



# Business Analytics **Forum**

See The Future Of Decision Making

**November 11-13, 2014** Gold Coast Convention and Exhibition Centre Queensland, Australia

## Building Smarter Enterprises One Step at a Time -- A Journey to Secure Cloud

Scott Masson

Senior Product Manager – IBM Cognos



# How is IT Delivered?

There are three ways to deliver IT capabilities

**Software, hardware,  
& networking**



**Pre-integrated  
systems & appliances**



**Provided  
as a service**





# Security remains the top concern for Cloud Computing adoption

**80%**

Of enterprises consider security the #1 inhibitor to cloud adoptions

*“How can we be assured that our data will not be leaked and that the vendors have the technology and the governance to control its employees from stealing data?”*

**48%**

Of enterprises are concerned about the reliability of clouds

*“Security is the biggest concern. I don’t worry much about the other “-ities” – reliability, availability, etc.”*

**33%**

Of respondents are concerned with cloud interfering with their ability to comply with regulations

*“I prefer internal cloud to (public) IaaS. When the service is kept internally, I am more comfortable with the security that it offers.”*

Source: Driving Profitable Growth Through Cloud Computing, IBM Study (conducted by Oliver Wyman)



# Some recent challenges in the Cloud

## Security Fears Delay Google, CSC Cloud Computing Project In L.A.

By [Andrew R Hickey](#), CRN

2:58 PM EST FR

RELATED: [VIDEOS](#) | [SLIDE SHOWS](#) | [CHANNELCASTS](#) | [COMMENTS](#)

RELATED VIDEOS

Page 1 of 2

IT security fears have caused [Google](#) and solution provider CSC to miss the completion deadline for a massive cloud computing project for the City of Los Angeles, delays that could force the companies to reimburse some of the project costs as they work to get the deployment back on track.



Google (NSDQ:[GOOG](#)) and CSC missed the June 30 deadline to

## Report: Amazon, Lilly split over cloud liability

August 2, 2010 — 7:28am ET | By [George Miller](#)

Eli Lilly may have split with Amazon Web Services in their much heralded cloud computing relationship. The reason: legal indemnification.

*SearchCloudComputing.com* reported the split last week, though it later posted a comment from Amazon saying that the cloud-pioneering drugmaker "has not dropped its use of AWS." Eli Lilly has not yet replied to a *Fierce* request for comment made late last week.

RELATED STORIES

- Amazon
- IBM touts cloud computing ability to cut trial costs
- Eli Lilly uses cloud computing for clinical data analysis
- Amazon answers biopharma's cloud interest
- Lilly continues

## Amazon: Enterprises Should Adjust Expectations for Cloud

By Nancy Gohring, IDG News

[Print](#) [Digg](#) [Twitter](#) [Facebook](#) [More](#)

The reported problems Amazon had last week in negotiating a contract with Eli Lilly point to a disconnect between what cloud providers offer and what large enterprises expect -- though

## Is Microsoft Missing A Cloud Security Trick?

Microsoft had little to say on security at its Worldwide Partner Conference. Larry Walsh thinks it should build security into its cloud message

## IT leaders start to question cloud interoperability

[Angelica Mari](#)

Wednesday 04 August 2010 10:20

As security issues around cloud-based systems begin to be addressed, concerns around how to make applications talk to each other have begun to move to the front of CIOs' minds, according to research

BUSINESS CENTER

August 18, 2008 11:40 AM

## Google Solves Long Gmail Outage, but Questions Remain

By Juan Carlos Perez, IDG News

[Print](#) [Digg](#) [Twitter](#) [Facebook](#) [More](#)

Late Friday night Google solved the third Gmail outage of the past two weeks, but questions remain about the stability of the Webmail service, which is affecting the Google Apps hosted software suite.



# There is hope ...

## Analyst firm estimates cloud security market to hit US\$1.5b by 2015

By Angela Moscaritolo

Oct 22, 2010 12:45 PM

Tags: [Analyst](#) | [firm](#) | [estimates](#) | [cloud](#) | [security](#) | [market](#) | [to](#) | [hit](#) | [\\$1.5](#) | [bil](#)

**Forrester says "highly secure and trusted" cloud services will emerge.**

The cloud security market is expected to grow to US\$1.5 billion by 2015, with nearly five percent of IT security technology spending allocated for those services, according to a report released by research firm Forrester.

Over the next five years, "highly secure and trusted" cloud services will emerge, and security is expected to become an enabler of the cloud, rather than an inhibitor, according to the [report](#), which is based on interviews with more than 24 IT and IT security product vendors, integrators, consultants and cloud providers.

Currently, the cloud security market is valued at around \$200 million, with less than one percent of IT security spending allocated for the cloud, Jonathan Penn, vice president at Forrester, told SCMagazineUS.com.

- “highly secure and trusted” cloud services will emerge
- Cloud security to grow to US\$ 1.5 billion by 2015
- Security expected to become an enabler versus an inhibitor
- IT spending growth on cloud is increasing



# Categories of Cloud Computing Risks

## Control

Many companies and governments are uncomfortable with the idea of their information being located on systems they do not control.

**Providers must offer a high degree of security transparency to help put customers at ease**

## Data

Migrating workloads to a shared network and compute infrastructure increases the potential for unauthorized exposure.

**Authentication and access as well as protection along the data life-cycle become increasingly important**

## Reliability

High availability will be a key concern. IT departments will worry about a loss of service should outages occur.

**Mission-critical applications may not run in the cloud without strong availability guarantees**

## Compliance

Complying with SOX, HIPAA and other regulations may prohibit the use of clouds for some applications.

**Comprehensive auditing capabilities are essential**

## Security Management

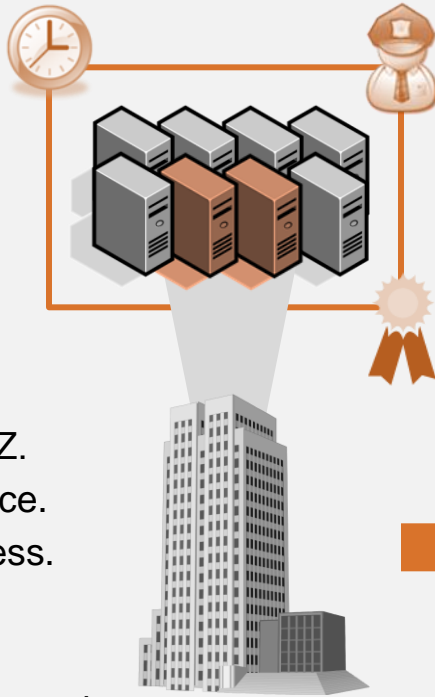
Even the simplest of tasks may be behind layers of abstraction or performed by someone else.

