Agenda

1. Session Overview
2. Cloud Security
3. Summary and Conclusion

2

Session Agenda

- Session Overview
- Cloud Security
- Summary & Conclusion

3

What is the class about?

- Course description and syllabus:
  - » http://www.nyu.edu/classes/jcf/CSCI-GA.3033-001/
  - » http://www.cs.nyu.edu/courses/summer12/CSCI-GA.3033-001/
- Session 8 Reference material:
  - » Security-related links as noted in presentation

4

Icons / Metaphors

- Information
- Common Realization
- Knowledge/Competency Pattern
- Governance
- Alignment
- Solution Approach

5

Agenda

1. Session Overview
2. Cloud Security
3. Summary and Conclusion

6

Agenda: Cloud Security

- Cloud security challenges
- Cloud security approaches
  - Encryption
  - Tokenization/obfuscation
  - Cloud security alliance standards
  - Cloud Security models and related patterns
- Cloud security in mainstream vendor solutions
- Mainstream Cloud security offerings
  - Security assessment
  - Secure Cloud architecture design
- Cloud security project: Ongoing programming project (Part V – Builds on Part IV)
  - Design a secure Cloud architecture to support the deployment of a secure version of the course project application.

7

Cloud Ecosystem Model – Predicted Evolution

By 2012, many of the fears associated with IaaS (transaction and data/security integrity) are resolved, with customers realizing that its value lies less with cost savings and more with agility (for large enterprises), service levels and compliance for SMBs.

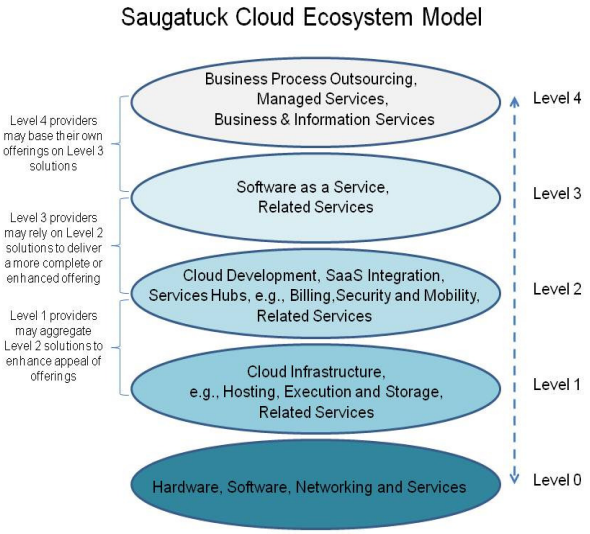
Level 4: BPO / Managed Services. *Specialized expertise often delivered in conjunction with a Cloud-based solution, e.g., Mobility as a Service, Cloud-based security.*

Level 3: SaaS (Waves I-III) and related services. *Business solutions delivered from the Cloud, typically in a multi-tenant architecture, and billed under subscription model.*

Level 2: Cloud development, PaaS, SaaS integration, Service Hubs, *including billing, administration, aggregation, security and mobility solutions, systems and infrastructure management, data warehousing, data access and analysis, and related professional services.*

Level 1: Cloud-based On-Demand infrastructure providers and platforms *that host SaaS and other on-demand solutions and provide service offerings to manage infrastructure platforms (collocation);*

Level 0: Suppliers *of hardware, system software and utilities, data center management software, networking equipment, hardware and software, and associated services*

