內部控制制度設計範例

依據內部控制制度設計原則「四、設計步驟」，以 XX 機關為例，說明設計內部控制制度之步驟，提供各機關設計內部控制制度之參考。

一、確認目標

目標分為整體層級目標及作業層級目標，整體層級目標係指各機關依法定職掌所定之願景、策略及施政目標，該目標明確闡述機關之施政重點及長期展望，並為機關全體人員共同遵循的方向。

各機關可將整體層級目標逐級往下延伸至各單位，並參考業務職掌，據以辨識相連結之作業層級目標。因此，機關全體人員便有共同之整體層級目標及具體之作業層級目標可資遵循，以達成機關之願景及使命。

「確認目標」之範例，請參閱附件「XX 機關內部控制制度範例」之「壹、整體層級目標及機關組織職掌」、「貳、作業層級目標及機關組織圖」及「參、機關分層負責明細表」。

二、風險評估

風險係指面對一些事件之發生，可能會影響機關目標之達成，並且極可能會影響對人民所提供之服務，又機關任何業務之推展都可能面臨風險，因此要強化內部控制之前提即是要做好風險評估，以辨識無法達成機關整體層級與作業層級目標之內、外在風險因素，繼而分析風險之影響程度及發生之可能性，考量風險評估之結果及風險容忍度，據以擇定應進行風險處理之業務項目。

各機關之風險評估程序得參考「行政院所屬各機關風險管理及危機處理作業基準」及「風險管理及危機處理作業手冊」辦理，因應機關特性有適宜之風險評估方法，亦可逕行採用。

「風險評估」之設計結果範例，請參閱附件「XX 機關內部控制制度範例」之「肆、風險評估」。

三、選定業務項目

根據風險評估結果，應就超過機關風險容忍度之主要風險項目，找出對應之相關業務項目，其中有關共通性業務，可參採各權責機關所定之共通性作業範例。

四、設計控制作業

各機關應針對選定業務項目之重要環節，設計相關之控制重點，如文件

是否經適當核准，事件是否經妥善記錄，物品是否定期盤點，狀況是否適時通報，預算或績效是否進行分析比較、職能是否明確劃分等。

「設計控制作業」之設計結果範例，請參閱「XX 機關內部控制制度範例」之「伍、控制作業」。

五、建立檢查機制

風險可能會隨著時間、環境、政策或機關組織變革等因素之變化而有增減，原設計之控制作業亦可能已不合時宜或不復需要，因此，各機關應執行下列之檢查機制：

(一)例行監督：由機關內部各單位主管於例行業務督導作業中，及時評估內部控制制度之有效性。

(二)自行檢查：由機關內部各單位每年至少自行檢查一次內部控制制度設計及執行之有效性，包含：

１、整體層級自行檢查：得參考「政府內部控制觀念架構」之「控制環境」、「風險評估」、「控制作業」、「資訊與溝通」及「監督」五項組成要素內涵及依各機關業務特性，列示評估重點。

２、作業層級自行檢查：得就一項作業項目製作一份自行檢查表，亦得將各項作業項目依性質分類，同一類之作業項目合併成一份自行檢查表，其格式可參採「內部控制制度共通性作業範例製作原則」所定自行檢查表辦理。如檢查重點有不適用情形者，應於檢查情形說明欄中敘明。

(三)稽核評估：由機關統合或運用行政管考、人事考核、政風查核、政府採購稽核、事務管理工作檢核及內部審核等稽核評估職能，協助審視內部控制制度之有效性。

「建立檢查機制」之設計結果範例，請參閱「XX 機關內部控制制度範例」之「陸、監督」及「柒、自行檢查之表件格式」。

附件

XX 機關(機關名稱)
內部控制制度範例

中華民國 XXX 年 XX 月 XX 日核定(核定日期)

中華民國 XXX 年 XX 月 XX 日修訂(最新修訂日期)

目次

壹、整體層級目標及機關組織職掌

一、 整體層級目標：

（一） 參與國家資通安全建設，提升政府資安防護能力。
（二） 推動政府機關業務資訊化，提升資訊服務效能。
（三） 辦理資訊教育訓練，提升政府公務員資訊專業素養。
（四） 推動中文交換共通平台機制，促進網路中文資料之流通。
（…餘略）

