Security and Cloud Computing

Martin Borrett, Lead Security Architect NE Europe,
WW Service Management Tiger Team

IBM Software

PCTY2010

Pulse Comes to You

Optimising the World's Infrastructure

27 **May** - London

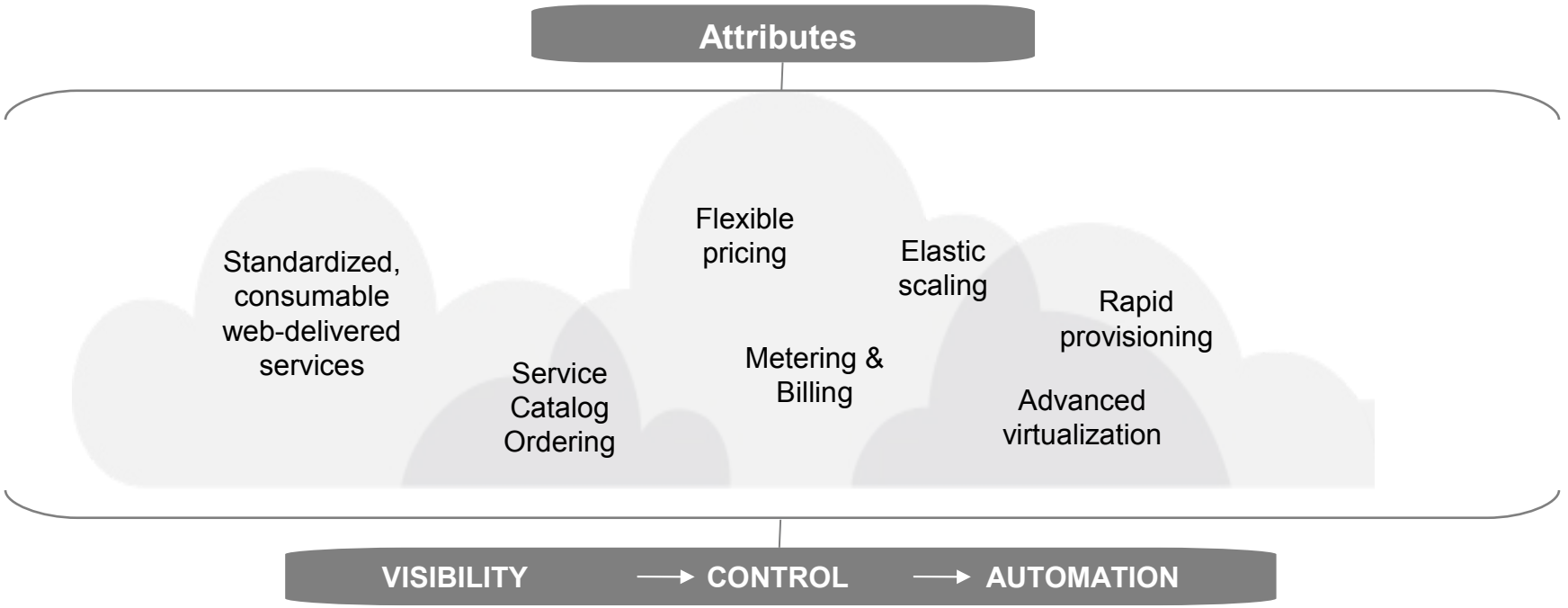
Agenda

- Brief Introduction to Cloud Computing
- Security: Grand Challenge for the Adoption of Cloud Computing
- Cloud Security = SOA Security + Secure Virtualized Runtime
- IBM Cloud Security Offerings

Brief Introduction to Cloud Computing

What is Cloud Computing?

