



文件編號	IMS-P-019	文件名稱	組織全景評鑑管理程序書		
機密等級	內部使用	版次	2.1	頁次	1 / 8

管理系統文件

文件類別	第二階文件	
文件編號	IMS-P-019	
文件名稱	組織全景評鑑管理程序書	
發行單位	國立虎尾科技大學	
發行日期	110年03月29日	
版次	2.1	
適用單位/範圍	全校 (凡業務涉及個資蒐集、處理、利用之單位皆適用之)	
訂修廢單位	審查	核准

(原版簽名頁保存於IMS推動小組)



文件編號	IMS-P-019	文件名稱	組織全景評鑑管理程序書		
機密等級	內部使用	版次	2.1	頁次	3 / 8

1. 目的

為了提供本校於推動資安及個資保護管理作業規範時，全面廣泛地了解本校全景及利害關係者之需要與期望，以順利確定資通安全之方針與界定資安及個資保護管理制度（IMS）之實施範圍。

2. 適用範圍

鑑別本校全景及利害關係者之需要與期望作業之管理。

3. 參考文件

3.1. 資通安全管理法。

3.2. 資通安全管理法施行細則。

3.3. 國際標準資訊安全管理系統(ISO27001：2013)。

3.4. 國際標準個人資訊管理系統(BS 10012)最新規範。

3.5. 教育體系資通安全暨個人資料管理規範。

3.6. IMS-M-002 適用性聲明書。

3.7. IMS-P-005 資安及個資保護目標管理程序書。

4. 名詞定義

無。



文件編號	IMS-P-019	文件名稱	組織全景評鑑管理程序書		
機密等級	內部使用	版次	2.1	頁次	4 / 8

5. 作業內容

5.1 組織全景評鑑管理流程圖

作業流程	權責單位	相關表單
組織全景鑑別需求	IMS 推動小組	
鑑別願景及目標	IMS 推動小組	組織全景評鑑表
鑑別核心業務	IMS 推動小組	組織全景評鑑表
鑑別利害關係者	IMS 推動小組	組織全景評鑑表
鑑別需求與期望	IMS 推動小組	組織全景評鑑表
風險與衝擊分析	IMS 推動小組	組織全景評鑑表
擬定因應對策	IMS 推動小組	組織全景評鑑表
決定IMS範圍	IMS 推動小組	組織全景評鑑表
審核	資通安全暨個人資料保護推動委員會	組織全景評鑑表
紀錄保存	IMS 推動小組	



文件編號	IMS-P-019	文件名稱	組織全景評鑑管理程序書		
機密等級	內部使用	版次	2.1	頁次	5 / 8

5.2 產生組織全景鑑別需求

5.2.1 依據教育體系資通安全暨個人資料管理規範參考 ISO/IEC 27001:2013 及 BS 10012:2017 兩項管理標準之條文要求，需進行組織全景評鑑作業，以決定與本校營運目標相關，且會影響本校達成資安及個資保護管理制度（IMS）預定成果的外部與內部議題。

5.2.2 在鑑別組織全景時，IMS 推動小組須先取得「資通安全長」對組織營運宗旨與目標之看法與共識。

5.3 鑑別願景及目標

鑑別組織全景時，IMS 推動小組應依資通安全長簽署及正式對外公布之資料，鑑別使命、核心價值、願景及營運目標，並記載於「IMS-P-019-01 組織全景評鑑表」中，以利下一階段組織全景鑑別作業。

5.4 鑑別核心業務

其次，IMS 推動小組應鑑別核心（關鍵）業務流程，並將核心業務流程及重要工作項目，記載於「IMS-P-019-01 組織全景評鑑表」中。

5.5 鑑別利害關係者

完成核心業務流程鑑別後，IMS 推動小組應鑑別與本校核心（關鍵）業務流程相關之內部及外部之利害關係者，並將相關利害關係者記載於「IMS-P-019-01 組織全景評鑑表」中。

5.6 鑑別需求與期望

鑑別與本校核心業務相關之利害關係者後，IMS 推動小組應綜整本校營運目標，以鑑別本校內部及外部利害關係者對本校各項業務之需要與期望，並記載於「IMS-P-019-01 組織全景評鑑表」中。

5.7 風險與衝擊分析

5.7.1 針對「IMS-P-019-01 組織全景評鑑表」中所鑑別出利害關係者的每一項需要與目標，無論其是否納入 IMS 實施或驗證範圍，需進行分析當未符合利害關係者的需要與目標時，可能造成的衝擊情境，以及該威脅可能對組織造成之衝擊程度等級。

