Week 5 - 8 Notes

[**Week 5: Access Control Concepts**](#_esh1bukbz2fv) **5**

[Access Control (访问控制)](#_ub394mheopx7) **5**

[What (Definition: 定义）](#_qqf3xd2a3joh) 5

[关于Access Control 的单词/词语：](#_jm3lgzn08746) 6

[Access Control Concepts (5个概念):](#_mtsyycrsf8x) **7**

[Identity (身份)](#_ypp2zqqeo3et) 7

[Uniqueness (唯一性)](#_lpsjdst5ektl) 8

[Definition (定义）](#_eo2x9n4ek2jo) 8

[Examples (例子)](#_u9htqb9tevrm) 8

[Non-descriptive (非描述性的)](#_xhgq2ud3whx3) 8

[Definition (定义）](#_vx3v7gxq9z0k) 8

[Examples (例子）](#_t1a308zbrpq7) 8

[Issuance (发行)](#_sk52ckzhbdgc) 9

[Definition (定义)](#_an8x4o5idbnt) 9

[Examples (例子）](#_kpsu2g1sgkf5) 9

[Identification Component Requirements (标识组件要求)](#_ibt91byq8io6) 9

[Identification and Authentication(识别和认证)](#_ndmokuwore60) 9

[Definition:](#_juiowq4t6u7x) 9

[Example:](#_bw5v5en9l0i9) 10

[Authorization (授权)](#_sqklbv81kk6p) 10

[Identity Management 身份管理](#_x1cli6tllkv8) 11

[Accountability (问责制)](#_a9h60kkx9d86) 12

[What to keep in mind when dealing with auditing](#_4kji8srdxarw) 13

[Password Management](#_ahovvs18vw6m) 13

[Password security](#_furzlj5j0js6) 14

[Tutorial Week 5](#_s2lilokj06c1) **14**

[Question 1](#_qr0s7wjnfdrx) 14

[Three diff factors](#_6tunqjpzkjhl) 14

[Two Factors Necessary (Choose 2 from above)](#_pepxq3vtqu1g) 14

[Question 2](#_jy1eroqln4uv) 14

[Question 3](#_hlhuy5cc9l4o) 15

[Question 4](#_hw3tcwfkophw) 15

[Question 5](#_eldhenanwb01) 15

[Physical Preventives](#_tzk6jl2n505j) 16

[Physical Detectives](#_u9dj2vp87e9j) 16

[Technical Real Life examples:](#_kyhtfi9zc0xz) 16

[● Online banking includes the:](#_waot7sxt6sks) 16

[● School security system](#_p5sk2ienz7k9) 16

[Administrative Real life examples:](#_e3nypfmq7a2u) 17

[Question 6](#_obklzg11ply3) 17

[Question 7](#_zgo9ldgwqpw0) 17

[Question 8](#_2e7w41q18udh) 18

[Corrective control](#_llysn5hclw9j) 18

[Recovery control](#_ltzx6lnw74jc) 18

[Question 9](#_98vei61mqfcv) 18

[Example of lack of Administrative Control](#_hocb97vxg966) 19

[Question 10](#_6p80xr8stvdx) 19

[C.E.R.T](#_30ykg6ammrpg) 19

[CERT Australia](#_yqgw9xll6qqu) 19

[AusCERT](#_lfzarh1yilcc) 19

[Question 11](#_50cxd9gox1f3) 20

[Targets](#_q6cdm6ia0fhl) 20

[How](#_b4xk1577artj) 20

[Week 6: Access Control Practices](#_f9yd052sw9ct) **20**

[Access Control Practices](#_rrp0o15mq86s) 20

[Security controls 安全控制](#_7n6txfua8ksw) 21

[Definition](#_uefyeo5x7nf0) 22

[Advantages](#_mjbqtxn2n6qh) 22

[What is it for?](#_980vpcxju2ts) 22

[There are Two ways of categorising Security Controls: 有两种方法可以对安全控制进行分类。](#_csngk2h6ayru) 23

[1. Administrative Controls](#_qbbj3062q56y) 24

[Definition](#_5dm3qufilcf5) 24

[Categories of Administrative Controls:](#_q3piybpqey0n) 24

[Importance of Administrative Controls:](#_uh83dktclfd6) 24

[Examples:](#_xkbx1m6xlwp1) 25

[2. Technical Controls (aka Logical Controls)](#_5xufqkm5ilim) 25

[Definition:](#_5n3kllkv6okj) 25

[Importance of Technical controls:](#_vio2y29s30tz) 26

[Examples：](#_wafo972twmi7) 26

[Preventative](#_1el25sdet6ru) 26

[Detective](#_fjhqscjwycne) 26

[Corrective/Recovery](#_vbsyc87h8zp6) 26

[3. Physical Controls 物理控制](#_flcx9efs6nbk) 27

[Definition:](#_1jz1gdhpnpw8) 27

[Importance of Physical controls:](#_4e7nvxw7g6yn) 27

[Examples:](#_u92zh91i2j9c) 27

[Categorising according to the different phases of the control process](#_q3v7cq3zh35n) 28

[A general example:](#_b8orhzam4v4x) 29

[Real-life Example](#_sk56om5q1r24) 30

[Commonly Used Security Methods 常用的安全方法](#_vlurd1gy8abq) 30

[Least Privilege](#_bzb8cpciaxyp) 31

[Advantages:](#_3d72du39v0bo) 32

[Disadvantages:](#_ouzm2idelzdc) 32

[Importance:](#_83qjanm83in7) 33

[Defense in Depth (multiple types of security controls in different layers)](#_evhdmfysu3pz) 33

[● Advantage](#_fpsxne47kc8y) 33

[Minimisation](#_4w7yq2mi8jsv) 35

[Keep Things Simple](#_vwhjmqu1rrpw) 35

[Compartmentalisation](#_ci950h30yjh1) 36

[Tutorial Week 6](#_y5138qmapvvj) **37**

[Question 1](#_dwen1mwlrv6w) 37

[Confidentiality](#_4bp5qspn62kn) 37

[Availability](#_1k5ffuwaunwv) 37

[Integrity](#_opc8t3hva2o8) 37

[Three types of control](#_uzpfe3l0jvbu) 37

[Preventive controls:](#_5q67qfvvcdz3) 37

[Technical Controls:](#_a88rpf5mlyvc) 38

[Question 2](#_2fql0cktgb21) 38

[Availability](#_ioyj0ndizzg4) 38

[Administrative](#_nxm7wtj5ui0i) 38

[Physical](#_n9afk7pjkn2i) 38

[Question 3](#_1afzrkl2zq0e) 39

[Minimisation (similar to least privilege)](#_lec2wy4ou8bk) 39

[Leverage unpredictability](#_pzyfci1jkjvt) 40

[Question 4](#_jqms54471hzg) 40

[Least privileges](#_ef1bn5chr040) 40

[Compartmentalisation](#_mivwpl1idnyz) 40

[Compartmentalise :](#_8ef9lex8fri) 40

[Defence in depth](#_c7omn88pvf8i) 41

[Question 5](#_adi3myxvuxfl) 41

[Question 6](#_pbtjv2k0l171) 41

[Ports and Protocols](#_3ygbr541ntmc) 43

[Question 7](#_onxkk1tbdzcm) 43

[Physical Preventive:](#_5awq9jorxjyg) 43

[Physical Detective :](#_pub6qw15pmvx) 44

[Defense-in-depth:](#_qcnu15cuejxz) 44

[Question 8](#_6wra52e338zp) 44

[Question 9](#_r99gly1g3w93) 44

[Least Privilege](#_wqfcgzbkd6qq) 44

[Minimisation](#_1rwqk2jpja8s) 44

[Keep things simple](#_jv8qmje2jpty) 44

[Question 10](#_ezxo3klefd2e) 45

[Deterrent control](#_g5cnk49gkm9g) 45

[**Week 7: Busniess Continuity I**](#_b2lbgti7nhvt) **45**

[Comprehensive approach to business continuity plan](#_u2f65gseca2x) 45

[Risk Management 风险管理](#_fskhaxn7ev6t) 46

[Risk Management 风险管理](#_kaj65x4w65i1) 46

[Risk management plan consists of three stages](#_6wdttmbrgi7) 47

[1. Plan 计划](#_nzocscr1yhg5) 47

[2. Collect information/perform risk analysis 收集信息/进行风险分析](#_36vq2xf2tnk4) 47

[3. Define recommendations 确定建议](#_jllft3hg8zfb) 47

[How to determine risk 如何确定风险](#_le9r6jy072vd) 48

[● Likelihood 可能性](#_cbrgcmuol49p) 48

[Residual risk 剩余风险](#_rawc8grbg0jn) 49

[Risk Management Plan 风险管理计划](#_wbva6waj2m6k) 51

[Risk management involves three major undertakings:](#_xp0iqenlvebj) 51

[Risk management: formal process 风险管理：正式程序](#_qs4j0s75l79) 52

[Who is to undertake this risk assessment, and How](#_1azsza83mzrp) 52

[Single Loss Expectancy 单次损失预期](#_k4ewieq129kt) 56

[Annualized rate of occurrence (ARO). 年化发生率（ARO）](#_ff86ic1wcz6e) 57

[The Cost Benefit Analysis (CBA) Formula:](#_e258zaf6uuxs) 58

[Risk Analysis](#_k4ggljltsvb6) 61

[Purpose: 目的](#_qnkqd9e2cld4) 62

[Definition: 定义](#_ohaap0jdb1tj) 62

[What Risk Analysis do: 风险分析的作用](#_x7sqjp3h1ud3) 62

[What should be done by a team:一个团队应该做什么](#_qwouiuh3vad6) 63

[Strategies to Address Risks](#_m4ggjg2gz7q2) 65

[Defend 保卫](#_x3yg29h2iwwt) 65

[Transfer 转移](#_j7q17yopvv02) 67

[Mitigate 缓解](#_dp2zfvnb46q4) 68

[Terminate 终止](#_jageusveoggt) 68

[Accept 接受](#_cajhc0apu9dy) 68

[Asset Management](#_22tm0afsj7yk) 70

[Change Management](#_vdyvcc6ih2at) 73

[**Tutorial Week 7**](#_8f5t3i94j94h) **90**

[Week 8: Business Continuity Planning II](#_49k9982o4zao) **101**

[Business Continuity Planning 业务连续性规划](#_4i2udpbl5mzu) 101

[Definition:](#_57f7kveotqzq) 101

[BCP purposes:](#_mberytcsjl5u) 101

[Disaster Recovery Planning 灾难恢复计划](#_avt3gkn997gq) 101

[Requirements](#_slee2qi53b6l) 102

[Disasters 灾难](#_7gnrnjjvzet) 103

[BCP Process](#_o0evdp9q4jxo) 103

[Initiation Process of BCP | BCP before carrying out过程](#_to3px4selp97) 105

[Business Impact Analysis 业务影响分析](#_o2bq0iaa8tn1) 106

[Maximum tolerable downtime (MTD) 可容忍的最大停机时间](#_fpxfk3433dyi) 109

[Examples](#_76us2hc9l69u) 110

[The recovery point objective (RPO) 恢复点的目标](#_sawv3587ai7a) 111

[Definition:](#_y8ec3rrji3o7) 111

[The recovery time objective (RTO) 恢复时间的目标](#_tj8co2qlp5zw) 112

[Definition:](#_kua24blar2l3) 112

[Work Recovery Time 工作恢复时间](#_xiczzs1nvlx3) 113

[Definition:](#_j7le46c40p9e) 113

[Examples of Recovery Parameters 恢复参数的例子](#_d1du54djmhot) 113

[Recovery Parameters Timeline 恢复参数时间表](#_wgfm5fb11ziv) 116

[Recover Time over Complexity of Method 恢复时间超过方法的复杂性](#_gd9lw5xk0z) 117

[Optimum time to set RPO, MTD and RTO 设定RPO、MTD和RTO的最佳时间](#_sypoirt2ljda) 117

[Offsite Facilities (related to RTO) 场外设施（与RTO有关）](#_a6rgjy1punba) 118

[Alternate Processing Facilities 替代处理设施](#_9nwo1yfr4bcy) 118

[公司可以从三种主要的租赁或租用的场外设施中进行选择：](#_kvez50qgt06t) 119

[1. Hot site](#_gxmfkvxoskoo) 119

[2. Warm site](#_1gfjnoja3s7n) 120

[3. Cold site](#_dudpgl9wwh0c) 121

[Conclusion](#_g3qzrqinrig7) 121

[Quick overview of the differences between offsite facilities:](#_l6qbaknjmdbb) 122

[Hot Site Advantages](#_rmih368mg3rm) 122

[Hot Site Disadvantages](#_gtw2faj3z3uc) 122

[Warm and Cold Site Advantages](#_y6c8g0vi56m1) 122

[Warm and Cold Site Disadvantages](#_pmwxuz1bf6fx) 123

[4. Tertiary Sites 第三级网站](#_wpemi3nhn1ym) 123

[5. Reciprocal Agreements 互惠协议](#_vezlgmedfdtw) 123

[Important issues need to be addressed before a disaster hits if a company decides to participate in a reciprocal agreement with another company:](#_d5k6mqkfk74d) 124

[Offsite Location 场外地点](#_gw7rle46z3) 125

[Redundant Sites 冗余站点](#_fxhj0hr34mbt) 125

[Contingency Plans 应急计划( Discovery Recovery Planning: DRP)](#_97nwaduxx6hf) 126

[Supporting information & Appendices 支持性资料和附录](#_yy1480gz9ilh) 126

[Main phases 主要阶段](#_wi6egd63mmxf) 126

[1. Supporting information and Appendices 支持性资料和附录](#_7bm78zhx64lz) 127

[2. Activation and Notification Phase 激活和通知阶段](#_tmy2smrxaug6) 128

[3. Recovery Phase 恢复阶段](#_f57f17kmdeh7) 130

[4. Reconstitution Phase 重组阶段](#_1b4kj8pndl7) 133

[**Tutorial Week 8**](#_3wlkjsaezw3r) **135**

## Week 5: Access Control Concepts

## Access Control (访问控制)

### What (Definition: 定义）

* ***Access controls*** are security features that control how users and systems communicate and interact with other systems and resources.

Access control 是一种控制users怎么运用其他系统和资源的安全功能

* They protect the systems and resources from unauthorized access and can be components that participate in determining the level of authorization after an authentication procedure has successfully completed.

它们保护着系统和资源,防止資料 在未 獲授權情況下存取，并且可以是在身份验证过程成功完成后参与确定授权级别的组件.

* Access control is a broad term that covers several different types of mechanisms that enforce access control features on computer systems, networks, and information.

Access control 是一个广义术语，涵盖了几种不同类型的机制，这些机制在计算机系统、网络和信息上实施访问控制功能

* Access control is extremely important because it is one of the first lines of defense in battling unauthorized access to systems and network resources.

Access control 的重要性在于它是与未经授权访问系统和网络资源作斗争的第一道防线之一

### 关于Access Control 的单词/词语：

Identification

• Subjects supplying identification information - 主体提供身份信息

主题(subject)代表着使用者, 物体（object）代表着被使用的事物

Eg. User access interface (用户访问接口)

User is the subject and interface is the object

在不同的情况下，subject和object都不一样，

有些情况下的subject有可能是另一种情况下的object.

• Username, user ID, account number - 用户名、用户ID、账号

• Authentication - 验证

• Verifying the identification information - 验证身份信息

• Passphrase, PIN value, biometric, one-time password, password - 密码、PIN 值、生物识别、一次性密码、密码

• Authorization - 授权

• Using criteria to make a determination of operations that subjects can carry out on objects - 使用标准来确定主体可以对客体执行的操作

• Accountability - 问责制

• Audit logs and monitoring to track subject activities with objects - 审计日志和监控以跟踪主题与对象的活动

## Access Control Concepts (5个概念):

* Identity (身份)
* Identification and authentication (识别和认证)
* Authorization (授权)
* Accountability (问责制)
* Password management (密码管理)

### Identity (身份)

Creating or issuing secure identities should include three key aspects (制定或颁发安全身份的三个关键特征):

* Uniqueness (唯一性)
* Non-descriptive (非描述性的)
* Issuance (发行)

#### 

#### Uniqueness (唯一性)

##### Definition (定义）

* Uniqueness refers to the identifiers that are specific to an individual, meaning every user must have a unique ID for accountability.

唯一性是指特定于个人的标识符，这意味着每个用户都必须具有唯一的 ID 以进行问责。

##### Examples (例子)

* Retina scan - 视网膜扫描
* Fingerprints - 指纹
* Iris scan - 虹膜扫描

#### Non-descriptive (非描述性的)

##### Definition (定义）

* Non-descriptive means that neither piece of the credential set should indicate the purpose of that account.

非描述性意味着凭证集的任何部分都不应指示该帐户的用途

##### Examples (例子）

* For example, a user ID should not be “administrator,” “backup\_operator,” or “CEO.”

用户 ID 不应是”管理员”, “备份操作员”或“CEO”

#### Issuance (发行)

##### Definition (定义)

* These elements are the ones that have been provided by another authority as a means of proving identity.

这些元素是由另一个权威机构提供的，作为证明身份的手段

##### Examples (例子）

* ID cards are a kind of security element that would be considered an issuance form of identification.

身份证是一种安全元素，可被视为身份证明的发行形式

#### Identification Component Requirements (标识组件要求)

When issuing identification values to users, the following should be in place:

向用户发布标识值时，应具备以下条件:

* Each value should be unique, for user accountability

每个值都应该是独特的，以便用户负责

* A standard naming scheme should be followed.

应遵循标准命名方案

* The value should be non-descriptive of the user’s position or tasks.

该值不应描述用户的职位或任务

* The value should not be shared between users.

该值不应在用户之间共享

### **Identification and Authentication(**识别和认证)

#### Definition:

* **Identification** describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. Once a person has been identified through the user ID or a similar value, she must be **authenticated**, which means she must prove she is who she says she is.

标识描述了一种确保主体（用户、程序或进程）是它声称的实体的方法。可以使用用户名或帐号来提供标识。一旦通过用户 ID 或类似值识别了一个人，就必须对她进行身份验证，这意味着她必须证明她是她所说的那个人。

* Three general factors can be used for authentication:
* something a person knows/ authentication by knowledge (你知道的东西）eg. 妈妈，家乡
* something a person has/ authentication by ownership （拥有的东西）eg. Identification Card 身份证，Passport 护照
* something a person is/ authentication by characteristic (你是什么东西）eg. Uniqueness, Iris Scan虹膜，Fingerprint Scan指纹
* Strong authentication contains two out of these three methods: something a person knows, has, or is.
* Strong authentication is also sometimes referred to as **multi-authentication**, which just means that more than one authentication method is used. **Three-factor authentication** is possible, which includes all authentication approaches.

#### Example:

* User ID,
* MAC address,
* IP address,
* Personal Identification Number (PIN),
* Identification Badges,
* Email Address

### **Authorization** (授权)

* Once the subject provides its credentials and is properly identified, the system it is trying to access needs to determine if this subject has been given the necessary rights and privileges to carry out the requested actions.

一旦主体提供了其凭证并被正确识别，它试图访问的系统就需要确定该主体是否已被授予必要的权利和特权来执行所请求的操作。

Eg. Different positions will have different rights and privileges to carry out the requested actions

* For example, a teacher and a student in school will have different rights to access different platforms on a school system. A teacher will be able to carry out certain tasks that a student cannot.
* The system will look at some type of access control matrix or **compare security labels** to verify that this subject may indeed access the requested resource and perform the actions it is attempting. If the system determines that the subject may access the resource, it authorizes the subject.

系统将查看某种类型的访问控制矩阵或比较安全标签，以验证该主体是否确实可以访问所请求的资源并执行它正在尝试的操作。如果系统确定主体可以访问资源，则它授权主体。

#### Identity Management 身份管理

* Identity management is a broad and loaded term that encompasses the use of different products to identify, authenticate, and authorize users through automated means.

身份管理是一个广泛而丰富的术语，包括使用不同的产品通过自动化方式识别、验证和授权用户。

* The following are many of the common questions enterprises deal with today in controlling access to assets:
* What should each user have access to?
* Who approves and allows access?
* How do the access decisions map to policies?
* Do former employees still have access?
* How do we keep up with our dynamic and ever-changing environment?
* What is the process of revoking access?
* How is access controlled and monitored centrally?
* Why do employees have eight passwords to remember?

### Accountability (问责制)

* Auditing 审计 capabilities ensure users are accountable for their actions, verify that the security policies are enforced, and can be used as investigation tools.

审计功能确保用户对他们的行为负责，验证安全策略是否得到执行，并可作为调查工具使用。

* There are several reasons why network administrators and security professionals want to make sure accountability mechanisms are in place and configured properly: 网络管理员和安全专家要确保问责机制到位并配置得当，有几个原因。
* to be able to track bad deeds back to individuals 能够追溯到个人的不良行为
* detect intrusions 检测入侵行为
* reconstruct events and system conditions 重构事件和系统条件
* provide legal recourse material 提供法律追索材料
* produce problem reports 制作问题报告
* Audit documentation and log files hold a mountain of information—the trick is usually deciphering it and presenting it in a useful and understandable format.

以一种有用和可理解的形式呈现

* Accountability is tracked by recording user, system, and application activities. This recording is done through auditing functions and mechanisms 机制 within an operating system or application.

通过记录用户、系统和应用程序的活动来跟踪责任制。

* Audit trails contain information about operating system activities, application events, and user actions. 操作系统活动、应用程序事件和用户行动。
* Audit trails can be used to verify the health of a system by checking performance information or certain types of errors and conditions. 审计跟踪可以通过检查性能信息或某些类型的错误和状况来验证系统的健康状况
* After a system crashes, a network administrator often will review audit logs to try and piece together the status of the system and attempt to understand what events could be attributed to the disruption. 在系统崩溃后，网络管理员通常会审查审计日志，试图拼凑出系统的状态，并试图了解哪些事件可以归因于系统的中断

#### What to keep in mind when dealing with auditing

1. Store the audits securely. 安全地储存审计结果。
2. The right audit tools will keep the size of the logs under control. 正确的审计工具会使日志的大小得到控制。
3. The logs must be protected from any unauthorized changes in order to safeguard data. 日志必须受到保护，防止任何未经授权的更改，以保护数据
4. Train the right people to review the data in the right manner. 培训正确的人以正确的方式审查数据。
5. Make sure the ability to delete logs is only available to administrators. 确保删除日志的能力只对管理员有效。
6. Logs should contain activities of all high-privileged accounts (root, administrator). 日志应包含所有高权限账户（root、管理员）的活动。

### Password Management

* Different types of password management technologies have been developed to get these pesky users off the backs of IT and the help desk by providing a more secure and automated password management system. The most common password management approaches are listed next:

不同类型的密码管理技术已经被开发出来，通过提供一个更安全和自动化的密码管理系统，让这些讨厌的用户从IT部门和服务台的背上消失。接下来列出了最常见的密码管理方法。

* **Password Synchronization -** Reduces the complexity of keeping up with different passwords for different systems. 密码同步 - 减少了为不同系统保持不同密码的复杂性。eg. The password of our Axis, Moodle and Computer system accounts are the same.
* **Self-Service Password Reset** - Reduces help-desk call volumes by allowing users to reset their own passwords. 自助式密码重设 - 通过允许用户重设自己的密码来减少服务台的呼叫量。
* **Assisted Password Reset** - Reduces the resolution process for password issues for the help desk. This may include authentication with other types of authentication mechanisms (biometrics, tokens). 辅助密码重置 - 减少服务台解决密码问题的过程。这可能包括用其他类型的认证机制（生物识别技术、令牌）进行认证。

#### Password security

* Password generation: system vs user 密码生成：系统与用户
* Password strength: length, complexity, dynamic… 密码强度：长度、复杂性、动态...
* Password ageing & rotation 密码的老化和轮换
* Limit login attempts 限制登录尝试

## Tutorial Week 5

### Question 1

What are the three (3) different factors that are used for authentication?

For each factor, give an example.

Finally, describe a situation where a combination of at least two factors is necessary and briefly explain why

#### Three diff factors

1. Sth a person knows (Pwd Pin)
2. Sth a person has (Token)
3. Sth a person is (Biometrics Thumbprint, Thumb, Iris)

#### Two Factors Necessary (Choose 2 from above)

* Companies Card access and Biometrics to verify identity
* Companies Pin and Thumbprint
* Internet Banking Pin and Message sent to phone

### Question 2

One important requirement when assigning value to an identity is that the value must be non-descriptive.

Explain (Provide Definition) what it means by ‘‘non-descriptive” and why (Give Example) it is required so.

Neither piece of the cred set shld indicate the purpose of the acct

Eg. user id not (backup op, ceo, administrator) - does not show who it belongs to

### Question 3

Describe 描述 two types of technical controls that can be used for building access and specify which one you would use for low-security set-up required to protect a generic PC lab against unauthorised entry 普通的电脑室免遭未经授权的进入.

(Find Two out of Five Types of Technical controls from the chart. Examples listed have to be relevant to the question. (In this case: Physical Building access))

Preventive Technical controls include Access cards, biometrics, Pin (personal id number)

Detective Technical controls include CCTV.

Low security - Biometrics, Pin, Access Card,

\* Need to write what type of biometrics

### Question 4

Auditing is used for multiple purposes in a security system. Describe three major security issues addressed by the use of auditing. (Describe : Definition, Describe three issues addressed: Give the reasons why auditing is important WHY)

审计在安全系统中被用于多种目的。描述通过使用审计解决的三个主要安全问题。

To be able to:

Detect intrusion

reconstruct events and system conditions

provide legal recourse material

### Question 5

Physical controls are often neglected when security systems are developed but nonetheless they are a critical component of an effective security solution. (Statement)

Describe two physical preventive types of controls as well as two physical detective types of controls and specify a scenario in which a combination of the two is necessary.

在开发安全系统时，物理控制往往被忽视，但它们是有效的安全解决方案的重要组成部分。描述两种物理预防类型的控制和两种物理检测类型的控制，并说明在什么情况下需要结合这两种控制。

#### Physical Preventives

* Turnstiles
* Automated barriers
* Bollards

Physical Preventive controls include turnstiles, automated barriers and bollards.

#### Physical Detectives

* Cctv
* smoke detector

Scenario (Physical)

CCTV and Biometrics (Data Centre)

A data centre will have to have CCTV and Biometrics in place.

Hospital

School

Research Lab

#### Technical Real Life examples:

##### Online banking includes the:

* technical preventive controls such as (Passwords)

密码

* Technical deterrent (Message on website to prevent people from hacking)

网站上的信息，以防止人们的黑客行为

* Technical detective (Audit)

审计

##### School security system

* Technical preventive (Passwords)

密码

* Technical deterrent (Message on website to prevent people from hacking)

网站上的信息，以防止人们的黑客行为

* Technical detective (Antivirus software)

杀毒软件

* Technical Corrective (Recycle bin)

回收站

* Technical Recovery (Recovery technologies)

恢复技术

#### Administrative Real life examples:

* Big organisations:
* Administrative deterrent (Penalty and termination policy)

处罚和解雇政策

* Administrative preventive (Security awareness and training)

安全意识和培训

* Administrative detective (Security reviews, performance evaluations)

安全审查、绩效评估

* Administrative Corrective (Incident handling procedures)

事故处理程序

* Administrative recovery (Contingency plans and Disaster recovery plans)

应急计划和灾难恢复计划

### **Question 6**

When developing a security system, it is important to plan for cases which the preventive measures in place fail and, consequently, the system integrity is compromised. From a security perspective what are the two main avenues that are generally considered for continuity/restoration of services? (Recovery)

在开发一个安全系统时，重要的是要对预防措施失败的情况进行规划，从而使系统的完整性受到损害。从安全的角度来看，通常考虑的两个主要途径是什么，用于服务的连续性/恢复？

Access controls fail

If fail and integrity is compromised:

(Backup - offsite storage backups(Offline)

Ensure restoration of services, test the backup so that the backup will not fail (once in 6 months or once a year)

(Under the 5th stage of Security Controls: Recovery, list out 2 examples)

### Question 7

The integrity principle in the context of data security deals with the correctness of the data and the aim is to prevent damage from personnel inside or outside the organization. What is the first measure that needs to be put in place to help with the data integrity protection?

数据安全方面的完整性原则涉及到数据的正确性，其目的是防止组织内部或外部人员的破坏。为帮助保护数据的完整性，首先需要采取的措施是什么？

Implement access controls. Users will only have limited access, this reduces the chance that a basic mist can result in a major damage to the data that is being protected.

### Question 8

Explain the difference between corrective and recovery controls.