"Cloud" is a new consumption and delivery model for many IT-based services, in which the user sees only the service, and has no need to know anything about the technology or implementation



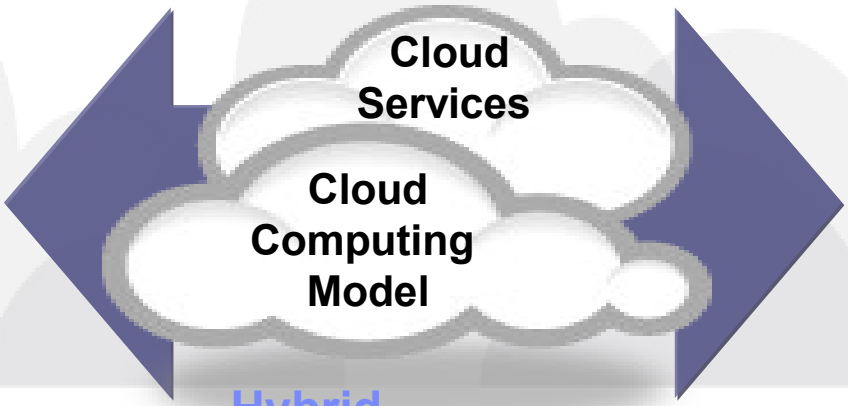
....service oriented and service managed

Cloud Computing Delivery Models

Flexible Delivery Models

Public …

- Service provider owned and managed
- Access by subscription
- Delivers select set of standardized business process, application and/or infrastructure services on a flexible price per use basis



Private …

- Privately owned and managed.
- Access limited to client and its partner network.
- Drives efficiency, standardization and best practices while retaining greater customization and control

Hybrid …

Access to client, partner network, and third party

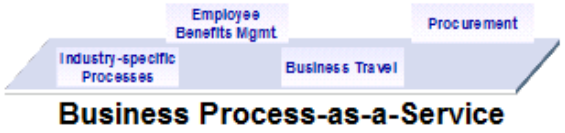
….Standardization, capital preservation, flexibility and time to deploy

