BCM營運持續管理
- DRP災難復原計畫

Agenda

課程目標

真實故事

何謂BCM營運持續管理

IT營運持續管理生命週期

課程目標

1

課程目標

透過本課程您將可了解：

1. 營運持續管理的內涵
2. 國際標準與Good Practice
3. IT營運持續之生命週期管理

真實故事

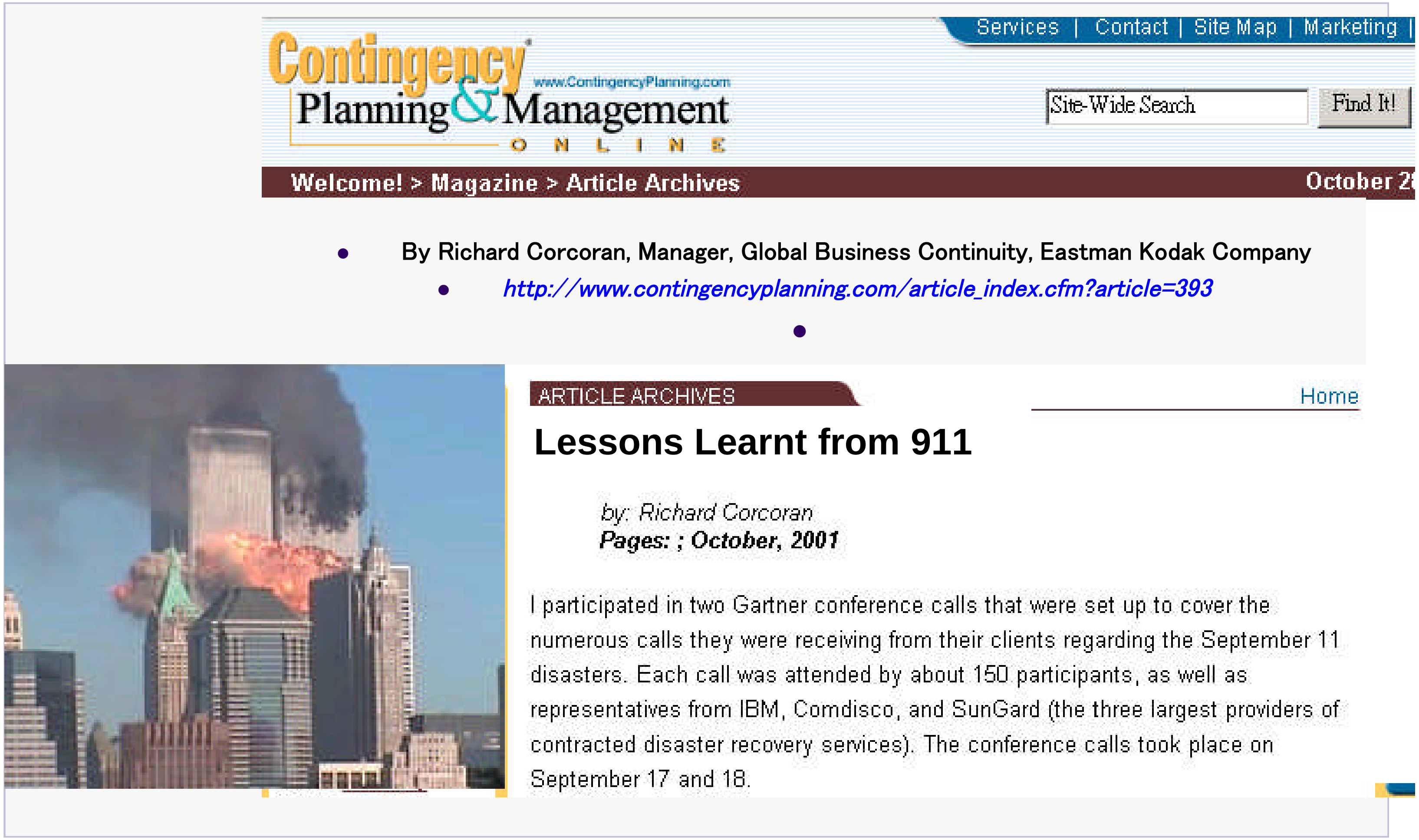
It may happen to you…

2

曾經發生過…

- 有**350**家企業於**1993**年炸彈攻擊事件中在世貿大樓營運
- 其中有**150**家長達一年無法營運

再度發生…


Services | Contact | Site Map | Marketing |
Contingency Planning & Management ONLINE
www.ContingencyPlanning.com
Site-Wide Search
Find It!
Welcome! > Magazine > Article Archives
October 2
ARTICLE ARCHIVES
Home

- By Richard Corcoran, Manager, Global Business Continuity, Eastman Kodak Company
  - *http://www.contingencyplanning.com/article_index.cfm?article=393*

Lessons Learnt from 911

by: Richard Corcoran
Pages: ; October, 2001

I participated in two Gartner conference calls that were set up to cover the numerous calls they were receiving from their clients regarding the September 11 disasters. Each call was attended by about 150 participants, as well as representatives from IBM, Comdisco, and SunGard (the three largest providers of contracted disaster recovery services). The conference calls took place on September 17 and 18.

摩根史坦利的危機應變

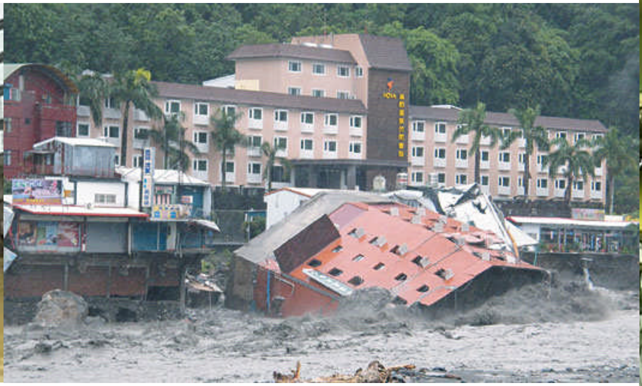
- 當8:48分第一架飛機撞上世貿大樓時，安全主管在一分鐘後緊急廣播，員工立即進行疏散
- 9:15分在Seventh Avenue設立應變指揮中心，於九點二十五分啟動位於Varick街的資訊備援中心與建立位於紐澤西州Harberside的第二辦公室，恢復各系統運作。
- 該公司9:03 分即啟動企業備援計畫疏散3500名員工，9:50分全部員工疏散完畢，9分鐘後大樓全部倒塌。
- 在關鍵時刻立即啟動營運持續計畫，成功的保護了公司最重要的資產及員工的生命。由於營運復原迅速，讓客戶的權益完全受到保護，除維持對客戶的承諾，更建立了長遠的信任關係。
- **危機應變成功重要因素：**
  - 發生時，員工被授權作決策，不須請示高層主管。使得3500名員工能在第一時間下樓。
  - 意外發生時，利用預先規劃的備援網路及電話線，成功的向員工及外界報導現況，維持通訊及指揮系統的暢通。
  - 事先規劃的設備清理計畫，該公司的電腦備援系統順利的在9:25分即開始運作，電腦中斷時間不超過1個小時

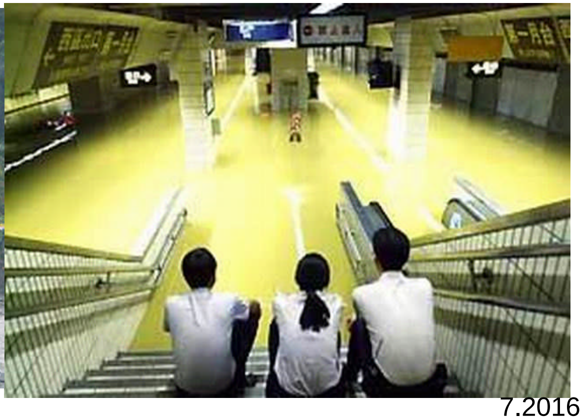
發生在別人身上的…

- 2005年卡崔娜（ Katrina）為美國史上登陸第三強之颶風
- 整體證實死亡統計人數為656人(至09/13止) 。受災人數約二十七萬。整體損失將達3,000 億美元
- 紐奧良市堤防設計無法對規模三以上之颶風提供保護
- 紐奧良市80%地區遭水淹沒
- 約四萬五千位災民聚集在超級巨蛋及會議中心
- 經濟影響：油價、重建經費、保險理賠、物價的波動
- 災民的安置問題
- 救援物資的運補問題
- 後續重建問題

也曾發生在我們身上…

- 2001年9月納莉風災，台北捷運停駛三個月，交通黑暗期半年之久，北市政府共損失22億元
- 南港軟體園區停擺一個半月
- 四家固網業者及六家行動電話業者均無一倖免，電信機房與網路設備紛紛傳出災情
- 2009年8月8日，莫拉克風災造成南部、東部嚴重災情





發生在我身上…

- 1999年921大地震

何謂BCM營運持續管理

3

營運持續管理(BCM)、營運持續計畫(BCP)與災難復原(DRP)

BCM：
一個完整的**Framework**，包含了**BCP**與**DR**，確保企業在不同的情況下能繼續營運。

BCP:
轉移系統到另一個備用環境、讓企業用不同的模式繼續營運以及與相關利害關係人、客戶與股東…等互動之計畫。

DRP:

回復組織被中斷的**IT**與通信能力之計畫。

BCM營運持續管理國際標準與Good Practice

ISO 22301

- **ISO 22301:2012 Societal security -- Business continuity management systems --- Requirements**

ISO27031

- **Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity**

Business Continuity Institute's Good Practice Guidelines (GPG)

DRI International Institute's Professional Practices for Business Continuity Planners

BCM Lifecycle

營運持續管理生命週期

3

營運持續計畫涵蓋的內容(續)

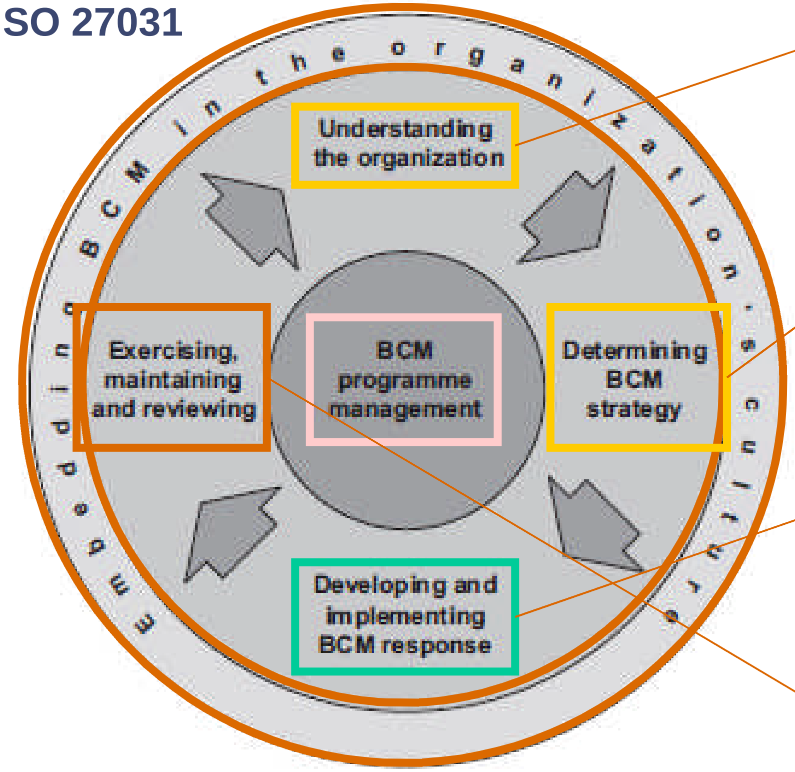
營運持續計畫最主要的目的在於協助組織業務在遭遇異常中斷時，可維持其功能持續運作。

一個完整的營運持續應含蓋：

- 中斷**發生前**的處理
- 中斷**發生時**的處理
- 中斷**發生後**的處理

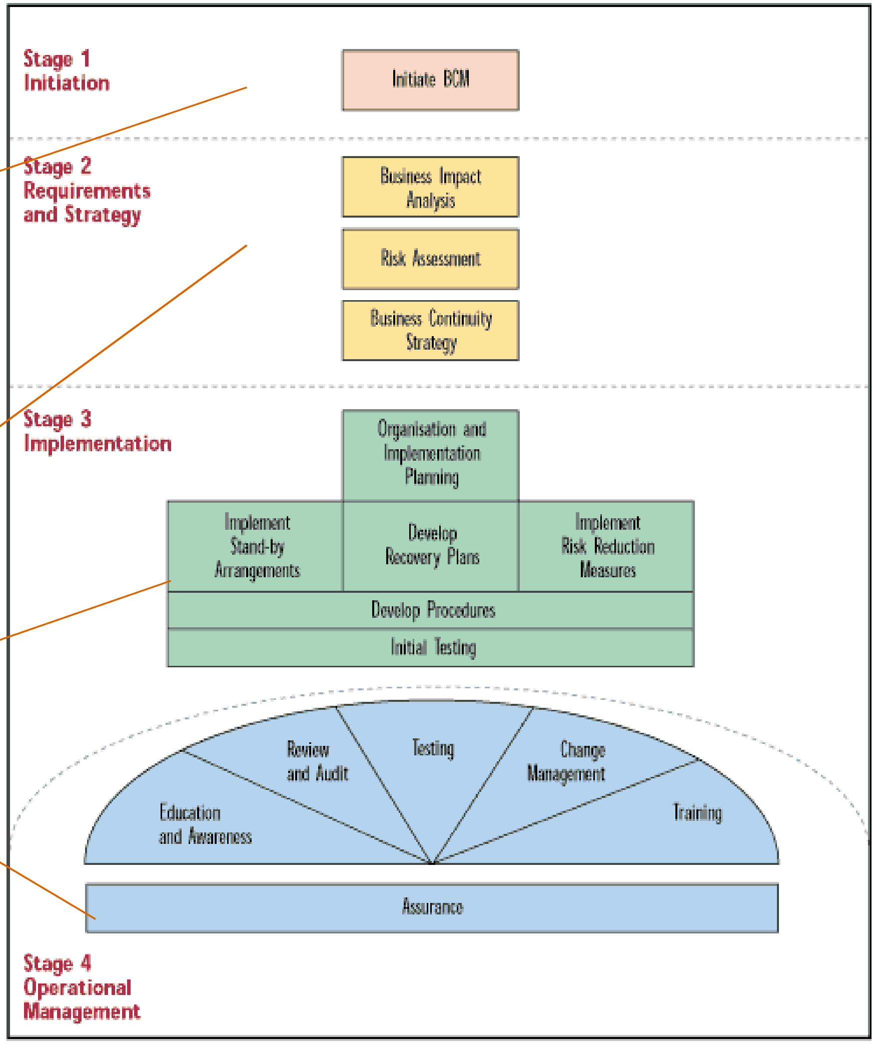
BCM Lifecycle

ISO 22301
ISO 27031



Embedding BCM in the organization's culture
Understanding the organization
Determining BCM strategy
Developing and implementing BCM response
Exercising, maintaining and reviewing
BCM programme management

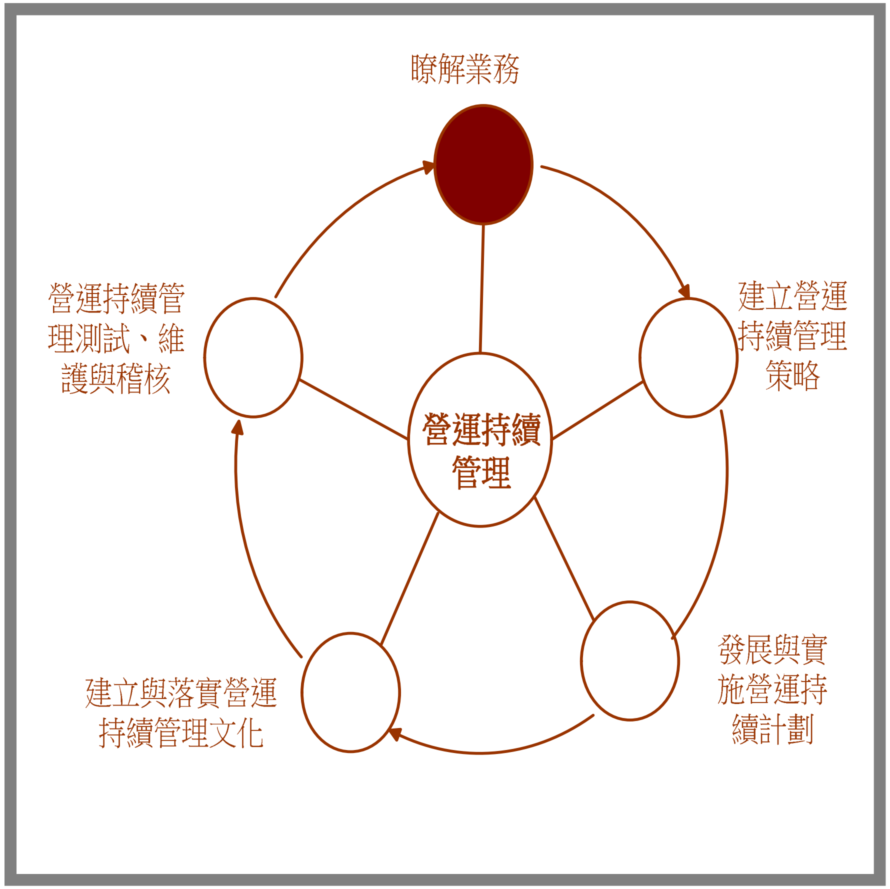
[ITSCM]



