談恩隆事件對資訊安全秩序的影響

主講人：李俊隆

- 法斯特科技（股）公司 －資訊處副總經理
- 美商 **CTS Components Taiwan Co., － Information System Manager**

Sarbanes-Oxley Act OVERVIEW

- 何謂恩隆事件
- 沙班尼斯－歐克斯里法案
- SOX404 管理階層內控評估
- Ｃ公司實務面研討

何謂『恩隆事件』

- 美國恩隆公司(Enron Corp.)成立於1985年，爲全世界最大的能源公司
- 連續六年榮獲美國《財星雜誌》(Fortune)評定爲『最具創意企業』
- 2000年名列美國前五百大企業第七位
- 2000年榮獲英國《金融時報》(Financial Time) 頒發『年度能源公司獎』及『最大膽的成功投資獎』

何謂『恩隆事件』(續)

- 華爾街分析師推薦「買進」投資標的
- 美各州退休金力捧之所愛
- 倒閉前，名列美國第七大企業，獲利超過 1000 億美元，擁有 2 萬名員工遍佈全球
- 爲美國人最愛任職的百大企業

美國資本市場『九一一』事件翻版

- 2001年12月2日恩隆無預警地宣佈破產
- 633億美元之資產成爲當時美國史上最大規模的破產聲請保護案
- 美林證券 (Merrill Lynch)、花旗集團 (Citigroup)、大通摩根 (J.P. Morgan Chase)及安達信會計事務所 (Arthur Andersen LLP)無一幸免被牽累

五大會計師事務所

- 1990年代併購風氣盛行，最後成爲五大會計師事務所：
- Arthur Andersen LLP (勤業)
- PricewaterhouseCoopers LLP (資誠)
- KPMG LLP (安侯建業)
- Deloitte & Touche LLP (眾信)
- Emst & Young LLP (致遠)

恩隆事件對金融風暴影響

- 公司員工、退休基金、投資人、融資銀行、華爾街分析師及信用評機構等
- 美國股市一落千丈，創 1997年來最低
- 創1930年代經濟大恐慌之後「新政時期」七十年來建構之公司治理法制及市場管理制度崩潰
- 美股市在後半年內跌掉15兆美元，相當全台灣53年之產值

1930年代經濟大蕭條時期

- 1929-1932年間美國史上經濟大蕭條期間，道瓊指數下跌了九成
- 1933 美政府國會製訂:
  The Securities Act of 1993 (1993證券法)
  The Securities Exchange Act of 1994
  (1994證交法）
- 使美國成爲全世界最有效率的資本市場

其他企業醜聞之骨牌效應

- 2002年上半年頻傳財務弊案之其他企業:
  - 全錄 (Xerox)
  - 泰科 (Tyco)
  - 環球通訊 (Global Crossing)
  - 阿德菲爾通訊 (Adephia)
  - 默克藥廠 (Merck)
  - 英克隆 (ImClone)
  - 南健 (HealthSouth)

再破紀錄－美史上最大宗破產案

- 2001年1月28日環球通訊 (Global Crossing) – 全球電信龍頭之一，通訊網路連結高達27國兩百座城市，聲請破產保護, 約270億美元
- 2002年7月21日世界通訊(WorldCom) – 全美第二大長途電話公司，聲請破產保護金額高達 1,070億美元

企業改革法案之催生

- 於投資大眾、輿論及美國會期中選舉壓力下，以幾近全數通過迅速制定沙班尼斯－歐克斯里法案 (簡稱 SOX)
- 美國布希總統於2002年7月30日簽署《The Sarbanes-Oxley Act of 2002》其法案編號爲「H.R.3763」係由參議員 Paul S. Sarbanes 及眾議員 Michael G. Oxley 爲原提案人而名之

The Sarbanes-Oxley Act

- SOX涉及層面廣泛, 舉凡公司治理的內控機制到外控機制皆在規範之列,包括:
  - 強化公司管理階層之經理責任及獨立董事、審計委員會之監督義務
  - 會計師專業之業務限制及管理
  - 相關會計審計相關準則之制定、修正或採行
  - 律師、證券分析師、投資銀行、信用評等機構等，全納入規範

The Sarbanes-Oxley Act (續)

- SOX共有 11 章 66 條款 157 小項
- 第一章：設立《公開發行公司會計監督委員會 – PCAOB》接受證券交易委員會 (SEC) 監督並賦予非營利法人，並非美國政府一部分亦非其代理機關
- SOX104規定對會計師事務所之檢查次數, 含外國部分適用

The Sarbanes-Oxley Act (續)

- 第二章規定查核人員之獨立性：
  - 業者與客戶間的內部稽核委外服務禁止
  - 過去五年內不可同一簽證會計師為之
  - 利益迴避－旋轉門條款，實際會計執行人一年內不得為該同屬會計師事務所者

The Sarbanes-Oxley Act (續)

- 第三章企業責任之規範:
  - SOX302: 財務報表之企業責任，報告簽署，國外子公司同時適用性
- 第四章強化財務揭露:
  - 增訂利益迴避條款, 禁止對管理階層爲私人借貨, 含子公司貨款于董事、高階經理人或相當職務者

The Sarbanes-Oxley Act (續)

- SOX404: 管理階層有關內部控制之評估:
  - 負建立並維持適當之內部控制結構及程序之義務 (針對財務報告)
  - 內部控制結構及程序之有效性評估 (針對會計年度)
  - 上述須爲會計事務所進行證明並提出報告