…. Customization, efficiency, availability, resiliency, security and privacy

ORGANIZATION → CULTURE → GOVERNANCE

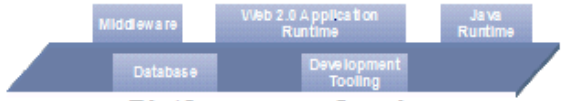
…service sourcing and service value

Responsibilities of Provider and Subscriber



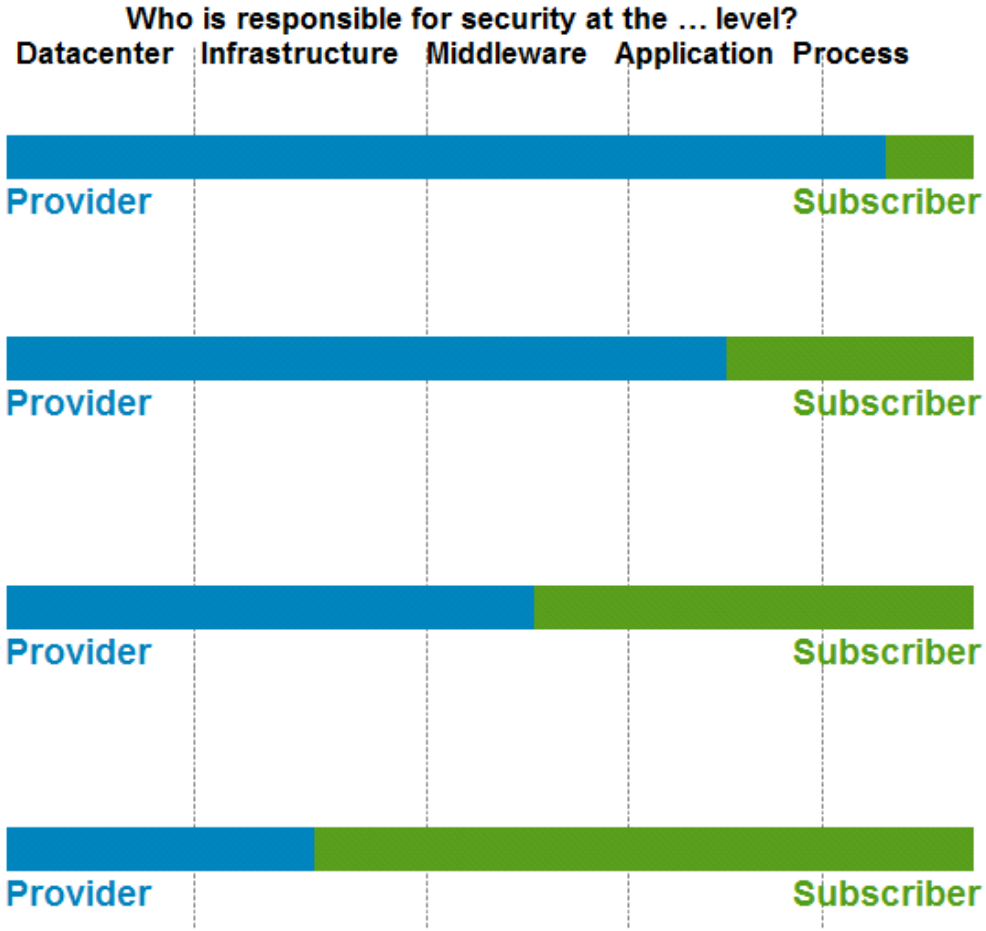
Business Process-as-a-Service

Application-as-a-Service



Platform-as-a-Service

Infrastructure-as-a-Service



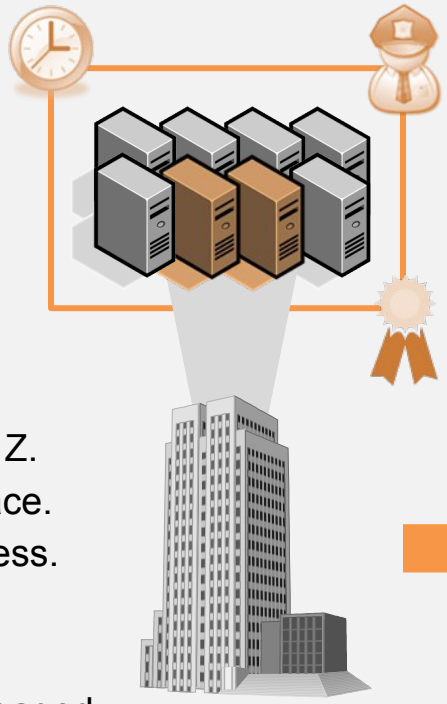
☆ Provider/Subscriber service agreement determines actual responsibilities.

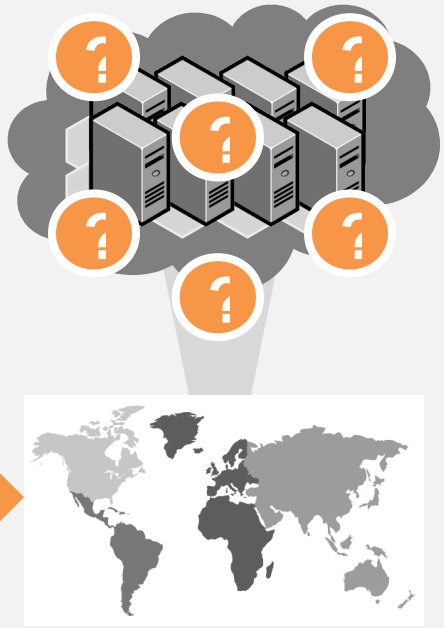
Security – Grand Challenge for the Adoption of Cloud Computing

Simple Example

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?

Security Remains the Top Concern for Cloud Adoption

80%

Of enterprises consider security the #1 inhibitor to cloud adoptions

48%

Of enterprises are concerned about the reliability of clouds

33%

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

*"**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?"*

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

*"**I prefer internal cloud to 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)

Specific Customer Concerns Related to Security

Protection of intellectual property and data	30%
Ability to enforce regulatory or contractual obligations	21%
Unauthorized use of data	15%
Confidentiality of data	12%
Availability of data	9%
Integrity of data	8%
Ability to test or audit a provider's environment	6%
Other	3%

Source: Deloitte Enterprise@Risk: Privacy and Data Protection Survey

What is Cloud Security?

