



Business Technology Briefing: Fear of Flying, And How You Can Overcome It

Joseph Tobloski

Senior Director for Data & Platforms R&D

Accenture Technology Labs

Technology

Fear of Flying And How You Can Overcome It

May 2011

>
accenture

High performance. Delivered.

Agenda

The environment

Five principles for crafting a security strategy

Where Accenture stands



The Environment



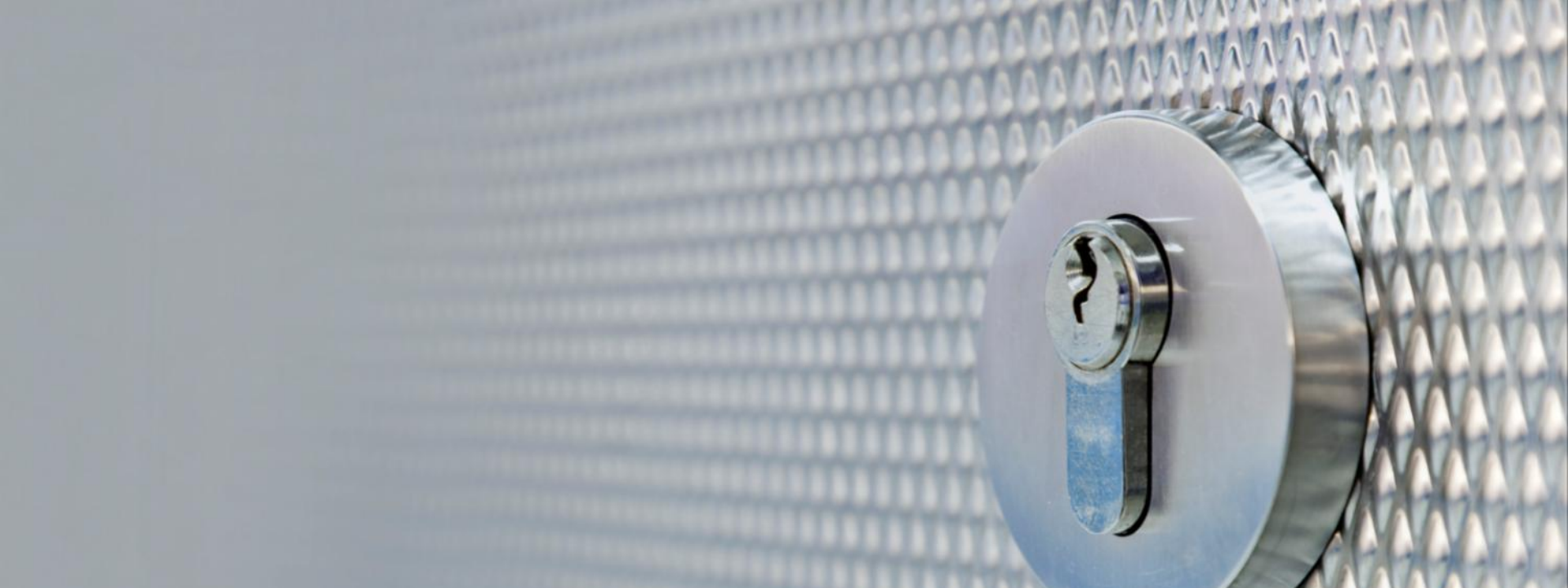
Ready or not, the cloud is here

- Enterprise data no longer rests solely within the enterprise data center, nor is it necessarily owned by the enterprise.
- Legal and regulatory barriers, real or perceived, have significantly slowed enterprise cloud adoption.
- Transition to cloud is inevitable — remaining on sidelines is not an option.



Preparing for the inevitable transition

- Understand the risks associated with the cloud, including multi-tenancy, regulatory and commercial.
- Develop a risk management framework for securing and governing applications, data and processes.
- Architect solutions (composed of people, processes, and technology) to consistently address these risks.




Five principles for crafting a security strategy

Five principles for crafting a security strategy



1. Know your appetite for privacy and security risk.
2. Expect to share responsibility.
3. Demand transparency and accountability from cloud providers.
4. Use the cloud to solve identity and access management issues.
5. Architect solutions that address the risk.

Know your appetite for privacy and security risk



- Legal and regulatory issues are exacerbated in a cloud setting
- Classify your data and your applications to make strategic decisions about what you're moving to the cloud
- Consider data location issues
 - Regulated data remains regulated regardless of location.
- Cloud computing risk management framework
 - Rationalize legal, reputational, cost impacts of security and compliance breaches

