Cloud Computing

- Cloud Issues and Challenges
  Standard and Law

Agenda

- Introduction
  - Issues & challenges
- Cloud Security
  - Security & attack
- Cloud Standard and Law
  - Guideline for secure cloud
  - Law and privacy

Cloud Standard and Law

Outline

- Introduction
  - Why we need a security standard and obey the law
  - Business, risk and money
- Cloud Security Alliance (CSA)
  - Governance and operation
- Law and Privacy
  - Which one is important
- Summary

Security

- A lot of cloud services are provided by many companies
  - Storage, web hosting, business model …etc.
  - Dropbox, Amazon EC2 and Salesforce.
  - Cloud computing is full range of services.
- Also, these are many traditional and cloud security issues
  - How can we go smoothly?

Security Issue

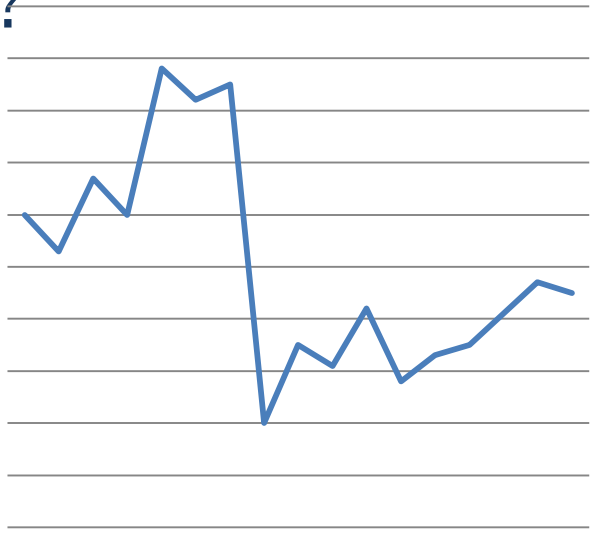
- Cloud computing is the subset of computer services
  - It also has the same problems of traditional security issue.
    - Hardware, software and management attacks.
- Cloud computing has other particular problem
  - Under the concept of on-demand service, users share all of the resources.
    - Incomplete isolation technique would increase the security risk.

Risk

- In addition to the security issue, users also concern the security risk
  - How about the security management?
  - How about the incident response and remediation?

Why so Serious?

- In companies, each time of security problem means an economic loss
  - Stopping service one hour not only stops making money but also loss the customers.
  - Company's reputation is the most important part.
- How can we find the best solution?
  - Where is the security guideline?



Back to the Cloud

- In recent years, cloud computing is popular and lots of companies want to join into this industry
  - Every company want to be the leader.
  - Every company want to design the standard.
- View to the security , there are lots of the cyber security standard
  - ISO 27002
  - NIST
  - RFC 2196
- There is the cloud security standards?

Cloud Security Alliance

Standard

- Cloud security alliance (CSA) is a not-for-profit organization
  - Try to promote the use of best practices for providing security assurance within Cloud Computing.
  - Provide education on the uses of Cloud Computing.
- CSA provides general views of cloud computing, security issue which may be encountered and some security suggestion
  - User can use the cloud control matrix to build a secure cloud environment

