德明財經科技大學

資訊安全風險評鑑與管理規定

機密等級：一般

文件編號：Takming-ISMS-B-003

版　次：V 1.1

初版日期：107.12.25

修　訂　紀　錄

版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	107.12.25	N/A	執行小組	初版
1.1	108.09.11	2	執行小組	加入行政院國家資通會報

1. **目的**

為定義德明財經科技大學(以下簡稱本校)對資訊安全風險評估之責任、方法及程序。本規定係評估本校資訊安全管理系統(Information Security Management System , ISMS) 範圍內之資訊資產在機密性、完整性及可用性的風險。

為確保達成制度管理目標，並預防或減少非預期之影響，以達成持續改善，應於規劃期間或重大變更時，評估管理目標異動與達成情形，如有異動或未達成狀況，則應規劃因應風險與機會之行動，將各項行動整合及實作於管理制度中，並評估此行動之有效性。

2. **適用範圍**

適用於本校資訊資產。

3. **名詞定義**

3.1 機密性（Confidentiality，簡稱 C）

指資訊不應被未授權人存取的特性，確保只有經過授權的人才能存取資訊。

3.2 完整性（Integrity，簡稱 I）

指資訊的正確性與完整性的特性。

3.3 可用性(Availability，簡稱 A)

指被授權人於需要時可取得資訊的特性。

3.4 風險評鑑

係鑑別組織各業務流程內資訊資產在面對可能發生的風險時所可能產生的損失與影響。

3.5 風險（Risk）

威脅會利用資產的弱點造成資產的損失或損壞的潛在可能性。

3.6 威脅（Threat）

資訊資產所面臨的事件，可能會對系統或組織及其資產造成傷害，威脅必須利用資產的弱點才能對資產造成傷害。

3.7 弱點（Vulnerability）

指單一或一系列會讓威脅有機可趁而造成資產損害的狀況，資產的脆弱點本身並不會造成傷害。

3.8 風險處理

選擇與實施各項控制措施，以修正風險的過程。

3.9 風險擁有者（Risk owner）

負有控制流程或資產的產生、開發、維護、使用及安全管理責任的個人或個體。

4. **權責**

4.1 資訊安全執行小組召集人

4.1.1 核准可接受風險值

4.1.2 「風險處理計畫表」之審查及確認執行成效。

4.2 資訊安全執行分組

4.2.1 建立並維護系統化之風險評鑑方法。

4.2.2 建議風險評鑑之時機與範圍。

4.2.3 監督風險評鑑之執行。

4.2.4 彙總「風險處理計畫表」，提報資訊安全執行小組召集人。

4.3 流程/系統主管人員

4.3.1 擔任風險擁有者

4.3.2 審核風險評鑑結果與可接受風險值

4.3.3 審核「風險處理計畫表」

4.4 資訊資產管理者

4.4.1 執行風險評鑑作業。

4.4.2 擬訂「風險處理計畫表」並執行之。

4.4.3 「資訊資產清冊」之管理與維護。

5. 要求事項

5.1 風險評鑑執行時機

為確保達成制度管理目標，並預防或減少非預期之影響，以達成持續改善，應於規劃期間(每年至少一次)執行風險評鑑，如有異動或未達成狀況，則應規劃因應風險與機會之行動，將各項行動整合及實作於管理制度中，並評估此行動有效性。

(1)營運組織變更。

(2)作業流程改變。

(3)資訊資產新增或變更 。

(4)發生重大資訊安全事件。

5.2 風險評鑑執行方式

5.2.1 確認營運流程與資訊系統安全等級

5.2.1.1.在 ISMS 的範圍內，確認本校營運處理流程與系統，含本校業務之主要流程，與支援流程之相關流程。

5.2.1.2.確認營運處理流程與系統主管人員。

5.2.1.3.應參考行政院國家資通會報「資訊系統分級與資安防護基準作業規定」，鑑別適用範圍內資訊系統之安全等級，其安全等級應採鑑別結果最高者，應執行風險評鑑與處理流程。

5.2.2 資訊資產分析

5.2.2.1. 各流程與系統主管人員應指定資訊資產管理者定期(至少每年一次)對所負責之流程進行重要資訊資產及與資訊安全管理相關的其他資產盤點作業。並加以整編且隨時更新「資訊資產清冊」。

5.2.2.2.資訊資產價值鑑別

資訊資產權責單位應鑑別其所管轄內所有資訊資產之價值。資訊資產價值除考量資訊資產機密等級之外，尚需考量資訊資產之可用性及完整性，其評估標準如下：

(1)機密性

評估標準	數值
該資訊資產無特殊之機密性要求	1
該資訊資產僅供組織內部人員或被授權之單位及人員使用	2
該資訊資產僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用	3
該資訊資產所包含資訊為組織或法律所規範的機密資訊	4