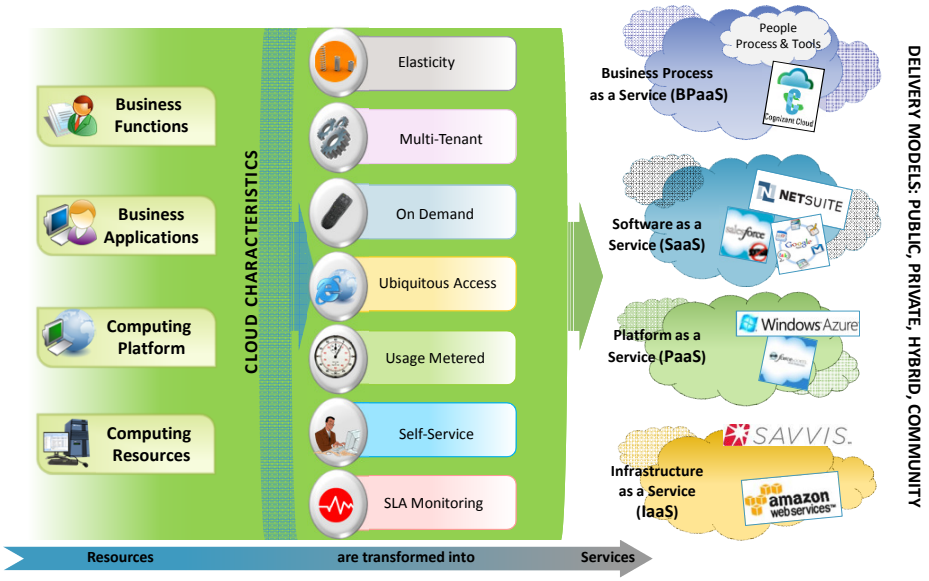


Source: Saugatuck Technology

8

Evolutionary Model of Cloud Computing

An evolutionary model where resources are consumed and accessed as service over a network



9

A Myriad of Challenges (1/3)

Topic	Points to consider
Privacy	▪ Cloud provides control and can monitor "at will" all the communications (i.e., access to data?)
Compliance	▪ Community or hybrid deployment modes are required which are typically more expensive and may offer restricted benefits ▪ Regulatory compliance
Security	▪ Multi-tenancy of service, data and process require clear governance ▪ Cloud trust models - trusted security and information insurance may require to know what is occurring inside the "black box" of a cloud offering to ensure secure operations ▪ Application/system security ▪ Risk assessments
Legal	▪ Significant number of trademark filings since 2007
Availability and Performance	▪ Business concerns around acceptable performance and cloud providers shutting down, maturity is evolving ▪ Singular dependence on network-based offerings raises a question as to business continuity when the network is unavailable or unreliable

10 10

A Myriad of Challenges (2/3)

Topic	Points to consider
Control	▪ Ownership; Perception of 'relinquishing' control to third party ▪ Change; change to transformation timeline and process
Maturity	▪ Evolving standards making it difficult to achieve vendor neutrality ▪ Evolving technologies and business models ▪ Evolving vendors providing Cloud service and deployment models and vendor lock-in is a risk with the current maturity of cloud computing (vendors survivability, chaining of outsourcing,
Governance	▪ Key factors such as data Integrity, monitoring, auditing and financial controls
Architecture	▪ Availability of Platform, Application Support ▪ Security Access Levels ▪ Vendor Product Licensing model
Applications	▪ Applications licensing in a virtual world ▪ Application migration ▪ Application criticality
Multi-tenancy	▪ Multi-Tenant Software Usage Model ▪ Multi-Tenant Application Instance Model ▪ Multi-Tenant Infrastructure Sustain Model

11

11 11

A Myriad of Challenges (3/3)

Topic	Points to consider
Workload Type	▪ Customer facing UI ▪ Batch jobs ▪ High performance apps ▪ Application performance sensitive to variations
Communication between layers	▪ Asynchronous ▪ Standards based ▪ Enterprise connectivity
Development	▪ Vendor lock-in platform specific API's ▪ Support for development, Unit Testing ▪ Learning curve to adopt – Google App Engine, Force.com ▪ Vendor support – Availability of forums, documents
Access to data	▪ Need to relational database ▪ Large data storage
Provider restrictions	▪ No of instances that can be created ▪ Autoscaling
Technical Considerations	▪ Hardware platform ▪ Operating System ▪ Bandwidth required ▪ Performance and capacity ▪ Storage ▪ Enterprise management and monitoring (automating the solution)