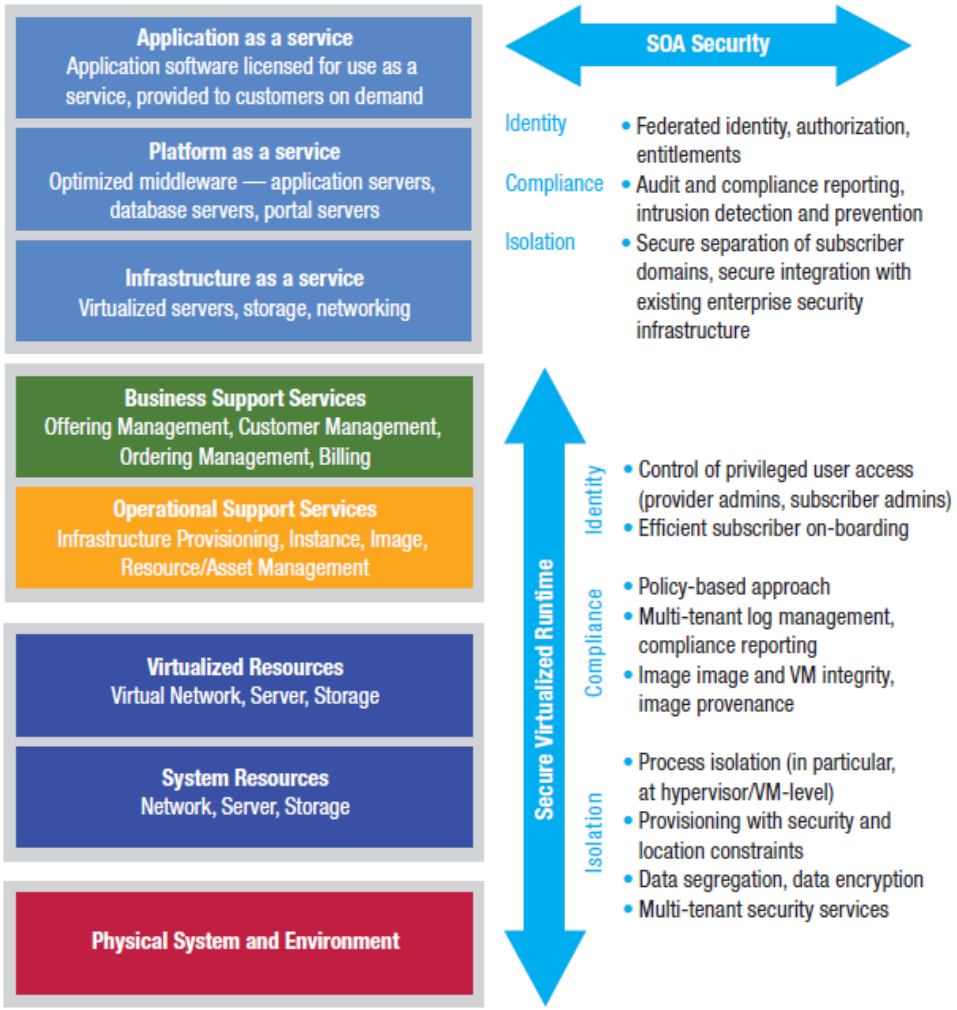
Confidentiality, integrity, availability of business-critical IT assets

Stored or processed on a cloud computing platform

There is nothing new under the sun
but there are lots of old things we don't know.