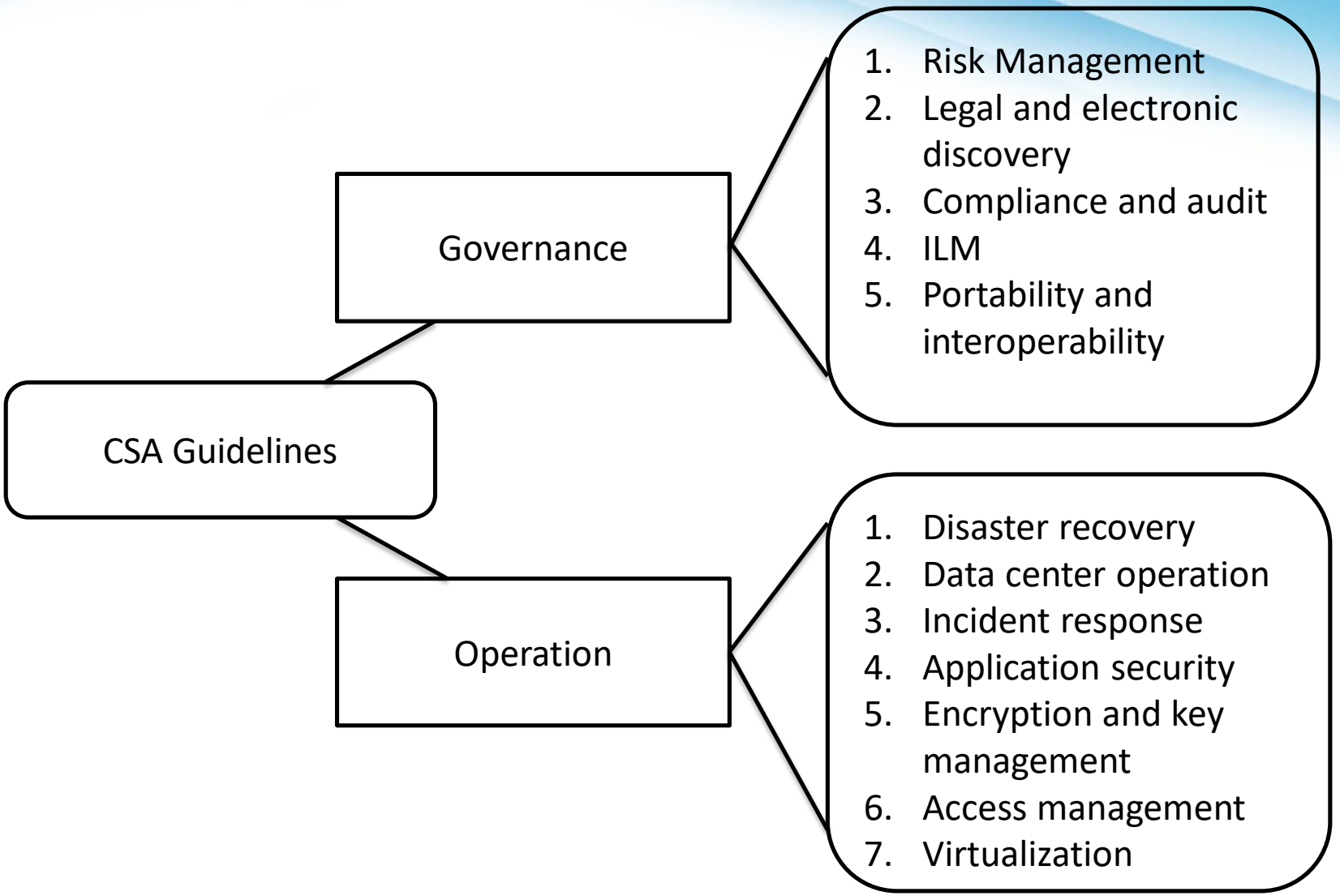
Security Matrix

Control Area	Control ID	Control Specification	Network	Compute	Storage	App	Data	Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		COBIT 4.1	
									SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer		
Compliance - Audit Planning	CO-01	Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.	X	X	X	X	X	X	X	X	X	X		ME 2.1 ME 2.2 PO 9.5 PO 9.6	45
Compliance - Independent Audits	CO-02	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)	X	X	X	X	X	X	X	X	X	X	X	DS5.5 ME2.5 ME 3.1 PO 9.6	45 45
Compliance - Third Party Audits	CO-03	Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements.	X	X	X	X	X	X	X	X	X	X		ME 2.6 DS 2.1 DS 2.4	45 45
Compliance - Contact / Authority Maintenance	CO-04	Liaisons and points of contact with local authorities shall be maintained in accordance with business and customer requirements and compliance with legislative, regulatory, and contractual requirements. Data, objects, applications, infrastructure and hardware may be assigned legislative domain and jurisdiction to facilitate proper compliance	X	X	X	X	X	X	X	X	X	X	X	ME 3.1	
Compliance -	CO-05	Statutory, regulatory, and contractual	X	X	X	X	X	X	X	X	X	X	X	ME 3.1	

Cloud Control Field

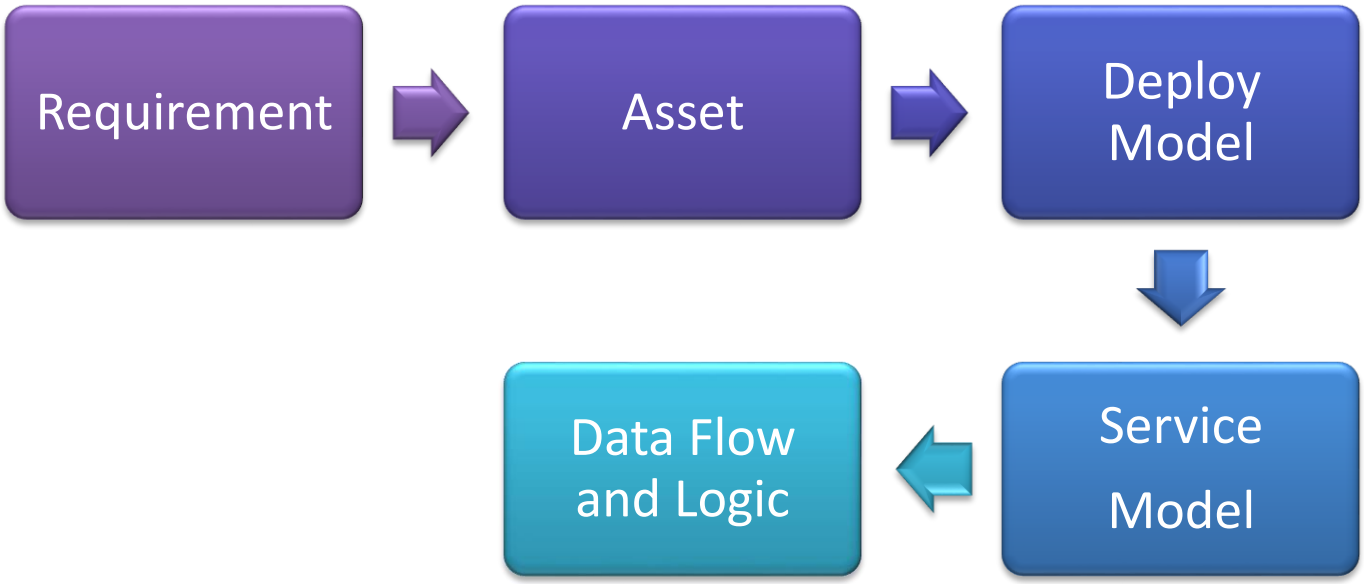
- CSA separates cloud computing into two fields which has total 12 subprojects:
  - Governance
  - Operation
- Cloud governance introduces how to build a secure cloud service
  - Cloud company build a secure environment.
  - How does the cloud customer choose a secure platform.
- Cloud operation introduces how to solve security problem and maintain a secure cloud environment.