**Providers must supply easy controls to manage security settings for application and runtime environments**

# Balancing Reward with Control and Risk

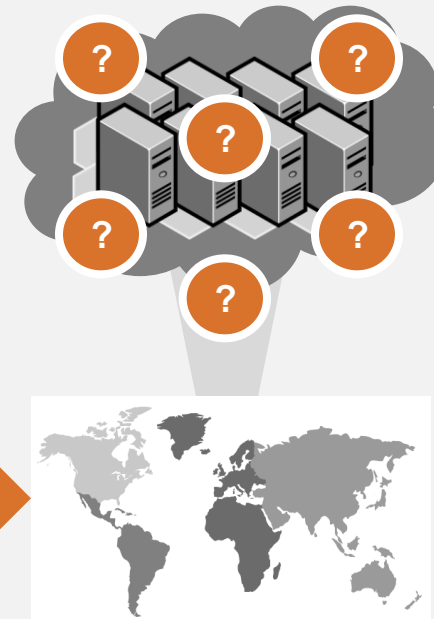
## Today's Data Center

## Tomorrow's Public Cloud



### We Have Control

- It's located at X.
- It's stored in server's Y, Z.
- We have backups in place.
- Our admins control access.
- Our uptime is sufficient.
- The auditors are happy.
- Our security team is engaged.



### Who Has Control?

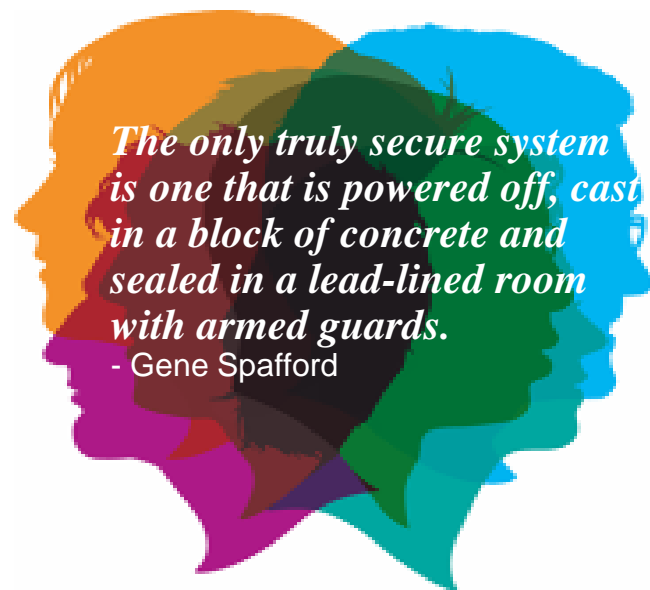
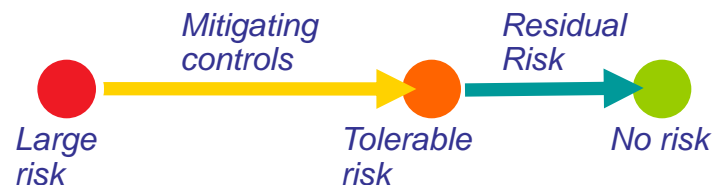
- Where is it located?
- Where is it stored?
- Who backs it up?
- Who has access?
- How resilient is it?
- How do auditors observe?
- How does our security team engage?



# Risk is not a four letter word



- Successful organizations embrace security as a business enabler
- They do this by taking a risk based approach to security.
- Successful information security organizations:
  - Understand the current state of information security in their organization
  - Implement mitigating controls to reduce risk to an acceptable state
  - Understand and accept the residual risk in light of their mitigating controls.
- With their operational risk under control, the business is free to innovate and embrace new challenges while remaining completely secure.
- Through out this process, information security plays the role of a business enabler by effectively managing information security risk for the business.

