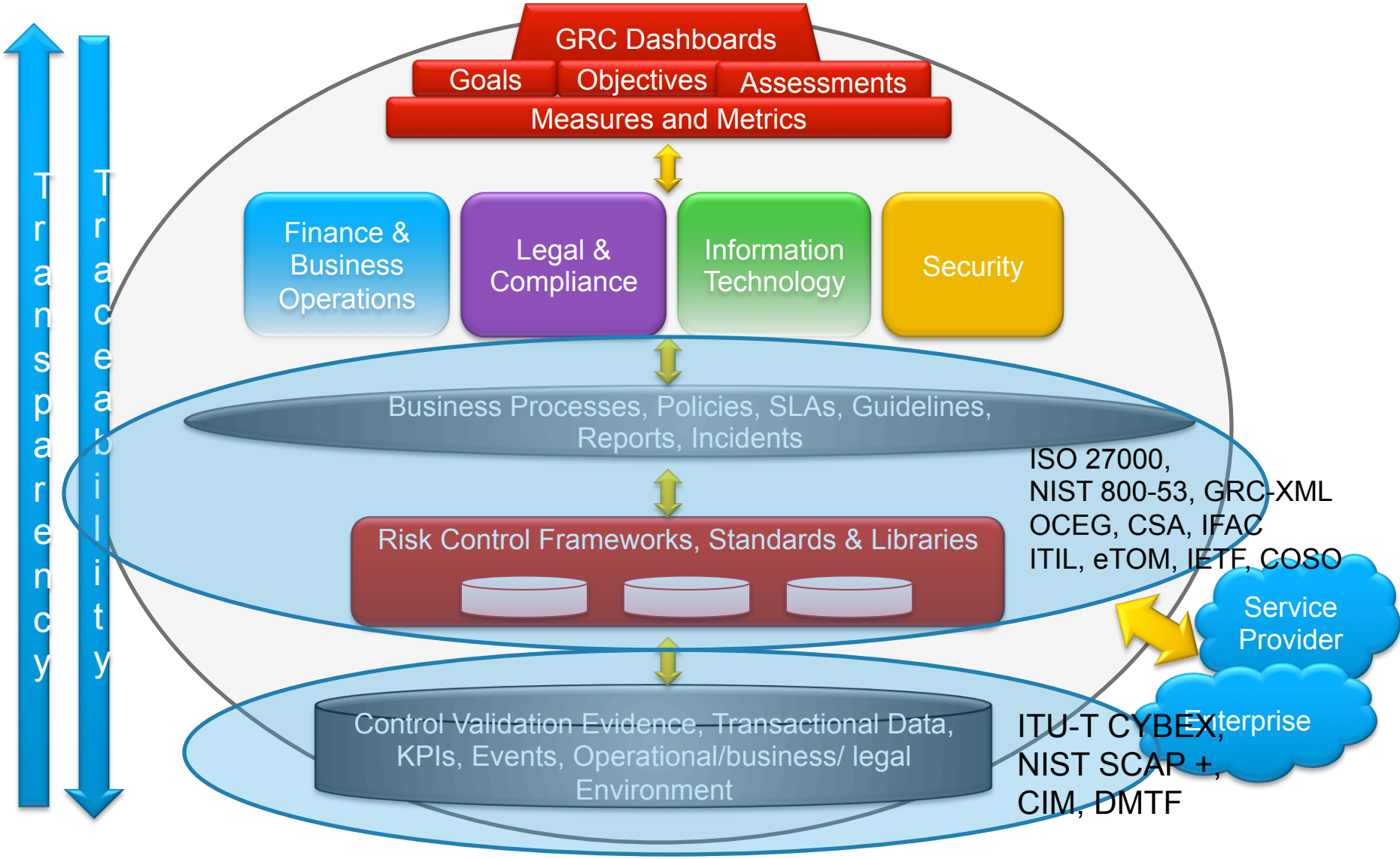
Why do we need Standards?