Cloud Control Field (cont'd)



Before Join in Cloud

- CSA provides five steps
  - How to choose a suitable cloud platform



Before Join in Cloud (cont'd)

- Step 1: understand your requirement
  - CSA classify the usage of cloud into two classes: data and application.
  - Depended on your usage, understand which one is running on your cloud platform.
- Step 2: assess your assets
  - Depended on the important of data and application, you should provide difference level of security protection.

Before Join in Cloud (cont'd)

- Step 3: choose the deploy model
  - Depended on your secure requirement, different deploy model has difference default protection properties.
  - Private cloud in internal environment has highest default protection.
- Step 4: choose the cloud service model and vendor
  - SaaS has the lower responsibility and IaaS need to rebuild the security mechanism by yourself.
- Step 5: understand the data flow and program logic
  - Designed a reasonable and effective secure cloud service requires company full understand the workflow of service and possible threats.

Prepared

- After five steps, companies and customers can both select the cloud platform which meets the requirement
  - But there are many security issue need to be concerned.
- Combined with the full understand of requirement and classify the assert, cloud users could design the suitable secure environment.
  - Build the service environment or platform.
  - Operate the service.
  - Keep the service quality.

Governance

Operation

CLOUD SECURITY ALLIANCE

Governance

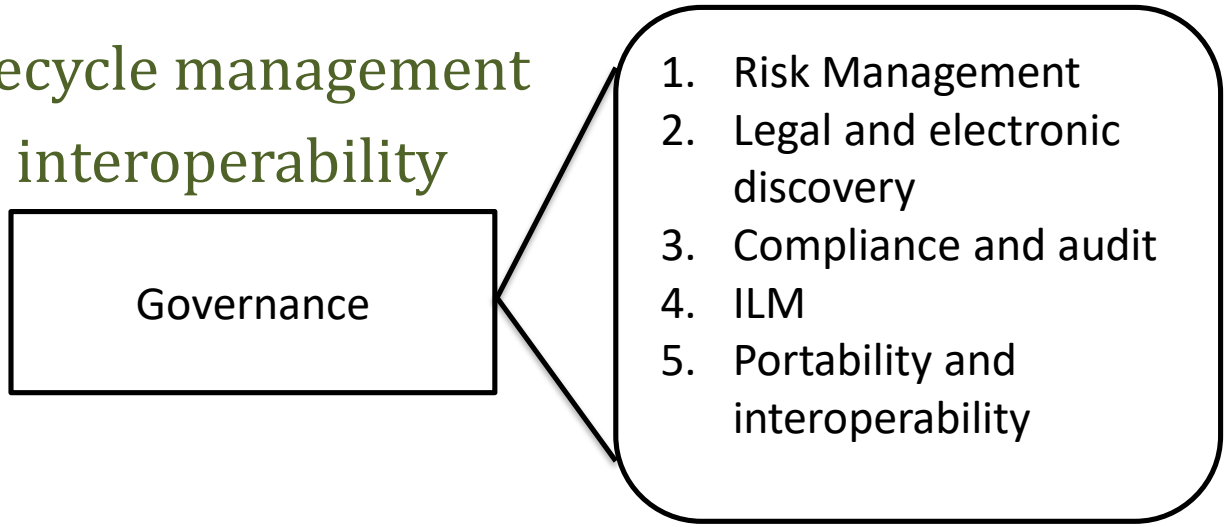
- Governance and enterprise risk management
- Legal and electronic discovery
- Compliance and audit
- Information Lifecycle Management
- Portability and interoperability

Governance

- In cloud computing, companies provide many services to users and customers use services what they need
  - How to reduce the security risk when using cloud computing?
- The security risk in cloud computing include
  - Any kind of emergency.
  - Audit and law problem.
  - Migration between two cloud vendor.
  - …etc.
- Governance is a guideline when choosing a suitable cloud vendor and service model.

Governance (cont'd)

- In governance field, CSA proposed five classes which need to be concerned and CSA given some suggestions
  - Governance and enterprise risk management
  - Legal and electronic discovery
  - Compliance and audit
  - Information lifecycle management
  - Portability and interoperability



Risk Management

- In cloud computing, an effective risk management follows a well-defined information security management processes
  - Extendibility
  - Reproducibility
- The management processes are elasticity when business growth and can be used in difference enterprises.

Risk Management

Management

- Enterprises should design the security metric and standard before design the security management
  - Everyone needs to understand and record the security metric.
  - Enterprises use parts of profits used in security controls.
  - Enterprises assess of audit to keep the security requirement.

