Risk and Controls for SaaS

Robert Fly
Vice President, Product Security

Crispen Maung
Technology Audit & Compliance
Senior Director

Your success.
Our cloud.

SOFTWARE

salesforce.com

Safe Harbor

Safe harbor statement under the Private Securities Litigation Reform Act of 1995: This presentation may contain forward-looking statements that involve risks, uncertainties, and assumptions. If any such uncertainties materialize or if any of the assumptions proves incorrect, the results of salesforce.com, inc. could differ materially from the results expressed or implied by the forward-looking statements we make. All statements other than statements of historical fact could be deemed forward-looking, including any projections of subscriber growth, earnings, revenues, or other financial items and any statements regarding strategies or plans of management for future operations, statements of belief, any statements concerning new, planned, or upgraded services or technology developments and customer contracts or use of our services.

The risks and uncertainties referred to above include – but are not limited to – risks associated with developing and delivering new functionality for our service, our new business model, our past operating losses, possible fluctuations in our operating results and rate of growth, interruptions or delays in our Web hosting, breach of our security measures, the outcome of intellectual property and other litigation, risks associated with possible mergers and acquisitions, the immature market in which we operate, our relatively limited operating history, our ability to expand, retain, and motivate our employees and manage our growth, new releases of our service and successful customer deployment, our limited history reselling non-salesforce.com products, and utilization and selling to larger enterprise customers. Further information on potential factors that could affect the financial results of salesforce.com, inc. is included in our annual report on Form 10-K for the most recent fiscal year ended January 31, 2011. This documents and others are available on the SEC Filings section of the Investor Information section of our Web site.

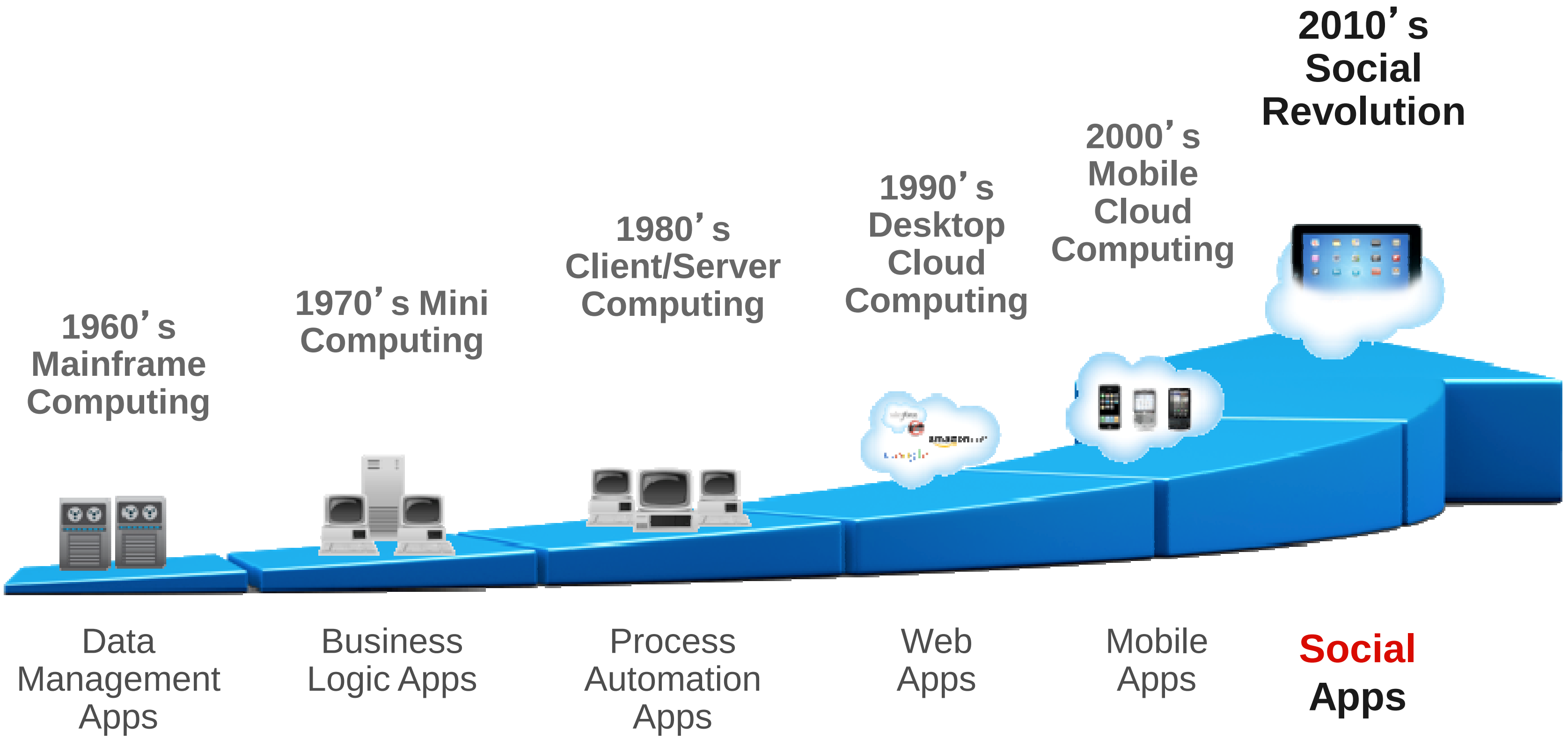
Any unreleased services or features referenced in this or other press releases or public statements are not currently available and may not be delivered on time or at all. Customers who purchase our services should make the purchase decisions based upon features that are currently available. Salesforce.com, inc. assumes no obligation and does not intend to update these forward-looking statements.