12

12 12

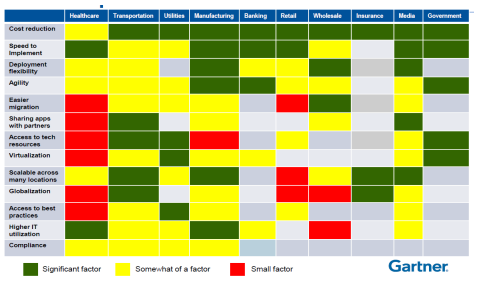
Cloud Challenges and Security

- … Security & Trust issues…
  - » See handout "Understanding Cloud Security Challenges"
- Application Software Engineering
  - » Cost of Developing Applications (of various types)
  - » Cloud-Enabling Legacy Apps
- Application Deployment and Execution Management
  - » Dynamic Resource Provisioning in Elastic Manner
  - » Cost Minimisation
  - » Performance / Quality / SLA
- Multiple Platforms and Application Scalability
  - » Brokering Across Multiple Clouds
    - Private, Public, Inter Clouds
  - » Seamless scalability
    - to support varied workloads, users, QoS req.

13

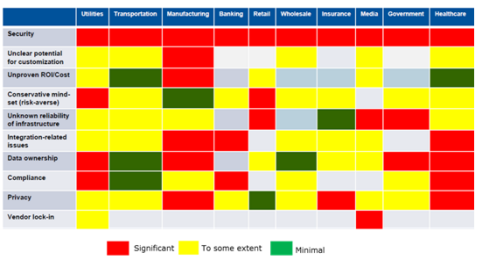
Top Drivers and Challenges – Also See Handout "Reimaging IT"

Capex funding pressures, changing business conditions, driving operational efficiency and organizational development are the key focus areas across verticals



Drivers

- Cost reduction
- Speed to Implement
- Deployment flexibility
- Agility
- Higher IT utilization
- Scalable across locations



Challenges

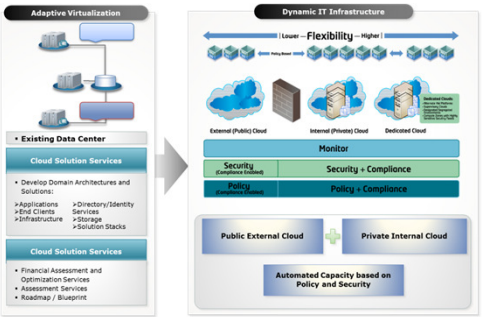
- Conservative mind-set (risk-averse)
- Vendor lock-in
- Data ownership
- Privacy & Compliance
- Security
- Integration issues

14

Sample Secure Private Cloud Implementation

Design

- Custom design based on business requirements, proven reference architectures, and best practices.
- Optimized across best-of breed and client-preferred vendors.
- Defines network, system, and storage requirements, as well as security, provisioning, event and performance management.
- Produces a full BoM ready for vendor order placement and implementation.



Deployment

- Develops a Private Cloud infrastructure in a physical datacenter location, which can be either within client datacenter or in hosted co-location facility.
- Includes deployment, configuration, and testing of physical assets, as well as Physical to Virtual (P2V) Factory, if required.
- Identifies opportunities for enhancement based on detailed comparison to reference architectures.

15

Cloud Security Approaches

- Encryption
- Tokenization/obfuscation
- Cloud security alliance standards
- Cloud Security models and related patterns

16

Encryption vs. Obfuscation?

- Encryption here refers to some method of modifying data so that it is meaningless and unreadable in it's encrypted form
  - » It also must be reasonably secure, that is it must not be easily decrypted without the proper key.
- Anything less than that will be referred to as *obfuscation*
  - » This is data that is rendered unusable by some means, but is not considered as a serious form of encryption

17

Is Encryption Necessary?

