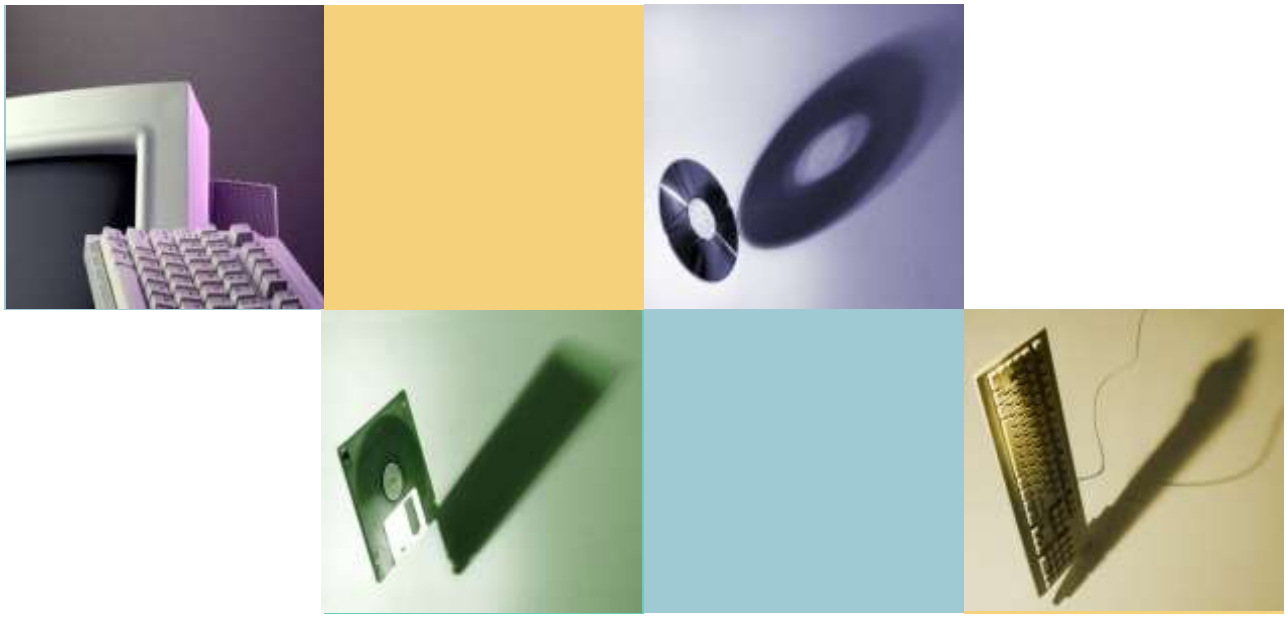
ISMS導入建置作業



國立宜蘭大學圖書資訊館

網路組 曾國旭

Wednesday, Feb 26 2014

Agenda

- ISO 27001介紹
  - Lead Auditor Course
  - ISO 27000 Family/Series
  - ISO 27001 Controls
- ISMS導入建置
- Q and A



Lead Auditor Course

- BS 7799 / ISO 27001:2005主導稽核員課程(五天，含2小時筆試)
  - 資訊和資訊安全
  - BS 7799 / ISO 27001:2005介紹
  - BS 7799 / ISO 27001:2005稽核流程
  - 風險評鑑和風險處理
  - 安全控制措施和對策
  - 稽核階段
  - 稽核報告
  - 第三方評鑑和驗證



ISO 27001過去與現在

- BS 7799標準更新之歷史
  - 1995：英國公佈BS 7799 Part I
  - 1998：英國公佈BS 7799 Part II
  - 1999 英國公佈新版BS 7799 Part I、Part II
  - 2000：ISO通過成為ISO/IEC 17799 Part I
  - 2002：BS 7799:2-2002 –資訊安全管理系統驗證規範
  - 2005：ISO/IEC 17799:2005
  - **2005：ISO 27001 ISMS認證標準**
  - **2007：ISO/IEC 17799作業規範，正名為ISO 27002**

