水利署臺北水源特定區管理分署
高階風險評鑑作業標準書

V2.0

文件編號	WRATB-ISMS-3-001
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		規範高階風險評鑑作業，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

評估水利署臺北水源特定區管理分署(以下稱本分署)資通系統(服務)之安全等級，以作為評估是否執行詳細風險評鑑之準則。

1. 範圍

本分署所有資通資通系統。

2. 相關文件

2.1 資通安全責任等級分級辦法

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 核定「WRATB-ISMS-4-014 資通系統(服務)安全等級評估表」。

3.2.2 資通系統(服務)負責人

3.2.2.1 執行資通系統(服務)的安全等級評估。

3.2.2.2 填寫「WRATB-ISMS-4-014 資通系統(服務)安全等級評估表」。

3.3 輸入資通系統(服務)名稱

3.3.1 資通系統(服務)負責人於「WRATB-ISMS-4-014 資通系統(服務)安全等級評估表」中輸入資通系統(服務)名稱與系統(服務)說明，進行資通系統(服務)安全等級評估。

3.4 識別業務屬性

3.4.1 依據業務屬性，進行資通系統(服務)分類，將資通系統(服務)分成下列類別：

3.4.1.1 行政類：係指本分署內部輔助科室之業務。如秘書、會計、人事、政風等支援服務事項之科室。

3.4.1.2 業務類：指本分署內部業務單位之業務。

3.5 識別資通系統類別

3.5.1 評估資通系統為核心系統或非核心系統。

3.5.2 若為核心系統，則說明核心資通服務名稱。

3.5.3 若為各科室業務或共用資訊資產之資通服務，則選擇「不適用」。

3.6 設定安全等級

3.6.1 由資通系統(服務)負責人根據「安全等級設定原則」評估四個影響構面的衝擊以及填寫影響構面等級。

3.6.2 安全等級區分為「普級」、「中級」、與「高級」三項。

3.6.3 安全等級整體歸屬則採取「最大原則」，即為四個影響構面等級最大者為最後資訊服務的安全等級。

3.6.4 安全等級設定原則

3.6.4.1 機密性：資通系統(服務)發生資安事件時，可能造成資料外洩或遭竄改等情事，導致資料機密性受到損害。「機密性」影響構面安全等級設定原則如下：

安全等級	安全等級評估說明
普	▪ 發生資通安全事件致資通系統受影響時,可能造成未經授權之資訊揭露,對本分署之營運、資產或信譽等方面將產生有限之影響。
中	▪ 發生資通安全事件致資通系統受影響時,可能造成未經授權之資訊揭露,對本分署之營運、資產或信譽等方面將產生嚴重之影響。

安全等級	安全等級評估說明
高	▪ 發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對本分署之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。

3.6.4.2 完整性：資通系統(服務)委外開發與營運時，若未有效執行資安防護作為，可能會造成資通系統(服務)完整性遭受破壞。「完整性」影響構面安全等級設定原則如下：

安全等級	安全等級評估說明
普	▪ 發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對本分署之營運、資產或信譽等方面將產生有限之影響。
中	▪ 發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對本分署之營運、資產或信譽等方面將產生嚴重之影響。
高	▪ 發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對本分署之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。

3.6.4.3 可用性：評估本影響構面安全等級時，應考量資通系統(服務)可容許中斷時間、資通系統(服務)受影響程度等。「可用性」影響構面安全等級設定原則如下：

安全等級	安全等級評估說明
普	▪ 發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對本分署之營運、資產或信譽等方面將產生有限之影響。 ▪ 容許中斷時間較長（超過 72 小時）。

安全等級	安全等級評估說明
中	▪ 發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對本分署之營運、資產或信譽等方面將產生嚴重之影響。 ▪ 容許中斷時間短。（中斷時間介於 24 小時至 72 小時之間）
高	▪ 發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對本分署之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。 ▪ 容許中斷時間非常短（小於 24 小時）。

3.6.4.4 法律遵循性：本影響構面之危害程度評估係基於本分署負有遵守法律規章之責任與義務下，如發生違法情事時，本分署將面臨之衝擊，本影響構面衝擊後果之嚴重程度係取決於法令規定。「影響法律規章遵循」影響構面安全等級設定原則如下：

安全等級	安全等級評估說明
普	▪ 其他資通系統設置或運作於法令有相關規範之情形。
中	▪ 如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或本分署執行業務之公正性及正當性，並使本分署或其所屬人員受行政罰、懲戒或懲處。
高	▪ 如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或本分署執行業務之公正性及正當性，並使本分署所屬人員負刑事責任。

3.6.5 完成安全等級設定後，應評估下列項目:

3.6.5.1 RPO（Recovery Point Objective）資料復原點目標。

3.6.5.2 RTO(Recovery Time Objective)復原時間目標。

3.6.5.3 MTD（Maximum Tolerable Downtime）最長可接受的中斷時間。

3.7 安全等級核定

3.7.1 資通系統(服務)負責人於完成安全等級評估作業後，應由科室主管進行複核。

3.7.2 若科室主管維持初估之結果，則於「異動」欄位填入【NA】表示不需調整；若有異動，則填入異動原因，並調整安全等級。

4. 產出紀錄

4.1 WRATB-ISMS-4-014 資通系統(服務)安全等級評估表