營運持續管理的生命週期

瞭解業務

主要是要透過業務衝擊分析BIA ,風險評鑑 Risk Assessment (RA) 去區分關鍵活動 (Mission Critical Activity, MCA)、瞭解其運作所需要的內外在資源、MCA的致命點以及其可能遭遇的內外在衝擊。



營運持續管理的生命週期

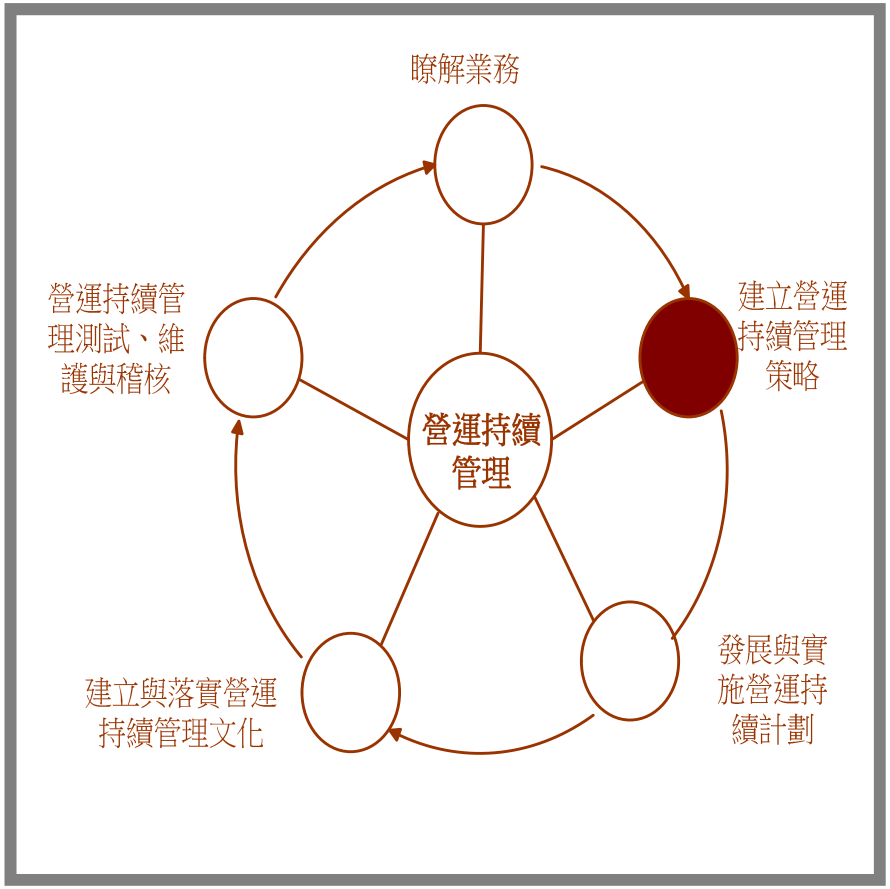
建立營運持續管理策略

例如說決定採取哪種 BCM 策略模型

- Active/Backup – 備份
- Active/ Active – 負載平衡
- Alternate site – 替代地點

處理風險的策略可從下面方向考慮

- 避免風險
- 降低風險
- 轉移風險
- 接受風險

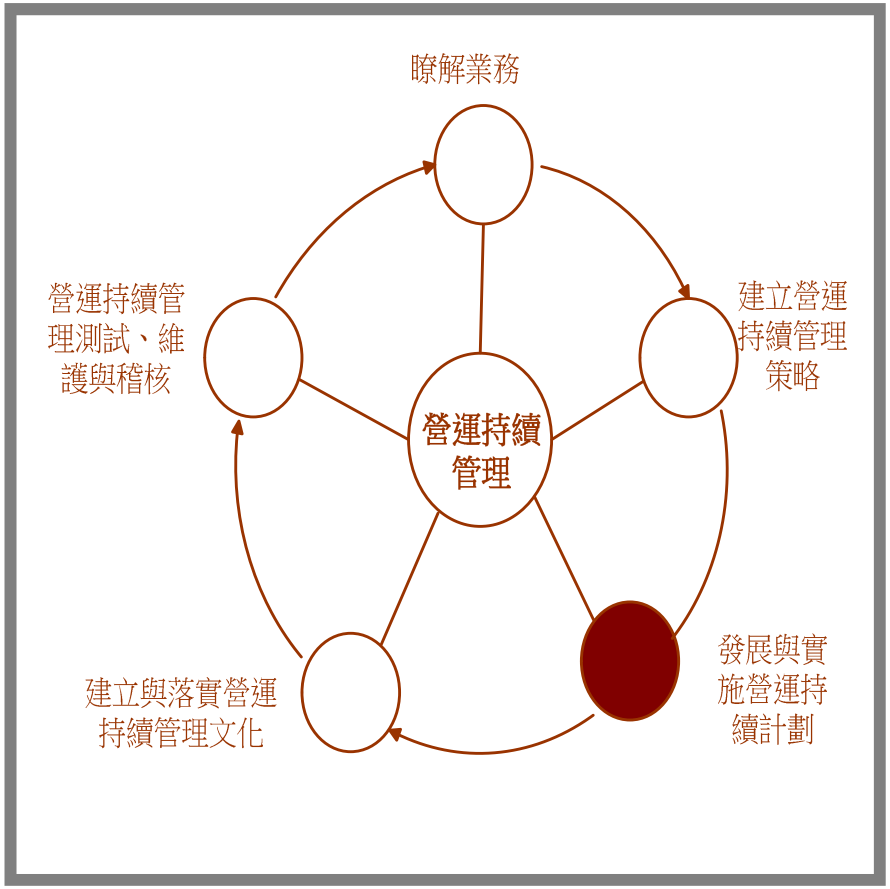


營運持續管理的生命週期

發展與實施營運持續管理計劃

一般營運持續管理計劃會包括

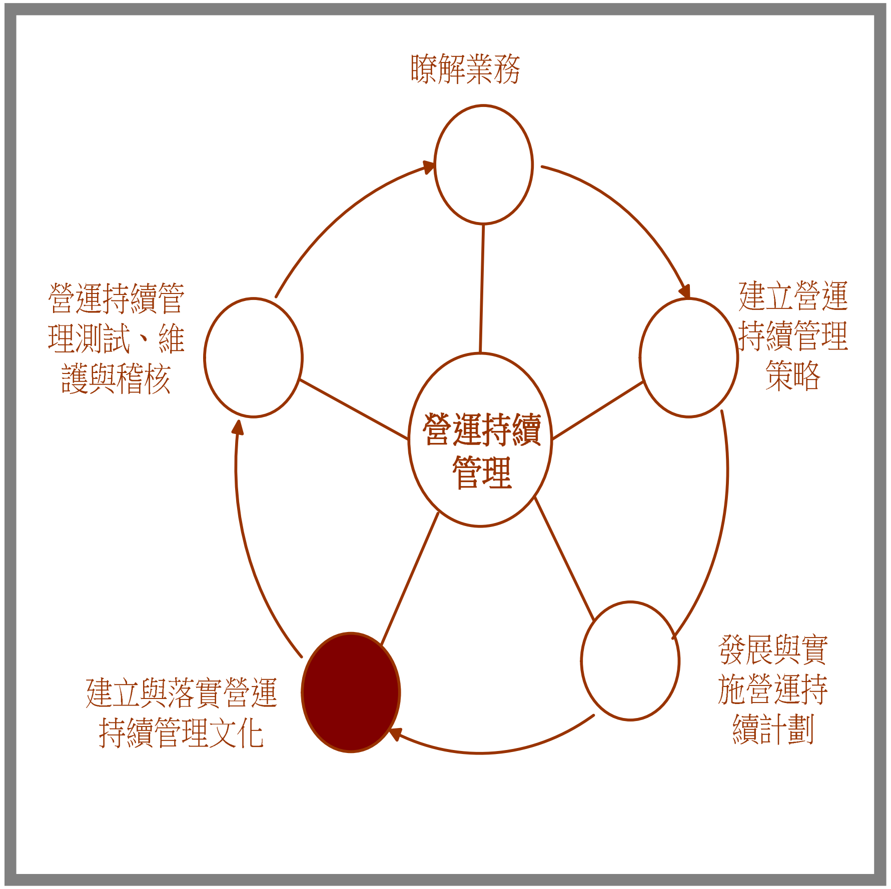
- 對策
- 計畫啟動條件
- 職責說明
- 緊急程序
- 備援程序
- 時間目標(如RTO與RPO)
- 復原程序
- 認知與教育訓練
- 維護時間表
- 程序文件化



營運持續管理的生命週期

建立與落實營運持續管理文化

透過教育訓練等動作達成



營運持續管理的生命週期

演練

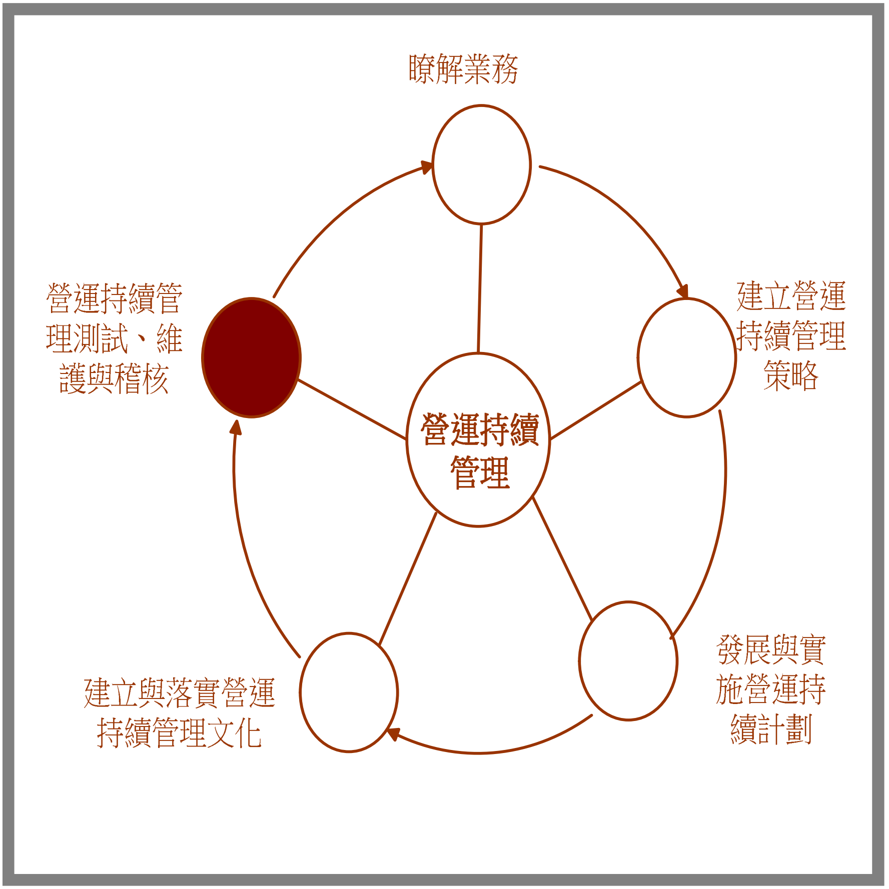
- 狀況演練、復原測試、測試異地復原、測試供應商的設施與服務、完整演練
- 透過演練以證實BCM的適任性與能力

維護

- 因下列某些因素改變進行更新維護
  - 營運策略、法令、場所、資源、
    - 設備或作業變更、風險、人員變動、供應商或客戶

稽核

- 進行變更管制、稽核，確保整體計畫處於最新狀況



BCM vs. ITSCM

4

BCM vs. ITSCM

Business Continuity Management (BCM)

- is focused on managing risks to ensure that at all times an organization can continue operating to a pre-determined minimum level.

IT Service Continuity Management (ITSCM)

- must be a part of the overall BCM process
- is focused on the Continuity of IT Services to the business

BCP (企業永續計畫) v.s. DRP (災難復原計畫)

Business Continuity Plan (BCP)

Business continuity planning is best described as the process and procedures that an organization can put in place to ensure that essential business functions continue to operate during and after a disaster.

By having a BCP, organizations seek to prevent interruption of mission critical services. This type of planning enables them to re-establish services to a fully functional level as quickly and smoothly as possible.

BCPs generally cover most or all of an organization's critical business processes and operations.

目標是企業可以在經歷災難時或後，還能持續運作

Disaster Recovery Plan (DRP)

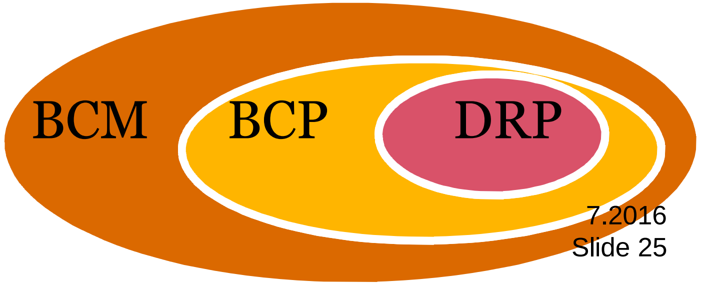
As part of the business continuity process an organization will normally develop a series of DRPs.

These are more technical plans that are developed for specific groups within an organization to allow them to recover a particular business application.

The most well known example of a DRP is the Information Technology (IT) DRP.

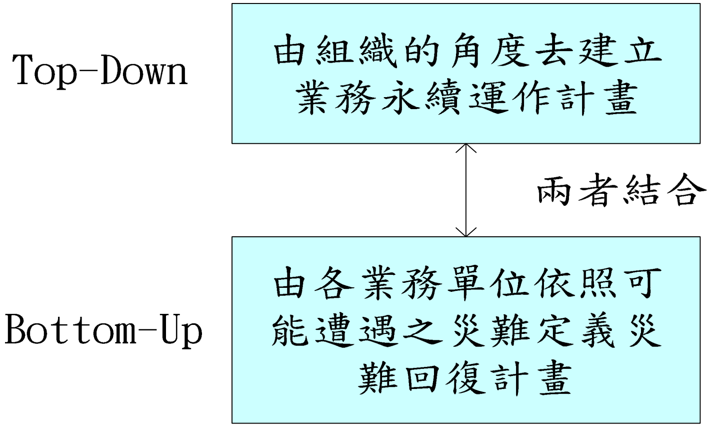
Other traditional areas requiring specific DRPs include call centers, warehouses, distribution centers and any other areas of specialized activities.

著重在災難中復原(Recovery)，期望縮短災難發生對營業中斷的影響時間(加速復原)



BCP (企業永續計畫) v.s. DRP (災難復原計畫)

- BCP 與 DRP 必需要相互配合
  - BCP 需要 DRP 說明執行時的細節。
  - 只考慮 DRP，可能會乎略營運持續運作的需求



Top-Down

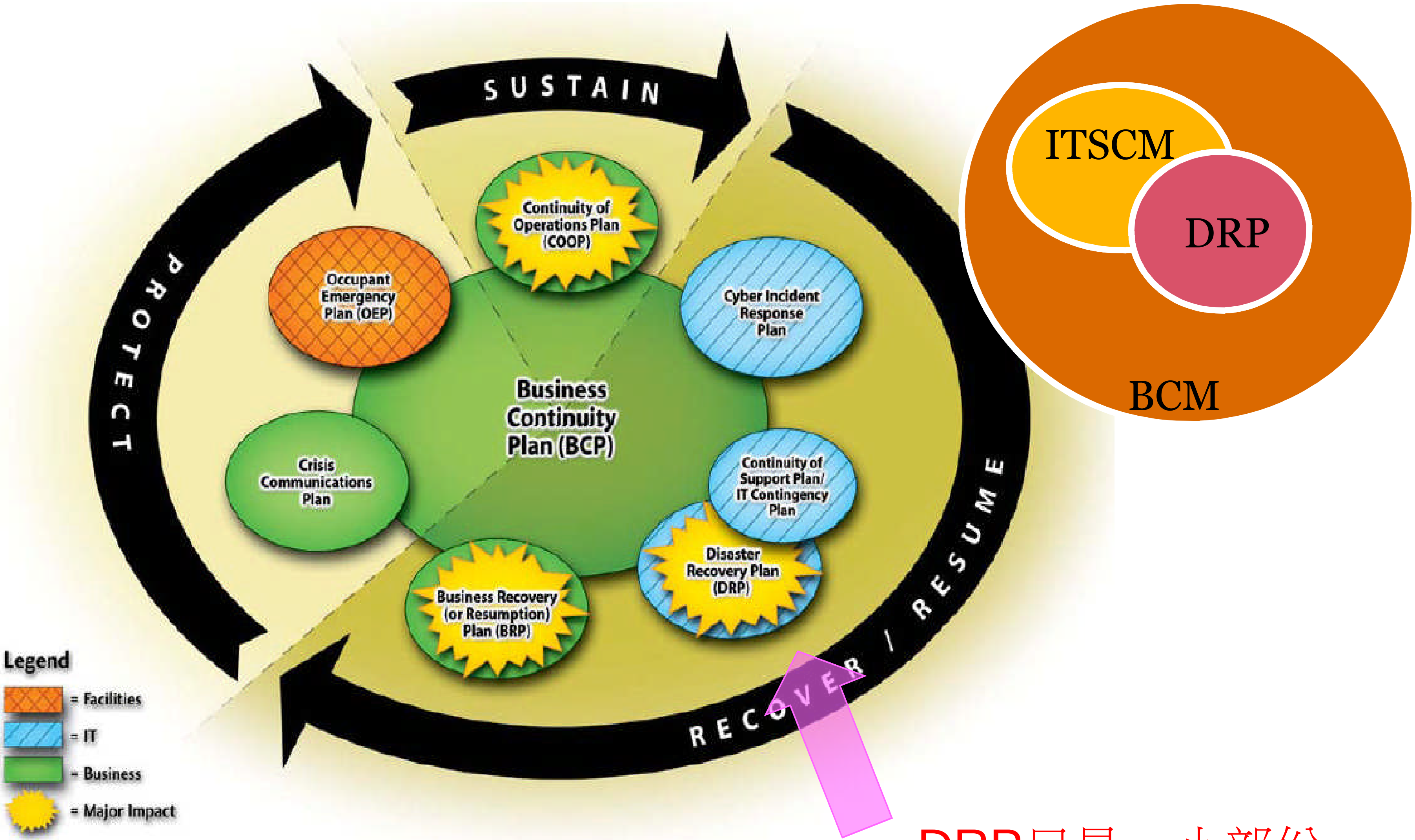
由組織的角度去建立業務永續運作計畫

兩者結合

Bottom-Up

由各業務單位依照可能遭遇之災難定義災難回復計畫

BCP vs. DRP


SUSTAIN
PROTECT
RECOVER / RESUME
Business Continuity Plan (BCP)
Continuity of Operations Plan (COOP)
Occupant Emergency Plan (OEP)
Cyber Incident Response Plan
Crisis Communications Plan
Continuity of Support Plan/ IT Contingency Plan
Disaster Recovery Plan (DRP)
Business Recovery (or Resumption) Plan (BRP)
Legend
= Facilities
= IT
= Business
= Major Impact
ITSCM
DRP
BCM

DRP只是一小部份

DR = Remote redundant異地備援？

Disaster Recovery=>災難復原or異地備援？

Disaster Recovery should include

- Local redundant or backup,...(在地備援, HA, Cluster,...)
- Remote redundant or backup,...(異地備援)
- Anything can let company recover from disaster!