Compare

Explain the similarities (Definition of both, both is \_\_\_\_)

(Definition of both, description, Advantage and Disadvantage, Examples)

解释纠正性控制和恢复性控制之间的区别。

Definition: Recovery controls are for recovering more serious situations from damage.

#### Corrective control

Example:

Recycle bin in Windows helps to correct accidental deletion. When an item is accidentally deleted, it goes into the recycle bin and users are still able to retrieve the files within a specific amount of time.

#### Recovery control

Example:

Chkdsk which helps to recover files that have been erased.

### Question 9

Many organizations develop security systems which are focused entirely on physical and technological security controls. Explain why this is insufficient and provide examples how the security could be compromised. (Explain why it is insufficient: Find what is missing and list why it is important to have the missing item)

许多组织开发的安全系统完全集中在物理和技术安全控制上。解释为什么这是不充分的，并举例说明安全可能受到损害。

Cyber security has 3 main aspects: People, Process, Systems

We need **Administrative Controls** as well.

If overlooked, an experienced attacker will be able to breach the security set up because the issue of information ownership is properly handled.

Thus an attacker may not need to break into the better protector systems as the access to confidential information is unlikely to be thoroughly control.

#### Example of lack of Administrative Control

Email to all users instead of only those that should have access to it.

Disposal of older hardware is not done in a secure manner and harddrives are simply thrown into a bin in from which an attacker can extract critical information such as passwords or confidential records.

### Question 10

What is CERT-Australia? What is AusCERT? What is ASD? Why is it important from a data security point of view to know about each of them?

#### C.E.R.T

**-** Computer Emergency Response Team

#### CERT Australia

The national computer emergency response team. CERT Australia provides advice and support on cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest.

#### AusCERT

A non-profit organisation that provides advice and solutions to cybersecurity threats and vulnerabilities. The organisation covers their costs through member subscriptions, attendees to the annual AusCERT conference and service contracts.

CERT educates people about disaster preparedness for hazards that may impact their area and trains them in basic disaster response skills, such as fire safety, light search and rescue, team organization, and disaster medical operations. Knowing about each of them allows us to be better prepared in tackling cyber-security threats.

### Question 11

What is sender policy framework (SPF)? Explain the type of attacks that SPF addresses.

The Sender Policy Framework (SPF) is an email authentication protocol and part of email cybersecurity used to stop phishing attacks. It allows your company to specify who is allowed to send email on behalf of your domain.

This is useful because in a typical phishing attack, the threat actor spoofs the sender address to look like an official business account or someone the victim may know.

#### Targets

* Email spoofing
* Phishing attacks

#### How

The protection of your outbound email is implemented by configuring a TXT record in your public DNS which lists the servers that are allowed to send email from your mail domain. Nothing is configured on the mail server itself.

The Sender Policy Framework (SPF) email authentication method aims to reduce spam and fraud by making it harder for email senders to hide their identity. SPF detects email spoofing by providing a process to verify who is permitted to send emails on your behalf.

## Week 6: Access Control Practices

### Access Control Practices

* Deny access to systems to undefined users or anonymous accounts.

拒绝未定义的用户或匿名账户对系统的访问。

* Limit and monitor the usage of administrator and other powerful accounts.

限制和监控管理员和其他强大账户的使用。

* Suspend or delay access capability after a specific number of unsuccessful logon attempts

在特定数量的不成功的登录尝试后，暂停或延迟访问能力

* Remove obsolete user accounts as soon as the user leaves the company

一旦用户离开公司，立即删除过时的用户账户

* Suspend inactive accounts after 30 to 60 days.

在30至60天后暂停不活跃账户。

* Enforce strict access criteria.

执行严格的访问标准。

* Enforce the need-to-know and least-privilege practices. (need to know: 只让我们知道应该知道的东西 例如：老师的内容和学生的内容不一样) （least privilege : giving an employee the only enough rights and privilege to carry out what they are supposed to do and nothing more)
* Disable unneeded system features, services and ports.

禁用不需要的系统功能、服务和端口。

* Replace default password settings on accounts.

替换账户上的默认密码设置。

* Limit and monitor global access rules.

限制和监控全局访问规则

* Remove redundant resource rules from accounts and group memberships.

从账户和组成员资格中删除多余的资源规则。

* Remove redundant user IDs, accounts, and role-based accounts from resource access lists.

从资源访问列表中删除多余的用户ID、账户和基于角色的账户。

* Enforce password rotation.

强制执行密码轮换。

* Enforce password requirements (length, contents, lifetime, distribution, storage, and transmission).

执行密码要求（长度、内容、寿命、分发、存储和传输）。

* Audit system and user events and actions, and review reports periodically.

审计系统和用户的事件和行动，并定期审查报告。

* Protect audit logs.

保护审计日志。

### **Security controls** 安全控制

* Safeguards to prevent, detect, correct or minimise security risks.

预防、检测、纠正或尽量减少安全风险的保障措施。

* Set of actions for data security

促进数据安全的一套行动

#### Definition

Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks.

安全控制是一套建议的网络防御行动，提供了具体和可操作的方法来阻止当今最普遍和最危险的攻击。

#### Advantages

* A principle benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results.

控制措施的一个原则性好处是，它们优先考虑并集中于数量较少的具有高回报结果的行动。

* The Controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners.

这些控制措施是有效的，因为它们来自于领先的威胁报告中强调的最常见的攻击模式，并在非常广泛的政府和行业从业者社区中得到了审查。

#### What is it for?

* They were created to answer the question, "what do we need to do to stop known attacks."

它们的创建是为了回答 "我们需要做什么来阻止已知的攻击 "这一问题。

* The key to the continued value is that the Controls are updated based on new attacks that are identified and analysed by groups from Verizon to Symantec so the Controls can stop or mitigate those attacks.

持续价值的关键是，控制措施会根据从Verizon到赛门铁克的团体所识别和分析的新攻击进行更新，以便控制措施能够阻止或减轻这些攻击。

### There are Two ways of categorising Security Controls: 有两种方法可以对安全控制进行分类。

1. Categorising according to nature of the control 根据控制的性质进行分类

* Administrative Controls 行政控制
* Technical Controls/ Logical Controls 技术控制/逻辑控制
* Physical Controls 物理控制

2. Categorising according to the different phases 阶段 of the control process

* Deterrent 威慑力
* Preventative 预防性的
* Detective 探测
* Corrective 纠正
* Recovery/ Compensatory 恢复性/补偿性

Categorising according to nature of the control

#### Administrative Controls

These include the developing and publishing of policies, standards, procedures, and guidelines; risk management; the screening of personnel; conducting security-awareness training; and implementing change control procedures.

这包括制定和发布政策、标准、程序和准则；风险管理；人员筛选；进行安全意识培训；以及实施变更控制程序。

##### Definition

* Administrative controls refer to policies, procedures, or guidelines that define personnel or business practices in accordance with the organisation's security goals.

行政控制是指根据组织的安全目标确定人员或业务实践的政策、程序或准则。

* Administrative controls are the process of developing and ensuring compliance with policy and procedures.

行政控制是制定和确保遵守政策和程序的过程

* They tend to be things that employees may do, or must always do, or cannot do. 它们往往是员工可能做的事情，或必须一直做的事情，或不能做的事情

##### Categories of Administrative Controls:

* Policies 政策
* Standards 标准
* Procedures 程序
* Guidelines 准则

##### Importance of Administrative Controls:

行政控制的重要性：

If overlooked, an experienced attacker will be able to breach the security set up because the issue of information ownership is properly handled.

如果被忽视，一个有经验的攻击者将能够突破安全设置，因为信息所有权问题得到了适当的处理。

##### 

##### Examples:

* Policies (Eg. Business Continuity Plan, Access Control Policy, Disaster Recovery Plan）
* Procedures
* Personnel Controls ( Def: Personnel controlling indicates strengths and weaknesses of the company. Its purpose is to effectively exploit the potential of all employees to achieve the maximum benefit within the organisation. 人事控制表明公司的优势和劣势。其目的是有效地挖掘所有员工的潜力，以实现组织内的最大利益。）
* Supervisory structure 监管结构 (Def: a board of management of which nonmanagerial workers are members, having supervisory powers over some aspects of management decision-making. 由非管理人员担任成员的管理委员会，对管理决策的某些方面拥有监督权。)
* Testing ( Eg. Vulnerability Scanning, Penetration Testing 渗透测试, Security Audit/Review, Risk Assessment , Security Scanning)

#### Technical Controls (aka Logical Controls)

These consist of implementing and maintaining access control mechanisms, password and resource management, identification and authentication methods, security devices, and the configuration of the infrastructure. 这些包括实施和维护访问控制机制，密码和资源管理，识别和认证方法，安全设备，以及基础设施的配置。

##### Definition:

Technical controls are the **hardware** and **software components** that protect a system against cyberattacks.

技术控制是保护系统免受网络攻击的硬件和软件组件。

Firewalls, intrusion detection systems (IDS), encryption, and identification and authentication mechanisms are examples of technical controls.

防火墙、入侵检测系统（IDS）、加密以及识别和认证机制是技术控制的例子。

May refer to：

* identification and authentication methods
* security devices
* configuration of the infrastructure

##### Importance of Technical controls:

Technical controls perform many critical functions, such as keeping unauthorized individuals from gaining access to a system and detecting when a security violation has occurred.

技术控制发挥了许多关键功能，如防止未经授权的个人进入系统，并在发生安全违规时进行检测。

##### Examples：

###### Preventative

* Encryption 加密
* Smart cards 智能卡
* Network authentication 网络认证
* Access control lists (ACLs) 访问控制列表（ACL）。
* File integrity auditing software 文件完整性审计软件
* Patching 打补丁
* IPS (Intrusion Prevention System) 入侵预防系统

###### Detective

* Security logs
* NIDS (Network Based Intrusion Detection System) 基于网络的入侵检测系统
* HIDS ( Host Based Intrusion Detection System) 基于主机的入侵检测系统

###### Corrective/Recovery

* IPS (Intrusion Prevention System） 入侵预防系统
* Restore from backups 从备份中恢复
* Patching 修补

#### Physical Controls 物理控制

Depending on the organization physical security countermeasures will vary. A government agency such as the Department of Defense may have armed guards at the door of the building. Many organizations are not in the position of breaching national security so armed guards are not a necessity. In many cases a receptionist greets any new visitors and makes the appropriate arrangements for an on-site visit.

根据组织的不同，物理安全对策也会有所不同。像国防部这样的政府机构可能会在大楼的门口配备武装警卫。许多组织并不处于破坏国家安全的地位，因此武装警卫并不是必要的。在许多情况下，接待人员会迎接任何新的来访者，并为现场访问做出适当的安排。

##### Definition:

These entail controlling individual access into the facility and different departments, locking systems and removing unnecessary floppy or CD-ROM drives, protecting the perimeter of the facility, monitoring for intrusion, and environmental controls.

##### Importance of Physical controls:

Physical security keeps your employees, facilities, and assets safe from real-world threats. These threats can arise from internal or external intruders that question data security. Physical attacks can cause a safe area to break into or the invasion of a restricted area part.

##### Examples:

* Automated barriers & bollards 自动屏障和护柱
* Building management systems like Heating, HVAC, lifts/elevators control, etc. 楼宇管理系统，如供暖、HVAC、升降机/电梯控制等
* CCTV- Closed Circuit TV
* Electronic article surveillance - EAS 电子设备监控 - EAS
* Fire detection 火灾探测
* GIS mapping systems GIS制图系统
* Intercom & IP phone 对讲机和IP电话
* Lighting control system 照明控制系统
* Perimeter intrusion detection system 周边入侵检测系统
* Radar based detection & Perimeter surveillance radar 基于雷达的检测& 周边监控雷达
* Security alarm 安全警报
* Video wall
* Power monitoring system 电力监控系统
* Laptop Locks 笔记本电脑锁

### Categorising according to the different phases of the control process

* Deterrent: controls to discourage attacks at the first place, deter people from breaching security, e.g warning, banner, logon message, fake CCTV cameras to warn people, security measures on websites to tell people that they are protected

威慑：控制首先阻止攻击，阻止人们破坏安全，例如警告、横幅、登录消息、假闭路电视摄像头警告人们，网站上的安全措施告诉人们他们受到保护

* Preventive: controls that make it hard for attacks to succeed, e.g. firewall (stops unwelcomed traffic), encryption, locked doors

预防性：使攻击难以成功的控制，例如防火墙（阻止不受欢迎的流量）、加密、锁门

* Detective: controls that detect if an attack has occurred, e.g. checksum, intrusion detection system, rotation of duties, security audits, monitors and sensors, motion sensors installed in the buildings to detect intruders, CCTV cameras, sometimes firewall that tells when an attack has been made on the system, intrusion detection systems that monitor the activity on the hosts and computers over the network

侦探性：检测是否发生攻击的控制，例如校验和、入侵检测系统、职责轮换、安全审计、监视器和 sensors，安装在建筑物中以检测入侵者的运动传感器，闭路电视摄像机，有时会告知系统何时受到攻击的防火墙，通过网络监视主机和计算机上的活动的入侵检测系统

* Corrective: corrective aspects of security, controls that reverse the damage, e.g. version control, incident handling procedures, fire extinguishers, undo, recycle bin, DOS attack (ban the IP addresses to stop from jamming the servers), Fire extinguishers (putting out fires when it has happened), Incident handling procedures (tells employees what to do when an incident happens)

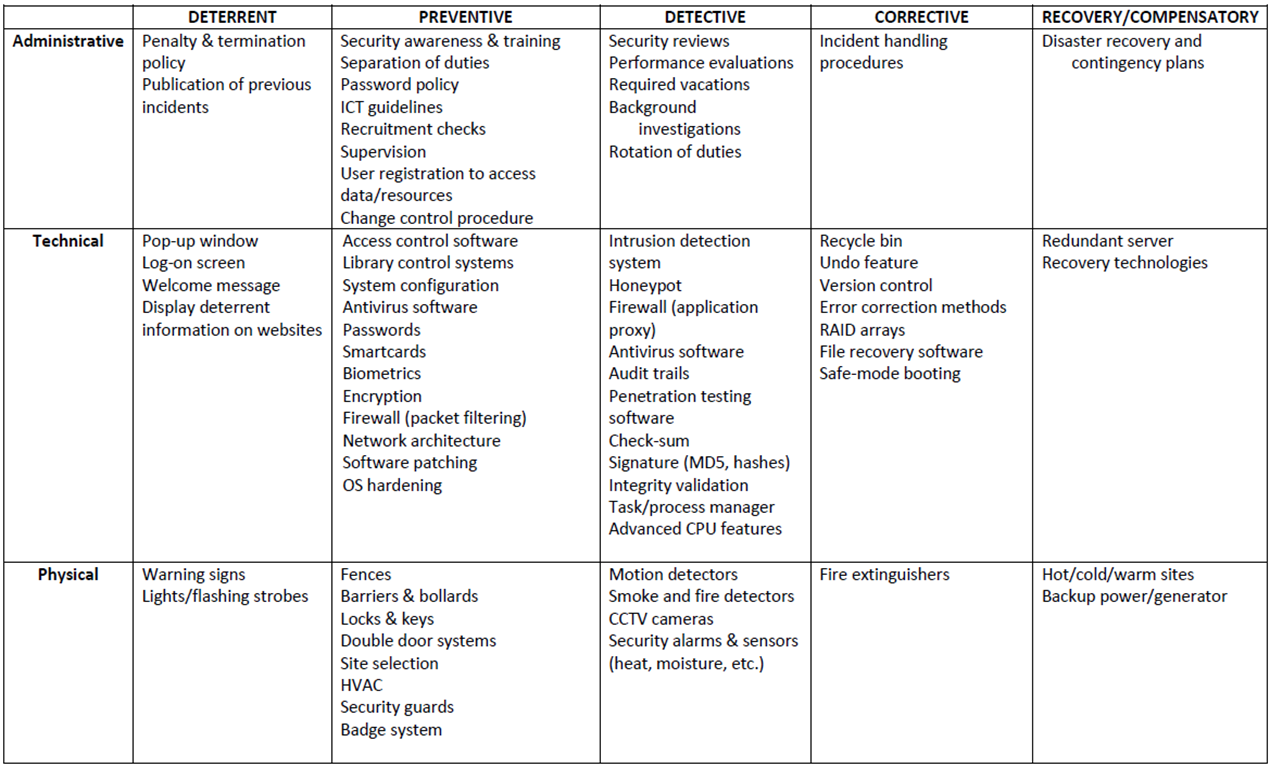
纠正：安全的纠正方面，扭转损害的控制，例如版本控制、事件处理程序、灭火器、撤销、回收站、DOS攻击（禁止IP地址以阻止干扰服务器）、灭火器（发生火灾时灭火）、事件处理程序（告诉员工发生事件时该怎么做）

* Recovery: controls that bring the system back after a major disaster like earthquakes or tsunamis , e.g. disaster recovery plan, hot/cold/warm sites, backup power,

恢复：在地震或海啸等重大灾难发生后使系统恢复的控制措施，例如，灾难恢复计划、热/冷/热站点、备用电源。

#### A general example:

Speeding (have fines and punishment, and preventive controls like speed bumps, detection – security cameras)



#### Real-life Example

**Speeding:** deterrent - having fines and punishment 罚款，惩罚, preventive controls like speed bumps减速带, detection security cameras 超速监控, corrective - enforcement of fines and punishments 执法, recovery - none

**Fire Hazards:** *deterrent* - flyers or advertisements how to prevent fire hazards from happening, *preventive* - making sure no open stoves are left unattended, power sockets are turned off when not in use 确保没有开放的炉子无人看管，不使用时关闭电源插座, *detective* - smoke detectors 烟雾探测器, cctv at home 家用监控 *corrective -* fire extinguishers 灭火器 , *recovery -* insurance and funds kept for a rainy day 保险和存款

### Commonly Used Security Methods 常用的安全方法

To address the key requirements of the AIC triad, one can employ a number of commonly used security methods:

* Least privilege
* Defense-in-depth
* Minimization
* Keep things simple
* Compartmentalization
* Use choke points
* Fail securely/safely
* Leverage unpredictability
* Separation of duties

#### Least Privilege

**States that:** do not provide more privileges than are required. This applies to both users and applications. 不要提供超过所需的权限。这同时适用于用户和应用程序。

* Example: No administrative rights to guests accounts, unidentified applications should not be able to have the power to change the system file etc.) 例如。对客人的账户没有管理权限，不明身份的应用程序不应该有改变系统文件的权力等)
* This principle applies not only to privileges of users and applications on a computer system, but also to other noninformation systems privileges of an organization’s staff.

这一原则不仅适用于计算机系统上的用户和应用程序的特权，而且也适用于一个组织的工作人员的其他非信息系统的特权

* The principle of least privilege is a preventive control, because it reduces the number of privileges that may be potentially abused and therefore limits the potential damage.

最小特权原则是一种预防性控制，因为它减少了可能被潜在滥用的特权的数量，因此限制了潜在的损害

* Some examples of application of this principle include the following:
* Giving users only read access to shared files if that’s what they need, and making sure write access is disabled

如果用户需要的话，只给他们阅读共享文件的权限，并确保禁止写入权限

* Not allowing help desk staff to create or delete user accounts if all that they may have to do is to reset a password

如果服务台工作人员只需要重设密码，就不允许他们创建或删除用户账户

* Not allowing software developers to move software from development servers to production servers

不允许软件开发人员将软件从开发服务器转移到生产服务器上

* Privilege : The ability to access data to run processes and applications

特权：访问数据以运行进程和应用程序的能力

* Product: keep system more stable by giving less privilege to untrustworthy users

产品：通过给予不值得信任的用户较少的特权，使系统更加稳定。

##### Advantages:

* Minimizes the attack surface, diminishing avenues a malicious actor can use to access sensitive data or carry out an attack by protecting superuser and administrator privileges.
* Reduces malware propagation by not allowing users to install unauthorized applications. The principle of least privilege also stops lateral network movement that can launch an attack against other connected devices by limiting malware to the entry point.
* Improves operational performance with reductions in system downtime that might otherwise occur as a result of a breach, malware spread or incompatibility issues between applications.
* Safeguards against human error that can happen through mistake, malice or negligence.

##### Disadvantages:

The two big problems with least privilege are minimal access and expiration of access.

* Minimal access

When assigning or providing access, in many cases an admin is not sure whether or not someone needs access. In the past, if an admin was not sure if a user needed access, the default rule was to go ahead and provide the user with access. While this potentially minimized support desk calls and user frustration, it introduced considerable risk.

If you provide additional access and it is not needed, no one ever notifies the help desk. Ultimately, providing access to a user beyond what he or she needs to perform his/her role leads to a massively increased attack surface that leaves organizations wide open to damage from hackers and insiders.

* Expiration of access

The second big problem with data access is expiration. In most organizations, once access is provided to a piece of information, it is never removed.Over the course of employment at an organization, as a user’s role and responsibilities change (or the technologies they need to access grow), more access is granted to the user. However, rarely is the previous access, when no longer relevant to a user’s role, removed.

##### Importance:

* The principle of least privilege is an important information security construct for organizations operating in today’s hybrid workplace to help protect them from cyberattacks and the financial, data and reputational losses that follow when ransomware, malware and other malicious threats impact their operations.
* The principle of least privilege strikes a balance between usability and security to safeguard critical data and systems by minimizing the attack surface, limiting cyberattacks, enhancing operational performance and reducing the impact of human error.

#### **Defense in Depth** (multiple types of security controls in different layers)

深度防御（不同层次的多种类型的安全控制）

* The principle of defense in depth is about having more than one layer or type of defense.

深度防御的原则是指拥有一个以上的防御层或类型。

##### **Advantage**

The reasoning behind this principle is that any one layer or type of defense may be breached, no matter how strong and reliable you think it is, but two or more layers are much more difficult to breach.

这一原则背后的理由是，任何一层或一种类型的防御都可能被攻破，无论你认为它多么强大和可靠，但两层或更多的防御则更难攻破。

* Defense in depth works best when you combine two or more different types of defense mechanisms—
* such as using a firewall between the Internet and your LAN, plus the IP Security Architecture (IPSEC) to encrypt all sensitive traffic on the LAN. In this scenario, even if your firewall is compromised, the attackers still have to break IP Security to get to your data flowing across the LAN.

例如，在互联网和你的局域网之间使用防火墙，加上IP安全架构（IPSEC）来加密局域网上的所有敏感流量。在这种情况下，即使你的防火墙被破坏，攻击者仍然必须打破IP安全架构，以获得你在局域网上流动的数据。

Eg.

1st layer – Deterrent control (easy to implement, use it to warn hackers to not attack, breaching policies may not be legal)

2nd layer – Preventive control (Firewall installed on server that monitors all the traffic gg btw the internet and internal network and intercept any suspicious activities)

3rd layer – Detective layer (Network monitoring tools like intrusion detection systems that will alert ppl on any attacks being made on the system)

4th layer – Corrective layer (software installed like antivirus that could get rid of virus that the computer has been infected)

5th layer – Recovery layer (Data backup, another image of the system software for recovery in the event that the system breaks)

Generally, different types of controls should be used together:

* first, preventive controls should be in place to try and prevent security incidents from happening at all;
* second, detective controls are necessary so that you can know whether preventive controls are working or have failed;
* and third, corrective controls are needed to help you respond effectively to security incidents and contain damage.
* However, the defense in depth principle does not mean that you should indiscriminately apply all the controls and security measures you can get your hands on: balance has to be found between security provided by the defense in depth approach and the financial, human, and organizational resources you are willing to expend following it. This balance is addressed by the cost-benefit analysis.

#### Minimisation

*States that:*  the system should not run any applications that are not strictly required to complete its assigned task

规定：系统不应运行任何非严格要求的应用程序，以完成其指定的任务

* The minimization principle is the cousin of the least privilege principle and mostly applies to system configuration.

最小化原则是最小特权原则的表哥，主要适用于系统配置

* For example, a computer whose only function is to serve as an e-mail server should have only e-mail server software installed and enabled. All other services and protocols should either be disabled or not installed at all to eliminate any possibility of compromise or misuse.

例如，一台唯一功能是作为电子邮件服务器的计算机应该只安装和启用电子邮件服务器软件。所有其他服务和协议应被禁用或根本不安装，以消除任何妥协或误用的可能性。

* Advantages: Adherence to the minimization principle not only increases security but usually also improves performance, saves storage space, and is a good system administration practice in general.

优点。坚持最小化原则不仅可以提高安全性，而且通常还可以提高性能，节省存储空间，一般来说是一种良好的系统管理实践

#### Keep Things Simple

Definition/ Principle： a security system should be kept simple as any complexity introduced leads to insecurity in the overall system

安全系统应保持简单，因为引入的任何复杂性都会导致整个系统的不安全。

* Complexity is the worst enemy of security. Complex systems are inherently more insecure because they are difficult to design, implement, test, and secure.
* The more complex a system, the less assurance we may have that it will function as expected.

一个系统越复杂，我们就越不能保证它能按预期运行

* Although complexity of information systems and processes is bound to increase with our increasing expectations of functionality, we should be very careful to draw a line between avoidable and unavoidable complexity and not sacrifice security for bells and whistles, only to regret it later.

尽管随着我们对功能的期望值越来越高，信息系统和流程的复杂性必然会增加，但我们应该非常小心地在可避免的和不可避免的复杂性之间划出一条界限，不要为了铃声和口哨而牺牲了安全，事后才后悔

* When you have to choose between a complex system that does much and a simple system that does a bit less but enough, choose the simple one.

#### Compartmentalisation

to prevent the compromise of the entire system, use a compartment approach to the system design and implementation

* Compartmentalization, or the use of compartments (also known as zones, jails, sandboxes, and virtual areas), is a principle that limits the damage and protects other compartments when software in one compartment is malfunctioning or compromised.
* Real life example: It can be best compared to compartments on ships and submarines, where a disaster in one compartment does not necessarily mean that the entire ship or submarine is lost.
* **Definition**: Compartmentalization in the information security context means that applications run in different compartments are isolated from each other. In such a setup, the compromise of web server software, for example, does not take down or affect e-mail server software running on the same system but in a separate compartment. Zones in Solaris 10 implement the compartmentalization principle and are powerful security mechanisms.

## Tutorial Week 6

### Question 1

* Give an example of administrative preventive controls that addresses Confidentiality and briefly explain how.
* Give an example of technical corrective controls that addresses Integrity and briefly explain how.

#### Confidentiality

- No leak (the secrecy of the data is maintained at all times)

#### Availability

- Users must be able to use the system when they need to (The systems and networks should provide adequate capacity to perform in a predictable manner with an acceptable level of performance.)

#### Integrity

- No modifications and Accuracy( Accuracy and reliability of information

Prevent unauthorised and improper modifications)

#### Three types of control

* Administrative controls
* Technical (Software part eg. penetration testing) controls
* Physical controls

##### **Preventive controls**:

Training of employees about security awareness. Eg. enhances security awareness of phishing attacks.

How: With security awareness training, users will be able to identify and spot phishing emails that attempt to steal account information

##### **Technical Controls**:

Recycle bin in windows helps to recover files that are accidentally deleted by authorised users.

### Question 2

Describe one (1) example of administrative preventive controls and one (1) example of physical recovery controls, both of which must address Availability. For each example, briefly explain how it helps address availability.

#### Availability

Definition: The systems and networks should provide adequate capacity to perform in a predictable manner with an acceptable level of performance.

##### Administrative

(The soft part of things: Policy, trainings, procedures, software based)

* Policy that prevent unauthorised people from entering
* Change control procedure, change management ensure that new software development will not crash existing appication due to thorough testing.
* Penetration testing

##### Physical

(Physical part of things, Physical infrastructure)

Backup sites, Backup systems, Warm site, cold site, UPS (Uninterruptible Power Supply), Hot sites, Backup power so that when a system is down, data can be retrieved from the backup sites and will thus will make the data available as quickly as possible. (Example + how it addresses availability)

### Question 3

A small health organization has asked for advice in regards to improving its security system. The organization is already implementing a defense-in-depth mechanism which combines a firewall with the encryption of traffic to prevent confidential information being accessed by unauthorised personnel. The company has very limited funding and you can only suggest two additional security mechanisms (security methods) to be considered. Describe the mechanism you have selected and justify your selection.