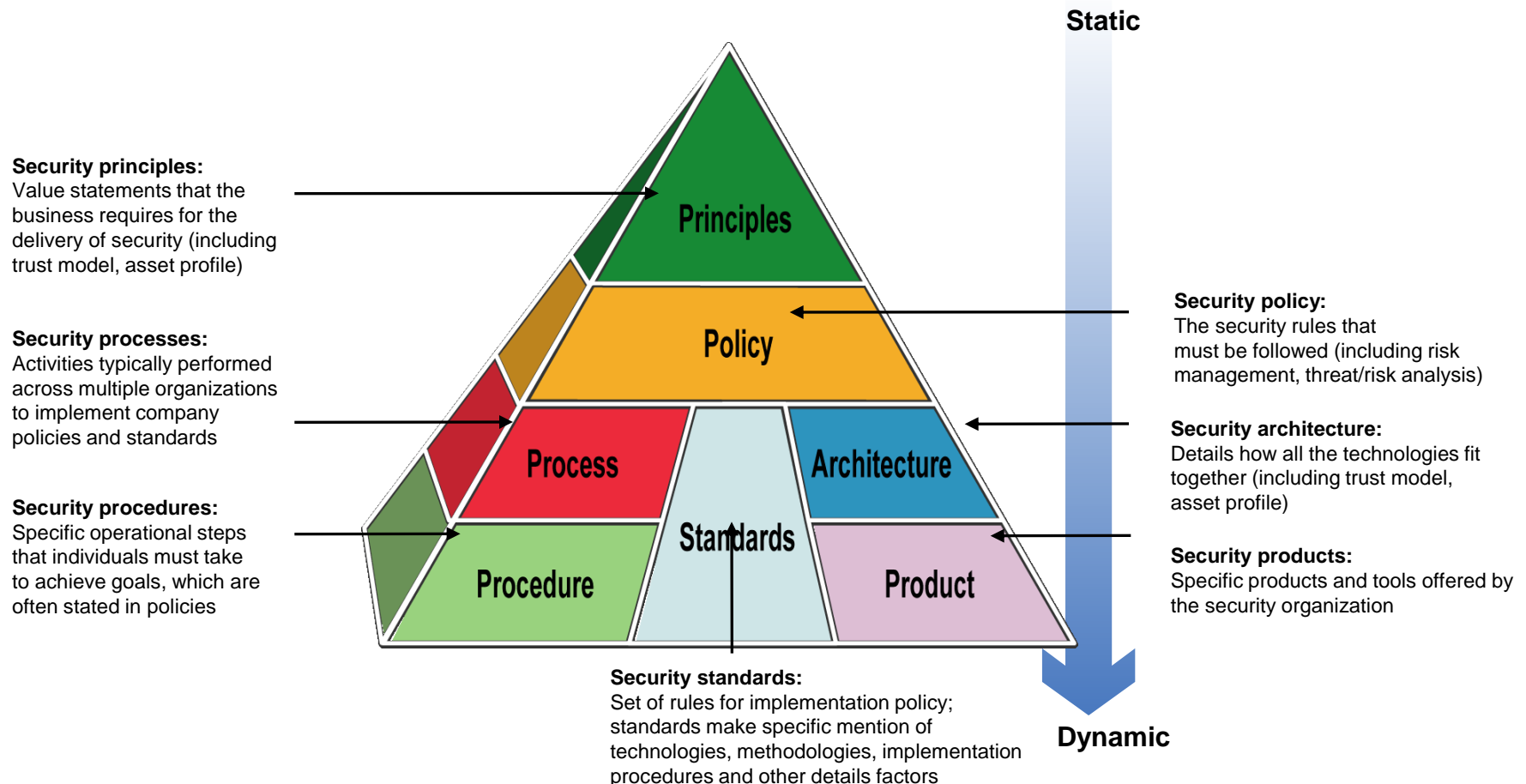




# The true strength of a security program lies in its structure and governance.



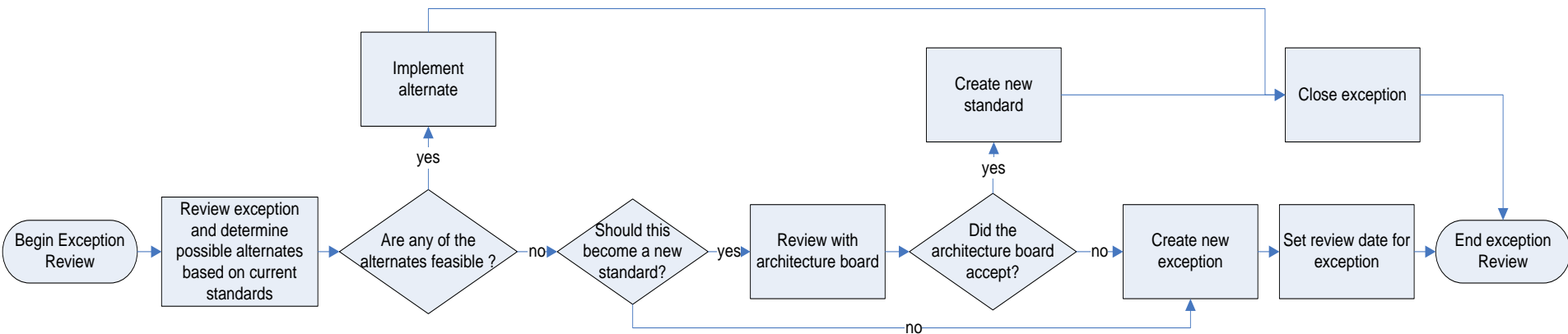
A strong security program begins with the security principals. These strongly governed principals are basis of security program, and there should be tracability of these principals through out the security program.



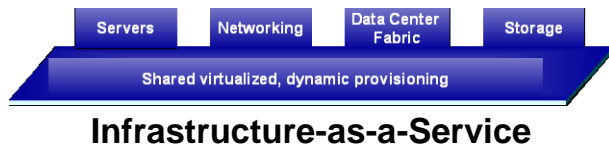
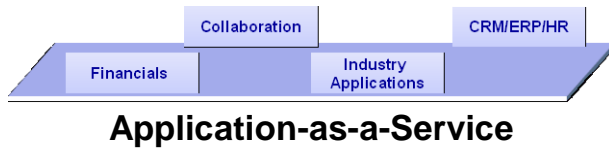


# As with other successfully governed programs, an exception process and remediation cycle is key for Continuous Improvement

An effectively governed security program should have an exception process with a regular review to ensure the exception is still required. There should also be a feedback cycle to consider establishing new standards and to consider refining existing standards where exceptions have been created.