做到了異地備援層次，可以對更多樣的災難有應變之措施或政策

- 例如地震、風災、火災、水災等區域性災難，在地備援是無法應付
- **在做異地備援前應該做好在地備援，否則動不動就啟動異地備援，未免太過於勞師動眾**

僅有「備援」是不夠的！『復原』才是終極目標！

- 或是說『永續』才是終極目標

為什麼要有災難復原計畫

在從IT災難事件中復原時，時間(時效)是最重要的

當重要資料、網路或是資訊系統無法存取後，損失將隨著一分一秒地流逝而快速增加

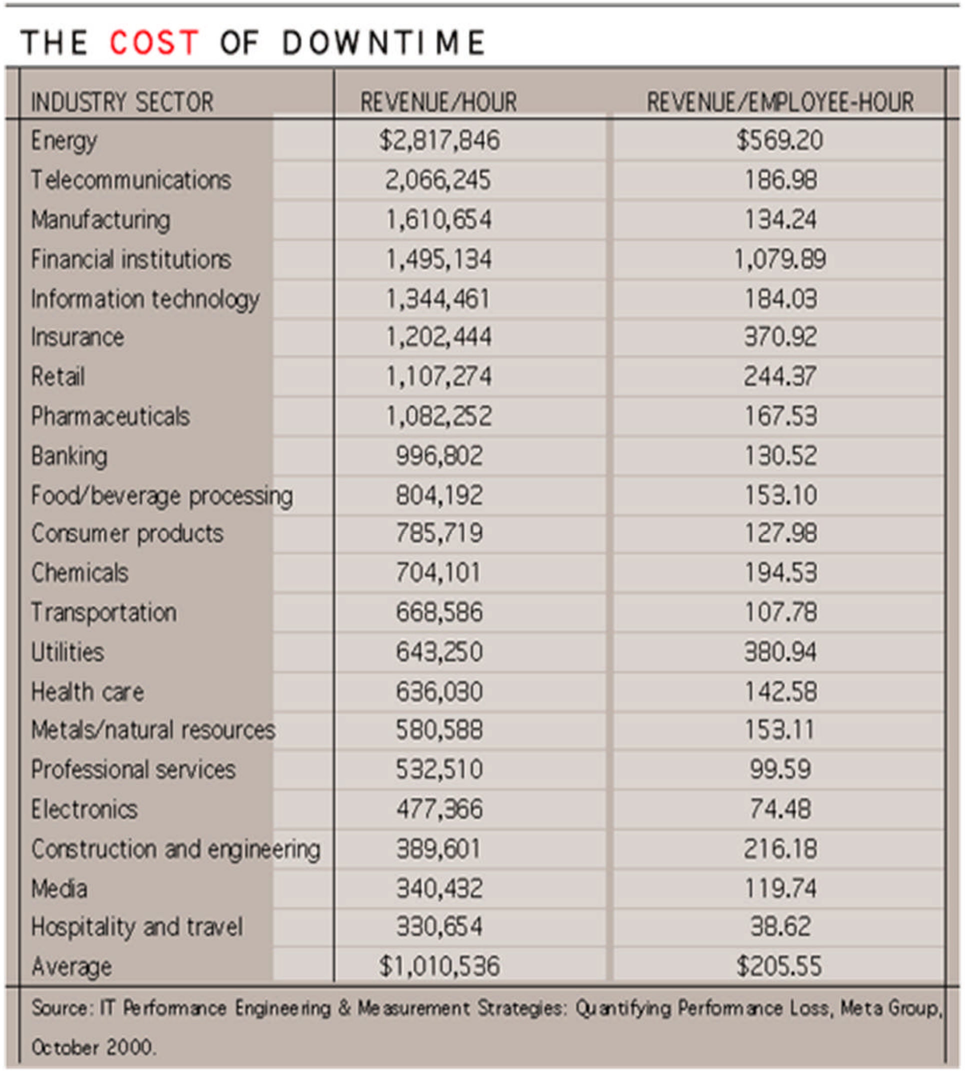
如果有一套計畫來因應災難事件，那麼將可以有條理、有組織地將災難事件時間縮短

- 這計畫可能小到只是備份重要的資料或是大到複製整個運作系統
- 可以採用公司的資源或是外部資源

目標

- 營運持續(Business Continuity)

損失有多大？每小時各行業的損失



THE COST OF DOWNTIME

INDUSTRY SECTOR	REVENUE/HOUR	REVENUE/EMPLOYEE-HOUR
Energy	$2,817,846	$569.20
Telecommunications	2,066,245	186.98
Manufacturing	1,610,654	134.24
Financial institutions	1,495,134	1,079.89
Information technology	1,344,461	184.03
Insurance	1,202,444	370.92
Retail	1,107,274	244.37
Pharmaceuticals	1,082,252	167.53
Banking	996,802	130.52
Food/beverage processing	804,192	153.10
Consumer products	785,719	127.98
Chemicals	704,101	194.53
Transportation	668,586	107.78
Utilities	643,250	380.94
Health care	636,030	142.58
Metals/natural resources	580,588	153.11
Professional services	532,510	99.59
Electronics	477,366	74.48
Construction and engineering	389,601	216.18
Media	340,432	119.74
Hospitality and travel	330,654	38.62
Average	$1,010,536	$205.55

Source: IT Performance Engineering & Measurement Strategies: Quantifying Performance Loss, Meta Group, October 2000.

Failure to keep operating

Fortune 1000 study

- Average loss $78K (約273萬台幣), up to $500K(約1,750萬台幣)
- 65% failing over 1 week never reopen
- Loss of market share common

什麼是災難復原 (Disaster Recovery)?

Disaster越來越多樣

- 傳統像：地震、風災、水災、火災、電力損壞等等
- 新的有：示威抗議、恐怖攻擊、駭客入侵
- Information Security Disaster Recovery是目前需要考慮的

災難復原(DR)應該可算是營運持續運作(Business Continuity, BC)的一個環節

目標：在遭遇Natural disaster, infrastructure failure, human errors等事件，企業可以回復營運

常見災難類型

- **Natural Events** 天然災害

– Earthquake 地震

– Flood 水災

– Mudslide 山崩

– Hurricane 颶風

– Blizzard 暴風雪

– Tornado 龍捲風

- **Accidents** 意外事故

– Explosion 爆炸

– Fire 火災

– Power outages 電力中斷

– Broken pipes 管道破損

– Collisions from vehicles 車輛碰撞

– Hazardous material spill 危險物品散落

– Nuclear disaster 核災

- **Attack** 外來攻擊

– Terrorism, Sabotage and Acts of War 恐怖行動,破壞及戰爭

– Bombing 炸彈

– Kidnapping 綁架

– Mailing or spreading life-threatening bacteria or viruses 郵寄或散佈細菌或病毒

- **Miscellaneous Events** 其他事件

– Explosion 爆炸

– Hardware, software failure 軟硬體失效

– Employee evacuation absence員工離職

– Testing outage 測試中斷

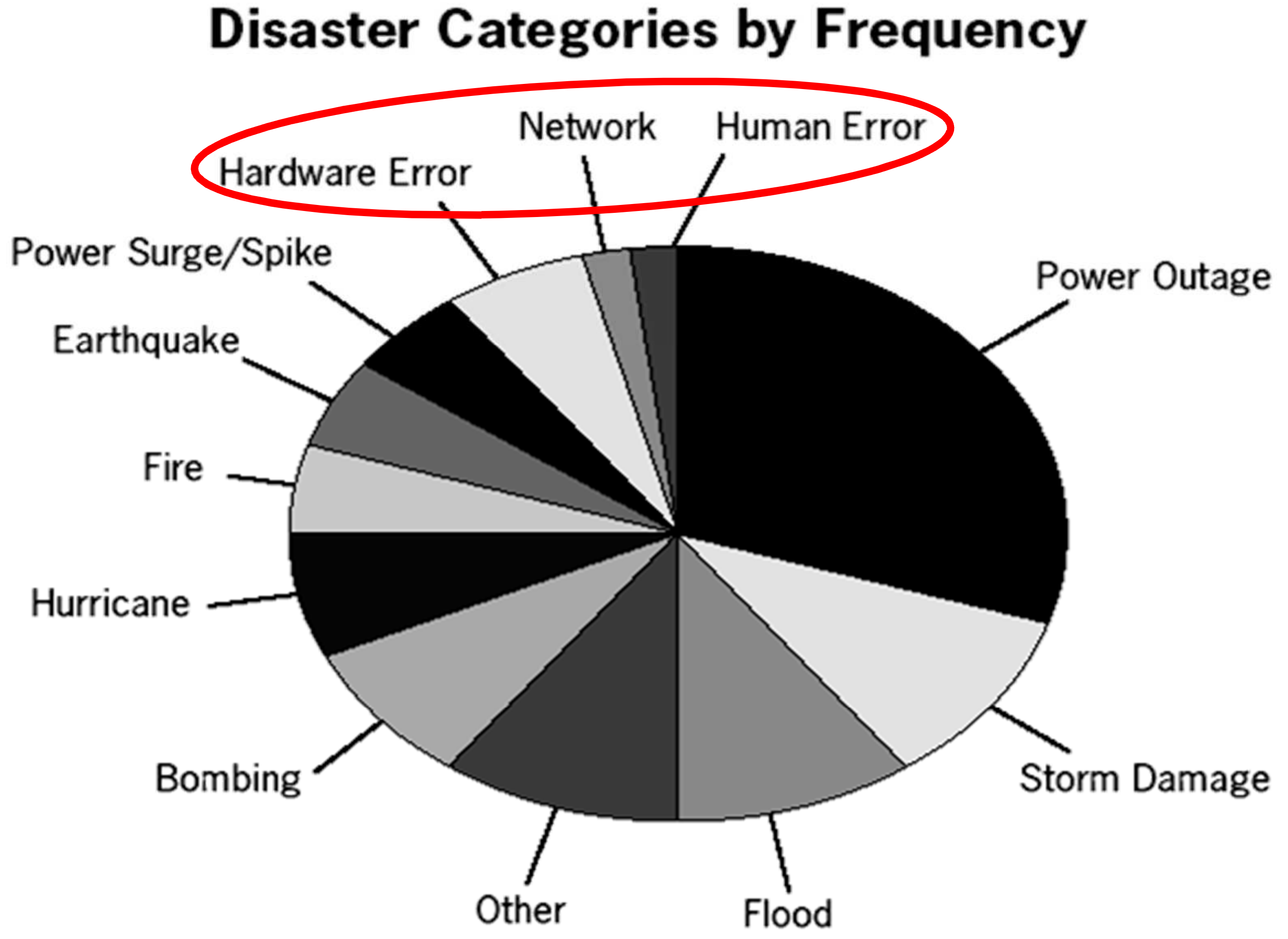
– Human error and omission人員錯誤及失職

– Disgruntled employee員工不滿

– Malicious mischief 惡意破壞

– Riot 暴動

各種類型災難的發生機率

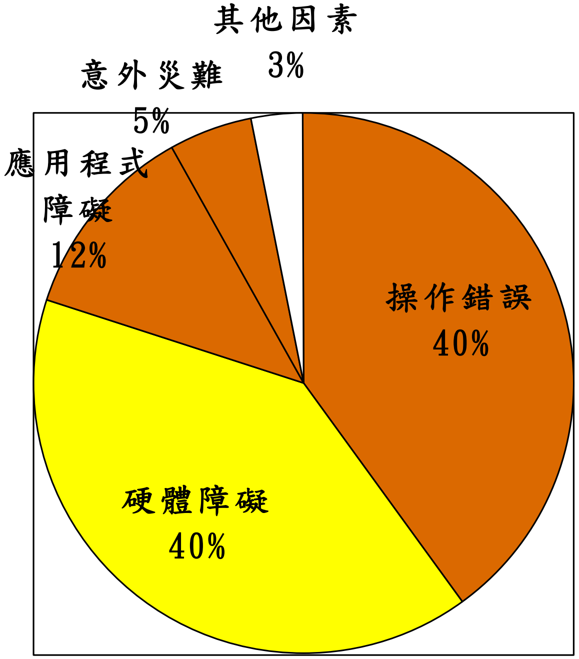


Source: © Contingency Planning Research, a division of Eagle Rock Alliance, West Orange, NJ, www.eaglerockalliance.com.

災難發生後造成系統中斷時間分析

造成系統中斷，各因子所佔中斷時間(Downtime)之比率分析

- 40% operation error
- 40% hardware error
- 12% application failure
- 5% disaster
- 3% other environmental



80%的Downtime是因為人為操作錯誤或是硬體障礙，這也是為何要強調Procedure & Plan

ITSCM Planning

災難復原計畫的規劃

5

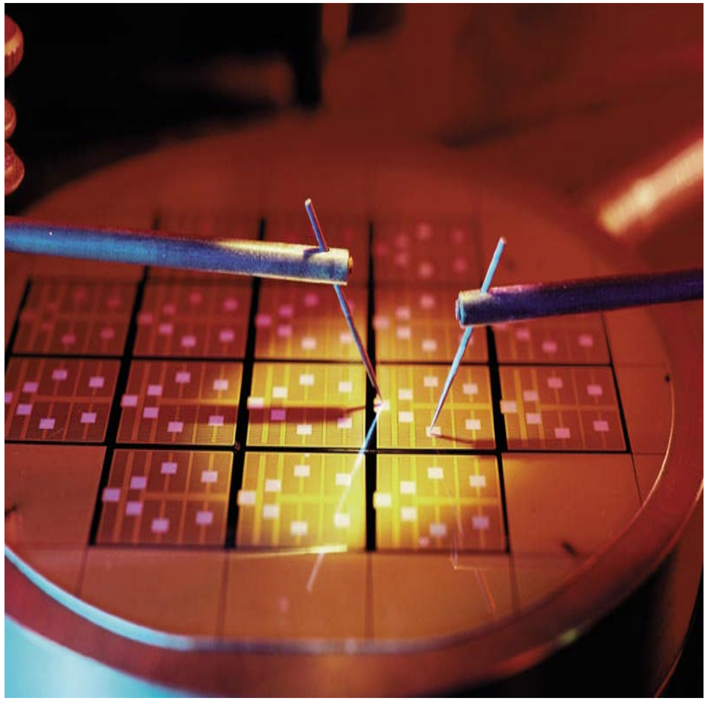
營運持續計畫涵蓋的內容

DRP 災害復原

使用者復原計畫

緊急應變

危機處理 **(Communication & PR)**



Disaster Recovery Plan (DRP)