Risk management framework

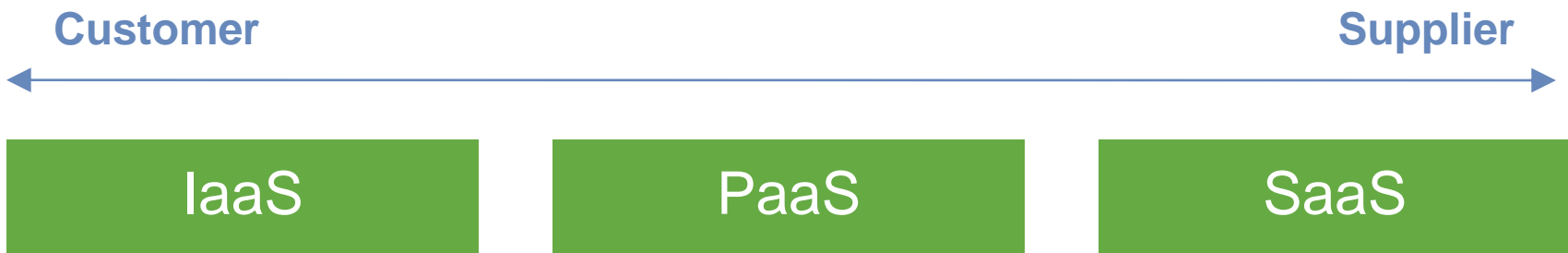
Defining a cloud risk framework helps organizations with the following activities:

Move to the cloud	Gain visibility in the cloud	Secure the cloud
Find the right mix of guidance and standards.	Use mechanisms to check cloud provider security health.	Add new applications and users in a manner that works for your organization.
Harmonize regulatory regimes and legal requirements from different industries, countries, jurisdictions.	Verify continuation of technical and operational security controls.	Stay on the right side of privacy law.
Verify SLA/contract terms established with the cloud service provider.	Sense and predict when systems will deviate from the norm.	Provide checklist of “must-have” security criteria.
		Ensure vulnerabilities are caught early.
		Ensure strong coordination with and direction of system integrators.