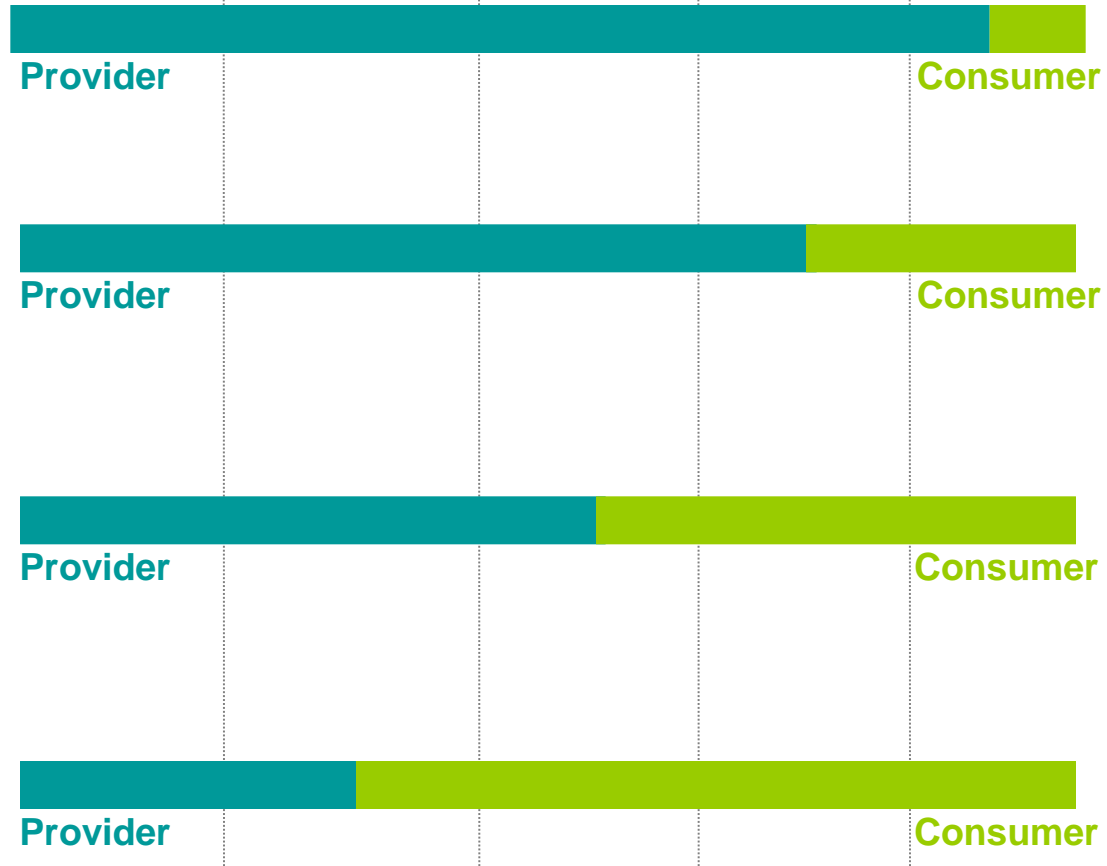


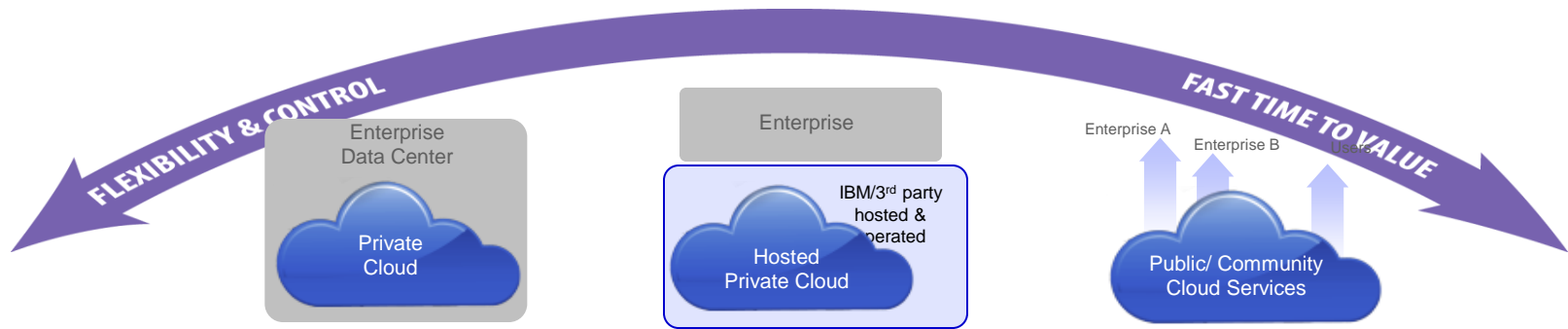
# Coordinating information security is both the responsibility of the provider and the consumer



Who is responsible for security at the ... level?

*Datacenter Infrastructure Middleware Application Process*





## Top private workloads

- Data mining, text mining, or other analytics
- Security
- Data warehouses or data marts
- Business continuity and disaster recovery
- Test environment infrastructure
- Long-term data archiving/preservation
- Transactional databases
- Industry-specific applications
- ERP applications

***Database- and application-oriented workloads emerge as most appropriate***

## Top public workloads

- Audio/video/Web conferencing
- Service help desk
- Infrastructure for training and demonstration
- WAN capacity, VOIP Infrastructure
- Desktop
- Test environment infrastructure
- Storage
- Data center network capacity
- Server

***Infrastructure workloads emerge as most appropriate***



# The Conversation on Cloud Security

## IBM Security Framework



Describes the business landscape of security

## IBM Cloud Security Guidance



Describes the technology landscape

## IBM Capabilities & Offerings to Help



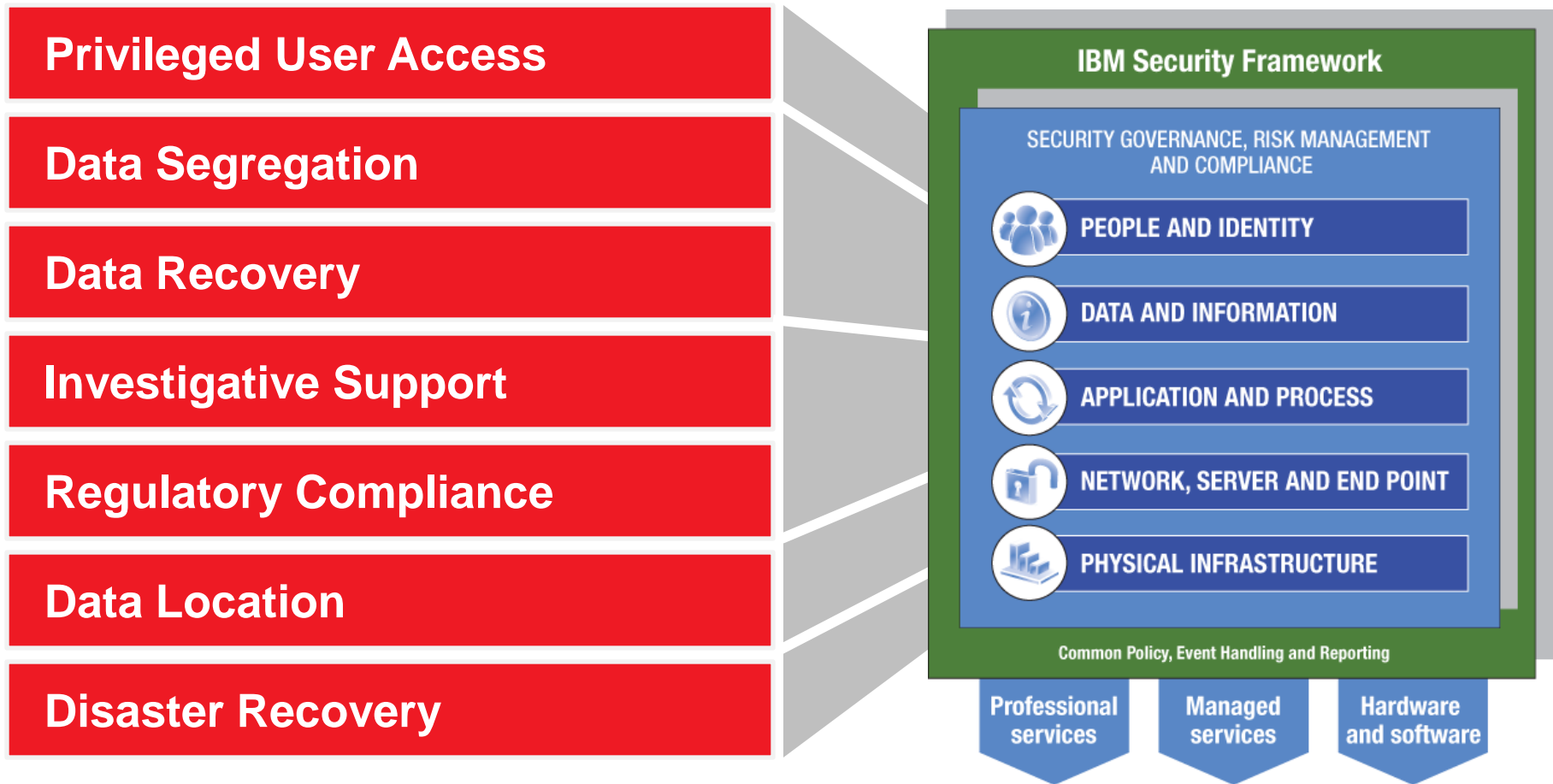
Catalogues of products, services and solutions