\* Defence in depth - Different layers of controls

Small organisation and limited funding (sugg solutions must address these constraints)

Touches on commonly used security methods

#### Minimisation (similar to least privilege)

* applies to system configuration
* States that one should not run any software, applications or services that are not strictly required to the entrusted job
* Eg. computer which only function is to serve as an email server, should only have the email server and software installed on the computer, all other services as per protocols should either be disabled or not installed at all to eliminate any possibility of the compromise or misuse
* Advantages: Increases security and improve performance, save storage space and is also a good system administration in practice.
* Principle: hardening the organisation server by disabling the services that are redundant or removing programs that are not necessary in order to reduce the attacks on the server
* Summary: able to harden org server, disable unnecessary services, restrict accesses, perform on a need to basis, use the least privilege principal
* Does not need require company to buy solutions, only need to use the current system that the organization has and enforce such principals

#### Leverage unpredictability

* Eg. announce on the organisation website web that using firewall that logs all traffic to and from the network and the logs are reviewed by the organisation
* No need to disclose the type and vendor of the firewall, where it is located, the frequency of use and any backup firewalls or network disruption detections are put in place
* Principle in this case: telling the public about the existence of such security controls, public able to get the gist of what is happening in the organisation and warn them about the effects of trying to compromise the security of the organisation

### Question 4

A retailer is selling goods via both physical and online stores. The online store allows customers to create their own accounts, update personal and financial information, order goods, and track order status. It also links to the inventory management back-end. It has been suggested that three universal security methods; Least privileges, Compartmentalisation, and Defense-in-depth need to be used to enhance the security of the system. Describe your interpretation of these three (3) security methods in this particular scenario. (Definition, Example, Principle, Advantage and Disadvantages)

\*Physical and online store

#### Least privileges

Do not grant users or the staff more privilege than they should have. Only give them the privileges they need for their duties.

#### Compartmentalisation

Definition: Putting things into different categories

Parts

Web server ( in demilitarised zone DMZ)

Front end systems and Backend systems

#### Compartmentalise :

* segregation of front end systems from the back end systems
* If they are not in physical servers, they can be on virtual machines
* Users able to retrieve webpage from web servers without accessing any materials on the backend
* Pulling happens when information is transferred from one system to another (eg. info keyed in -> inventory -> management -> system -> person reads and sends order to warehouse -> ship)

#### Defence in depth

Multiple layers to the defence: Online stall has personal and financial information. In order to protect the info, multiple layers need to be used.

Layers : (Outer to inner layer) Firewall. Intrusion detection system (IDS). Secure data with encryption. Search for more information and examples on these layers

(two layer firewall: internet facing and internal facing firewall)

### Question 5

With the help of an example, explain the principle Fail securely.

* Definition : If a security measure or control has failed, the system is not rendered to an insecure state.
* Eg. firewall fails, shld fall towards a deny all rule instead of permit all ( Firewall: There are many firewall rules. Person whos job is to key,delete, amend and add firewall rule. Eg. users cannot access the database servers and only the web servers. Because database server is in the internal network. Firewall rule states who can access what etc. on 80, there is http protocol bec access the webpage stored in web server. Firewall has a particular deny all rule : unless all rules are followed, deny all rule is activated)

\* Does not mean close everything in all cases

* Physical example: Building access control system: Doors should open when there is a fire should default to open doors when humans are trapped in the buildings instead of close as human lives takes priority over the risk of unauthorised access which may be dealt with using other forms of controls that does not endanger the lives of people during emergency situations.

### Question 6

With the help of an example, explain why the principle of minimization is important from the point of view of system security. (Definition, Example, Principle, Advantage, Importance)

Minimisation Principle: Only run applications that are strictly necessary to perform its tasks and nothing more because when there are more applications running, the higher the chance for something to go wrong and the security will be compromised

A common approach to breach security is to attack services which are running on a host machine, such as Telnet.

TELNET is commonly used by terminal emulation programs that allow you to log into a remote host. However, TELNET can also be used for terminal-to-terminal communication and interprocess communication. TELNET is also used by other protocols (for example, FTP) for establishing a protocol control channel.

To limit the number of options for hackers, it is imperative to shut down all services that are not essential to improve the running of the system.

An application may have weaknesses that can be exploited and thus, if they are not running, the system will be more secure.

Disabling redundant services is a major task to server hardening. With minimisation principle, the priority is to have the least privileges as possible

Example:

In the case of the Firewall Rule in minimisation principle, port 80, HTTP is the protocol. Inside the firewall, there are alot of protocols and ports. For example:

* FTP(File Transfer Protocol: works on a client-server model, it is a standard communication protocol used for the transfer of computer files from a server to a client on a computer. FTP is a network protocol for transmitting files between computers over Transmission Control Protocol/Internet Protocol (TCP/IP) connections.) protocol in port 21.
* TELNET is in port 23.
* SSH is another service is in port 22.
* SMTP (Simple Mail Transfer Protocol: for mail services) in port 25

Minimisation: disable services that you do not need, unnecessary services should be disabled eg. If an organisation does not need to use FTP, disable FTP bec FTP is not secure as FTP transfer files in clear files.

* Instead of having FTP, use SFTP (Secure File Transfer Protocol)
* Since TELNET is also not secure as TELNET also send files in clear text, disable TELNET and enable SSH (Secure Shell) instead.

#### Ports and Protocols

As per its word definition, a protocol is a set of rules. In computer networking, a protocol defines a standard way for computers to exchange information. Most common protocols used in computer networks and the internet are TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and IP (Internet Protocol).

A port in computer networking is a logical access channel for communication between two devices. Bi-directional communications and more complex connections may use multiple ports (channels) simultaneously.

Data on the Internet is organised into standard TCP or UDP packets. Network clients use different ports (or channels) to transfer this data. Generally one port is used to send data and another to receive it, so packets don't collide. The port number (and the destination IP address) is included as part of the header each packet is given. Ports range from 1 to 65535 for the TCP and UDP protocols.

### **Question 7**

You are asked to give an advice on the security set-up for a medical research laboratory which has computer terminals connected to a server that stores sensitive information. a) Suggest two physical preventive controls and two physical detective controls that can be used and explain your choice. b) The laboratory is going to provide an Internet presence to assist researchers in finding information online. However, this raises a serious concern that the sensitive information is accessed by intruders from the outside world. Under the defense-in-depth principle, suggest specific security solutions for at least two layers of defense that may be deployed to mitigate the risk.

#### Physical Preventive:

(Since it is in a medical research lab, assume that it is a physical site)

Security guards, Bollard, Biometrics Access Control

Backup Files (in case of an attack)

#### **Physical Detective** :

CCTV, Smoke Detectors, Fire alarm

#### Defense-in-depth:

**(**eg. having a preventive, detective and corrective control)

* Preventive - firewall (stops bad traffic before it enters the network)
* Detective - Intrusion detection system, Logging (helps to detect malicious activities)
* Corrective - Backups (helps to restore the data damaged or modified by intruders)

### **Question 8**

It is often suggested to suspend or delay access capability after a number of unsuccessful login attempts. Describe the reason behind this suggestion and clearly indicate what security threat this recommended practice addresses.

This helps prevent hackers from carrying out Brute force attack, Password guessing when it is done automatically.

### Question 9

With the help of examples explain the differences between three universal security principles/methods:

Least privilege, Minimization, and Keep things simple. (Definition, Advantages and Disadvantages, Principles, Importance)

#### Least Privilege

Normal users do not have the same level of power as compared to administrators. Normal users should not be able to change, view system critical files. Normal users are given as least privilege as possible.

#### Minimisation

Disable redundant services or services that are unnecessary for example FTP, TELNET.

#### Keep things simple

For making decisions between different choices, pick the one that does the job but simple. Not making things difficult.

### Question 10

The logon screen of workstations in an organisation reads ”Warning: All activity is constantly monitored and logged, including hostname and IP address.”

Explain the purpose of this notice and determine the type of security control and the universal security method of this practice.

(Types of security control - Preventive, Deterrent, Detective, Corrective, Recovery)

(Universal security method - Commonly used security methods)

**Purpose: (based on this scenario)**

#### Deterrent control

This is used to discourage malicious activities by users. Users will know that people at the backend will be able to see their activities.This security method leverages unpredictability.

## Week 7: Busniess Continuity I

### Comprehensive approach to business continuity plan

**业务连续性计划的综合方法**

* **Prevention**: risk management plan (this lecture) – what to do to prevent incidents

预防：风险管理计划--如何预防事故的发生

* **Preparedness**: business impact analysis – if incidents do happen, what would be the impact

准备工作：业务影响分析--如果事件真的发生，会有什么影响？

* **Response**: incident response plan – what to do when incidents happen

应对措施：事件应对计划--当事件发生时该怎么做

* **Recovery**: recovery plan – how to recover after an incident/disaster

恢复：恢复计划--事件/灾难发生后如何恢复

****

### Risk Management 风险管理

**Risk**

* **Definition:** An uncertain event that, if it occurs, has a positive or negative effect on objectives
* **Definition:** An uncertain event that, if it occurs, has a positive or negative effect on objectives

### Risk Management 风险管理

* A proactive attempt to recognize and manage internal events and external threats that affect the likelihood of success

主动尝试认识和管理影响成功可能性的内部事件和外部威胁

* What can go wrong (risk event)

可能出错的地方（风险事件）

* How to minimize the risk event’s impact (consequences)

如何将风险事件的影响（后果）降到最低？

* What can be done before an event occurs (anticipation)

在事件发生前可以做什么（预期）

* What to do when an event occurs (contingency plans)

当事件发生时该怎么做（应急计划）

### Risk management plan consists of three stages

**风险管理计划包括三个阶段**

#### Plan 计划

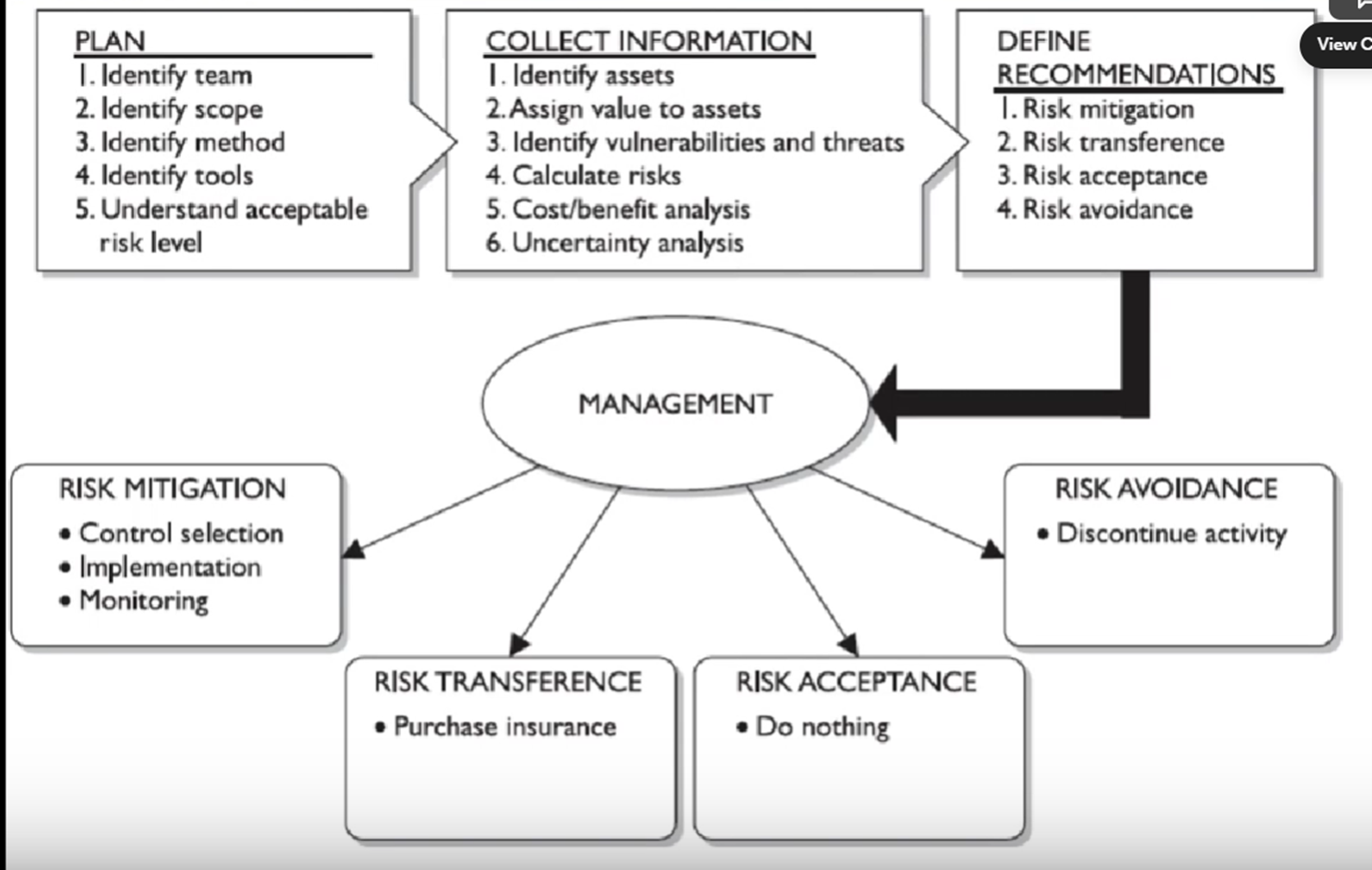
* 1. Identify team 确定团队
  2. Identify scope 确定范围
  3. Identify method 确定方法
  4. Identify tools 识别工具
  5. Understand acceptable risk level 理解可接受的风险水平

#### Collect information/perform risk analysis 收集信息/进行风险分析

* 1. Identify assets 识别资产
  2. Assign value to assets 为资产分配价值
  3. Identify vulnerabilities and threats 识别脆弱性和威胁
  4. Calculate risks 计算风险
  5. Cost/benefit analysis 成本/效益分析
  6. Uncertainty analysis 不确定性分析

#### Define recommendations 确定建议

* 1. Defend the risk: lock the door, install IDS, block specific ports associated with specific attacks 防御风险：锁住门，安装IDS，阻止与特定攻击有关的特定端口
  2. Mitigate the risk: incident response, disaster recovery, and business continuity plans 减轻风险：事件响应、灾难恢复和业务连续性计划
  3. Transfer the risk: outsource 转移风险：外包
  4. Avoid/terminate the risk: disable USB port 避免/终止风险：禁用USB端口
  5. Accept the risk: do nothing 接受风险：什么都不做



### How to determine risk 如何确定风险

* Loss/damage 损失/损坏

#### Likelihood 可能性

* + **Definition:** Likelihood is the probability that a specific vulnerability will be the object of a successful attack.

定义: 可能性是指某一特定漏洞成为成功攻击对象的概率。

* + In risk assessment, you assign a numeric value to likelihood. The National Institute of Standards and Technology recommends in Special Publication 800-30 assigning a number between 0.1 (low) and 1.0 (high).

在风险评估中，你要给可能性分配一个数字值。美国国家标准和技术研究所在特别出版物800-30中建议指定一个0.1（低）和1.0（高）之间的数字。

* + For example, the likelihood of an asset being struck by a meteorite while indoors would be rated 0.1. At the other extreme, receiving at least one e-mail containing a virus or worm in the next year would be rated 1.0. You could also choose to use a number between 1 and 100 (zero is not used, since vulnerabilities with a zero likelihood have been removed from the asset/vulnerability list). Whichever rating system you choose, use professionalism, experience, and judgment—and use the rating model you select consistently. Whenever possible, use external references for likelihood values that have been reviewed and adjusted for your specific circumstances. Many asset/vulnerability combinations have sources for likelihood, for **Example**:

例如，一项资产在室内被陨石击中的可能性将被评为0.1。在另一个极端，在未来一年内至少收到一封含有病毒或蠕虫的电子邮件，将被评为1.0。你也可以选择使用1到100之间的数字（不使用零，因为可能性为零的漏洞已经从资产/漏洞列表中删除）。无论你选择哪种评级系统，都要使用专业性、经验和判断力--并持续使用你所选择的评级模型。在可能的情况下，使用外部参考资料，以获得经过审查和调整的可能性值，以适应你的具体情况。许多资产/脆弱性的组合都有可能性的来源，**例如：**

* + - The likelihood of a fire has been estimated actuarially for each type of structure.

每种类型的结构发生火灾的可能性都进行了精算估计。

* + - The likelihood that any given e-mail contains a virus or worm has been researched.

任何特定的电子邮件包含病毒或蠕虫的可能性已经被研究过。

* + - The number of network attacks can be forecast based on how many assigned network addresses the organization has.

网络攻击的数量可以根据该组织有多少个分配的网络地址来预测。

* Effectiveness of existing controls

现有控制的有效性

* Uncertainty of vulnerability knowledge

脆弱性知识的不确定性

### Residual risk 剩余风险

For each threat and its associated vulnerabilities that have residual risk, you must create a preliminary list of potential controls. Residual risk is the risk to the information asset that remains even after the application of controls.

对于每个具有剩余风险的威胁及其相关的漏洞，你必须创建一个潜在控制的初步清单。剩余风险是对信息资产的风险，即使在应用了控制措施后仍然存在。

* **Definition:** Risk not yet addressed by existing controls

定义: 现有控制措施尚未解决的风险

* Residual risk=Total risk x Control gap

剩余风险=总风险x控制差距

If a company addresses 20% of the risk, then the control gap will be 80%

For each threat and its associated vulnerabilities that have residual risk, you must create a preliminary list of potential controls. Residual risk is the risk to the information asset that remains even after the application of controls.

如果一个公司解决了20%的风险，那么控制差距将是80%。

对于每个具有剩余风险的威胁及其相关的漏洞，你必须创建一个潜在控制的初步清单。剩余风险是指即使在应用了控制措施之后，对信息资产仍然存在的风险。

**Risk is**

**风险是**

the *likelihood* of the occurrence of a vulnerability

发生漏洞的可能性

**multiplied by**

**乘以**

the *value* of the information asset

信息资产的价值

**Minus**

**减去**

The percentage of risk mitigated by *current controls*

*目前的控制措施*所缓解的风险的百分比

**Plus**

**加**

The *uncertainty* of current knowledge of the vulnerability

目前对脆弱性的认识的不确定性

**Formula: Risk =**the *likelihood* of the occurrence of a vulnerability \* the *value* of the information asset - The percentage of risk mitigated by *current controls +* The *uncertainty* of current knowledge of the vulnerability

### Risk Management Plan 风险管理计划

Risk management plans usually have four, linked, objectives. These are:

风险管理计划通常有四个相互关联的目标。这些目标是：

1. to eliminate risks;

消除风险

1. to reduce to ‘acceptable’ levels those that cannot be eliminated; and then either

将那些无法消除的问题减少到 "可接受 "的水平；然后，或者

1. to live with them, exercising carefully the controls that keep them ‘acceptable’;

与他们一起生活，小心翼翼地进行控制，使他们保持 "可接受"

1. to transfer them, by means of insurance, to some other organization.

通过保险的方式，将它们转移到其他组织。

**Risk Management**

**风险管理**

Risk management is the process of identifying risk, as represented by vulnerabilities, to an organization’s information assets and infrastructure, and taking steps to reduce this risk to an acceptable level. Each of the three elements in the C.I.A. triad, is an essential part of every IT organization’s ability to sustain long-term competitiveness.

风险管理是指识别组织的信息资产和基础设施的风险（以脆弱性为代表），并采取措施将这种风险降低到可接受的水平的过程。C.I.A.三要素中的每一个，都是每个IT组织保持长期竞争力的重要组成部分。

### Risk management involves three major undertakings:

**风险管理涉及三项主要工作:**

* **Risk identification** is the examination and documentation of the security posture of an organization’s information technology and the risks it faces.

风险识别是对一个组织的信息技术的安全态势和它所面临的风险的检查和记录。

* **Risk assessment** is the determination of the extent to which the organization’s information assets are exposed or at risk.

风险评估是确定组织的信息资产被暴露或面临风险的程度。

* **Risk control** is the application of controls to reduce the risks to an organization’s data and information systems

风险控制是应用控制措施来减少组织的数据和信息系统的风险。

### Risk management: formal process 风险管理：正式程序

The risk assessment must be a formal process. In other words, the process must be planned, and the input data, their analysis and the results should all be recorded.

风险评估必须是一个正式的过程。换句话说，这个过程必须是有计划的，而且输入的数据、它们的分析和结果都应该被记录下来。

* Planning 规划
* Documentation 文件
* Assurance 保证

### Who is to undertake this risk assessment, and How

**谁来进行这一风险评估，以及如何进行？**

* **Periodic review 定期审查**

The first is that the standard expects that **periodic reviews** of security risks and related controls will be carried out –taking account of new threats and vulnerabilities, assessing the impact of changes in the business, its goals or processes, technology and/or its external environment (such as legislation, regulation or society) and simply to confirm that controls remain effective and appropriate. **Periodic review is a fundamental requirement of any risk assessment or risk management strategy.**

首先，该标准希望对安全风险和相关控制措施进行**定期审查**--考虑到新的威胁和漏洞，评估企业、其目标或流程、技术和/或其外部环境（如立法、法规或社会）的变化所产生的影响，以及简单地确认控制措施仍然有效和适当。定期审查是任何风险评估或风险管理战略的一个基本要求。

* **Appropriately qualified and experienced person 有适当资格和经验的人**

The second is that it is an assumption of the standard ‘that the execution of its provisions is entrusted to appropriately qualified and experienced people’. It is essential that risk assessment – the core competency of information security management – is conducted by **an appropriately qualified and experienced person**. This is logical; the key step on which the entire ISMS will be built needs, itself, to be solid. The ISO27001 auditor will therefore want to see documentary evidence of the formal qualifications and experience of this person.

第二，该标准的一个假设是 "将其规定的执行委托给有适当资格和经验的人"。风险评估--信息安全管理的核心能力--必须由具有适当资格和经验的人进行。这是符合逻辑的；整个ISMS系统赖以建立的关键步骤本身就必须是坚实的。因此，ISO27001审核员将希望看到这个人的正式资格和经验的文件证据。

**Risk Assessment**

**风险评估**

**Quantitative risk assessment**

**量化风险评估**

**Purpose:** Quantitative risk analysis attempts to assign real and meaningful numbers to all elements of the risk analysis process.

目的: 定量风险分析试图为风险分析过程中的所有要素分配真实和有意义的数字。

**Example:** These elements may include safeguard costs, asset value, business impact, threat frequency, safeguard effectiveness, exploit probabilities, and so on.

例子: 这些要素可能包括保障成本、资产价值、业务影响、威胁频率、保障有效性、利用概率等等。

When all of these are quantified, the process is said to be quantitative.

当所有这些都被量化时，这个过程就被说成是定量的。

**Quantitative risk analysis** also provides concrete probability percentages when determining the likelihood of threats. Each element within the analysis (asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items) is quantified and entered into equations to determine total and residual risks.

定量风险分析在确定威胁的可能性时也提供具体的概率百分比。分析中的每个元素（资产价值、威胁频率、脆弱性的严重程度、影响损害、保障成本、保障有效性、不确定性和概率项目）都被量化并输入方程，以确定总风险和剩余风险。

**Limitations:** Purely quantitative risk analysis is **not possible** because the method attempts to quantify qualitative items, and there are always **uncertainties** in quantitative values.

局限性: 纯粹的定量风险分析是不可能的，因为该方法试图对定性的项目进行量化，而定量的数值总是存在不确定性。

**Issues addressed: 解决的问题**

1. the probability of an event occurring 事件发生的概率
2. the likely loss should it occur. 一旦发生可能造成的损失

A single figure is produced from these two elements, by simply multiplying the potential loss (measured in monetary terms) by its probability (measured as a percentage). This is sometimes called the ‘annual loss expectancy’ (ALE) or the ‘estimated annual cost’ (EAC).

通过简单地将潜在的损失（以货币计量）乘以其概率（以百分比计量），就可以从这两个要素中得出一个单一的数字。这有时被称为 "年度损失预期"（ALE）或 "估计年度成本"（EAC）。

**(ALE) = potential loss ($) x probability (%)**

**(ALE) = 潜在损失 ($) x 概率 (%)**

Clearly, **the higher the number** that an event or risk has, **the more serious** it is for the organization. It is then possible to rank events in order of risk (ALE) and to make decisions based upon this.

显然，一个事件或风险的数字越高，它对组织的影响就越严重。这样就有可能按照风险（ALE）对事件进行排序，并在此基础上做出决策。

**Limitations/ Disadvantages: 局限性/劣势**

The problems with this type of risk analysis are usually associated with the **unreliability and inaccuracy of the data**. Probability is usually assessed subjectively and is rarely precise. In some cases, this approach can promote or reflect complacency about the real significance of particular risks.

这种类型的风险分析的问题通常与数据的不可靠和不准确有关。概率通常是主观评估的，很少是精确的。在某些情况下，这种方法会促进或反映对特定风险的真正意义的自满。

The monetary value of the potential loss is also often assessed subjectively, and when the two components are multiplied together, the answer is equally subjective.

In addition, controls and countermeasures often have to tackle a number of potential events, and the events themselves are frequently interrelated. A detailed ranking in order of ALE can make it difficult to identify these interrelationships and lead to poor decisions about controls, and this approach is not, therefore, recommended.

潜在损失的货币价值也往往是主观评估的，当这两部分相乘，答案同样是主观的。

此外，控制和反措施往往要处理一些潜在的事件，而这些事件本身又经常是相互关联的。按照ALE的顺序进行详细排序，会使人难以识别这些相互关系，并导致控制措施的决策失误，因此，不建议采用这种方法。

**Qualitative Risk Assessment/Analysis:**

**定性风险评估/分析**

**Definition**: does not assign numbers and monetary values to components and losses. Instead, qualitative methods walk through different scenarios of risk possibilities and rank the seriousness of the threats and the validity of the different possible countermeasures based on opinions.

定义：不给组成部分和损失分配数字和货币价值。相反，定性方法通过不同的风险可能性情景，并根据意见对威胁的严重性和不同的可能对策的有效性进行排序。

**Qualitative analysis techniques include:**

**定性分析技术包括:**

1. judgment 判断
2. best practices 最佳做法
3. intuition 直觉
4. experience 经验

**Examples of qualitative techniques to gather data are:**

**收集数据的定性技术的例子是:**

Delphi, brainstorming, storyboarding, focus groups, surveys, questionnaires, checklists, one-on-one meetings, and interviews.

Delphi、头脑风暴、故事板、焦点小组、调查、问卷、检查表、一对一会议和访谈。

**The risk analysis team** 风险分析小组

will determine the best technique for the threats that need to be assessed, as well as the culture of the company and individuals involved with the analysis.

将确定需要评估的威胁的最佳技术，以及公司的文化和参与分析的个人。

The team that is performing the risk analysis gathers personnel who have experience and education on the threats being evaluated. When this group is presented with a scenario that describes threats and loss potential, each member responds with their gut feeling and experience on the likelihood of the threat and the extent of damage that may result.

执行风险分析的团队聚集了对所评估的威胁具有经验和教育的人员。当这个小组收到描述威胁和潜在损失的方案时，每个成员都会根据自己的直觉和经验对威胁的可能性和可能造成的损失程度做出反应。 v

**Concepts**

**概念**

### Single Loss Expectancy 单次损失预期

is the calculation of the value associated with the most likely loss from an attack. It is a calculation based on the value of the asset and the exposure factor (EF), which is the expected percentage of loss that would occur from a particular attack, as follows**:**

是计算与最有可能遭受攻击的损失有关的价值。它是基于资产的价值和风险系数（EF）的计算，风险系数是指某一特定攻击所带来的预期损失的百分比，如下所示:

**SLE = asset value x exposure factor (EF%)**

**SLE=资产价值×风险系数（EF%）**

where **EF equals the percentage loss** that would occur from a given vulnerabi lity being exploited.

其中EF等于特定漏洞被利用所造成的损失百分比

Example:

For example, if a Web site has an estimated value of $1,000,000 (value determined by asset valuation), and a deliberate act of sabotage or vandalism (hacker defacement) scenario indicates that 10 percent of the Web site would be damaged or destroyed after such an attack, then the SLE for this Web site would be $1,000,000 0.10 $100,000.

例如，如果一个网站的估计价值为1,000,000美元（价值由资产评估决定），而蓄意的破坏或毁坏行为（黑客污损）情况表明，在这种攻击后，10%的网站将被损坏或摧毁，那么这个网站的SLE将是1,000,000 \*0.10 =100,000。

### **Annualized rate of occurrence (ARO).** **年化发生率（ARO）**

This calculates how often an organisation expects an event. It is simply how often you expect a specific type of attack to occur per year.

