水利署臺北水源特定區管理分署
詳細風險評鑑作業標準書

V2.0

文件編號	WRATB-ISMS-3-002
分類等級	內部使用
初版日期	
修訂日期	

制訂	審查	會辦	核准

文件編修紀錄

發行／修訂版本	發行／修訂生效日期	發行/修訂內容說明	制訂	審查	核准	備註
V1.0		規範詳細風險評鑑作業，制定本作業標準書。		資通安全執行秘書	資通安全處理小組召集人	
V2.0		機關 112 年 9 月組織改造後名稱修正、內文、分類修訂		資通安全執行秘書	資通安全處理小組召集人	

目錄

0. 目的 4
1. 範圍 4
2. 相關文件 4
2.1 WRATB-ISMS-3-001 高階風險評鑑作業標準書 4
2.2 經濟部水利署資通安全維護計畫_C 級 4
2.3 資通系統風險評鑑參考指引(V4.0) 4
3. 作業說明 4
3.1 名詞定義 4
3.2 角色與權責 4
3.3 作業時機 5
3.4 鑑別資訊資產價值 5
3.5 威脅與脆弱性識別 6
3.6 評估控制措施 8
3.7 殘餘風險 8
4. 產出紀錄 8
4.1 WRATB-ISMS-4-010 資訊資產暨風險評鑑表 9

0. 目的

為規範水利署臺北水源特定區管理分署(以下稱本分署)評估資訊資產價值，識別資產威脅、脆弱性，並評估威脅等級、脆弱等級，以計算資訊資產風險等級等作業活動，故制訂本作業標準書。

1. 範圍

本分署提報之核心資通系統及重要系統。

2. 相關文件

2.1 WRATB-ISMS-3-001 高階風險評鑑作業標準書

2.2 經濟部水利署資通安全維護計畫_C 級

2.3 資通系統風險評鑑參考指引(V4.0)

3. 作業說明

3.1 名詞定義

無。

3.2 角色與權責

3.2.1 科室主管

3.2.1.1 審核「WRATB-ISMS-4-010 資訊資產暨風險評鑑表」。

3.2.1.2 監督與管理風險改善作業。

3.2.2 資通系統(服務)負責人

3.2.2.1 執行本作業標準書之作業活動，撰寫「WRATB-ISMS-4-010 資訊資產暨風險評鑑表」。

3.2.2.2 擬定與執行風險改善作業。

3.3 作業時機

3.3.1 資通系統(服務)負責人於完成「WRATB-ISMS-3-001 高階風險評鑑作業標準書」後，經核定安全等級為「高」或「中」的資通系統(服務)需要執行本作業標準書之相關活動。

3.4 鑑別資訊資產價值

3.4.1 評估資訊資產在資通安全事故發生時，破壞「機密性」、「完整性」、「可用性」造成的後果，對本分署衝擊的嚴重性。鑑別資訊資產的價值，將識別的後果分別給予一個值，選擇每一資產的「機密性」、「完整性」、「可用性」代表值的最高值，則為資訊資產的價值。

3.4.2 資通系統(服務)負責人於鑑別資訊資產價值時，應將鑑別之過程紀錄填寫於「WRA10-ISMS-4-010 資訊資產暨風險評鑑表」中的「機密性」、「完整性」、「可用性」欄位中。

3.4.3 鑑別資訊資產價值之方法，說明如下:

3.4.3.1 機密性

價值	說明
1	■ 漏失資訊之機密性保護，所造成後果輕微或可忽視者。 ■ 此資訊資產無特殊之機密性要求，可對外公開之資訊。
2	■ 漏失資訊之機密性保護，所造成的後果嚴重且其災害會影響業務。 ■ 此資訊資產僅供機關內部人員或授權之人員使用。
3	■ 漏失資訊之機密性保護，所造成的後果很嚴重且其災害會影響業務深遠或信譽受損。 ■ 此資訊資產所包含資訊為機關或法律所規範的機密資訊。

3.4.3.2 完整性

價值	說明

價值	說明
1	■ 若遭受未經授權的破壞或竄改，所造成後果是輕微或可忽視者。
2	■ 若遭受未經授權的破壞或竄改，會造成組織嚴重的後果，且其災害會影響組織業務運作。
3	■ 若遭受未經授權的破壞或竄改，會造成組織很嚴重的後果，且其災害會影響組織業務停頓或信譽受損。