The Sarbanes-Oxley Act (續)

- 第五章規範分析師之利益衝突:
- 第六章規範《證交會 (SEC)》職權
- 第七章爲研究報告之要求
- 第八章探究企業之刑事詐欺責任:
  - SOX806 吹哨者保護條款，明令不得對提供線索協助偵查員工有任何相對不利之舉動

The Sarbanes-Oxley Act (續)

- 第九章規範白領階級之加重刑罰：
  - SOX906 規範財務報告責任者，違反保證規定之相關刑罰
- 第十章爲企業所得稅之申報
- 第十一章企業詐欺責任之規範:
  - 公務進行中意圖損害文書之完整性或減低其可利用性之行爲，刑罰之

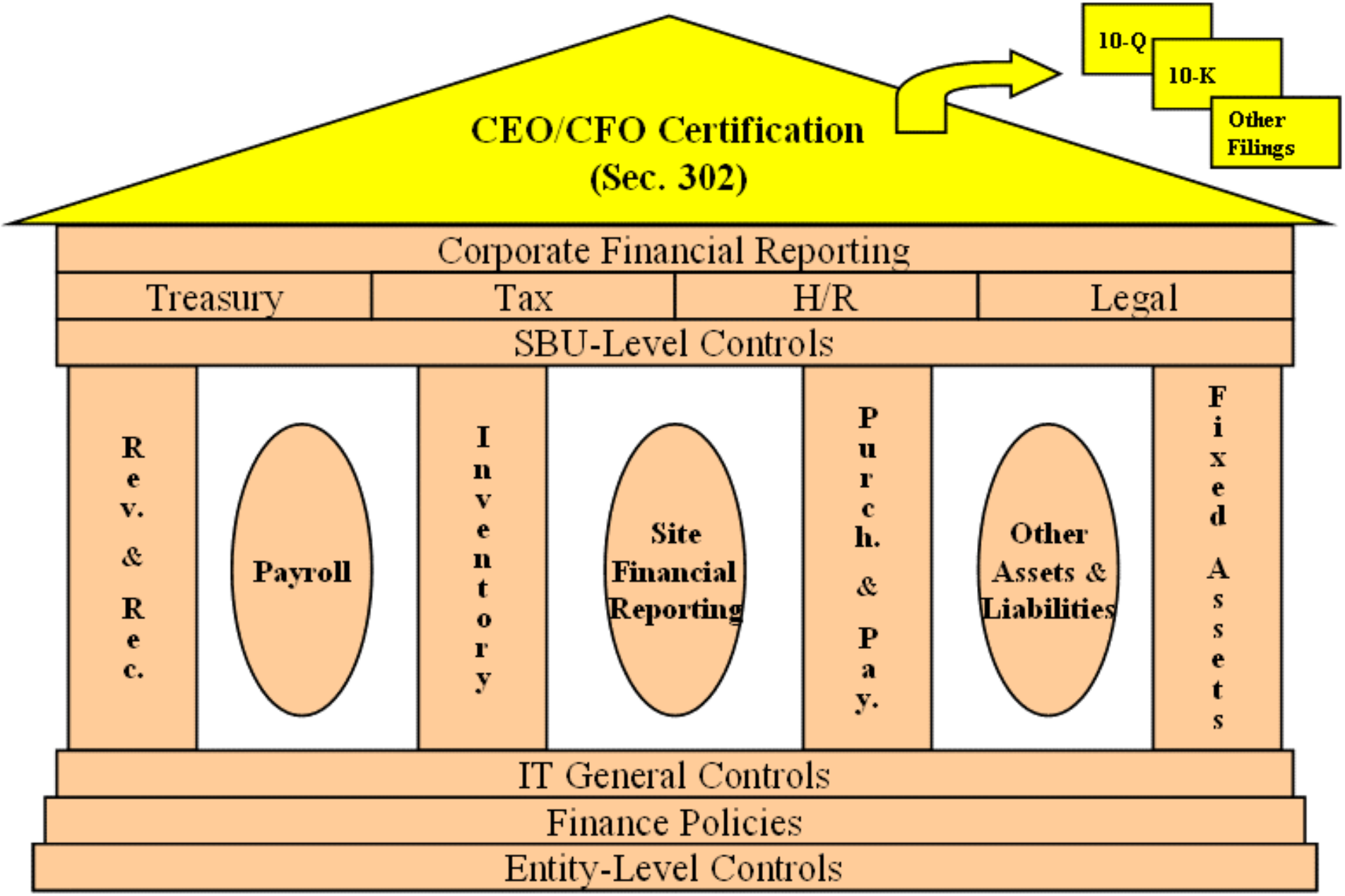
The Sarbanes-Oxley Act (續)

- **The scope of the Act is expansive, impacting a wide variety of areas:**

- Corporate Governance
  - **Code of Ethics**
  - **Whistleblower Hotline**
  - **Composition of Board of Directors & Audit Committee**

- Auditor Independence
  - **Independence of External Audit Firm**
  - **Pre-approval of all Audit & non-Audit Services**

- Reliability of Financial Reporting
  - **Executive certification of financial statements (Sections 906, 302)**
  - **Management reporting on internal controls (Section 404)**


10-Q
10-K
Other Filings
CEO/CFO Certification
(Sec. 302)
Corporate Financial Reporting
Treasury
Tax
H/R
Legal
SBU-Level Controls
Rev. & Rec.
Payroll
Inventory
Site Financial Reporting
Purch. & Pay.
Other Assets & Liabilities
Fixed Assets
IT General Controls
Finance Policies
Entity-Level Controls

資訊安全秩序在SOX的職責

資訊安全秩序在SOX的職責(續)

CONTROL OBJECTIVES
SUMMARY TABLE

The following chart provides an indication, by IT process and domain, of which information criteria are impacted by the high-level control objectives, as well as an indication of which IT resources are applicable.