Risk Management

Enterprise Risk

- Companies in cloud computing lose the control of system and security management
  - Service level agreement (SLA) is only one to ensure the risk management.
  - Enterprise should choose the cloud vendor which can provide the suitable SLA.
- Depended on SLA, companies usually cannot test the security management
  - Avoid to affect the other user.
  - Avoid to affect the QoS of cloud environment.

Information Risk

- Information risk management is used for information C.I.A. properties
  - Cloud users need to build the SLA requirement and collect necessary information to design the management policy.
  - In SaaS, the major security information are provided by cloud vendor.
  - In IaaS, users need to collect and control almost all of information.

Third-party Apps

- Cloud users need to review the information transfer chain between cloud service and third-party service
  - Service relation and dependence.
  - Cloud vendor's third-party application management
  - Response mechanism for service interruption
  - Third-party application's extendibility.

Legal and Electronic Discovery

Legal

- In cloud computing, data is not controlled by customers
  - Instead, cloud vendor hosts all data in cloud environment.
  - How to identify the liability is the important things.
- A complete cloud law management has three parts
  - Functionality
    - Definition the cloud service and functionality.
  - Judicature
    - Legal norms of cloud service and data management.
  - Contract
    - The structure of contract, terms, conditions and the law enforcement agencies.

Electronic Discovery

- Compared with traditional service
  - Cloud computing provides services anywhere and anytime.
  - Cloud computing uses virtualization that users unknown the location of the service and data.
  - The legal liability may be different in different countries.
- Difference countries has difference law norms
  - Electronic evidence.
  - Record system.
  - Management policy.

Legal and Electronic Discovery

Suggestions

- Both vendor and customer fully understand the roles of law
  - Electronic evidence, legal recourse and the expert testimony.
- Cloud vendor needs to keep the system secure
  - Provides reliability evidences when customers required.
  - Recover the data assets when customers terminate the contract.
- Cloud security agreement should be review and audit by third-party
  - Test QoS and detect the system vulnerabilities.

Compliance and audit

Compliance & Audit

- In cloud computing, the system separated into several parts
  - It is easy to extend, manage and operate.
  - It is hard to supervise and audit.
- Cloud auditors need to gain rich experience such that
  - Supervise the vendor easily and effectively.
  - Distinction between liability.

Compliance and audit

Readiness

- In cloud computing, companies should prepare well for audit
  - Legal department
    - Help to review the cloud service contract, supervise the cloud vendor and resolver the legal disputes.
  - Right of audit
    - Cloud service contract should be changed to satisfy the customer's requirement.