災難復原計畫中Key elements是什麼？

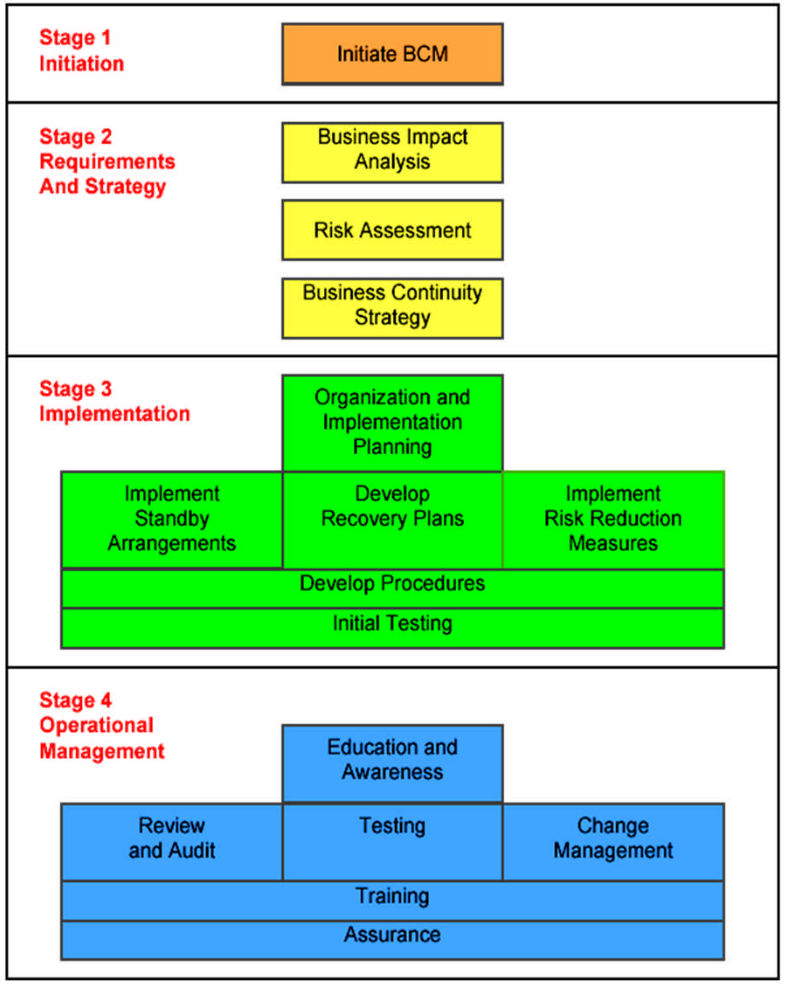
- 明確的目標定義
  - including recovery goals and objectives
- 啟動權定義
  - WHO can activate the team's recovery plan
- 工作組織
  - title and functions of each recovery team or team member
- 資訊文件
  - specific methods for contacting recovery team members and alternates, vendors, support agencies, suppliers, and all those with whom special disaster contracts and agreements are in effect
- 明確範圍定義
  - specific to disaster reactions (which disaster types will or will not be addressed in the plan)
- 落實訓練
  - Training of employees in recovery procedures
- 計畫檢討
  - Ongoing review and revision of the plan

災難復原規劃 ***(Disaster Recovery Plan)***

災難復原規劃要做什麼？

- 找到業務上的脆弱點
  - *identifying* business vulnerabilities
- 評估業務中斷的影響
  - *assessing* the impact of a disruption,
- 訂定一套風險控制的策略
  - *developing* a strategy to manage the risks and
- 製訂出一套整合的營運持續計劃
  - *implementing* an integrated business continuity program

ITSCM (IT Service Continuity Management)



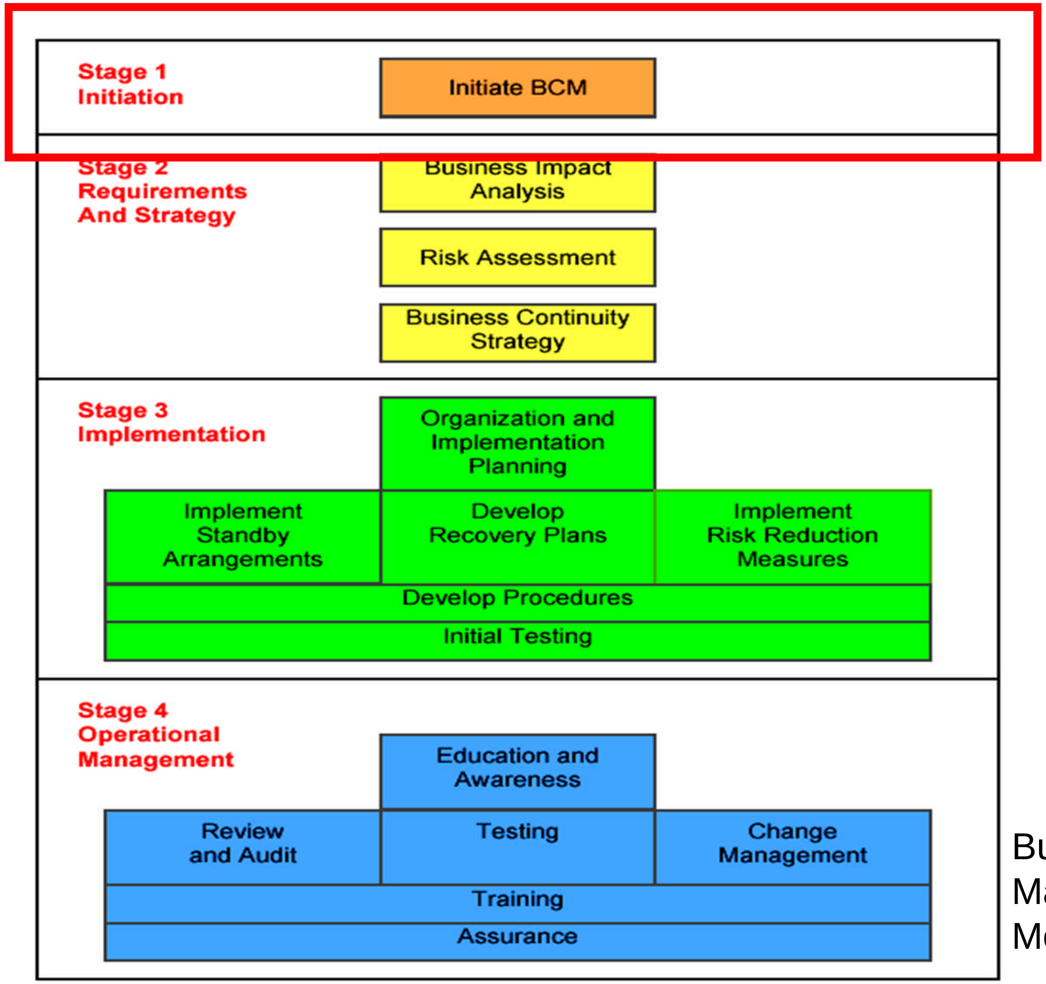
Phase One 1 Define ITSCM Scope, policy

Phase Two 2 診斷及分析，備援方案及架構 （Assessments and Analyses , Solutions Architecture & Strategy ）

Phase Three 3 導入管理Implementation Management（Implementation）

Phase Four 4 測試及維護Testing & Maintenance（Operational & Management）

Stage 1 – Initiation



Business Continuity Management Process Model

Initiate BCM

- Policy setting
- Specify terms of reference and scope
- **Allocate Resources**
- Define the project organization and control structure
- Agree project and quality plans

Scope of ITSCM

Business processes to be covered and their IT support requirements

Risks that need to be addressed

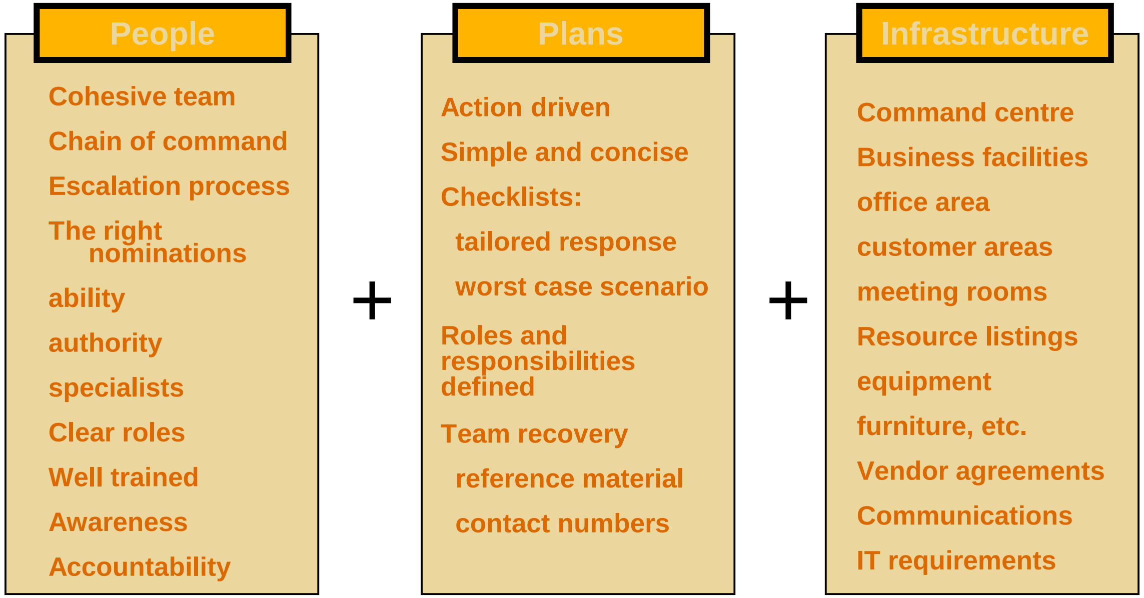
- Risks '**in scope**'
  - Risks that could result in serious disruption to business processes
  - Poison Gas, Power Loss, Earthquake, Bomb….
- Risks '**out of scope**'
  - Longer-term risk e.g. changes in business direction, diversification, restructuring, etc.
  - **Minor technical faults** (for example, non critical disk failure). Covered by Incident Management and Availability Management

Business Continuity Capabilities

Our approach focuses on three key areas which are essential ingredients in achieving an effective continuity capability.

People + Plans + Infrastructure = Continuity Capability

We consider each of these three categories in turn in order to help our clients to develop their own effective and sustainable business continuity capabilities.



People

Cohesive team

Chain of command

Escalation process

The right nominations

ability

authority

specialists

Clear roles

Well trained

Awareness

Accountability

+

Plans

Action driven

Simple and concise

Checklists:

tailored response

worst case scenario

Roles and responsibilities defined

Team recovery

reference material

contact numbers

+

Infrastructure

Command centre

Business facilities

office area

customer areas

meeting rooms

Resource listings

equipment

furniture, etc.

Vendor agreements

Communications

IT requirements

Phase I – 產出

DRP第一章

- 災難復原計畫的標的
  - 範疇(Scope)
    - Risk in Scope
    - XX資訊系統或XX業務
    - 發生XX之危險事件(hazard)或災難(disaster)時之因應計畫

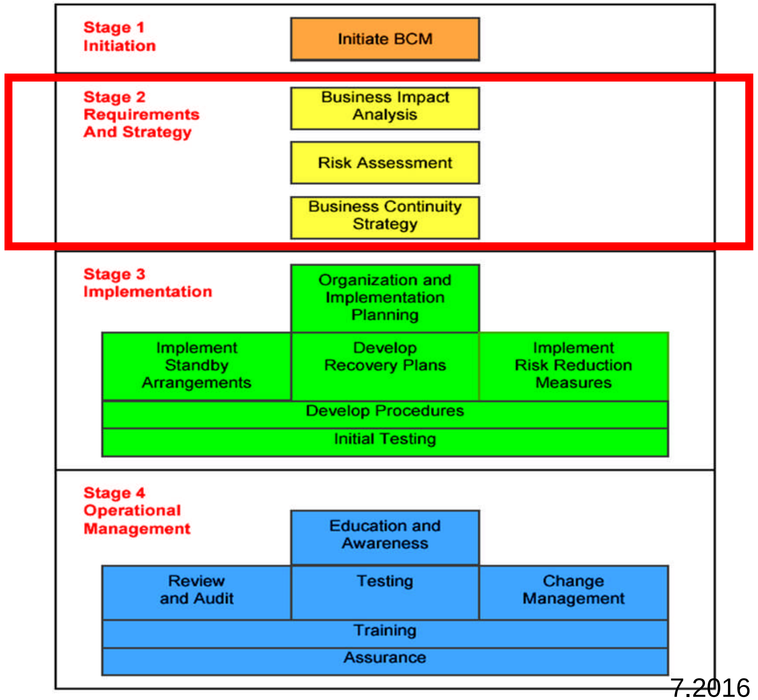
Stage 2 –
Requirements and Strategy

Requirements

- Business Impact Analysis (BIA)
- Risk Assessment

Strategy

- Business Continuity Strategy



Business Impact Analysis

- Identify critical business process

- Identify potential damage or loss that may result in a **disruption to critical** business process

- Identify the form that damage or loss may take

Phase II – 需求分析與策略定義

Requirements Analysis and Strategy Definition

- 定義災難復原規劃打算在什麼災難情形下，企業營運可以恢復運作，以及其中斷營運的損失

需求分析(Requirements Analysis)

- perform Business Impact Analysis (BIA) and risk assessment
- Identify preventive controls

策略定義(Strategy Definition)

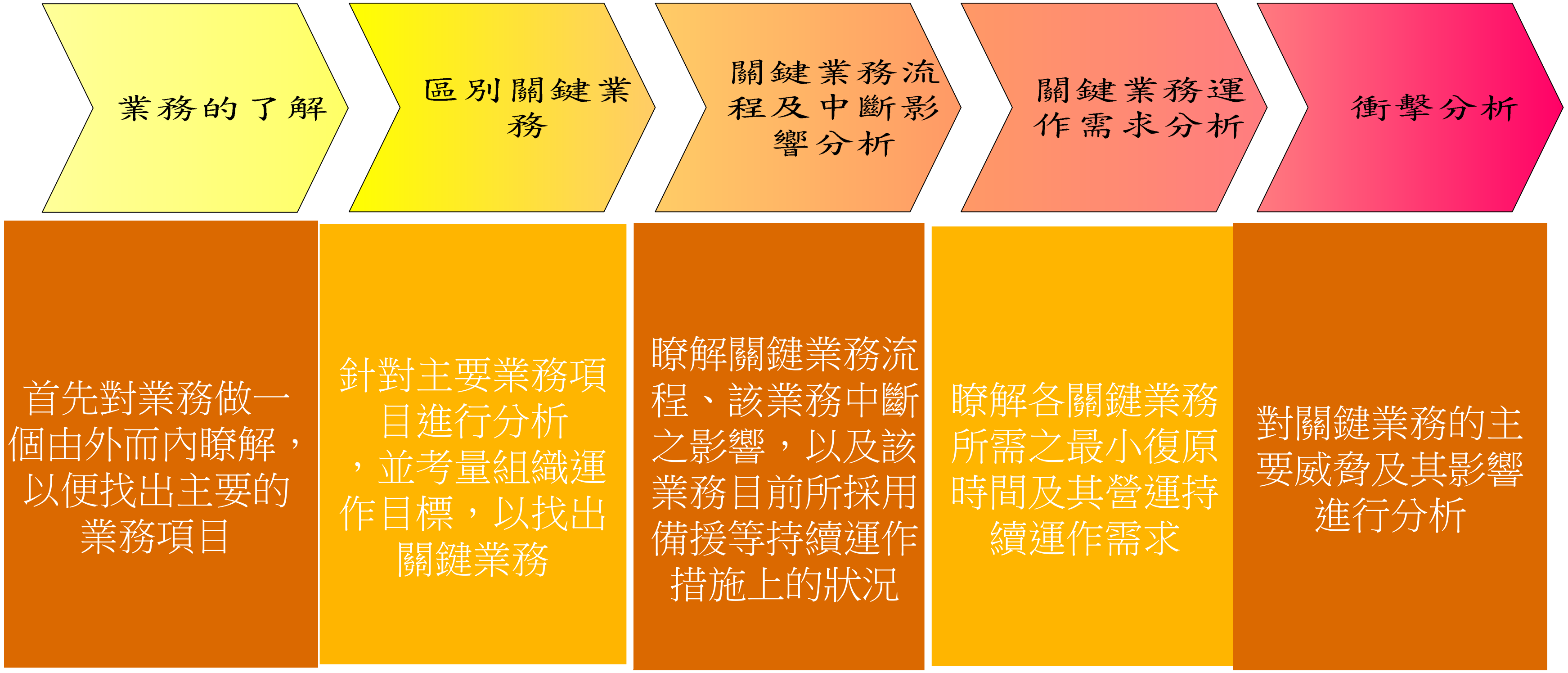
- determine and agree on Risk reduction measures and recovery options to support the requirements

BIA (Business Impact Analysis)

風險評估(Risk Assessment)

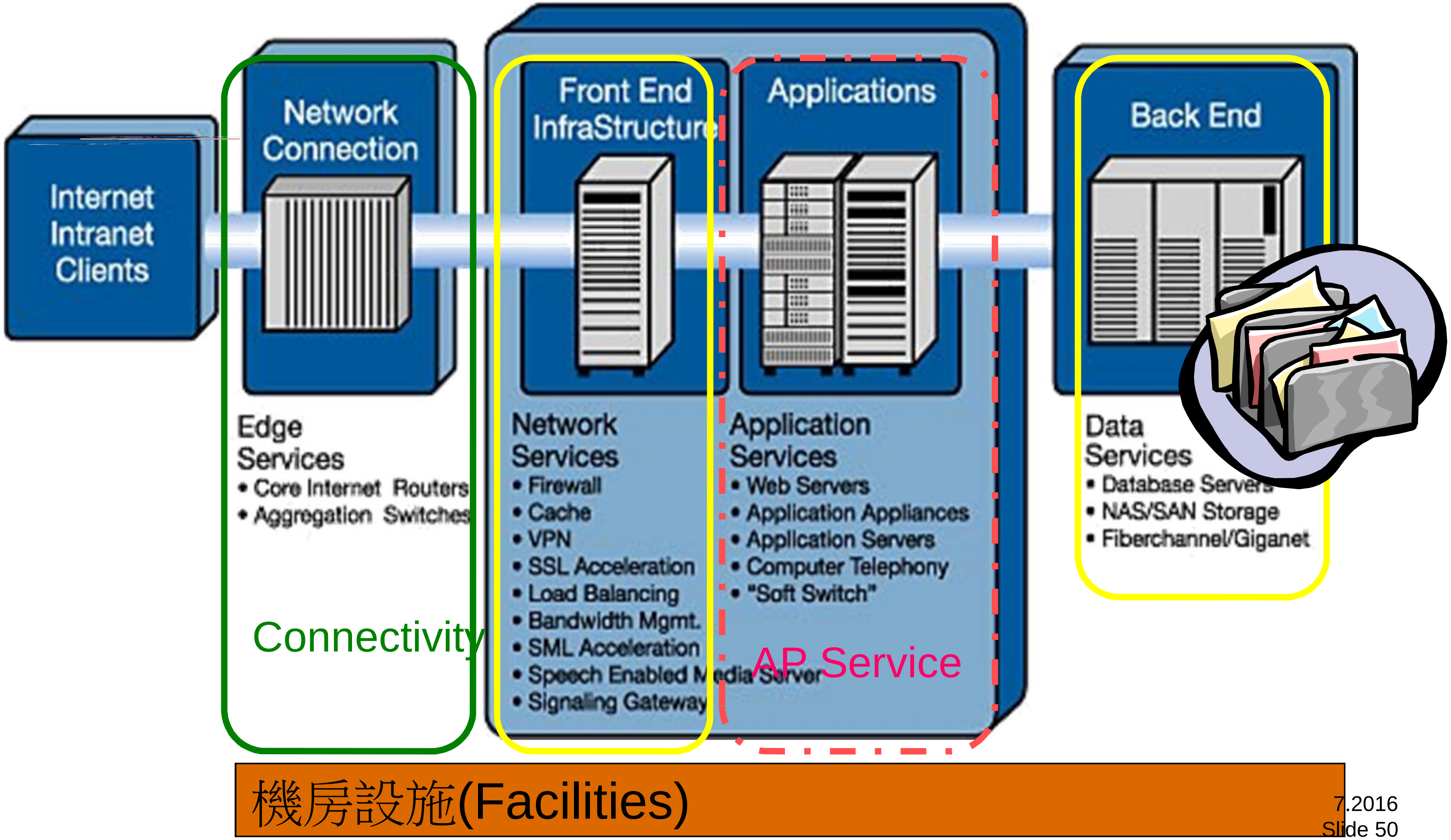
- 找出風險(Identify risks, know your vulnerability)
- 列出風險損害(Cost of risk)
  - Financial loss, damage reputation, regulatory breach
- 風險控制對策(Strategy)
- 風險依據控制法分類(Group by control element)
- 控制風險之成本分析(Cost of protecting, likes preventive control)
- 訂定各風險之優先順序(Priority)
- 列出不可控制之因子(Out-of-control variances)
- 選擇可執行/值得執行的控制對策