# Gartner's security risks of cloud computing

*...map directly to the IBM Security Framework.*

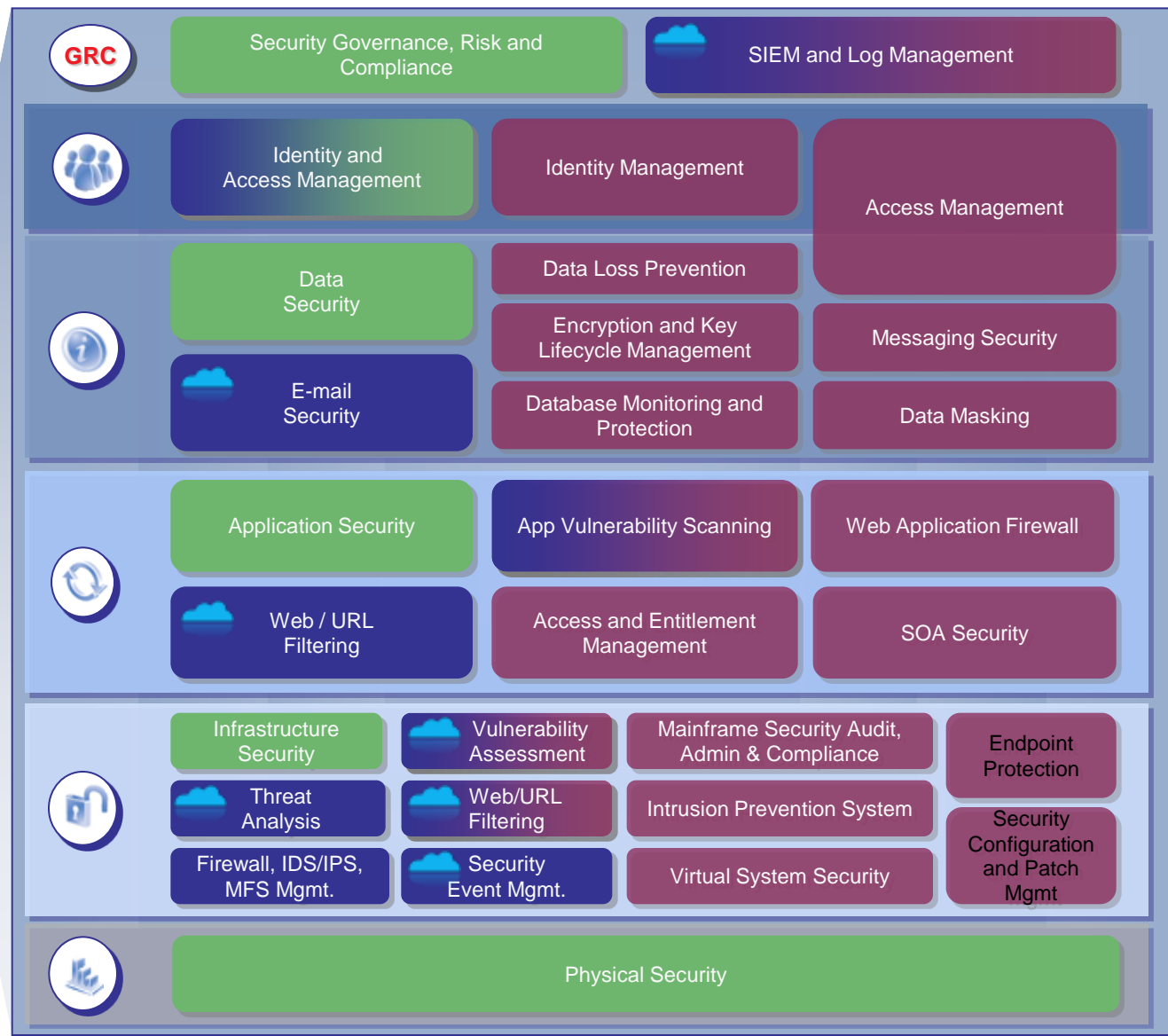




# IBM security portfolio... *solutions to meet your needs*



- = Professional Services
- = Cloud-based & Managed Services
- = Products







# How Enterprises Can Get Started on Business Analytics\*

- Map your BA requirements and IT culture to key Analytics Cloud use cases
- Evaluate and consider scenarios where Analytics on the Cloud may be a right or wrong fit for you

## Five Scenarios for Analytics & Cloud

*Elasticity:* applications with strong seasonal variance in activity. (ex: Retail)

*Co-Existence:* on-premises BA complemented with Cloud BI (ex: General Ledger vs Sales & Marketing)

*Cloud-Native:* BA applications which use cloud-resident data sources (ex: CRM, Social Media).