ISO 27000 Family/Series

ISMS Standard / Guidance	ISO 27000 Series(2005~)	2005	2000~2002	Before 2000
ISMS資安管理系統認證標準	ISO 27001	ISO 27001:2005 (BS 7799-2:2005)	BS 7799-2:2002	BS 7799-2:1999
ISMS作業規範	ISO 27002	ISO 17999:2005 (BS 7799-1:2005)	ISO 17999:2000	BS 7799-1:1999
ISMS導入指南	ISO 27003			
資安管理評測標準	ISO 27004			
資安風險管理	ISO 27005			
國際認可組織對驗證機關的規範	ISO 27006			
ISMS稽核參考指南	ISO 27007			



ISO 27001 Controls

<table>
<tr><td colspan="4">Security Policy</td></tr>
<tr><td colspan="4">Organization of Information Security</td></tr>
<tr><td colspan="4">Asset Management</td></tr>
<tr><td>Human Resources Security</td><td>Physical and Environmental Security</td><td>Communications and Operations Management</td><td rowspan="2">Information System Security Development and Maintaince</td></tr>
<tr><td colspan="3">Access Control</td></tr>
<tr><td colspan="4">Information Security Incident Management</td></tr>
<tr><td colspan="4">Business Continuity Management</td></tr>
<tr><td colspan="4">Compliance</td></tr>
</table>

教育版ISMS與國際版ISMS的差別在於教育版ISMS刪除或合併部份的控制措施（國際版133項、教育版100項）



Agenda

- ISO 27001介紹
  - Lead Auditor Course
  - ISO 27000 Family/Series
  - ISO 27001 Controls
- ISMS導入建置
- Q and A