DOMAIN		PROCESS	Information Criteria							IT Resources				
			effectiveness	efficiency	confidentiality	integrity	availability	compliance	reliability	people	applications	technology	facilities	data
Planning & Organisation	PO1	Define a strategic IT plan	P	S						✓	✓	✓	✓	✓
	PO2	Define the information architecture	P	S	S	S					✓			✓
	PO3	Determine technological direction	P	S								✓	✓	
	PO4	Define the IT organisation and relationships	P	S						✓				
	PO5	Manage the IT investment	P	P					S	✓	✓	✓	✓	
	PO6	Communicate management aims and direction	P					S		✓				
	PO7	Manage human resources	P	P						✓				
	PO8	Ensure compliance with external requirements	P					P	S	✓	✓			✓
	PO9	Assess risks	P	S	P	P	P	S	S	✓	✓	✓	✓	✓
	PO10	Manage projects	P	P						✓	✓	✓	✓	
	PO11	Manage quality	P	P		P			S	✓	✓	✓	✓	
Acquisition & Implementation	AI1	Identify automated solutions	P	S							✓	✓	✓	
	AI2	Acquire and maintain application software	P	P		S		S	S		✓			
	AI3	Acquire and maintain technology infrastructure	P	P		S						✓		
	AI4	Develop and maintain procedures	P	P		S		S	S	✓	✓	✓	✓	
	AI5	Install and accredit systems	P			S	S			✓	✓	✓	✓	✓
	AI6	Manage changes	P	P		P	P		S	✓	✓	✓	✓	✓
Delivery & Support	DS1	Define and manage service levels	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	DS2	Manage third-party services	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	DS3	Manage performance and capacity	P	P			S				✓	✓	✓	
	DS4	Ensure continuous service	P	S			P			✓	✓	✓	✓	✓
	DS5	Ensure systems security			P	P	S	S	S	✓	✓	✓	✓	✓
	DS6	Identify and allocate costs		P					P	✓	✓	✓	✓	✓
	DS7	Educate and train users	P	S						✓				
	DS8	Assist and advise customers	P	P						✓	✓			
	DS9	Manage the configuration	P				S		S		✓	✓	✓	
	DS10	Manage problems and incidents	P	P			S			✓	✓	✓	✓	✓
	DS11	Manage data				P			P					✓
	DS12	Manage facilities				P	P						✓	
	DS13	Manage operations	P	P		S	S			✓	✓		✓	✓
Monitoring	M1	Monitor the processes	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	M2	Assess internal control adequacy	P	P	S	S	S	P	S	✓	✓	✓	✓	✓
	M3	Obtain independent assurance	P	P	S	S	S	P	S	✓	✓	✓	✓	✓
	M4	Provide for independent audit	P	P	S	S	S	P	S	✓	✓	✓	✓	✓

(P) primary (S) secondary

(✓) applicable to

Organization Communications & Responsibilities	
Objectives	**Questions**
A1.1 Organizational Alignment IT has a formal process to assess and meet the needs of the organization. *RISK*: If IT strategies are not aligned with the overall objectives of the organization, IT will not be able to fully support the business requirements.	What process is in place to ensure IT activities are aligning with the organizational strategy (future needs)? What are all the steps in the process, when does each step occur, who is responsible for ensuring execution of the steps, and what proof exists that the process is occurring as stated? Describe the process that you utilize to identify technology needs of the organizational business groups? (i.e. do you conduct needs assessments)? Once current, needs are identified – what process exists to ensure that they are addressed? (e.g. Do you keep a log of requests, incorporating needs into long range plans? Is there a prioritization or review process with leaders of the appropriate business groups?) How do you ensure that solution(s) have addressed organizational needs? (e.g. Do you conduct a survey to see if needs are addressed?) What process exists to communicate that technology needs have been identified and addressed (e.g. monthly status report)?

B. Application Systems Development and Maintenance

End-user Approval	
Objectives	**Questions**
B1.1 Request Approval There is appropriate end-user approval of all new program requests or existing application modifications that impact end-user functionality to ensure the relevance and appropriateness of the request or modification. *RISK:* The lack of formalized measures to ensure adequate end-user involvement in the application design phase increases the risk that the application will not meet organizational needs.	How do you ensure that there is appropriate business/end-user management review and approval of system/program change requests? Are approvals documented (if so, specify the form) and filed? Note: Please indicate all parties involved per significant application (indicating why their approval is appropriate) and provide evidence that the approval occurred. Do not worry about *emergency changes;* this will be discussed later.
B1.2 Pre-implementation End-user Approval There is appropriate end-user approval of application	Describe how end-users provide approval and education of changes or new systems/programs prior to the changes being implemented into production.