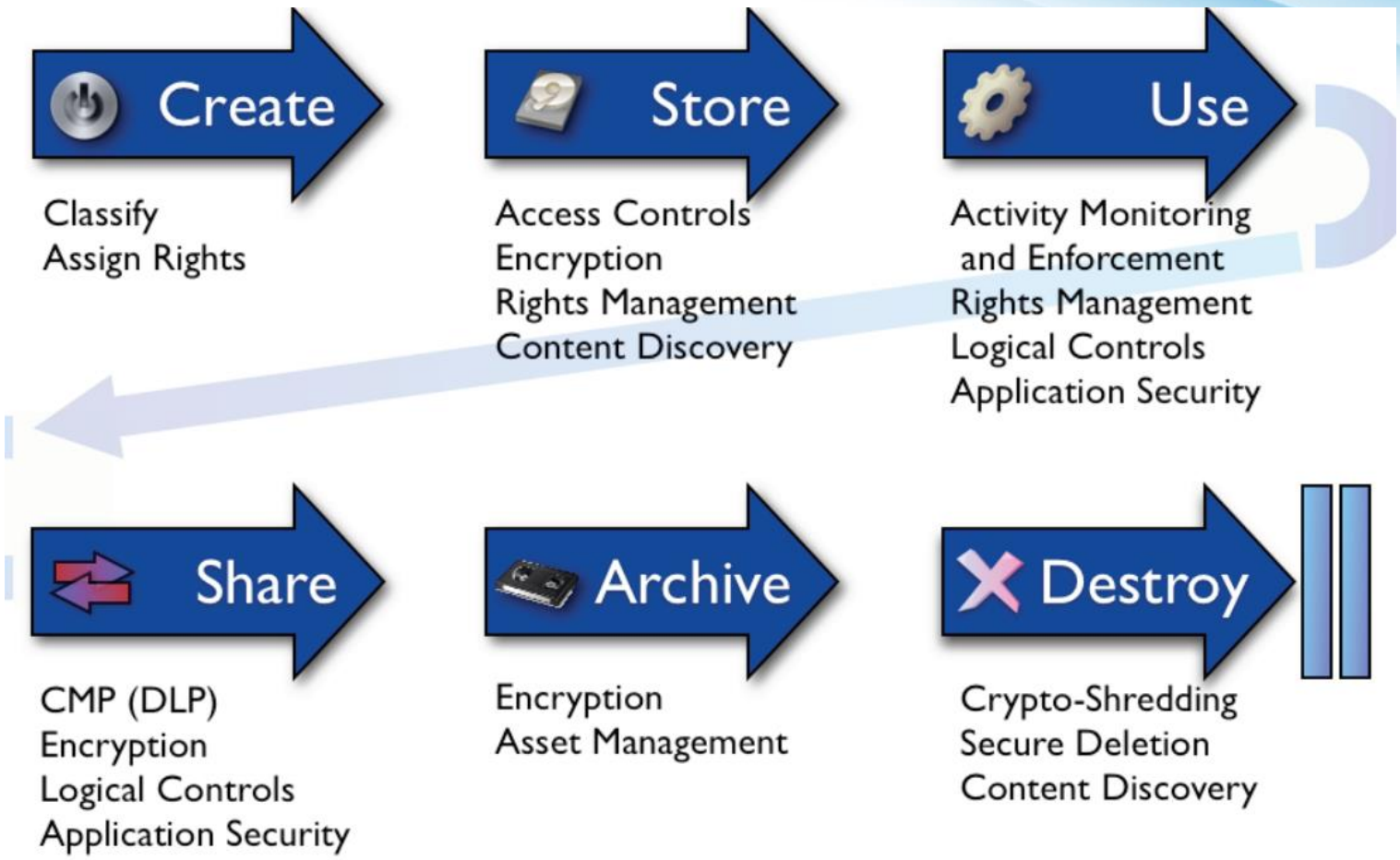
Information lifecycle management

ILM

- The goal of information lifecycle management (ILM)
  - Improve the system performance.
  - Increate the service functionality.
- In cloud computing, data security lifecycle is challenged
  - More elasticity
  - Multi-tenant
  - The new design concept of logic
  - Public environment
- Cloud users should care about the six phrases of data life

Information lifecycle management

ILM (cont'd)



Information lifecycle management

Suggestion

- Cloud customers should understand the full secure process of data
  - include storage location, encryption method and management policy.
  - should be written in the SLA.
- Understand the data could be confiscated
  - Cloud vendor need to notify the users.
  - Cloud vendor need to protect the data which cannot be modified or damaged.

Information lifecycle management

Suggestion

- Only the data owner has the right of access control
  - Cloud vendor need to disable all access at the beginning.
  - Even cloud vendor's staff cannot access the data without the permission.
- Understand the security boundary
  - The encryption system, key management and how to choose the security key.
  - The data isolation technique, backup and recover system.

Portability and interoperability

Portability

- Cloud computing is the new service model for companies
  - Company choose the cloud vendor by cost, service quality, properties and other factors.
- Company may migrate from one cloud vendor into another cause by
  - New service contract would increate the operating costs.
  - Cloud vendor ceases operation or stop providing some services.

Portability and interoperability

Interoperability

- Companies need to design the system and secure guideline for particular cloud vendor
  - Migrate to another vendor would need to modify the system or re-build the new system.
- The difficulty of porting service platform depends on the cloud model
  - SaaS usually concerns the data and service platform.
  - IaaS needs to consider the underlying system which may be incompatible.

Portability and interoperability

Suggestion

- Understand the storage space and the bandwidth of network before migration
  - Depending on the other user's experience, migrate the physical machine usually more effective and less cost.
  - Record all the detail when migration.
- For IaaS
  - Understand the image compatibility before migration.
  - Understand the subsequent disposal when hardware are eliminated

Portability and interoperability

Suggestion (cont'd)

- For PaaS
  - Understand the migration tools what vendor provided.
  - Understand the migration affect include performance and QoS.
  - Understand how to test and examine the new environment.
- For SaaS
  - Data duplicate and backup periodically.
  - The customized plug-ins should able to be re-build.
  - Understand any migration laws and regulations.

Governance

Operation

CLOUD SECURITY ALLIANCE

Operation

- Users or customers could be encountered the security problem on cloud
  - Difference between traditional data center and cloud.
  - Security problem on large scale data center.
  - Backup and recover policy.
- CSA provides many suggestion
  - Any kind of secure events occurred when company run the service on the cloud computing environment.
  - The secure factors need to be concerned.

Operation (cont'd)

- Similar with governance, CSA proposed five classes which need to be concerned and CSA given some suggestions
  - Traditional security, business continuity and disaster recovery.
  - Data center operations
  - Incident response, notification and remediation
  - Application security
  - Encryption and key management
  - Identity and access management
  - Virtualization

Disaster recovery & Data Center

Disaster Recover

- Similar with traditional data center, cloud computing needs to design the policy of business continuity planning (BCP) and disaster recover(DR)
  - Every components in system could be failure.
  - The large system is hard to keep the system stability.
  - The disaster, like file disaster or earthquake, could damage the cloud infrastructure.

Data Center

- Service-level agreement (SLA) is part of service contract
  - Classify the service and define the delivery time or performance.
- Traditional data center usually allocates the fix number of server or resource to customers
  - It is easy to overestimate or underestimate.
- How to dynamically allocate all resource?
  - Reach the SLA requirement.
  - Reduce the probability of overestimate

Disaster recovery & Data Center

Suggestion

- Keep in mind: centralized management means concentration risk.
- Cloud vendor needs to have a strict management mechanism
  - Access control and manage policy.
  - Background checks of employees.
  - Internal/external security control file.
- Cloud customers should be possible to
  - On-site investigate the cloud infrastructure.
  - View and understand the BCP and DR.

