

**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。

*Advantages:*

* keep your business trading during and after an incident
* recover operations more quickly after interruptions
* reduce costs and duration of any disruption
* mitigate risks and financial exposure
* build customer confidence and trust
* safeguard company reputation
* develop confidence within the business
* comply with regulatory or legal requirements
* insure against otherwise unacceptable risks
* save lives, if dangerous events (such as a fire) occur

*Importance:*

A business continuity plan positions your organization to survive serious disruption. It eliminates confusion common to every disaster, providing a clear blueprint for what everyone should do.

**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

*Importance:*

A DRP aims to help an organization resolve data loss and recover system functionality so that it can perform in the aftermath of an incident, even if it operates at a minimum level.

*Advantages:*

* Cost-Efficiency.
* Increased Employee Productivity.
* Greater Customer Retention.
* A Better Understanding of Scalability.

**Difference between BCP and DRP**

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.

**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。

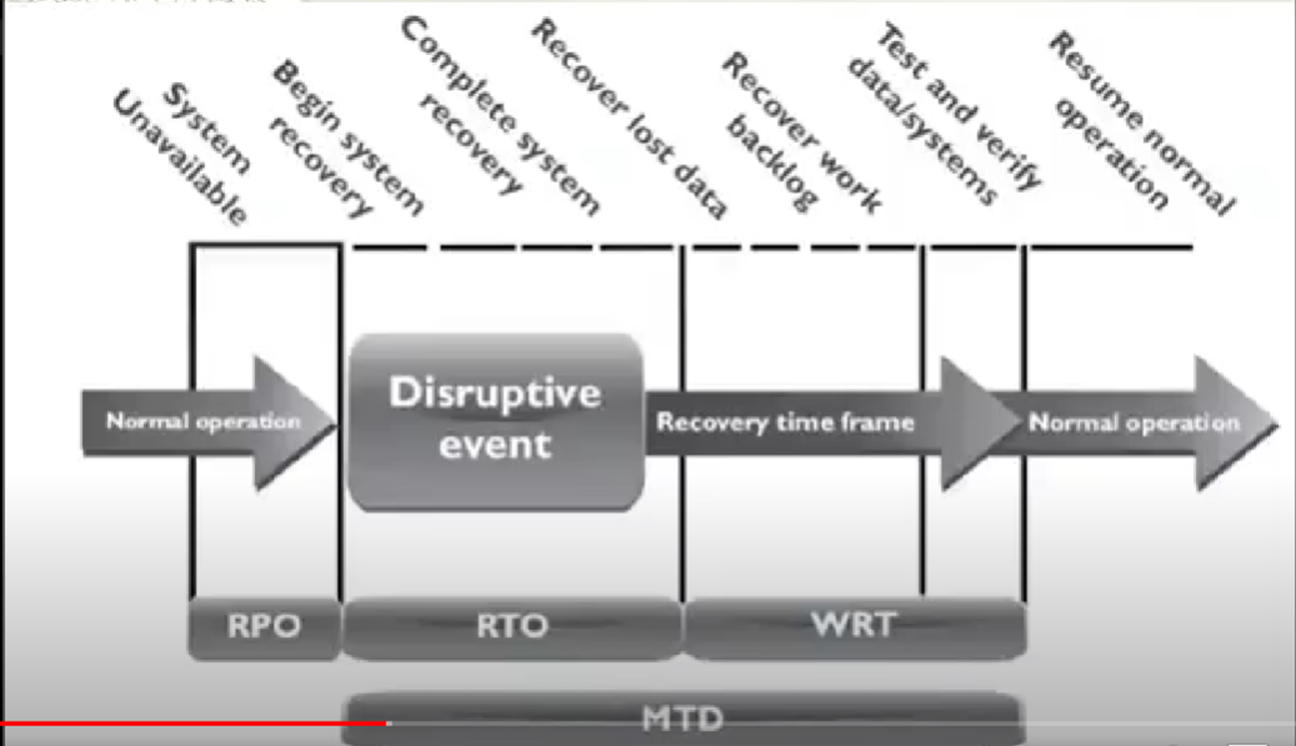
* The RTO value for mission-critical data processing is two minutes or less. This means that the technology that carries out the processing functionality for this type of data cannot be down for more than two minutes.