二、 機關組織職掌：

（一） 各機關申請設置電子計算機之審核事項。
（二） 各機關使用電子計算機效率之查核事項。
（三） 各機關電子計算機作業設備相互支援之輔導及協調事項。
（四） 各機關電子計算機作業有關人員之訓練事項。
（五） 共同性程式之設計及研究發展事項。
（六） 其他有關電子處理事項。
（…餘略）

貳、作業層級目標及機關組織圖

一、 作業層級目標：

（一）完成政府機關電腦效率查核。

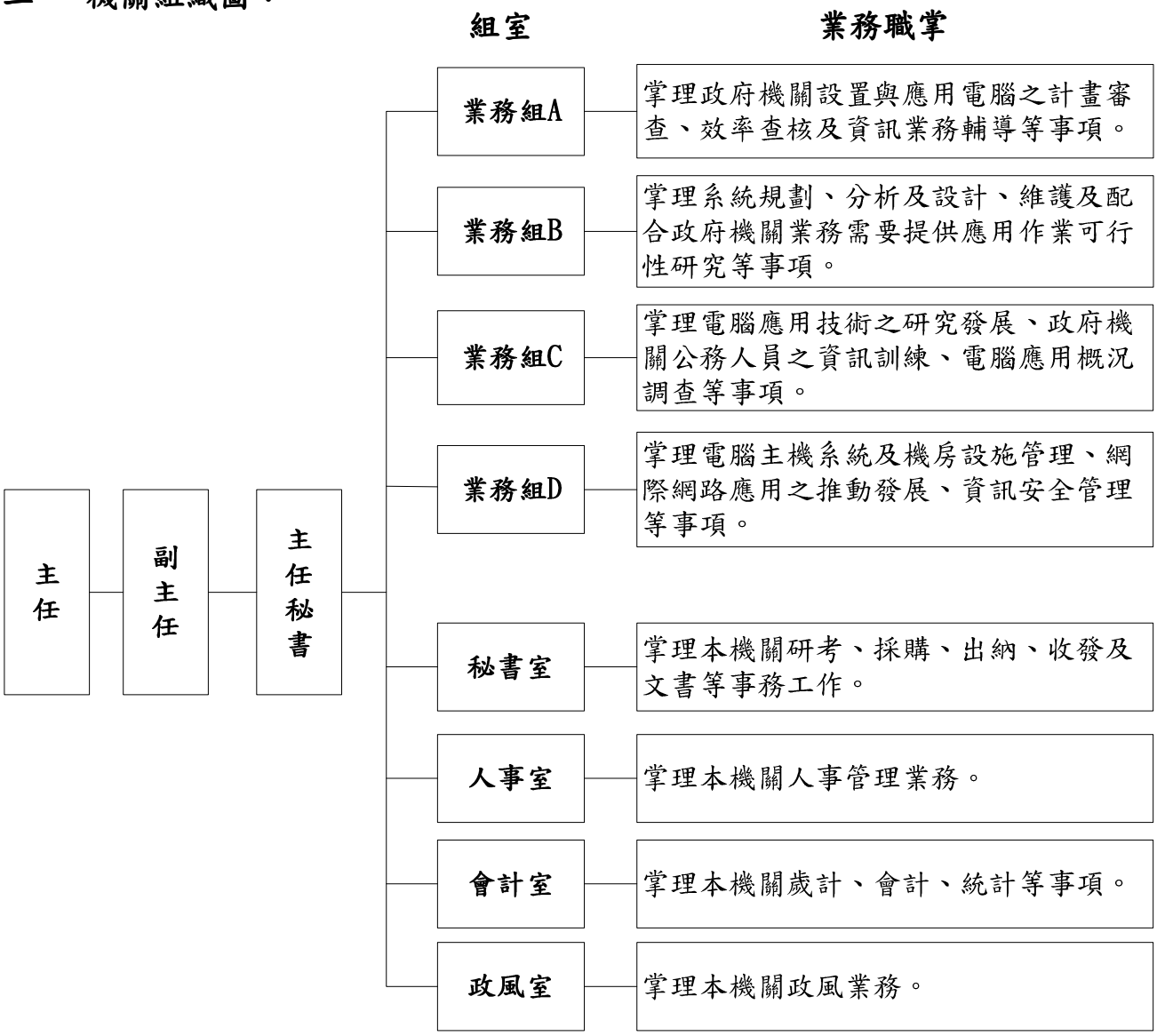
（二）促進政府共通性軟體之發展。

（三）落實公務人員資訊訓練計畫。

（四）**强化資訊安全管理防護能量。**

（…餘略）

二、 機關組織圖：



參、機關分層負責明細表(註:得以註明出處或建立來源連結之方式辦理)