Ambrose Bierce, The Devil's Dictionary

IBM Point of View: Security and Cloud Computing



SOA Security

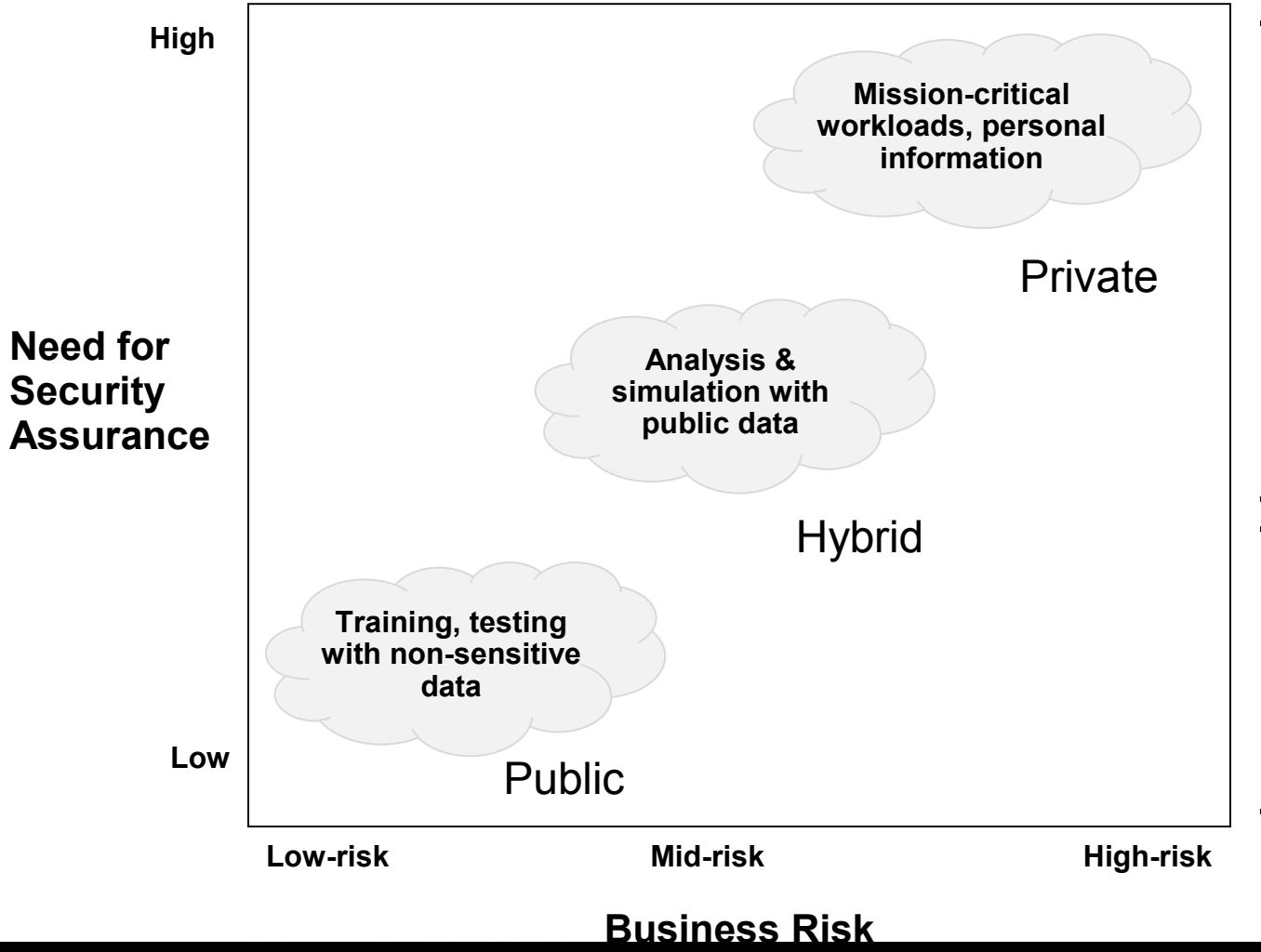
+

Secure Virtualized Runtime

=

Cloud Security

Security as a Potential Market Differentiator: Different Workloads have Different Risk Profiles



High value / high risk workloads need

- Quality of protection adapted to risk
- Direct visibility and control
- Significant level of assurance