5.7.2 IMS 推動小組應依據「表 1：組織全景風險鑑別等級表」之判定



文件編號	IMS-P-019	文件名稱	組織全景評鑑管理程序書		
機密等級	內部使用	版次	2.1	頁次	6 / 8

條件，判斷威脅衝擊之等級，並將判斷結果記載於「IMS-P-019-01 組織全景評鑑表」中。

表 1：組織全景風險鑑別等級表

等級	威脅衝擊程度
1	<p>未能達成需要與目標，對組織無傷害：</p> <p>(1) 對組織業務營運無任何影響。</p> <p>(2) 不會造成組織營收之負成長。</p> <p>(3) 組織已將相關風險，納入 IMS 實施與驗證範圍，進行處置與管理，並擬訂適當之控制措施。</p> <p>(4) 不存在任何法令/法規/契約之要求，或不違反相關之規定。</p>
2	<p>未能達成需要與目標，對組織產生輕微傷害：</p> <p>(1) 對組織業務營運造成輕微之影響，威脅造成之衝擊可接受。</p> <p>(2) 對組織營收造成可接受之小量負成長。</p> <p>(3) 組織已將相關風險，利用契約或保險等措施進行轉嫁。</p> <p>(4) 可能違反組織內部規範及任何法令/法規/契約之要求。</p>
3	<p>未能達成需要與目標，對組織產生中度傷害：</p> <p>(1) 對組織業務營運造成一定之影響，威脅對組織造成之衝擊產生一定之損害。</p> <p>(2) 對組織營收造成一定程度之負成長，無法接受。</p> <p>(3) 組織已與相關需要與目標之需求單位進行溝通，並獲得其書面同意接受該風險。</p> <p>(4) 可能違反法令/法規之要求。</p>
4	<p>未能達成需要與目標，對組織產生嚴重傷害：</p> <p>(1) 對組織業務營運造成嚴重之影響，威脅對組織造成之衝擊產生重大之損害。</p> <p>(2) 對組織營收造成難以承擔之負成長，可能導致大量虧損。</p> <p>(3) 組織對於相關風險，已陳報最高管理者，經過其同意接受風險，但未獲相關需要與目標之需求單位同意。</p> <p>(4) 可能違反法令/法規之要求。</p>
5	<p>未能達成需要與目標，對組織產生重大營運災難：</p> <p>(1) 對組織業務營運造成極嚴重之影響，極可能導致組織結束營運。</p> <p>(2) 對組織營收造成難以承擔之虧損，極可能導致組織結束營運。</p> <p>(3) 組織對於相關風險，未採取任何因應措施。</p> <p>(4) 可能違反法令/法規之要求。</p>

5.8 因應對策鑑別



文件編號	IMS-P-019	文件名稱	組織全景評鑑管理程序書		
機密等級	內部使用	版次	2.1	頁次	7 / 8

5.8.1 對「IMS-P-019-01 組織全景評鑑表」中，利害關係者所有層面之需要與目標進行討論，決定是否採取適當之因應對策或接受風險，將準備採取之因應對策敘述於「IMS-P-019-01 組織全景評鑑表」中，並確認所採取之因應對策與 ISO 27001 控制條款間之關係，以彙整到「IMS-M-002 適用性聲明書」。

5.8.2 部分無法對應 ISO 27001 控制條款之風險處理對策，亦應妥善分析處置，確實對「IMS-P-019-01 組織全景評鑑表」中所鑑別之每一項需要與目標，進行風險管理。

5.9 決定 IMS 範圍

IMS 推動小組應考量若未滿足利害關係者之需要與目標時，可能對本校所造成之衝擊，提出 IMS 實施與驗證範圍綜合建議，由「資通安全長」決定是否將各項需要與目標納入 IMS 實施或驗證範圍，並將明確之 IMS 驗證範圍描述載明於「IMS-M-002 適用性聲明書」中。

5.10 審核

5.10.1 IMS 推動小組應將「IMS-P-019-01 組織全景評鑑表」呈報「資通安全暨個人資料保護推動委員會」進行審核，俾使最高管理階層能清楚了解本校營運要求、利害關係者期望、與本校實施 IMS 範圍之關聯性，以及可能存在之衝擊，以期給予最高之關注及保證，提供相關利害關係者信心，並就相關風險選擇其重要關注項目列入資通安全目標中定期量測。

5.10.2 組織全景評鑑作業應每年至少重新進行一次評估及審查，並在有任何關於營運流程之改變、組織結構變更，或利害關係者產生新需要或期望時，修訂「IMS-P-019-01 組織全景評鑑表」之各項內容，且當變更較為明顯而必要時，應一併修訂「IMS-M-002 適用性聲明書」。

5.11 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	組織全景評鑑表	電子計算機中心	至少 3 年

6. 附件



文件編號	IMS-P-019	文件名稱	組織全景評鑑管理程序書		
機密等級	內部使用	版次	2.1	頁次	8 / 8

6.1 IMS-P-019-01 組織全景評鑑表。