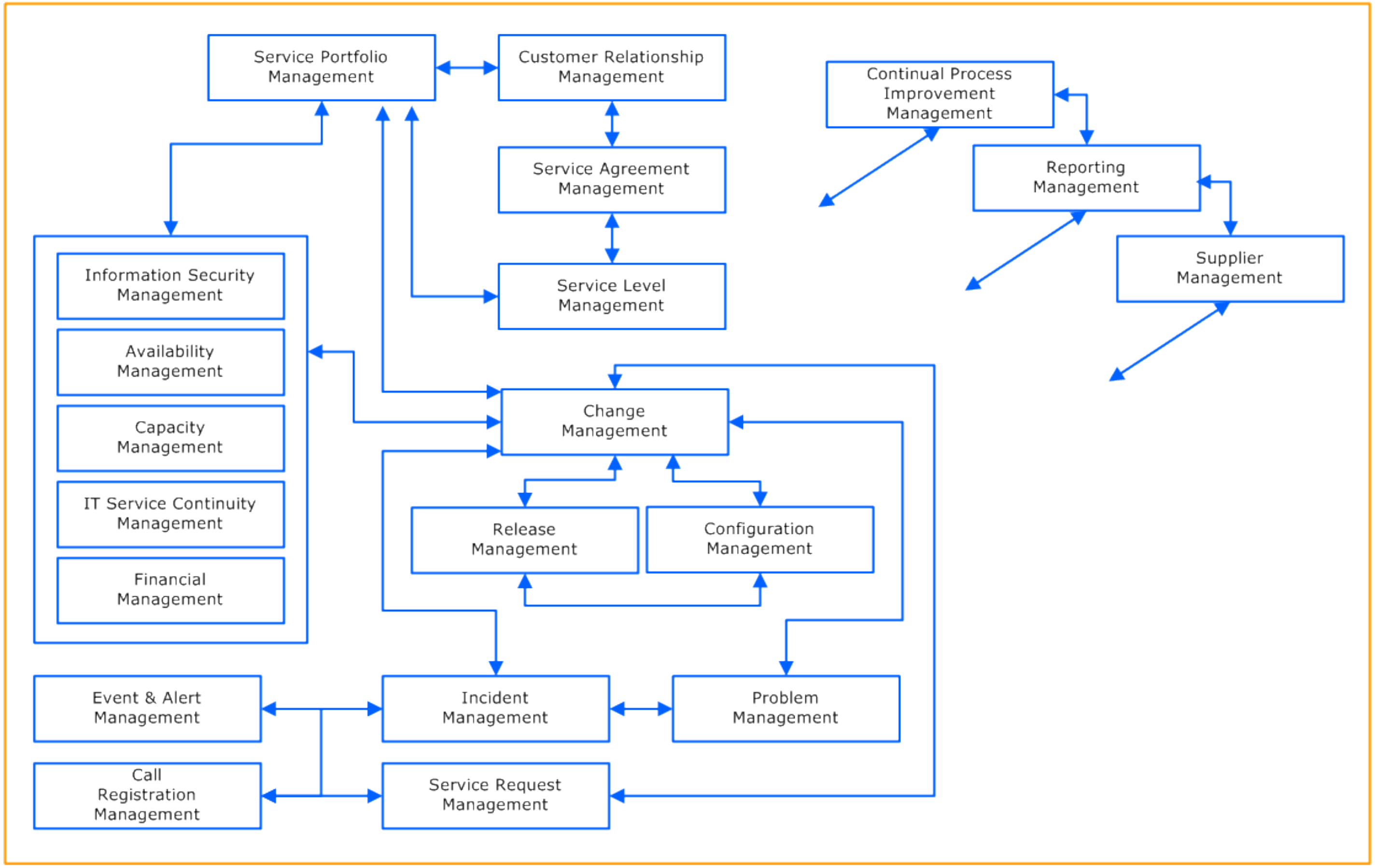
Week 13 – Advanced Topics on Security

IT Service Delivery

ITIL Process


Service Portfolio Management
Customer Relationship Management
Continual Process Improvement Management
Service Agreement Management
Reporting Management
Service Level Management
Supplier Management
Information Security Management
Availability Management
Capacity Management
IT Service Continuity Management
Financial Management
Change Management
Release Management
Configuration Management
Event & Alert Management
Incident Management
Problem Management
Call Registration Management
Service Request Management

http://www.mitsm.de/itil-wiki/process-descriptions-english/main-page

Security Operations

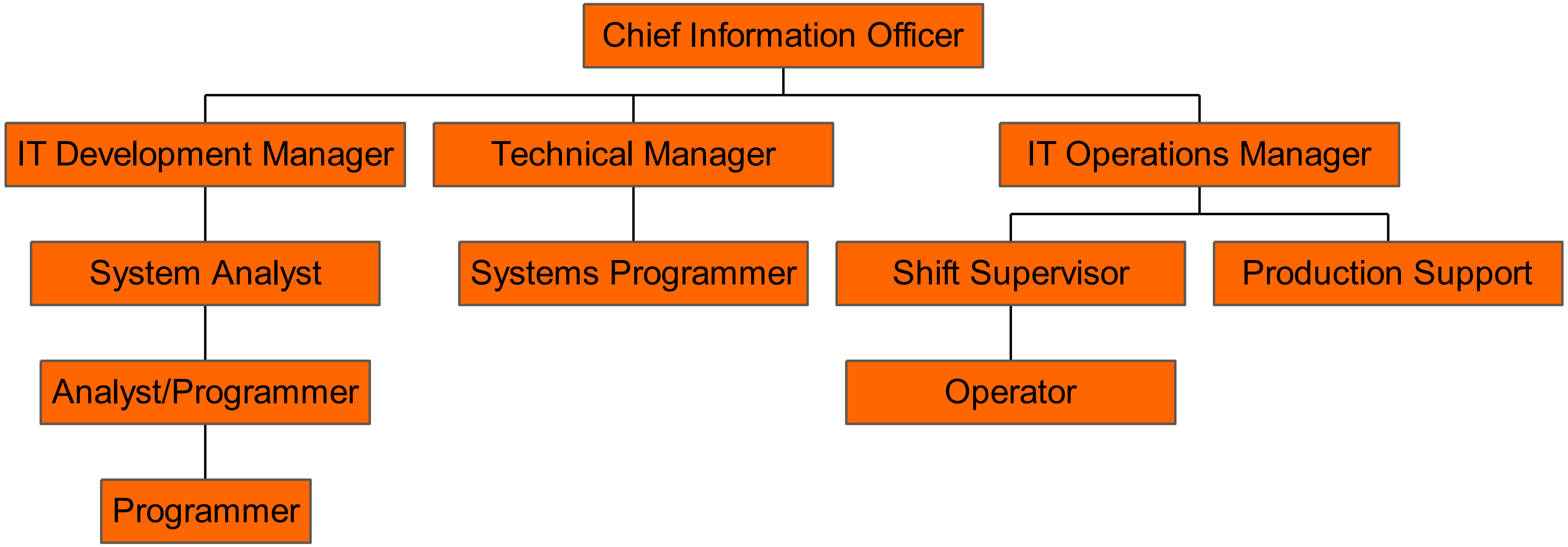
Operations Security

Operations Security is used to identify the controls over hardware, media, and the operators with access privileges to any of these resources.