XX 機關分層負責明細表					
單位	工作項目	權責區分			備考
		第一層	第二層	第三層	
		主任 副主任	主任秘書	各組室主管	
各單位共同事項	一、本機關法規之制（訂）定、修正及廢止事項。 二、根據院頒施政方針擬訂本機關各單位年度施政計畫。 …餘略	核轉或核定 核定	審核 審核	擬辦 擬辦	
業務組 A	一、各機關設置及應用電腦計畫之審議事項。 二、中央政府各機關年度資訊概算之審議事項。 …餘略	核定 核定	審核 審核	擬辦 擬辦 核定	重大事項由第一層核定
業務組 B	一、各項應用作業系統之可行性研究事項。 二、各項應用作業系統之規劃事項。 …餘略			核定 核定	重大事項由第一層核定
業務組 C	一、資訊技術應用研究計畫之核定事項。 二、資訊技術應用研究工作之執行事項。 …餘略	核定	審核	擬辦 核定	重大事項由第一層核定
業務組 D	一、本處資訊安全政策、規範及計畫等核定事項。 二、電腦主機、工作站及伺服器等管理及維護事項。 …餘略	核定	審核	擬辦 核定	重大事項由第一層核定
秘書室	一、本機關年度施政計畫之編報與管制事項。 二、本機關應向行政院、立法院、監察院提供之相關資料。 …餘略	核定 核定	擬辦 擬辦		
會計室	一、年度概（預）算之彙編事項。 二、分配預算之籌編、執行控制、申請修改分配預算及經費之審核動支事項。 …餘略	核定 核定	審核 審核	擬辦 擬辦	
人事室	一、本機關人員之派免遷調事項。 二、職務歸系作業案件之核辦事項。 …餘略	核定	審核 核定	擬辦 擬辦	
政風室	一、本機關政風工作業務之綜合規劃事項。 二、本機關政風督導小組工作推行事項。 …餘略	核定 核定	審核 審核	擬辦 擬辦	

肆、風險評估

一、風險辨識

為達成「推動政府機關業務資訊化，提升資訊服務效能」之目標，本機關提出開發共通性套裝軟體供政府各機關使用之業務計畫，如會計系統、薪資系統等，於系統維運過程，須配合相關法規或機關需求進行系統功能增修，進而發行更新版本之檔案。由於現今電腦病毒肆虐，為確保上傳檔案之「可用性」，應加強控制其掃毒機制及一旦發生中毒之通報及處理措施，以降低風險。

本機關參考「風險管理及危機處理作業手冊」中所列之風險來源，進行風險辨識。主要風險來源有科技之應用，其風險情境及影響為「本機關之網頁檔案，若遭病毒感染，承辦人員未落實通報機制，將延誤處理時機，影響服務品質，損及機關形象」。因此本機關辨識出「網頁檔案遭病毒感染」之主要風險項目。

二、風險分析

本機關參考「風險管理及危機處理作業手冊」附錄二之風險評估工具，並考量機關業務特性，訂定適用於本機關之「影響之敘述分類表」及「機率之敘述分類表」，以作為衡量風險影響程度及發生機率之標準。**(註：各機關應依業務特性，自行訂定妥適之影響及機率等級評量標準，並依風險容忍度，選定低度、中度、高度及極度危險風險之範圍，以利各機關適性、彈性地決定風險等級。)**

(一) 影響之敘述分類表

等級	衝擊或後果	形象	目標達成
3	非常嚴重	機關形象受損	經費/時間大量增加
2	嚴重	跨部門形象受損	經費/時間中度增加
1	輕微	部門形象受損	經費/時間輕微增加

(註：各機關應依業務特性，自行訂定妥適之影響等級評量標準。)