这计算了一个组织对一个事件的预期频率。简单地说，就是你预计某种特定类型的攻击每年会发生多少次。

Example:

A successful deliberate act of sabotage or vandalism might occur about once every two years, in which case the ARO would be 50 percent (0.50), whereas some kinds of network attacks can occur multiple times per second. To standardize calculations, you convert the rate to a yearly (annualized) value. This is expressed as the probability of a threat occurrence.

一个成功的蓄意破坏或破坏行为可能每两年发生一次，在这种情况下，ARO将是50%（0.50），而某些类型的网络攻击每秒可能发生多次。为了使计算标准化，你可以将比率转换为年度（年化）值。这被表示为威胁发生的概率。

Once each asset’s worth is known, the next step is to ascertain how much loss is expected from a single expected attack, and how often these attacks occur. Once those values are established, the equation can be completed to determine the overall lost potential per risk. **This is usually determined through an annualized loss expectancy (ALE), which is calculated from the ARO and SLE, as shown here:**

一旦知道了每项资产的价值，下一步就是要确定一次预期的攻击会带来多少损失，以及这些攻击发生的频率如何。一旦确定了这些价值，就可以完成方程式，以确定每个风险的总体损失潜力。**这通常是通过年化损失预期（ALE）来确定的，它是由ARO和SLE计算出来的，如图所示。**

**ALE = SLE x ARO**

Using the example of the Web site that might suffer a deliberate act of sabotage or vandalism and thus has an SLE of $100,000 and an ARO of 0.50, the ALE would be calculated as follows:

以可能遭受蓄意破坏或毁坏的网站为例，因此其SLE为100,000美元，ARO为0.50，ALE的计算方法如下:

ALE = $100,000 x 0.50 = $50,000

### **The Cost Benefit Analysis (CBA) Formula**:

成本收益分析

Subtract the revised ALE, estimated based on the control being in place, known as **ALE(post)**. Complete the calculation by subtracting the **annualized cost of the safeguard (ACS).**

减去修订后的 ALE，该 ALE 是根据现有控制估算的，称为 ALE(post)。通过减去保障措施 (ACS) 的年化成本来完成计算。

**CBA = ALE(prior) - ALE(post) - ACS**

**Risk Assesment**

**Disadvantages of Risk Assessment:**

Risk assessment can be a time-consuming process to meet standards

为了达到标准，风险评估可能是一个耗时的过程

**Tools to asses and handle threats 评估和处理威胁的手段**

There are an increasing number of software tools available that can, to a varying extent, automate the risk assessment process and generate the statement of applicability.

现在有越来越多的软件工具可以在不同程度上实现风险评估过程的自动化，并生成适用性声明

Use of tools is optional, organisations need to examine their pros & cons

工具的使用是可选的，组织需要审查其利弊。

**Purpose:** In theory, such a tool ought to encourage the user to perform a thorough and comprehensive security audit on the organization’s information systems, and ought not to produce too much paperwork as a result.

目的：在理论上，这样的工具应该鼓励用户对组织的信息系统进行彻底和全面的安全审计，并且不应该因此而产生过多的文件。

The organization will need to compare tools before making a selection and should concentrate, in the comparison process, on the extent to which the tool really does easily and effectively automate the risk assessment and statement of applicability development process; the amount of additional paperwork it generates; the flexibility it offers for dealing with changing circumstances and frequent, smaller-scale risk assessments; and the meaningfulness of the results it generates. Of course, normal due diligence should also be done into the status of the supplier and manufacturer of the product to ensure that it is properly supported and likely to continue to be. References might also be sought from happy customers. ( Tools could generate and plot graphs or templates for risk assessment from surveys)

在做出选择之前，组织将需要对工具进行比较，在比较过程中，**应集中注意该工具在多大程度上真正做到了风险评估和适用性声明开发过程的自动化**；**它产生的额外文书工作的数量；它为处理不断变化的情况和频繁的、小规模的风险评估提供的灵活性；以及它产生的结果的意义**。当然，还应该对产品的供应商和制造商的状况进行正常的尽职调查，以确保它得到适当的支持并可能继续下去。也可以从快乐的客户那里寻求参考。(工具可以从调查中生成和绘制风险评估的图表或模板）。

**Cons/Disadvantages of using RA tools:**

**使用RA工具的缺点/劣势:**

* Organisation would be too dependent on these risk assessment tools

组织将过于依赖这些风险评估工具

* Everytime an organisation hires new people they would have to train the new people on how to use these softwares

每当一个组织雇用新人时，他们就必须培训新人如何使用这些软件。

**Alternatives if RA tools are not used:**

**如果不使用RA工具，则有替代方案:**

Risk assessments can, with difficulty, be done without using such tools.

如果不使用这种工具，风险评估是很难完成的。

A thorough risk assessment of any significant business will be very time- consuming, and even more so if a software tool is not used.

对任何重要的业务进行彻底的风险评估都是非常耗时的，如果不使用软件工具，就更耗时了。

‘Time-consuming’ means up to three months, or even longer for larger organizations. The use of a software tool will depend on the culture of the organization and the preferences of the information security adviser and manager.

耗时 "是指长达三个月的时间，对于大型组织来说甚至更长。软件工具的使用将取决于组织的文化以及信息安全顾问和经理的偏好。

Practically speaking, once the organization has decided to purchase such a tool, it becomes dependent on that tool and on the staff members who are trained to use it. In considering the appropriate route forward, consideration should be given to the speed with which incoming staff can become familiar with the chosen risk assessment tool; practicality and ease of use are likely to be key attributes

实际上，一旦组织决定购买这种工具，它就会依赖这种工具和接受培训使用这种工具的工作人员。在考虑适当的前进路线时，应考虑到新员工熟悉所选风险评估工具的速度；实用性和易用性可能是关键属性。

### Risk Analysis

**风险分析**

**Importance: 重要性**

* Controls usually should not cost more than the amount of damage that is being reduced. Thus an organisation should compare the cost of the control and the benefit that you reap from the control in terms of reducing the quantitative risk. Implement the control if the benefit outweighs the cost. If the cost is too high then the control is not worth it, an organisation can then choose to accept the risk. Through risk analysis, an organisation could compare and rank the risk based on which is important and address the important threat first.

控制措施的成本通常不应超过所减少的损失量。因此，一个组织应该比较控制的成本和你从控制中获得的减少数量风险的利益。如果收益超过了成本，就实施控制。如果成本太高，那么这个控制就不值得，那么一个组织就可以选择接受风险。通过风险分析，一个组织可以根据哪些风险是重要的进行比较和排序，并首先解决重要的威胁。

* Security can be quite complex, even for well- versed security professionals, and it is easy to apply too much security, not enough security, or the wrong security components, and to spend too much money in the process without attaining the necessary objectives. Risk analysis helps companies prioritize their risks and shows management the amount of money that should be applied to protecting against those risks in a sensible manner.

安全可能是相当复杂的，即使对精通安全的专业人员来说也是如此，而且很容易应用太多的安全，没有足够的安全，或错误的安全组件，并在这个过程中花费太多的钱而没有达到必要的目标。风险分析帮助公司确定其风险的优先次序，并向管理层展示应该以合理的方式用于保护这些风险的资金数额。

#### Purpose: 目的

identify weaknesses, potential attacks and estimate potential damage

确定弱点、潜在的攻击和估计潜在的损害

#### Definition: 定义

Risk analysis, which is really a tool for risk management, is a method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security safeguards. **Risk analysis is used to ensure that security is cost-effective, relevant, timely, and responsive to threats**.

风险分析，实际上是一种风险管理的工具，是一种识别脆弱性和威胁并评估可能影响的方法，以确定在何处实施安全保障措施。风险分析被用来**确保安全的成本效益、相关性、及时性和对威胁的反应。**

**A risk analysis has four main goals**:

**风险分析有四个主要目标:**

1. Identify assets and their value to the organization.

识别资产和它们对组织的价值。

1. Identify vulnerabilities and threats.

识别脆弱性和威胁。

1. Quantify the probability and business impact of these potential threats.

量化这些潜在威胁的概率和商业影响。

1. Provide an economic balance between the impact of the threat and the cost of the countermeasure.

在威胁的影响和应对措施的成本之间提供一个经济平衡。

#### What Risk Analysis do: 风险分析的作用

Risk analysis provides a cost/benefit comparison, which compares the annualized cost of safeguards to the potential cost of loss. A safeguard, in most cases, should not be implemented unless the annualized cost of loss exceeds the annualized cost of the safe- guard itself.

风险分析提供了一种成本/效益比较，它将保障措施的年化成本与潜在的损失成本进行比较。在大多数情况下，除非损失的年化成本超过安全防护措施本身的年化成本，否则不应实施保障措施。

Example: This means that if a facility is worth $100,000, it does not make sense to spend $150,000 trying to protect it. It is important to figure out what you are supposed to be doing before you dig right in and start working.

例子。这意味着，如果一个设施价值10万美元，花15万美元来保护它是没有意义的。重要的是，在你直接开始工作之前，要弄清楚你应该做什么。

Anyone who has worked on a project without a properly defined scope can attest to the truth of this statement. Before an assessment and analysis is started, the team must carry out project sizing to understand what assets and threats should be evaluated. Most assessments are focused on physical security, technology security, or personnel security. Trying to assess all of them at the same time can be quite an undertaking.

任何在没有正确定义范围的情况下从事过项目的人都可以证明这一说法的真实性。在评估和分析开始之前，团队必须进行项目规模的确定，以了解哪些资产和威胁应该被评估。大多数评估都集中在物理安全、技术安全或人员安全方面。试图在同一时间对所有这些进行评估可能是一项相当大的工程。

#### What should be done by a team:一个团队应该做什么

* **Team:** of the team’s tasks is to create a report that details the asset valuations. Senior management should review and accept the lists, and make them the scope of the IRM project. If management determines at this early stage that some assets are not important, the risk assessment team should not spend additional time or resources evaluating those assets.

团队：团队的任务之一是创建一份报告，详细说明资产评估。高级管理层应该审查和接受这些清单，并将其作为IRM项目的范围。如果管理层在这个早期阶段确定某些资产并不重要，风险评估小组就不应该花费额外的时间或资源来评估这些资产

* **During discussions**: with management, everyone involved must have a firm understanding of the value of the security AIC triad (availability, integrity, and confidentiality) and how it directly relates to business needs.

在讨论过程中：与管理层一起，每个人都必须对安全AIC三要素（可用性、完整性和保密性）的价值以及它与业务需求的直接关系有坚定的理解。

* **Management:** should outline the scope, which most likely will be dictated by organizational governance, risk management, and compliance as well as budgetary constraints. Many projects have run out of funds, and consequently stopped, because proper project sizing was not conducted at the onset of the project.

管理：应该列出范围，这很可能是由组织治理、风险管理、合规性以及预算限制决定的。许多项目由于在项目开始时没有进行适当的项目定位而耗尽了资金，并因此而停止。

**Importance and purpose:** A risk analysis helps integrate the security program objectives with the company’s business objectives and requirements. The more the business and security objectives are in alignment, the more successful the two will be. The analysis also helps the company draft a proper budget for a security program and its constituent security components. Once a company knows how much its assets are worth and the possible threats they are exposed to, it can make intelligent decisions about how much money to spend protecting those assets.

重要性和目的：风险分析有助于将安全计划目标与公司的业务目标和要求相结合。**业务和安全目标**越一致，两者就越成功。该分析还有助于公司为安全计划及其组成的安全组件起草一个适当的预算。一旦公司知道其资产的价值以及它们可能面临的威胁，它就可以对花多少钱来保护这些资产做出明智的决定。

* **Management:** A risk analysis must be supported and directed by senior management if it is to be successful. Management must define the purpose and scope of the analysis, appoint a team to carry out the assessment, and allocate the necessary time and funds to conduct the analysis. ***It is essential for senior management to review the outcome of the risk assessment and analysis and to act on its findings.***

管理。风险分析要想成功，必须得到高级管理层的支持和指导。管理层必须确定分析的目的和范围，任命一个团队来进行评估，并分配必要的时间和资金来进行分析。***高级管理层必须审查风险评估和分析的结果，并根据其结果采取行动。***

### Strategies to Address Risks

**应对风险的策略**

**Strategies to address risks:**

**应对风险的策略:**

1. Defend 保卫
2. Transfer 转移
3. Mitigate 减轻影响
4. Terminate/Avoid 终止/避免
5. Accept 接受

#### Defend 保卫

**Purpose**: 目的

* To reduce the likelihood of the risk coming through.

为了减少风险出现的可能性。

**How it is carried out: 如何进行**

1. **The defend control strategy attempts to prevent the exploitation of the vulnerability.**

**防御控制策略试图防止漏洞的利用。**

* This is the preferred approach and is accomplished by means of countering threats, removing vulnerabilities from assets, limiting access to assets, and adding protective safeguards.

这是**首选**的方法，通过对抗威胁、消除资产的脆弱性、限制对资产的访问和增加保护性保障措施来实现。

* Organizations can mitigate risk to an asset by countering the threats it faces or by eliminating its exposure. It is difficult, but possible, to eliminate a threat.

各组织可以通过对抗资产所面临的威胁或消除其风险来减少资产的风险。消除威胁是困难的，但也是可能的。

For example, in 2002 McDonalds Corporation, which had been subject to attacks by animal rights cyberactivists, sought to reduce risks by imposing stricter conditions on egg suppliers regarding the health and welfare of chickens. This strategy was consistent with other changes made by McDonalds to meet demands from animal rights activists and improve relationships with these groups.

例如，在2002年，麦当劳公司受到了动物权利网络活动家的攻击，它试图通过对鸡蛋供应商施加更严格的关于鸡的健康和福利的条件来减少风险。这一策略与麦当劳为满足动物权利活动家的要求和改善与这些团体的关系而做出的其他改变是一致的。

1. **Another defend strategy is the implementation of security controls and safeguards to deflect attacks on systems and therefore minimize the probability that an attack will be successful.**

**另一个防御策略是实施安全控制和保障措施，以转移对系统的攻击，从而将攻击成功的概率降到最低。**

* An organization with dial-in access vulnerability, for example, may choose to implement a control or safeguard for that service. An authentication procedure based on a cryptographic technology, such as RADIUS (Remote Authentication Dial-In User Service), or another protocol or product, would provide sufficient control. On the other hand, the organization may choose to eliminate the dial-in system and service to avoid the potential risk

例如，一个有拨号访问漏洞的组织，可以选择对该服务实施控制或保障。基于加密技术的认证程序，如RADIUS（远程认证拨入用户服务），或其他协议或产品，将提供足够的控制。另一方面，该组织可以选择取消拨号系统和服务，以避免潜在的风险。

#### Transfer 转移

**Purpose:** The transfer control strategy attempts to shift risk to other assets, other processes, or other organizations.

目的：转移控制策略试图将风险转移到其他资产、其他过程或其他组织。

**How it is carried out:** Contact the other party if the risk comes through. This can be accomplished by rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing insurance, or implementing service contracts with providers.

**如何进行:** 如果风险来了就联系对方。这可以通过重新思考如何提供服务，修改部署模式，外包给其他组织，购买保险，或与供应商实施服务合同来实现。

**Example:** many organizations want Web services, including Web presences, domain name registration, and domain and Web hosting. Rather than implementing their own servers and hiring their own Webmasters, Web systems administrators, and specialized security experts, savvy organizations hire an ISP or a consulting organization to provide these products and services for them. This allows the organization to transfer the risks associated with the management of these complex systems to another organization that has experience in dealing with those risks. A side benefit of specific contract arrangements is that the provider is responsible for disaster recovery, and through service level agreements is responsible for guaranteeing server and Web site availability.

例如：许多组织希望得到网络服务，包括网络存在、域名注册、域名和网络托管。精明的组织没有实施他们自己的服务器和雇用他们自己的网站管理员、网络系统管理员和专门的安全专家，而是雇用一个ISP或一个咨询组织为他们提供这些产品和服务。这使得该组织可以将与管理这些复杂系统有关的风险转移给另一个有处理这些风险经验的组织。具体合同安排的一个附带好处是，供应商负责灾难恢复，并通过服务水平协议负责保证服务器和网站的可用性。

#### Mitigate 缓解

The mitigate control strategy attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.

缓解控制策略试图通过计划和准备来减少利用漏洞造成的影响。

**This approach requires the creation of three types of plans**:

**这种方法需要建立三种类型的计划。**

* the incident response plan, 事件响应计划。
* the disaster recovery plan, 灾难恢复计划。
* the business continuity plan. 业务连续性计划。

#### Terminate 终止

**Definition/Purpose:** The terminate control strategy directs the organization to avoid those business activities that introduce uncontrollable risks. (Terminate what you are doing that causes the risk)

定义/目的：终止控制策略指导组织避免那些引入不可控风险的商业活动。(终止你正在做的导致风险的事情）。

**How it is done:** If an organization studies the risks from implementing business-to-consumer e-commerce operations and determines that the risks are not sufficiently offset by the potential benefits, the organization may seek an alternate mechanism to meet customer needs perhaps developing new channels for productdistribution or new partner- ship opportunities. By terminating the questionable activity, the organization reduces the risk exposure.

如何做到这一点: 如果一个组织研究了实施企业对消费者电子商务业务的风险，并确定这些风险没有被潜在的利益充分抵消，那么该组织可能会寻求一种替代机制来满足客户的需求，也许会开发新的产品分销渠道或新的合作伙伴机会。通过终止有问题的活动，该组织减少了风险暴露。

#### Accept 接受

**(Especially if the risk is relatively low) 特别是在风险相对较低的情况下**

**Purpose:** The accept control strategy is the choice to do nothing to protect a vulnerability and to accept the outcome of its exploitation. This may or may not be a conscious business decision.

目的：接受控制策略是选择不做任何事情来保护一个漏洞，接受其被利用的结果。这可能是也可能不是一个有意识的商业决定。

**The only industry-recognized valid use of this strategy occurs when the organization has done the following:**

**业界公认的这种策略的唯一有效使用是在组织已经做了以下工作的情况下。**

1. Determined the level of risk

确定了风险的程度

1. Assessed the probability of attack

评估了攻击的概率

1. Estimated the potential damage that could occur from attacks

估计攻击可能造成的潜在损失

1. Performed a thorough cost benefit analysis

进行彻底的成本效益分析

1. Evaluated controls using each appropriate type of feasibility

使用每一种适当的可行性类型来评估控制措施

1. Decided that the particular function, service, information, or asset did not justify the cost of protection

决定特定的功能、服务、信息或资产不值得付出保护的代价

**This strategy is based on the conclusion that the cost of protecting an asset does not justify the security expenditure.**

**这一策略是基于这样的结论：保护资产的成本并不能证明安全支出的合理性。**

**Example**

suppose it would cost an organization $100,000 per year to protect a server. The security assessment determined that for $10,000 the organization could replace the information contained in the server, replace the server itself, and cover associated recovery costs. In this case, management may be satisfied with taking its chances and saving the money that would normally be spent on protecting this asset. If every vulnerability in the organization is handled by means of acceptance, it may reflect an inability to conduct proactive security activities and an apathetic approach to security in general. It is not acceptable for an organization to adopt a policy that ignorance is bliss and hope to avoid litigation by pleading ignorance of its obligation to protect employee and customer information. It is also unacceptable for management to hope that if they do not try to protect information, the opposition will assume that there is little to be gained by an attack. The risks far outweigh the benefits of this approach.

假设一个组织每年要花费10万美元来保护一台服务器。安全评估确定，只要花10,000美元，该组织就可以替换服务器中包含的信息，替换服务器本身，并支付相关的恢复费用。在这种情况下，管理层可能会满足于抓住机会，节省通常用于保护这一资产的资金。如果组织中的每一个漏洞都是通过接受的方式来处理的，这可能反映了组织没有能力进行主动的安全活动，以及对一般的安全采取冷漠的态度。一个组织如果采取无知是福的政策，并希望通过辩称对保护员工和客户信息的义务无知来避免诉讼，这是不可接受的。同样不能接受的是，管理层希望如果他们不努力保护信息，对手就会认为攻击没有什么好处。这种做法的风险远远超过了好处。

**Acceptance as a strategy is often mistakenly chosen based on the school of fish’s justification that sharks will not come after a small fish in a school of other small fish. But this reasoning can be very risky.**

**接受作为一种策略，往往是根据鱼群的理由而错误地选择的，即鲨鱼不会来追捕其他小鱼群中的一条小鱼。但这种推理可能是非常危险的。**

### Asset Management

**资产管理**

Assets may be **tangible (computers, facilities, supplies) or intangible (reputation,** data, intellectual property). It is usually harder to quantify the values of intangible assets, which may change over time.

资产可能是**有形的（计算机、设施、用品）或无形的（声誉、数据、知识产权）**。无形资产的价值通常更难量化，它可能会随着时间的推移而改变。

**Tangible Assets 有形资产**

Definition: Physical form, assets that can be sell in the market for fixed value

定义: 物质形态，可以在市场上以固定价值出售的资产

**Intangible Assets 无形资产**

Definition: Non-physical form

定义: 无形的形式

An asset can have both quantitative and qualitative measurements assigned to it, but these measurements need to be derived.

一项资产可以有定量和定性的衡量标准，但这些衡量标准需要得出。

**How the value is derived 价值是如何得出的**

* The actual value of an asset is determined by the **cost** it takes to **acquire, develop, and maintain it.**

一项资产的实际价值是由获取、开发和维护它所需的成本决定的。

* The value is determined by the importance it has to the owners, authorized users, and unauthorized users. Some information is important enough to a company to go through the steps of making it a trade secret.

价值是由它对所有者、授权用户和未授权用户的重要性决定的。有些信息对一个公司来说足够重要，以至于要通过各种步骤使其成为商业秘密。

* The value of an asset should reflect all identifiable costs that would arise if the asset were actually impaired.

一项资产的价值应该反映出如果资产实际减值会产生的所有可识别成本。

**Example:** If a server cost $4,000 to purchase, this value should not be input as the value of the asset in a risk assessment. Rather, the cost of replacing or re- pairing it, the loss of productivity, and the value of any data that may be corrupted or lost must be accounted for to properly capture the amount the company would lose if the server were to fail for one reason or another.

例子。如果一台服务器的购买成本为4,000美元，那么在风险评估中不应将这一价值作为资产的价值输入。相反，更换或重新配对的成本，生产力的损失，以及任何可能被破坏或丢失的数据的价值，都必须被计算在内，以正确掌握公司在服务器由于某种原因发生故障时的损失金额。如果服务器由于某种原因发生故障，公司将会损失多少。

**The following issues should be considered when assigning values to assets:**

**在给资产分配价值时，应考虑以下问题:**

1. Cost to acquire or develop the asset

获取或开发该资产的成本

1. Cost to maintain and protect the asset

维护和保护资产的成本

1. Value of the asset to owners and users

资产对所有者和使用者的价值

1. Value of the asset to adversaries

该资产对对手的价值

1. Value of intellectual property that went into developing the information

用于开发信息的知识产权的价值

1. Price others are willing to pay for the asset

其他人愿意为该资产支付的价格

1. Cost to replace the asset if lost

如果丢失，更换资产的成本

1. Operational and production activities affected if the asset is unavailable

如果资产无法使用，运营和生产活动受到影响

1. Liability issues if the asset is compromised

如果资产受到损害，责任问题

1. Usefulness and role of the asset in the organization

资产在组织中的有用性和作用

Understanding the value of an asset is the first step to understanding what security mechanisms should be put in place and what funds should go toward protecting it. A very important question is how much it could cost the company to not protect the asset.

了解一项资产的价值是了解应该建立什么安全机制和应该用什么资金来保护它的第一步。一个非常重要的问题是，如果不保护该资产，公司可能要付出多大的代价。

### Change Management

**变革管理**

**Definition:** process of implementing changes in a controlled manner for e.g. maintaining information integrity.

定义：以有控制的方式实施变化的过程，例如，保持信息的完整性。

**Importance: 重要性**

* Changes often happen on a very frequent basis e.g. I few are writing a piece of program, we are writing it incrementally, everytime a change ais made we have to push for those changes. That’s why we need standard procedures for pushing changes.

变化经常发生在非常频繁的基础上，例如，我几个人在写一个程序，我们是以递增的方式写的，每次有变化，我们都要推送这些变化。这就是为什么我们需要标准的程序来推送更改。

* Unmanaged changes to IT systems and networks can recklessly increase risk to enterprises. The key is rolling out an accepted change management process, and sticking to it.

对IT系统和网络不加管理的改变会肆无忌惮地增加企业的风险。关键是推出一个公认的变更管理流程，并坚持下去。

**There are different kinds of changes. 有不同种类的变化**

* Standard changes: low risk, follow standard procedure

标准变化：低风险，遵循标准程序

* Approved by top-management : should follow the process of change management

由最高管理层批准：应遵循变革管理的程序

**Examples**

Changes can be in the hardware or software of the system, patches or updates, new technology like facial recognition. Updates in the policy or when businesses are acquired by other businesses. All these changes need to go through change management. **For minor changes such as adding a user or changing some non-critical user configurations, may not need to follow change management procedures.**

变化可以是系统的硬件或软件，补丁或更新，新技术如面部识别。政策的更新或企业被其他企业收购时。所有这些变化都需要经过变更管理。**对于小的变化，如增加一个用户或改变一些非关键的用户配置，可能不需要遵循变化管理程序。**

Unmanaged changes to IT systems and networks can recklessly increase risk to enterprises. The key is rolling out an accepted change management process, and sticking to it.

对IT系统和网络不加管理的改变会肆无忌惮地增加企业的风险。关键是推出一个公认的变更管理流程，并坚持下去。

**Disadvantages/ Limitations/ Downsides: 劣势/局限性/缺点**

Many of the exposures associated with lack of change management are more complex and subtle than in the example. This is due to the complex nature of today's network environments. Networks are complicated ecosystems and dependencies are not always clear, especially to someone who only sees part of the whole system at a time. A database administrator changing an IP address could lead to a critical service outage. A router administrator that configures a new static route may inadvertently redirect or block traffic from hundreds of remote offices.

许多与缺乏变革管理相关的风险比例子中的更加复杂和微妙。这是由于当今网络环境的复杂性质所决定的。网络是复杂的生态系统，依赖关系并不总是很清楚，特别是对于那些每次只看到整个系统的一部分的人来说。一个数据库管理员改变一个IP地址可能会导致一个关键的服务中断。一个路由器管理员配置了一个新的静态路由，可能会在无意中重定向或阻止来自数百个远程办公室的流量。

**Purpose: 目的**

The purpose of change management is to prevent unintended consequences, such as the ones described, and ensure that changes or alterations to systems are implemented according to an approved framework or model. That's not something many employees would argue with. The problem occurs when an employee, such as the firewall admin in our example above, thinks that circumventing the system will allow things to work more efficiently--or feels that following the processes somehow detracts from getting "real work" done. So the challenge is not simply putting change management in place, but also gaining buy-in from all users of the system so that they're incented to follow the change management process rather than circumvent it.

变革管理的目的是防止出现诸如上述的意外后果，并确保对系统的改变或改动是根据一个经批准的框架或模式来实施。这并不是很多员工会争论的问题。问题是，当一个员工，比如我们上面例子中的防火墙管理员，认为规避系统可以使事情更有效地进行时，或者认为遵循流程在某种程度上会减损 "真正的工作 "的完成。因此，面临的挑战不仅仅是将变革管理落实到位，而且还要获得系统所有用户的支持，从而激励他们遵循变革管理流程，而不是绕过它。

**Recommended auditing change management in following areas:**

**建议在以下方面对变革管理进行审计:**

1. Acceptance 接受
2. Awareness 认知
3. Policies and Procedures 政策和程序
4. Tools and Automation 工具和自动化
5. Skills and Expertise 技能和专业知识
6. Responsibility and Accountability 责任和问责
7. Measurement 测量

Operational change management brings discipline and quality control to IS. Attention to governance and formal policies and procedures will ensure its success. Adopting formalised governance and policies for operational change management delivers a more disciplined and efficient infrastructure. This formalisation requires communication; the documentation of important process workflows and personnel roles; and the alignment of automation tools, where appropriate. Where change management is non-existent, it is incumbent on IS’s senior management to provide the leadership and vision to jump-start the process. By defining processes and policies, IS organisations can demonstrate increased agility in responding predictably and reliably to new business demands.

<Organisation> (hereafter called ‘the company’) management has recognised the importance of change management and control and the associated risks with ineffective change management and control and have therefore formulated this Change Management and Control Policy in order to address the opportunities and associated risks.