- Data encryption is a hot topic these days
  - » Hardly a new subject
  - » Has received and increasing amount of attention largely due to ecommerce
  - » Protecting credit card numbers, medical data and other sensitive information has become more important than ever before, and on a larger scale
- It is important to consider some related decisions that need to be made first
  - » It may become clear that encryption is not necessarily what is required
  - » Decide first before launching into a discussion on algorithm choices and methods of implementing encrypt

18

Why Obfuscation vs. Strong Encryption Algorithm - Example

- A good example would be an audit report on a medical system
  - Report may be generated for an external auditor, and contain sensitive information
  - The auditor will be examining the report for information that indicates possible cases of fraud or abuse
- Assumption
  - Management has required that Names, Social Security Numbers and other personal information should not be available to the auditor except on an as needed basis
  - Data needs to be presented to the auditor, but in a way that allows the examination of all data, so that patterns in the data may be detected

19

Why Obfuscation vs. Strong Encryption Algorithm - Solution

- Encryption would be a poor choice in this example, as the data would be rendered into ASCII values outside of the range of normal ASCII characters
  - This would be impossible to read
- A better choice might be to obfuscate the data with a simple substitution cipher
  - While this is not considered encryption, it may be suitable for this situation
- When the auditor finds a possible case of abuse, he will need the real name and SSN of the party involved
  - He could obtain this by calling a customer service representative at the insurance company that supplied the report, and ask for the real information
- The obfuscated data is read to the customer service rep, who then inputs it into an application that supplies the real data
- The importance of using pronounceable characters becomes very clear
  - Strong encryption would render this impossible

20

Why Obfuscation vs. Strong Encryption Algorithm - Sample Program

```
create  or replace package obfs
is
   function obfs( varchar2 in ) return varchar2;
   pragma restrict_references( obfs, WNPS, WNDS );
   function unobfs( varchar2 in ) return varchar2;
   pragma restrict_references( unobfs, WNPS, WNDS );
end;
/
create or replace package body obfs
is
    xlate_from varchar2(62) := '0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz';
    xlate_to varchar2(62) :=      'nopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklm';

function obfs ( clear_text_in varchar2 ) return varchar2
is
    begin
        return translate( clear_text_in, xlate_from, xlate_to );
    end;
function unobfs ( obfs_text_in varchar2 ) return varchar2
Is
    begin
        return translate( obfs_text_in, xlate_to, xlate_from );
    end;
end;
/
```

21

Why Obfuscation vs. Strong Encryption Algorithm - Sample Output

```
SSN        OBFS SSN
---------- ----------
540407786  srnrnuuvt
542800170  srpvnnoun
542802063  srpvnpntq
541466830  srorttvqn
```

As you can see, it wouldn't be very difficult to decipher this scheme given enough data.

A somewhat more effective method involves chopping the text into segments and rearranging it as well as obfuscating it

Below is some sample output from this algorithm:

```
OBFS       OBFS
---------- ----------
540407786  &24B23B&Z
542800170  -4B*23&&&
542802063  -4Z&23-&_
541466830  *2_423ZZ&
```

While this is still not encryption, this data would be more difficult to decipher without the key

22

Masking

- Another way to hide sensitive data is through masking
  - This is different from the previous example in that the clear text cannot be reconstructed from the displayed data
- This is useful in situations where it is only necessary to display a portion of the data
  - A good case for this method is the receipts printed at gas stations and convenience stores
  - When a purchase is made with a credit card, the last 4 digits of the credit are often displayed as clear text, while the rest of the credit card number has been masked with a series of X's