Section B General Controls Checklist

Objective	Sub	Description	Responsible	Last Update	Approved ?
B3.1		End User Approval			
B3.1	**1**	Request Approval	Sharukh Munji	06/10/04	No
B3.1	**2**	End User Approval	Sharukh Munji	06/10/04	No
B3.2		Conversion Standards			
B3.2	**1**	System Conversion	Sutter / Bozovsky/Wang	06/10/04	No
B3.2	**2**	Data Conversion	Sutter / Bozovsky/Wang	06/10/04	No
B3.1		Request & Design Approval	Todd Smith	06/10/04	No
B3.2		Specifications & Requirements	Sutter / Bozovsky/Wang	06/10/04	No
B3.3		Integrity of Production Data & Programs	Sutter / Bozovsky/Wang	06/10/04	No
B3.4		Access Control	Sutter / Bozovsky/Wang	06/10/04	No
B3.5		Documentation	Sutter / Bozovsky/Wang	06/10/04	No
B3.6		Pre-Implementation IT Approval	Todd Smith	06/10/04	No
B4.1		Testing Standards	Sharukh Munji	06/10/04	No
B4.2		End User Testing Involvement	Sharukh Munji	06/10/04	No
B5.1		Implementation Integrity	Sutter / Bozovsky/Wang	06/10/04	No
B6.1		Segregation Of Duties	Todd Smith	06/10/04	No
B7.1		Change Control for Emergency Update	Sutter / Bozovsky/Wang	06/10/04	No

C. Computer Operations and Facilities

C1. Computer Operations

C1.1	**OBJECTIVE**: Batch Processing - Procedures governing batch processing activities exist, are communicated and enforced by management, and are reviewed/updated periodically. **RISK:** Without these procedures governing computer operations, there is an increased risk of non-optimal, erroneous or inconsistent production processing. **RESPONSIBLE PERSON(S)**: IT Management Official, IT Computer Operations Personnel

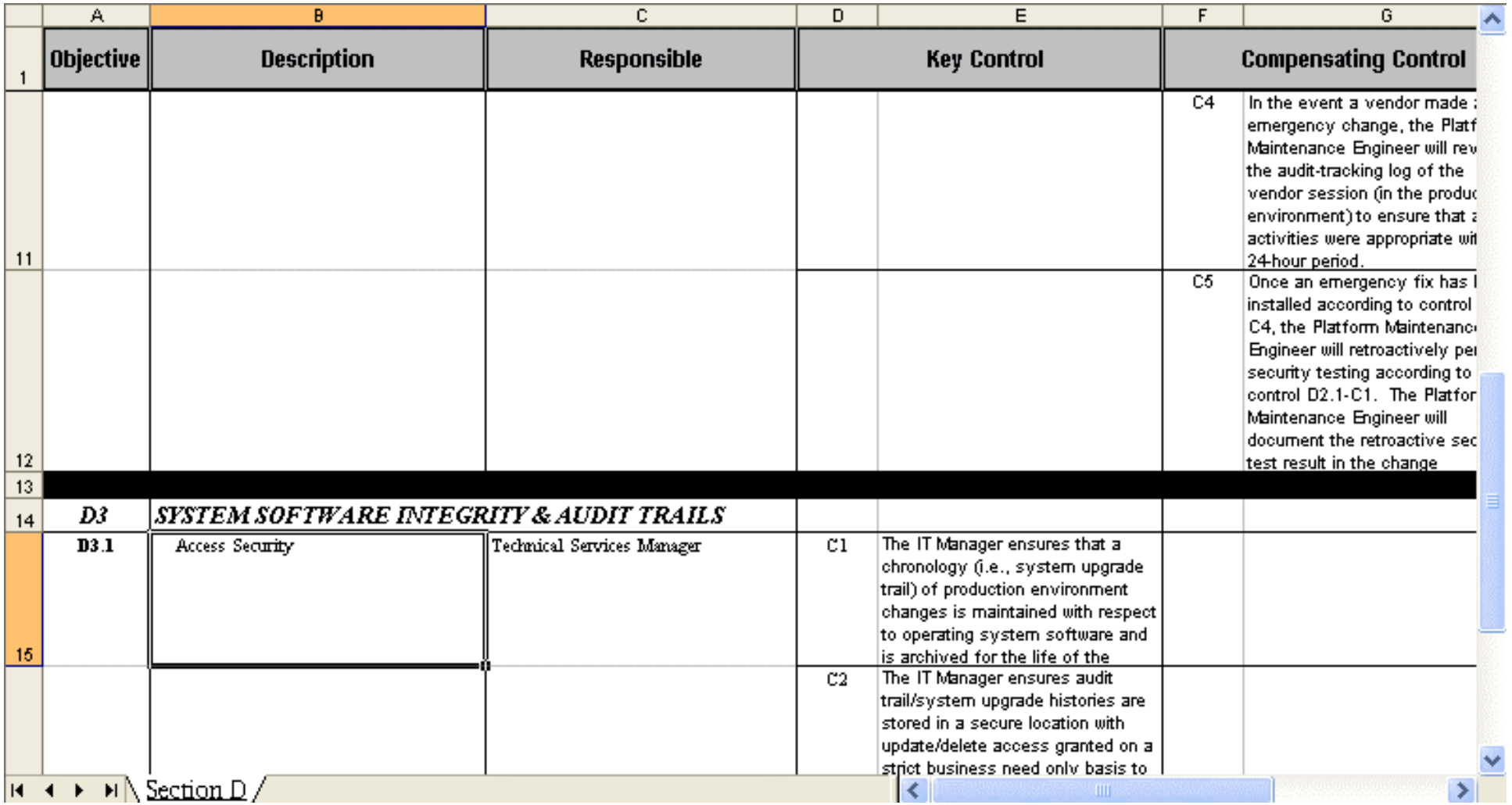
Control Technique	Test Procedure	Test Result	Test Ref.
C1.1-C1 – All Sarbanes business processes that have application system batch processing activities (that are non-IT maintenance-related) are inventoried and documented in a production schedule that includes the following: • Brief description of the batch job/job stream and the related business process that it supports • Assigned IT programming support personnel • End-user contacts for problem notification • Scheduled processing intervals • Run-time parameters required • Job pre-requisite processes	• Obtain from the IT Application Lead access to the folder containing the production schedule(s). • Review a sample of production schedule(s) to ensure that it conforms to standards outlined in C1.1-C1.		