This policy applies to all parties operating within the company’s network environment or utilising Information Resources. It covers the data networks, LAN servers and personal computers (stand-alone or network-enabled), located at company offices and company production related locations, where these systems are under the jurisdiction and/or ownership of the company or subsidiaries, and any personal computers, laptops, mobile device and or servers authorised to access the company’s data networks. No employee is exempt from this policy.

**Change Procedure**

**更改程序**

The change management structure should be codified as an organization policy. Procedures for the operational aspects of the change management process should also be created. Change management policies and procedures are forms of directive controls. The following subsections outline a recommended structure for a change management process.

变革管理结构应被编入组织政策中。还应该建立变革管理过程中的操作程序。变革管理政策和程序是指令性控制的形式。以下各小节概述了变革管理过程的建议结构。

1. **Requests:** Proposed changes should be formally presented to the committee in writing. The request should include a detailed justification in the form of a business case argument for the change, focusing on the benefits of implementation and costs of not implementing. Can assign priority to these changes.

**要求:** 拟议的变化应以书面形式正式提交给委员会。请求应包括以商业案例论证形式提出的详细理由，重点说明实施的好处和不实施的成本。可以为这些变化分配优先权。

1. **Impact Assessment:** Members of the committee should determine the impacts to operations regarding the decision to implement or reject the change.

**影响评估:** 委员会成员应确定关于实施或拒绝变革的决定对运营的影响。

1. **Approval/Disapproval:** Requests should be answered officially regarding their acceptance or rejection.

**批准/不批准:** 应正式答复关于接受或拒绝的请求。

1. **Build and Test:** Once the proposal has been approved, the software would have to be put in an isolated environment but one that iss similar to the production system to test whether if everything works. Subsequent approvals are provided to operations support for test and integration development. A fallback plan should be in place such that the organisation would be able to recover from those unsuccessful changes. Go back to the previous working stage. The fallback has to be put in place before the testings are carried out.

建立和测试。一旦建议被批准，软件就必须被放在一个隔离的环境中，但这个环境与生产系统类似，以测试是否一切正常。随后的批准将提供给运营支持以进行测试和集成开发。应该有一个回退计划，这样组织就能从那些不成功的变化中恢复过来。回到以前的工作阶段。在进行测试之前，必须将回退计划落实到位。

The necessary software and hardware should be tested in a nonproduction environment. All configuration changes associated with a deployment must be fully tested and documented. The security team should be invited to perform a final review of the proposed change within the test environment to ensure that no vulnerabilities are introduced into the production system. Change requests involving the removal of a software or a system component require a similar approach. The item should be removed from the test environment and have a determination made regarding any negative impacts.

必要的软件和硬件应该在非生产环境中测试。所有与部署相关的配置变化都必须被充分测试和记录。应邀请安全团队在测试环境中对拟议的变更进行最终审查，以确保没有漏洞被引入生产系统。涉及移除软件或系统组件的变更请求需要采取类似的方法。该项目应从测试环境中移除，并对任何负面影响进行判断。

1. **Notification:** System users and stakeholders are notified of the proposed change and the schedule of deployment.

**通知:** 系统用户和利益相关者被告知拟议的变化和部署时间表。

1. **Implementation:** The change is deployed incrementally, when possible, and monitored for issues during the process.

**实施:** 在可能的情况下，变化是渐进式部署的，并在过程中监测问题。

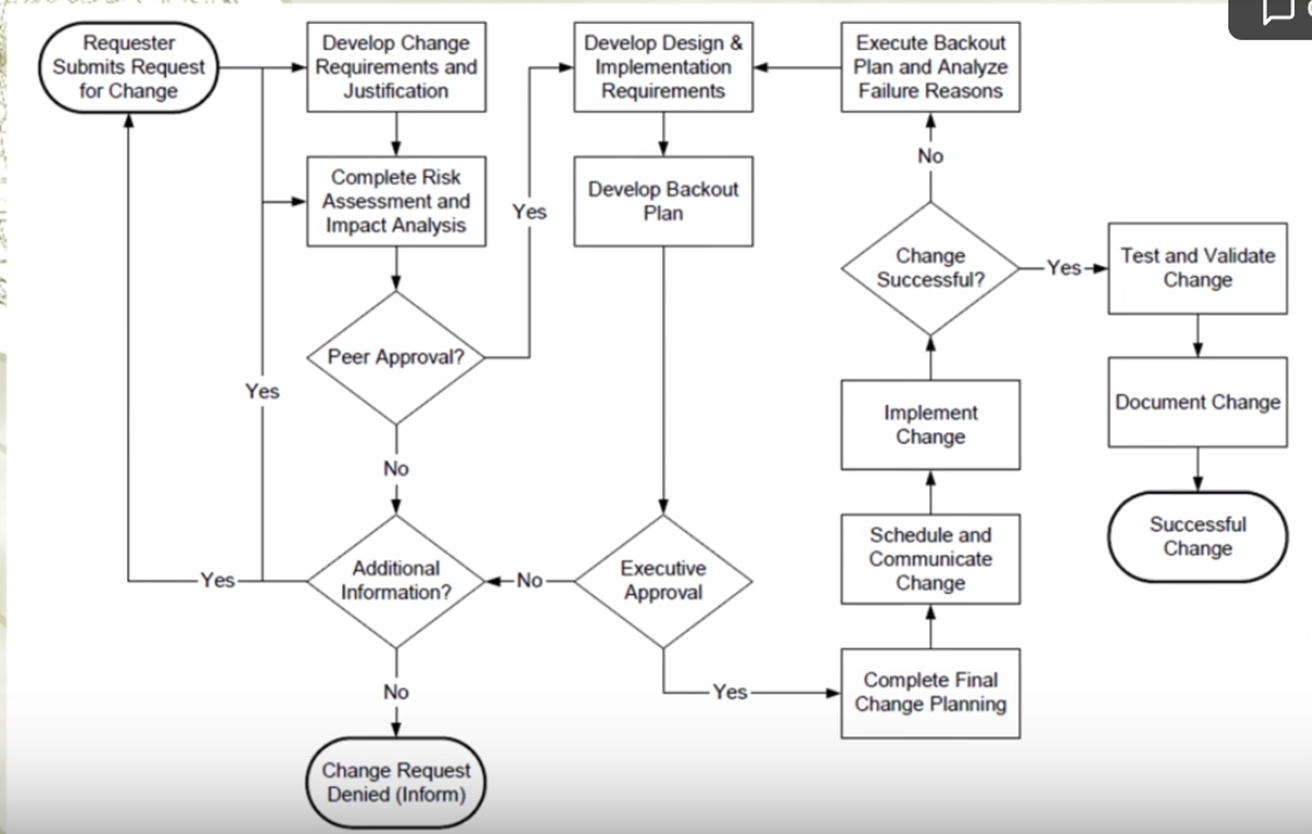
1. **Validation:** The change is validated by the operations staff to ensure that the intended machines received the deployment package. The security staff performs a security scan or review of the affected machines to ensure that new vulnerabilities are not introduced. Changes should be included in the problem tracking system until operations has ensured that no problems have been introduced.

**验证:** 操作人员验证该变化，以确保预期的机器收到部署包。安全人员对受影响的机器进行安全扫描或审查，以确保没有引入新的漏洞。变更应包括在问题跟踪系统中，直到操作人员确保没有引入问题。

1. **Documentation:** The outcome of the system change, to include system modifications and lessons learned, should be recorded in the appropriate records. This is the way that change management typically interfaces with configuration management.

**文件:** 系统变更的结果，包括系统的修改和经验教训，应该记录在适当的记录中。这就是变更管理与配置管理的典型对接方式。

**Basic Change Management Workflow 基本变革管理工作流程**

****

**Change Review**

**变革回顾**

1. **Change Monitoring 变化监测**

* Checking the desired functionality 检查所需的功能
* Monitoring network, server, performance 监控网络、服务器、性能

**Importance of CM: 变化监测的重要性**

After a period of time, if a bug suddenly comes up, the organisation would still have to document the issue and escalate it.

一段时间后，如果突然出现了一个错误，该组织仍将不得不记录这个问题并将其升级。

**How:**

Different tools could be used to monitor these changes.

可以使用不同的工具来监测这些变化。

1. **Measuring success of the change: 衡量变革的成功:**

**Technical objectives:** whether the changes accomplishes everything that it is set to accomplish, and that there are no technical issues.

**技术目标：**变化是否完成了它所设定的所有目标，并且没有技术问题。

**Business objectives:** ensure that the changes that are made meet business objectives e.g. if it is set to increase productivity, ensure that is being met. Or if it is set to solve certain issues, whether that goal is being met.

**业务目标：**确保所做的改变符合业务目标，例如，如果它被设定为提高生产力，确保这一点正在得到满足。或者，如果它被设定为要解决某些问题，那么这个目标是否正在实现。

1. **Change Management Assessment 变革管理评估**

Assessing change management as a culture, whether it has been properly adhered to or whether the employees are not aware of it or accept the change management procedures. The organisation can run audits on the change management process to see if it is working.

评估变革管理作为一种文化，是否得到了适当的遵守，或者员工是否没有意识到或接受变革管理程序。组织可以对变革管理程序进行审计，看它是否有效。

1. **Business Continuity 业务连续性**

If any changes are made, business continuity plans should be maintained accordingly.

如果有任何变化，应相应地维护业务连续性计划。

**This policy applies to all parties operating within the company’s network environment or utilising Information Resources. It covers the data networks, LAN servers and personal computers (stand-alone or network-enabled), located at company offices and company production related locations, where these systems are under the jurisdiction and/or ownership of the company or subsidiaries, and any personal computers, laptops, mobile device and or servers authorised to access the company’s data networks. No employee is exempt from this policy.**

**In order to fulfil this policy, the following statements shall be adhered to:**

**Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.**

**Operational Procedures**

**操作程序**

**Operational Procedures**

**操作程序**

The change control process shall be formally **defined and documented**. A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures).

应正式**定义和记录**变更控制流程。应制定变更控制流程，以控制对公司所有关键信息资源（如硬件、软件、系统文件和操作程序）的变更。

This documented process shall **include management responsibilities and procedures**. Wherever practicable, operational and application change control procedures should be integrated.

这个文件化的过程应包括管理责任和程序。 在可行的情况下，操作和应用变更控制程序应被整合。

**What Change Management should include**

**变革管理应包括哪些内容**

**Should include (at the least) the following phases:**

**应包括（至少）以下阶段:**

1. Logged Change Requests; 记录的变更请求。
2. Identification, prioritization and initiation of change;

变更的识别、优先级和启动。

1. Proper authorisation of change; 变更的适当授权。
2. Requirements analysis; 需求分析
3. Inter-dependency and compliance analysis; 相互依赖性和合规性分析
4. Impact Assessment; 影响评估.
5. Change approach; 变更方法
6. Change testing; 变更测试
7. User acceptance testing and approval; 用户验收测试和批准
8. Implementation and release planning; 实施和发布计划
9. Documentation; 文件
10. Change monitoring; 变更监测
11. Defined responsibilities and authorities of all users and IT personnel;

界定所有用户和IT人员的责任和权限

1. Emergency change classification parameters. 紧急变更分类参数

**Documented Change**

**记录的变化**

**All change requests shall be logged 所有的变更请求都应记录在案**

whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented.

无论是批准还是拒绝，都要在一个标准化的中央系统中进行。所有变更请求的批准及其结果都应被记录下来。

**Documented audit trail 文件化的审计跟踪**

A documented audit trail, **maintained at a Business Unit Level**, containing relevant information shall be maintained at all times. This should **include change request documentation, change authorisation and the outcome of the change.** No single person should be able to effect changes to production information systems without the approval of other authorised personnel.

应**在业务单位层面保持**一个包含相关信息的文件化审计跟踪，并一直保持。 这应**包括变更请求文件、变更授权和变更结果**。 未经其他授权人员的批准，任何一个人都不能对生产信息系统进行更改。

**Risk Management**

**风险管理**

* A risk assessment shall be performed for all changes and dependant on the outcome.

对所有的变化都应进行风险评估，并视结果而定。

* An impact assessment should be performed.

应进行影响评估。

* The impact assessment should include

影响评估应包括

* the potential effect on other information resources

对其他信息资源的潜在影响

* potential cost implications.

潜在的成本影响。

* consider compliance with legislative requirements and standards.

考虑是否符合立法要求和标准。

**Change Classification**

**变化分类**

All change requests shall be prioritised in terms of

所有的变更请求都应按以下方面进行优先排序

* benefits, 效益
* urgency, 迫切性
* effort required 所需的努力
* potential impact on operations. 对业务的潜在影响

**SLA’s (Service Level Agreements)**

**SLA（服务水平协议）**

**Changes affecting SLA‘s 影响服务水平协议的变化**

The impact of change on existing SLA’s shall be considered. Where applicable, changes to the SLA shall be controlled through a formal change process which includes contractual amendments.

应考虑变化对现有服务级协议的影响。在适用的情况下，对服务级协议的变更应通过正式的变更程序加以控制，其中包括合同的修订。

**Version Control**

**版本控制**

Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.

任何软件的改变和/或更新都应通过版本控制来控制。较旧的版本应根据公司的保留和存储管理政策予以保留。

**Testing**

**测试**

Changes shall be tested in an i**solated, controlled, and representative environment** (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.

在实施之前，应在一个隔离的、受控的和有代表性的环境中对变更进行测试（如果这种环境是可行的），以尽量减少对相关业务流程的影响，评估其对操作和安全的影响，并验证只进行了预期的和经批准的变更。

**Approval**

**审批**

All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed and proposed changes were tested.

所有的变更在实施前都应得到批准。变更的批准应基于正式的验收标准，即变更请求是由授权的用户完成的，影响评估已经执行，拟议的变更已经测试。

**Communicating changes (and involve the users!)**

**沟通变化（并让用户参与！）**

All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.

所有受变化影响的用户都应被告知该变化。 用户代表应签收该变更。在接受变更之前，应要求用户提出意见和评论。

**Implementation**

**实施**

Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes.

只有在经过适当的测试和利益相关者的批准后，才会进行实施。所有的重大变化都应被视为新系统的实施，并应被确立为一个项目。重大变化将根据开发和实施上述变化所需的努力来分类。

**Fall back**

**回落**

Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.

应记录中止和从不成功的变更中恢复的程序。如果变更的结果与预期的结果不同（如变更测试中所确定的），应注意受影响地区的恢复和连续性的程序和责任。回归程序将被落实到位，以确保系统能够恢复到实施变更之前的状态。

**Documentation**

**文件**

Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.

信息资源文件应在每次变更完成后进行更新，旧的文件应按照文件和数据保留政策归档或处理。

Information resources documentation is used for reference purposes in various scenarios i.e. further development of existing information resources as well as ensuring adequate knowledge transfer in the event of the original developer and/or development house being unavailable. It is therefore imperative that information resources documentation is complete, accurate and kept up to date with the latest changes. Policies and procedures, affected by software changes, shall be updated on completion of each change.

信息资源文件在各种情况下被用于参考目的，即进一步开发现有的信息资源，以及确保在原始开发者和/或开发公司无法使用的情况下进行充分的知识转移。 因此，信息资源文件必须完整、准确，并保持最新的变化。受软件变更影响的政策和程序，应在每次变更完成后进行更新。

**Business Continuity Plans (BCP)**

**业务连续性计划**

Business continuity plans shall be updated with relevant changes, managed through the change control process. Business continuity plans rely on the completeness, accuracy and availability of BCP documentation. BCP documentation is the road map used to minimise disruption to critical business processes where possible, and to facilitate their rapid recovery in the event of disasters.

业务连续性计划应根据相关的变化进行更新，通过变更控制程序进行管理。业务连续性计划依赖于BCP文件的完整性、准确性和可用性。 BCP文件是用于尽可能减少关键业务流程中断的路线图，并在发生灾难时促进其迅速恢复。

**Emergency Changes**

**紧急变化**

Specific procedures to ensure the proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.

确保适当控制、授权和记录紧急变更的具体程序应到位。具体的参数将被定义为标准，以便将变化归为紧急变化。

**Change Monitoring**

**变化监测**

All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

所有的变化一旦被推广到生产环境中，将被监控。与设计规格和测试结果的偏差将被记录下来，并上报给解决方案所有者批准。

**Roles and responsibilities (From highest rank to lowest)**

**角色和责任(从最高等级到最低等级)**

**Members of the Board 董事会成员**

* Members of the Board shall ensure that the necessary information security controls are implemented and complied with as per this policy.

董事会成员应确保根据本政策实施和遵守必要的信息安全控制。

**Information Security Manager 信息安全经理**

* Establish and revise the information security strategy, policy and standards for change management and control with input from interest groups and subsidiaries;

利用利益集团和子公司的意见，建立和修订信息安全战略、政策和变革管理和控制标准。

* Facilitate and coordinate the necessary counter measures to change management and control initiatives and evaluate such policies and standards;

促进和协调必要的应对措施，以改变管理和控制举措，并评估此类政策和标准。

* Establish the security requirements for change management and control directives and approval of the change management and control standards and change control/ version control products;

建立变更管理和控制指令的安全要求，批准变更管理和控制标准以及变更控制/版本控制产品。

* Co-ordinate the overall communication and awareness strategy for change management;

协调变革管理的整体沟通和认识战略。

* Acts as the management champion for change management and control;

担任变革管理和控制的管理负责人。

* Provide technical input to the service requirements and co-ordinate affected changes to SLA’s where applicable.

为服务要求提供技术投入，并在适用的情况下协调对服务水平协议的影响变化。

* Establish and co-ordinate appropriate interest group forums to represent, feedback, implement and monitor change management and control initiatives;

建立和协调适当的利益集团论坛，以代表、反馈、实施和监测变革管理和控制举措

* Coordinate the implementation of new or additional security controls for change management.

协调实施新的或额外的安全控制措施，以促进变革管理。

**Operations Manager 业务经理**

* Implement, maintain and update the change management and control strategy, baselines, standards, policies and procedures with input from all stakeholders;

利用所有利益相关者的意见，实施、维护和更新变革管理和控制战略、基线、标准、政策和程序。

* Approve and authorise change management and control measures on behalf of the <Organisation>;

代表<组织>批准和授权变更管理和控制措施。

* Ensure that all application owners are aware of the applicable policies, standards, procedures and guidelines for change management and control;

确保所有的应用程序拥有者都了解适用的政策、标准、程序和变更管理和控制的准则。

* Ensure that policy, standards and procedural changes are communicated to applicable owners and management forums;

确保政策、标准和程序的变化被传达给适用的业主和管理论坛。

* Appoint the necessary representation to the interest groups and other forums created by each company for Information Security Management relating to change management and control;

任命必要的代表参加各公司为信息安全管理创建的与变革管理和控制有关的兴趣小组和其他论坛。

* Establish and revise the information security strategy, policy and standards for change management and control;

建立和修订信息安全战略、政策和变革管理与控制标准。

* Facilitate and co-ordinate the necessary change management and control initiatives within each company;

促进和协调各公司内部必要的变革管理和控制举措。

* Report and evaluate changes to change management and control policies and standards;

报告并评估变更管理和控制政策及标准的变化。

* Co-ordinate the overall communication and awareness strategy for change management and control;

协调变革管理和控制的整体沟通和认识战略。

* Co-ordinate the implementation of new or additional security controls for change management and control

协调新的或额外的安全控制措施的实施，以促进变化管理和控制

* Review the effectiveness of change management and control strategy and implement remedial controls where deficits are identified;

审查变革管理和控制战略的有效性，并在发现缺陷时实施补救性控制。

* Provide regular updates on change management and control initiatives and the suitable application;

定期提供关于变革管理和控制举措的最新信息以及合适的应用。

* Evaluate and recommend changes to change management/ version control solutions;

评估并建议修改变更管理/版本控制解决方案。

* Co-ordinate awareness strategies and rollouts to effectively communicate change management and control mitigation solutions in each company.

协调宣传战略和推广工作，以便在每个公司有效地传达变革管理和控制缓解方案。

* Establish and implement the necessary standards and procedures that conform to the Information Security policy;

建立和实施符合信息安全政策的必要标准和程序。

* Responsible for approving, authorising, monitoring and enforcing change management initiatives and related security controls within all <ORGANISATION> companies and divisions;

负责批准、授权、监测和执行所有<ORGANISATION>公司和部门的变革管理举措和相关安全控制。

* Ensure that all solution owners are aware of policies, standards, procedures and guidelines for change management and control.

确保所有解决方案的拥有者都了解有关变更管理和控制的政策、标准、程序和准则。

* Ensure the compliance of this policy and report deviations to the Information Manager.

确保本政策得到遵守，并向信息经理报告偏差情况。

**IT Service Provider IT服务提供者**

* Shall comply with all change management and control statements of this policy.

应遵守本政策的所有变更管理和控制声明。

**Solution Owners 解决方案的拥有者**

* Shall comply with all information security policies, standards and procedures for change management and control;

应遵守所有关于变更管理和控制的信息安全政策、标准和程序。

* Report all deviations.

报告所有的偏差。

**IT Governance Value statement**

**IT治理价值声明**

Changes that materially affect the financial process must be evaluated and reported at some interval. Financial system upgrades or replacements will require new certification. The implication is that Sarbanes-Oxley compliance is reliant on the changes you make to the operational systems and procedures.

对财务流程有重大影响的变化必须在一定的时间间隔内进行评估和报告。财务系统的升级或替换将需要新的认证。其含义是，萨班斯-奥克斯利法案的合规性依赖于你对操作系统和程序的改变。

**Policy Access Considerations**

**政策访问的考虑因素**

All IT personnel 所有IT人员

Business Unit Management teams 业务单位管理团队

Executive Directors 执行董事

## Tutorial Week 7

Question 1

Risk analysis is an integral part of the process of developing a security system. What is risk analysis used for and how does it influence the overall security system?

Risk Management, Risk Assessment and Risk Analysis

Risk Management: Risk management is the overall management to manage risks. Risk Assessment is only part of risk management. Risk management also involves planning and monitoring/maintaining that are not covered in risk assessment.

Risk assessment: is part of risk management and is a framework to manage risk at a particular point in time.

Risk analysis is the actual step carried out to quantify impact, likelihood of different risk items in order to determine the risk levels and for making recommendations.

* Risk analysis is used primarily to identify the threats oto an organisation’s assets and to estimate the potential damage that ma need to be dealt with if any of the threats turned out to be real.
* For example, risk analysis may be used to determine what threats one needs to deal with when protecting a medical database and the cost associated with a case in which some patient records are accessed by unauthorised persons.

Question 2

An important step in risk analysis is to determine the value of an asset. Give five (5) different questions you think might help with the task of determining the asset value.

Questions:

How much is the cost to acquire

How much is the value of the asset to adversaries

How much is the price others are willing to pay for the assets.

Other questions:

* Cost to acquire or develop the asset
* Cost to maintain and protect the asset
* Value of the asset to owners and users
* Value of the asset to adversaries
* Price others are willing to pay fo the asset
* Cost to replace the asset if lost
* Operational and production activities affected if the asset is unavailablie
* Liability issues if the asset is compromised
* Usefulness and role of the asset in the organisation

Question 3

Give two (2) examples of intangible assets and explain why it is often more difficult to determine the value of an intangible asset than a tangible one.

Eg. Rep and data

Hard to quantify values of intangible assets which may change over time.

Tangible: eg. computers, harddrive and facilities

Assets may be tangible(computers, facilities, supplies) or intangible (reputation, data, intellectual property). It is usually harder to quantify the values of intangible assets, which may change overtime. How do you put a monetary value on a company’s reputation? This is not always an easy question to answer, but it is important to do so.

Question 4

A backup data centre is located in a remote area. It has been determined that in the event of a severe cyclone, which happened twice in the last 40 years, the backup data centre suffers 50% damage. The cost to rebuild the centre is currently $1 million. What is the single loss expectancy for the centre suffering from such a severe cyclone? What is the annualised loss expectancy? If the insurance premium for such events is $10,000 per annum, would it be wise to consider insuring the centre to address the risk? Explain your reasoning.

SLE = asset value x exposure factor

SLE is the loss that you experience to the asset due to the event, in this case is 1mil, therefore (1mil x 50%) , SLE = 500k

ALE = SLE x ARO

500k x (2/40) = 10k

Since, 10k<25k, lt is wise to pay an insurance premium of $10,000 to cover a potential damage of $25,000 from a cost-benefit perspective.

Other possible answer:

Last 40 years - Twice (Very ambiguous)

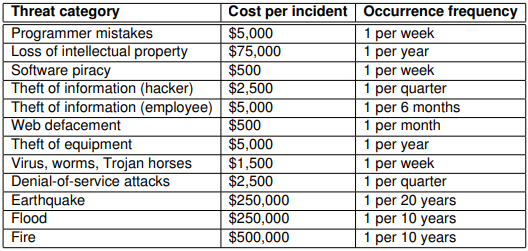
1 year -> (1/40)\*(2) = 0.5% (Exposure Factor)

SLE -> 500k

ALE = 500k x (1/20) = 25k (May be fixed or minimum or maximum)

Question 5

Consider the following risk analysis of a software company

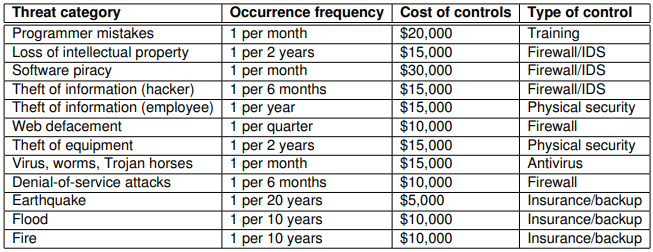


Calculate the SLE, ARO, and ALE for each threat category listed in the above table.

• How did the software company arrive at the values shown in the table?

• Assume that the company has implemented controls to address the risk shown in the analysis

and the new figures after one year are shown below. Assume that the cost per incident figures are still the same. Recalculate SLE, ARO, and ALE values for each category. Comment on the results.



SLE = Cost of the Incident x 1 (for all because it only takes into account one incident and the overall frequency for all is 1)

ARO

1. 52 = 1 x 52weeks
2. 1

ALE

1. $260 000= 52 x $5000

If ALE after is the same or more than the ALE before, the control is not effective

Answer:

| Threat Category | Cost/Incident  ($) | Occurence freq. | SLE | ARO | ALE |
| --- | --- | --- | --- | --- | --- |
| Programmer mistakes | 5,000 | 1 per week | 5,000 | 52.0 | 260,000 |
| Loss of intellectual property | 75,000 | 1 per year | 75,000 | 1.0 | 75,000 |
| Software piracy | 500 | 1 per week | 500 | 52.0 | 26,000 |
| Theft of information (hacker) | 2,500 | 1 per quarter | 2,500 | 4.0 | 10,000 |
| Theft of information (employee) | 5,000 | 1 per 6 months | 5,000 | 2.0 | 10,000 |
| Web defacement | 500 | 1 per month | 500 | 12.0 | 6,000 |
| Theft of equipment | 5,000 | 1 per year | 5,000 | 1.0 | 5,000 |
| Virus, worms, Trojan horses | 1,500 | 1 per week | 1,500 | 52.0 | 78,000 |
| Denial-of-service attacks | 2,500 | 1 per quarter | 2,500 | 4.0 | 10,000 |
| Earthquakes | 250,000 | 1 per 20 years | 250,000 | 0.05 | 12,500 |
| Flood | 250,000 | 1 per 10 years | 250,000 | 0.1 | 25,000 |
| Fire | 500,000 | 1 per 10 years | 500,000 | 0.1 | 50,000 |

The company may subjectively evaluate the cost per incident, and may have record of previous incidents to estimate frequency. Estimates from other sources may also be available.

Except for insured items (fully cover the damage), SLE generally does not change even when new controls are put in place, only ARO and ALE change.

| Threat category | SLE | ARO | ALE  (After) | ALE (before) | CC | Y/N |
| --- | --- | --- | --- | --- | --- | --- |
| Programmer mistakes | $5.000 | 12 | $60,000 | $260,000 | $20,000 | Y |
| Loss of intellectual property | $75,000 | 0.5 | $37,500 | $75,000 | $15,000 | Y |
| Software piracy | $500 | 12 | $6,000 | $26,000 | $30,000 | N |
| Theft of information (hacker) | $2,500 | 2 | $5,000 | $10,000 | $15,000 | N |
| Theft of information (employee) | $5,000 | 1 | $5,000 | $10,000 | $15,000 | N |
| Web defacement | $500 | 4 | $2,000 | $6,000 | $10,000 | N |
| Theft of equipment | $5,000 | 0.5 | $2,500 | $5,000 | $15,000 | N |
| Virus, worms, Trojan horses | $1,500 | 12 | $18,000 | $78,000 | $15,000 | Y |
| Denial-of-service attacks | $2,500 | 2 | $5,000 | $10,000 | $10,000 | N |
| Earthquakes | $0 | 0.05 | $0 | $12,500 | $5,000 | Y |
| Flood | $0 | 0.1 | $0 | $25,000 | $10,000 | Y |
| Fire | $0 | 0.1 | $0 | $50,000 | $10,000 | Y |

Question 6

A recent security audit at an organisation has revealed that the processor of an important internal server has a critical design flaw that could be exploited to reveal confidential system information. This is a hardware vulnerability and there are no current fixes. It is also determined that it is not cost effective to upgrade to a new server and the current server must continue its operation to serve users within the organisation. The organisation needs to address this particular risk immediately. Identify two (2) strategies that can be used to address the risk. For each strategy, give an example and briefly explain how it helps.