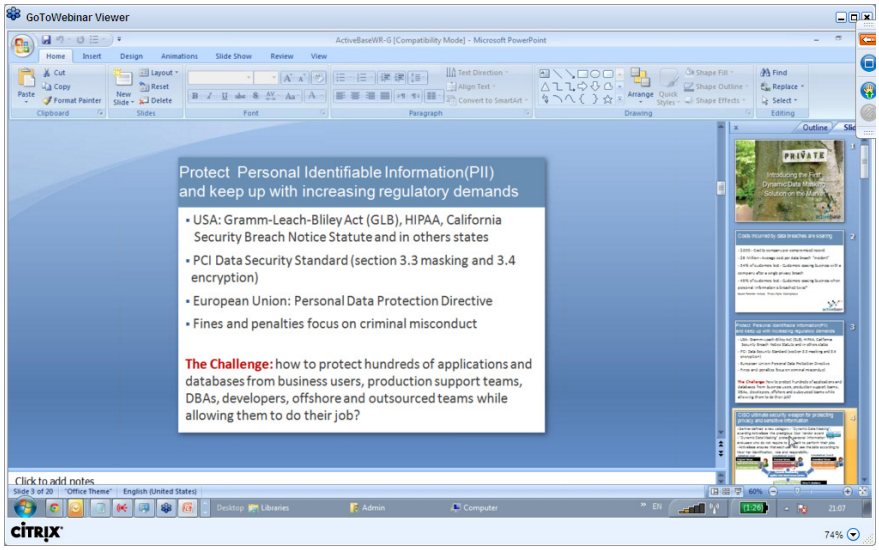
```
Slop n Slurp 1 Stop Shop
5/25/2012 8:53 P.M.
Football Burrito   1   2.49   2.49
Premium Gasoline  12.5 1.699 21.24
                             =====
                             23.73

AMEX 2/02  XXXX-XXXXXX-65498
```

  - This method can also be used for reports where the person reading the report requires only a portion of the sensitive data
    - This method is also commonly used for the account numbers on printed transactions from ATM's

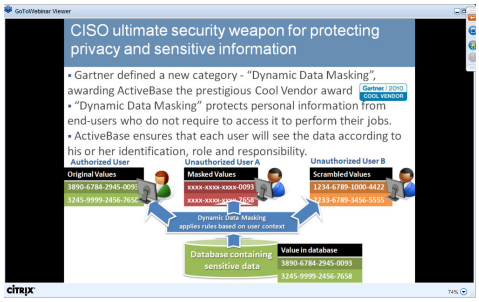
23

Dynamic Data Masking – The Challenge



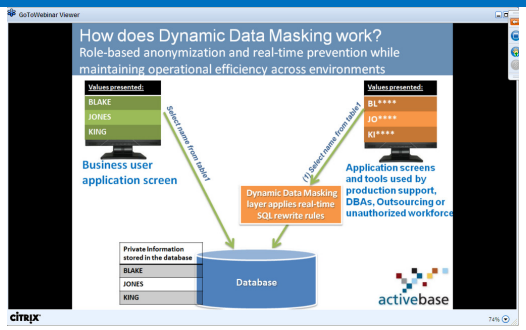
24

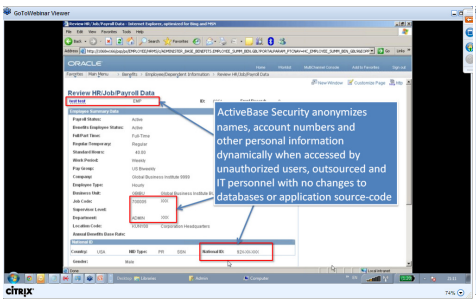
Dynamic Data Masking (1/3)

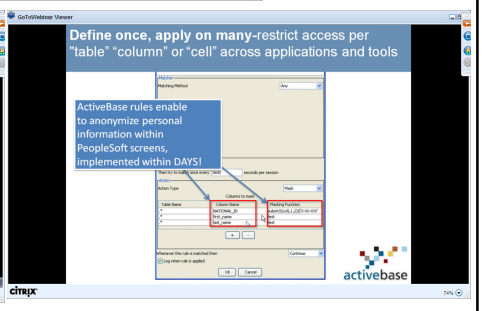


25

Dynamic Data Masking (2/3)