BIA流程

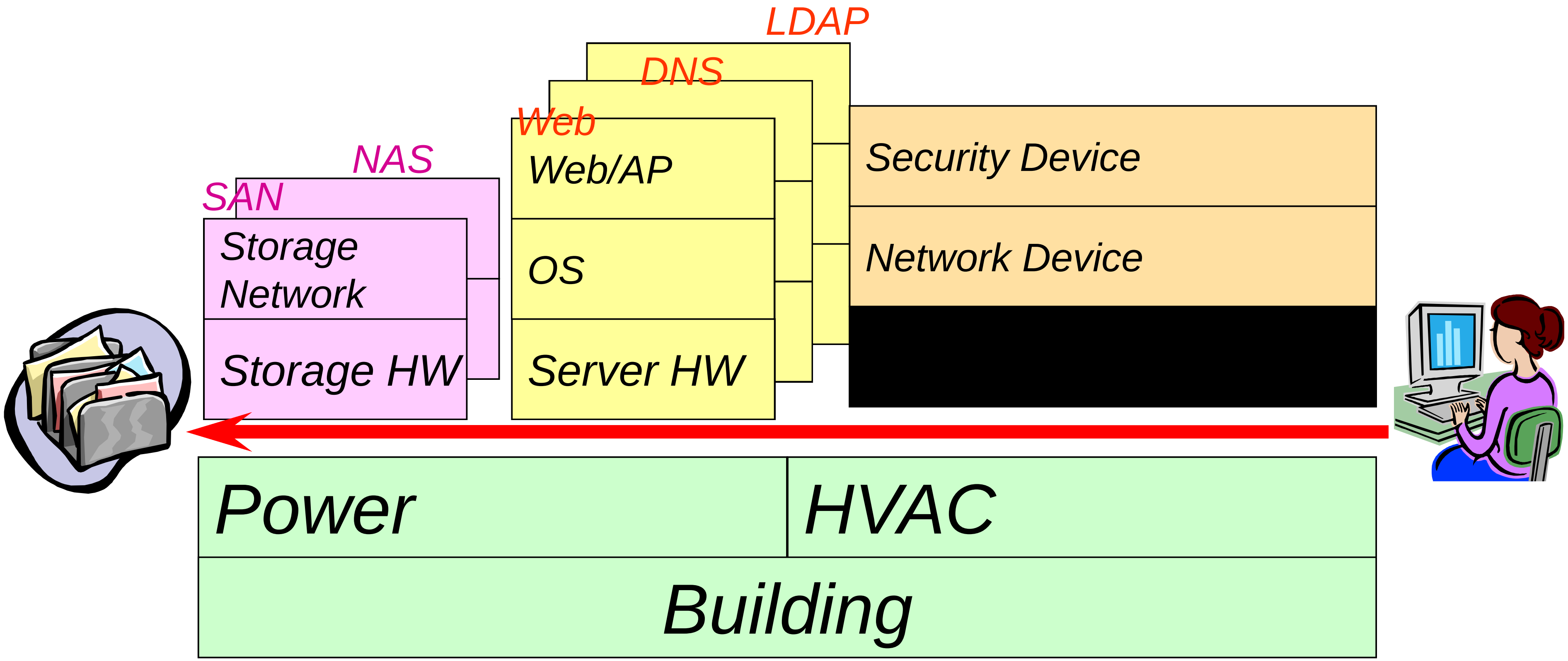


業務的了解	區別關鍵業務	關鍵業務流程及中斷影響分析	關鍵業務運作需求分析	衝擊分析
首先對業務做一個由外而內瞭解，以便找出主要的業務項目	針對主要業務項目進行分析，並考量組織運作目標，以找出關鍵業務	瞭解關鍵業務流程、該業務中斷之影響，以及該業務目前所採用備援等持續運作措施上的狀況	瞭解各關鍵業務所需之最小復原時間及其營運持續運作需求	對關鍵業務的主要威脅及其影響進行分析

分析重要資訊系統的備援標的物



IT資訊系統架構中的各個組成



LDAP

DNS

Web

Web/AP

OS

Server HW

NAS

SAN

Storage Network

Storage HW

Security Device

Network Device

[redacted]

Power

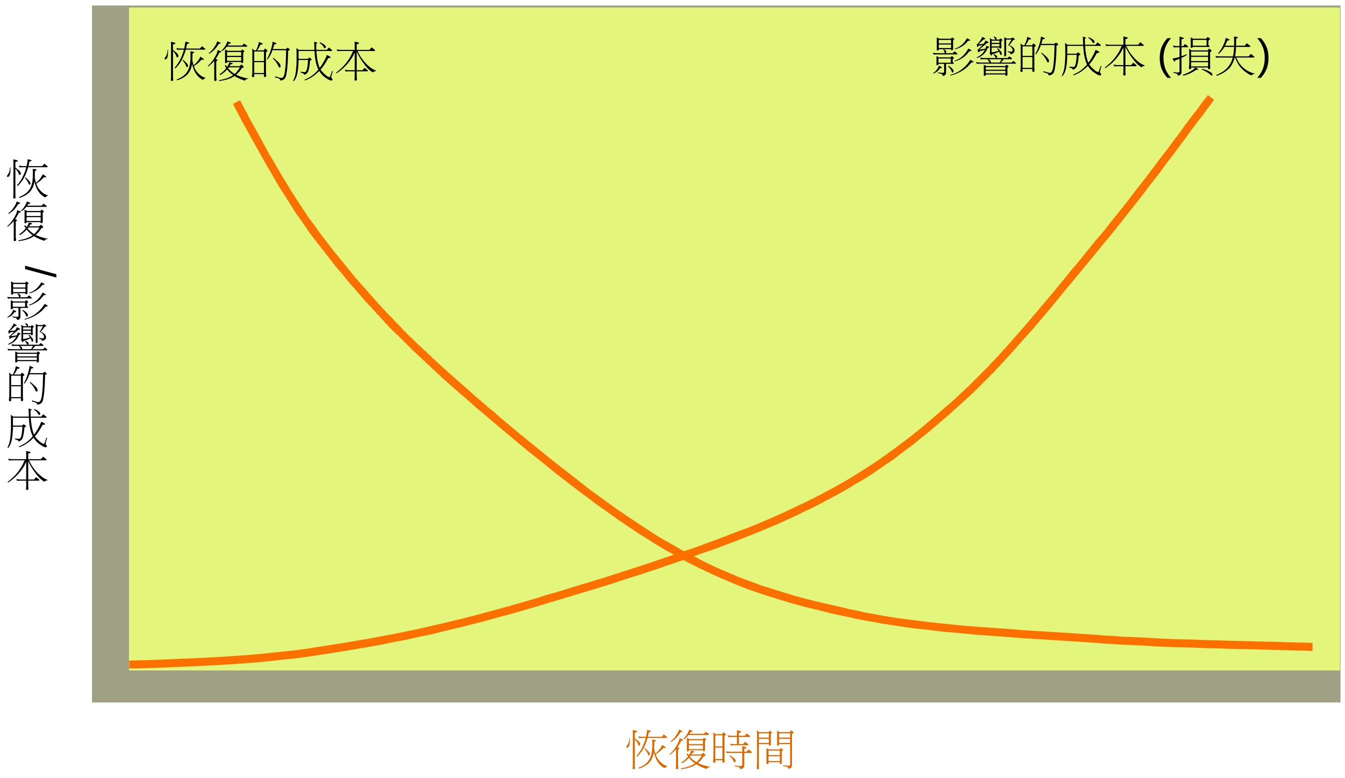
HVAC

Building

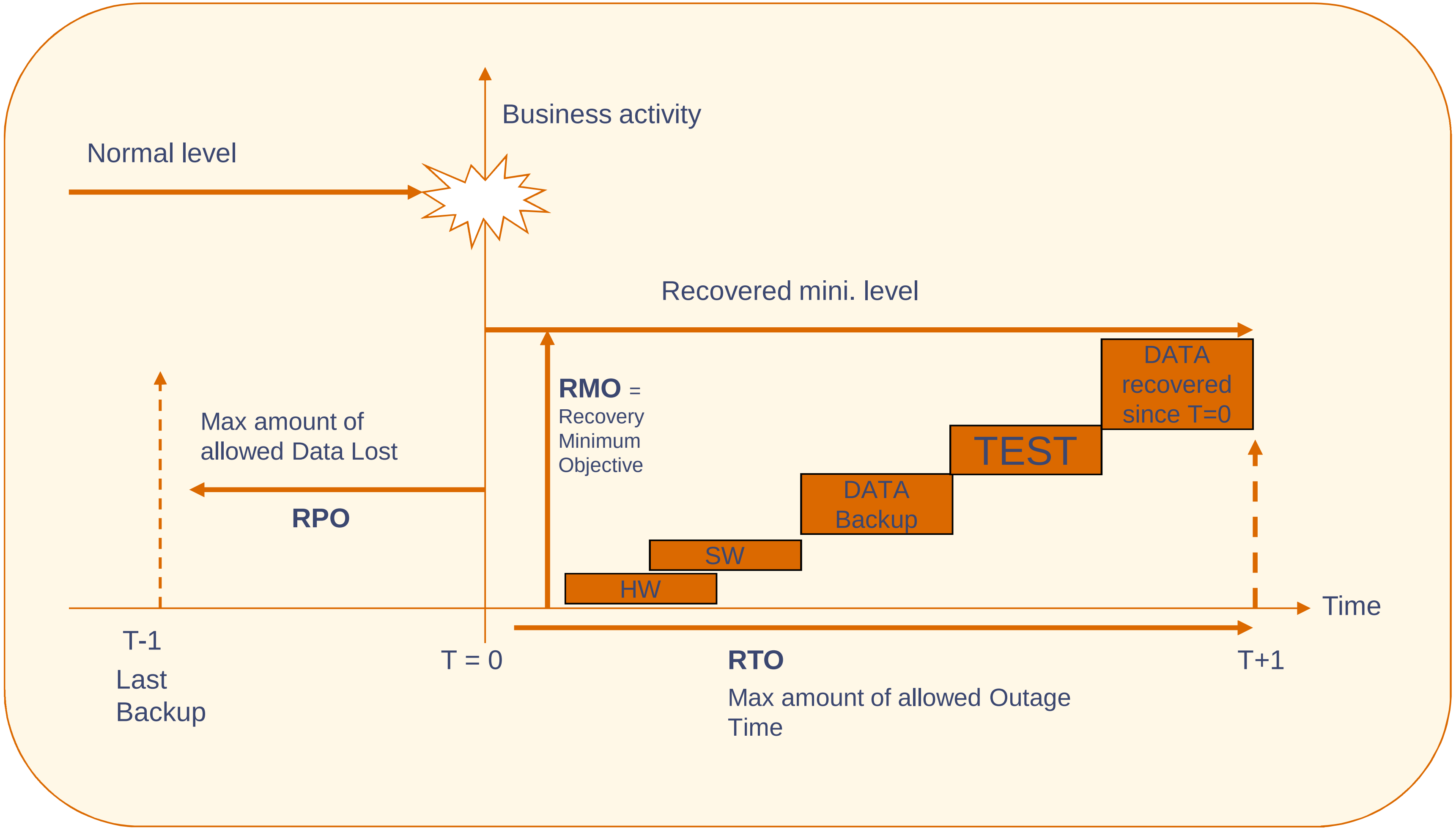
Any component's outage will cause interrupt of service. Every component needs backup/recovery.

關鍵業務運作需求分析 (cont.)