Disaster recovery & Data Center

Suggestion (cont'd)

- Companies need to understand the contract of
  - Recovery time
  - Recovery object
  - Recovery policy
- Customers need to gain the right or permission
  - Audit the SLA by third-party.
  - Understand the process, policy and affect of system patch.

Incident Response

- The properties of cloud computing could be hard to manage and response the incident events
  - Large scale, shared resource and automated management.
  - Cloud vendor needs a standard operation process (SOP) for incident response.
- The cloud vendor provides the complexity and large-scale service
  - It is hard to monitor the traces and response the incident immediately.
  - Each services could cross-impact the management policy.

Views

- View for monitor
  - We need the security operation center (SOC).
  - Each new services and resources should be monitored by SOC.
  - SOC provides the notification and guideline for emergency or security events.
- View for customer
  - Customers need to evaluate the SLA which meets the requirement or not.
  - Customers should understand the SOP for incident response.

Standard Operating Procedures (SOPs)

Suggestion

- Before using cloud computing
  - Define the normal events and unusual events.
  - Test your system which is compatible with cloud environment or not.
- SOC is usually used in single or pure environment
  - In multi-tenant environment, SOC needs to be modified to monitor data from any source.
  - Application layer firewall and log file are helpful on multi-tenant for SOC.
- Each sensitive data should be encrypted to reduce the losses.

Application Security

- In cloud computing
  - Cloud vendor provides the environment to users.
  - Users run the applications which may be designed by users or third-party.
- Similar with normal applications, services in cloud also need to well-design and keep it secure
  - Preliminary analysis and confidentiality
  - Integrate and availability tests
  - Demilitarized Zone

Interoperation

- Services and applications in cloud interactive frequently
  - The dependencies between applications affect the system security.
  - Third-party applications also can damage and change the system stability.
  - The test tools cloud vendor provided can help system to enhance system security.

Suggestion

- In the application development lifecycle, we need to concern the three parts
  - Security threats and trust model.
  - Cloud platform program assessment tool.
  - Application's quality check point.
- Keep in mind
  - Cannot suppose all communications are in security channel.
- The storage and management for application certificate are important.

Encryption

- How to avoid the data be theft is the important security issue
  - Cloud vendor cannot guarantee that sensitive data be in the secure protection.
  - The encryption is the efficient way to protect the important data.
- In some country, data which is hosted or must be encryption
  - Personal information.
  - State secure file.
  - …etc.

Key management

- The encryption system can provide the information security for data
  - Dependent by the encryption algorithm, e.g. Caesar shift or AES.
  - Dependent by the key selection.
  - Dependent by the key management.

Management

- Encrypting and decrypting data costs many resource and time
  - Classify the data by sensitive and importance.
  - Choose the suitable the encryption algorithm.
- In cloud, encryption system is frequency used
  - Simple or common password is useless.
  - A non-secure key management would damage the encryption system.

Encryption &
Key Management

Suggestion

- Cloud customers need to understand the encryption system using in cloud
  - Encryption algorithm and costs.
  - Key management and Key generation policy.
- Customers need to specify the encryption service in SLA
  - The encryption system should be audited by third-party.
  - Limitation for length and strength of key is required.

Access Management

Access Control

- After keeping data in security environment and encryption, we need to understand the access control policy
  - Guest can accessed the sensitive data is dangerous.
- In cloud computing, number of users is larger beyond our imagination
  - Complex of access control policy
  - Add / delete user's access right immediately.
  - Identify and authorize the user.

Access Management

IAM

- The identify and access management (IAM) system in cloud should be fair and rigorous assessed
  - Identity provision
  - Authentication
  - Union management
  - Authorization and user configuration
- Customers can use the third-party authorization
  - OpenID, Google or Facebook
- Cloud vendor need to provide the (single sign-on) SSO
  - Avoid the repeated login

Virtualization

- In cloud, virtualization technique is widely used
  - Abstract and integrate the resource.
  - Easily to provide the on-demand resource to users.
- Virtualized resource means mix all resource
  - Concentration of risk.
  - Each user must meet the secure requirement.
- Hypervisor monitor and communicate with virtualization machine (VM)
  - Break the hypervisor could break all system.
  - Attacking to hypervisor is the new malicious methods.

Suggestion

- Understand the virtualization technique used in cloud environment
  - The security and isolation of hypervisor.
  - The default configure and setting must be secure.
  - The resource image of VM must be tested and verified.
- The hypervisor owns the high secure permission
  - Only few staff and users has the right to access the hypervisor.
  - Each access to hypervisor must be recorded.