Agenda

- Intro
- State of Cloud Computing
- CSA Domains
  - Risks and Controls
- Auditing Tips

Ten Year Computing Cycles

10X more users with each cycle



1960’s Mainframe Computing

Data Management Apps

1970’s Mini Computing

Business Logic Apps

1980’s Client/Server Computing

Process Automation Apps

1990’s Desktop Cloud Computing

Web Apps

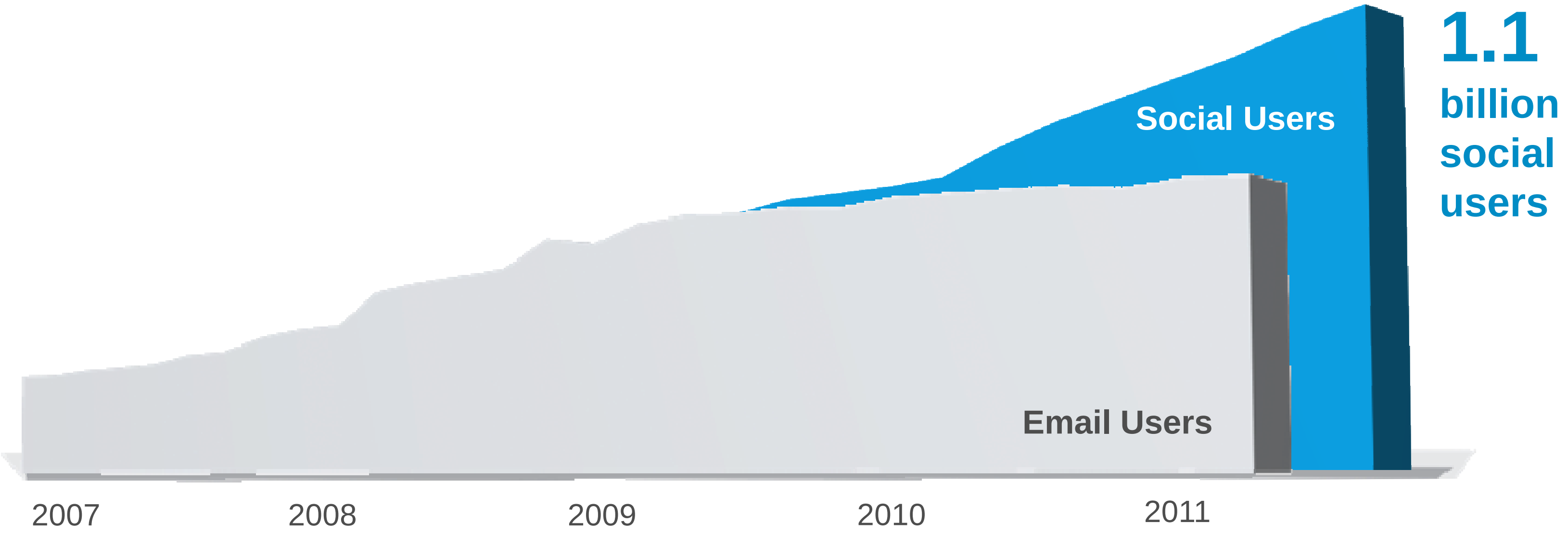
2000’s Mobile Cloud Computing

Mobile Apps

2010’s Social Revolution