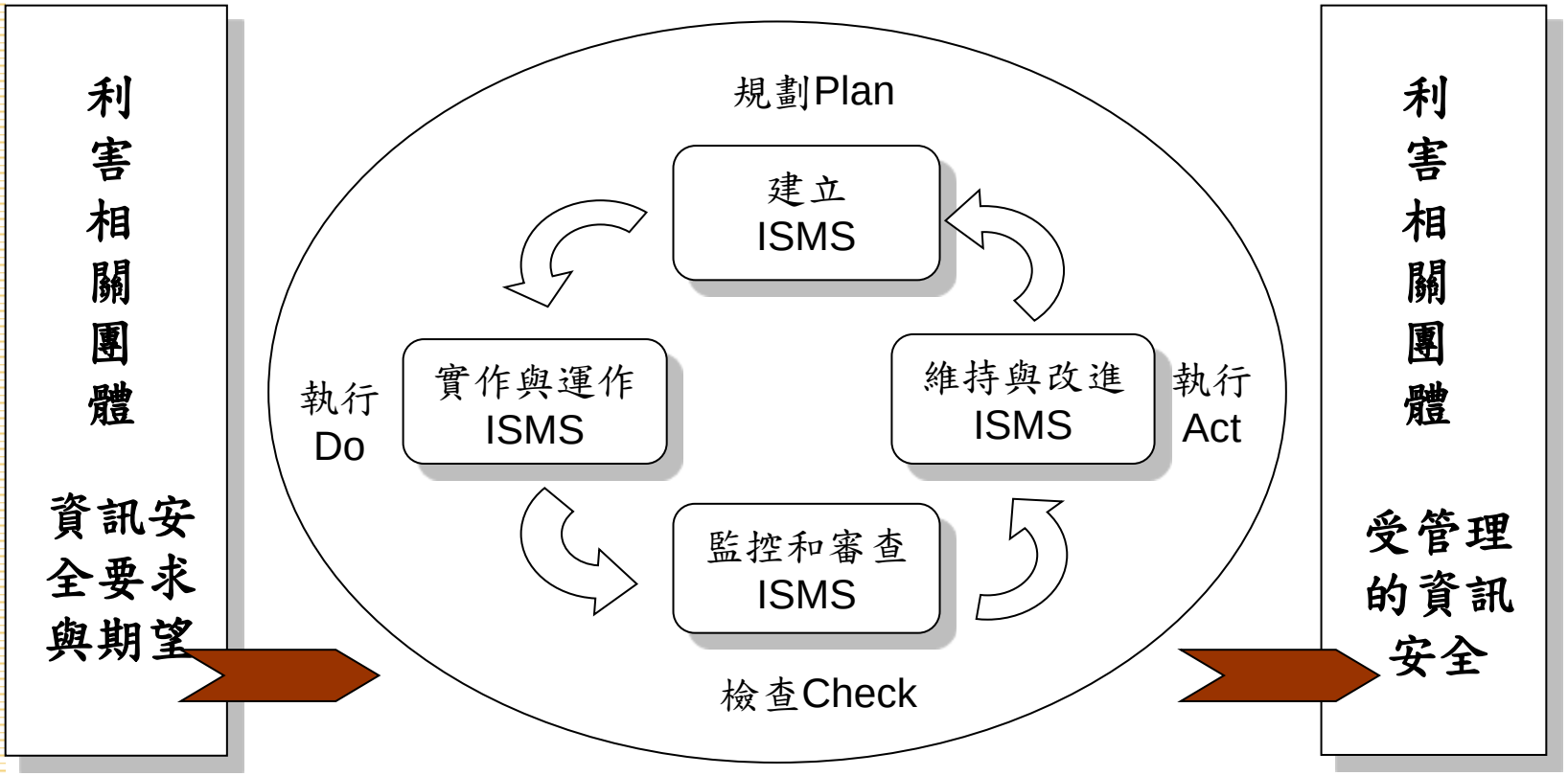
資訊安全三大原則

- 機密性(Confidentiality)：
  確保只有經授權的人才可以取得資訊，避免資訊洩露。
- 完整性(Integrity)：
  確保資訊不受未經授權的竄改與資訊處理方法的正確性。
- 可用性(Availability)：
  確保經授權的使用者，在需要時可以取得資訊，並使用相關資產。