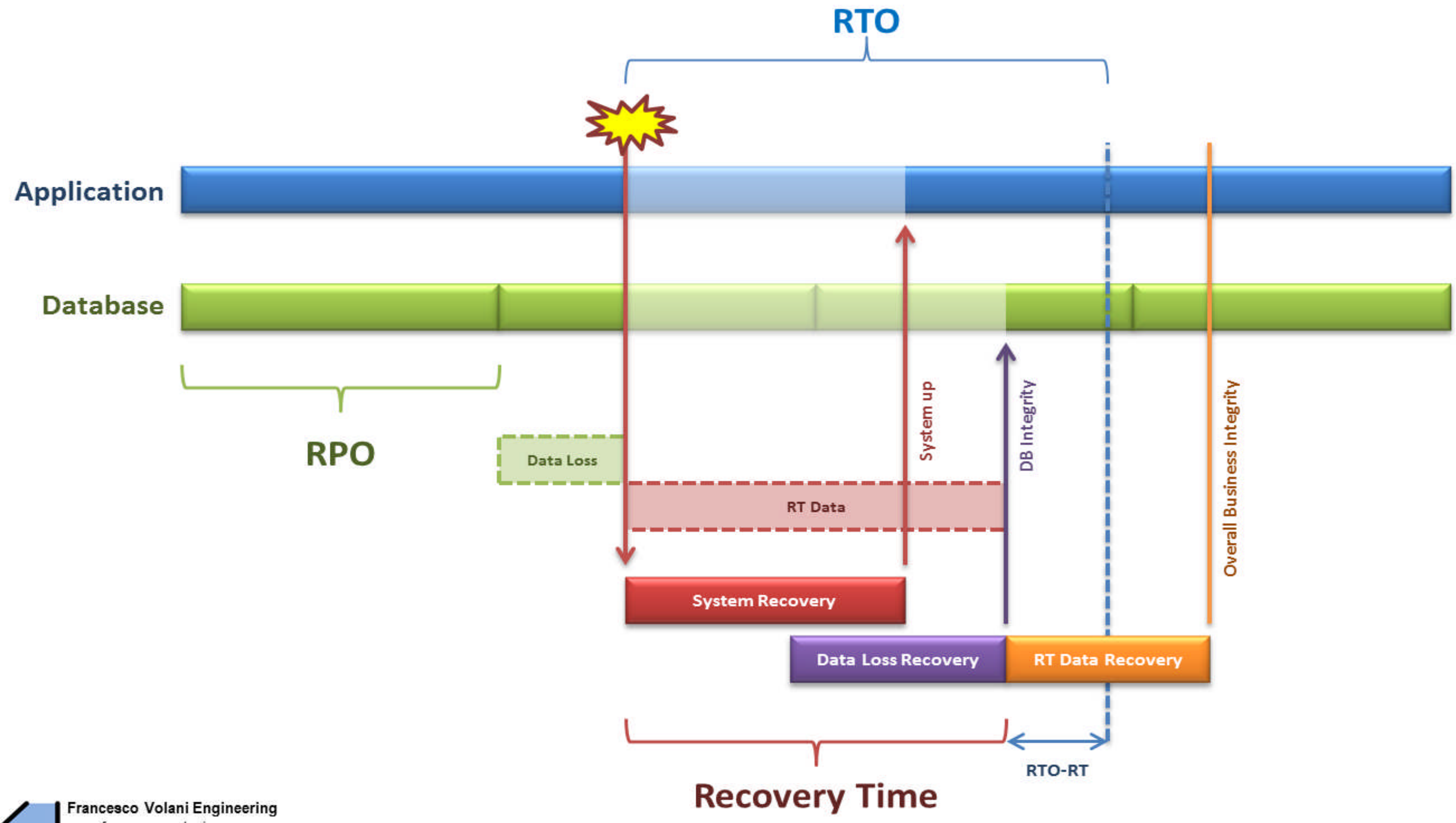
決定關鍵的恢復時間點之分析圖



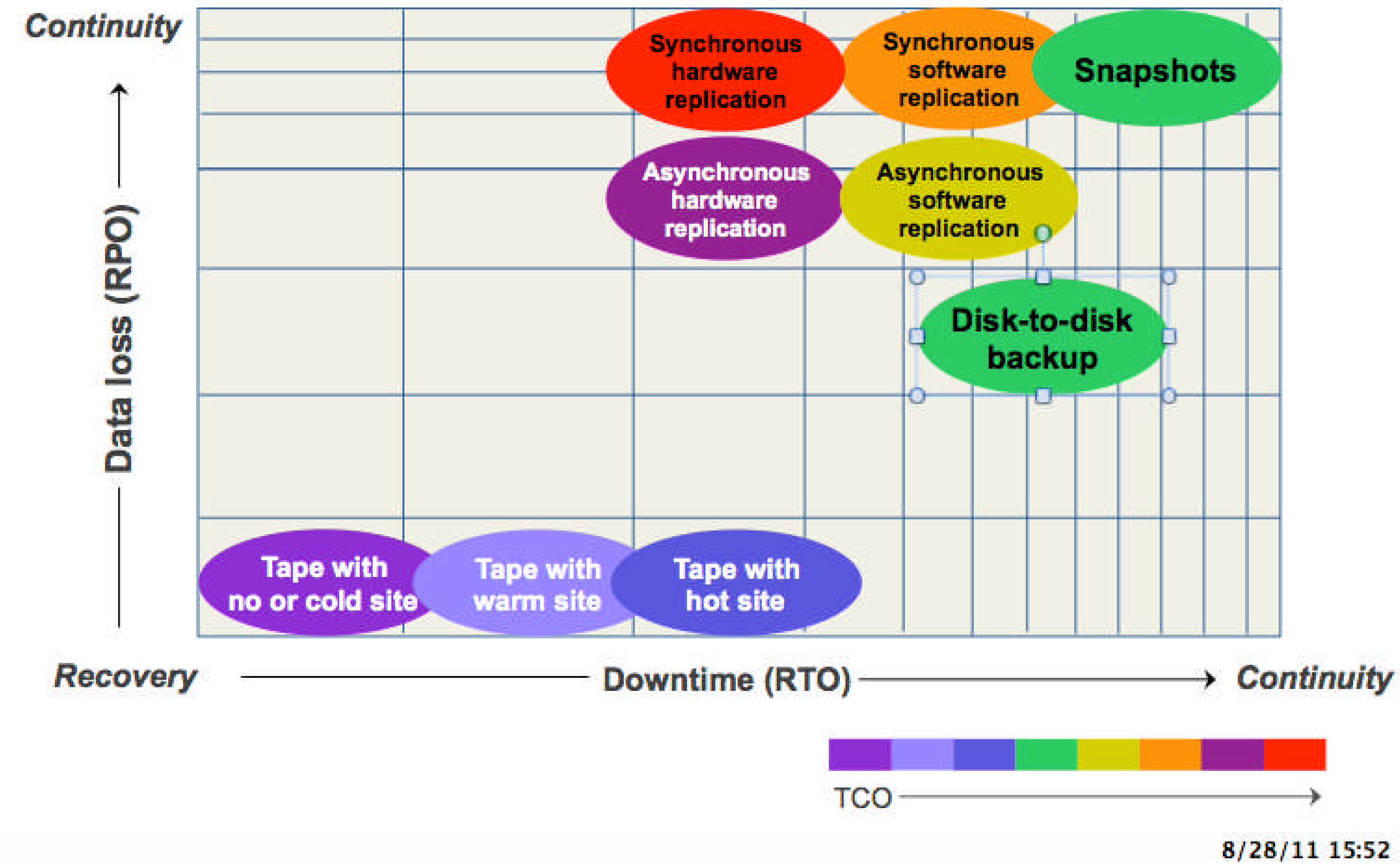
Determination of Recovery Point Objective (RPO) and Recovery Time Objective (RTO)



RPO/RTO



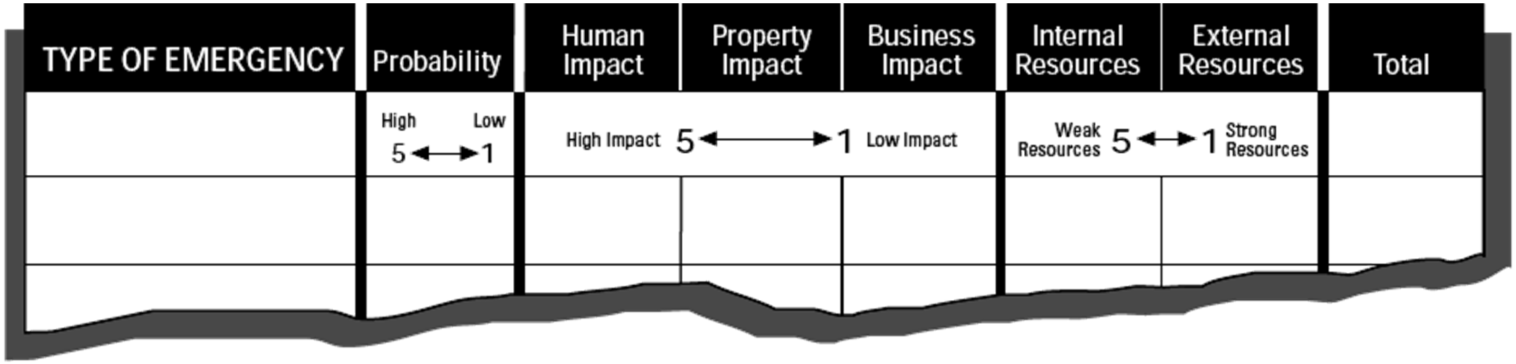
Francesco Volani Engineering
www.francescovolani.org


Continuity
Data loss (RPO)
Synchronous hardware replication
Synchronous software replication
Snapshots
Asynchronous hardware replication
Asynchronous software replication
Disk-to-disk backup
Tape with no or cold site
Tape with warm site
Tape with hot site
Recovery
Downtime (RTO)
Continuity
TCO
8/28/11 15:52

http://seacliffpartners.com/wordpress/?p=706

風險評估(Risk Assessment)

風險評估評分範例



TYPE OF EMERGENCY	Probability	Human Impact	Property Impact	Business Impact	Internal Resources	External Resources	Total
	High Low 5 ←→ 1	High Impact 5 ←→ 1 Low Impact			Weak Resources 5 ←→ 1 Strong Resources		

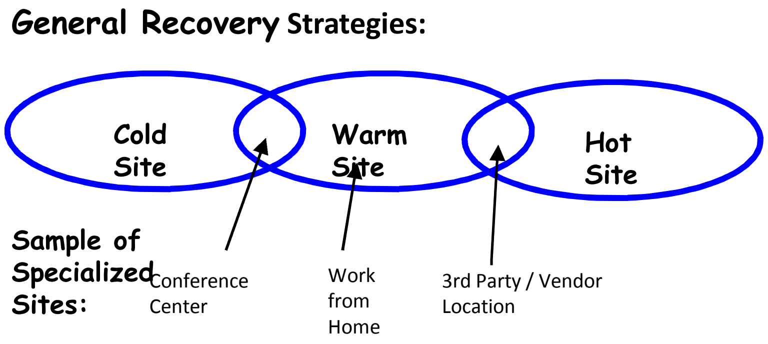
Business Continuity Strategy

Risk Reduction Measures, e.g.

- A comprehensive backup and recovery strategy, including off-site storage
- The elimination of single points of failure
- Outsourcing services to more than one provider
- Greater security controls

Recovery Options, e.g.

- Do nothing
- Manual Workarounds
- Reciprocal arrangements
- Gradual Recovery (cold standby)
- Intermediate Recovery (warm standby)
- Immediate Recovery (hot standby)


General Recovery Strategies:
Cold Site
Warm Site
Hot Site
Sample of Specialized Sites:
Conference Center
Work from Home
3rd Party / Vendor Location

風險控制方法或策略範例

週期性備份資料、AP與OS等重要資訊資產

重要系統或元件採冗餘(Redundant)設計

系統組態設定與需求資訊文件化保存

主中心系統與備援中心系統輪流切換運作

適當的機房基礎設施的管理與監控

預留較大的 Capacity (like DDoS)

風險控制方式之選擇範例

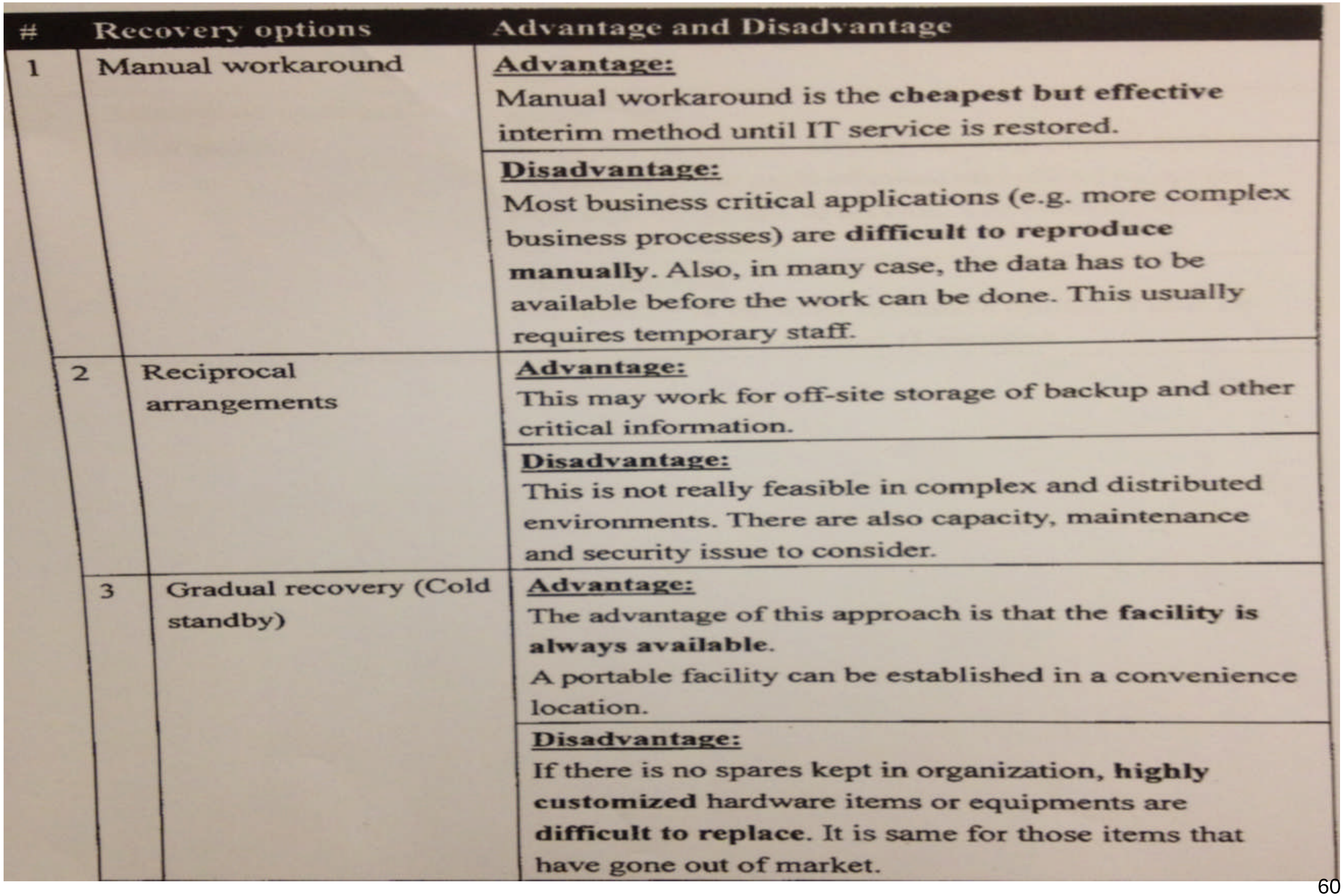
備份考量

- 媒體存放於那裡
- 什麼資料需要備份
- 多久備份一次
- 當事件發生時，需要多快取得備份媒體
- 授權誰可以存取備份媒體
- 多久可以從備份媒體中取回資料

選擇

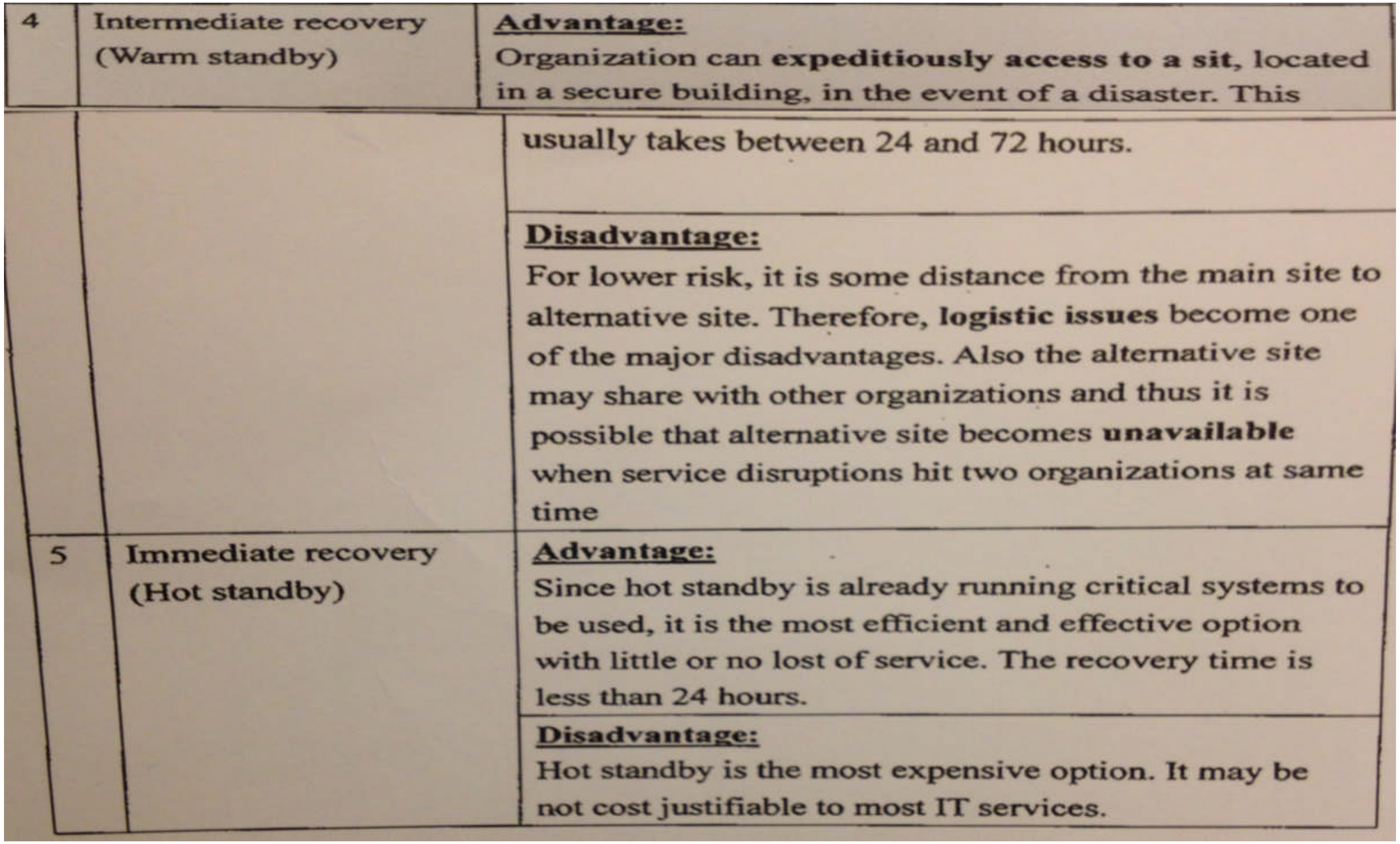
- 磁帶備份、磁碟備份
- 差異性備份(Incremental backup)、Full Backup
- 同步、非同步
- File level、Block Level

Business Continuity Strategy



#	Recovery options	Advantage and Disadvantage
1	Manual workaround	**Advantage:** Manual workaround is the **cheapest but effective** interim method until IT service is restored.
		Disadvantage: Most business critical applications (e.g. more complex business processes) are **difficult to reproduce manually**. Also, in many case, the data has to be available before the work can be done. This usually requires temporary staff.
2	Reciprocal arrangements	**Advantage:** This may work for off-site storage of backup and other critical information.
		Disadvantage: This is not really feasible in complex and distributed environments. There are also capacity, maintenance and security issue to consider.
3	Gradual recovery (Cold standby)	**Advantage:** The advantage of this approach is that the **facility is always available**. A portable facility can be established in a convenience location.
		Disadvantage: If there is no spares kept in organization, **highly customized** hardware items or equipments are **difficult to replace**. It is same for those items that have gone out of market.

Business Continuity Strategy



4	Intermediate recovery (Warm standby)	**Advantage:** Organization can **expeditiously access to a sit**, located in a secure building, in the event of a disaster. This usually takes between 24 and 72 hours.
		Disadvantage: For lower risk, it is some distance from the main site to alternative site. Therefore, **logistic issues** become one of the major disadvantages. Also the alternative site may share with other organizations and thus it is possible that alternative site becomes **unavailable** when service disruptions hit two organizations at same time
5	Immediate recovery (Hot standby)	**Advantage:** Since hot standby is already running critical systems to be used, it is the most efficient and effective option with little or no lost of service. The recovery time is less than 24 hours.
		Disadvantage: Hot standby is the most expensive option. It may be not cost justifiable to most IT services.