3.4.3.3 可用性

價值	說明
1	■ 此資訊資產可容許失效 1 個工作天以上。
2	■ 此資訊資產可容許失效 4 個工作小時以上,8 個工作小時以下。
3	■ 此資訊資產僅容許失效 4 個工作小時以下。

3.5 威脅與脆弱性識別

3.5.1 若資訊資產價值為 3，則須識別此資訊資產的威脅與脆弱性，並評估威脅等級、脆弱等級，並計算此資訊資產的風險等級。若資產價值為 2 或 1，則不須執行資訊資產威脅與脆弱性的識別作業。

3.5.2 依據識別出的威脅與脆弱性，評估威脅發生的可能性及脆弱性被利用的程度。以下說明評估準則:

3.5.2.1 威脅發生的可能性

數值	說明
1	■ 發生可能性低(發生頻率為每年或更低)，沒發生過或不可能發生。

數值	說明
2	■ 發生可能性中等(發生頻率為每季或每半年)，曾發生過但次數很少。
3	■ 發生可能性高(發生頻率為每月或更頻繁)，過去經常發生。

3.5.2.2 脆弱性被利用的程度

數值	說明
1	■ 很難被利用。
2	■ 被利用的難易度適中。
3	■ 很容易被利用。

3.5.3 識別出的威脅與脆弱性，分別填於「WRATB-ISMS-4-010 資訊資產暨風險評鑑表」中的「威脅」與「脆弱性」欄位中。

3.5.4 識別出的威脅發生的可能性及脆弱性被利用的程度，則分別填於「WRATB-ISMS-4-010 資訊資產暨風險評鑑表」中的「安控前」之「威脅等級」與「脆弱等級」欄位中。(填寫數值)

3.5.5 完成「威脅等級」與「脆弱等級」的填寫後，「WRATB-ISMS-4-010 資訊資產暨風險評鑑表」將自動計算出此資訊資產的風險等級。

3.5.5.1 資訊資產的風險值 = 資訊資產價值 X 威脅等級 X 脆弱等級。

3.5.5.2 風險等級的評估準則，說明如下:

風險等級	說明
低	■ 風險值為 1 - 6。
中	■ 風險值為 7 - 12。
高	■ 風險值為 13 - 27。

3.6 評估控制措施

3.6.1 風險等級為「高」的風險項目，應提出改善處理之控制措施，將控制措施填入「WRATB -ISMS-4-010 資訊資產暨風險評鑑表」中「風險降低原因說明」的欄位中，並擬定「WRATB -ISMS-4-015 矯正及預防行動報告單」。

3.6.2 風險控制措施的方法主要分成以下四種：

3.6.2.1 降低風險

針對不同的領域進行管控，以達到風險值降低之目的。

3.6.2.2 轉移風險

利用轉嫁的方式降低風險，例如購買保險以補償方式降低風險。

3.6.2.3 避免風險

利用取代方案或其他之資產以替代此資產所帶來之風險，不過若採取此方法，需再評估替代方案之可行性，以及帶來的風險值。前提是替代方案能帶來更低的風險。

3.6.2.4 接受風險

在以上三個方式都無法採用時，管理階層可以決定接受此風險，也就是接受此風險。

3.6.3 完成「風險降低原因說明」欄位的填寫後，則重新評估威脅發生的可能性及脆弱性被利用的程度，並分別填於「WRATB -ISMS-4-010 資訊資產暨風險評鑑表」中的「安控後」之「威脅等級」與「脆弱等級」欄位中。(填寫數值)

3.7 殘餘風險

3.7.1 若資訊資產於「安控後」的風險等級仍為「高」者，可提報資通安全處理小組會議決議是否接受該剩餘風險，若資通安全處理小組會議決議無法接受該剩餘風險，則進行第 2 次風險處理與風險評鑑；若資通安全處理小組會議可接受該殘餘風險，惟部份風險改善因改善期間過長或成本過高導致無法立即改善者，得採取短期補償措施，輔以長期持續追蹤進行改善。

4. 產出紀錄

4.1 WRATB-ISMS-4-010 資訊資產暨風險評鑑表