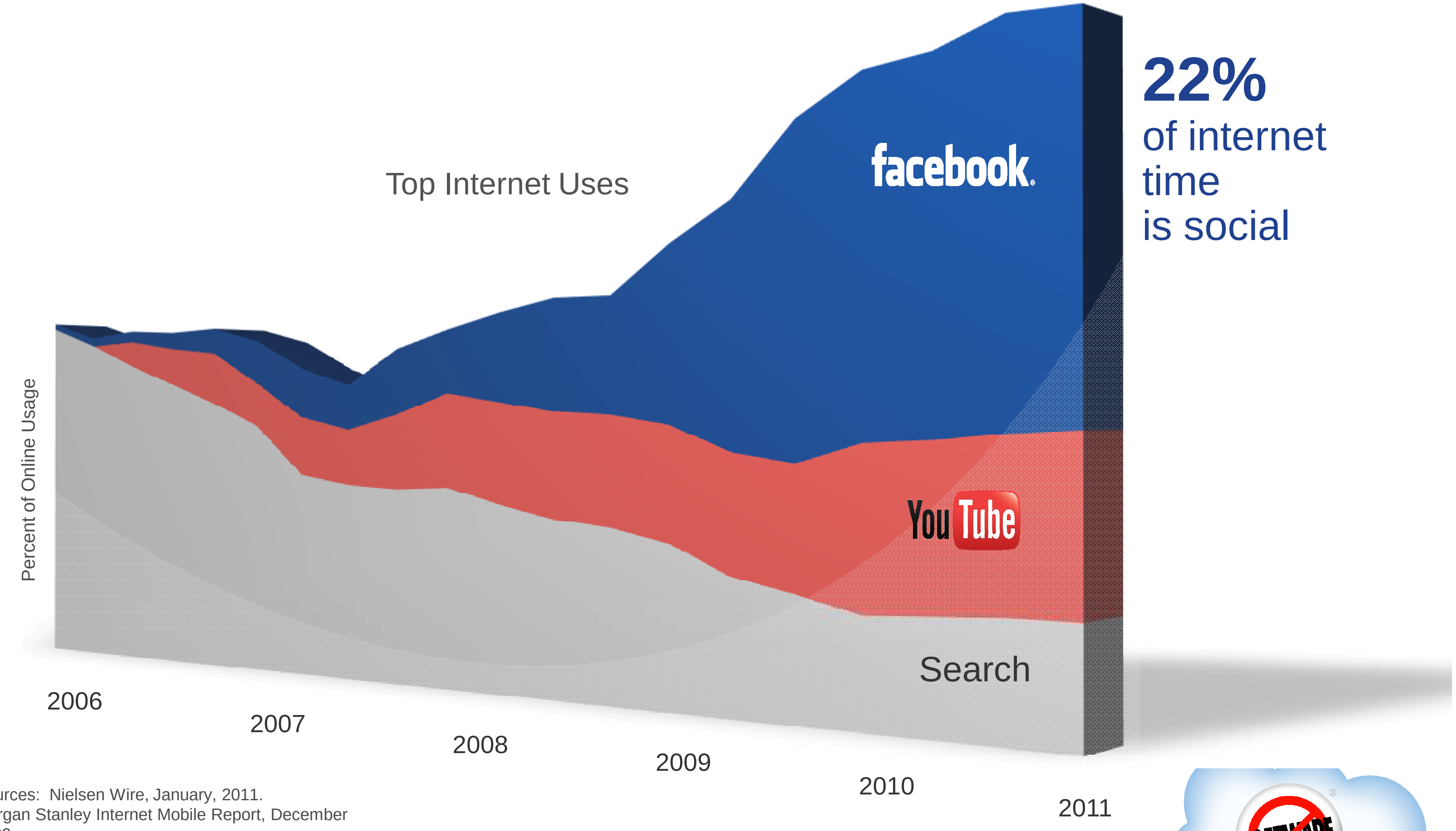
Social Apps

Social Revolution: Social Networking Surpasses Email



Source: Comscore, June 2011

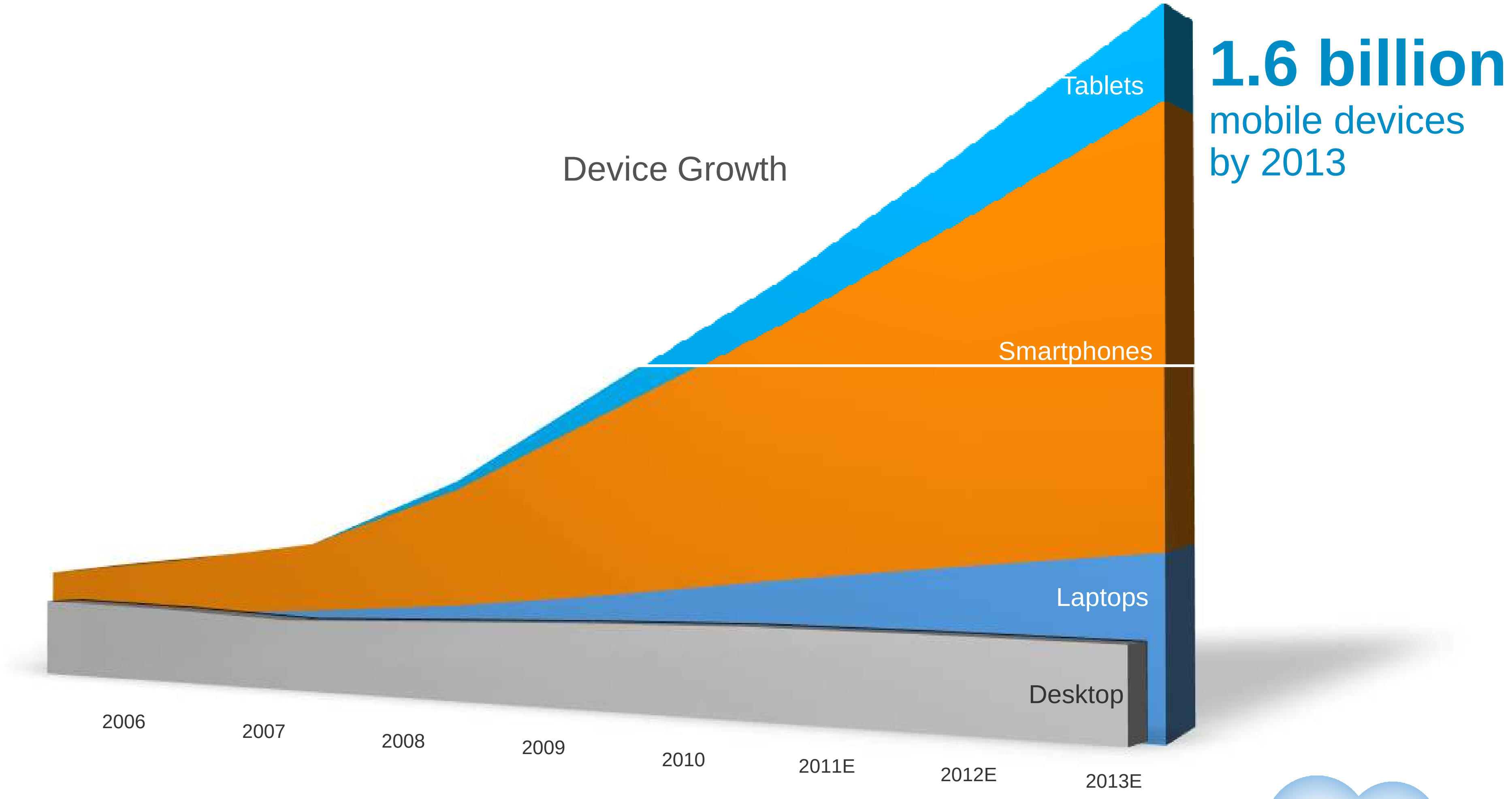
Social Revolution: Facebook Eats the Web



22%
of internet
time
is social

Sources: Nielsen Wire, January, 2011.
Morgan Stanley Internet Mobile Report, December 2009

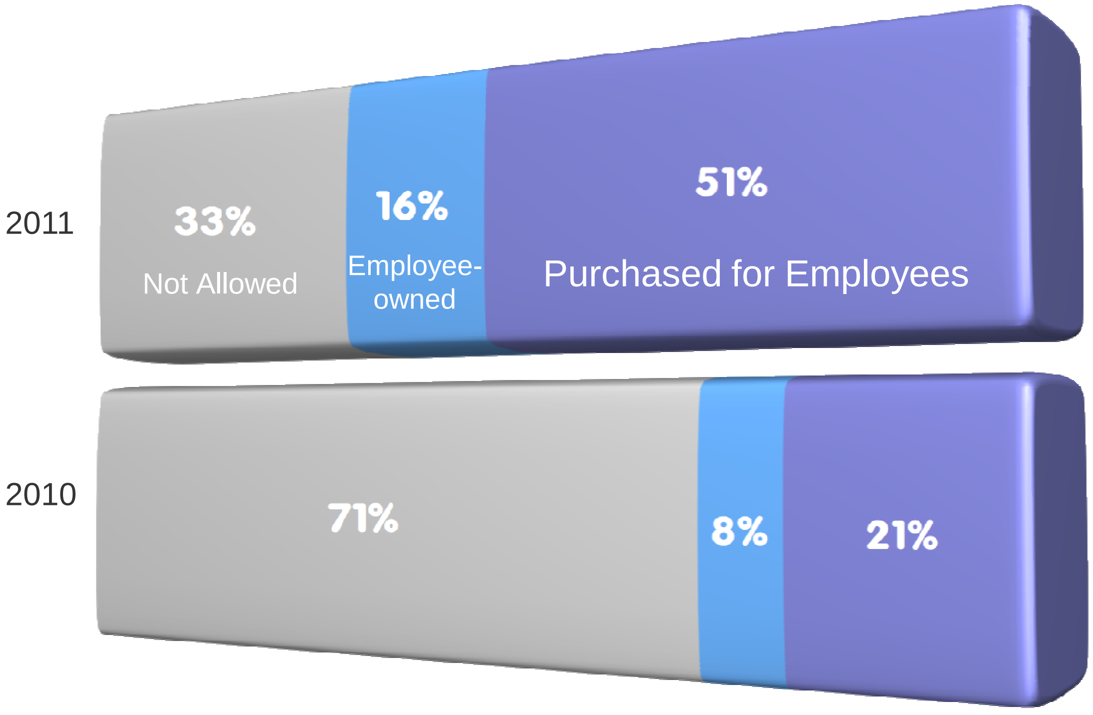
Social Revolution: Next Generation Devices Changing How We Access the Web