(2)完整性

評估標準	數值
該資訊資產本身完整性要求極低	1
該資訊資產本身具有完整性要求，當完整性遭受破壞時，不會對組織造成傷害	2
該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，但不至於太嚴重	3
該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，甚至造成業務終止	4

(3)可用性

評估標準	數值
該資訊資產可容許失效 3 工作天以上	1
該資訊資產可容許失效 8 工作小時以上，3 工作天以下	2
該資訊資產僅容許失效 4 工作小時以上，8 工作小時以下	3
該資訊資產僅容許失效 4 工作小時以下	4

5.2.2.3.資訊資產價值之決定將依據資訊資產之機密性、完整性及可用性評估之後，取3者之最大值以為資訊資產之價值。

5.2.2.4.資訊資產管理者應依據資訊資產清冊之機密性、可用性及完整性之評估標準，確認資產價值。

5.2.2.5.資訊資產管理者應將「資訊資產清冊」及價值評估結果，陳報至流程/系統主管人員進行審核。

5.2.3 弱點威脅評估

弱點與威脅項目的評估係針對本校營運情況評估各資訊資產可能存在的弱點與可能面臨的威脅。應將各類資訊資產可能面臨之威脅與弱點項目，分別建立「威脅及弱點評估表」。並依據威脅及弱點等級評估其事件發生機率。

(1)威脅等級

評估標準	評估值
威脅發生之可能性為低	1
威脅發生之可能性為中	2
威脅發生之可能性為高	3

(2)弱點等級

評估標準	評估值
該弱點不容易被威脅利用	1
該弱點容易被威脅利用	2
該弱點非常容易被威脅利用	3

5.2.4 風險值計算

5.2.4.1.評估威脅發生之可能性及弱點受到威脅利用之容易度，計算出風險值。

5.2.4.2.風險值=（資訊資產價值×威脅等級×弱點等級）

5.3 風險管理執行方式

5.3.1 可接受風險值的決定

5.3.1.1.決定可接受風險準則：訂出可接受風險準則，包含適法性與其他相關依據等，以及排序後選定可接受之準則，需由「資訊安全執行分組」提報「資訊安全執行小組」召集人核定。

5.3.1.2.資訊資產之可接受風險值，需經流程/系統主管人員審核，並由「資訊安全執行分組」提交「資訊安全執行小組」召集人審核。

5.3.1.3.「資訊安全執行分組」應針對高於可接受風險值項目，產出

「風險評鑑彙整表」作為風險管理之依據。

5.3.2 選擇控制措施

5.3.2.1.超出可接受風險值之項目，應選擇適當之控管措施，並產出「風險處理計畫表」，說明風險控管措施之執行辦法。

5.3.2.2.考量「風險處理計畫表」所提之各項降低風險方式以預估在特定風險控制項目實施後，該控制項目對其標的風險項目可能達成的效果並預估在實施風險控制措施後原風險項目的殘餘風險。

5.3.2.3.「風險處理計畫表」與其殘餘風險，需經流程/系統主管人員審核，並提交「資訊安全執行小組」召集人審核後列入追蹤管理程序。

5.3.2.4.「資訊安全執行分組」依據風險控管措施評估是否新增或修訂「適用性聲明書」。

5.3.3 風險改善狀況的後續追蹤

5.3.3.1.「資訊安全執行分組」應針對「風險處理計畫表」彙整控管，持續追蹤至完成改善為止。

5.3.3.2.「資訊安全執行分組」應針對「風險處理計畫表」各項措施建立有效性量測指標，並納入「目標達成計畫與量測表」量測項目中。

5.3.3.3.各項風險改善措施完成後，應配合定期風險評鑑確認其威脅弱點程度，以確保相關改善措施的有效性。

5.4 覆核

5.4.1 監控

控制措施的實施必須建立相對應的指標或紀錄，以反應出控制措施實施的狀況及成效，便於管理階層及相關人員做定期或不定期審視。

5.4.2 持續改善

為保持本風險評鑑方法之有效性與適用性，「資訊安全執行分組」得定期檢討可接受風險值與「威脅及弱點評估表」之項目。以期確保資訊資產均處於最佳保護之下，提供持續不中斷的營運。

6. 參考文件

6.1 資訊資產管理規定。

6.2 威脅及弱點評估表。

6.3 風險評鑑彙整表。

6.4 資訊資產清冊。

6.5 適用性聲明書。

6.6 風險處理計畫表。

6.7 資訊系統分級與資安防護基準作業規定(行政院資通安全作業規範)。

6.8目標達成計畫與量測表。