Audit and monitoring is the ***mechanisms***, ***tools*** and ***facilities*** that permits the identification of security events for reporting to appropriate parties. (ISC^2 Study Guide)

IT Department Organization

IT Department Organization



Organization of Computer Operations

1. IT Operations Management
2. Input/output control
3. Data entry
4. Computer operations
5. Production control and scheduling
6. Library management and change management

1. IT Operations Management

IT Operations Management has the overall responsibility for developing computer operations standards and procedures for efficient and effective operations

IT Management is also responsible for ensuring that there are sufficient IT resources to meet the current and future business needs

1. IT Operations Management

Means to manage and control IT operations

- Recruit sufficient computer operators
- Organize communication between shifts
- Provide operations documentation to support computer operations
- Set up processing checklists and priorities

1. IT Operations Management

- Obtain and review:
  - Hardware and software problem report
  - Statistics of scheduled and unscheduled system downtime
  - Re-run jobs and the reasons
  - CPU utilization
  - Computer storage utilization
  - SLA achievement

2. Input/Output Control

Data Input Control

- Receive source documents for batch data entry
- Authenticate the source documents
- Use batch and control totals to ensure all source documents are processed
- Input the data in a timely manner

2. Input/Output Control

Data Output Control

- Output is produced in the proper format and distributed to the appropriate users in a secure manner
- Control of production report distribution
  - Predefined report recipients
  - Check completeness before distribution
  - Recipient check all reports received

2. Input/Output Control

- Restrict access to spooled reports to prevent
    - Compromise confidentiality
    - Unauthorized report deletion
    - Computer generation of negotiable instruments
        - Sequence control
        - Detection of missing of negotiable instruments
- Inventory of sensitive and critical stationaries
    - Keep in a secure location
    - Properly recorded
    - Stock taking on a regular basis

3. Data Entry

Enter data by using data entry device to create data file for subsequent processing

Key verification is a common control technique for verifying the accuracy of inputted data

Sufficient audit trail for checking when required

4. Computer Operations

Carry out ad-hoc and scheduled computer jobs

Guided by operation procedures to ensure computer operations are carried in a efficient and effective manner

Example of operation procedures

- System startup and shut down procedures
- Error handling procedures
- Data backup and restore procedures

4. Computer Operations

Operation tasks

- Restart and shut down computers
- Running and monitoring computer jobs
- Report printing
- Backup/restore of system and data files
- House keeping
- Control access to the data processing centre and computing facilities
- Participate in disaster recovery testing

4. Computer Operations

- Maintain registers and operational statistics for measuring SLA achievement
- Report equipment failures and operating errors
- Ensure an adequate supply of computer consumables

5. Production Control and Scheduling

Schedule computer jobs processing sequence, for both ad-hoc and routine jobs

Define the conditions for starting/re-starting a job

Define job dependencies

Ensure all jobs are completely processed

Manual processing of scheduled job or using job scheduling software

5. Production Control and Scheduling

Manual

- Rely on operator to run a job
- Use job processing checklist for controlling job processing
- Manual job monitoring and logging
- Job processing records review by supervisor to ensure computer jobs are accurately and completely process
- Effective for simple batch jobs

5. Production Control and Scheduling

- Automatic (Job Scheduling Software)
  - Automatic processing of batch jobs
  - Setup once
  - Control job dependence
  - Error detection and logging

6. Library Management and Change Management

Manage computer tapes/cartridges movement

- Recording of receiving, lending, removing of computer tapes/cartridges
- Regular stock taking to detect missing of computer tapes/cartridges
- Proper audit trail of computer tapes/cartridges movement

6. Library Management and Change Management

Manage production software inventory

- Software version control
- Job control language and processing parameter control
- Computer source and object control (e.g. synchronization)
- Logging of addition, deletion and updating of software inventory

Operations Administration

Operations Administration

1. Background checking
2. Segregation of duties
3. Job Rotation
4. Least privilege
5. Need to know

1. Background Check

Verification checks before employing an operations staff for

- HKID
- Availability of satisfactory character references
- Checking of the applicant’s curriculum vitae
- Confirmation of claimed academic and professional qualifications

2. Segregation of Duties

Ensure critical stages of a process are not under the control of a single individual

Errors and irregularities performed by one user can be detected by another user

Potential damage can be minimized

2. Segregation of Duties

Appropriate segregation of duties between

- Users
- IT developers
- Data center staff

Achieved by

- Policies
- Procedures
- Organization structure

So that no one individual can perform unauthorized activities

2. Segregation of Duties

In computer operations, the following duties can be defined

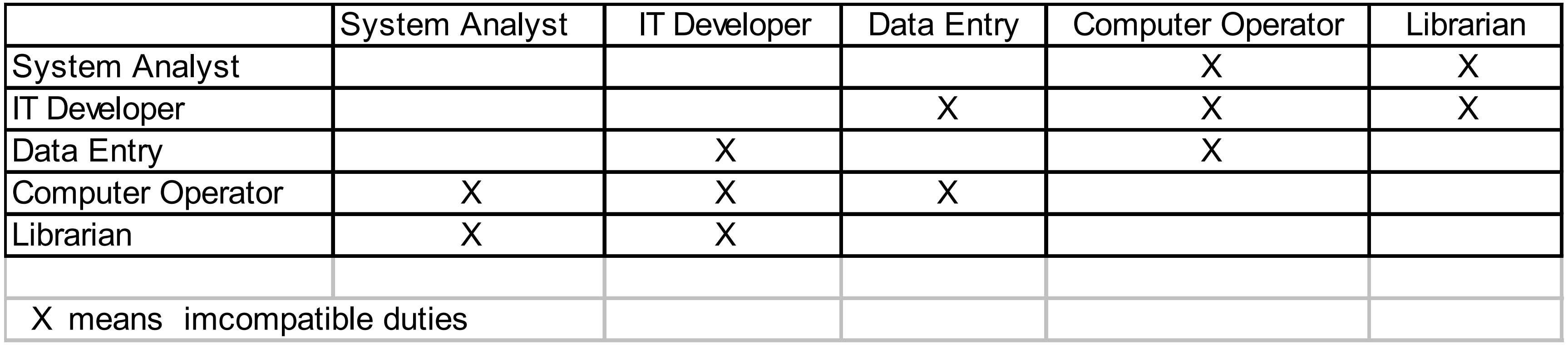
- Production Control
- Data Entry
- Librarian
- Operator
- System Programmer

2. Segregation of Duties

In software programming, the following function groups can be defined

- System Analyst
- Programmer
- Database Administrator
- Security Officer
- Quality Assurance

2. Segregation of Duties



	System Analyst	IT Developer	Data Entry	Computer Operator	Librarian
System Analyst				X	X
IT Developer			X	X	X
Data Entry		X		X	
Computer Operator	X	X	X		
Librarian	X	X			
X means imcompatible duties					

3. Job Rotation

A detective control

Require operations staff to rotate their job duties on a regular basis for allowing another staff to detect anomalies

Having human resources policy to require operations staff to take annual leave for at least 2 consecutive weeks

4. Least Privilege

Preventive control

Only the minimum access privilege is granted to perform a task

Purpose of least privilege is to ensure that a task can only be performed by authorized user

For example

- “Super User” privilege is not granted to Operations staff

5. Need To Know

Preventive control

Only those users who need to perform a task is provided with the information and knowledge for processing the task

This can be achieved by restricting users to access operations manual, system documents, etc.