E. SECURITY ADMINISTRATION

E1. Overall Security Organization and Policies

E1.3	**OBJECTIVE**: Processes are in place (1) to identify, on an on-going basis, the vulnerabilities at all technology layers (application, operating system, network) for all significant system/data assets, and (2) to design and implement specific security specification requirements within logical security control mechanisms to mitigate the identified vulnerabilities. **RISK**: The lack of established processes for the on-going identification of vulnerabilities, which facilitates the design and implementation of control mechanisms to addresses these vulnerabilities, increases the risk that significant system/data assets will be compromised. **RESPONSIBLE PERSON**: Todd Smith/Sharukh Munji/Troy Tate

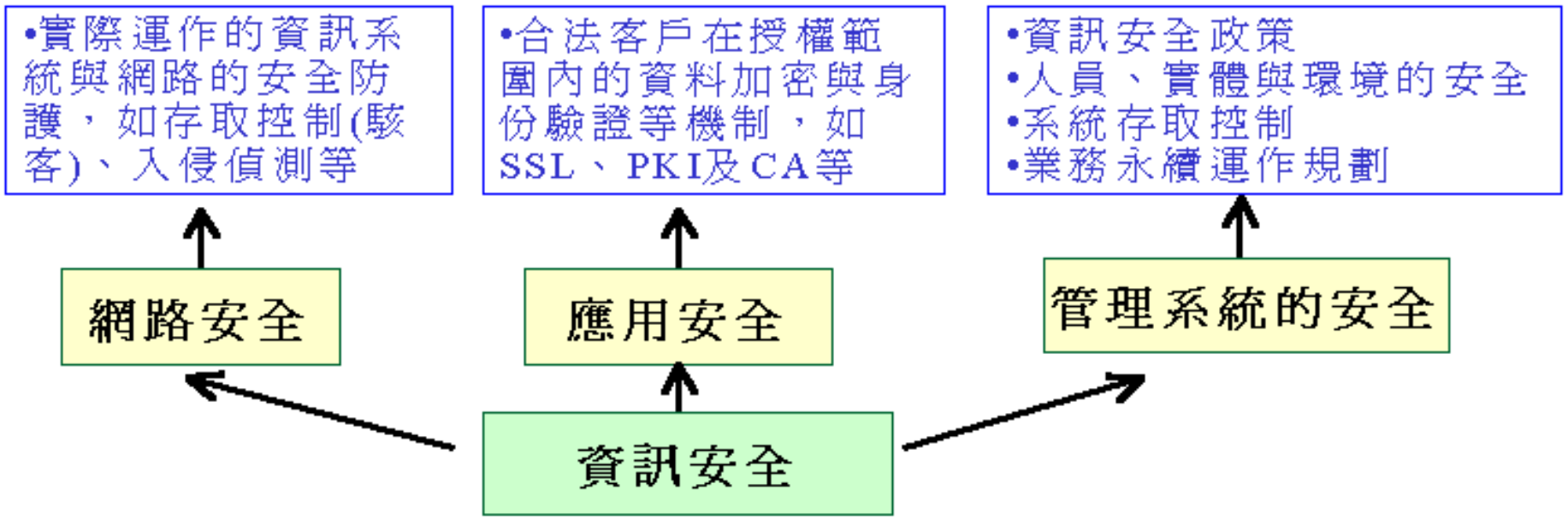
Control Technique	Control Type			Test Procedure	Test Result	Test Ref.
E1.3-C1 System version levels (Application & OS) are documented. Documentation is reviewed against known vulnerabilities and actions approved by owner using change management process.						
E1.3-C2 Network access paths are documented.						
E1.3-C3 A problem management system has been defined and implemented. Problems are recorded, analyzed & resolved in a timely manner.						



	A	B	C	D	E	F	G
1	**Objective**	**Description**	**Responsible**	**Key Control**		**Compensating Control**	
11						C4	In the event a vendor made a emergency change, the Platf Maintenance Engineer will rev the audit-tracking log of the vendor session (in the produc environment) to ensure that a activities were appropriate wit 24-hour period.
12						C5	Once an emergency fix has b installed according to control C4, the Platform Maintenanc Engineer will retroactively per security testing according to control D2.1-C1. The Platfor Maintenance Engineer will document the retroactive sec test result in the change
13							
14	***D3***	***SYSTEM SOFTWARE INTEGRITY & AUDIT TRAILS***					
15	**D3.1**	Access Security	Technical Services Manager	C1	The IT Manager ensures that a chronology (i.e., system upgrade trail) of production environment changes is maintained with respect to operating system software and is archived for the life of the		
				C2	The IT Manager ensures audit trail/system upgrade histories are stored in a secure location with update/delete access granted on a strict business need only basis to		