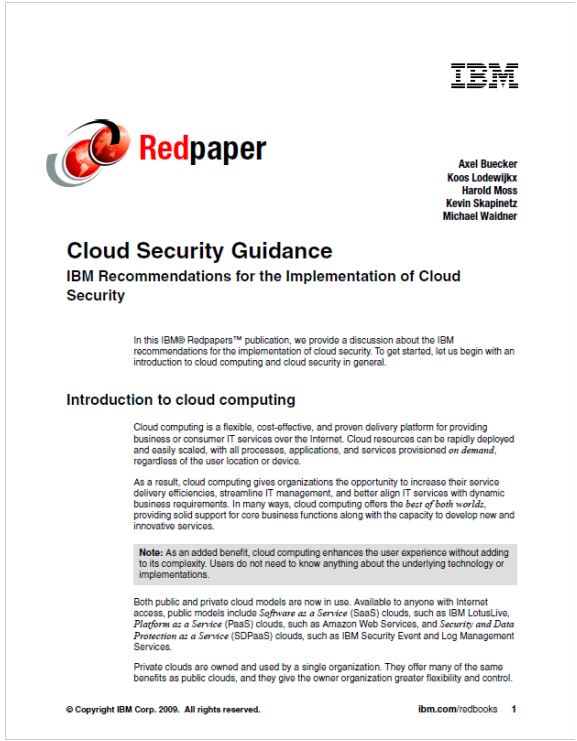
Today's clouds are primarily here:

- Lower risk workloads
- One-size-fits-all approach to data protection
- No significant assurance
- Price is key

IBM Cloud Security Offerings

IBM Cloud Security Guidance document

- Based on cross-IBM research and customer interaction on cloud security
- Highlights a series of best practice controls that should be implemented
- Broken into 7 critical infrastructure components:
  - *Building a Security Program*
  - *Confidential Data Protection*
  - *Implementing Strong Access and Identity*
  - *Application Provisioning and De-provisioning*
  - *Governance Audit Management*
  - *Vulnerability Management*
  - *Testing and Validation*



IBM

Redpaper

Axel Buecker
Koos Lodewijkx
Harold Moss
Kevin Skapinetz
Michael Waidner

Cloud Security Guidance

IBM Recommendations for the Implementation of Cloud Security

In this IBM® Redpapers™ publication, we provide a discussion about the IBM recommendations for the implementation of cloud security. To get started, let us begin with an introduction to cloud computing and cloud security in general.

Introduction to cloud computing

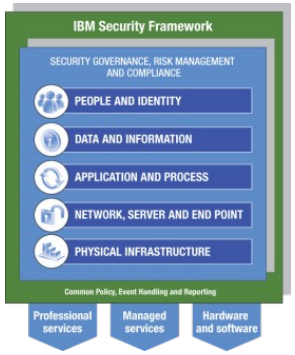
Cloud computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications, and services provisioned *on demand*, regardless of the user location or device.

As a result, cloud computing gives organizations the opportunity to increase their service delivery efficiencies, streamline IT management, and better align IT services with dynamic business requirements. In many ways, cloud computing offers the *best of both worlds*, providing solid support for core business functions along with the capacity to develop new and innovative services.

Note: As an added benefit, cloud computing enhances the user experience without adding to its complexity. Users do not need to know anything about the underlying technology or implementations.

Both public and private cloud models are now in use. Available to anyone with Internet access, public models include *Software as a Service* (SaaS) clouds, such as IBM LotusLive, *Platform as a Service* (PaaS) clouds, such as Amazon Web Services, and *Security and Data Protection as a Service* (SDPaaS) clouds, such as IBM Security Event and Log Management Services.

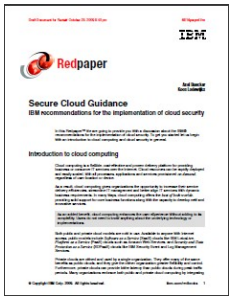
Private clouds are owned and used by a single organization. They offer many of the same benefits as public clouds, and they give the owner organization greater flexibility and control.