(二) 機率之敘述分類表

等級	可能性分類	詳細之描述
3	幾乎確定	每月發生一次之可能性
2	可能	每季發生一次之可能性
1	幾乎不可能	每年發生一次之可能性

(註：各機關應依業務特性，自行訂定妥適之機率等級評量標準。)

三、風險評量

經過風險分析結果，考量本機關人力、資源、組織環境等因素，擬將發生風險時影響程度「輕微(1)」或「嚴重(2)」，但「幾乎不可能(1)」發生，及發生風險時影響程度「輕微(1)」，但「可能(2)」發生之「中」或「幾乎不可能發生(1)」之「低」風險圖象區域(如下表灰色區域)，定為本次風險評估之風險容忍範圍，超出此範圍之風險項目，皆優先納入風險處理。**(註：各機關應自行評估風險容忍範圍並適時檢討。)**

本機關主要風險項目經評估後，其發生機率等級為1，影響程度等級為3，屬高度風險，超出本機關可容忍之風險範圍，應即進行風險處理，以降低風險。

風險分布

影響程度	幾乎不可能(1)	可能(2)	幾乎確定(3)
非常嚴重(3)	3（高度）	6（高度）	9（極度）
嚴重(2)	2（中度）	4（高度）	6（高度）
輕微(1)	1（低度）	2（中度）	3（高度）

發生機率

(註：各機關應依業務特性，自行擇用妥適的風險評量標準(如 3X3 表格、4X4 表格等)，並依風險容忍度，選定低度、中度、高度及極度危險風險之範圍，以利各機關適性、彈性地決定風險等級。)

伍、控制作業

本機關各項控制作業，係為確保各項業務活動皆已有效運作，相關控制重點已併入各項業務活動之作業流程中設計，包括核准、驗證、調節、覆核、定期盤點、記錄核對、職能分工、實體控制與計畫、預算或前期績效之分析比較等程序。本機關已依據風險評估結果，訂定對下列業務項目之控制作業：

一、 共通性業務：（如附件）

二、 個別性業務：（如附件）

（一） 資訊安全管理業務

（二） …(視機關業務職掌，並依重要性、風險性原則選定業務項目)

陸、 監督

本機關為強化資訊安全，目前已導入 ISO 27001 之資訊安全管理制度(ISMS)，資訊安全之監督實施方式有：

一、 由內部各單位主管例行督導各項資安業務。

二、 每年由內部各單位自行檢查一次內部控制制度設計及執行之有效性。

三、 由政風單位進行內部資訊安全查核。

四、 每年請外部驗證機構至本機關進行資安稽核。

柒、 自行檢查之表件格式

一、整體層級自行檢查表：

為評估機關整體內部控制制度設計及執行之有效性，應將內部控制之組成要素納入機關整體層級自行檢查表中，每年至少自行檢查一次，遇有特殊情形，得隨時辦理，其中「控制作業」一項，並應納入作業層級自行檢查表中進行檢查。

XX機關內部控制制度整體層級自行檢查表

XXX年度

自行檢查單位：＿＿＿＿　　檢查日期：XXX年XX月XX日

組成要素	評估重點	自行檢查情形		檢查情形說明
		符合	未符合	
一、控制環境	●是否建立及維持公務職業操守與倫理價值觀念? ●是否辦理宣導及教育訓練、提升員工瞭解與落實執行工作之專業知識、經驗及服務觀念? （…餘略）			
二、風險評估	●是否辨識影響目標達成之風險因素(事項)? ●是否監督並定期檢討可容忍之風險項目? (…餘略)			
三、控制作業	●是否訂定對各單位多項業務有廣泛影響之控管措施或控制規範? ●是否將各項控制作業納入作業層級自行檢查? （…餘略）			
四、資訊與溝通	●是否適時有效編製或蒐集資訊，並傳達給相關人員? ●是否與內部全體人員及外部人士進行溝通? （…餘略）			
五、監督	●是否建立對內部控制制度設計及執行成效之例行監督? ●是否統合或運用相關稽核評估職能，以協助審視內部控制制度設計及執行之有效性? （…餘略）			
結論/需採行之改善措施：				
填表人：　　複核：　　內控召集人：				