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。

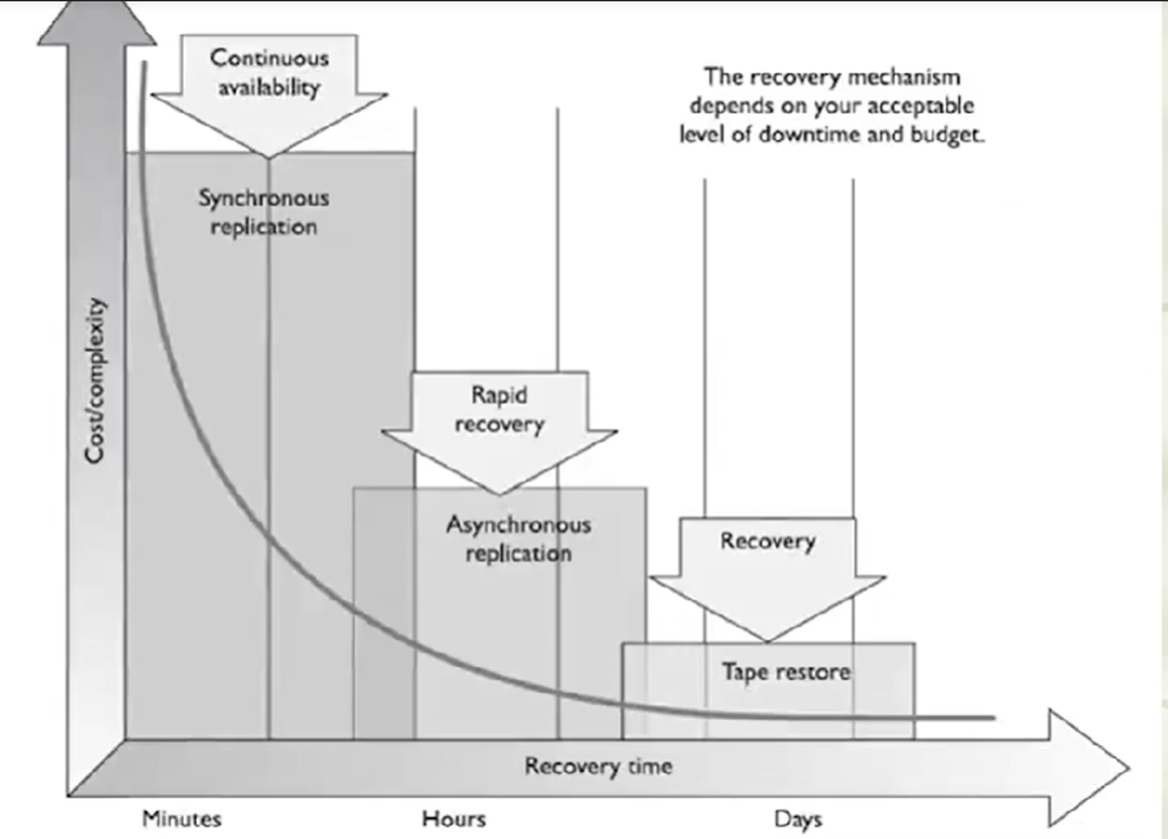
* The company may choose to have a cluster technology in place that will shift the load once it notices that a server goes offline.

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。

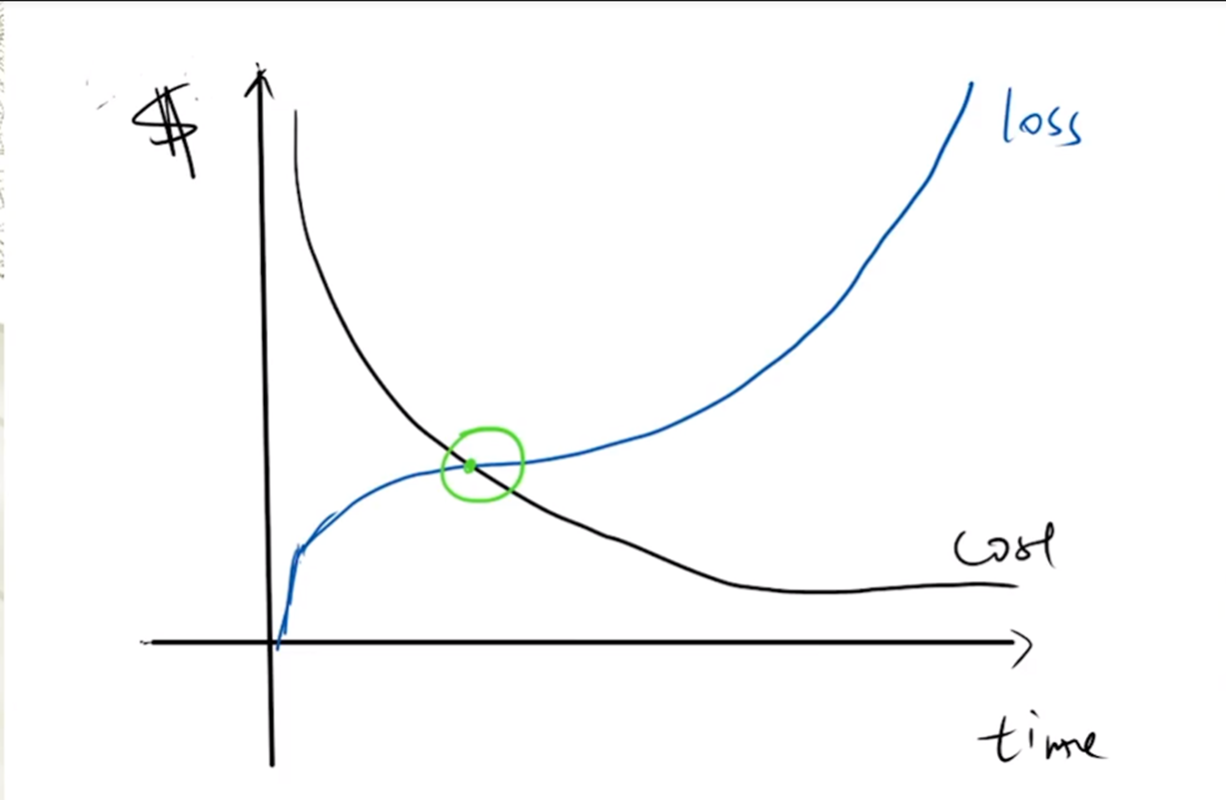
**Recovery Parameters Timeline 恢复参数时间表**



**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：**

1. **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。

1. **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。

1. **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。

**The following provides a 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

1. **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。

1. **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。

1. **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。

1. **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

1. **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。