Business 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）

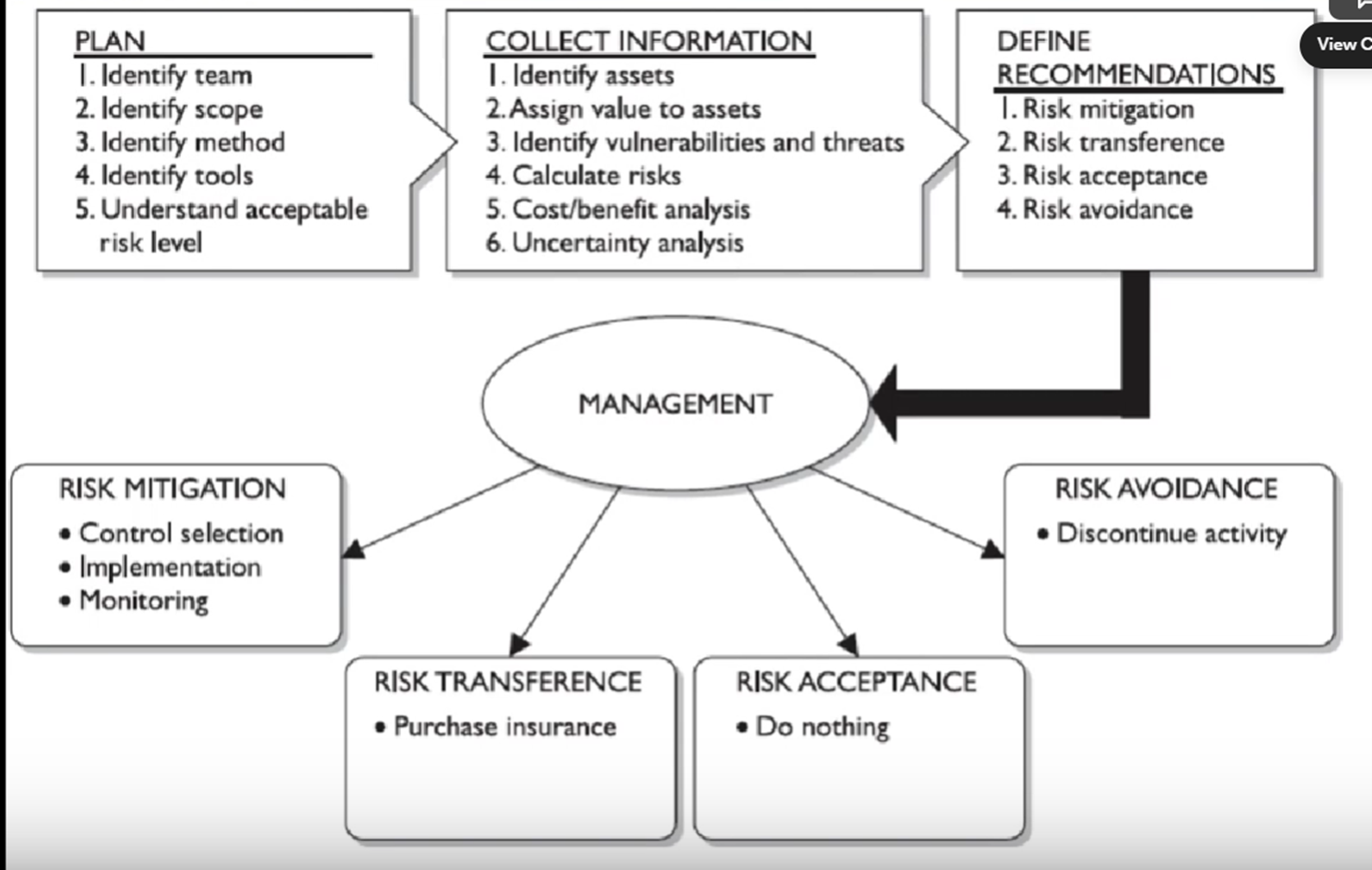
* What to do when an event occurs (contingency plans)