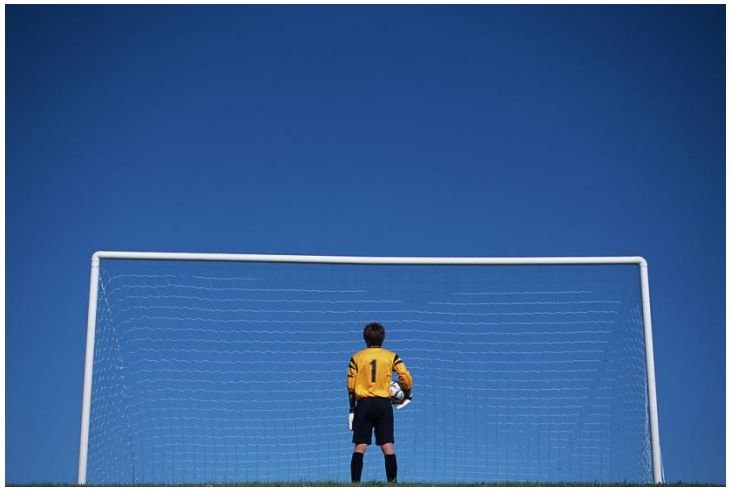
Summary

- Cloud security alliance (CSA) provides the security guidance and separate cloud security
  - Two field: governance and operation.
  - Twelve sub-categories.
- Each sub-categories introduce the problem could occurred and given some suggestions.
- In three service model, CSA provides the general views and give difference suggestions for difference model.

Law and Privacy

The Real World

- Like the real world, criminals are around of us and we can be the victim anytime and anywhere
  - In the computer would, crackers hide in the network and try to attack anything interesting.
  - Lawless employees also try to sale the sensitive and important data.
- Law is the last line of defense.



Enforcement

- Users try to believe the performance and protection what company claim
  - But lots of security incidents are frequency appeared in the news.
    - In 2011, Dropbox claims all data in server are encrypted, but…
  - User are beginning to doubt the company's guarantee.
- Law can provide the basic protection
  - Company needs to provide the basic security protection and basic quality of service.
  - Also, law resolves the dispute between user and company.

Online Shopping

- It is popular and convenient to purchase on the internet
  - People can buy books, foods, and the car on the web.
  - People could not see the product until receive the product.
- There are many problems on online shopping
  - There are some difference between image and product.
  - It may be some mistake on the price.
  - The personal information could be hijacked or therft.

Security Protection

- On the customers view
  - All personal data must be under the full protection.
  - Everything must be meet the description of the product.
- On the companies view
  - Security protection is not just the responsibility of the company.

- But world is not all liking wishful!

Privacy

- On the other hand, the privacy is the basic personal right
  - No one shall be subjected to arbitrary interference.
  - Everyone has the right to the protection of the law against such interference or attacks.
- The privacy includes
  - Personal information.
  - Religion and sexual orientation.

Net Generation

- Now is the net generation
  - Every teenager is living in internet.
  - Everyone can find lots of interesting information in internet.
    - Phone number, intimate photos or contents of email.
- Users need someone to protect the privacy
  - The law and government can provides the basic and strong protection.
  - But in sometime, the law is also broken the right of privacy.

Information Protection

USA PATRIOT Act

LAW AND PRIVACY

Personal Information

- Everyone in the internet would leave some traces
  - User leaves the personal information to apply for Google and Facebook account.
  - User leaves the name, phone number and address to buy something.
- This information can be used on some malicious behavior
  - Fake identity.
  - Internet fraud

Law of Personal Information

- In 2010, Taiwan government enact laws to protect the personal information
  - It specifies the limitation of personal information collection, process and usage.
  - Companies need to provide the evidence actively to exclude the liability.

Clause

- There are many clauses to specify the usage of personal information and the penalty of breaking the law
  - Everyone can apply for compensation top to twenty thousand when personal information has been violated.
  - When a crime occurs, companies need to provide the evidence that they has been meet the requirement of the law.

Company Risk

- From the probability point of view
  - Each company may lose the sensitive information.
  - Cloud company has lots personal information.
  - If company lost 1/20 data (e.g. Five thousand data)
    - Fines would be up to one million NT dollars.
  - Also, company lose his corporate image.

Traces

- Companies are invested in the preservation of evidence to avoid penalties of laws
  - Companies try to keep traces and logs which records all operations.
- The record system must be stable and reliable
  - But there are few guideline used for record system.
  - Company also need to modify all system to interact with record system.
    - It would be complex, massive and expansive.

When Crime Occurred

- The traces is the first solution used to identify the attribution of responsibility
  - Traces must be clean and cannot be modified.
  - The method of keeping trace also need to be trusted.
- But unlike the fingerprint or DNA, electronic evidences are easier to modify or fake
  - Keeping the isolation between traces and system is important.

In Cloud

- In cloud computing
  - Traces would growth into a massive and large size such that finding the crime evidence is difficult.
  - The large size of traces means the difficult of keep record stable and reliable.
- How to duplicate, isolate and manage the traces?
  - Replica and off-site backup.
  - Automation and systematization.
  - Reduce human intervention.