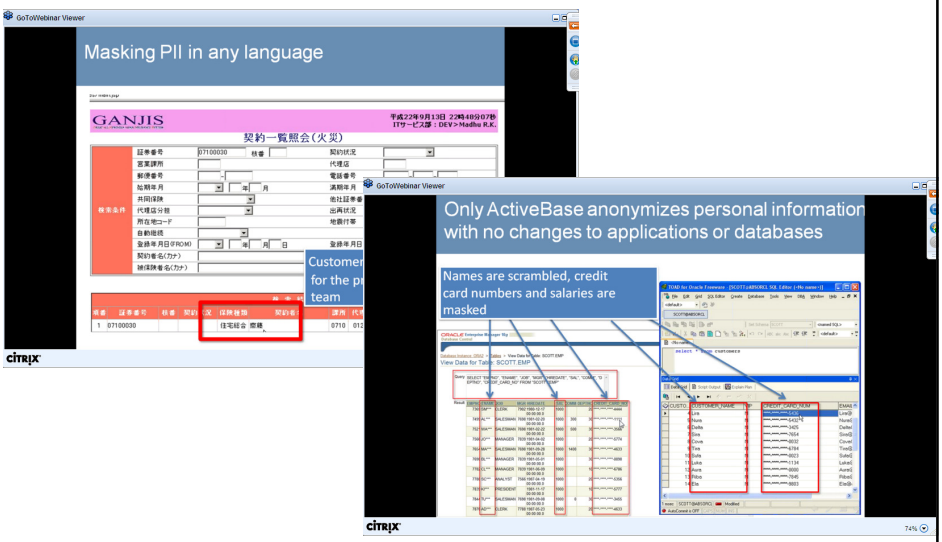






26

Dynamic Data Masking (3/3)



27

Encryption

- See handout “Data Encryption Illustrated”
- There is a lot of background material available for cryptography if you are interested in learning more about this.
  - » http://www.mach5.com/crypto
  - » http://www.counterpane.com/sites.html
- Book
  - » *Applied Cryptography* by Bruce Schneier
- Source code under demos programs
  - » Obfuscation_demo.tar.gz

28

Tokenization

- See handout “Tokenization (Liaison Technologies)”

29

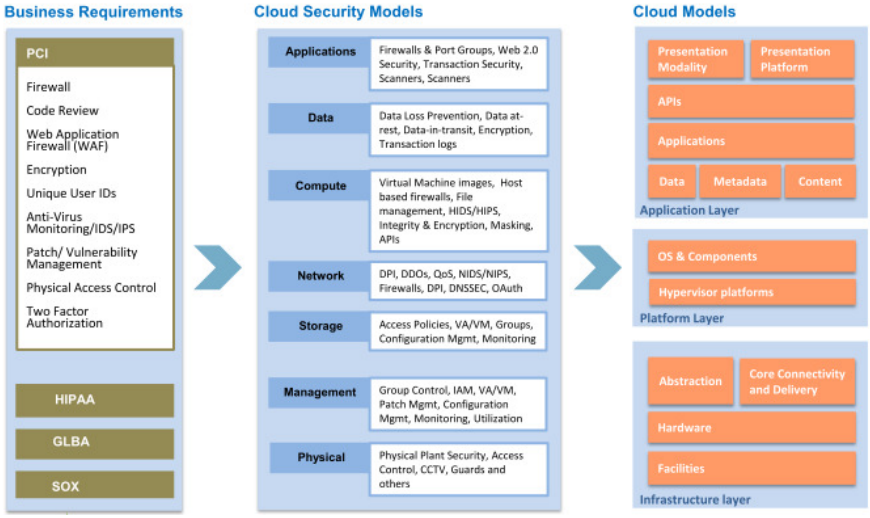
Session 1 Sequel - Cloud Security Standards