Section D

資訊安全範圍 –
資策會MIC 經濟部ITIS 計畫



公認的資訊安全政策標準

- 企業在採用風險管理模型，可參考國際間相當多公認的資訊安全政策標準，例如COBIT 、BS7799 、ISO17799 、GAPSIT 、RFC-2196 、FISCAM 、SysTrust 、GASSP ，其中以BS7799/ISO17799 最廣爲資訊安全管理顧問所引用 。
- 我國經濟部標準檢驗局於2002年12月5日亦正式公告CNS 17799

BS 7799 標準及其制定(一)

BS 7799 的製定乃是基於工業界、政府機關及商界業等的需求因應而生， 以建構一個共同框構以協助公司建構(develop)、實施 (implement) 和有效地衡量 (measure) 其資訊安全管理施行，和稽核公司內部機密性的管控流程。

BS 7799 標準及其制定(一)

- BS 7799 包含有兩個部分：
- l　第一部分：資訊安全管理實施要則。
- 　(Part One：Code of practice for information security management)
- l　第二部分：資訊安全管理系統規範。
- (Part Two: Specification for information security management systems)

BS 7799 標準及其制定 (二)

- 1995: BS 7799 頒行,當做一種指引方針文件 (guidance document)

1999: 重大篇幅增訂和修正，成二大部分:第一部分是屬於指導綱要文件 (guidance document) 已被使用到 ISO 17799 當做基礎核心於2000年12月頒行，而第二部分則隸屬於認證管理系統標準， 其格式仍然被視爲不適用於 ISO 現行階段使用。

BS 7799 標準及其制定 (三)

- 7799-1：1999 共有12章，其中第3章至第12章的名稱，與BS 7799-2的第4章第1節至第10節的名稱相同，而這10個小節也就是控制集匯整而成的10個大類 ，隨著 BS 7799-1 成爲 ISO 的標準，這10 個大類也成爲 ISO 17799的重點
- BS 7799-2 總共分爲4章，並於第4章列舉了 36 個控制目標，以及127個控制項目，不過 BS 7799補充說明，這些控制目標及控制項目並不周嚴，並非適用於所有狀況，也未將所有個別環境或技術考量列入考慮

ISO 17799 標準及其制定 （一）

- BS 7799-1 於2000年12月獲得 ISO 審議通過，成爲國際標準 ISO 17799，至於 BS 7799-2，預料也將會在未來獲得 ISO 審議通過
- ISO 17799並未提供驗證的標準，而是在於成爲資訊安全應用上的最佳指導綱要，而 BS 7799-2則爲認證上的遵循標準。

ISO 17799 標準及其制定 （二）

- **BS7799/ISO17799** 資訊安全管理**10**大準則之架構

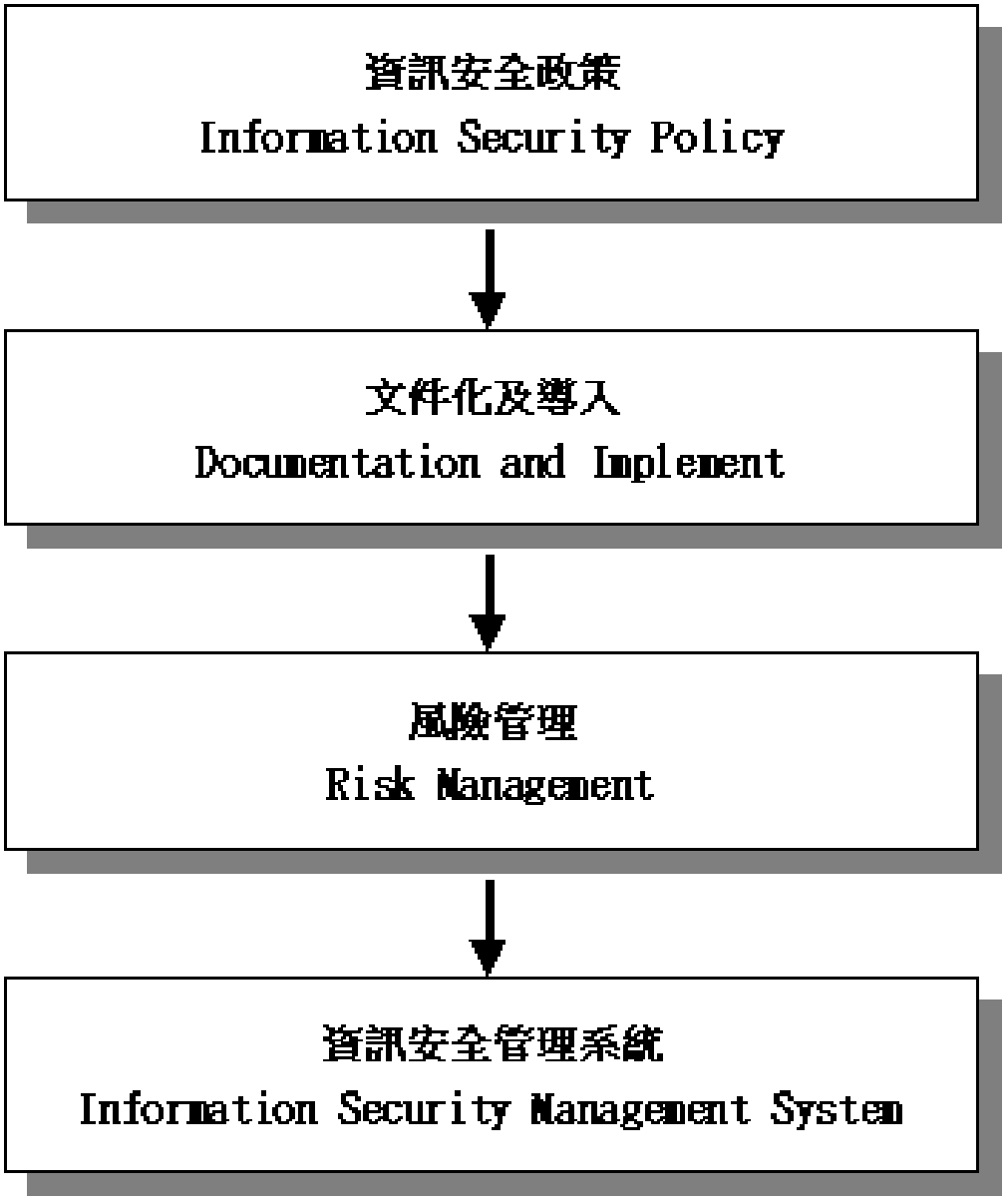
步驟一	步驟二	步驟三	步驟四	步驟五	步驟六	步驟七	步驟八	步驟九	步驟十
資訊安全政策	資訊安全組織	資產分類與控制	人員安全	實體與環境安全	電腦與網路管理	系統存取控制	系統開發與維護	業務永續運作規劃	政策法規遵行