Source: Gartner Research; Smartphone, Tablet, and PC Forecast, December 2010.

Social Revolution: Employees Forcing an Unprecedented Pace of Change

CIOs Surveyed on Tablet Usage

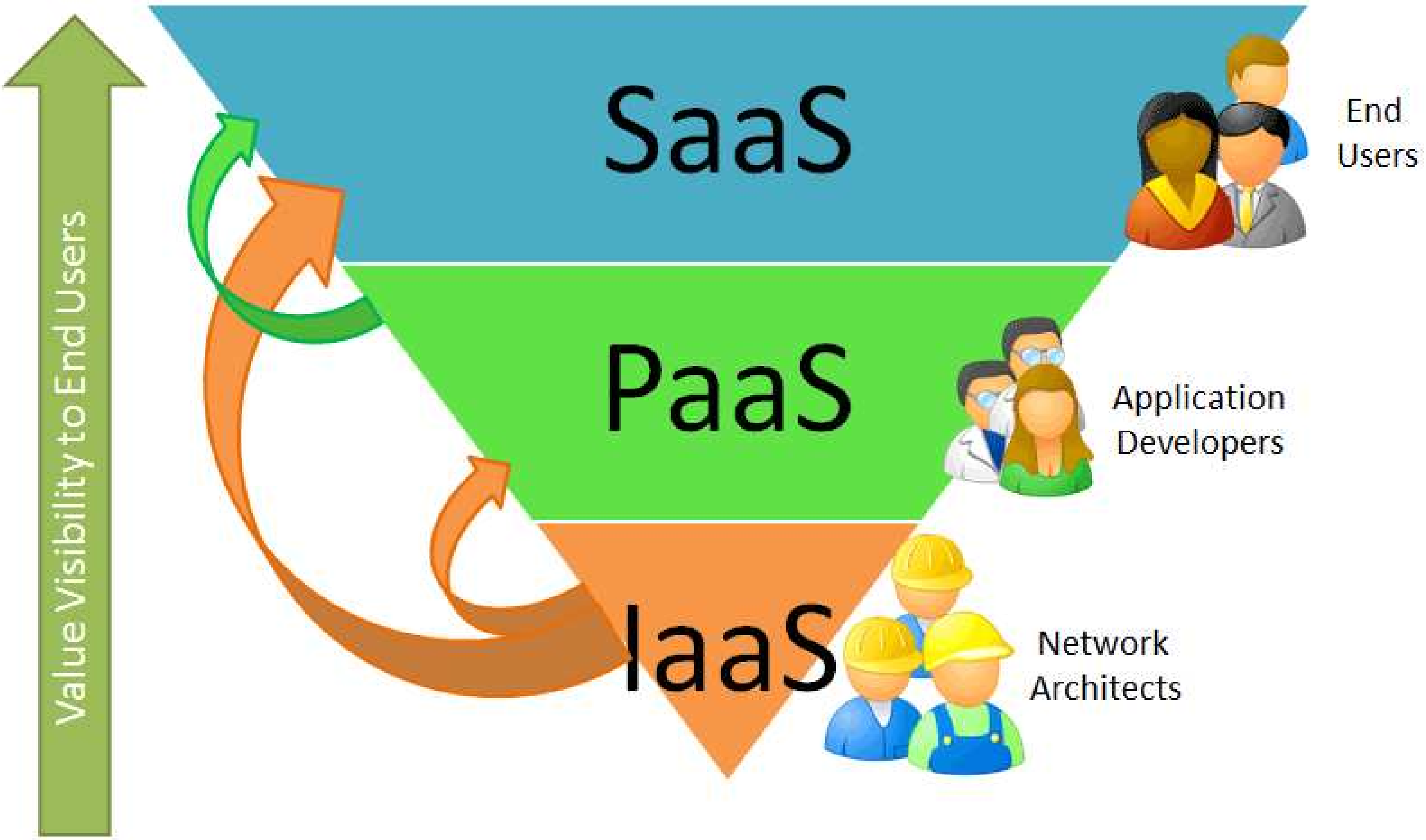


“...fastest ramping mobile device ever.”

Morgan Stanley

Morgan Stanley, “Tablet Demand and Disruption”, February 14, 2011.