Reduce the risk of unauthorised system access

Operations Controls

Change controls

Problem management

Capacity management

Document controls

Media handling

Operations acceptance test

Audit trails

Virus controls

Physical (Environmental) Security

Physical Security

Physical facility is the building or vehicle housing the system and network components

The physical characteristics of these structures and vehicles determine the level of physical threats such as fire and unauthorised access

The facility's geographic location determine the characteristics of natural threats such as earthquakes and flooding

Physical Security

Natural Environmental Threats	Supply System Threats	Manmade Threats	Politically Motivated Threats
Floods, fire, earth quake…	Power outages, communication interruptions,…	Explosions, disgruntled employees, fraud,…	Strikes, riots, civil disobedience,…

Physical Security

Element for Physical Security Measures

Determent

- Convince people not to attack

Detection

- Alarms, guards, and other means of detecting attacks

Delay

- Elements that slow down an attacker, e.g. locks & safes

Response

- Guards or a call to the police

Physical Security - Controls

Administrative controls

- facility selection, facility construction and management, personnel control, evacuation procedure, system shutdown procedure, fire suppression procedure, handling procedures for other exceptions such as hardware failure, bomb threats, etc.

Physical controls

- facility construction material, key and lock, access card and reader, fence, lighting, etc.

Technical controls

- physical access control and monitoring system, intrusion detection and alarm system, fire detection and suppression system, uninterrupted power supply, heating / ventilation / air conditioning system (HVAC), disk mirroring, data backup, etc.

Security Considerations Of Physical Security

- What are the security considerations in protecting the equipment when they go into the cloud?
- Access Control
  - Who have access to the servers and storage devices?
- Against Hazards
  - Fire and smoke sensors
  - Fire extinguishers
  - Water sensor and raised floors
  - UPS
- Against Attacks
  - Fast recovery at a backup site
- Retiring Devices
  - Define retirement process of failed or used storage devices

Security Considerations Of Physical Security - Access Control

Access Control and Auditing

- Lock and key
- Access card and reader
- Fence
- Lighting
- Doorway and Man-trap

Access Monitoring and Intrusion Detection

- Patrol force / security guard
- Technical access monitoring controls
- Alarm System

Physical Access Security

Access control facility

- Fence, Gate and Turnstile
- Mantrap
- Lighting
- CCTV
- Guards

Fence, Gate and Turnstile

Fence and gate

- Mark the boundary of a facility for deterring unauthorized access
- Must be tall enough for stopping a determined intruder

Turnstile is a revolving gate that restrict the number of users to enter or leave a facility at a time for pedestrian traffic control

Mantrap

Mantrap consists of a set of double doors where one of the doors can be opened at a time for access control

For additional security, person entering and leaving a facility can be monitored and controlled by a guard

Lighting

One of the most basic (and cheapest) components of a security system

Carefully designed and coordinated interior and exterior lighting systems can exert a significant deterrent effect

Closed Circuit Television (CCTV)

For preventing and detecting of abnormal events

Locate CCTV in strategic points such as:

- Entries to Data Centre
- Unmanned machine rooms

Live events should be recorded and retained for future analysis and/or prosecution

Guards

Good for controlling physical access and perimeter security, e.g. register visitors, escorting visitors

Will be more effective if supplemented by locked doors and CCTV

Good for situation (e.g. during emergency) which require making immediately judgments and decisions

Guards must be trained so that they can perform their work effectively

Access Control System

There are three types of user authentication methods for controlling user access:

- Something an individual knows (e.g. password)
- something an individual possesses (e.g. smart card)
- something an individual has (e.g. fingerprint)

These methods can be used alone or in combination

Programmable Lock

Programmable lock require user to enter a pattern of digits (lock combination) on the numeric key pad for determining whether access is allowed

Programmable lock can be mechanically or electronically based

Suitable for areas with low access security controls as password can be obtained by observing an authorised user entering the lock combination

Memory Card

Memory card store, but not process information

Memory card is significantly more secure than password, especially if memory card must be presented for entering and leaving the controlled areas

More administrative overhead for managing the memory cards, e.g. lost cards handling

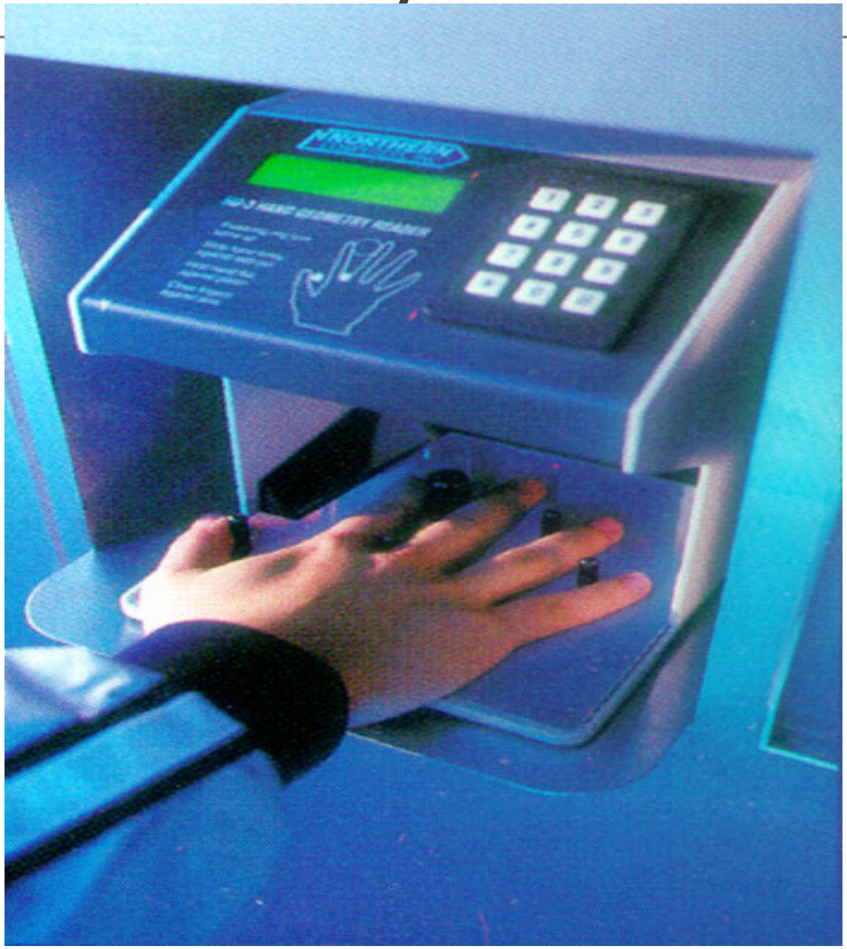
Biometrics Systems

Biometrics system identify people by a unique human characteristics such as size and shape of a hand, fingerprint, voice, iris, etc.