- Use of available technical expertise, enhanced trade
- Common metrics for service level expectations
- Essential to the cloud supply chain
- Open global markets
- Required by legal and accounting professions
- Increased automation

GRC Automation



GRC Automation Standards



International Standards driving Cloud Trust

Frameworks and Guidance to provide transparency via automation

- International Telecommunications Union (ITU-T) Study Group 17, Question 4
  - Cyber Security Exchange (CYBEX)
  - Pulls together techniques and protocols to enable continuous monitoring and incident coordination
- International Standards Organization (ISO) 27000 SC 27 JTC 1
  - Security standards framework and ISMS Guidance
  - Risk assessment process
- Internet Engineering Task Force (IETF)
  - Protocols to enable secure exchange of information, such as incidents
- Cloud Security Alliance (CSA)
  - Developing guidance and set of cloud specific controls
  - Work in process of integration into international standards bodies
- National Institute of Standards and Technology (NIST)
  - Security Content Automation Protocol (SCAP) plus standards joint from MITRE and NIST also in ITU CYBEX
- Open Compliance and Ethics Group (OCEG)
  - GRC-XML used to format reports that include risk information and rules
- International Federation of Accountants (IFAC)
  - Develops international standards on ethics, auditing and assurance, education, and public sector accounting

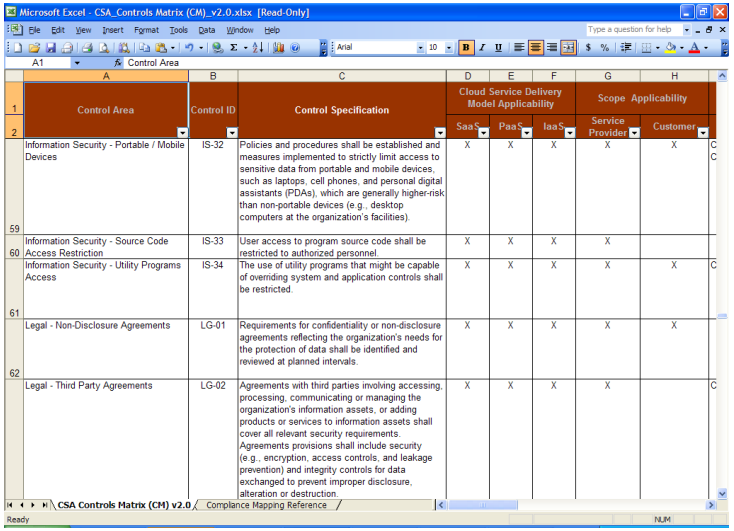
Current State of GRC enabled Cloud Trust

- Consensus Assessment Initiative
  - Lightweight common assessment criteria
  - 148 Questions to assess security of a cloud provider
  - Cloud specific controls developed with CSA guidance

CAI™
Consensus Assessments Initiative

- Cloud Control Matrix
  - 98 controls
  - Bridging regulatory governance and practical compliance
  - Similar to the audit world's concept of "continuous audits"

CCM™
Cloud Controls Matrix


Microsoft Excel - CSA_Controls Matrix (CM)_v2.0.xlsx [Read-Only]

	Control Area	Control ID	Control Specification	Cloud Service Delivery Model Applicability			Scope Applicability	
				SaaS	PaaS	IaaS	Service Provider	Customer
59	Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	X	X	X	X	X
60	Information Security - Source Code Access Restriction	IS-33	User access to program source code shall be restricted to authorized personnel.	X	X	X	X	
61	Information Security - Utility Programs Access	IS-34	The use of utility programs that might be capable of overriding system and application controls shall be restricted.	X	X	X	X	X
62	Legal - Non-Disclosure Agreements	LG-01	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of data shall be identified and reviewed at planned intervals.	X	X	X	X	X
	Legal - Third Party Agreements	LG-02	Agreements with third parties involving accessing, processing, communicating or managing the organization's information assets, or adding products or services to information assets shall cover all relevant security requirements. Agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.	X	X	X	X	

CSA Controls Matrix (CM) v2.0 | Compliance Mapping Reference
Ready

- Cloud Audit
  - Provides a namespace to assist with automation of audit and assessment