Cloud Anatomy



Value Visibility to End Users

SaaS

End Users

PaaS

Application Developers

IaaS

Network Architects

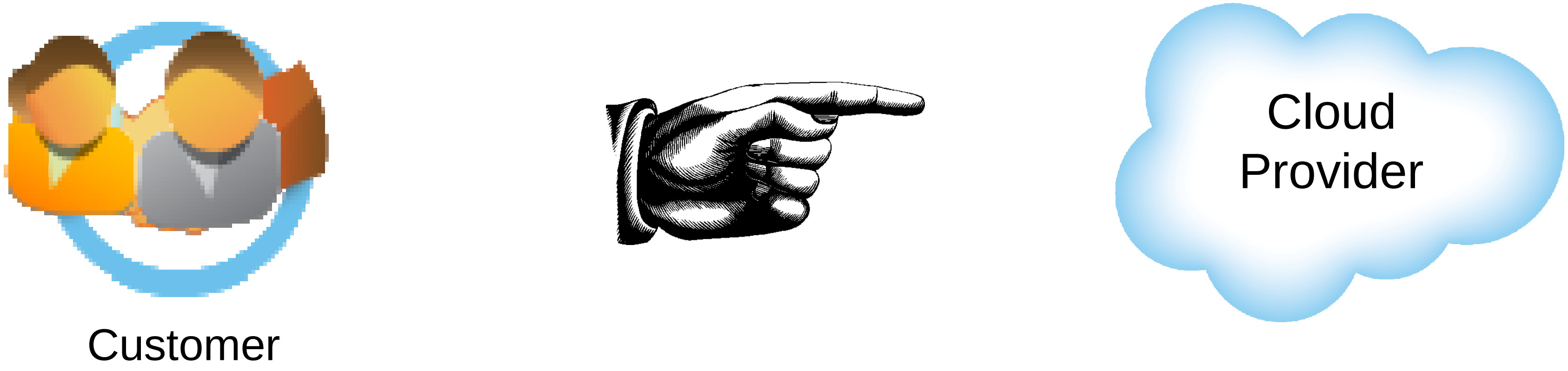
Control Ownership Clarity

CONTROL OWNER?	SaaS	PaaS	IaaS
Data	Joint	Tenant	Tenant
Application	Joint	Joint	Tenant
Compute	Provider	Joint	Tenant
Storage	Provider	Provider	Joint
Network	Provider	Provider	Joint
Physical	Provider	Provider	Provider

Finger Pointing Exercise

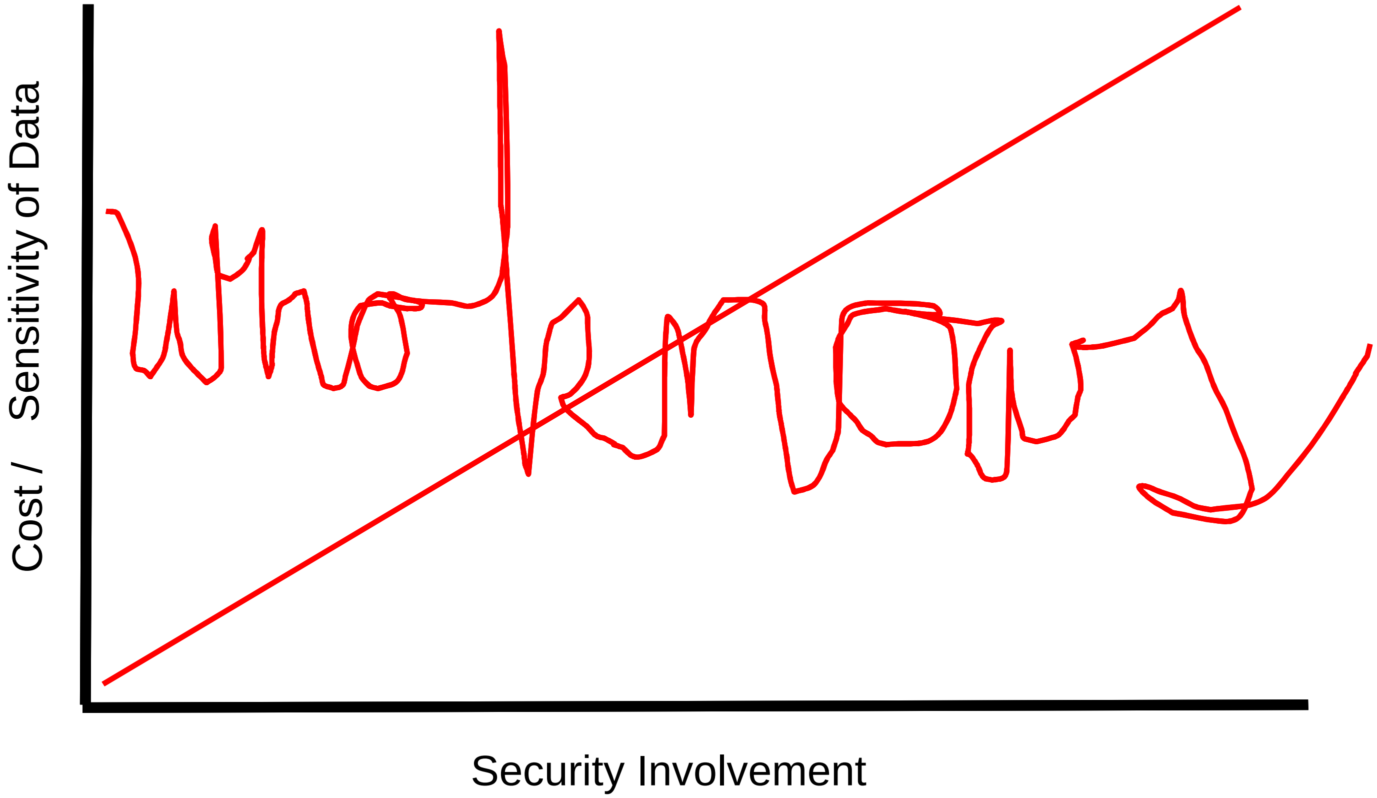
Customer’s Password Compromised

Service Outage



Customer Employee Downloads All Data

Security & Audit Involvement



CSA Domains

Sections:

Cloud Architecture

Governing in the Cloud

Operating in the Cloud

CSA Domains

Section I - Cloud Architecture

Domain 1: Cloud Computing Architectural Framework

Cloud Computing Architecture

The Cloud Is

Less Secure

The Cloud Is

More Secure

Context

We hold these truths to be self-evident, that not all clouds are created equal.

Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah
Blah blah blah blah blah blah Blah blah blah blah blah blah Blah blah blah blah blah blah Blah

CSA Domains

Section II - Governing in the Cloud

Domain 2: Governance and Enterprise Risk Management
Domain 3: Legal and Electronic Discovery
Domain 4: Compliance and Audit
Domain 5: Information Lifecycle Management
Domain 6: Portability and Interoperability

Governance and Enterprise Risk Management

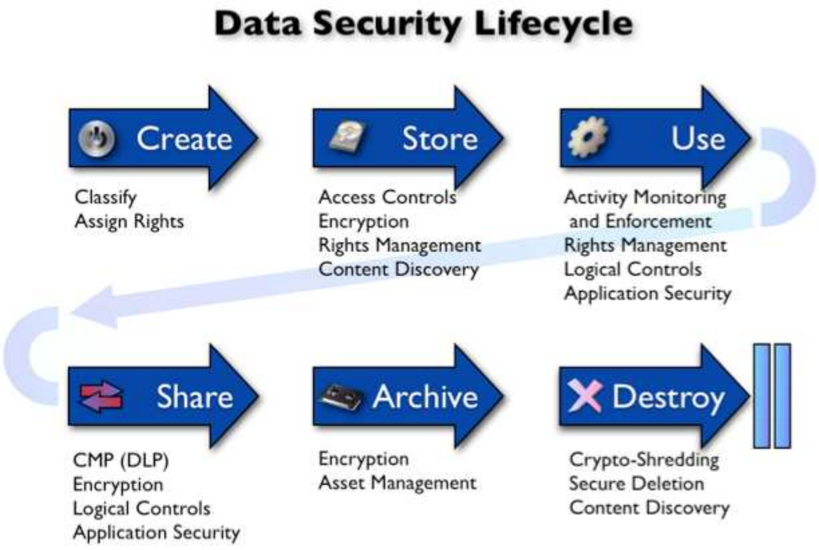
- The identification and implementation of the **appropriate** organizational structures, processes, and controls to maintain effective information security governance, risk management, and compliance.
- Assure reasonable information security across the **information supply chain**
- Governance Recommendations
  - Re-investment of cost savings
  - Robust information security governance
  - Assessed for sufficiency, maturity, and consistency
  - Collaborative governance structures
  - Service Level Agreements and contractual obligations
  - Metrics and standards for measuring performance and effectiveness
  - Documented and demonstrable

Legal and Electronic Discovery

- A complete analysis of Cloud Computing-related legal issues requires consideration of functional, jurisdictional, and contractual dimensions – BY YOUR LEGAL TEAM.
  - Data Residency
  - Other Regulatory Requirements
  - Encryption and/or Mashup capabilities
- Electronic Discovery
  - What can you do yourself?
  - How long are logs kept for?
  - Investigative support?
  - API accessible?

Information Lifecycle Management

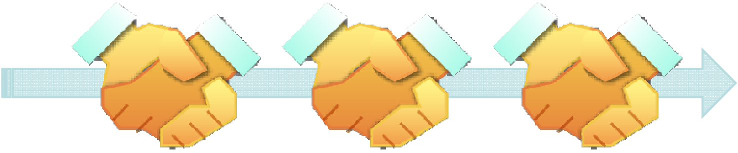
- Data Security
  - DLP
  - Data Discovery
  - Federation
- Location of Data
- Data Recovery – Sidekick/Danger
- Data Destruction – Facebook (Max Schrems)



Compliance and Audit

- Organizations should also assure reasonable information security across the information supply chain, encompassing providers and customers of Cloud Computing services and their supporting third party vendors, in any cloud deployment model.

Customer’s must have a 360°



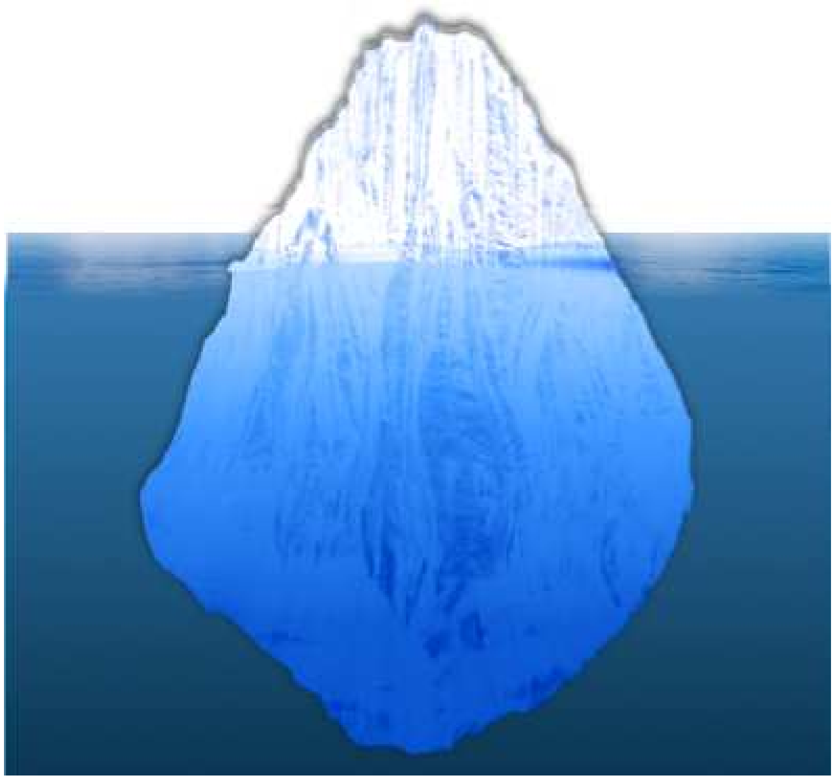
PaaS / SaaS
User

PaaS / SaaS
Provider

PaaS / SaaS
Sub contract
services

Focus on the “information
supply chain”