資料來源：BS7799/ISO17799，資策會MIC整理，2001年10月

各標準機構發行年代比較表

- 1995/2 英國BS 7799-1 公佈問世，成爲時界資訊安全指導綱要標準文件
- 1998/2 英國BS 7799-2 公佈問世，成爲時界資訊安全稽核標準文件
- 1999 瑞典 SS 62 7799 公佈問世，成爲廿世紀第二個公告資訊安全的國家
- 2000/12 國際 ISO 17799-1 公佈問世，成爲資訊安全界之國際標準
- 2002/12 中華民國 CNS 17799 公佈問世

發展資訊安全四個階段步驟



資訊安全政策的施行

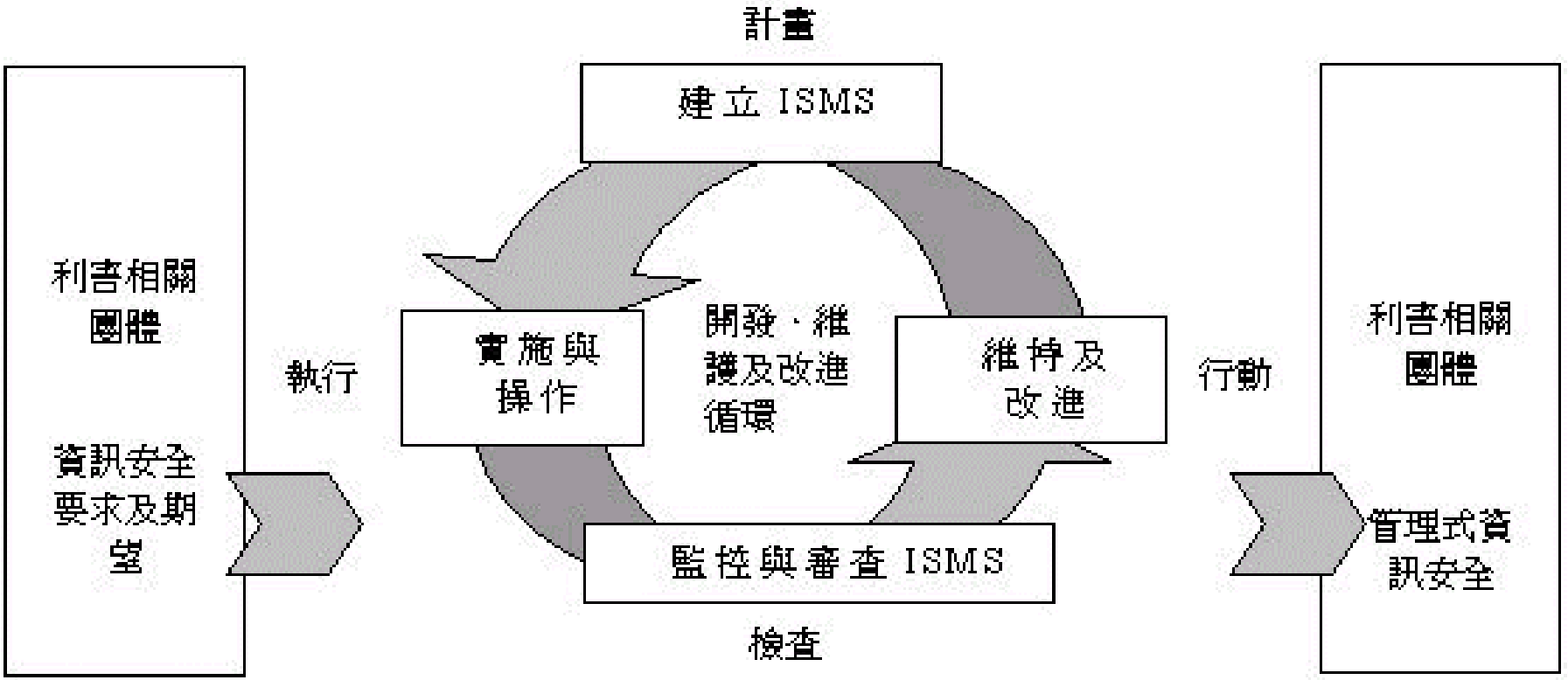
- 管理觀點

- 遵從合法性
- 遵從安全政策
- 技術符合性

