

水利署臺北水源特定區管理分署 風險評估與管理程序書

V2.0

文件編號	WRATB-ISMS-02-005
分類等級	內部使用
初版日期	
修訂日期	

制訂	審查	會辦	核准

本文件為水利署臺北水源特定區管理分署所有，禁止翻印

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		為規範本局各課室執行風險評鑑作業，建立本程序書初稿。		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
1.1	本分署提報之核心資通系統或重要系統。	4
1.2	本分署基礎環境設施。	4
2.	相關文件	4
2.1	WRATB-ISMS-2-013 矯正及預防措施程序書	4
2.2	WRATB-ISMS-3-001 高階風險評鑑作業標準書	4
2.3	WRATB-ISMS-3-002 詳細風險評鑑作業標準書	4
2.4	資通安全責任等級分級辦法	4
2.5	經濟部水利署資通安全維護計畫_C 級	4
2.6	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	5
3.3	維護資通系統(服務)清冊	6
3.4	安全等級評估	6
3.5	資產價值評估與風險評鑑	6
3.6	彙整風險評鑑結果	6
3.7	風險處理	7
4.	產出紀錄	7
4.1	WRATB-ISMS-4-013 資通系統(服務)清冊	7
4.2	WRATB-ISMS-4-014 資通系統(服務)安全等級評估表	7
4.3	WRATB-ISMS-4-015 矯正及預防行動報告單	7
4.4	風險評鑑報告	7
4.5	風險處理計畫	7

0. 目的

為確保能識別水利署臺北水源特定區管理分署(以下稱本分署)資訊資產的風險，進行風險評鑑及後續的風險處理作業，以期風險能夠獲得有效的管理。

1. 範圍

1.1 本分署提報之核心資通系統或重要系統。

1.2 本分署基礎環境設施。

2. 相關文件

2.1 WRATB-ISMS-2-013 矯正及預防措施程序書

2.2 WRATB-ISMS-3-001 高階風險評鑑作業標準書

2.3 WRATB-ISMS-3-002 詳細風險評鑑作業標準書

2.4 資通安全責任等級分級辦法

2.5 經濟部水利署資通安全維護計畫_C級

2.6 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

3.1.1 共同性系統：

3.1.1.1 包含共用性系統與共通性系統。

3.1.1.2 共用性系統指單一機關主責系統開發與資料管理，其餘機關僅涉及使用操作，如國稅系統。

3.1.1.3 共通性系統指單一機關主責系統開發與規格制訂，其餘機關除使用操作外，資料主要儲存於使用機關，如公文電子交換系統。

3.1.2 風險

某事件發生的機率與其結果之組合。

3.1.3 脆弱性

資訊資產本身的缺陷、管理或流程缺失、沒有適當的控制措施或實施控制措施時的缺失。

3.1.4 威脅

3.1.4.1 揭露脆弱性的潛在危險。

3.1.4.2 威脅是威脅主體藉由識別特定的脆弱性後，所採取的行動，行動結果將有危害資訊資產的可能性。

3.1.4.3 威脅主體可以是人、軟體或是天然災害。

3.2 角色與權責

3.2.1 資通安全長

3.2.1.1 審核「風險評鑑報告」及「風險處理計畫」。

3.2.2 資通安全執行秘書

3.2.2.1 指派人員撰寫「風險評鑑報告」及「風險處理計畫」。

3.2.2.2 於資通安全推動小組會議中，報告與說明風險改善情況。

3.2.3 資通安全執行小組

3.2.3.1 彙整各科室之風險評鑑作業紀錄。

3.2.3.2 彙整各科室之風險改善措施。

3.2.3.3 追蹤風險改善情況。

3.2.4 各科室主管

3.2.4.1 核准科室之「WRATB-ISMS-4-013 資通系統(服務)清冊」及「WRATB-ISMS-4-014 資通系統(服務)安全等級評估表」。

3.2.4.2 指定人員定期彙整與更新「WRATB-ISMS-4-013 資通系統(服務)清冊」。

3.2.4.3 監督與管理風險之改善作業。

3.2.5 資通系統(服務)負責人

3.2.5.1 執行資通系統(服務)安全等級評估，並更新「WRATB-ISMS-4-014 資通系統(服務)安全等級評估表」。

3.2.5.2 執行「WRATB-ISMS-3-001 高階風險評鑑作業標準書」及「WRATB-ISMS-3-002 詳細風險評鑑作業標準書」。

3.2.5.3 擬定於實施風險改善措施。

3.3 維護資通系統(服務)清冊

3.3.1 資通系統(服務)負責人每年應評估其負責之資通系統(服務)，是否有新增、異動或下線之情況。

3.3.2 各科室負責之資通系統(服務)，由科室主管指派人員彙整於「WRATB-ISMS-4-013 資通系統(服務)清冊」中。

3.4 安全等級評估

3.4.1 資通系統(服務)負責人應每年定期或當資訊資產有重大變更時，執行資通系統(服務)之安全等級評估。

3.4.2 資通系統(服務)之安全等級評估作業，請遵循「WRATB-ISMS-3-001 高階風險評鑑作業標準書」之規範辦理。

3.4.3 於完成安全等級評估作業後，應更新「WRATB-ISMS-4-013 資通系統(服務)清冊」及「WRATB-ISMS-4-014 資通系統(服務)安全等級評估表」中相關欄位之內容。

3.5 資產價值評估與風險評鑑

3.5.1 於完成安全等級評估作業後，若資通系統(服務)的安全等級為「高」或「中」，則應進行資訊資產價值評估與風險評鑑作業。

3.5.2 執行資訊資產價值評估與風險評鑑作業，請遵循「WRATB-ISMS-3-002 詳細風險評鑑作業標準書」之規範辦理。

3.6 彙整風險評鑑結果

3.6.1 各科室於完成「WRATB-ISMS-3-001 高階風險評鑑作業標準書」與

「WRATB-ISMS-3-002 詳細風險評鑑作業標準書」後，應將作業紀錄交由資通安全執行小組進行彙整。

3.6.2 由資通安全執行秘書指派人員，彙整各科室的風險評鑑紀錄於「風險評鑑報告」中。

3.7 風險處理

3.7.1 各科室應針對風險等級為「高」的風險項目，遵循「WRATB-ISMS-2-013 矯正及預防措施程序書」之規範要求，擬定「WRATB-ISMS-4-015 矯正及預防行動報告單」，並交由資通安全執行小組進行彙整。

3.7.2 由資通安全執行秘書指派人員，彙整各科室的風險改善措施於「風險處理計畫」中。

3.7.3 「風險評鑑報告」及「風險處理計畫」應經由內部簽核流程至資通安全長進行審核。

3.7.4 資通安全執行小組應持續追蹤風險處理之改善情形，直到風險等級降為「中」或「普」為止。

3.7.5 風險評鑑結果與風險處理之改善情形，應於資通安全處理小組會議中報告說明。

4. 產出紀錄

4.1 WRATB-ISMS-4-013 資通系統(服務)清冊

4.2 WRATB-ISMS-4-014 資通系統(服務)安全等級評估表

4.3 WRATB-ISMS-4-015 矯正及預防行動報告單

4.4 風險評鑑報告

4.5 風險處理計畫