Information Protection

USA PATRIOT Act

LAW AND PRIVACY

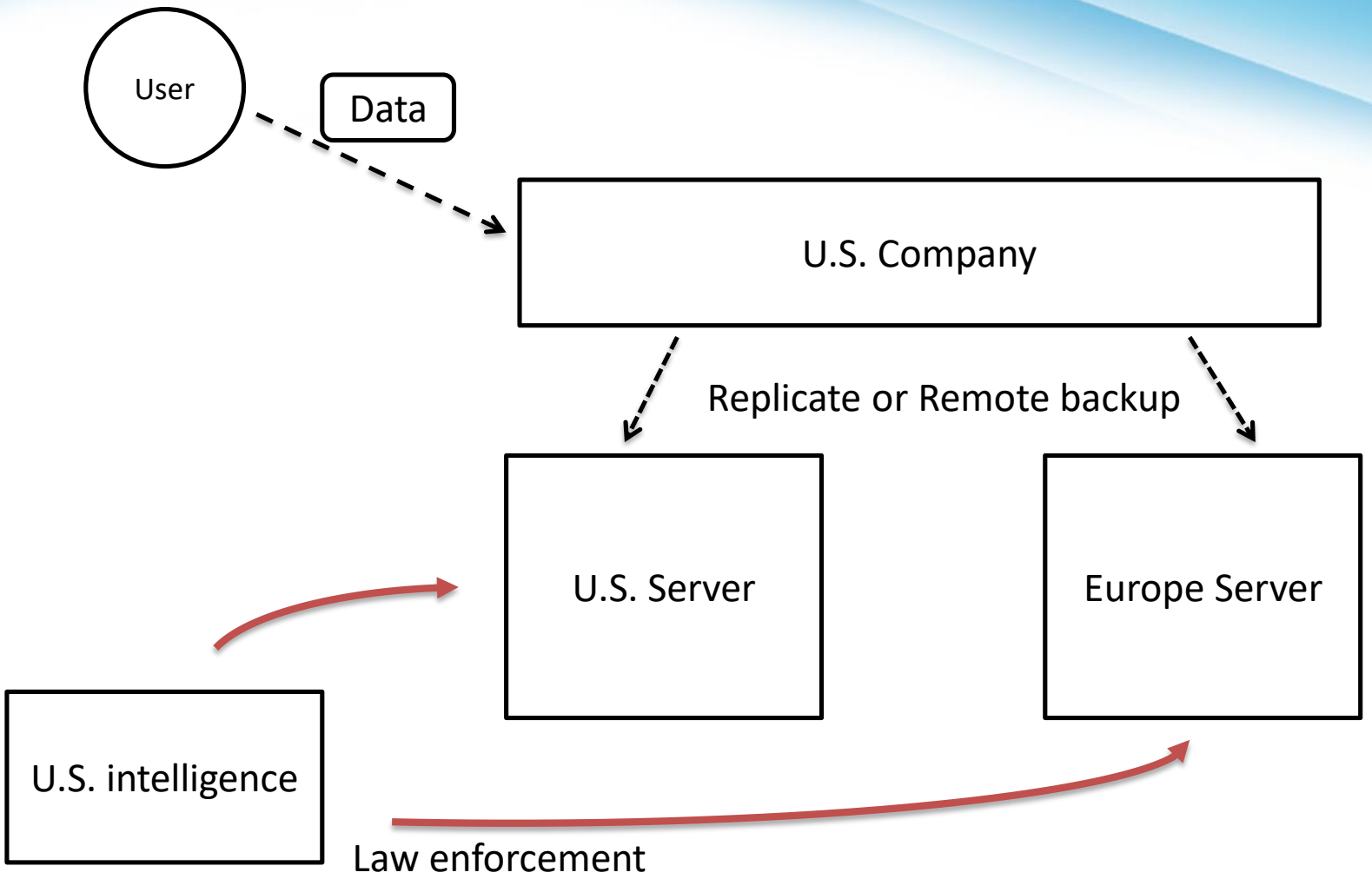
Outside the Law

- In a special case, law may be outside the country
  - One user in A country would be under the law of B country.
- Cloud provides service to anywhere on the world
  - Server and user are usually located at the difference country.
  - Have Foreign country the right to access the user data?

USA Patriot Act

- One of the most important news in cloud computing is USA patriot act
  - U.S. government has the right to access all of data in the U.S. country.
  - Also, U.S. government has the right to access the data which is hosted by U.S. companies no matter what the data at USA or at foreign country.
- Microsoft and Google recognized to provide the data to the U.S. intelligence
  - The data are located on the server in Europe.

USA Patriot Act (cont'd)



Affect

- Users mistrust the cloud service
  - User data could be access without any permission.
  - User cannot keep secret in the internet.
- Lots of important institution are limited to use the cloud service
  - The sensitive data, important service and technique cannot be hosted on the cloud companies.
  - If necessary, all data must be encrypted and independent stores the key.

Summary

- Cloud computing is the new industry
  - The laws grow up slower than cloud computing service.
  - The old provision cannot meet the companies' or customers' requirement.
  - The new provision still not well-develop.
- Depending the properties of cloud
  - Cloud computing service cannot avoid the need to provide cross-country service.
  - There may have some conflict between local laws and foreign laws.

Summary (cont'd)

- The privacy is the popular issue for cloud security issue
  - Cloud services is growing rapidly and around of our life.
  - Cloud vendors and companies own lots of customers private information and data.
- The law is used to protect our right
  - When government needs to protect the most people, the privacy of small number of people will be violated.
  - Who wants to be a small part of the victims?

Reference

- Cloud Security Alliance (CSA) https://cloudsecurityalliance.org/
- News
  - http://www.zdnet.com.tw/news/software/0,2000085678,20126532,00.htm
  - http://www.informationsecurity.com.tw/article/article_detail.aspx?tv=11&aid=6286
  - http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021
- All resources of the materials and pictures were partially retrieved from the Internet