Benefits of Biometrics for access control

- More secure as sharing/stealing of access card is eliminated
- Administrative time for handling lost card is reduce
- Convenience

Security Access Control
Hand Geometry Reader



Network Operation Centre
Closed-circuit TV Surveillance System (CCTV)

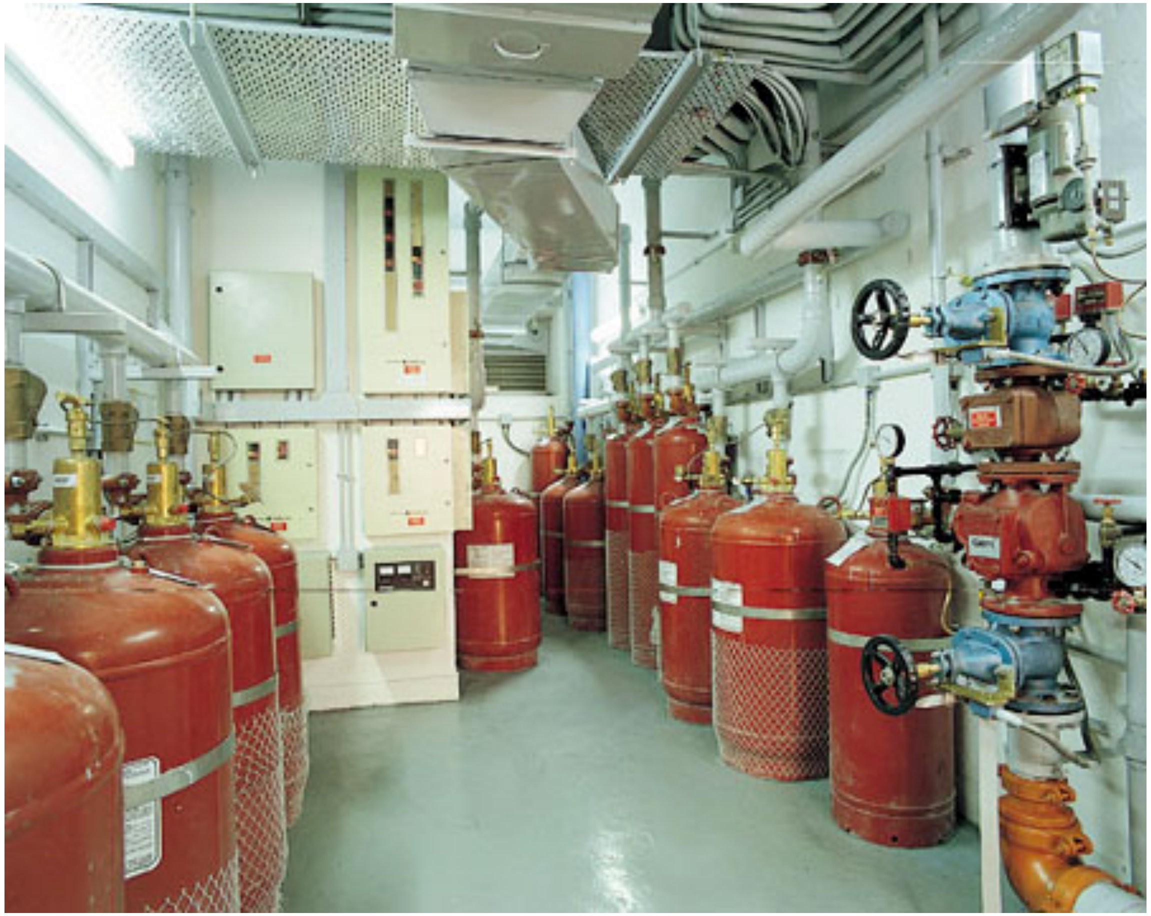
Security Operation Center

Computer Room Air Conditioning CRAC

Configured with a fail-safe back-up system and with temperature and humidity control

Uninterruptible Power Supply (UPS)

FM 200 Fire Suppression System and Pre-Action Sprinkler System



Cages, Racks and Cabinets

Cloud Computing

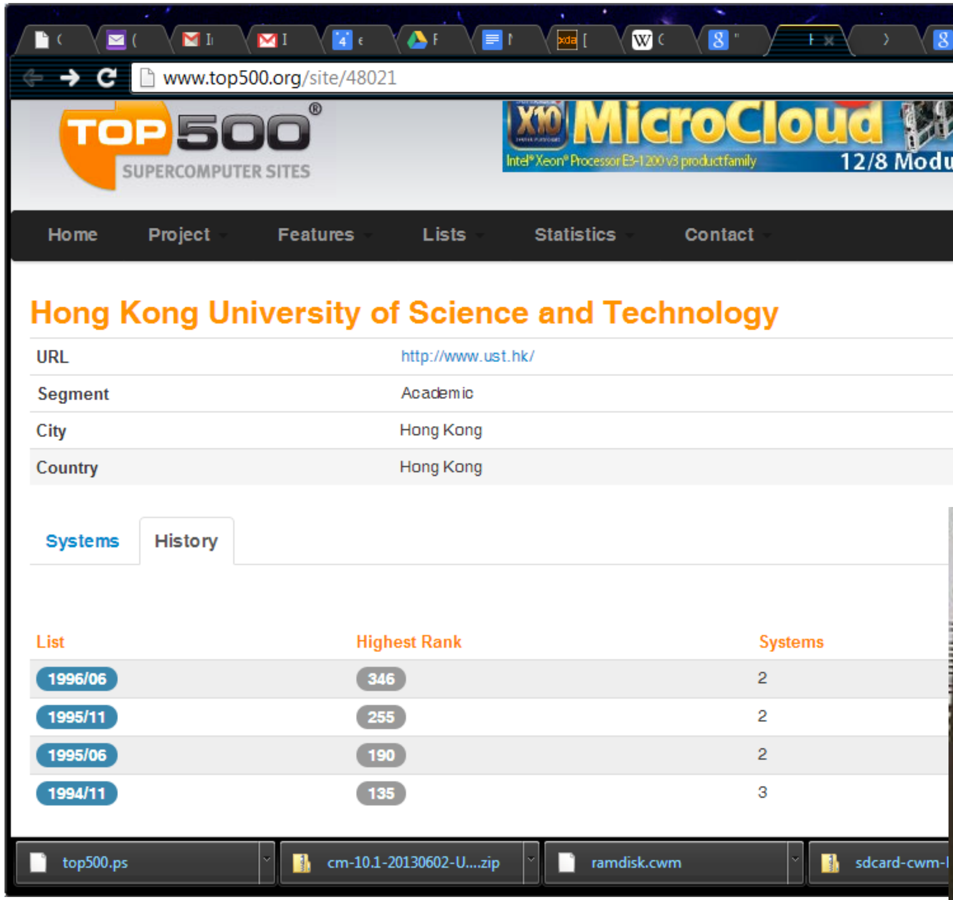
Grid Computing

Grid computing is the federation of computer resources from multiple locations to reach a common goal.

The grid can be thought of as a distributed system with non-interactive workloads that involve a large number of files.

UST has two supercomputer during 1994 - 1996

Top 500 Supercomp es


www.top500.org/site/48021
TOP500 SUPERCOMPUTER SITES
Home
Project
Features
Lists
Statistics
Contact
top500.ps
cm-10.1-20130602-U....zip
ramdisk.cwm
sdcard-cwm-