Transfer risk

Eg. Purchase insurance : Insurance provider pay for the damage if there are damage

Accept the risk

Shld know what will happen assuming the cost of the asset outweighs the risk and the benefits

Mitigate the risk

Put controls on the risk, put

Early detection and response

Create incident response plan to deal with such an attack

Answer:

It is not expected that Prevent or Avoid strategies can be used because of the constraints.

* Strategy 1 : Mitigate the risk. Monitor the server and ask users to monitor their accounts for any suspected activity so early detection and response can be performed. Encrypt user data and perform frequent backup to prevent data from being stolen or damaged. Create incident response plan to deal with such an attack.
* Strategy 2 : Accept the risk. This strategy accepts the risk, knowing that it could happen - assume that the cost much outweighs the benefits.
* Strategy 3: Transfer the risk. This means transfer the risk to another organisation. The simplest form being purchasing insurance. If there is any damage caused by such an attack, the insurance provider will pay the damage.

Question 7

List and briefly describe five sections which are usually found in a policy.

Choose four from the following:

* Purpose: Explains the reason for the policy
* Related documents: Lists any documents (or other policy) that affect the contents of this policy
* Cancellation: Identifies any existing policy that is cancelled when this policy becomes effective.
* Background: Provides amplifying information on the need for the policy
* Scope: States the range of coverage for the policy (to whom or what does the policy apply)
* Policy statement: Identifies the actual guiding principles or what is to be done
* Action: Specifies what actions are necessary and when they are to be accomplished
* Responsibility: States who is responsible for what
* Ownership: Identifies who sponsored the policy and from whom it derives its authority, as well as defines who may change the policy.

Question 8

Describe an example wherein unmanaged changes to IT systems and networks can increase risk to enterprises. Describe how the risk can be minimized if changes are managed carefully.

**Example**

1. Remote access to the internal server - opens the firewall port, introduces unauthorised hackers to also gain access to internal server remotely

**How**

1. Impl change management process whereby approval has to be granted by the superior before the firewall administrator can open the firewall port to allow access to the internal server. Only when he is granted access to open the access to the internal server, the firewall administrator should also monitor traffic from remote to internal server to make sure that the traffic is legitimate and not suspicious.

Question 9

Describe how you would measure the success of a change management program?

Compare the outcomes vs expectations the organisation has ( eg on time, on budget, meats tech and busin or human obj)

Answer

This is an open question: One obvious approach is to compare the delivered outcomes and the expectations before the change.

Some other examples can also include:

* Installation: It is on time
* Installation: It is on budget
* Installation: It meets the technical objective
* Implementation: The business objectives are met
* Implementation: The human objectives are met

Question 10

What are basic elements that you can expect to see in a change management and control policy. Briefly describe each of them.

Change Management is the discipline of understanding, adjusting and adapting to a new normal after an enterprise transformation.

Change control is the process of how changes to requirements are sourced, analyzed, managed, and included in the roadmap and implementation schedule.

Change Management is about molding hearts and minds. Change Control is about governing the requirements management.

Change Management is about not letting investment into a transformation come to naught. Change Control is about not letting the requirements runaway train derail a project or a program.

Change Management may or may not involve technology involvement. Change Control is a part of the overall IT enablement realm.

Change Management could impact an entire company. Typically, Change Control is about a specific project and a set of requirements.

Question 11

Using the quantitative risk assessment approach, a software company is assessing the risk due to programmer mistakes which happen five (5) times every four (4) weeks on average and cause a damage of $10,000 per incident.

* Calculate the current SLE, ARO and ALE values.
* The company is considering two possible controls described below to address this risk. Using the cost-benefit analysis (CBA) approach, derive the SLE, ARO, ALE, ACS and CBA values for each case and state clearly which control should be selected to address the risk due to the programmer mistakes.
* Control A (training staff) costs $150,000 per annum and reduces the frequency of mistakes to one (1) every fortnight.
* Control B (smart backup and version control) costs $100,000 per annum and reduces the damage to $5,000 per incident.
* Current values
* SLE = $10,000
* ARO = 52 x 5/4 = 65
* ALE = 65 x $10,000 = $260,000
* Control A
* SLE = $10,000
* ARO = 52 x ½ = 26
* ALE = 26 x $10,000 = $260,000
* ACS = $150,000
* CBA = $650,000 - $260,000 - $150,000 = $240,000
* Control B
* SLE = $5,000
* ARO = 65
* ALE = 65 x $5,000 = $325,000
* ACS = $100,000
* CBA = $650,000 - $325,000 - $100,000 = $225,000
* Conclusion: Control A should be selected because iths CBA is better than that of Control B by $15,000

Question 12

Describe an example wherein unmanaged changes to IT systems and networks can increase risk to enterprises. Describe how the risk can be minimised if changes are managed carefully.

Take for example, a team of developers that has just written a much better looking and easier to use version of the organisation’s website. The only problem is that it cant be tested by the remote QA team because the firewall is blocking access. Waiting for change management approval could take weeks, so as the firewall admin, it may be very tempting to want to help out the development team by temporarily opening a port on the firewall. Sadly, we’ve all seen some variation of how that story ends: a worm or Trojan is introduced onto the internal network, a sniffer is planted on a server and credentials are stolen, or a previously protected database is exposed to attackers.

Question 13

Explain the differences between the two roles in a change management process: Change Manager vs Change Coordinator

* Hierarchy: as far as the hierarchy is concerned, Change Manager sits above Change Coordinator, Change Manager actually appoints Change Coordinatior(s). There could be multiple Change Coordinators for multiple business IT units, each looking after their own area. However, usually there is only one Change Manager.
* Responsibilities: Change Manager has the overall responsibility for the organisation and acts at a high level. A Change Coordinator on the other hand is usually appointed for a particular change, and “responsible for planning and coordinating all of the phases of the change from initiation through acceptance and documentation” . Change Coordinators will provide updates to Change Manager on a regular basis. That is to say that Change Coordinators assist Change Manager.

## Week 8: Business Continuity Planning II

### Business Continuity Planning 业务连续性规划

#### Definition:

Business continuity planning (BCP) is a process designed to reduce the organisation’s business risk arising from an unexpected disruption of the critical functions/operations (manual or automated) necessary for the survival of the organisation.

业务连续性计划（BCP）是一个过程，旨在减少组织生存所需的关键功能/操作（手动或自动）意外中断而产生的业务风险。

#### BCP purposes:

* Reduce business risks

减少商业风险

* Make sure that any disruptions and losses due to the incidents or disasters are minimised

确保最大限度地减少由于事件或灾难造成的任何干扰和损失。

### Disaster Recovery Planning 灾难恢复计划

*DRP purposes:* (part of RBCP) aka Contingency Plans

DRP目的：（RBCP的一部分）又称应急计划

* Coordinating recovery after a disaster

协调灾难后的恢复工作

* Often referred to as restoring information system and operational facilities after a disaster.

通常被称为在灾难发生后恢复信息系统和操作设施。

A disaster recovery plan should have at least the following components:

灾难恢复计划至少应包括以下内容。

* recovery coordinator

恢复协调人

* recovery team

恢复小组

* recovery analysis and planning

恢复分析和规划

* damage assessment and salvage operations

损害评估和打捞行动

* recovery communications

恢复通讯

* employee support and assistance.

雇员支持和协助

Preparing for an emergency typically involves:

紧急情况的准备工作通常包括

* Planning

规划

* Practising

练习

* Rehearsing

排练

* Evaluating

评估

* Adjusting

调整

#### Requirements

There should be well documented procedures, strategies etc. This requires setting up an Emergency Response Team and inclusion of that information in BCP.

应该有完善的程序和战略等文件。这需要建立一个应急小组，并将这些信息纳入BCP

Team should have general and local responsibilities.

团队应该有总体和局部的责任

They should for example facilitate evacuation and shut down, protect companies properties and potentially cooperate with local authorities such as fire department.

例如，他们应该为疏散和关闭提供便利，保护公司财产，并可能与消防部门等地方当局合作

Depending on the type of disasters, there could be different plans.

根据灾害的类型，可能有不同的计划。

### Disasters 灾难

Definition:

Disasters are disruptions that cause critical information resources to be inoperative for a period of time, adversely impacting business operations.

灾害是指导致关键信息资源在一段时间内无法使用，对业务运营产生不利影响的干扰。

There are three classifications of threats that can cause disasters:

有三种分类的威胁可以造成灾难：

* Natural 自然灾害
* earthquakes, floods, tornados, severe thunderstorms and fire etc.

地震、洪水、龙卷风、强雷暴和火灾等。

* Environmental 环境灾害
* Power shortages, staff shortages, unavailability resources, electrical power, telecommunications, equipment failure and software error etc.

电力短缺、人员短缺、无法获得资源、电力、电信、设备故障和软件错误等。

* Human 人为灾害
* operator error, terrorist attacks, hacker attacks or viruses etc.

操作员错误、恐怖袭击、黑客攻击或病毒等。

### BCP Process

The business continuity planning process can be divided into the following lifecycle phases:

业务连续性规划过程可分为以下生命周期阶段：

1. *Develop the continuity planning policy statement.* Write a policy that provides the guidance necessary to develop a BCP, and that assigns authority to the necessary roles to carry out these tasks.

制定连续性规划政策声明。编写一份政策，为制定BCP提供必要的指导，并将权力分配给必要的角色来执行这些任务。

1. *Conduct the business impact analysis (BIA)*. Identify critical functions and systems and allow the organization to prioritize them based on necessity. Identify vulnerabilities and threats, and calculate risks.

进行业务影响分析（BIA）。识别关键功能和系统，让组织根据必要性确定其优先次序。识别脆弱性和威胁，并计算风险。

1. *Identify preventive controls.* Once threats are recognized, identify and implement controls and countermeasures to reduce the organization’s risk level in an economical manner.

确定预防控制措施。一旦认识到威胁，确定并实施控制和对策，以经济的方式降低组织的风险水平。

1. *Develop recovery strategies.* Formulate methods to ensure systems and critical functions can be brought online quickly.

制定恢复战略。制定方法以确保系统和关键功能能够快速上线。

1. *Develop the contingency plan.* Write procedures and guidelines for how the organization can still stay functional in a crippled state.

制定应急计划。为组织如何在瘫痪的状态下仍能保持运作写出程序和准则。

1. *Test the plan and conduct training and exercises.* Test the plan to identify deficiencies in the BCP, and conduct training to properly prepare individuals on their expected tasks.

测试计划并进行培训和演习。测试计划以确定BCP中的不足之处，并进行培训，使个人对其预期的任务有适当的准备。

1. *Maintain the plan.* Put in place steps to ensure the BCP is a living document that is updated regularly.

维护该计划。采取措施，确保BCP是一份定期更新的活文件。

### Initiation Process of BCP | BCP before carrying out过程

The BCP effort has to result in a sustainable, long-term program that serves its purpose—assisting the organization in the event of a disaster. The effort must be well thought out and methodically executed. It must not be perceived as a mere “public relations” effort to make it simply appear that the organization is concerned about disaster response. The **initiation process** for BCP might include the following:

BCP的努力必须产生一个可持续的、长期的计划，以达到其目的--在发生灾难时帮助组织。这项工作必须经过深思熟虑并有条不紊地执行。它不能被看作是一种单纯的 "公共关系 "努力，让人觉得该组织对灾难反应很关注。BCP的**启动过程**可能包括以下内容。

* Setting up a budget and staff for the program before the BCP process begins. Dedicated personnel and dedicated hours are essential for executing something as labor-intensive as a BCP.

在BCP进程开始之前，为该计划设定预算和人员。专门的人员和专门的时间对于执行像BCP这样的劳动密集型项目是必不可少的。

* Setting up the program would include assigning duties and responsibilities to the BCP coordinator and to representatives from all of the functional units of the organization.

建立该计划将包括向BCP协调员和组织所有职能单位的代表分配职责和责任。

* Senior management should kick off the BCP with a formal announcement or, better still, an organization-wide meeting to demonstrate high-level support. Awareness-raising activities to let employees know about the BCP program and to build internal support for it.

高级管理层应该以正式宣布的方式启动BCP，或者最好是召开一次全组织的会议，以表明高层的支持。开展提高认识的活动，让员工了解BCP计划，并为其建立内部支持。

* Establishment of skills training for the support of the BCP effort.

建立支持BCP工作的技能培训。

* The start of data collection from throughout the organization to aid in crafting various continuity options.

开始从整个组织收集数据，以帮助制定各种连续性的方案。

* Putting into effect “quick wins” and gathering of “low-hanging fruit” to show tangible evidence of improvement in the organization’s readiness, as well as improving readiness.

将 "速赢 "付诸实施，并收集 "低垂的果实"，以显示组织准备情况改善的切实证据，以及改善准备情况。

### Business Impact Analysis 业务影响分析

Business Impact Analysis is assisting the design of our contingency which is assuming that bad things will happen. BIA is in the Preparedness stage.

业务影响分析正在协助我们的应急设计，这是假设坏事会发生。BIA处于准备阶段。

Risk Management includes controls that help the organisation prevent bad things from happening. Risk Management is in the Prevention stage.

风险管理包括帮助组织防止坏事发生的控制措施。风险管理处于预防阶段。

*Three steps* are typically involved in accomplishing the BIA:

在完成BIA的过程中，通常涉及三个步骤：

1. Determine mission/business processes and recovery criticality.

确定任务/业务流程和恢复的关键性。

Definition: Mission/Business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum time that an organization can tolerate while still maintaining the mission.

确定系统支持的任务/业务流程，确定系统中断对这些流程的影响，以及中断的影响和估计的停机时间。停机时间应反映一个组织在维持任务的同时所能容忍的最大时间。

1. Identify resource requirements.

确定资源需求

Definition: Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible.

Examples: of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.

现实的恢复工作需要对尽快恢复任务/业务流程和相关的相互依存关系所需的资源进行全面评估。应该确定的资源例子包括设施、人员、设备、软件、数据文件、系统组件和重要记录。

1. Identify recovery priorities for system resources.

确定系统资源的恢复重点

Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Priority levels can be established for sequencing recovery activities and resources. **Evaluate the impact of ceasing to perform these activities and identify priorities/ assign priorities**

根据前面活动的结果，系统资源可以更明确地与关键任务/业务流程和功能联系起来。可以为恢复活动和资源的排序建立优先级别。**评估停止执行这些活动的影响，并确定优先次序/分配优先次序**

1. Identify an acceptable level of loss may pertain to recovery criticality (recovery parameters)

确定一个可接受的损失水平，可能与恢复的关键性有关（恢复参数）

The ISCP Coordinator should next analyze the supported mission/business processes and with the process owners, leadership and business managers determine the acceptable downtime if a given process or specific system data were disrupted or otherwise unavailable. Downtime can be identified in several ways.

ISCP协调员接下来应该分析所支持的任务/业务流程，并与流程所有者、领导层和业务经理一起确定在特定流程或特定系统数据被中断或无法使用时可接受的停机时间。停机时间可以通过几种方式确定。

* **Maximum Tolerable Downtime (MTD) 最大可容忍的停机时间**. The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.
* MTD代表了系统所有者/授权官员愿意接受的任务/业务流程中断或扰乱的总时间，包括所有影响因素。确定MTD是很重要的，因为它可能会给应急计划人员留下不精确的方向：（1）选择一个适当的恢复方法，（2）在制定恢复程序时需要的细节深度，包括其范围和内容。
* **Recovery Time Objective (RTO) 恢复时间目标.** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD. When it is not feasible to immediately meet the RTO and the MTD is inflexible, a Plan of Action and Milestone should be initiated to document the situation and plan for its mitigation.

RTO定义了在对其他系统资源、支持的任务/业务流程和MTD产生不可接受的影响之前，一个系统资源可以保持不可用的最大时间量。确定信息系统资源的RTO对于选择最适合满足MTD的适当技术非常重要。当立即满足RTO是不可行的，并且MTD是不灵活的，应该启动一个行动计划和里程碑，以记录这种情况并计划其缓解。

* **Recovery Point Objective (RPO) 恢复时间点目标.** The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process.

RPO表示在中断或系统中断之前，任务/业务流程数据在中断后可以恢复的时间点（鉴于数据的最新备份副本）。与RTO不同，RPO不是作为MTD的一部分来考虑的。相反，它是任务/业务流程在恢复过程中可以容忍多少数据损失的一个因素。

Because the RTO must ensure that the MTD is not exceeded, the RTO must normally be shorter than the MTD. For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD.

因为RTO必须确保不超过MTD，RTO通常必须比MTD短。例如，系统故障可能会阻止一个特定的过程完成，由于重新处理数据需要时间，所以必须在RTO中加入额外的处理时间，以保持在MTD规定的时限内。

***<Recovery Parameters>***

### Maximum tolerable downtime (MTD) 可容忍的最大停机时间

Definition:

Outage time that can be tolerated by the company as a result of various unfortunate events

由于各种不幸的事件，公司可以容忍的停工时间

The BIA identifies which of the company’s critical systems are needed for survival and estimates the outage time that can be tolerated by the company as a result of various unfortunate events.

The outage time that can be endured by a company is referred to as the maximum tolerable downtime (MTD) or maximum period time of disruption (MPTD)

BIA确定了公司的哪些关键系统是需要生存的，并估计了公司因各种不幸事件而可以容忍的停工时间。公司可以忍受的停工时间被称为最大可容忍的停工时间（MTD）或最大中断时间（MPTD）

The following are some MTD estimates that an organization may use. Note that these are sample estimates that will vary from organization to organization and from business unit to business unit:

以下是一个组织可以使用的一些MTD估算。请注意，这些是样本估计，在不同的组织和不同的业务单位会有所不同。

* **Nonessential 非必要的** 30 days
* **Normal 通常** 7 days
* **Important 重要的** 72 hours
* **Urgent 紧急的** 24 hours
* **Critical 关键的** Minutes to hours

Each business function and asset should be placed in one of these categories, depending upon how long the company can survive without it. These estimates will help the company determine what backup solutions are necessary to ensure the availability of these resources. The shorter the MTD, the higher priority of recovery for the function in question. Thus, the items classified as Urgent should be addressed before those classified as Normal.

每项业务功能和资产都应该被归入其中一个类别，这取决于公司在没有它的情况下可以生存多久。这些估计将帮助公司确定哪些备份解决方案是必要的，以确保这些资源的可用性。MTD越短，有关功能恢复的优先级就越高。因此，归类为紧急的项目应该在归类为正常的项目之前解决。

#### Examples

* For example, if being without a T1 communication line for three hours would cost the company $130,000, the T1 line could be considered Critical and thus the company should put in a backup T1 line from a different carrier.
* If a server going down and being unavailable for ten days will only cost the company $250 in revenue, this would fall into the Normal category, and thus the company may not need to have a fully redundant server waiting to be swapped out. Instead, the company may choose to count on its vendor’s service level agreement (SLA), which may promise to have it back online in eight days.

例如，如果没有T1通信线路三小时会使公司损失130,000美元，那么这条T1线路可能被认为是关键的，因此公司应该从不同的运营商那里投入一条备份的T1线路。如果一台服务器发生故障并在10天内无法使用，只会使公司损失250美元的收入，这将属于正常类别，因此公司可能不需要有一个完全冗余的服务器等待被替换掉。相反，该公司可以选择依靠其供应商的服务水平协议（SLA），它可能承诺在8天内恢复在线。

* Sometimes the MTD will depend in large measure on the type of business in question. For instance, a call center—a vital link to current and prospective clients—will have a short MTD, perhaps measured in minutes instead of weeks. A common solution is to split up the calls through multiple call centers placed in differing locales. If one call center is knocked out of service, the other one can temporarily pick up the load. Manufacturing can be handled in various ways. Examples include subcontracting the making of products to an outside vendor, manufacturing at multiple sites, and warehousing an extra supply of products to fill gaps in supply in case of disruptions to normal manufacturing.

有时，MTD将在很大程度上取决于有关业务的类型。 例如，一个呼叫中心--与当前和潜在客户的重要联系--将有一个很短的MTD，也许是以分钟而不是以星期来衡量。一个常见的解决方案是通过放置在不同地点的多个呼叫中心来分担电话。如果一个呼叫中心停止服务，另一个呼叫中心就可以暂时接替它。制造业可以用各种方式处理。例如，将产品的生产分包给外部供应商，在多个地点进行生产，以及在正常生产中断的情况下储存额外的产品供应以填补供应缺口。

### The recovery point objective (RPO) 恢复点的目标

#### Definition:

Determined based on the acceptable data loss in case of disruption of operations. It indicates the earliest point in time to which it is acceptable to recover the data.

根据业务中断情况下可接受的数据损失来确定。它表明可以接受恢复数据的最早时间点。

The Recovery Point Objective (RPO) is the acceptable amount of data loss measured in time. This value represents the earliest point in time at which data must be recovered. The higher the value of data, the more funds or other resources that can be put into place to ensure a smaller amount of data is lost in the event of a disaster.

恢复点目标（RPO）是以时间衡量的可接受的数据损失量。这个值代表了数据必须被恢复的最早时间点。数据的价值越高，可以投入更多的资金或其他资源，以确保在灾难发生时损失较少的数据。

### The recovery time objective (RTO) 恢复时间的目标

#### Definition:

Determined based on the acceptable downtime in case of a disruption of operations. It indicates the earliest point in time at which the business operations must resume after disaster.

根据业务中断时可接受的停机时间来确定。它表明灾难发生后，业务运作必须恢复的最早时间点。

* The Recovery Time Objective (RTO) is the earliest time period and a service level within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in business continuity.

恢复时间目标（RTO）是指灾难发生后必须恢复业务流程的最早时间段和服务水平，以避免与业务连续性中断有关的不可接受的后果。

* The RTO value is smaller than the MTD value, because the MTD value represents the time after which an inability to recover significant operations will mean severe and perhaps irreparable damage to the organization’s reputation or bottom line.

RTO值比MTD值要小，因为MTD值代表的是无法恢复重要业务的时间，在这之后将意味着对组织的声誉或底线造成严重的、也许是不可弥补的损害。

* The RTO assumes that there is a period of acceptable downtime. This means that a company can be out of production for a certain period of time (RTO) and still get back on its feet. But if the company cannot get production up and running within the MTD window, the company is sinking too fast to properly recover.

RTO假设有一段可接受的停工期。这意味着公司可以在一定时间内停产（RTO），仍然可以恢复正常。但如果公司不能在MTD窗口内恢复生产，公司就会沉沦得太快，无法正常恢复。

### Work Recovery Time 工作恢复时间

#### Definition:

The Work Recovery Time (WRT) is the remainder of the overall MTD value. RTO usually deals with getting the infrastructure and systems back up and running, and WRT deals with restoring data, testing processes, and then making everything “live” for production purposes.

工作恢复时间（WRT）是整个MTD值的剩余部分。RTO通常是指让基础设施和系统恢复运行，而WRT是指恢复数据、测试流程，然后让一切 "活 "起来用于生产。

—-------------------------------------------------------------------------------------------------------------------------------------

Both RPO and RTO are based on time parameters. **The lower the time requirements, the higher the cost of recovery strategies.**

RPO和RTO都是基于时间参数的。**时间要求越低，恢复策略的成本就越高。**

* If the RPO is in minutes (lowest possible acceptable data loss) then data mirroring should be implemented as the recovery strategy.

如果RPO是以分钟为单位（可接受的最低数据损失），那么应该实施数据镜像作为恢复策略。

* If the RTO is less, then the alternate site might be preferred over a hot-site contract.

如果RTO较少，那么备用站点可能比热站点合同更受欢迎。

* The lower the RTO, the lower the disaster tolerance. Disaster tolerance is a time gap within which the business can accept the non-availability of IT facilities.

RTO越低，灾难容忍度越低。灾难容忍度是一个时间差，在这个时间差内，企业可以接受IT设施的不可用性。

### Examples of Recovery Parameters 恢复参数的例子

The RTO, RPO, and WRT values are critical to understand because they will be the basic foundational metrics used when determining the type of recovery solutions a company must put into place, so let’s dig a bit deeper into them.

RTO、RPO和WRT值的理解至关重要，因为它们将是在确定公司必须投入的恢复解决方案类型时使用的基本基础指标，所以让我们更深入地挖掘它们。

* RTO is the duration of time and a service level that a business process must be restored to in order to ensure that unacceptable consequences associated with a disaster are not endured.

RTO是指业务流程必须恢复到的时间长度和服务水平，以确保不承受与灾难有关的不可接受的后果。

* Let’s say a company has determined that if it is unable to process product order requests for 12 hours, the financial hit will be too large for it to survive. So the company develops methods to ensure that orders can be processed manually if their automated technological solutions become unavailable. But if it takes the company 24 hours to actually stand up the manual processes, the company could be in a place operationally and financially where it can never fully recover. So RTO deals with “how long do we have to get everything up and working again?”

比方说，一家公司已经确定，如果它在12小时内无法处理产品订单请求，那么财务上的打击将是巨大的，它将无法生存。因此，该公司开发了一些方法，以确保在其自动化技术解决方案不可用的情况下，可以手动处理订单。但是，如果该公司需要24小时才能真正建立起人工流程，那么该公司在运营和财务上就可能处于一个永远无法完全恢复的状态。因此，RTO处理的是 "我们要在多长时间内让一切重新开始工作？"

* Now let’s say that the same company experienced a disaster and got its manual processes up and running within two hours, so it met the RTO requirement.

现在我们说，同一家公司经历了一场灾难，并在两小时内恢复了人工流程的运行，所以它满足了RTO的要求。

* But just because business processes are back in place, we still might have a critical problem.

但是，仅仅因为业务流程已经恢复到位，我们仍然可能有一个关键问题。

* The company has to restore the data it lost during the disaster. It does no good to restore data that is a week old. The employees need to have access to the data that was being processed right before the disaster hit.

公司必须恢复它在灾难中丢失的数据。恢复一周前的数据是没有用的。员工需要访问灾难发生前正在处理的数据。

* If the company can only restore data that is a week old, then all the orders that were in some stage of being fulfilled over the last seven days could be lost. If the company makes an average of $25,000 per day in orders and all the order data was lost for the last seven days, this can result in a loss of $175,000 and a lot of unhappy customers. So just getting things up and running (RTO) is part of the picture. Getting the necessary data in place so that business processes are up to date and relevant (RPO) is just as critical.

如果公司只能恢复一周前的数据，那么过去七天内处于某种阶段的所有订单都可能丢失。如果公司平均每天的订单量为25,000美元，而过去七天的所有订单数据都丢失了，这可能导致17.5万美元的损失和大量不满意的客户。因此，只是让事情启动和运行（RTO）是其中的一部分。获得必要的数据，使业务流程是最新的和相关的（RPO），也同样关键。

The actual MTD, RTO, and RPO values are derived during the BIA. The impact analysis is carried out to be able to apply criticality values to specific business functions, resources, and data types.

实际的MTD、RTO和RPO值是在BIA期间得出的。进行影响分析是为了能够对特定的业务功能、资源和数据类型应用临界值。

* The company must have data restoration capabilities in place to ensure that mission-critical data is never older than one minute. The company cannot rely on something as slow as backup tape restoration, but must have a high-availability data replication solution in place.