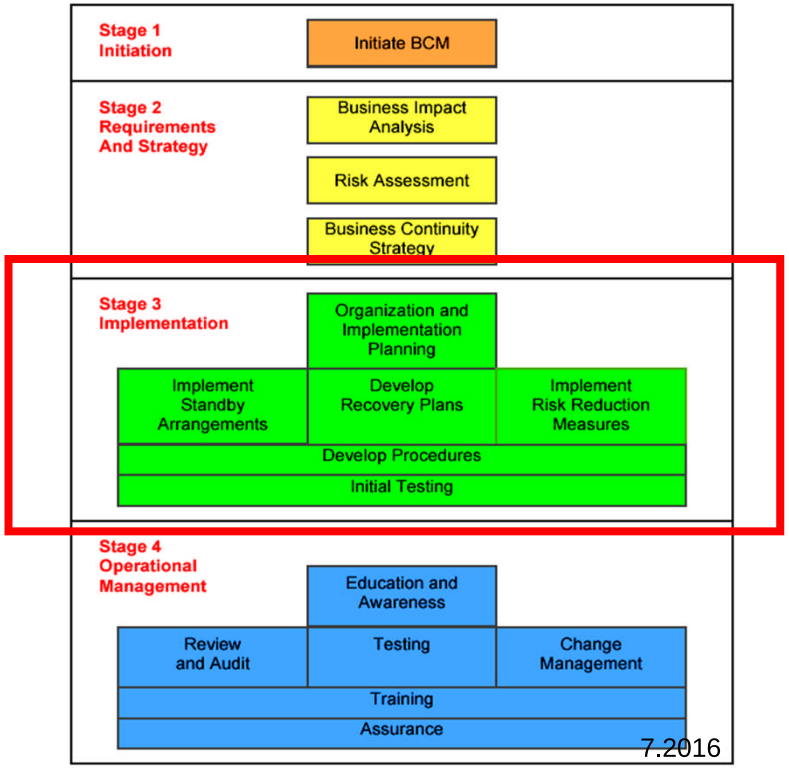
Phase II – 產出

DRP第二章

- 企業營運影響分析(風險評估(BIA)報告)
  - 損害分析
    - 什麼風險→造成什麼損失(Lost impact analysis)
  - 期望目標(多久可以達到復原,回復所需時間)
    - XX資訊系統在YY事件(Thread)下，回復所需時間
    - WW業務系統在ZZ事件(Thread)下，回復所需時間
  - Recommended recovery priorities & strategies
    - 各系統或業務的復原優先順序
    - 所採用的復原策略為何

Stage 3 - Implementation

- Organization & Implementation planning
- Implement risk reduction measures
- Implement stand-by arrangements
- Develop ITSCM plans
- Develop **procedures**
- Initial testing



Phase III – 執行 (Implementation)

- 成立工作小組，並訂定災難復原執行計畫 (establish the organization and develop implementation plans)

- 設立待命備份資源(implement Stand-by arrangements)— Checklist/Support Information

- 設立降低風險措施(implement risk reduction measures）

- 訂定災難復原計畫(develop IT recovery plans)

- 訂定標準作業程序(develop Standard Operating Procedures (SOPs))-- (Step-by-Step Procedure)

- 進行災難復原計畫測試-計畫演練(undertake initial tests)

BCM工作組織

1. 確立人員及執掌

2. 管理階層

- 災害評估
- 監督

3. IT部門

- 網路
- 系統及AP
- 作業程序

4. 業務單位

- 採購
- 生產
- 銷售

5. 公關

- 最新情況

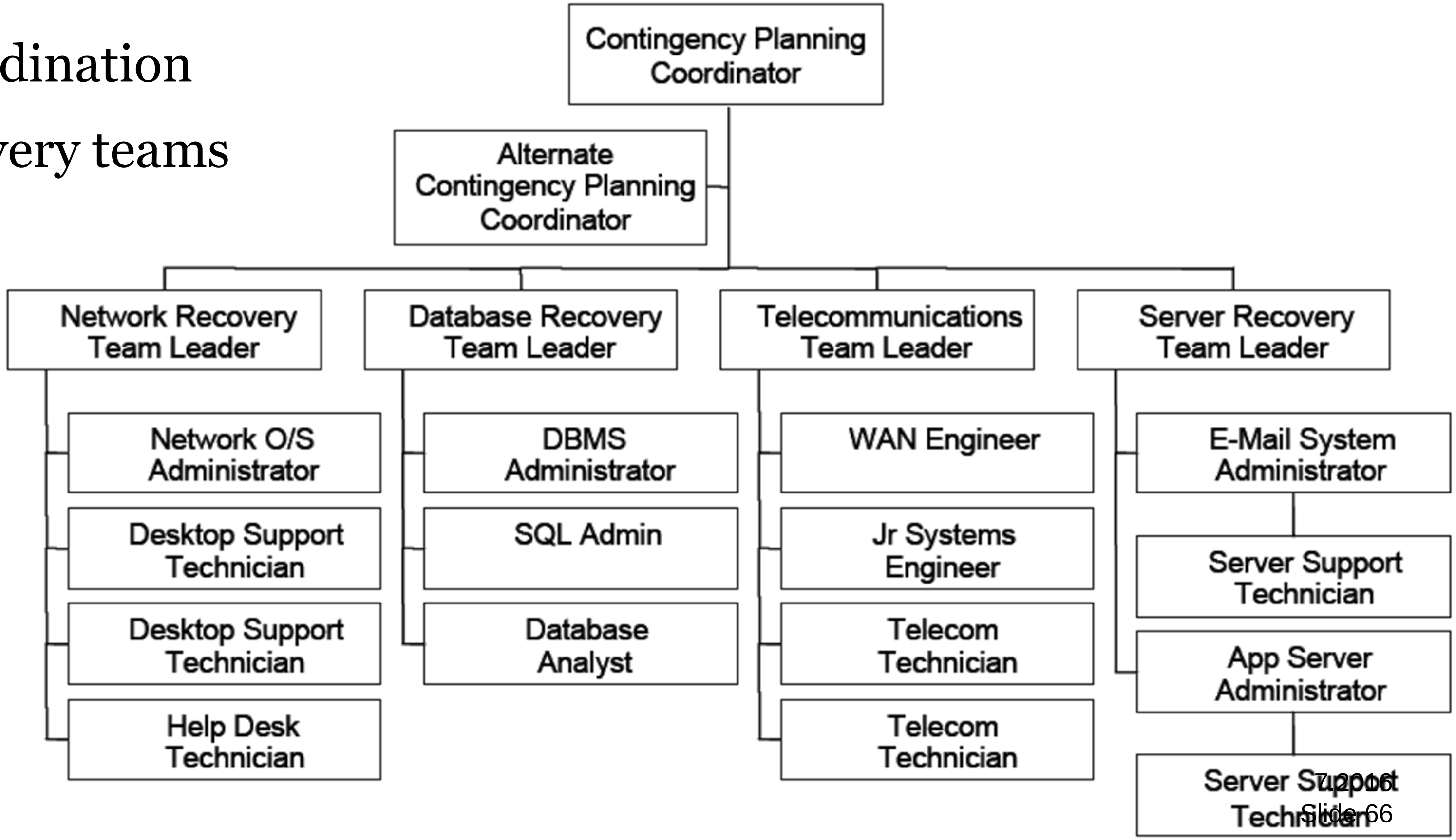
Organization Planning

- Three-tier structure
  - Executive
  - Co-ordination
  - Recovery teams

IT工作組織範例

Organization Planning

- Three-tier structure
  - Executive
  - Co-ordination
  - Recovery teams



Contingency Planning Coordinator

Alternate Contingency Planning Coordinator

- Network Recovery Team Leader
  - Network O/S Administrator
  - Desktop Support Technician
  - Desktop Support Technician
  - Help Desk Technician
- Database Recovery Team Leader
  - DBMS Administrator
  - SQL Admin
  - Database Analyst
- Telecommunications Team Leader
  - WAN Engineer
  - Jr Systems Engineer
  - Telecom Technician
  - Telecom Technician
- Server Recovery Team Leader
  - E-Mail System Administrator
  - Server Support Technician
  - App Server Administrator
  - Server Support Technician

IT工作小組範例

Senior Management Official

Management Team

Damage Assessment Team

Operating System Administration Team

Systems Software Team

Server Recovery Team (e.g., client server, Web server)

LAN/WAN Recovery Team

Database Recovery Team

Network Operations Recovery Team

Application Recovery Team(s)

Telecommunications Team

Hardware Salvage Team

Alternate Site Recovery Coordination Team

Original Site Restoration/Salvage Coordination Team

Test Team

Administrative Support Team

Transportation and Relocation Team

Media Relations Team

Legal Affairs Team

Physical/Personnel Security Team

Procurement Team (equipment and supplies)

人員工作代理制度

Implement

Implement risk reduction measures, e.g.

- Installation of UPS and back-up power
- Fault tolerant systems
- Offsite storage and archiving
- Disk mirroring
- Spare equipment

Implement stand-by arrangements, e.g.

- Negotiating for third party recovery facilities and entering into a contractual arrangement
- Preparing and equipping the stand-by accommodation
- Purchasing and installing stand-by computer systems

Develop ITSCM Plans

Implementation Planning

Co-ordination Plan	Recovery Plan
. Emergency Response Plan . Damage Assessment Plan . Salvage Plan . Vital Records Plan . Crisis Management and Public Relations Plan	. Accommodation and Services Plan . Computer Systems and Network Plan . Telecommunication Plan . Security Plan . Personnel Plan . Finance and Administration Plan

Develop ITSCM Procedures

Co-ordination Plan:

- Notification/Activation Phase (災難通告及復原啟動)
  - Notification Procedure
    - 災難發生時通知誰，做什麼…；復原啟動時通知誰，做什麼…
    - 建立通報表(Tree狀或是表格式)
  - 損害評估(**Damage assessment**)
    - 提供是否啟動DR之決策參考
  - 啟動復原(**Plan activation**)(由決策者發佈災難復原啟動)

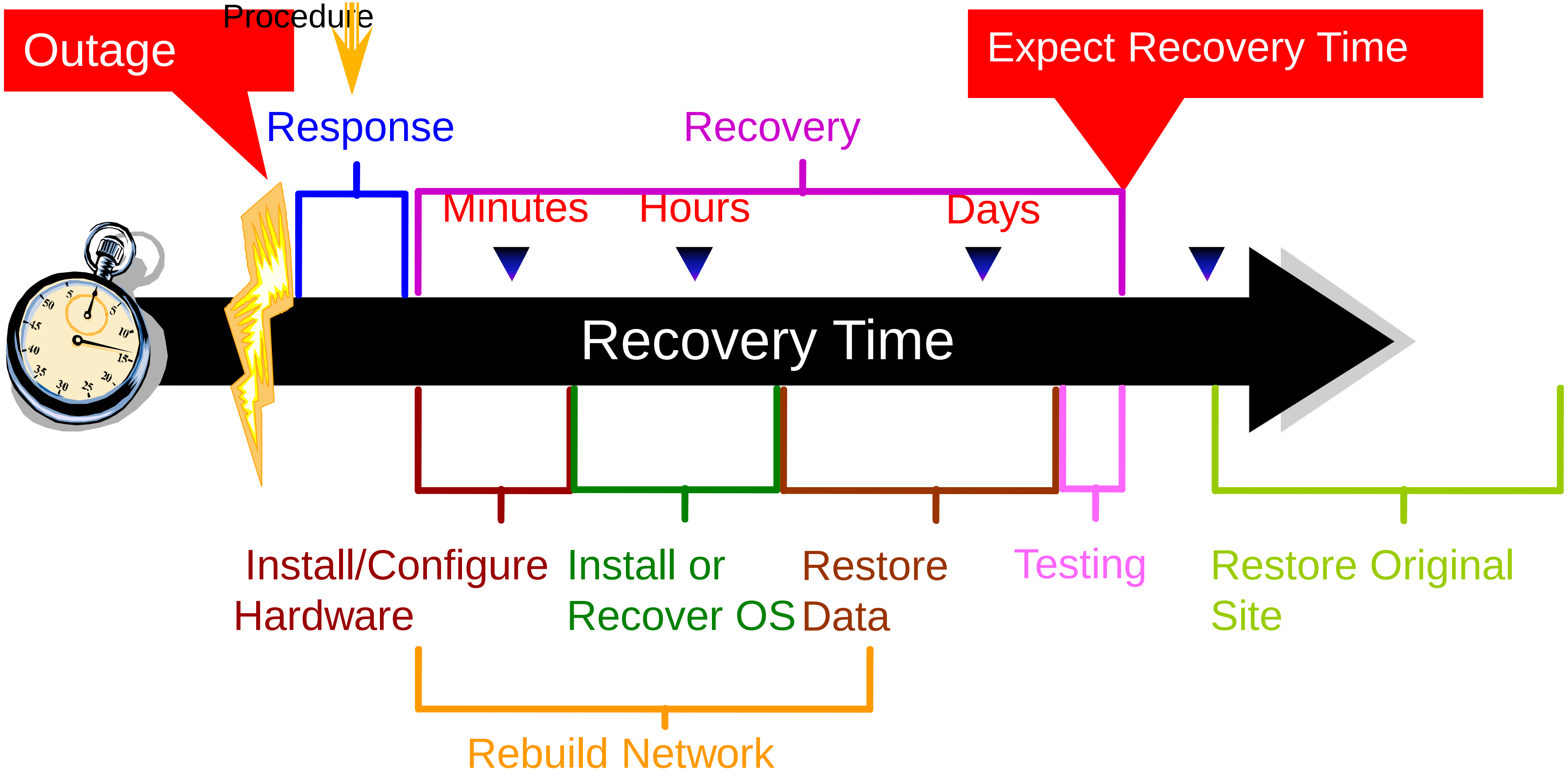
Recovery Plan:

- Recovery Phase
  - 復原順序(Sequence of recovery activities)
  - 復原程序(Recovery procedure)

- Reconstitution Phase
  - Restore original site
  - Test system
  - Terminate operations

Recovery Process

取得足夠資訊以判斷啟動何種災難復原，需制定Emergency Response Procedure



Outage

Expect Recovery Time

Response

Recovery

Minutes

Hours

Days

Recovery Time

Install/Configure Hardware

Install or Recover OS

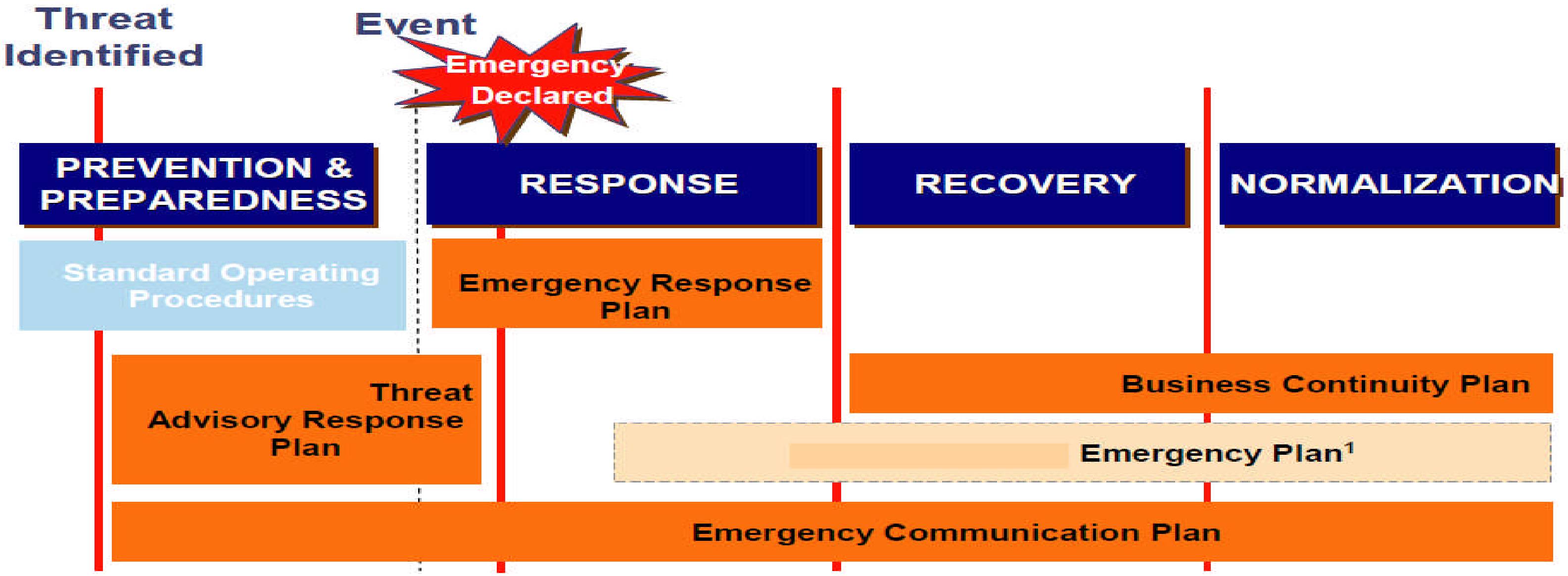
Restore Data

Testing

Restore Original Site

Rebuild Network

BCP will be activated if an emergency is declared as level 2 or above



Threat Identified

Event

Emergency Declared

PREVENTION & PREPAREDNESS

RESPONSE

RECOVERY

NORMALIZATION

Standard Operating Procedures

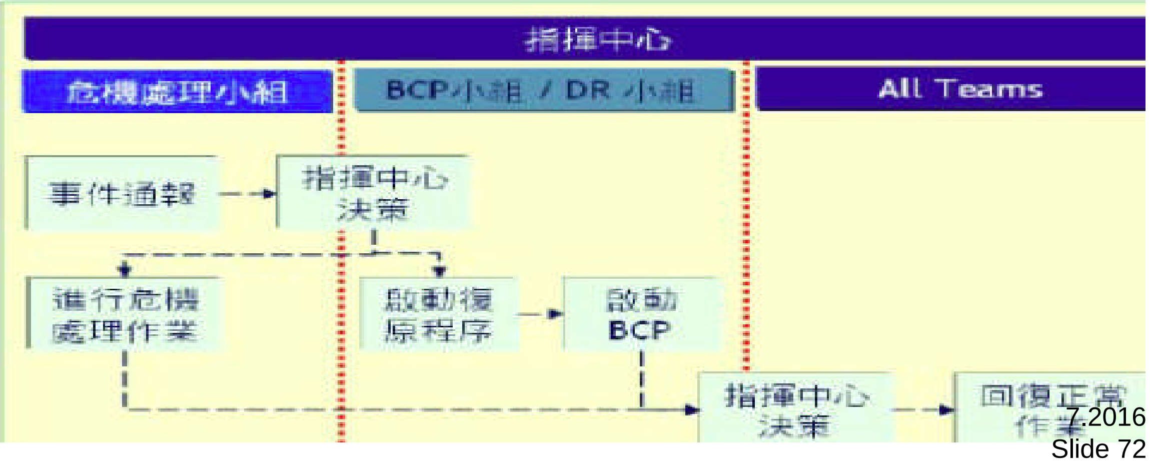
Emergency Response Plan

Threat Advisory Response Plan

Business Continuity Plan

Emergency Plan[1]