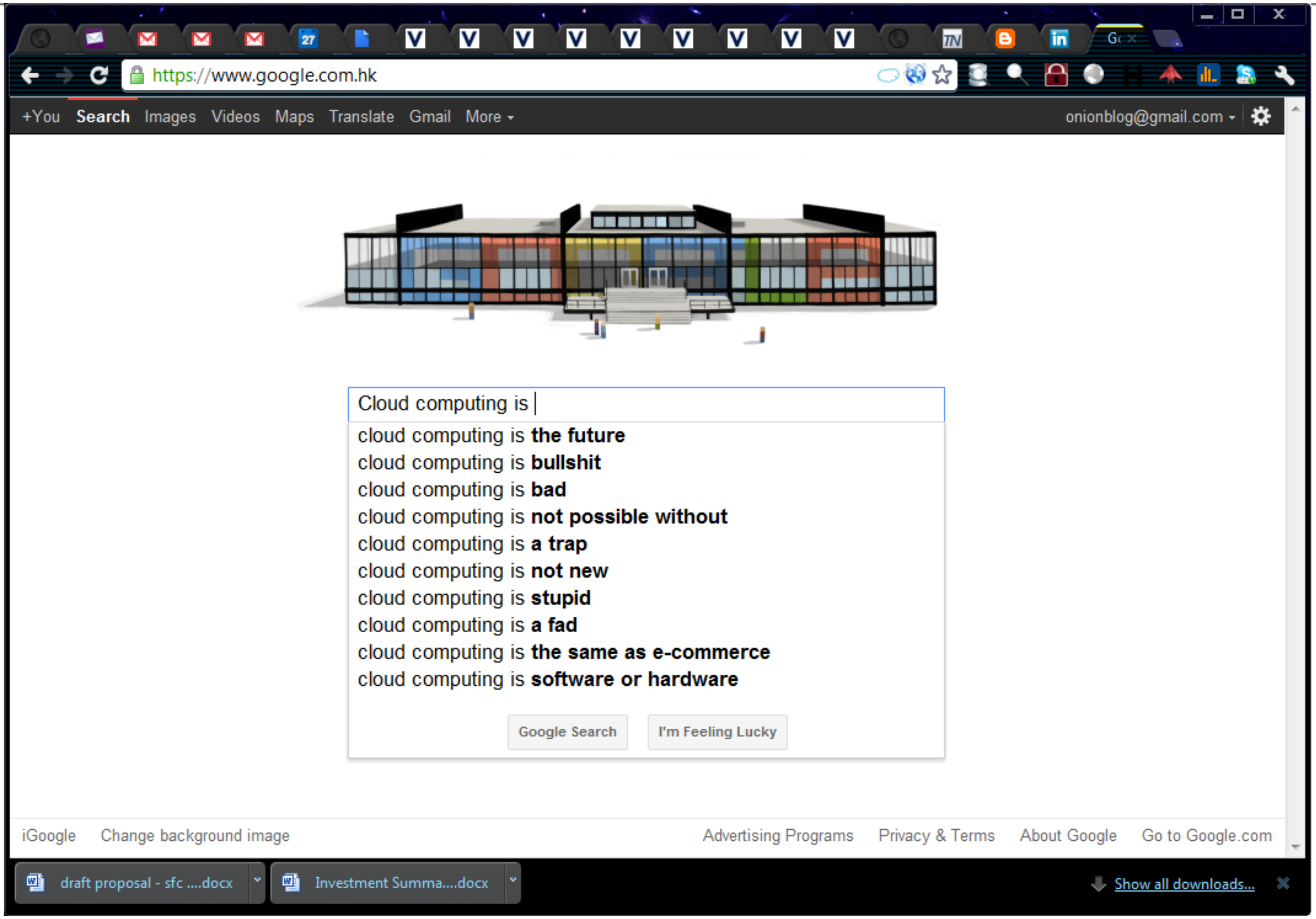
Hong Kong University of Science and Technology

URL	http://www.ust.hk/
Segment	Academic
City	Hong Kong
Country	Hong Kong

Systems History

List	Highest Rank	Systems
1996/06	346	2
1995/11	255	2
1995/06	190	2
1994/11	135	3

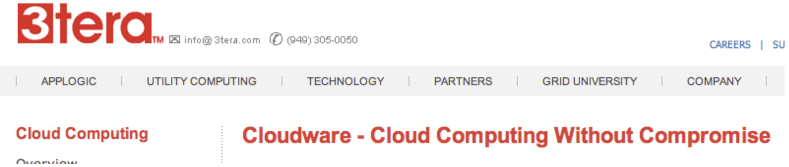
What is Cloud Computing?



Cloud computing is

cloud computing is **the future**
cloud computing is **bullshit**
cloud computing is **bad**
cloud computing is **not possible without**
cloud computing is **a trap**
cloud computing is **not new**
cloud computing is **stupid**
cloud computing is **a fad**
cloud computing is **the same as e-commerce**
cloud computing is **software or hardware**

Large Scale Cloud Computing



3tera™ info@3tera.com (949) 305-0050 CAREERS | SU

| APPLOGIC | UTILITY COMPUTING | TECHNOLOGY | PARTNERS | GRID UNIVERSITY | COMPANY |

Cloud Computing

Overview

Cloudware - Cloud Computing Without Compromise

3 Service Models of Cloud Computing

SaaS (Software-as-a-Service)

- The consumer uses the provider's applications on a cloud infrastructure
- E.g. Google Apps, Salesforce

PaaS (Platform-as-a-Service)

- The consumer deploy consumer-created or acquired applications onto the cloud infrastructure
- E.g. Windows Azure, Google AppEngine

IaaS (Infrastructure-as-a-Service)

- The consumer provision processing, storage, networks, and other fundamental computing resources
- E.g. Amazon EC2, GoGrid

Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Delivery Models

5 Essential Characteristics of Cloud Computing

Broad network access

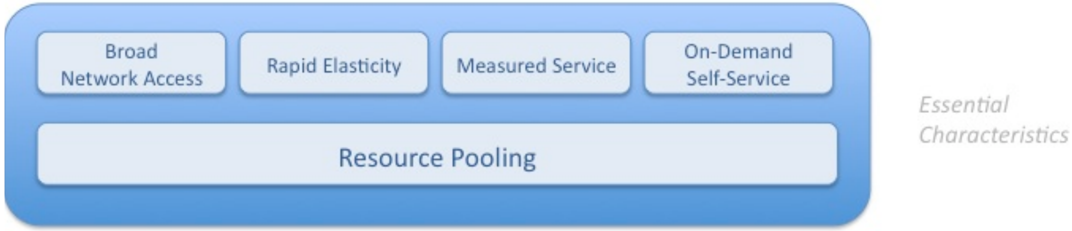
- Ubiquitous – can be accessed everywhere

Rapid elasticity

- Highly scalable, even appeared as "unlimited" to the users

Measured service

- Pay per use ("Taxi" metaphor)



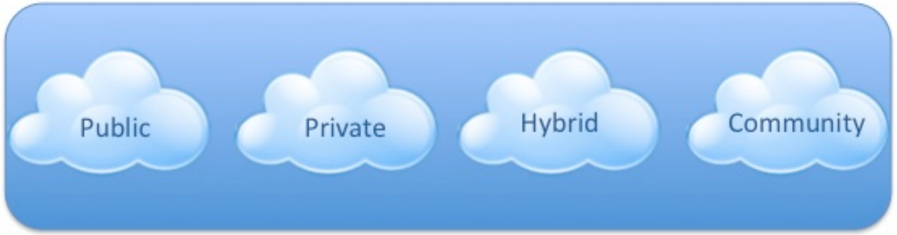
On-demand self-services

- Users can request the service automatically without human interaction with the service provider

Resources pooling

- Shared resource pool, user has no control over the exact location of the provided resources