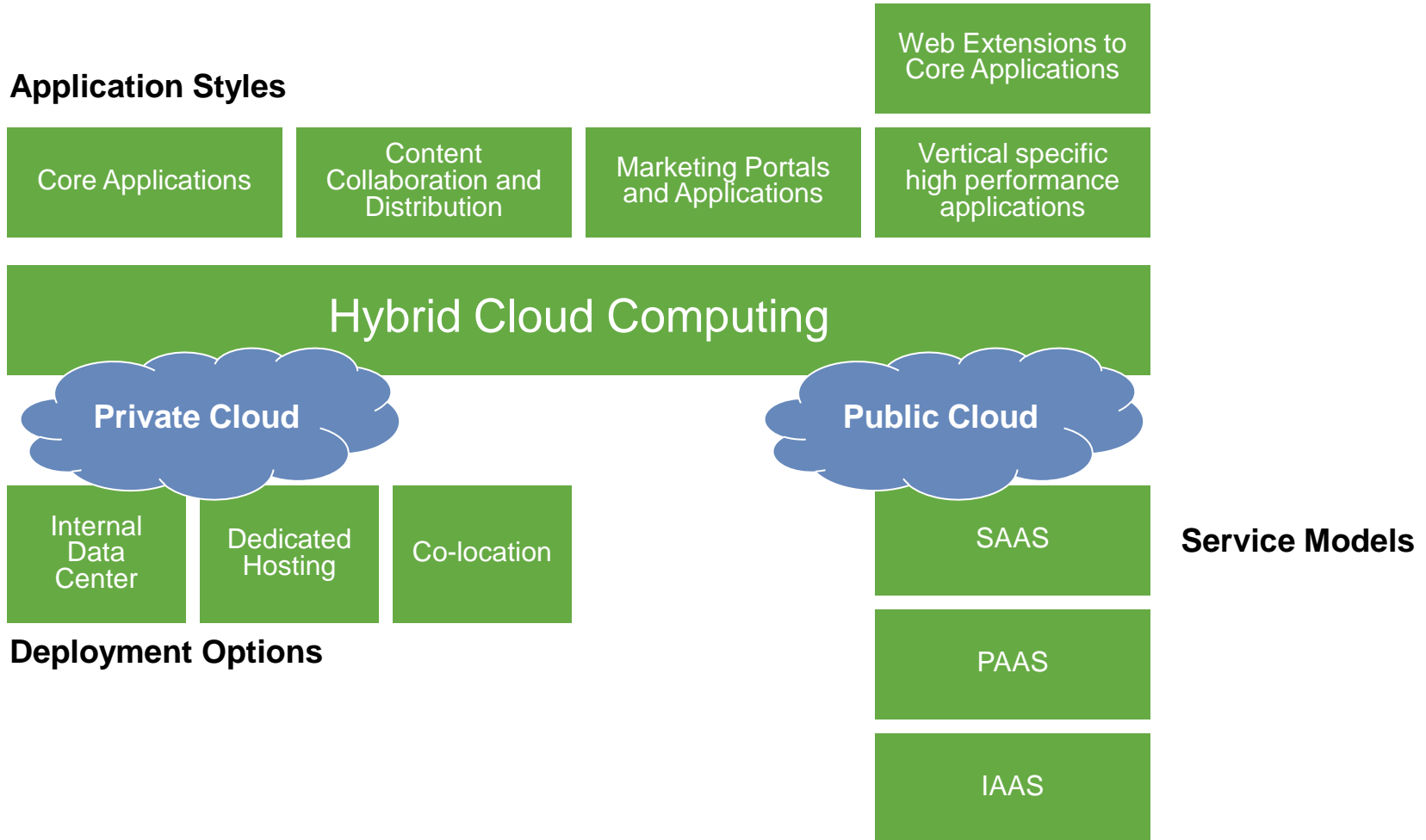
Expect to share responsibility

- Clarify roles (data controller, data processor, cloud provider, systems integrator)
- Cloud providers must share the risk and data owners must bear their legal obligations
- Choose a cloud model that works for you

Regulatory Compliance Burden



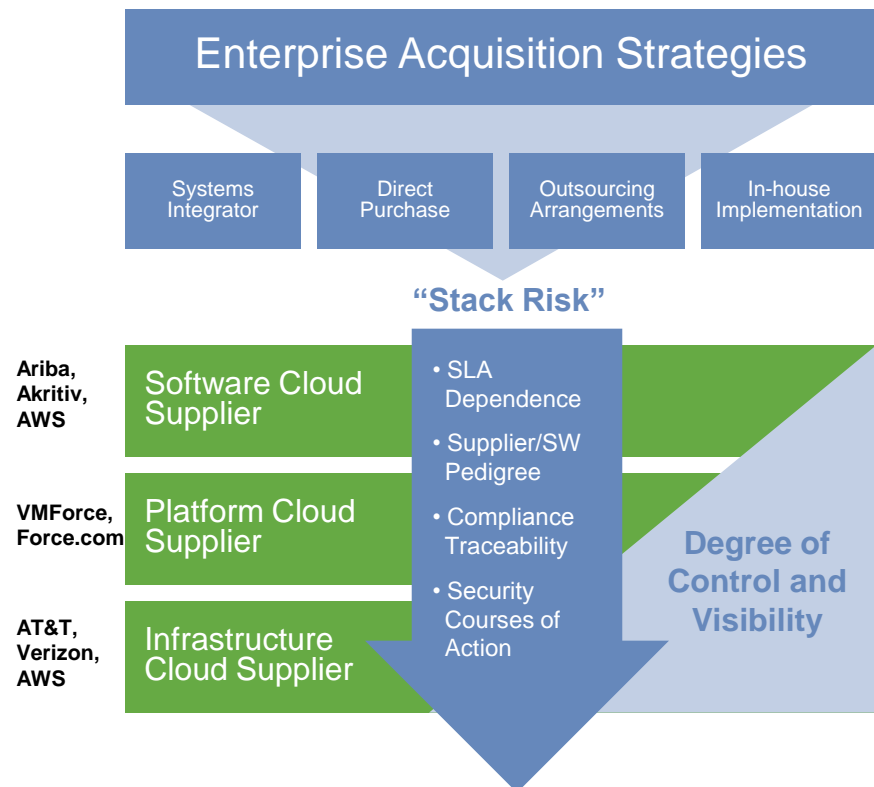
Hybrid business models




Demand transparency and accountability from cloud providers

- Require reasonable transparency & accountability
- Cloud providers as customers may lack visibility into the other provider's security
- Ask questions from the bottom up (through technology) and the top down (through security, compliance, governance)

The deeper the stack, the less visibility you have



Use the cloud to solve identity and access management issues



- Shift identity approach for added complexity of the cloud.
- Identity management might soon become a cloud service.
- Tie privileges to roles, not applications.
- Authenticate people, supporting processes, software.



Architect solutions that address the risk

- Consider hybrid cloud as a bridge solution for now.
- Evaluate each application individually.
- Implement security through a blend of methods:
 - Apply data encryption.
 - Limit the information sent to the cloud.
 - Mask sensitive information.
 - Consider multiple cloud vendors.
 - Apply encryption and/or tokenization at a proxy server.



Our point of view



It depends on the data

- Non-regulated, non-personal data
 - Few barriers to cloud use.
- Regulated, personal data
 - Regulatory compliance requires more than good security.
 - Security requires more than regulatory compliance
- Control is an illusion



Important principles

- Obtain necessary contractual terms.
- Understand privacy laws, ensure no violations.
- Involve the right people.
- Prohibit ad hoc cloud computing (or at the very least, audit).
- Read terms of service and then read them again.
- Have a backup plan



The day is coming ...

- Accenture is helping cloud providers understand regulatory environment.
- Providers will begin to accept necessary contractual requirements.
- You **must** recognize taking “smart” risk as a positive behavior.
- Companies will safely put more on the cloud, gaining immediate economic benefits.

Contact us

Joe Tobolski

Senior Director for Data & Platforms R&D

Accenture Technology Labs

joseph.f.tobolski@accenture.com