ISMS目的在於保護資訊資產的機密性、可用性與完整性。

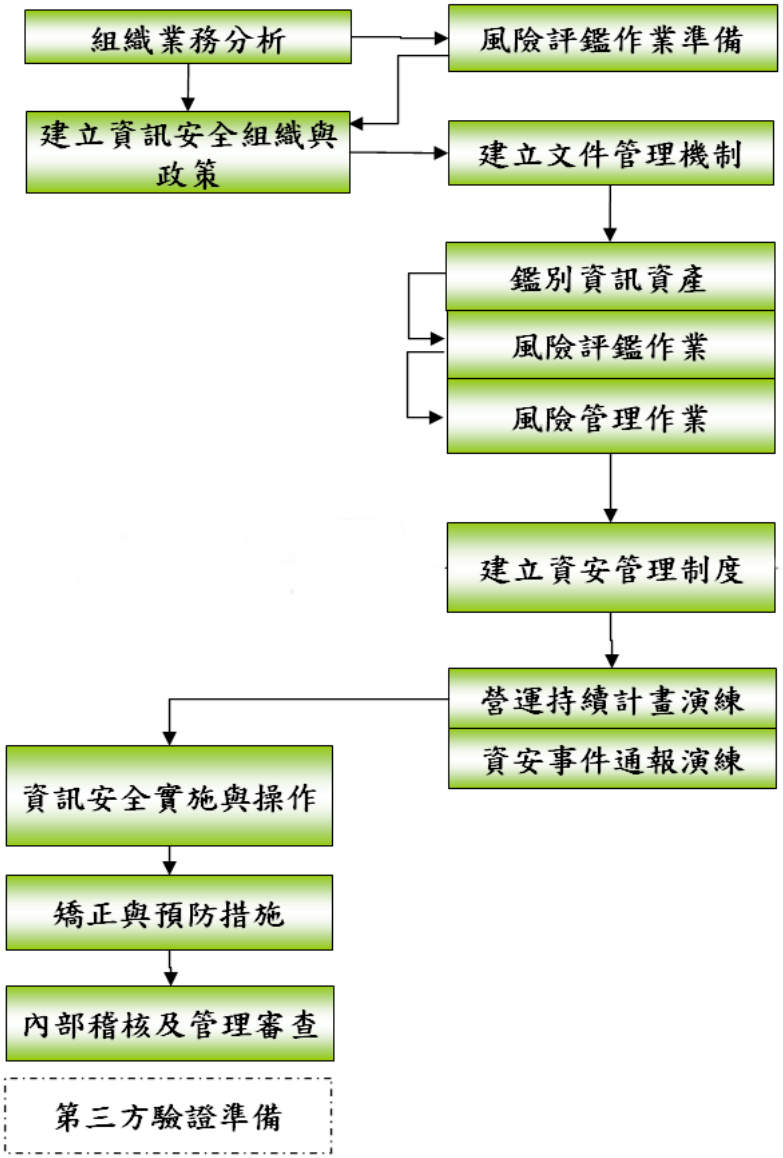


PDCA 過程模式Process model



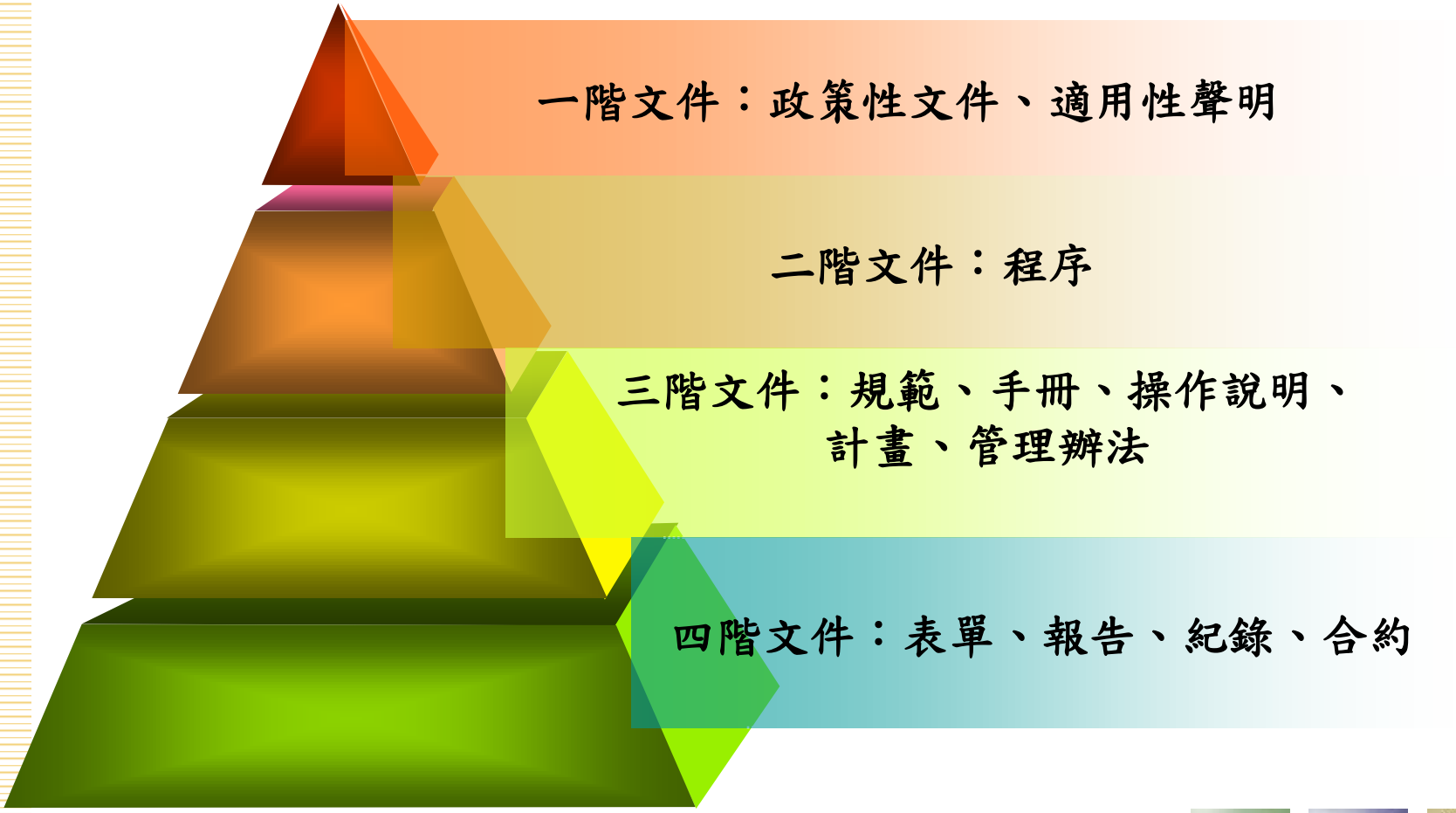
應用於ISMS過程之PDCA過程模式

ISMS建置執行概要


組織業務分析
風險評鑑作業準備
建立資訊安全組織與政策
建立文件管理機制
鑑別資訊資產
風險評鑑作業
風險管理作業
建立資安管理制度
營運持續計畫演練
資安事件通報演練
資訊安全實施與操作
矯正與預防措施
內部稽核及管理審查
第三方驗證準備