Terminology of cloud computing



Deployment Models

Public Cloud

- The cloud infrastructure is owned by an organization selling cloud services

Private Cloud

- The cloud infrastructure is operated solely for a single organization

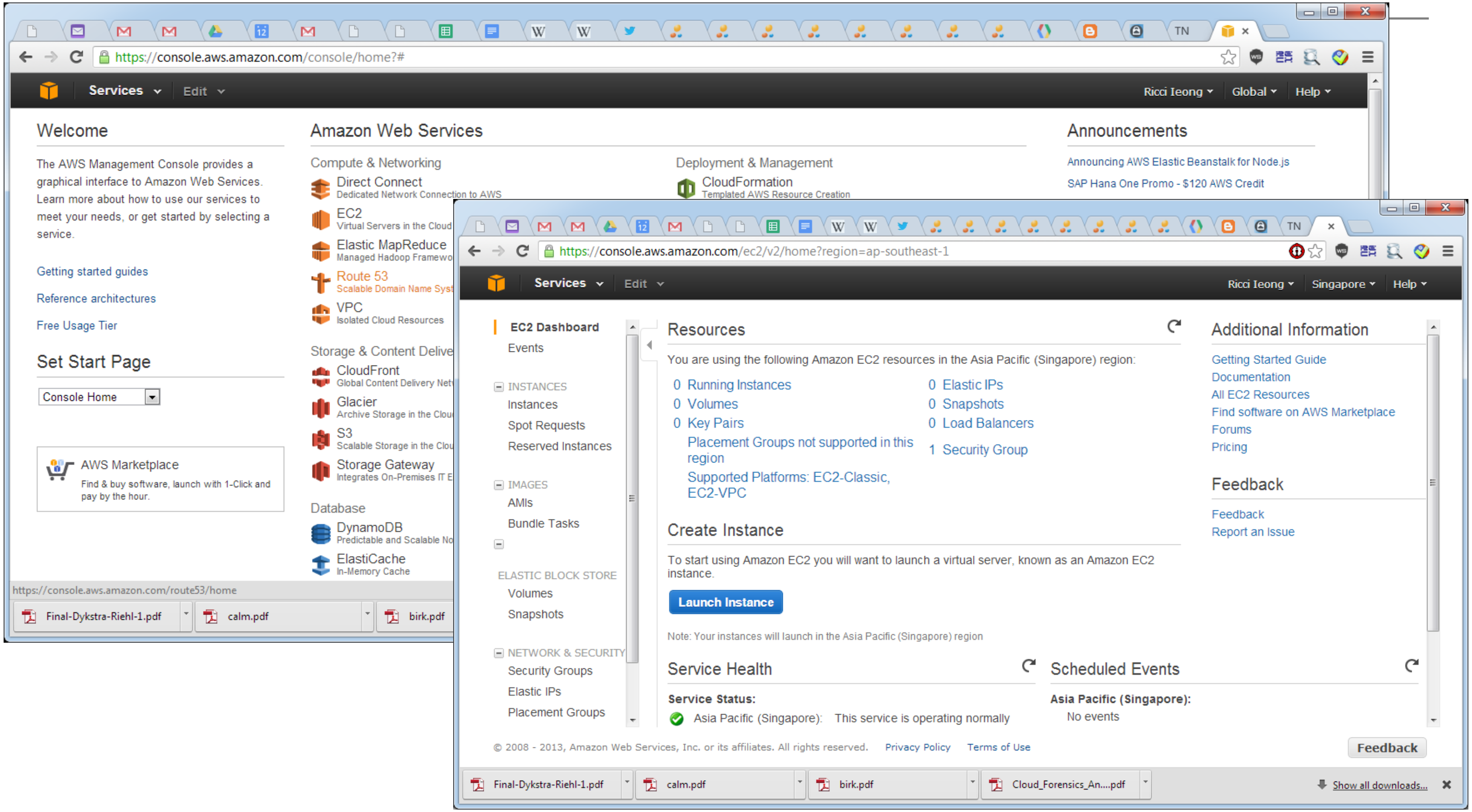
Community Cloud

- The cloud infrastructure is shared by several organizations having similar requirements

Hybrid Cloud

- The cloud infrastructure is a composition of two or more clouds (private, community, or public)

Amazon



https://console.aws.amazon.com/console/home?#

Services | Edit | Ricci Ieong | Global | Help

Welcome

The AWS Management Console provides a graphical interface to Amazon Web Services. Learn more about how to use our services to meet your needs, or get started by selecting a service.

Getting started guides

Reference architectures

Free Usage Tier

Set Start Page

Console Home

AWS Marketplace
Find & buy software, launch with 1-Click and pay by the hour.

Amazon Web Services

Compute & Networking

- Direct Connect – Dedicated Network Connection to AWS
- EC2 – Virtual Servers in the Cloud
- Elastic MapReduce – Managed Hadoop Framewo
- Route 53 – Scalable Domain Name Syst
- VPC – Isolated Cloud Resources

Storage & Content Delive

- CloudFront – Global Content Delivery Net
- Glacier – Archive Storage in the Clou
- S3 – Scalable Storage in the Clou
- Storage Gateway – Integrates On-Premises IT E

Database

- DynamoDB – Predictable and Scalable No
- ElastiCache – In-Memory Cache

Deployment & Management

- CloudFormation – Templated AWS Resource Creation

Announcements

Announcing AWS Elastic Beanstalk for Node.js

SAP Hana One Promo - $120 AWS Credit

https://console.aws.amazon.com/route53/home

Final-Dykstra-Riehl-1.pdf | calm.pdf | birk.pdf

https://console.aws.amazon.com/ec2/v2/home?region=ap-southeast-1

Services | Edit | Ricci Ieong | Singapore | Help

EC2 Dashboard
Events

INSTANCES
Instances
Spot Requests
Reserved Instances

IMAGES
AMIs
Bundle Tasks

ELASTIC BLOCK STORE
Volumes
Snapshots

NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups

Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Singapore) region:

- 0 Running Instances
- 0 Volumes
- 0 Key Pairs
- Placement Groups not supported in this region
- Supported Platforms: EC2-Classic, EC2-VPC
- 0 Elastic IPs
- 0 Snapshots
- 0 Load Balancers
- 1 Security Group

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Launch Instance

Note: Your instances will launch in the Asia Pacific (Singapore) region

Service Health

Service Status:

✓ Asia Pacific (Singapore): This service is operating normally

Scheduled Events

Asia Pacific (Singapore):

No events

Additional Information

Getting Started Guide
Documentation
All EC2 Resources
Find software on AWS Marketplace
Forums
Pricing