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**

1. 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
2. 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
3. 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。

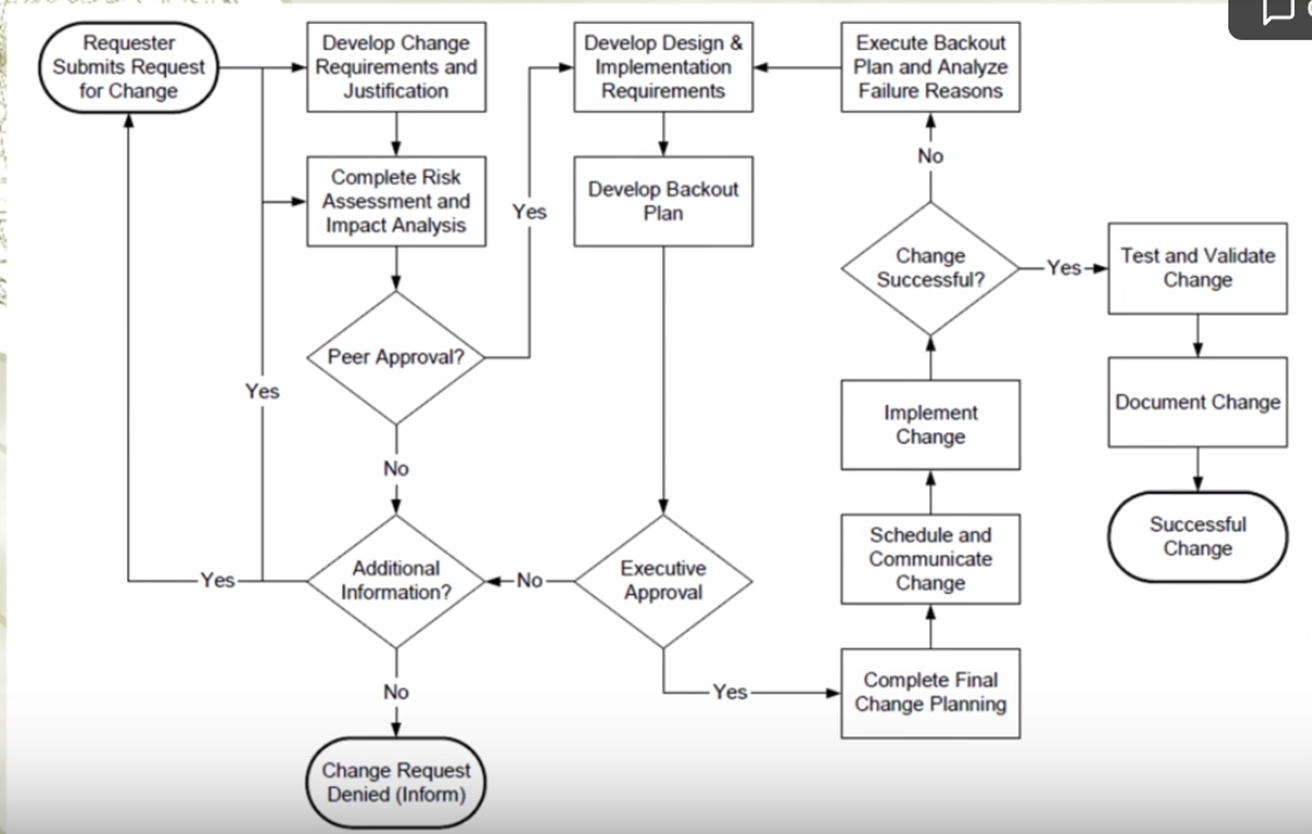
1. **Validation:** The change is validated by the operations staff to ensure that the intended machines received the deployment package. The security staff performs a security scan or review of the affected machines to ensure that new vulnerabilities are not introduced. Changes should be included in 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