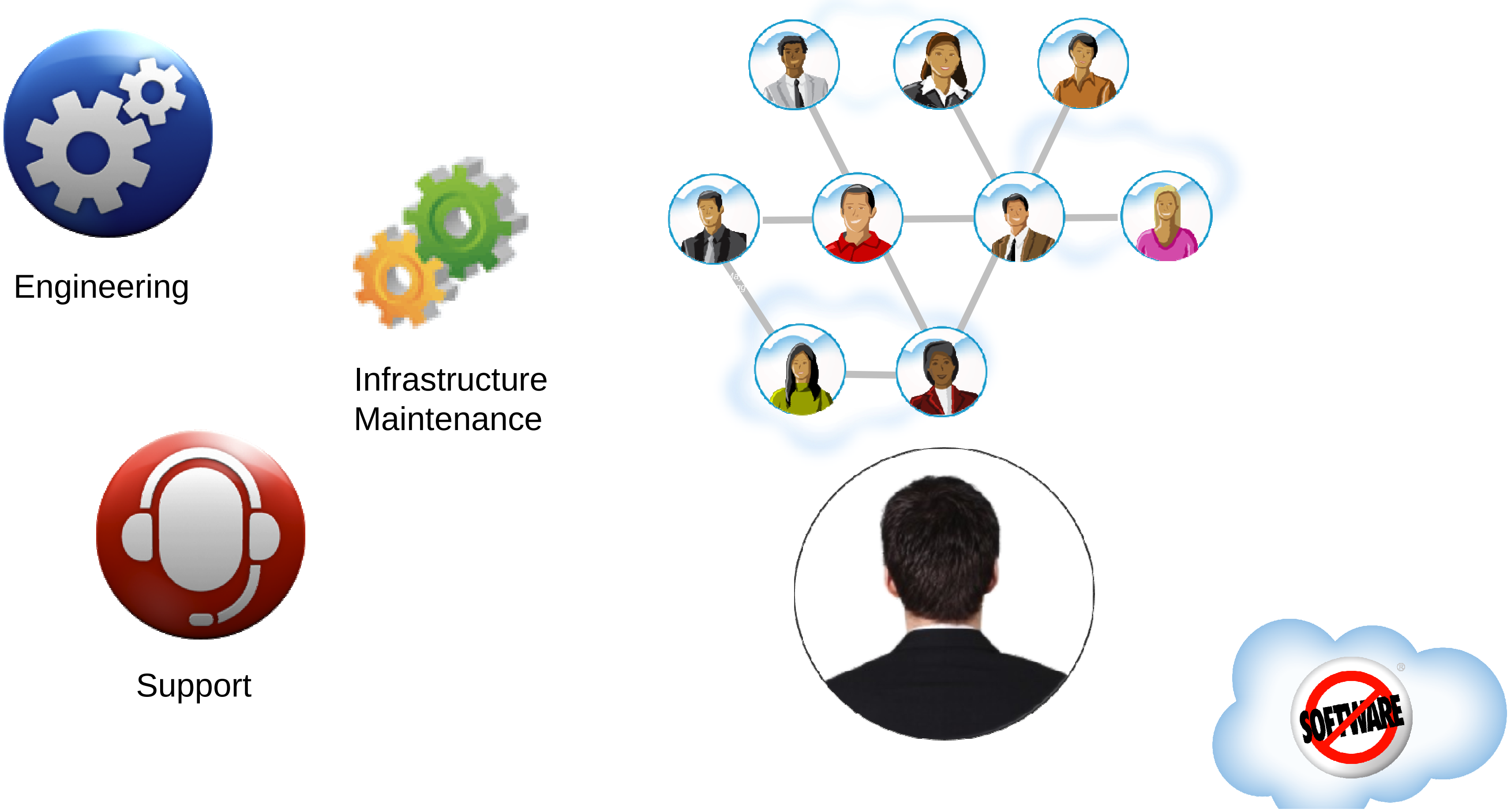
Compliance and Audit



Most of the security risk may be out of sight

Compliance and Audit

- Providers may leverage sub-contractors / other 3rd parties to deliver the service



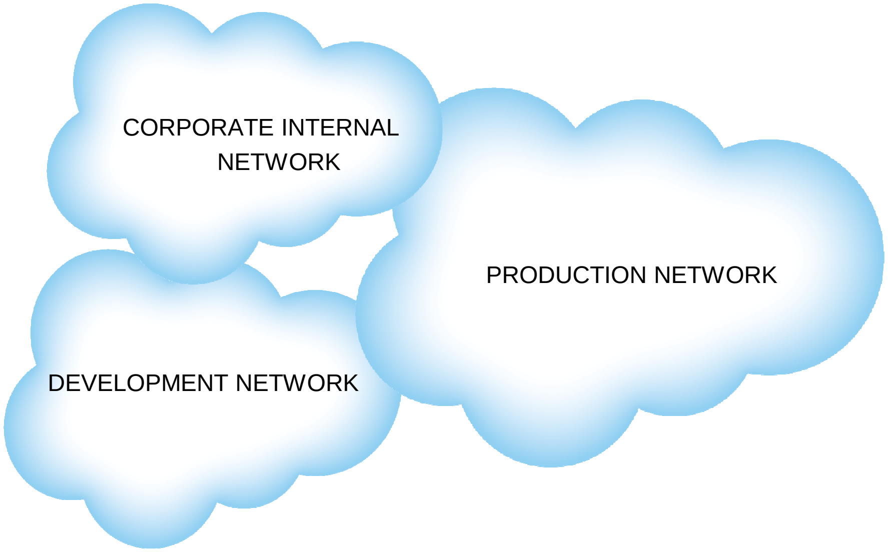
Engineering

Infrastructure Maintenance

Support

Compliance and Audit

Control Frameworks



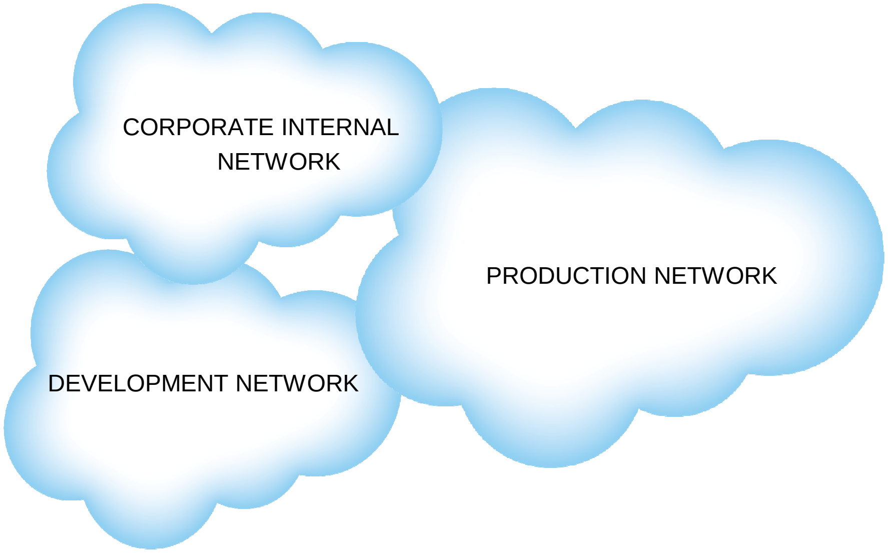
What controls do you apply?