- See Cloud-Standards.org
  - http://cloud-standards.org/wiki/index.php?title=Main_Page
  - Cloud Security Alliance
  - Cloud Standards Customer Council
  - Distributed Management Task Force (DTMF)
  - European Telecommunications Standards (ETSI)
  - National Institute of Standards and Technology (NIST)
  - Open Grid Forum (OGF)
  - Object Management Group (OMG)
  - Open Cloud Consortium (OCC)
  - OASIS
  - Storage Networking Industry Association (SNIA – CDMI, etc.)
  - Open Group
  - Association for Retail Technology Standards (ARTS)
  - TM Forum

30

Changing Security Patterns (1/2) – Cloud Security Models

Need to consider appropriate security profiles, resource management, security zones and other services required to deliver a "secure, controlled and compliant" cloud computing environment



31 31

Changing Security Patterns (2/2) – Sample Controls

32 32

Mainstream Cloud Security Offerings

- Security Assessment
- Secure Cloud Architecture Design

33

Sample Cloud Assessment Methodology Detailed

	Planning	Data Collection	Analysis	Recommendation
Activities	▪ Gather business and technology drivers ▪ Document application inventory ▪ Identify stakeholders and SMEs ▪ Schedule Interview and workshops ▪ Prepare & Signoff assessment plan	▪ Gather application details ▪ Understand application functionality & architecture ▪ Review application life cycle process ▪ Gather the model and current TCO / ROI ▪ Gather Governance, security, compliance & regulatory constraints ▪ Gather workload patterns, data integration processes and non functional attributes ▪ Refine assessment dimensions & attributes	▪ Evaluate Cloud Fitment ▪ Perform portability analysis ▪ Perform Cloud suitability analysis ▪ Enterprise Process Changes & Gap analysis ▪ Derive TCO / ROI ▪ Identify candidate Cloud applications ▪ Identify POC /POT	▪ Prepare CSA report ▪ Prepare recommendation report ▪ Present the findings to the stakeholders
Tools & Techniques	▪ Application plan template	▪ Application inventory template ▪ Application Assessment Questionnaire ▪ Interviews & Workshops	▪ Cloud Suitability model ▪ Application Portability model ▪ TCO / ROI Calculator ▪ Interviews & Workshops	▪ CSA Final Report template ▪ Recommendation Report template

34

Cloud Workshop – Typical Customer Questionnaire

Business Model

- How do the components in your value chain perform?
- What are the key services that can be delivered/consumed in the Cloud model?
- What are the key benefits (business case) that the customer can leverage from the Cloud model?

Business Process

- Which processes are core, which ones are contextual?
- Which of the key processes can be executed in the Cloud model?

Applications & Software

- What is the business dependency on in-house developed apps?
- What are the total costs (development, maintenance)?
- Which applications can be hosted on the Cloud model?

Technology & Infrastructure

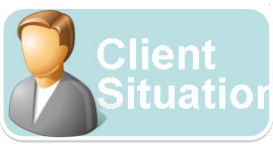
- What are the key Cloud delivery models that the customer can adopt?
- What are the key security issues that are associated with the model?

35

35 35

Case Study - Cloud Readiness Workshop

(Financial Services Industry)



Profile

One of leading financial institution in US with global presence

Problem definition

- Customer is in the process of adopting a cloud strategy and had shortlisted the Microsoft Cloud services as one of their key cloud platforms.
- As part of their cloud adoption readiness, the customer Enterprise Architecture team is in the process of evaluating & coming out with strategies in the area of
  - Security
  - Integration with on-premise services
  - Monitoring and Management
  - Autoscaling
  - Integration with on-premise build systems
  - Deployment models

Solution offered

- An in-depth Architecture strategy workshop was conducted to understand the customer's concerns and challenges and provided solution insights around
  - Security
  - Integration with on-premise services
  - Monitoring and Management
  - Autoscaling
  - Integration with on-premise build systems
  - Deployment models
- Proof of concepts were developed to evaluate Architectural scenarios around Azure based development and solution insights and challenges were presented to the customer