*Flexibility:* Cloud-based BA workspaces free power analysts from typical application constraints

*Intensive Analytic:* Extra analytical processing power on the cloud

## Cloud – Key Considerations

- How critical are security, risk, regulatory, and privacy considerations?
- How customizable are your data sources?
- Where is the project on IT's priority list?
- What growth do you anticipate for your application and organization?
- Do you need to convert CAPEX to OPEX?
- Where is the data?
- How soon do you go live?

\* Portions adapted from Forrester, "BI & the Cloud", 2010

# IBM Smart Business Development and Test on the IBM Cloud



## Offering website:

<http://www.ibm.com/cloud/solutions/development>

IBM Cloud portal: <http://www.ibm.com/cloud/enterprise>

## What is the service?

- A dynamic virtual development and test infrastructure service, designed for the enterprise, on the IBM Cloud

## What does it offer?

- Choice of virtual server configurations
- Option to add persistent storage charged per usage
- Network bandwidth charged per usage
- Choice of pre-configured software images
  - Rational Application Lifecycle Management software
  - Lotus, WebSphere, DB2 and Informix stacks
- Choice of base operating system – Linux (SUSE , Red Hat, Microsoft Windows (expected in Q4'10))

## What **payment** options are available?

- Pay-as-you-go option (per VM hour charge)
- Shared Reserved option
  - 6 bundles (small, medium, large for 6 or 12 months)
  - Reserved capacity plus discounted usage rate

## What support is available?

- Web-based forum for users to submit requests
- Premium support 24X7 \*



# IBM Cognos BI Software on the IBM Compute Cloud

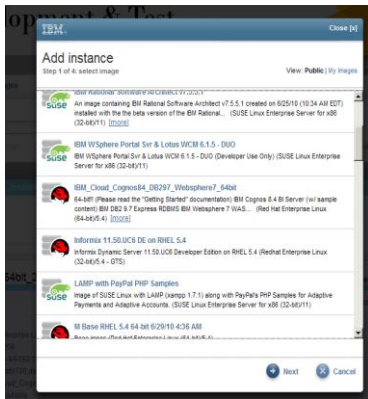
- Bring your own perpetual licenses
- IBM hosted pre-configured BI image with all pre-requisite middleware provisioned in minutes
- Proven practices on Cognos Cloud Deployments



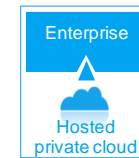
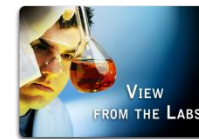
**Step 1** Click and Choose the Service you need

**Step 2** Choose the hardware and usage configuration

**Step 3** Application provisioned and ready to run



# Resources Available



- **Introduction** – provides some overall guidance and considerations (e.g. security, data location)
- **Installation and Configuration** – a step-by-step guide to installing Cognos BI to a single image
- **Security Best Practices** –securing your Cognos BI cloud deployment
- **Handling Cloud Topologies** – techniques to consider when moving from a single image to multiple images
- **Scalability and Performance Best Practices** – planning for scaling and ensuring a high performing solution
- **High Availability Best Practices** – ensuring that your cloud solution is highly available

Other resources include

- IBM Business Analytics and Cloud Computing book
- Proven Practices whitepaper

<http://www.ibm.com/developerworks/cloud/library/cl-cognosperfscle/>

# Security and resiliency complexities raised by virtualization

- New complexities

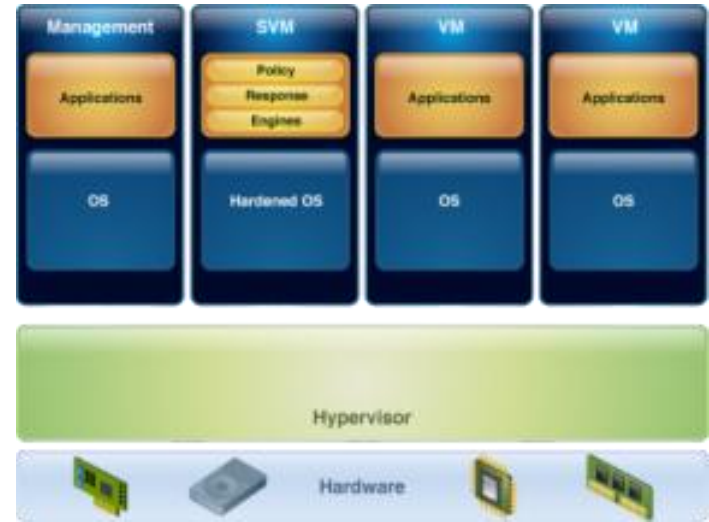
- Dynamic relocation of VMs
- Increased infrastructure layers to manage and protect
- Multiple operating systems and applications per server
- Elimination of physical boundaries between systems
- Manually tracking software and configurations of VMs

Before Virtualization



- 1:1 ratio of OSs and applications per server

After Virtualization



- 1:Many ratio of OSs and applications per server
- Additional layer to manage and secure



# Best Practices for Security Compliance in a Virtualized Environment\*

Configuration and change management processes should be extended to encompass the virtual infrastructure

Can add cost and complexity for system administrator to continuously reconfigure in a dynamic environment

Ensure patch management practices extend to virtualization

Maintain separate administrative access control although server, network and security infrastructure is now consolidated

Provide virtual machine and virtual network security segmentation

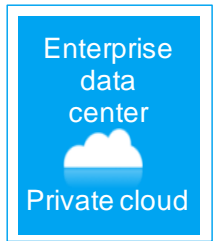
Maintain virtual audit logging



\*Source: RSA Security Brief: Security Compliance in a Virtual World  
[http://www.rsa.com/solutions/technology/secure/wp/10393\\_VIRT\\_BRF\\_0809.pdf](http://www.rsa.com/solutions/technology/secure/wp/10393_VIRT_BRF_0809.pdf)



# Cognos Deployment: Options that scale



## Business Drivers

- Control over infrastructure and data
- Simplest and most common deployment option aimed at a small amount of users and business units
- Lower Investment aimed at smaller organizations or small number of business units
- Resources available for administration

## Deployment Model

- Common gateway for user access
- Single or limited amount of dispatchers handling user requests
- Dedicated Cognos administrators manage application administration
- Relaxed security policies on objects but some report isolation exists