Feedback

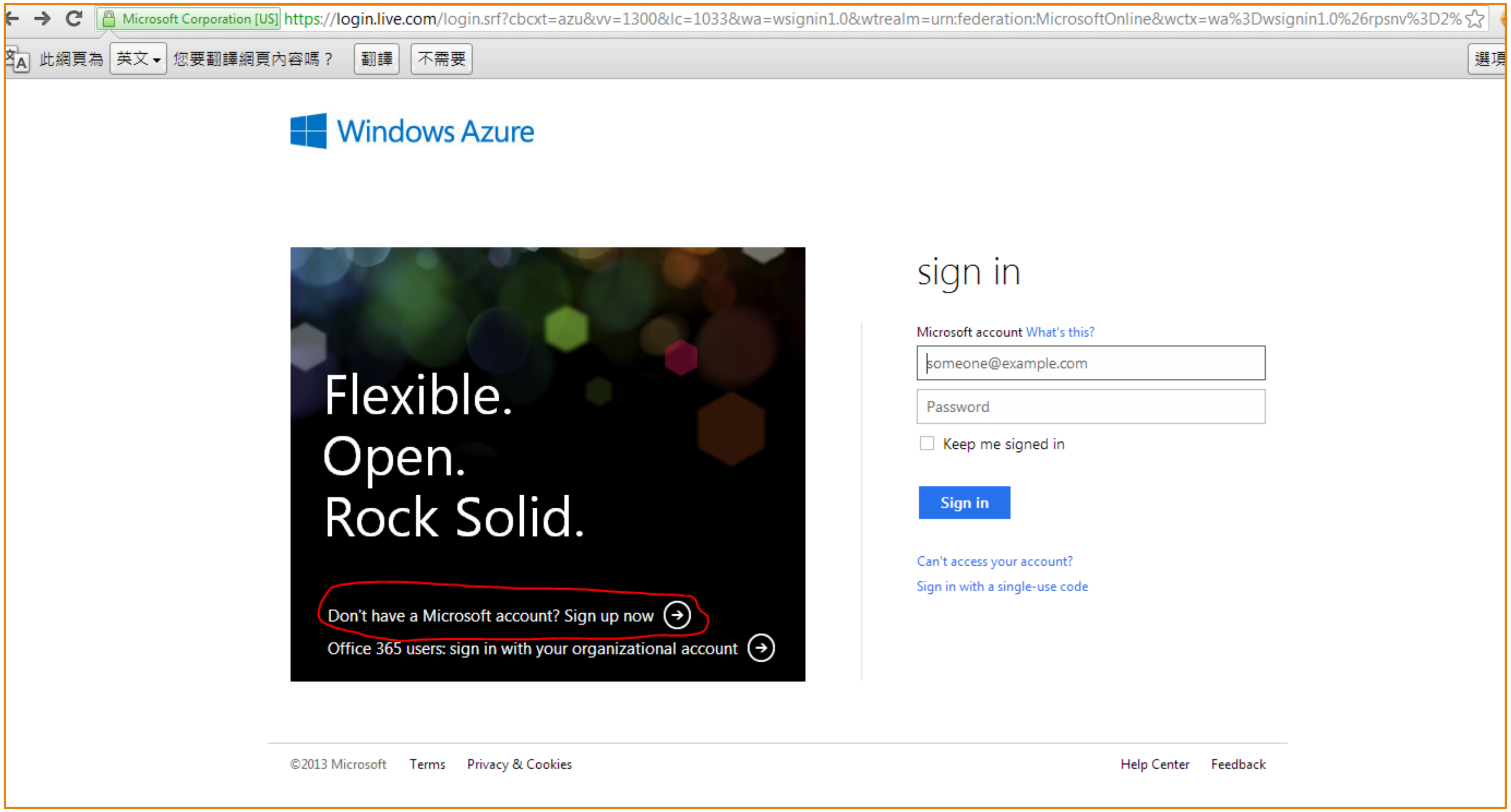
Feedback
Report an Issue

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Feedback

Final-Dykstra-Riehl-1.pdf | calm.pdf | birk.pdf | Cloud_Forensics_An....pdf | Show all downloads...

Windows Azure



https://login.live.com/login.srf?cbcxt=azu&vv=1300&lc=1033&wa=wsignin1.0&wtrealm=urn:federation:MicrosoftOnline&wctx=wa%3Dwsignin1.0%26rpsnv%3D2%

此網頁為 英文 您要翻譯網頁內容嗎？ 翻譯 不需要

Windows Azure

Flexible.
Open.
Rock Solid.

Don't have a Microsoft account? Sign up now

Office 365 users: sign in with your organizational account

sign in

Microsoft account What's this?

someone@example.com

Password

□ Keep me signed in

Sign in

Can't access your account?

Sign in with a single-use code

©2013 Microsoft Terms Privacy & Cookies Help Center Feedback

Cloud related threats

Isolation risk

De-perimeterization

Roles & responsibilities issues

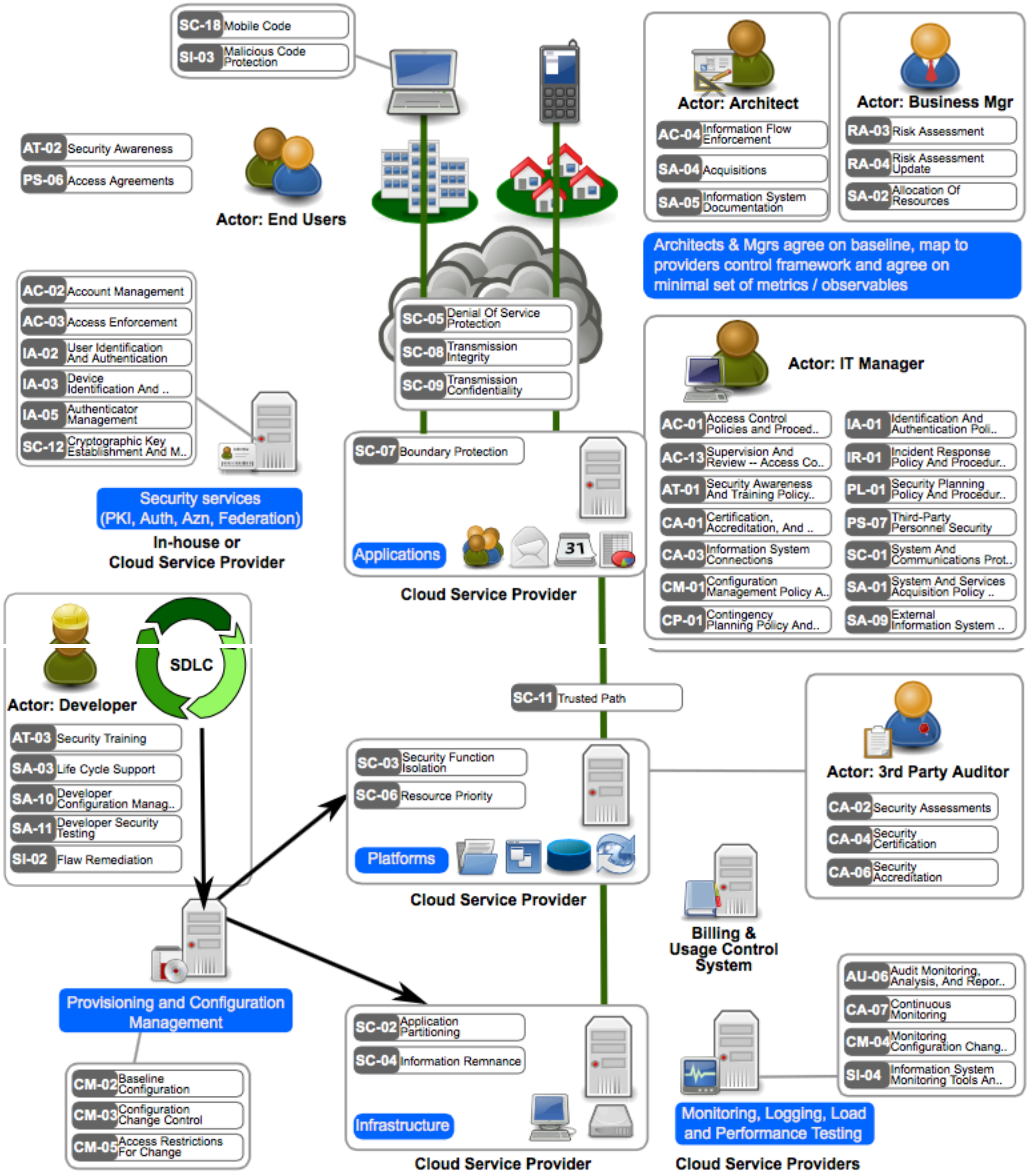
De-perimeterization

Forrester Research proposed Zero-Trust architecture

- No default trust for any entity including users, devices, applications and packets
- Keep the concept of protecting compartmentalize different segments to the network

VLAN (Virtual Local Area Network) can be used for segment the network but cannot enforce the control based on threats or detected privileged information

Cloud Security



SC-18 Mobile Code
SI-03 Malicious Code Protection

AT-02 Security Awareness
PS-06 Access Agreements

Actor: End Users

AC-02 Account Management
AC-03 Access Enforcement
IA-02 User Identification And Authentication
IA-03 Device Identification And ..
IA-05 Authenticator Management
SC-12 Cryptographic Key Establishment And M..