Highlights

- Customer received a better Solution clarity, challenges that helped them in their overall cloud adoption strategy exercise
- Enabled the customer Architecture team with solution strategies around Azure based development

36

36 36

Secure Cloud Architecture Design

- See handout “A Methodology for Security Assessment of Cloud Service Providers”
- See handout “Cloud Security – Use Case Scenario”

37

Agenda

1 Session Overview
2 Cloud Security
3 Summary and Conclusion

38

Assignments & Readings

- Readings
  - Slides and Handouts posted on the course web site
  - References (see Session 8 presentation)
- Assignment for session 8
  - As per Project Part IV at the end of session 8's slide presentation
  - Team Project #1 & 2 (continued) – See related slides in this section
  - Team Project #3 & 4 – See related slides in this section
- Ongoing class project and related Cloud framework setup
  - TDB further in session 8
- Ongoing class presentations
  - TBD further in session 8

39

BPaaS Project – Ongoing Project Part IV

- Leverage BPaaS frameworks to configure / create / extend BPaaS components for the course project application:
  - Update the following for your semester-long project application to allow the use of BPaaS-level components for the provider platform of your choice: high-level description, design/implementation considerations, and planned implementation timeline
  - Investigate application support from various BPaaS vendors (e.g., see list of vendors in the session 7 slides)
    - Pick (a) Cloud BPaaS vendor(s) and explain your choice
  - Configure the BPaaS environment if/as needed to meet the requirements of your project
  - Customize and program BPaaS-based application(s) as needed to support your Cloud project requirements

40

Team Project #1: Evaluate SaaS Vendor Horizontal Solutions

- ADP
- Cisco
- Cordys
- Eloqua
- Google
- Microsoft Online Services
- NetSuite
- Oracle OnDemand
- SAP
- SalesForce.com
- SuccessFactors
- Taleo
- Tibco
- Workday
- Zoho
- etc.

41

Team Project #2: Evaluate SaaS Vendor Vertical Solutions

- SmartStream
- Callidus Software
- TriZetto
- Fineos
- Misys
- Merced System, Inc.
- etc.

42

Team Project #3: Evaluate BPaaS Vendor Horizontal Solutions

- IBM
- Dell
- etc.

43

Team Project #4: Evaluate BPaaS Vendor Vertical Solutions

- IBM
- Dell
- etc.

44

Cloud Security Project – Ongoing Project Part V

- Cloud security project: Ongoing programming project (Part V – Builds on Part IV)
  - Design a secure Cloud architecture to support the deployment of a secure version of the course project application.
- Will be assigned/discussed in detail during Session 9

45

Next Session: Enterprise Cloud-Based HPC Applications

- Overview of High Performance Computing (HPC) on Cloud
- Enterprises HPC applications
  - High-performance grid computing
  - High-performance big data computing/analytics
  - High performance reasoning
- HPC Cloud vendor solutions
  - Compute grids
    - e.g., Windows HPC, Hadoop, Platform Symphony, Gridgain
  - Data grids
    - e.g., Oracle coherence, IBM Object grid, Cassendra, Hbase, Memcached
  - HPC hardware
    - e.g., GPGPU, SSD, Infiniband, Non blocking switches
- HPC on Cloud mainstream offerings
  - Reengineering of HPC applications to leverage HPC on Cloud
  - Hadoop performance tuning
  - etc.
- HPC projects - Ongoing programming projects (Part VI and VII – Build on Part V)
  - Design and develop high-performance application components for the course project application

46

Any Questions?

47

Appendix 1 – BPaaS Mainstream Offerings (Team Project #3/4)

- Business and technical services design and development
  - ISV-based
  - Product-based
    - IBM
    - Dell
- BPaaS migration
- Cloud process-centric application usage optimization

48

Appendix 2 - Cloud Security in Mainstream Vendor Solutions (Session 9)

- AWS
- Google AppEngine