二、作業層級自行檢查表：

以 XX 機關為例，掌理資訊安全之業務組 D 針對資訊安全事件通報之作業，參考「內部控制制度共通性作業範例製作原則」所定之自行檢查表格式，設計自行檢查表，以利檢視實際作業是否依程序執行及有無疏漏重要環節，其內容如下。

XX 機關內部控制制度作業層級自行檢查表

XXX 年度

自行檢查單位：業務組 D

作業類別(項目)：資訊安全事件通報　　檢查日期：XXX 年 XX 月 XX 日

檢查重點	自行檢查情形		檢查情形說明
	符合	未符合	
一、作業程序說明表及作業流程圖之製作是否與規定相符。 二、內部控制制度是否有效設計及執行。			
資訊安全事件通報 一、 記錄與通知: 1. 業務承辦人員是否有填寫「資訊設備或系統異常狀況處理紀錄表」 2. 業務承辦人員是否通知權責單位資安聯絡人? 二、 判斷資安事件： 資訊安全事件之認定是否經由資安聯絡人與業務相關人員依「資安事件影響等級」共同判斷? 三、 通報資安負責人： 1. 資安聯絡人是否有填寫「資訊安全事件通報單」? 2. 資安聯絡人是否將資訊安全事件通報機關資安負責人? 3. 資安負責人是否確認資安事件影響等級，並陳資訊安全推動小組執行秘書複核? 四、 通報管理階層： 1. 各級資安事件是否通報至資訊安全推動小組執行秘書? 2. 第 4 級資安事件是否通報至資訊安全推動小組召集人? 3. 若須向外通報，是否依程序通報至國家資通安全會報?			
結論/需採行之改善措施：			
填表人：　　複核：　　單位主管：			

附件

本機關之作業流程包含內部各單位之業務，所設計之控制作業皆併入作業流程中設計，詳列如下：

一、共通性業務

(一)出納業務

(二)財產管理業務

(三)政風業務

(四)…

二、個別性業務

(一)資訊安全管理業務

1. 資訊安全事故管理作業類別

(1)資訊安全事件通報作業項目

XX 機關資訊安全事件通報作業程序說明表

項目編號	KD03
項目名稱	資訊安全事件通報
承辦單位	**業務組 D**
作業程序說明	一、 業務承辦人員自行發現，或接獲通報資安事件或異常事件時，應填寫「**資訊設備或系統異常狀況處理紀錄表**」，並通報權責單位資安聯絡人。(參考資訊安全聯絡人員名冊) 二、 資安聯絡人接獲通知後，應與業務相關人員共同判斷是否為資訊安全事件。(參考**資訊安全事件管理程序書之資安事件等級說明**) 三、 若為資訊安全事件，資安聯絡人應依狀況評估事件影響等級，並填寫「**資訊安全事件通報單**」後通報機關資安負責人。 四、 資安負責人於收到「資訊安全事件通報單」後，依狀況確認事件影響等級，並陳資訊安全推動小組執行秘書複核後依程序進行通報。 (一)對內通報 各級資安事件均應通報至執行秘書，並通知權責人員進行事件處理；若為第 4 級則另須通報至資訊安全推動小組召集人。 (二)對外通報

	若影響等級為4級或由外部單位反應之資安事件，由資訊安全推動小組召集人判斷，決定是否向國家資通安全會報通報。
控制重點	一、 **記錄與通知**：業務承辦人員應填寫「資訊設備或系統異常狀況處理紀錄表」，並通知權責單位資安聯絡人。 二、 **判斷資安事件**：資安聯絡人應與業務相關人員共同判斷是否為資訊安全事件。 三、 **通報資安負責人：**資安聯絡人評估資安等級，並填寫**「資訊安全事件通報單」**，通報機關資安負責人，由資安負責人確認後陳資訊安全推動小組執行秘書複核。 四、 **通報管理階層：** 各級資安事件均應通報至執行秘書，第4級另應通報至資訊安全推動小組召集人，由其決定是否向國家資通安全會報通報。
法令依據	資訊安全事件管理程序書
使用表單	資訊安全聯絡人員名冊 資訊設備或系統異常狀況處理紀錄表 資訊安全事件通報單 資訊安全推動小組組織圖

XX 機關資安事件通報作業流程圖