Cloud Audit

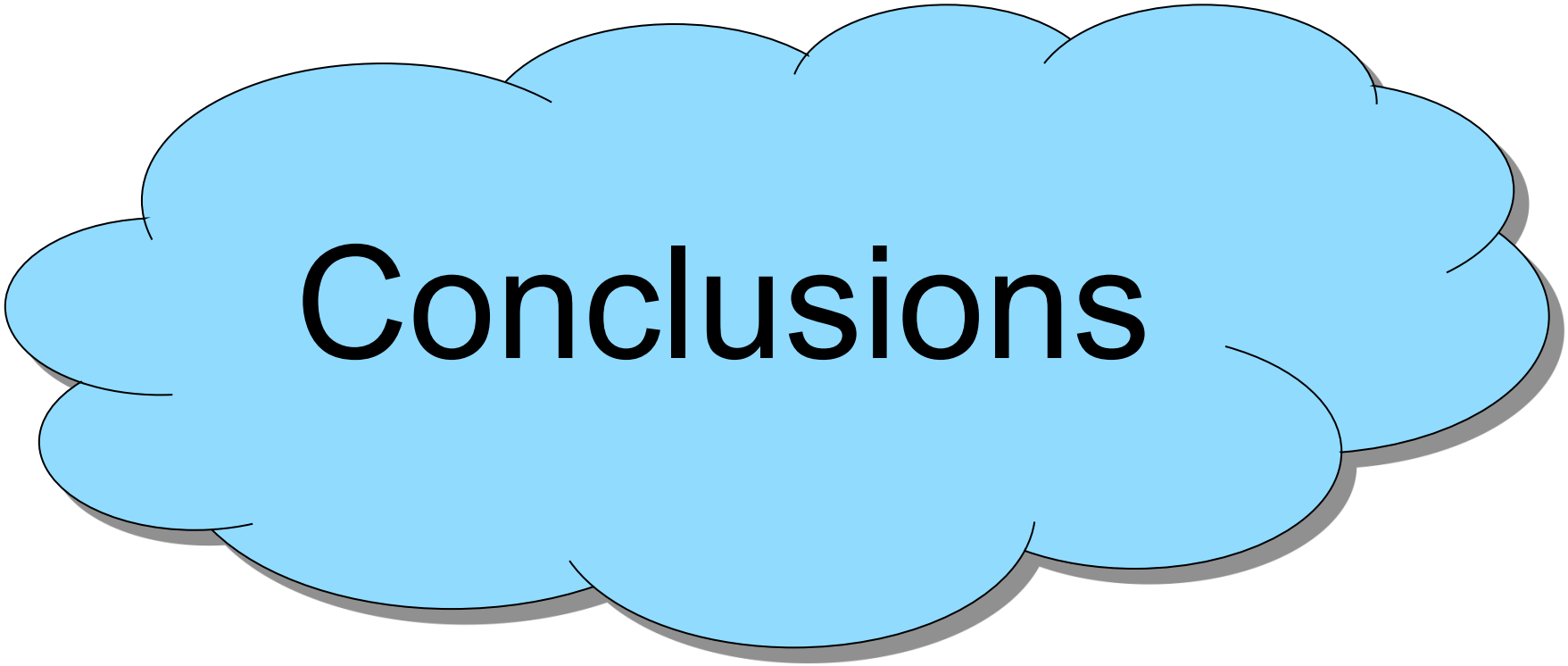
Cloud Computing and Intelligent Data Centers

- Quality of Service
- Service Level Management
- Rule-based service configuration
- Nested Multi-Tier Security
- Automated GRC
- LegalRuleML and SLAs

➢ Software Agents as Cloud Services
  - Ontologies
  - Rules

Cloud Computing and Intelligent Data Centers

- Common vocabulary for federated systems on the Cloud
- Semantic Heterogeneity
  - Interoperability/Portability
- Self-sustaining Data Centers
  - Dynamic deployment of resources
  - Interactive Service Providers-Consumers Audits
- Policy-based Multi-Tenancy



Questions?