IBM Security Framework

Security governance, risk management and compliance

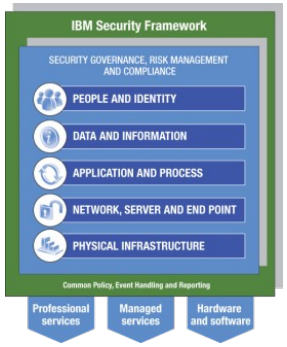
Customers require **visibility** into the security posture of their cloud. Trust is critical.



IBM Cloud Security Guidance Document

Implement a governance and audit management program

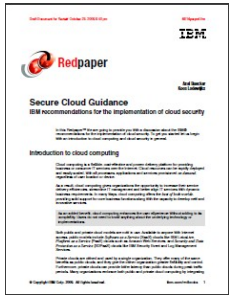
- Governance will be key to driving the trust and confidence customers will need.
- Provide access to tenant-specific log and audit data
- Create effective incident reporting for tenants
- Visibility into change, incident, image management, etc.
- Establish 3rd-party audits (SAS 70, ISO27001, PCI)



IBM Security Framework

People and Identity

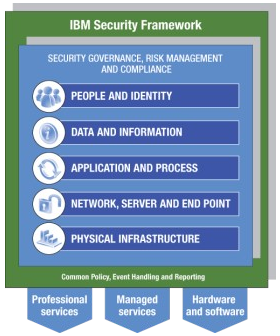
Customers require **proper authentication** of cloud users.



IBM Cloud Security Guidance Document

Implement strong identity and access management

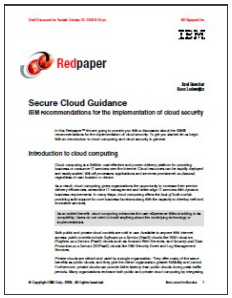
- Privileged Identity Management, privileged user monitoring, including logging activities, physical monitoring and background checking
- Utilize federated identity to coordinate authentication and authorization with enterprise or third party systems
- A standards-based, single sign-on capability can help simplify user logons for both internally hosted applications and the cloud.



IBM Security Framework

Data and Information

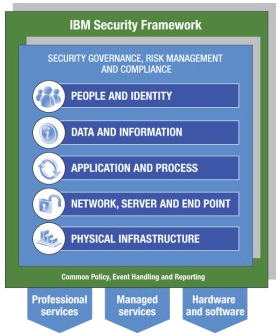
Customers cite **data protection** as their **most important** concern.



IBM Cloud Security Guidance Document

Ensure confidential data protection

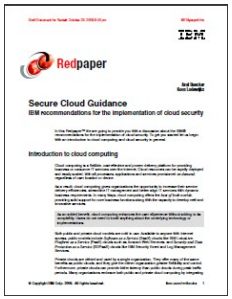
- Use a secure network protocol when connecting to a secure information store.
- Implement a firewall to isolate confidential information, and ensure that all confidential information is stored behind the firewall.
- Sensitive information not essential to the business should be securely destroyed.



IBM Security Framework

Application and Process

Customers require **secure cloud applications** and **provider processes**.



IBM Cloud Security Guidance Document

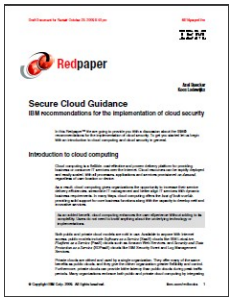
Establish application and environment provisioning

- Implement a program for application and image provisioning.
- A secure application testing program should be implemented.
- Ensure all changes to virtual images and applications are logged.
- Develop all Web based applications using secure coding guidelines.

IBM Security Framework

Network, Server and End Point

Customers expect a **secure** cloud **operating environment**.



IBM Cloud Security Guidance Document

Maintain environment testing and vulnerability/intrusion management

- Isolation between tenant domains
- Trusted virtual domains: policy-based security zones
- Built-in intrusion detection and prevention
- Vulnerability Management
- Protect machine images from corruption and abuse

Trusted Advisor | Solution Provider | Security Company | The Company

Security for the Cloud | Security from the Cloud

Security & Privacy Leadership

IBM Software

PCTY2010

Pulse Comes to You