ISMS 文件體系


一階文件：政策性文件、適用性聲明
二階文件：程序
三階文件：規範、手冊、操作說明、
計畫、管理辦法
四階文件：表單、報告、紀錄、合約

電算中心ISMS相關規範文件範例

文件編號	文件名稱	文件機密等級	相關表單編號	相關表單名稱	相關表單機密等級
NIU-ISMS-A-001	資訊安全政策	一般			
NIU-ISMS-B-001	資訊安全組織程序書	限閱	NIU-ISMS-D-001	資訊安全組織成員表	限閱
			NIU-ISMS-D-002	外來文件一覽表	限閱
			NIU-ISMS-D-003	外部單位聯絡清單	限閱
			NIU-ISMS-D-004	ISMS有效性量測表	限閱
NIU-ISMS-B-002	文件管理程序書	限閱	NIU-ISMS-D-005	文件調閱申請單	限閱
			NIU-ISMS-D-006	文件修訂建議表	限閱
			NIU-ISMS-D-007	資訊安全管理文件列表	限閱
			NIU-ISMS-D-008	資訊安全管理審查會議紀錄	限閱
NIU-ISMS-B-003	資訊資產管理程序書	限閱	NIU-ISMS-D-009	資訊資產清單	限閱
NIU-ISMS-C-001	資訊資產異動作業說明書	敏感	NIU-ISMS-D-015	資訊資產異動申請表	限閱
			NIU-ISMS-D-009	資訊資產清單	限閱

電算中心目前共有1份一階文件(政策)、14份二階文件(程序書)、5份三階文件(作業說明書)及47份四階文件(表單)



資產盤點

- 何謂「資產」？

  對組織有價值的任何事物

- 資產的分類
  - 實體資產，如電腦
  - 軟體資產，如應用系統
  - 資訊資產，如資料檔案
  - 書面文件，如合約
  - 人員、服務、組織的形象、…等
- 資產的價值

  依據機密性、完整性及可用性加以鑑別



電算中心資產清冊範例

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值
CCN-CM-001	CM	外網Core Router	Cisco骨幹路由器共7部	網路組	網路組	網路組	2	3	4	4
CCN-CM-002	CM	內網Core Router	Extreme 路由器1部	網路組	網路組	網路組	2	3	4	4
CCN-CM-003	CM	區網Switch	Extreme 3802、Cisco 2960共2 部	網路組	網路組	網路組	2	3	3	3
CCN-CM-004	CM	區域網路骨幹及服務	校園網路服務	網路組	網路組	網路組	2	3	4	4
CCN-CM-005	CM	廣域網路骨幹及服務	網際網路服務、TANet網路服務	網路組	網路組	網路組	2	3	4	4



風險評鑑與管理

- 依據資產本身的**威脅**及**弱點**計算風險值
- 威脅可能對系統、組織或資產造成一個有害的事件，如天災
- 弱點本身並不會造成傷害，如人員教育訓練不足。但如果沒有妥善管理，將促使威脅形成
- 風險處理方法
  - 避免風險
  - 降低風險到可接受的程度
  - 轉移風險
  - 接受剩餘的風險



電算中心資產威脅弱點評估表範例

資產編號	資產類別	資產名稱	資產價值	威脅	弱點	威脅等級(發生之可能性)			弱點等級(受到威脅利用之容易度)			風險值
						低(1)	中(2)	高(3)	低(1)	中(2)	高(3)	
CCS-HW-001	HW	重要系統主機	4	硬體失效	維護服務回應時間過長	1			1			4
				硬體失效	缺乏硬體耗損控管	1				2		8
				硬體失效	缺乏有效變更控制	1				2		8
				電源供應中斷	不穩定的電壓	1			1			4
				未經授權存取或使用	未確實陪同外部人員或清潔人員執行相關作業		2		1			8
				未經授權存取或使用	存取權限授與不當或未定期審查	1			1			4
				未經授權存取或使用	通行碼管理不足		2		1			8
				未經授權存取或使用	離開工作站未進行「登出」作業		2		1			8
				未經授權存取或使用	缺乏監督與稽核機制	1			1			4
				操作失誤	複雜的操作介面	1			1			4
				操作失誤	操作文件不足	1				2		8
				操作失誤	專業訓練不足	1			1			4