Emergency Communication Plan



損害評估 (Damage assessment)

事件原因

可能擴大影響層面、損害或中斷期間

事件影響範圍

實體設施狀態(機房、電力、空調狀態)

IT資產設備狀態(運作、停止運作或部分運作狀態)

IT資產損害種類(淹水、火/熱、電力突波)

需替換設備清單(軟硬體設備或零件)

預估回復正常運作所需時間(或稱可能服務中斷之時間)

啟動復原(Plan activation)

當損害評估(Damage assessment)的報告顯示已經達到啟動復原計畫時的條件(Criteria)

- 不同系統的啟動條件定義不同
- 條件(Criteria)範例
  - 影響設施程度範圍
  - 影響系統程度範圍
  - 影響重要系統資源(Critical system or asset)
  - 預估服務中斷時間

啟動復原計畫的決策者需要在DRP中定義

- 需要授權定義決策者之權利義務
- 依序接班備援人員的順序也要定義

通告災難復原小組(Notify Recovery Teams)

復原順序(Sequence of recovery activities)

依據系統重要的優先順序(Priority)來進行復原

- 以BIA的分析來做為排序參考

有些關聯性(Correlated)順序必須考量

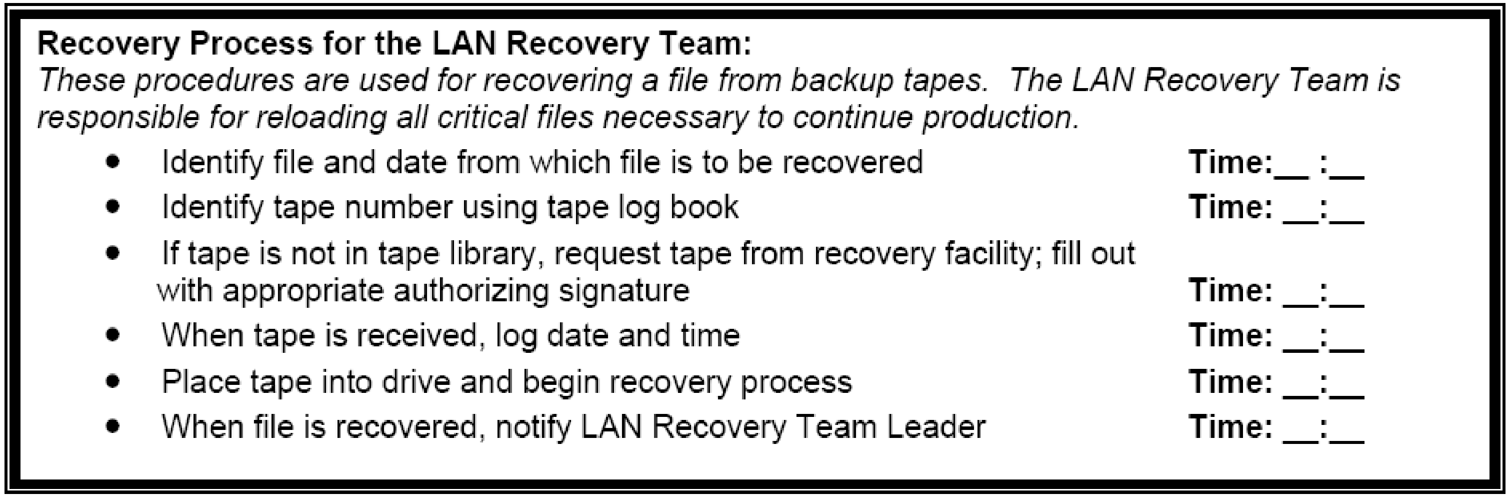
- OS->AP->Data
- Network->(Firewall,…Security Device)->DNS->Server
- LDAP->AP Server
- 設備採購->運送交貨->安裝上線
- 復原計畫無法如期達成時的備份計畫
    - 計畫A->計畫B->計畫C

復原程序 (Recovery Procedure)

由各自的復原工作小組執行其權責工作，各小組有其各自的復原程序，程序應包括

- 獲得授權進行損害設施或設備修復
- 通知該損害影響範圍的內外部相關人事
- 取得必須的資源(office supplies and work space)
- Installation and testing of replacement hardware and networks
- 取得並載入備份媒體
- Restoration of software and data 重裝OS與AP軟體 & 重新載入資料
- 測試復原系統之功能(包括資訊安全管控機制測試)
- 連線上網以及與其他系統間連線測試
- 成功地運轉復原系統各項功能並進行後續維運
- Different time zones in a multinational organization
- Business cut-off points

復原程序範例



Recovery Process for the LAN Recovery Team:
These procedures are used for recovering a file from backup tapes. The LAN Recovery Team is responsible for reloading all critical files necessary to continue production.

- Identify file and date from which file is to be recovered **Time:__ :__**
- Identify tape number using tape log book **Time: __:__**
- If tape is not in tape library, request tape from recovery facility; fill out with appropriate authorizing signature **Time: __:__**
- When tape is received, log date and time **Time: __:__**
- Place tape into drive and begin recovery process **Time: __:__**
- When file is recovered, notify LAN Recovery Team Leader **Time: __:__**

Initial Testing

Time objects

Staff preparedness and awareness

Staff duplication and potential over commitment of key resources

The responsiveness, effectiveness and awareness of external parties

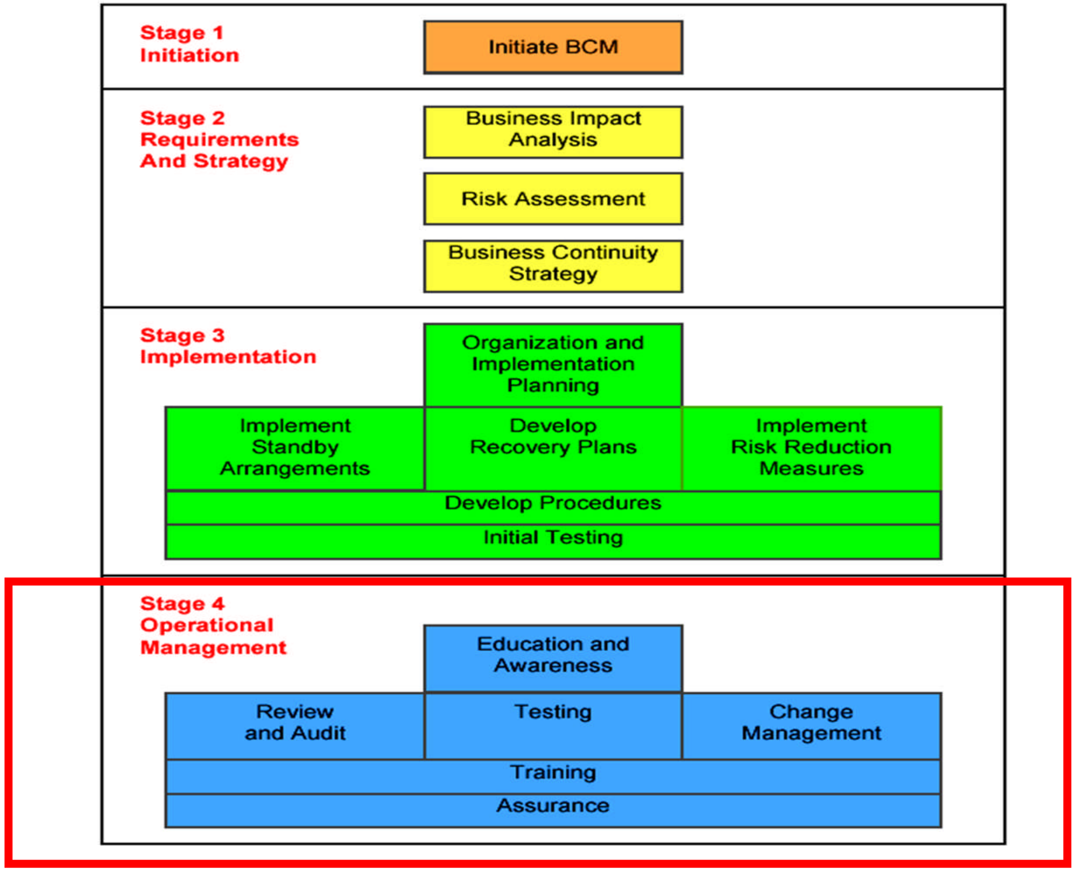
Phase III – 產出

DRP第三章

- 災難復原計畫
  - 復原組織架構圖：分工與責任範圍
  - 復原組織下各成員聯絡方式之清單
  - 其他相關的支援廠商聯絡清單
- 損害評估程序
- 復原程序
  - 標準操作程序(SOP)
  - 相關檢查核對清單(Check List)
    - 災難復原時所需之設備與設施需求檢查清單，包括名稱/型號、版本、規格、數量等等資訊
- 與其他支援廠商的SLA
- 異地備援機房交通路線圖、聯絡電話、食宿資訊

Stage 4 – Operational Management

To maintain the ITSCM as part of business as usual.



Phase IV – 維運管理 (1/2)

Operational Management

- Education and awareness
  - 包括內部相關單位組織及外部協力廠商或是(外包人員)。讓災難復原計畫中的日常工作整合進入各員工或是委外人員之工作項目中，融入日常例行公事(讓員工養成習慣)。
- Training
  - 標準作業程序(SOP)的操作訓練
- Review and Audit
  - 定期Review災難復原計畫，及稽核Education and awareness, Training之執行記錄，確保災難復原計畫日常工作之正常運作

Phase IV – 維運管理(2/2)

- Testing (演練)
  - 除了第一次建置完的災難復原計畫的測試，後續需要定期(一年至少一次)演練測試災難復原計畫。災難復原計畫之演練測試需要在主管或是稽核單位的監督下執行。
- Change Management(異動管理)
  - 依據演練測試結果以及Review災難復原計畫有不符合原目標時，需要有一套計畫修正(修訂)的管理辦法，以確保修正後之災難復原計畫依舊可由相關單位(人員)，依據相對的SOP進行日常維護、緊急應變或是災難復原。
- Assurance
  - 所有的維護管理工作，都是以確保災難復原計畫持續符合企業永續運作的計畫目標，並且所有日常維護管理工作都是相關

計畫測試(演練)的範圍

System recovery on an alternate platform from backup media

Coordination among recovery teams

Internal and external connectivity

System performance using alternate equipment

Restoration of normal operations

Notification procedures.

演練方法

沙盤推演(Classroom Exercises) (Desk Check/Checklist)

- 看過所有程序書的程序，沒有實際的操作，紙上談兵式地推演備援是否可以成功

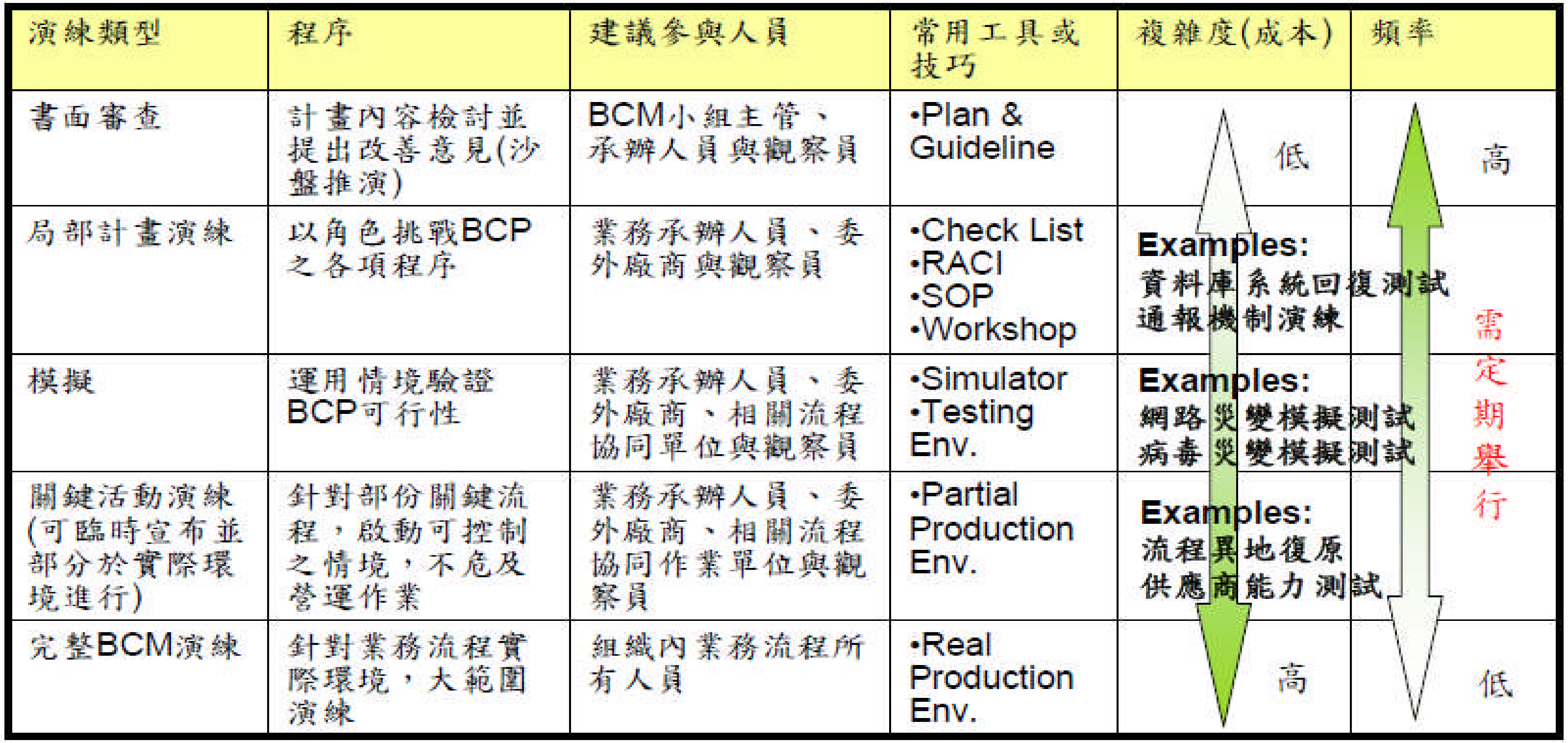
實際演練

- 實際模擬事件發生，真實切換系統(cutover)或是異地演練(relocation)

5種演練類型

於演練計畫中可規劃採用下列演練類型:

- 各演練類型均有優點與其限制，可視資源、成熟度等狀況混合進行
- 欲於實際環境進行演練前，需經過書面等類型演練，並確認各項準備措施之完整性
- 部分類型演練可事先規劃後，臨時公佈
- 參與人員與使用工具可彈性調整



演練類型	程序	建議參與人員	常用工具或技巧	複雜度(成本)	頻率
書面審查	計畫內容檢討並提出改善意見(沙盤推演)	BCM小組主管、承辦人員與觀察員	•Plan & Guideline	低	高
局部計畫演練	以角色挑戰BCP之各項程序	業務承辦人員、委外廠商與觀察員	•Check List •RACI •SOP •Workshop	Examples: 資料庫系統回復測試 通報機制演練	需定期舉行
模擬	運用情境驗證BCP可行性	業務承辦人員、委外廠商、相關流程協同單位與觀察員	•Simulator •Testing Env.	Examples: 網路災變模擬測試 病毒災變模擬測試	
關鍵活動演練(可臨時宣布並部分於實際環境進行)	針對部份關鍵流程，啟動可控制之情境，不危及營運作業	業務承辦人員、委外廠商、相關流程協同作業單位與觀察員	•Partial Production Env.	Examples: 流程異地復原 供應商能力測試	
完整BCM演練	針對業務流程實際環境，大範圍演練	組織內業務流程所有人員	•Real Production Env.	高	低

Phase IV – 產出

DRP第四章

- 訓練計畫
  - 災難復原計畫宣導(Awareness)
  - 損失評估程序及災難復原程序等訓練
- 日常維運管理程序
  - 災難復原計畫異動管理
- 稽核與演練計畫(驗證計畫)
  - 標準操作程序(SOP)
  - 相關檢查核對清單(Check List)
    - 災難復原時所需之設備與設施需求檢查清單，包括名稱/型號、版本、規格、數量等等資訊
- 與其他支援廠商的SLA
- 異地備援機房交通路線圖、聯絡電話、食宿資訊

Q & A