公司必须具备数据恢复能力，以确保关键任务的数据永远不会超过1分钟。公司不能依赖像备份磁带那样缓慢的恢复，而是必须有一个高可用性的数据复制解决方案。

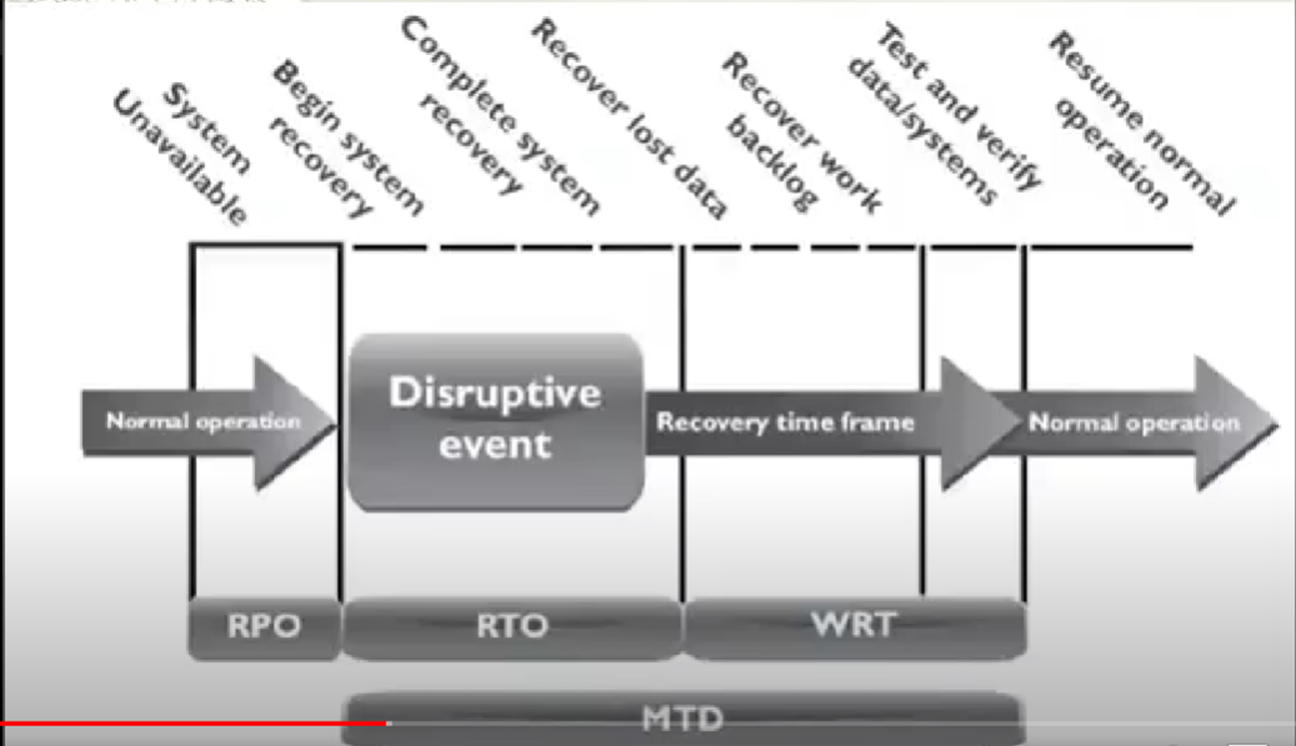
* The RTO value for mission-critical data processing is two minutes or less. This means that the technology that carries out the processing functionality for this type of data cannot be down for more than two minutes.

任务关键型数据处理的RTO值是两分钟或更少。这意味着执行这类数据的处理功能的技术不能停机超过两分钟。

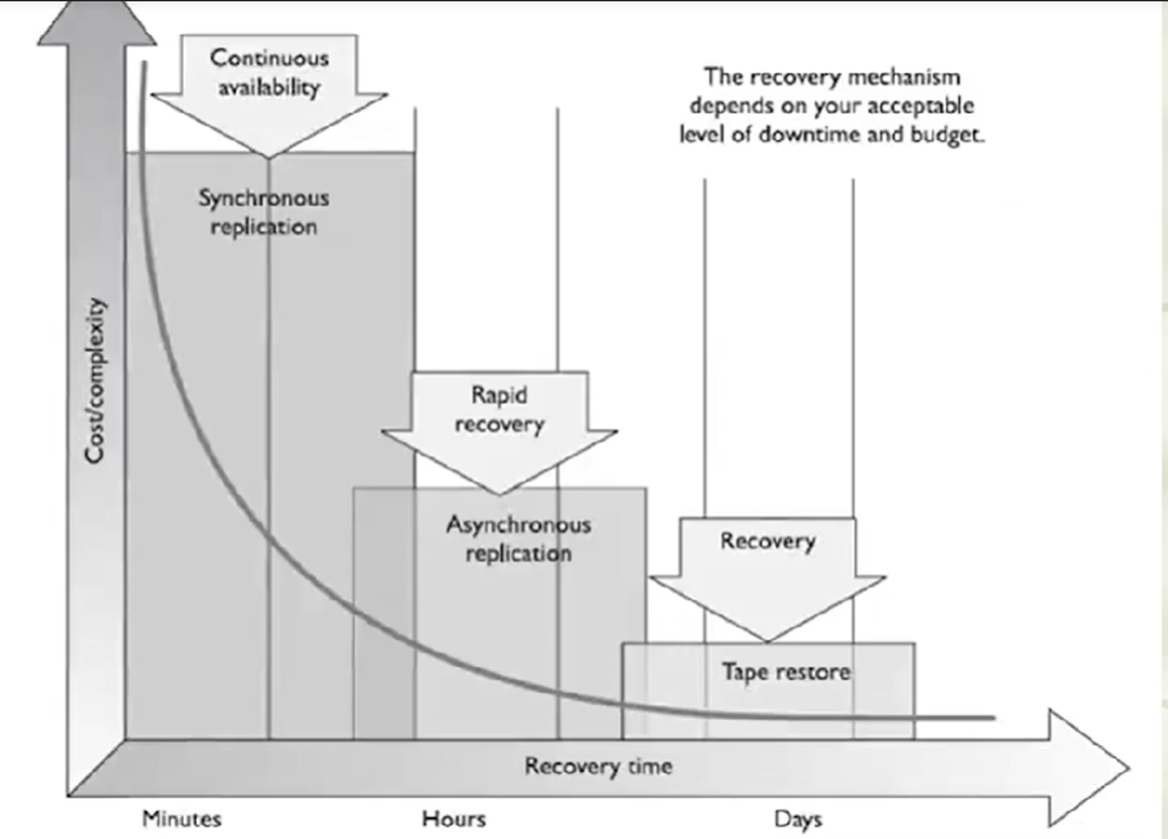
* The company may choose to have a cluster technology in place that will shift the load once it notices that a server goes offline.

公司可能会选择有一个集群技术，一旦发现有服务器离线，就会转移负载。

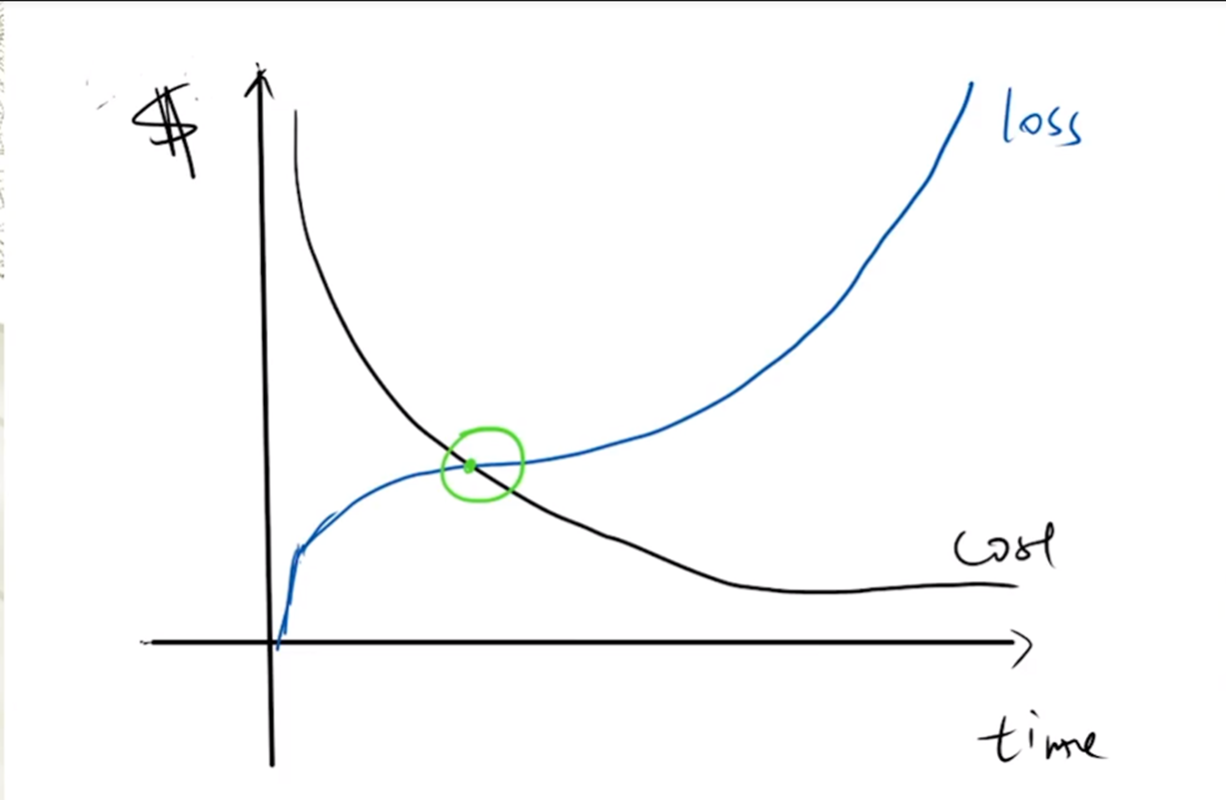
### Recovery Parameters Timeline 恢复参数时间表



### Recover Time over Complexity of Method 恢复时间超过方法的复杂性



### Optimum time to set RPO, MTD and RTO 设定RPO、MTD和RTO的最佳时间

****

* Cost of recovering is more than the cost of loss with every unit of time that passes before the Optimum time. The method may not be worth its price.

在最佳时间之前，每过一个单位的时间，恢复的成本就会超过损失的成本。该方法可能不值得它的价格。

* Cost of loss is more than the cost of recovery with every unit of time that passes after the Optimum time. Loss due to damage is too high.

在最佳时间之后，每过一个单位的时间，损失的成本就会超过恢复的成本。损害造成的损失太高。

### Offsite Facilities (related to RTO) 场外设施（与RTO有关）

#### Alternate Processing Facilities 替代处理设施

* Hot sites
* Warm sites
* Cold sites
* Mobile sites
* Reciprocal agreements 互惠协议

Importance of offsite facilities: For larger disasters that affect the primary facility, an offsite backup facility must be accessible.

对于影响主要设施的较大灾害，必须有一个异地的备份设施可以使用。

(How) Generally, contracts are established with third-party vendors to provide such services. The client pays a monthly fee to retain the right to use the facility in a time of need, and then incurs an activation fee when the facility actually has to be used.

一般来说，与第三方供应商签订合同以提供此类服务。客户每月支付费用以保留在需要时使用该设施的权利，然后在实际需要使用该设施时产生激活费。

In addition, there would be a daily or hourly fee imposed for the duration of the stay. This is why subscription services for backup facilities should be considered a short-term solution, not a long-term solution.

此外，还将在停留期间征收每日或每小时的费用。这就是为什么备份设施的订阅服务应被视为短期解决方案，而不是长期解决方案。

It is important to note that most recovery site contracts do not promise to house the company in need at a specific location, but rather promise to provide what has been contracted for somewhere within the company’s locale.

FYI: On, and subsequent to, September 11, 2001, many organizations with Manhattan offices were surprised when they were redirected by their backup site vendor not to sites located in New Jersey (which were already full), but rather to sites located in Boston, Chicago, or Atlanta. This adds yet another level of complexity to the recovery process, specifically the logistics of transporting people and equipment to unplanned locations.

值得注意的是，大多数恢复站点合同并不承诺将有需要的公司安置在某一特定地点，而是承诺在公司所在地的某个地方提供合同规定的内容。在2001年9月11日及其后，许多在曼哈顿设有办事处的组织惊讶地发现，他们的备份站点供应商没有把他们转到位于新泽西的站点（那里已经满员），而是转到位于波士顿、芝加哥或亚特兰大的站点。这给恢复过程增加了另一个层次的复杂性，特别是将人员和设备运送到计划外地点的物流。

**Companies can choose from three main types of leased or rented offsite facilities:**

#### 公司可以从三种主要的租赁或租用的场外设施中进行选择：

##### Hot site

* A facility that is leased or rented and is fully configured and ready to operate within a few hours.

一个租赁或租用的设施，在几小时内就能完全配置好并准备好运作。

* The only missing resources from a hot site are usually the data, which will be retrieved from a backup site, and the people who will be processing the data.

热站点唯一缺少的资源通常是数据，这些数据将从备份站点检索，以及处理数据的人员。

* The equipment and system software must absolutely be compatible with the data being restored from the main site and must not cause any negative interoperability issues.

设备和系统软件必须绝对与从主站点恢复的数据兼容，并且不能造成任何负面的互操作性问题。

* Some facilities, for a fee, store data backups close to the hot site. These sites are a good choice for a company that needs to ensure a site will be available for it as soon as possible.

一些设施，在收费的情况下，将数据备份储存在靠近热点网站的地方。对于需要确保尽快为其提供站点的公司来说，这些站点是一个不错的选择。

* Most hot-site facilities support annual tests that can be done by the company to ensure the site is functioning in the necessary state of readiness.

大多数热站点设施支持年度测试，可由公司进行，以确保站点在必要的准备状态下运行。

* This is the most expensive of the three types of offsite facilities. It can pose problems if a company requires proprietary or unusual hardware or software.

这是三种类型的场外设施中最昂贵的一种。如果一个公司需要专有或不寻常的硬件或软件，它可能会带来问题。

##### Warm site

* A leased or rented facility that is usually partially configured with some equipment, such as HVAC, and foundational infrastructure components, but not the actual computers.

租赁或租用的设施，通常部分配置了一些设备，如暖通空调，和基本的基础设施组件，但没有实际的计算机。

* In other words, a warm site is usually a hot site without the expensive equipment such as communication equipment and servers.

换句话说，一个温暖的站点通常是一个没有昂贵设备如通信设备和服务器的热站点。

* Staging a facility with duplicate hardware and computers configured for immediate operation is extremely expensive, so a warm site provides an alternate facility with some peripheral devices.

用重复的硬件和计算机配置成立即运行的设施进行分期是非常昂贵的，因此，一个温暖的站点提供了一个带有一些外围设备的备用设施。

* (Why companies use warm sites more often) This is the most widely used model. It is less expensive than a hot site, and can be up and running within a reasonably acceptable time period. **It may be a better choice for companies that depend upon proprietary and unusual hardware and software**, because they will bring their own hardware and software with them to the site after the disaster hits. Drawbacks, however, are that much of the equipment has to be procured, delivered to, and configured at the warm site after the fact, and the annual testing available with hot-site contracts is not usually available with warm-site contracts. Thus, a company cannot be certain that it will in fact be able to return to an operating state within hours.

这是最广泛使用的模式。它比热站点的成本低，并且可以在一个合理的可接受的时间段内启动和运行。**对于那些依赖专有和不寻常的硬件和软件的公司来说，这可能是一个更好的选择**，因为他们会在灾难发生后把自己的硬件和软件带到现场。然而，缺点是许多设备必须在事后采购、运送和配置到温暖站点，而且热站点合同所提供的年度测试通常并不适用温暖站点合同。因此，一个公司不能确定它实际上能够在几小时内恢复到运行状态。

##### Cold site

* A leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services.

租赁或租用的设施，提供基本环境、电线、空调、管道和地板，但不提供设备或附加服务。

* A cold site is essentially an empty data center.

冷门网站基本上是一个空的数据中心。

* It may take weeks to get the site activated and ready for work.

可能需要几周时间来激活网站并准备工作。

* The cold site could have equipment racks and dark fiber (fiber that does not have the circuit engaged) and maybe even desks. However, it would require the receipt of equipment from the client, since it does not provide any.

冷站点可以有设备机架和暗光纤（没有参与电路的光纤），甚至可能有办公桌。然而，它需要从客户那里接收设备，因为它不提供任何设备。

* **(Advantages vs Disadvantages)** The cold site is the least expensive option, but takes the most time and effort to actually get up and functioning right after a disaster, as the systems and software must be delivered, tweaked, and configured.

(优势与劣势）冷站是最便宜的选择，但在灾难发生后需要花费最多的时间和精力来实际启动和运行，因为系统和软件必须被交付、调整和配置。

* (**When is it used)** Cold sites are often used as backups for call centers, manufacturing plants, and other services that can be moved lock, stock, and barrel in one shot.

冷门网站通常被用作呼叫中心、制造厂和其他可以一次性移动的服务的备份。

#### Conclusion

Most companies use warm sites, which have some devices such as disk drives, tape drives, and controllers, but very little else.

大多数公司使用温暖的站点，这些站点有一些设备，如磁盘驱动器、磁带驱动器和控制器，但其他设备很少。

(Why they dont use a hot site) These companies usually cannot afford a hot site, and the extra downtime would not be considered detrimental.

这些公司通常负担不起一个热门网站，而且额外的停机时间也不会被认为是有害的。

A warm site can provide a longer-term solution than a hot site. Companies that decide to go with a cold site must be able to be out of operation for a week or two. The cold site usually includes power, raised flooring, climate control, and wiring.

与热站点相比，暖站点可以提供一个更长期的解决方案。决定采用冷场地的公司必须能够停业一周或两周。冷场地通常包括电源、高架地板、气候控制和布线。

### Quick overview of the differences between offsite facilities:

**以下是对场外设施的区别的快速概述：**

#### Hot Site Advantages

* Ready within hours for operation 几小时内即可投入使用
* Highly available 高度可用的
* Usually used for short-term solutions, but available for longer stays

通常用于短期解决方案，但可用于较长时间的停留

* Annual testing available 可进行年度测试

#### Hot Site Disadvantages

* Very expensive 非常昂贵
* Limited on hardware and software choices

在硬件和软件选择上受到限制

#### Warm and Cold Site Advantages

* Less expensive 价格较低
* Available for longer timeframes because of the reduced costs

由于成本降低，可用于更长的时间范围

* Practical for proprietary (def/ relating to an owner or ownership.) hardware or software use

适用于专有硬件或软件的使用

#### Warm and Cold Site Disadvantages

* Operational testing not usually available

通常不提供操作测试

* Resources for operations not immediately available

无法立即获得的行动资源

#### Tertiary Sites 第三级网站

* During the BIA phase, the team may recognize the danger of the primary backup facility not being available when needed, which could require a tertiary site.

在BIA阶段，团队可能会认识到主要备用设施在需要时无法使用的危险，这可能需要一个第三级站点。

* This is a secondary backup site, just in case the primary backup site is unavailable. The secondary backup site is sometimes referred to as a “backup to the backup.” This is basically plan B if plan A does not work out.

这是一个次要的备份站点，以备主要备份站点不可用。二级备份站点有时被称为 "备份的备份"。这基本上是B计划，如果A计划不成功。

#### Reciprocal Agreements 互惠协议

* Another approach to alternate offsite facilities is to establish a reciprocal agreement with another company, usually one in a similar field or that that has similar technological infrastructure.

另一种备用场外设施的方法是与另一家公司建立互惠协议，通常是类似领域的公司或拥有类似技术基础设施的公司。

* This means that company A agrees to allow company B to use its facilities if company B is hit by a disaster, and vice versa. This is a cheaper way to go than the other offsite choices, but it is not always the best choice. Most environments are maxed out pertaining to the use of facility space, resources, and computing capability.

这意味着A公司同意在B公司遭受灾难时允许B公司使用其设施，反之亦然。这是一种比其他异地选择更便宜的方式，但它并不总是最佳选择。大多数环境在设施空间、资源和计算能力的使用方面已经达到了极限。

* To allow another company to come in and work out of the same shop could prove to be detrimental to both companies. Whether it can assist the other company while tending effectively to its own business is an open question. The stress of two companies working in the same environment could cause tremendous levels of tension.

允许另一家公司进入并在同一商店工作，可能证明对两家公司都不利。它是否能在有效处理自己业务的同时协助另一家公司，是一个有待解决的问题。两家公司在同一环境中工作的压力可能会造成巨大的紧张。

* If it did work out, it would only provide a short-term solution. Configuration management could be a nightmare. Does the other company upgrade to new technology and retire old systems and software? If not, one company’s systems may become incompatible with that of the other company?

如果真的成功了，它也只能提供一个短期的解决方案。配置管理可能是一场恶梦。另一家公司是否会升级到新技术并退役旧系统和软件？如果没有，一家公司的系统可能会与另一家公司的系统不兼容？

### Important issues need to be addressed before a disaster hits if a company decides to participate in a reciprocal agreement with another company:

**如果一家公司决定参加与另一家公司的互惠协议，需要在灾难发生前解决一些重要问题：**

* How long will the facility be available to the company in need?

有需要的公司可以使用多长时间的设施？

* How much assistance will the staff supply in integrating the two environments and ongoing support?

在整合两种环境和持续支持方面，工作人员将提供多少援助？

* How quickly can the company in need move into the facility?

有需要的公司能多快地迁入该设施？

* What are the issues pertaining to interoperability?

与互操作性有关的问题是什么？

* How many of the resources will be available to the company in need?

有多少资源可以提供给有需要的公司？

* How will differences and conflicts be addressed?

将如何解决分歧和冲突？

* How does change control and configuration management take place?

变更控制和配置管理是如何进行的？

* How often can drills and testing take place?

演习和测试可以多长时间进行一次？

* How can critical assets of both companies be properly protected?

如何妥善保护两家公司的关键资产？

### Offsite Location 场外地点

Rules:

* When choosing a backup facility, it should be far enough away from the original site so that one disaster does not take out both locations. In other words, it is not logical to have the backup site only a few miles away if the company is concerned about tornado damage, because the backup site could also be affected or destroyed.

当选择一个备份设施时，它应该离原址足够远，这样，一场灾难就不会使两个地点都被摧毁。换句话说，如果公司担心龙卷风的破坏，将备份地点设在几英里之外是不符合逻辑的，因为备份地点也可能受到影响或被摧毁

* There is a rule of thumb that suggests that alternate facilities should be, at a bare minimum, at least 5 miles away from the primary site, while 15 miles is recommended for most low-to-medium critical environments, and 50 to 200 miles is recommended for critical operations to give maximum protection in cases of regional disasters.

有一个经验法则表明，备用设施至少应距离主站点5英里，而对于大多数中低度关键环境，建议15英里，对于关键业务，建议50至200英里，以便在发生区域性灾害时提供最大保护。

### Redundant Sites 冗余站点

* Some companies choose to have redundant sites, or mirrored sites, meaning one site is equipped and configured exactly like the primary site, which serves as a redundant environment.

一些公司选择拥有冗余站点，或镜像站点，即一个站点的设备和配置与主站点完全一样，作为一个冗余环境。

* The business-processing capabilities between the two sites can be completely synchronized. These sites are owned by the company and are mirrors of the original production environment.

两个站点之间的业务处理能力可以完全同步。这些站点由公司拥有，是原始生产环境的镜像。

* A redundant site has clear **advantages**: it has full availability, is ready to go at a moment’s notice, and is under the organization’s complete control.

冗余站点有明显的优势：它有充分的可用性，在接到通知后随时可以使用，并且在组织的完全控制之下。

* **Disadvantage:** This is, however, one of the most expensive backup facility options, because a full environment must be maintained even though it usually is not used for regular production activities until after a disaster takes place that triggers the relocation of services to the redundant site.

然而，这是最昂贵的备份设施选项之一，因为必须保持一个完整的环境，即使它通常不用于正常的生产活动，直到灾难发生后，触发了服务搬迁到冗余站点。

* But expensive is relative here. If the company would lose a million dollars if it were out of business for just a few hours, the loss potential would override the cost of this option. Many organizations are subjected to regulations that dictate they must have redundant sites in place, so expense is not an issue in these situations.

但这里的昂贵是相对的。如果该公司只是停业几个小时就会损失一百万美元，那么潜在的损失就会超过这个选项的成本。许多组织受到法规的约束，规定他们必须有冗余的站点，所以在这些情况下，费用不是问题。

### Contingency Plans 应急计划( Discovery Recovery Planning: DRP)

#### Supporting information & Appendices 支持性资料和附录

1. Business impact analysis 业务影响分析
2. Emergency contacts 紧急联系人
3. Recovery procedures 恢复程序

#### Main phases 主要阶段

1. Activation and notification 激活和通知
2. Recovery 恢复
3. Reconstitution 重组

There are five main components of the information system contingency plan (ISCP). The supporting information and plan appendices provide essential information to ensure a comprehensive plan. The Activation and Notification, Recovery, and Reconstitution Phases address specific actions that the organization should take following a system disruption or emergency.

信息系统应急计划（ISCP）有五个主要组成部分。支持信息和计划附录提供了基本信息，以确保一个全面的计划。激活和通知、恢复和重建阶段涉及组织在系统中断或紧急情况下应采取的具体行动。

#### Supporting information and Appendices 支持性资料和附录

* (What it includes) The supporting information component includes an **introduction and concept of operations section** providing essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain.

支持性信息部分包括**导言和行动概念部分**，提供基本的背景信息，使应急计划更容易理解、实施和维护。

* (What for) These details **aid in** understanding the applicability of the guidance, in making decisions on how to use the plan, and in providing information on where associated plans and information outside the scope of the plan may be found.

这些细节**有助于**理解指南的适用性，有助于就如何使用该计划做出决定，并提供关于在哪里可以找到该计划范围之外的相关计划和信息的信息。

* (What it includes) This section may contain the **roles and responsibilities** section and presents the overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams.

本节可包含**角色和责任**部分，并介绍应急小组的整体结构，包括各小组之间的等级和协调机制及要求。

* (What for) The section also provides an overview of team member roles and responsibilities in a contingency situation. Teams and team members should be designated for specific response and recovery roles during contingency plan activation.

本节还概述了小组成员在应急情况下的角色和责任。在应急计划启动期间，应指定小组和小组成员承担具体的反应和恢复作用。

#### Activation and Notification Phase 激活和通知阶段

* The Activation and Notification Phase defines initial actions taken once a system disruption or outage has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the plan.

激活和通知阶段定义了一旦发现或似乎即将发生系统破坏或中断时采取的初步行动。这个阶段包括通知恢复人员、进行故障评估和启动计划等活动。

* At the completion of the Activation and Notification Phase, ISCP staff will be prepared to perform recovery measures to restore system functions.

在启动和通知阶段完成后，ISCP工作人员将准备执行恢复措施，以恢复系统功能。

* **Activation criteria**: The ISCP should be activated if one or more of the activation criteria for that system are met. If an activation criterion is met, the designated authority should activate the plan
* **激活标准:** 如果满足该系统的一个或多个激活标准，就应该激活ISCP。如果满足了启动标准，指定机构应启动该计划
* **Notification procedures**: An outage or disruption may occur with or without prior notice.

**通知程序:** 停电或中断可能在事先通知或不通知的情况下发生。

For **example**, advance notice is often given that a hurricane is predicted to affect an area or that a computer virus is expected on a certain date. However, there may be no notice of equipment failure or a criminal act.

例如，通常会提前通知，预测飓风将影响某个地区，或预计在某个日期会出现计算机病毒。然而，对于设备故障或犯罪行为，可能没有通知。

Notification procedures should be documented in the plan for both types of situation.

在计划中应记录这两类情况的通知程序。

(How) The procedures should describe the methods used to notify recovery personnel during business and non business hours.

该程序应描述在工作和非工作时间内通知恢复人员的方法。

(Why) Prompt notification is important for reducing the effects of a disruption on the system; in some cases, it may provide enough time to allow system personnel to shut down the system gracefully to avoid a hard crash.

及时通知对于减少中断对系统的影响非常重要；在某些情况下，它可能提供足够的时间让系统人员优雅地关闭系统以避免硬崩溃。

(How) Following the outage or disruption, notification should be sent to the Outage Assessment Team so that it may determine the status of the situation and appropriate next steps.

在停电或中断后，应向停电评估小组发出通知，以便确定情况的状况和适当的下一步措施。

When outage assessment is complete, the appropriate recovery and system support personnel should be notified.

当停电评估完成后，应通知适当的恢复和系统支持人员。

* **Outage assessment:** To determine how the ISCP will be implemented following a system disruption or outage, it is essential to assess the nature and extent of the disruption.

**停电评估:** 为了确定在系统中断或停机后如何实施ISCP，必须评估中断的性质和程度。

The outage assessment should be completed as quickly as the given conditions permit, with personnel safety remaining the highest priority. When possible, the Outage Assessment Team is the first team notified of the disruption.