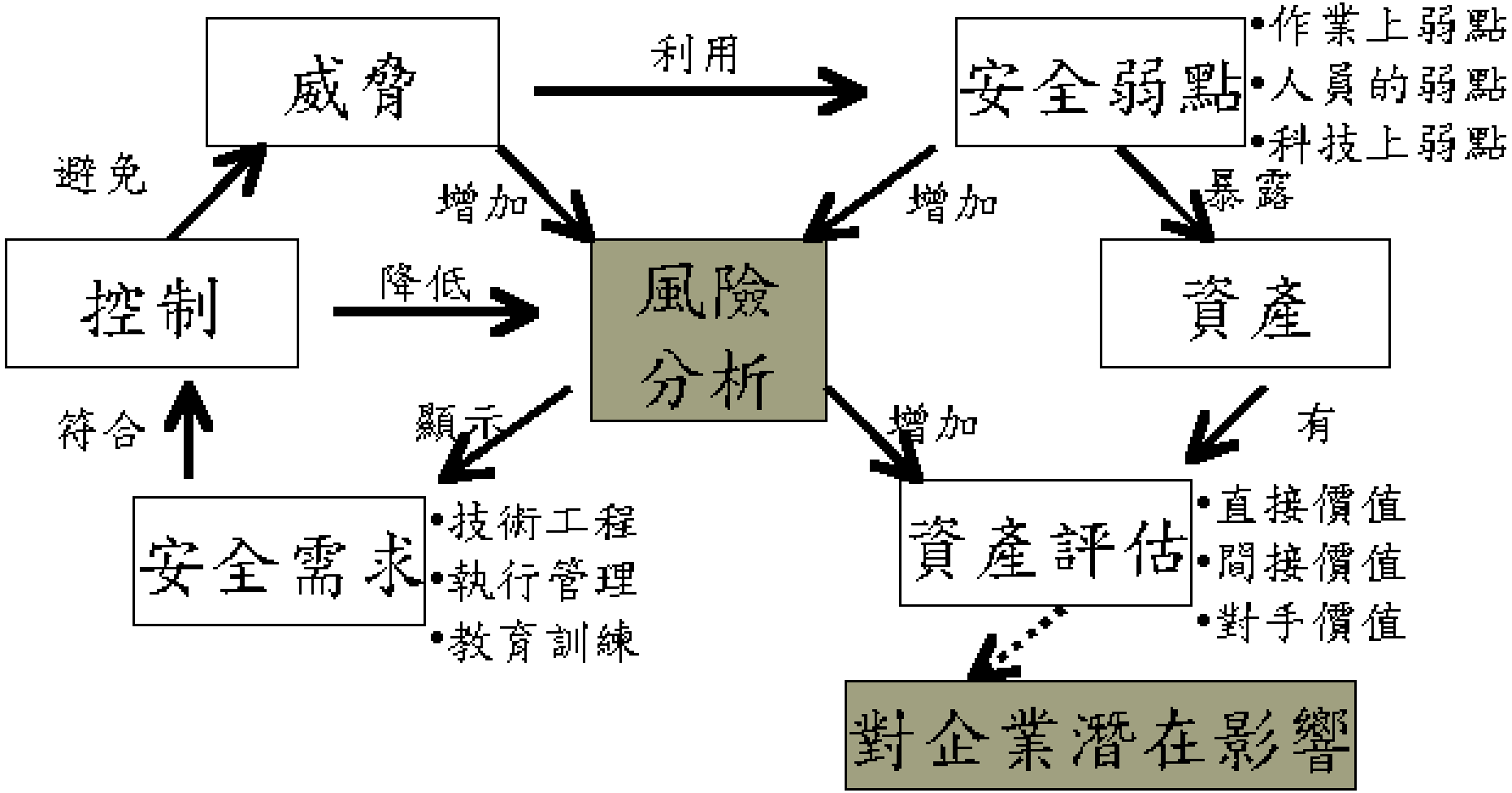
- 資訊安全管理系統範疇
- 風險評估
- 控制目標及要項
- 應用條款
- 企業回復計劃

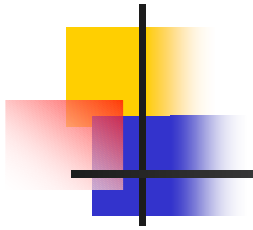
- 安全組織
- 資產分類及控管
- 人員安全
- 重要執行法則及登錄內容的保護，包含資料保護在內

組織建立ISMS - 經濟部標準檢驗局 CNS 17800



資訊安全風險評估流程


威脅
利用
安全弱點
•作業上弱點
•人員的弱點
•科技上弱點
避免
增加
增加
暴露
控制
降低
風險分析
資產
符合
顯示
增加
有
安全需求
•技術工程
•執行管理
•教育訓練
資產評估
•直接價值
•間接價值
•對手價值
對企業潛在影響



Q & A