Security services (PKI, Auth, Azn, Federation)

In-house or Cloud Service Provider

SC-05 Denial Of Service Protection
SC-08 Transmission Integrity
SC-09 Transmission Confidentiality

SC-07 Boundary Protection

Applications

Cloud Service Provider

Actor: Architect
AC-04 Information Flow Enforcement
SA-04 Acquisitions
SA-05 Information System Documentation

Actor: Business Mgr
RA-03 Risk Assessment
RA-04 Risk Assessment Update
SA-02 Allocation Of Resources

Architects & Mgrs agree on baseline, map to providers control framework and agree on minimal set of metrics / observables

Actor: IT Manager
AC-01 Access Control Policies and Proced..
AC-13 Supervision And Review -- Access Co..
AT-01 Security Awareness And Training Policy..
CA-01 Certification, Accreditation, And ..
CA-03 Information System Connections
CM-01 Configuration Management Policy A..
CP-01 Contingency Planning Policy And..
IA-01 Identification And Authentication Poli..
IR-01 Incident Response Policy And Procedur..
PL-01 Security Planning Policy And Procedur..
PS-07 Third-Party Personnel Security
SC-01 System And Communications Prot..
SA-01 System And Services Acquisition Policy ..
SA-09 External Information System ..

Actor: Developer
SDLC
AT-03 Security Training
SA-03 Life Cycle Support
SA-10 Developer Configuration Manag..
SA-11 Developer Security Testing
SI-02 Flaw Remediation

SC-11 Trusted Path

SC-03 Security Function Isolation
SC-06 Resource Priority

Platforms

Cloud Service Provider

Actor: 3rd Party Auditor
CA-02 Security Assessments
CA-04 Security Certification
CA-06 Security Accreditation

Billing & Usage Control System

Provisioning and Configuration Management

CM-02 Baseline Configuration
CM-03 Configuration Change Control
CM-05 Access Restrictions For Change

SC-02 Application Partitioning
SC-04 Information Remnance

Infrastructure

Cloud Service Provider

AU-06 Audit Monitoring, Analysis, And Repor..
CA-07 Continuous Monitoring
CM-04 Monitoring Configuration Chang..
SI-04 Information System Monitoring Tools An..

Monitoring, Logging, Load and Performance Testing

Cloud Service Providers

Final words

What else you have to learn

ITIL Process

- Operation Security
- Change Management
- Problem Management
- Capacity Management
- …

Secure Application Programming Practices

IT Security Policies and Security Management

Physical Security

What you can learn from exam?

…

Prepare for Future

Hot topics in IT Security Field

- Identity Management
- Online Fraud Detection
- Mobile and Cloud Security Architecture Design
- Cloud Security implementation
- Software Defined Network
- Application Security
- IoT Security

Prepare for Certificate

ISC2

- CISSP
- SSCP
- CSSLP
- CCSP
- CCFP

CSA

- CCSK

ISACA

- CISA
- CSX

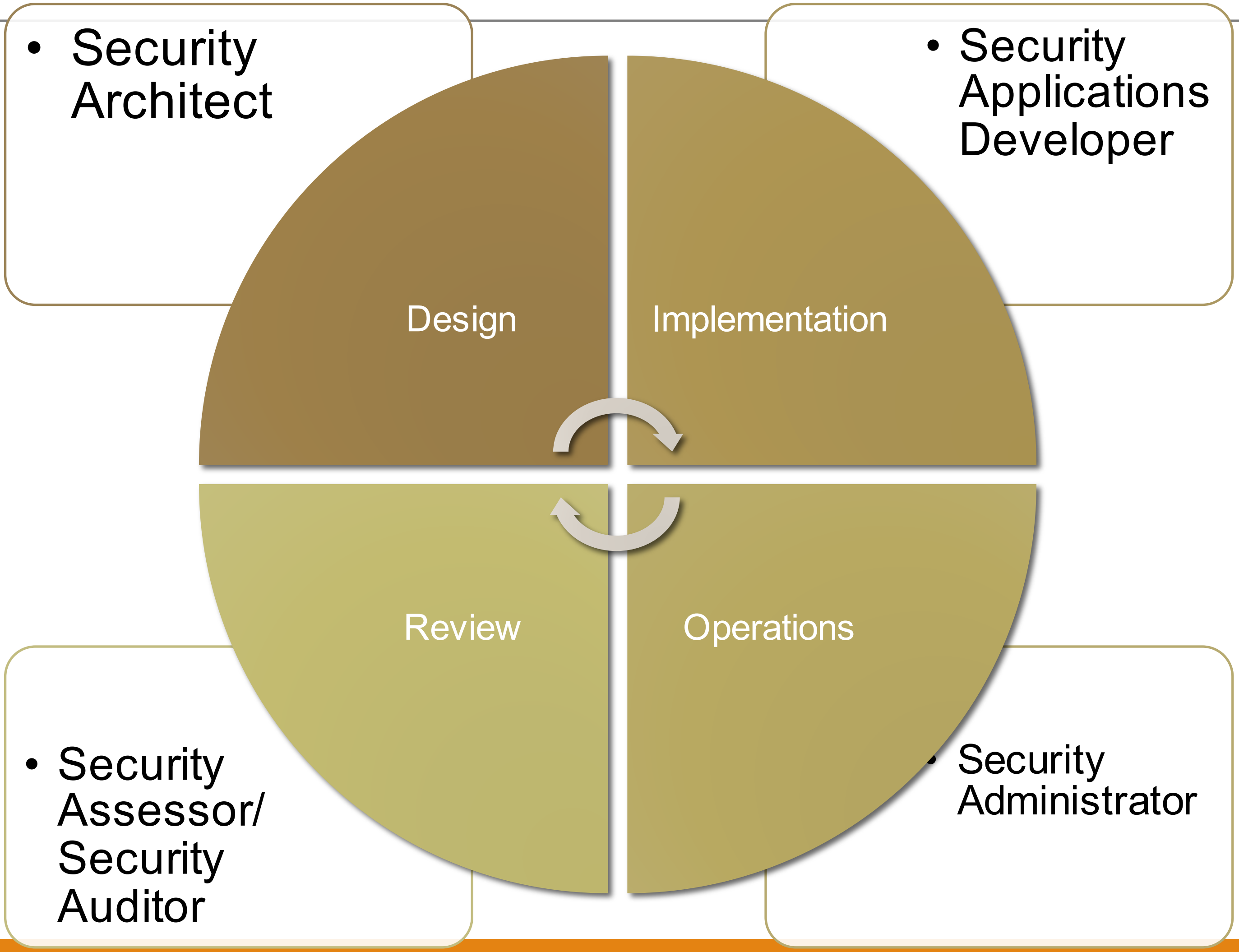
EC-Council

- CEH

SANS

- GCFA
- GCFE
- GREM
- GWAPT
- …

Security related work in HK industry



- Security Architect

- Security Applications Developer

- Security Assessor/ Security Auditor

- Security Administrator