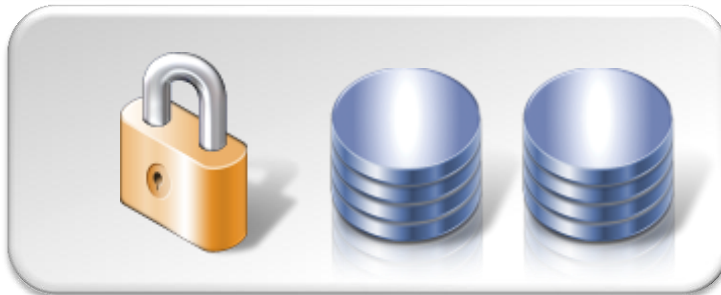
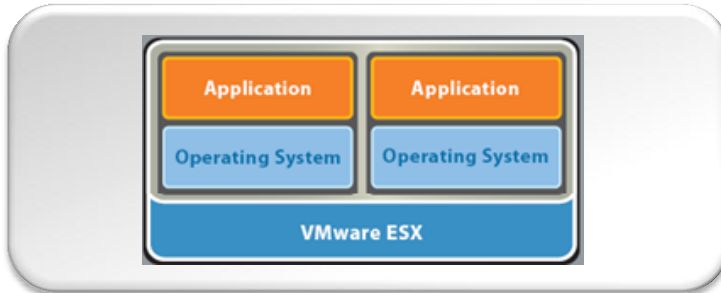
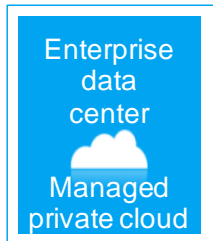
## Security/data Tier

- Mix of various database schemas with row level security and shared data sources
- Common security repository

## Benefits

- Reduced hardware requirements
- Application flexibility due to level of control
- Less management overhead with common security and reporting data sources

# Cognos Deployment: Options that scale



## Business Drivers

- Control over infrastructure and data
- Organizations standardizing on a shared reporting environment
- IT department available for administration

## Deployment Model

- Web server or farm handling users accessing a common portal
- Multiple virtualized dispatchers/servers shared amongst business units
- Internal IT manages application administration
- Segregated content leveraging object security policies

## Security/data Tier

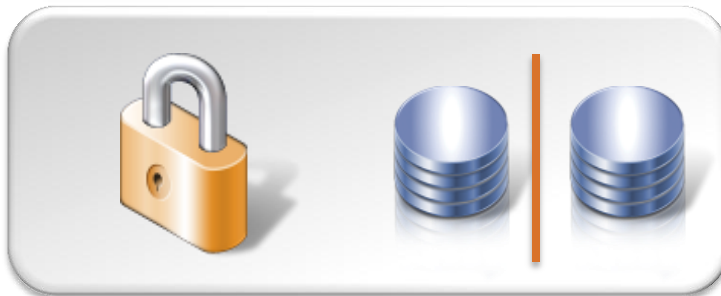
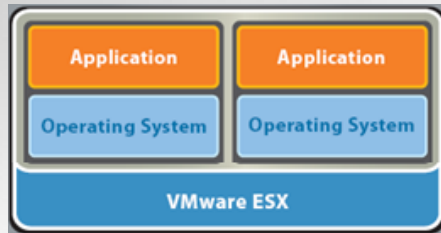
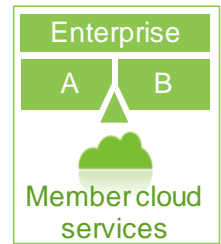
- Unique database schemas or data repositories with row level security coupled with some common data sources
- Common security repository with segregated business organizational units

## Benefits

- Reduced hardware requirements
- Application flexibility due to level of control
- Shared application servers reduces server under utilization
- Less management overhead with common security and shared reporting data sources



# Cognos Deployment: Options that scale



## Business Drivers

- Multiple distinct yet related business units sharing a common infrastructure
- 'Community' Cloud

## Deployment Model

- Individual business units accessing dedicated gateways and security providers
- Multiple virtualized dispatchers shared amongst business units
- Individual and shared reporting content
- Central IT manages application administration with some delegated admin privileges to business units

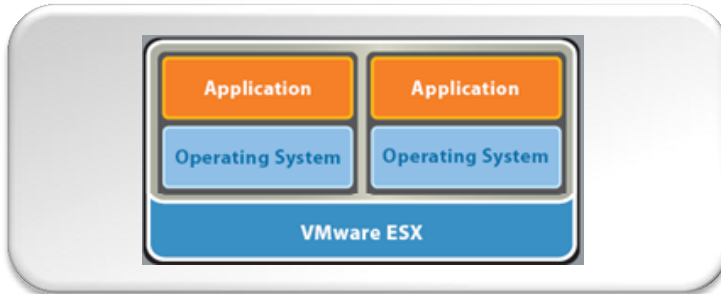
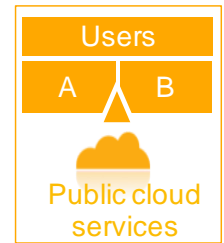
## Security/data Tier

- Unique database schemas and databases with row level security
- Common security repository with segregated business organizational units
- Object security policies segregates content

## Benefits

- Customized gateways provides consistent 'look and feel' for business units
- Shared application servers reduces server under utilization
- Centralized environment reduces capital required to build the infrastructure

# Cognos Deployment: Options that scale



## Business Drivers

- Low cost entry point shifts CapEx to OpEx
- 'Outsource' responsibilities at cost of control
- True multi-tenant deployment

## Deployment Model

- Tenants accessing common gateways
- Multiple virtualized dispatchers shared amongst tenants
- Multiple dedicated physical servers with virtualized partitions as required
- External IT manages application administration with some delegated privileges to tenants

## Shared security/data tier

- Unique databases with row level security (on or off premise)
- Shared security repository with isolated schemas or unique security sources
- Object security policies segregates and isolates content

## Benefits

- Customized gateways provides consistent 'look and feel' for tenants
- Flexibility of adding infrastructure as required by a tenant
- Quicker time to ROI