Are there any models that you can leverage?

- CobIT
- ITIL
- ISO 27001:2005
- SAS 70 / SSAE 16
- NIST 800-53

Compliance and Audit

Control Frameworks



ISO 27001:2005

- Security Policy
- Organization of information security
- External parties
- Asset management
- Information classification
- Human resources security
- Physical and environmental security
- **Communications and operations management**
- Access control
- Information system acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

Compliance and Audit

- **ISO 27001:2005**
- **10. Communications and operations management**
  - 10.2 Third party service delivery management
  - 10.2.1 Service Delivery
    - It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party
  - 10.2.2 Monitoring and review of third party services
    - The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.

Portability and Interoperability

- Various companies will in the future suddenly find themselves with urgent needs to switch cloud providers for varying reasons, including – cost increases, RIP, SLA not being met, etc.
- Are you a platform? “Steve Yegge Rant”
- Open Source vs Open APIs vs Open Standards
- Data Extraction
  - Automated Data Pulls?
  - MetaData?
  - Access Records?
- Mobile Proliferation
  - Stolen Devices
  - Encryption

CSA Domains

Section III. Operating in the Cloud

Domain 7: Traditional Security, Business Continuity, and Disaster Recovery
Domain 8: Data Center Operations
Domain 9: Incident Response, Notification, and Remediation
Domain 10: Application Security
Domain 11: Encryption and Key Management
Domain 12: Identity and Access Management
Domain 13: Virtualization

Traditional Security, BCP, DR

- The lack of transparency within Cloud Computing requires that BCP and DR professionals be continuously engaged in vetting and monitoring your cloud providers
- Confirm that the provider has an approved, current and implemented BCP / DR Policy
- Evidence of active management support and periodic review of the BC and DR Programs to ensure that the BC / DR Programs are active
- Evidence that the BC and DR programs are tested
- Inclusion of customers in the testing of these plans

Data Center Operations

- The challenge for consumers of cloud services is how to best evaluate the provider’s capabilities to deliver appropriate and cost-effective services, while at the same time protecting the customer’s own data and interests
  - Configuration Management
  - Change Management
  - Scalability & Capacity Planning
  - Patch Management
    - 3rd Party Code in the app tangent
  - Infrastructure Tools – IDS, DB Monitoring, etc
    - Who monitors? How are they alerted? What is the SLA to high risk alerts?
  - Access to Infrastructure

Incident Response, Notification and Remediation

- Flaws in infrastructure architecture, mistakes made during hardening procedures, and simple oversights present significant risks to cloud operations.
- “If a critical vulnerability is found or exploited how quickly can it be remediated?”
- Who are you notifying?
- How Fast???
- Transparency
- Customer Features

Application Security

- 75% of attacks are at the application layer (Gartner)
- Security Development Lifecycle
  - Tools
  - Training
  - Frameworks
  - “Done” requirements
- Vulnerability Assessments & Penetration Tests
  - Internal
  - External
  - Customer

Application Security

- Features
  - Security Features
    - Encryption Options
    - Appropriate Auditing/Logging
    - Granular Access Control
    - Restricted Network Access
    - "Opt-Out" Upgrades & Pre-Release Testing
  - Security Monoculture
    - Access URLs (eg: customer.my.salesforce.com)
    - Authentication Options
    - Access Restrictions (eg: IP Address Locking)

Encryption and Key Management

- Strong encryption is one method that Cloud Computing systems can use to protect data. While encryption itself doesn’t necessarily prevent data loss, safe harbor provisions in laws and regulations treat lost encrypted data as not lost at all.
- What data are you storing?
- Key Management
  - Who holds the keys? How are they rotated? Stored? Backed up?
- Algorithms & Crypto Agility

Identity and Access Management

- Extending an organization’s identity services into the cloud is a necessary precursor towards strategic use of on-demand computing services
- Provisioning
  - New User onboarding & employee deprovisioning
- Authentication
  - Multi-Factor
  - SAML, OAuth, etc
  - Mobile
- Authorization & Granularity
- How do they integrate into *your* tools

Virtualization

- Multitenancy
- *Extremely Important*
- Generally two types (VM and DB)

VM

Are there any shared resources outside of VM?
How are these secured?
VM Patching?
Defense in Depth Measures?

Database

How is data separated?
How are appropriate DB queries audited?
Defense in Depth Measures?

Virtualization

Select firstname from Contacts where firstname = ‘Frank’

and customer = ‘Acme’

How is this ensured?

Good Answers
Code Reviews
Parameterized Queries
Stored Procedures
Datastore abstraction
Build Automation
Data Verification
Automated Tools Testing
Static Analysis
Etc

http://www.example.com/importantsite/page.jsp?accountId=12345

Auditing Tips

- Spend time planning the audit and focuses on the service provided and known areas of risk for your company
- Ensure that you have specific security requirements to audit against that cannot be subject to miss interpretation
- Make sure that the security requirements are documented and that there is a contractual obligation on the side to the provider to meet those security requirements
- Keep and watchful eye on how your company uses the cloud provider, as it will change over time. Consequently the security controls and areas of risk will change.
- Ensure that the audit teams are aware of any changes in the security requirements
- Ensure that you use knowledgeable auditors who have experience in auditing cloud computing providers before
- Audit with peripheral vision – don’t be myopic in your audit approach or checklist driven

Questions