電算中心ISMS有效性量測範例

項次	量測項目		目標水準	量測方式	量測結果	差異說明
					填寫符合或不符合兩項	不符合需填寫差異說明內容
A.5	資訊安全政策訂定與評估	(1)資訊安全政策審查次數	≧1次/年	召開審查會議	■ 符合 □不符合	
		(2)資訊安全政策宣導次數	≧1次/年	會議、教育訓練	■ 符合 □不符合	
A.6	資訊安全組織	(1)有否確實簽署保密協議	不符≦2件	抽核內部與外部人員	■ 符合 □不符合	
		(2)管理審查會議召開次數	≧1次/年	查核會議紀錄	■ 符合 □不符合	
A.7	資訊資產分類與管制	(1)資訊資產清單是否定期更新	≧1次/年	查核資訊資產清冊	■ 符合 □不符合	
		(2)資訊資產清單符合分級與標示規定	不符≦2件	實地抽查實體設備標示情形	■ 符合 □不符合	
		(3)是否定期執行風險評鑑	≧1次/年	查核資訊資產清單、威脅及弱點評估表、風險改善計畫表	■ 符合 □不符合	

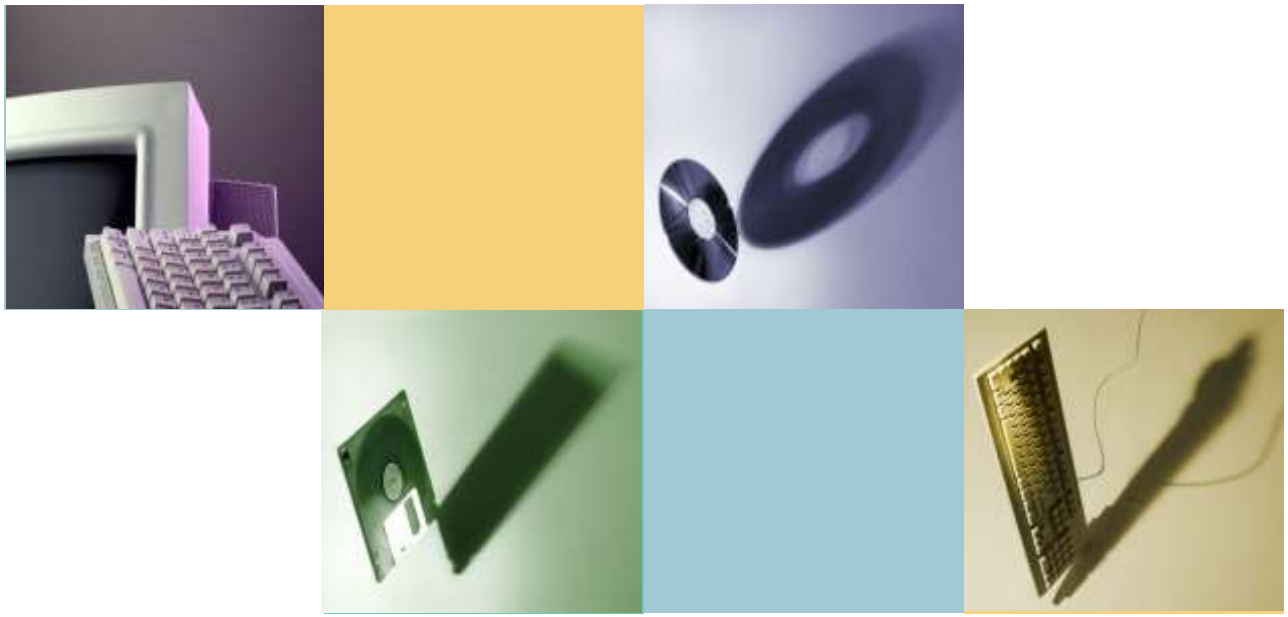


ISMS工作清單

工作項目	頻率
資產盤點	至少每年一次
風險評鑑	至少每年一次
帳號清查	至少每半年一次(特權帳號每三個月一次)
弱點掃描	至少每半年一次
BCP演練	至少每年一次
ISMS有效性量測	至少每年一次
軟體清查	至少每年一次
內部稽核	至少每年一次
管理審查會議	至少每年一次
第三方稽核	每年一次



Q and A



THANKS !