停电评估应在给定条件允许的情况下尽快完成，人员安全仍然是最优先考虑的。在可能的情况下，停电评估小组是第一个接到中断通知的小组。

Once impact to the system has been determined, the appropriate teams should be notified of updated information and the planned response to the situation

一旦确定对系统的影响，应将最新的信息和计划的应对措施通知给适当的团队

#### Recovery Phase 恢复阶段

* Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location.

恢复阶段的活动重点是实施恢复战略，以恢复系统能力，修复损坏，并在原地或新的替代地点恢复运行能力。

* At the completion of the Recovery Phase, the information system will be functional and capable of performing the functions identified in the plan.

在恢复阶段完成后，信息系统将发挥作用，并能够执行计划中确定的功能。

* Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation at an alternate system, or relocation and recovery at an alternate site. It is feasible that only system resources identified as high priority in the BIA will be recovered at this stage.

根据计划中定义的恢复策略，这些功能可能包括临时手工处理，在备用系统中恢复和操作，或在备用地点搬迁和恢复。在这个阶段，只有在BIA中被确定为高优先级的系统资源才会被恢复，这是可行的。

* **Sequence of Recovery Activities:**

The sequence of activities should reflect the system’s MTD to avoid significant impacts to related systems.

**恢复活动的顺序:** 活动的顺序应反映系统的MTD，以避免对相关系统的重大影响。

Procedures should be written in a stepwise, sequential format so system components may be restored in a logical manner.

程序应以逐步、连续的格式编写，以便系统组件可以以合乎逻辑的方式进行恢复。

If conditions require the system to be recovered at an alternate site, certain materials will need to be transferred or procured.

如果条件要求在另一地点恢复系统，需要转移或采购某些材料。

These items may include shipment of data backup media from offsite storage, hardware, copies of the recovery plan, and software programs. Procedures should designate the appropriate team or team members to coordinate shipment of equipment, data, and vital records.

这些项目可能包括从异地存储的数据备份媒体、硬件、恢复计划的副本和软件程序的运输。程序应该指定适当的团队或团队成员来协调设备、数据和重要记录的运输。

References to applicable appendices, such as equipment lists or vendor contact information, should be made in the plan where necessary.

必要时应在计划中提及适用的附录，如设备清单或供应商联系信息。

Procedures should clearly describe requirements to package, transport, and purchase materials required to recover the system.

程序应清楚地描述包装、运输和购买恢复系统所需材料的要求。

* **Recovery Procedures:** To facilitate Recovery Phase operations, the ISCP should provide detailed procedures to restore the information system or components to a known state. Procedures should be assigned to the appropriate recovery team and typically address the following actions**:**

**恢复程序**: 为了促进恢复阶段的操作，ISCP应该提供详细的程序，将信息系统或组件恢复到一个已知的状态。程序应分配给适当的恢复小组，通常涉及以下行动。

1. Obtaining authorization to access damaged facilities and/or geographic area;

获得进入受损设施和/或地理区域的授权。

1. Notifying internal and external business partners associated with the system;

通知与系统相关的内部和外部业务伙伴。

1. Obtaining necessary office supplies and work space;

获得必要的办公用品和工作空间。

1. Obtaining and installing necessary hardware components;

获得并安装必要的硬件组件。

1. Obtaining and loading backup media;

获取和加载备份介质。

1. Restoring critical operating system and application software;

恢复关键的操作系统和应用软件。

1. Restoring system data to a known state;

将系统数据恢复到一个已知的状态。

1. Testing system functionality including security controls;

测试系统功能，包括安全控制。

1. Connecting system to network or other external systems;

将系统与网络或其他外部系统连接起来

1. Operating alternate equipment successfully.

成功操作备用设备。

Recovery procedures should be written in a straightforward, step-by-step style. To prevent difficulty or confusion in an emergency, no procedural steps should be assumed or omitted. A checklist format is useful for documenting the sequential recovery procedures and for troubleshooting problems if the system cannot be recovered properly.

恢复程序应以直截了当、循序渐进的方式编写。为了防止在紧急情况下出现困难或混乱，不应假设或省略任何程序步骤。核对表的格式对于记录连续的恢复程序和在系统不能正常恢复时排除故障是很有用的。

* **Recovery Escalation and Notification:** Effective escalation and notification procedures should define and describe the events, thresholds, or other types of triggers that are necessary for additional action.

**恢复升级和通知:** 有效的升级和通知程序应该定义和描述事件、阈值或其他类型的触发器，这是采取额外行动的必要条件。

Actions would include additional notifications for more recovery staff, messages and status updates to leadership, and notices for additional resources.

行动将包括对更多恢复人员的额外通知，给领导的信息和状态更新，以及额外资源的通知。

Procedures should be included to establish a clear set of events, actions and results, and should be documented for teams or individuals as appropriate.

应包括程序，以建立一套明确的事件、行动和结果，并应酌情为团队或个人记录。

#### 4. Reconstitution Phase 重组阶段

Definition: The Reconstitution Phase is the third and final phase of ISCP implementation and defines the actions taken to test and validate system capability and functionality.

重建阶段是ISCP实施的第三个也是最后一个阶段，定义了为测试和验证系统能力和功能所采取的行动。

What: During Reconstitution, recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements.

在重建过程中，恢复活动已经完成，正常的系统操作已经恢复。如果原来的设施无法恢复，这个阶段的活动也可以应用于准备一个新的永久地点来支持系统处理的要求。

How: This phase consists of two major activities: validating successful recovery and deactivation of the plan.

这个阶段包括两个主要活动：验证成功恢复和停用计划。

* **Validation of recovery typically includes these steps:**

**对恢复的验证通常包括这些步骤:**

* **Concurrent Processing.** Concurrent processing is the process of running a system at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly and securely.

**并行处理:** 并发处理是指在两个不同的地方同时运行一个系统，直到有一定程度的保证，恢复的系统正确和安全地运行。

* **Validation Data Testing.** Data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely and are current to the last available backup.

**验证数据测试:** 数据测试是对恢复的数据进行测试和验证的过程，以确保数据文件或数据库已被完全恢复，并与最后的可用备份保持一致。

* **Validation Functionality Testing.** Functionality testing is a process for verifying that all system functionality has been tested, and the system is ready to return to normal operations.

**验证功能测试:** 功能测试是一个验证所有系统功能都已测试完毕的过程，系统已准备好恢复正常运行。

At the successful completion of the validation testing, ISCP personnel will be prepared to declare that reconstitution efforts are complete and that the system is operating normally. The ISCP Coordinator must determine if the system has undergone significant change and will require reassessment and reauthorization.

在成功完成验证测试后，ISCP人员将准备宣布重建工作已经完成，系统运行正常。ISCP协调员必须确定该系统是否发生了重大变化，需要重新评估和重新授权。

* Deactivation of the plan is the process of returning the system to normal operations and finalizing reconstitution activities to prepare the system against another outage or disruption. These activities include:

计划的停用是使系统恢复正常运行的过程，并最终完成重建活动，使系统准备好应对另一次停电或中断。这些活动包括:

* **Notifications.** Upon return to normal operations, users should be notified by the ISCP Coordinator (or designee) using predefined notification procedures.

**通知。**在恢复正常运作后，ISCP协调员（或指定人员）应使用预定的通知程序通知用户。

* **Cleanup.** Cleanup is the process of cleaning up work space or dismantling any temporary recovery locations, restocking supplies, returning manuals or other documentation to their original locations, and readying the system for another contingency event.

**清理。**清理是清理工作空间或拆除任何临时恢复地点的过程，重新储存用品，将手册或其他文件放回原处，并为另一个应急事件做好系统准备。

* **Offsite Data Storage.** If offsite data storage is used, procedures should be documented for returning retrieved backup or installation media to its offsite data storage location.

**异地数据存储。**如果使用异地数据存储，应记录将检索到的备份或安装媒体返回其异地数据存储位置的程序。

* **Data Backup.** As soon as reasonable following reconstitution, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup should be stored with other system backups and comply with applicable security controls.

**数据备份。**在重建后的合理时间内，应尽快对系统进行全面备份，并存储当前运行系统的新副本，以备将来恢复工作之用。这个完整的备份应与其他系统备份一起存储，并遵守适用的安全控制。

* **Event Documentation.** All recovery and reconstitution events should be well documented, including actions taken and problems encountered during the recovery and reconstitution efforts.

**事件记录。**所有的恢复和重建事件都应该被很好地记录下来，包括在恢复和重建工作中采取的行动和遇到的问题。

An after-action report with lessons learned should be documented and included for updating the ISCP. Once all activities and steps have been completed and documentation has been updated, the ISCP can be formally deactivated. An announcement with the declaration should be sent to all business and technical contacts.

应记录下行动后的报告，并将其包括在更新ISCP的报告中，以总结经验教训。一旦所有的活动和步骤都已完成，文件也已更新，ISCP就可以正式停用了。应向所有的商业和技术联系人发送一份声明。

## Tutorial Week 8

Question 1

Explain the fundamental difference between business continuity planning (BCP) and disaster recovery planning (DRP).

解释业务连续性计划（BCP）和灾难恢复计划（DRP）的根本区别。

Students should consult lecture slides on BCP to recognise that DRP is a sub-component of BCP (BCP consists of: BIA, COOP + DRP, Testing, and Maintenance). BCP is a process designed to reduce the organizations business risk arising from and unexpected disruption of the critical functions/operations (manual or automated) necessary for the survival of the organization, whilst DRP typically details the process IT personal still follow to restore the computer system and the operational facilities after a disaster

学生应该参考BCP的讲座幻灯片，认识到DRP是BCP的一个子组成部分（BCP包括：BIA、COOP+DRP、测试和维护）。BCP是一个过程，旨在减少组织生存所需的关键功能/操作（手动或自动）的意外中断所带来的业务风险，而DRP通常详细说明IT个人在灾难发生后恢复计算机系统和操作设施的过程。

Question 2

What is business impact analysis (BIA), and what is it used for?

什么是业务影响分析（BIA），它的用途是什么？

The BIA is the first phase of BCP. A crucial component of the initial planning stages, it serves as an investigation and assessment of the impact that various event can have on the organization. It includes:

BIA是BCP的第一个阶段。作为初始规划阶段的一个重要组成部分，它是对各种事件可能对组织产生的影响的调查和评估。它包括:

* Determine core business processes and recover criticality

确定核心业务流程和恢复的关键性

* Identify resource requirements

确定资源需求

* Identify recover priorities for system resources

确定系统资源的恢复优先级

Question 3

What is the fundamental difference between BIA and risk assessment?

BIA和风险评估之间的根本区别是什么？

Risk management focuses on identifying threats, vulnerabilities, and attacks in order to determine controls that can protect data. BIA on the other hand assumes that these controls have FAILED/BY-PASSED/INEFFECTIVE, and the attacks have been successful. BIA therefore addresses worst-case scenarios.

风险管理的重点是识别威胁、漏洞和攻击，以确定能够保护数据的控制措施。另一方面，BIA假设这些控制措施已经失败/未通过/无效，并且攻击已经成功。因此，BIA处理最坏的情况。

Question 4

The comprehensive approach to emergency or disaster management typically consists of four phases: Prevention, Preparedness, Response, and Recovery (PPRR). Which phase does Business Impact Analysis (BIA) belong to? Describe two (2) examples of critical activities of a typical software firm that need to be established as part of business impact analysis.

紧急情况或灾害管理的综合方法通常包括四个阶段。预防、准备、响应和恢复（PPRR）。业务影响分析（BIA）属于哪个阶段？描述两（2）个典型软件公司的关键活动的例子，这些活动需要作为业务影响分析的一部分来建立。

BIA belongs to: Preparedness

A software firm is similar to manufacturing firm as in the QLD BCP Guide, so example can be found similarly as follows

Securing contracts with clients

Developing software

Delivering and supporting developed software products

BIA属于: 准备工作

一家软件公司与QLD BCP指南中的制造公司类似，因此可以找到类似的例子如下

确保与客户签订合同

开发软件

交付和支持开发的软件产品

Question 5

Explain why it is important for large organizations to have a proper BCP in place? What is the implication if a lack of BCP is found?

解释为什么大型组织拥有适当的BCP很重要？如果发现缺乏BCP，会有什么影响？

Legal and regulatory req: many industries may find themselves bound by federal, state and local laws or regulations that require them to implement various degrees of Business Continuity Planning. For example, the officers and directors of publicly traded firms have a fiduciary responsibility to exercise due diligence in the execution of their business continuity duties. In other circumstances, the requirements(and consequence of failure) might be more severe. Emergency services, such as police, fire, and emergency medical operations, have a responsibility to the community to continue operations in the event of a disaster. Indeed, their services become even more critical in an emergency when public safety is threatened. Failure on their part to implement a solid BCP could result in the loss of life and/or property and the decreased confidence of the population in their government.

法律和法规要求：许多行业可能发现自己受到联邦、州和地方法律或法规的约束，要求他们实施不同程度的业务连续性规划。例如，上市公司的高管和董事有信托责任，在执行业务连续性职责时要尽职尽责。在其他情况下，要求（和失败的后果）可能更严重。紧急服务，如警察、消防和紧急医疗行动，对社区有责任在发生灾难时继续运作。事实上，当公共安全受到威胁时，他们的服务在紧急情况下变得更加重要。如果他们不能实施一个可靠的BCP，可能会导致生命和/或财产的损失，以及民众对政府的信心下降。

In many countries, financial institutions, such as banks, brokerages,and the firms that process their data, are governed by strict government and international banking and securities regulations designed to facilitate their continued operation to ensure the viability of the national economy. Why pharmaceutical manufacturers must produce products in less-than-optimal circumstances following a disaster, they are required to certify the purity of their products to government regulators. There are countless other examples of industries that are required to continue operating in the event of an emergency by various laws and regulations.

在许多国家，金融机构，如银行、经纪公司和处理其数据的公司，都受到严格的政府和国际银行和证券法规的约束，旨在促进其继续运作，以确保国民经济的生存能力。为什么药品制造商必须在灾难后不太理想的情况下生产产品，他们被要求向政府监管机构证明其产品的纯度。还有无数其他的例子，这些行业被各种法律和法规要求在紧急情况下继续运营。

Question 6

Consider the statement ‘‘Business continuity planning is only about recovery of computer systems.” Is it true or false? Explain your reasoning.

考虑一下''业务连续性计划只是关于计算机系统的恢复 "的说法。它是真的还是假的？解释一下你的推理。

In the past, continuity planning was frequently thought of as the recovery of computer or information technology systems and nothing more. This discipline is often referred to as disaster recovery planning. Experience in the field of continuity planning has shown that the recovery of IT functions alone does not ensure survival of the enterprise following a serious disruption or disaster. Complete recovery requires thorough knowledge of all aspects of the enterprise.

在过去，连续性规划经常被认为是计算机或信息技术系统的恢复，仅此而已。这门学科通常被称为灾难恢复规划。连续性规划领域的经验表明，仅仅恢复信息技术功能并不能确保企业在发生严重中断或灾难后的生存。完整的恢复需要对企业的所有方面有全面的了解。

Question 7

Does business continuity planning provide any additional benefits to an organization apart from providing the ability to recover from major disruptive events.

除了提供从重大破坏性事件中恢复的能力外，业务连续性规划是否为一个组织提供任何额外的好处。

There are other, less obvious benefits of continuity planning. In developing a comprehensive continuity planning infrastructure, the continuity planner must understand the business processes of his enterprise, and how information, goods, and services move within the organization. Equally important is knowing how information, goods, services, and cash flow in and out of the enterprise.

连续性规划还有其他一些不太明显的好处。在开发全面的连续性规划基础设施时，连续性规划人员必须了解企业的业务流程，以及信息、货物和服务如何在组织内流动。同样重要的是了解信息、货物、服务和现金如何在企业内流动和流出。

The collection and analysis of this knowledge could identify potential cost reductions by improving or creating operating efficiencies. The planner may also find opportunities for cost savings in business interruption insurance and directors and officer's coverage. These examples show that continuity planning could provide an advantage over competitors. As the importance of continuity planning becomes more well known, the lack of planning could even disqualify a company from consideration for new business.

对这些知识的收集和分析可以通过改善或创造运营效率来确定潜在的成本削减。规划者还可能发现在业务中断保险和董事及高级职员保险方面节省成本的机会。这些例子表明，连续性规划可以提供相对于竞争对手的优势。随着连续性规划的重要性越来越广为人知，缺乏规划的公司甚至会被取消新业务的考虑资格。

The continuity planning process also forces a review of various other components of the organization's infrastructure. Vital records management, data backup and storage, and physical, environmental, and information security controls must also be scrutinized when addressing continuity planning, and efficiencies may be discovered during the process

连续性规划过程也迫使人们对组织的基础设施的各种其他组成部分进行审查。重要的记录管理、数据备份和存储，以及物理、环境和信息安全控制，在处理连续性规划时也必须进行仔细审查，在这个过程中可能会发现效率。

Question 8

Describe the advantages and disadvantages of hot sites

描述热点网站的优势和劣势

Hot Sites' Advantages热门网站的优势

* Ready within hours for operation 几小时内即可投入使用
* Highly available 高度可用
* Usually used for short-term solutions, but available for longer stays

通常用于短期解决方案，但可用于较长时间的停留

* Annual testing available 可进行年度测试

Hot Sites’ Disadvantages 热门网站的劣势

* Very expensive 非常昂贵
* Limited on hardware and software choices 在硬件和软件选择上受到限制

Question 9

Describe the advantages and disadvantages of cold and warm sites.

描述的 cold and warm sites 的优势和劣势。

Warm and Cold Sites' Advantages 优势

* Less expensive 价格较低
* Available for longer time frames because of the reduced costs

由于成本降低，可用于更长的时间框架

* Practical for proprietary hardware or software use

适用于专有硬件或软件的使用

Warm and Cold Sites' Disadvantages

* Operational testing not usually available

通常不提供操作测试

* Resources for operations not immediately available

无法立即获得的行动资源

Question 10

What is the fundamental difference between recovery time objective (RTO) and maximum tolerable downtime (MTD)? Suppose that RTO has been fixed, which aspects of data backup could be influenced by MTD? Discuss.

恢复时间目标（RTO）和最大可容忍停机时间（MTD）的根本区别是什么？假设RTO已经固定，那么数据备份的哪些方面可能会受到MTD的影响？讨论一下。

Difference: RTO is the specified time frame for recovering critical infrastructure/core functions of an organization, for example the website is up but with only limited/core features. In contrast, MTD is the specified time frame for bringing back the whole system to normal, which means all features should be available just like before the disaster strikes.

区别。RTO是指恢复组织的关键基础设施/核心功能的特定时间框架，例如，网站已经启动，但只有有限的/核心的功能。相比之下，MTD是将整个系统恢复到正常状态的规定时间，这意味着所有的功能都应该像灾难发生前那样可用。

Discussion: The data recovery is actually done in the second stage and is governed by WRT, which is MTD-RTO. When RTO is fixed, the time for recovering data is directly dependent on MTD:

讨论。数据恢复实际上是在第二阶段进行的，并受WRT的制约，也就是MTD-RTO。当RTO是固定的，恢复数据的时间就直接取决于MTD。

* If MTD is large, the data recovery time is large, hence any backup method, such as incremental backup is ok as we can take several steps to actually recover the data

如果MTD很大，数据恢复时间也很大，因此任何备份方法，如增量备份都可以，因为我们可以采取几个步骤来实际恢复数据。

* If MTD is small, the data recovery time is small, we need to recover data quickly, so differential backup might be preferred as it takes less time

如果MTD较小，数据恢复时间较短，我们需要快速恢复数据，所以差分备份可能是首选，因为它花费的时间较短。

* If MTD is very small, just sufficient for other testing, we need high availability, which means data mirroring/redundancy/full backup is required.

如果MTD非常小，只够用于其他测试，我们需要高可用性，这意味着需要数据镜像/冗余/完整备份。

Question 11

What are the the MTD, RPO, RTO values of the following scenario: Susan is the new BCM coordinator and needs to identify various preventive and recovery solutions her company should implement for BCP/DRP efforts. She and her team have carried out an impact analysis and found out that the companys order processing functionality cannot be out of operation for more than 15 hours. She has calculated that the order processing systems and applications must be brought back online within eight hours after a disruption. The analysis efforts have also indicated that the data that are restored cannot be older than five minutes of current real-time data.

以下情景的MTD、RPO、RTO值是多少。苏珊是新的BCM协调员，需要确定她的公司应该为BCP/DRP工作实施的各种预防和恢复解决方案。她和她的团队进行了一次影响分析，发现公司的订单处理功能不能停止运行超过15小时。她计算了一下，订单处理系统和应用程序必须在中断后8小时内恢复在线。分析工作还表明，恢复的数据不能超过当前实时数据的5分钟。

MTD of the order processing functionality is 15 hours. RTO value is 8 hours. WRT value is 7 hours. RPO value is 5 minutes.

订单处理功能的MTD是15小时。RTO值为8小时。WRT值是7小时。RPO值为5分钟。

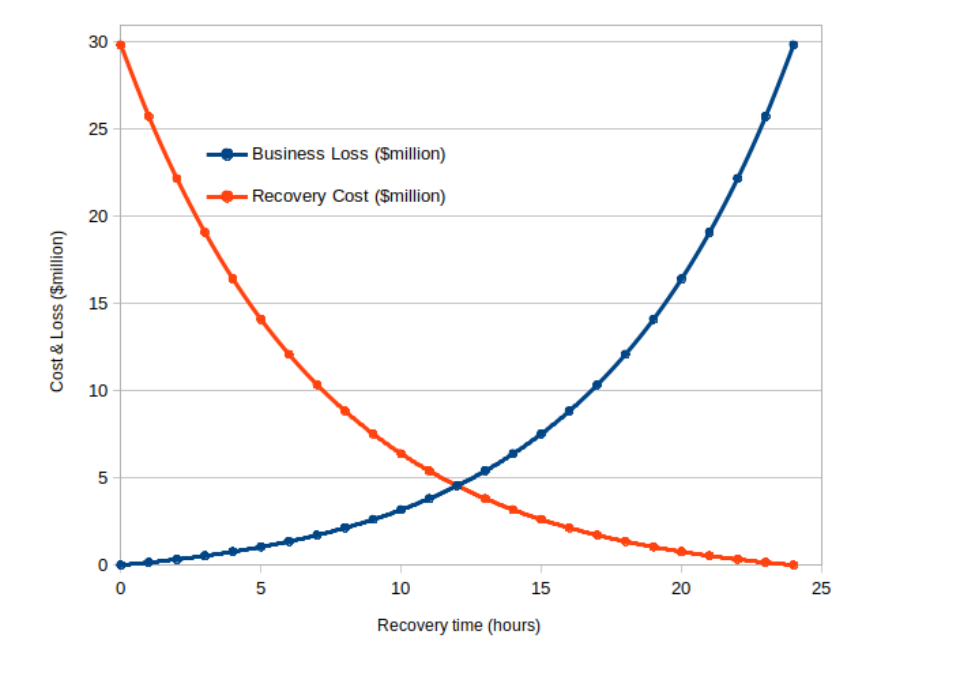
The order processing functionality as a whole has to be up and running within 15 hours. which is the maximum tolerable downtime (MTD). The systems and applications have to be up and running in eight hours, which is the Recovery Time Objective (RTO. RTO deals with technology, but we still need processes and people in place to run the technology. Work Recovery Time (WRT) is the remainder of the overall MTD value. RTO usually deals with getting the infrastructure and systems back up and running, and WRT deals with restoring data, testing processes, and then making everything live for production purposes. The data that are restored for this function can only be five minutes old; thus, the Recovery Point Objective (RPO) has the value of five minutes.

订单处理功能作为一个整体必须在15小时内启动和运行，这是最大可容忍的停机时间（MTD）。系统和应用必须在8小时内启动并运行，这是恢复时间目标（RTO）。RTO处理的是技术，但我们仍然需要流程和人员到位来运行技术。工作恢复时间（WRT）是整个MTD值的剩余部分。RTO通常处理的是让基础设施和系统恢复运行，WRT处理的是恢复数据，测试流程，然后让一切都为生产目的而运行。为这个功能恢复的数据只能是5分钟前的，因此，恢复点目标（RPO）的值是5分钟。

Question 12

The BIA team of an organization is determining the recovery time of their core system due to a disaster. The team has been able to plot the relationships between the business loss (due to ceasing of critical business activities) and the recovery cost (due to offsite facility and other related expenses) against recovery time below. The core system definitely needs to be recovered within 24 hours and the BIA team believes that a much quicker recovery can be achieved. Suppose that this is the only information available, suggest the optimal recovery time that the BIA team should aim for and explain your suggestion. Your argument must be based on the plot given below.

一个组织的BIA团队正在确定他们的核心系统在灾难中的恢复时间。该团队已经能够绘制出业务损失（由于关键业务活动的停止）和恢复成本（由于异地设施和其他相关费用）与恢复时间之间的关系。核心系统肯定需要在24小时内恢复，BIA团队认为可以实现更快的恢复。假设这是唯一可用的信息，建议BIA团队应该争取的最佳恢复时间并解释你的建议。你的论点必须基于下面给出的情节。



\*Find optimum point which is intersection between 2 curves = 12hrs

\*找到2条曲线的交点的最佳点=12小时

Students are expected to find the optimal point being the intersection between two curves, which is exactly 12 hours (the two curves have been specially created). They are also expected to explain that if recovery time is less than 12 hours the recovery cost is much more than the loss and it is not worth spending that much, whilst longer recovery time can significantly increase business loss.

学生们要找到最佳点，即两条曲线的交点，正好是12小时（这两条曲线是专门创建的）。他们还需要解释，如果恢复时间少于12小时，恢复成本就会远远超过损失，不值得花这么多钱，而更长的恢复时间会大大增加企业损失。

Furthermore, if the total cost is taken into account, the sum of the two curves also gives the minimum at that intersection (which gives a total cost of $9.1 millions, still much less than $30 millions perceived as maximum absorbed cost). In the absence of other information, the intersection is the best choice as far as the cost and loss are concerned

此外，如果考虑到总成本，两条曲线的总和也给出了该交叉点的最小值（这给出了910万美元的总成本，仍然远远低于被认为是最大吸收成本的3000万美元）。在没有其他信息的情况下，就成本和损失而言，该交叉点是最佳选择。

Question 13

What are the three main phases in a contingency plan as per the NIST SP800 standard? Briefly describe the activity in each phase.

根据NIST SP800标准，应急计划的三个主要阶段是什么？简要描述每个阶段的活动。

Students are expected to look up the NIST SP800 standard before answering this question.

在回答这个问题之前，学生应该先查一下NIST SP800标准。

* Phase 1 - Activation and notification: The Activation and Notification Phase defines initial actions taken once a system disruption or outage has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the plan. At the completion of the Activation and Notification Phase, information system contingency plan (ISCP) staff will be prepared to perform recovery measures to restore system functions.

阶段1--启动和通知。激活和通知阶段定义了一旦发现或似乎即将发生系统破坏或中断时采取的初步行动。这个阶段包括通知恢复人员、进行故障评估和启动计划的活动。在启动和通知阶段完成后，信息系统应急计划（ISCP）人员将准备好执行恢复措施，以恢复系统功能。

* Phase 2 - Recovery: Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location. At the completion of the Recovery Phase, the information system will be functional and capable of performing the functions identified in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation at an alternate system, or relocation and recovery at an alternate site. It is feasible that only system resources identified as high priority in the BlA will be recovered at this stage.

第二阶段 - 恢复。恢复阶段的活动重点是实施恢复战略，以恢复系统能力，修复损坏，并在原地或新的替代地点恢复运行能力。在恢复阶段完成后，信息系统将具备功能，能够执行计划中确定的功能。根据计划中确定的恢复策略，这些功能可能包括临时的手工处理，在备用系统中的恢复和操作，或者在备用地点的搬迁和恢复。在这个阶段，只有在BlA中被确定为高优先级的系统资源才会被恢复，这是可行的。

* Phase 3 - Reconstitution: The Reconstitution Phase is the third and final phase of ISCP implementation and defines the actions taken to test and validate system capability and functionality. During Reconstitution, recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. This phase consists of two major activities: validating successful recovery and deactivation of the plan.

第三阶段--重构。重建阶段是ISCP实施的第三个也是最后一个阶段，它定义了为测试和验证系统能力和功能而采取的行动。在重建过程中，恢复活动已经完成，正常的系统操作已经恢复。如果原来的设施无法恢复，这个阶段的活动也可以应用于准备一个新的永久地点来支持系统处理的要求。这个阶段包括两个主要活动：验证成功恢复和停用计划。