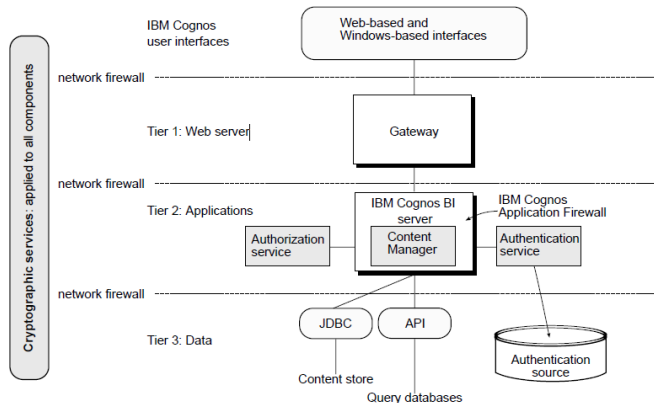
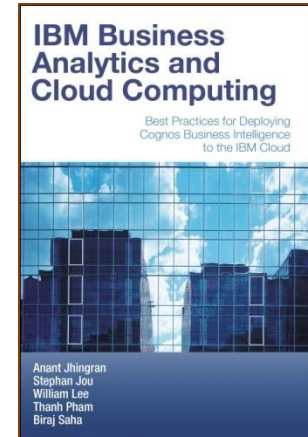


# Cognos Security Best Practices

## Roadside assistance on the journey towards secure deployments

Cognos continues to be an industry leader in security

- Publications
  - Redbooks, Redguides, etc
- Core documentation – Architecture and Deployment Guide
  - Securing the OS, network, application
- Proven Practices
  - Virtualization, security



**Table 2.1: Considerations for Locating Cognos Query Databases**

Query Database in the Cloud	Query Database On-Premises
Workloads require high performance (e.g., rapid queries or large amounts of data).	Workloads have acceptable query performance over a network connection.
New or existing data is easily moved to the cloud (e.g., test data) or is “cloud-born” (e.g., Salesforce data).	A large amount of data exists, or the data is difficult to move to the cloud.
An acceptable level of privacy/security comfort exists around the location of data (e.g., public or non-sensitive data).	Privacy, security, or legal reasons require data to remain on-premises.



# Integrate a cloud computing deployment as part of the existing IT optimization strategy and roadmap

## Consolidate

- Reduce infrastructure complexity
- Reduce staffing requirements
- Manage fewer things better
- Lower operational costs

## Virtualize

- Remove physical resource boundaries
- Increase hardware utilization
- Reduce hardware costs
- Simplify deployments



## Standardize and automate

- Standardize services
- Reduce deployment cycles
- Enable scalability
- Flexible delivery





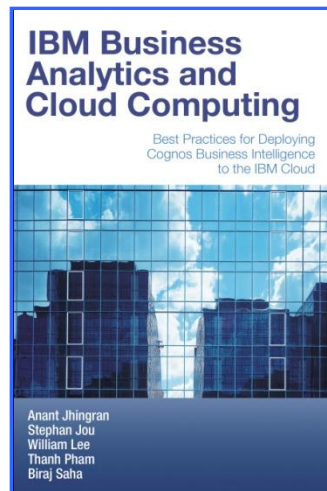
# Cloud Computing also provides the opportunity to simplify security controls and defences

	Cloud Enabled Control(s)	Benefit
<b>People and Identity</b>	<ul style="list-style-type: none"><li>▪ Defined set of cloud interfaces</li><li>▪ Centralized repository of Identity and Access Control policies</li></ul>	<ul style="list-style-type: none"><li>▪ Reduced risk of user access to unrelated resources.</li></ul>
<b>Information and Data</b>	<ul style="list-style-type: none"><li>▪ Computing services running in isolated domains as defined in service catalogs</li><li>▪ Default encryption of data in motion &amp; at rest</li><li>▪ Virtualized storage providing better inventory, control, tracking of master data</li></ul>	<ul style="list-style-type: none"><li>▪ Improved accountability, Reduced risk of data leakage / loss</li><li>▪ Reduced attack surface and threat window</li><li>▪ Less likelihood that an attack would propagate</li></ul>
<b>Process &amp; Application</b>	<ul style="list-style-type: none"><li>▪ Autonomous security policies and procedures</li><li>▪ Personnel and tools with specialized knowledge of the cloud ecosystem</li><li>▪ SLA-backed availability and confidentiality</li></ul>	<ul style="list-style-type: none"><li>▪ Improved protection of assets and increased accountability of business and IT users</li></ul>
<b>Network Server and Endpoint</b>	<ul style="list-style-type: none"><li>▪ Automated provisioning and reclamation of hardened runtime images</li><li>▪ Dynamic allocation of pooled resources to mission-oriented ensembles</li></ul>	<ul style="list-style-type: none"><li>▪ Reduced attack surface</li><li>▪ Improved forensics with ensemble snapshots</li></ul>
<b>Physical Infrastructure</b>	<ul style="list-style-type: none"><li>▪ Closer coupling of systems to manage physical and logical identity / access.</li></ul>	<ul style="list-style-type: none"><li>▪ Improved ability to enforce access policy and manage compliance</li></ul>

# Conclusions regarding information security and Cloud Computing



- Cloud Computing provides a compelling reason for businesses to change their IT sourcing strategy
- Cloud Computing allows the business to move significant amounts of IT CapEx into OpEx
- The panacea of Cloud Computing isn't without its information security risks but can be mitigated



Questions?





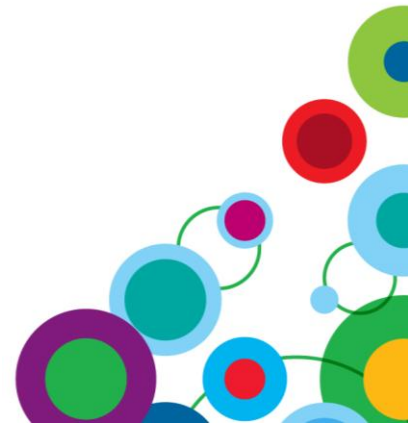
# **WIN** *an Apple<sup>®</sup> iPad*

Please remember to complete your session evaluation online at the Communication Station or point your Smart Phone browser to:

[www.spss.com/goldcoast](http://www.spss.com/goldcoast)



For a chance to win an Apple<sup>®</sup> iPad







# Disclaimer

© Copyright IBM Corporation 2010. All rights reserved.

**U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.**

**THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM’S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS AND/OR SOFTWARE.**

IBM, the IBM logo, ibm.com, and Cognos, are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)

Other company, product, or service names may be trademarks or service marks of others.

Thank You

