

機關檔案風險管理作業說明

壹、依據

- 一、檔案法第 1 條。
- 二、國家發展委員會檔案管理局組織法第 2 條。
- 三、檔案法施行細則第 27 條。
- 四、國家發展委員會檔案管理局中程施政計畫(106 至 109 年度)。
- 五、機關檔案風險管理制度推動實施計畫。

貳、目的

- 一、推動機關檔案風險管理作業標準化，強化各級檔案管理人員風險意識。
- 二、落實檔案風險控管機制，確保檔案永續典藏及便利開放應用。

參、實施對象

推動對象為中央及地方各級機關；中央三級以下機關及地方二級以下機關，由其上一級機關負責考評所屬機關執行成效。

肆、作業程序

自 109 年起，各機關於每年 3 月底前運用國家發展委員會檔案管理局（以下簡稱檔案局）提供之線上評估系統，完成風險評估，並依評估結果接續辦理風險處理與風險監控事宜。程序如下：

一、風險評估

(一) 前置作業

1. 依據機關檔案管理中長程規劃，確認檔案管理應達成之工作目標；同時整理前一年度檔案風險處理與監控結果，作為風險評估參據。
2. 各機關參考「機關檔案風險發生機率等級敘述參考表」（如附表 1-1）及「機關檔案風險影響程度等級敘述參考表」（如附表 1-2），並依機關業務性質、管有檔案價值、檔案管理狀況及內外部環境等情形，調整編定適合本機關之風險等級敘述表，以作為評定自行增列項目風險值之依據。
3. 各機關可容忍風險值（即發生機率等級與衝擊影響等級之乘積）界定為 2，亦即等於或大於 3 之中高度風險以上之風險項目，即應研訂處置方案並進行風險處理；至在可容忍範圍者，應持續監控。

(二) 風險辨識

1. 除了線上評估系統「機關檔案風險評量表」（如附表 2）預設之共通風險項目外，應參酌以下事項再行辨識增列風險項目：
 - (1) 衡酌檔案管理目標及例行業務風險，增列風險項目。
 - (2) 回顧檢討輿情反應、民眾陳情、內外在情勢、上級政策方向等，避免遺漏潛在風險因素。
 - (3) 檢核前一年度檔案風險處理與監控結果，確認是否增列風險項目。

2. 針對重新辨識後增列之風險項目，應辦理下述事項：

(1) 將該風險項目填列於線上評估系統。

(2) 再行調整編定適當之風險等級敘述表，列示機率與影響之等級敘述，以作為評定自行增列項目風險值之依據。

(三) 風險分析

1. 線上評估系統所預設之共通風險項目，各機關應逐項依系統所示等級判斷標準，判斷風險發生機率與影響程度等級。

2. 各機關增列之風險項目應依自訂之機率等級及影響等級，判定各項風險發生機率及影響程度等級。

3. 在評定風險等級時，機率與影響之評估皆以最嚴重者為評估等級，相關原則如下：

(1) 每一個風險項目預估發生機率之次數超過一次者，在評定影響程度時，以各次中最嚴重者為該風險項目之影響等級。

(2) 每一個風險項目預估將造成多重影響者，以風險等級最高者為該風險項目之影響等級。

(四) 風險評量

1. 各機關依據系統功能完成各項風險項目之評量，並由系統自動運算各項目之風險值，該值為發生機率與影響程度等級之乘積。

2. 各機關利用系統自動產出風險分析圖，各風險等級依分布區分為極度、高度、中高度、中度、低度等 5 個風險級別（分析圖及判斷基準如附表 3）：

- (1)極度風險(風險值 9)：應即刻採取改正行動。
- (2)高度風險(風險值 4~6)：必須研訂處置方案。
- (3)中高度風險(風險值 3)：必須明定管理階層權責並強化監督。
- (4)中度風險(風險值 2)：必須指定專人持續監控。
- (5)低度風險(風險值 1)：以一般步驟處理即可。

二、風險處理

各機關風險項目依前述評量結果，針對重要風險項目及高度風險以上之風險項目，於線上評估系統逐一規劃研訂因應措施(參考範例如附表 4)，並確實執行及自我控管。

三、風險監控

- (一)若機關訂有內部控制制度者，可擇選前述風險項目列入機關內部控制項目，續依內部控制規定(含自行評估、內部稽核等)辦理。
- (二)若機關未訂定內部控制制度者，由機關自行賡續控管或檢討改善。

四、風險滾推

各機關每年循環滾動辦理風險評估，依據風險監控結果，檢討前次實施之因應措施是否有效降低風險項目之風險值，並據以修正或設計新的因應措施。

五、附則

本作業說明如有未盡事宜，檔案局得適時補充或修正之。

附表 1-1 機關檔案風險發生機率等級敘述參考表

等級 (L)	發生類別	發生描述
3	幾乎確定發生	每月發生 1 次之可能性
2	可能發生	每季發生 1 次之可能性
1	幾乎不可能發生	每年發生 1 次之可能性

附表 1-2 機關檔案風險影響程度等級敘述參考表

等級 衝擊 或後果	3	2	1
	非常嚴重	嚴重	輕微
形象	引起社會大幅負面 討論與批評	新聞媒體負面報導或 網路傳播	無新聞媒體負面報導
人員 註1	死亡	重傷	輕傷
社會 反應	民眾抗議	團體陳情	個人陳情 (5 人次以上)
經費 增加	大量增加	中度增加	輕微增加
檔案 毀損 註2	毀損比例 10%以上	毀損比例 3%-9%	毀損比例 2%以下
檔案 遺失	遺失永久保存檔案， 且無複製品或可取 代之他機關檔案	遺失定期保存檔案， 且無複製品或可取 代之他機關檔案	遺失永久保存檔案， 但有複製品或可取 代之他機關檔案
影響檔案 管理內部 運作	中斷運作 2 日以上	中斷運作 1 日	中斷運作未達 1 日
影響檔案 服務	中斷服務 2 日以上	中斷服務 1 日	中斷服務未達 1 日
影響活動 舉辦	活動無法舉行	活動內容減少	活動延後舉行
影響計畫 執行	相關計畫無法執行	相關計畫重行修正	相關計畫延後執行

註：

1. 人員指機關內部人員或民眾。
2. 參考年度機關檔案管理調查之永久檔案毀損情形，訂定其比例。
3. 機關如需增列「衝擊或後果」項目者，可利用系統功能增列之。

附表 2 機關檔案風險評量表

編號	風險項目	發生機率 等級			影響程度 等級			不適用
		1	2	3	1	2	3	
【A】	共通項目							
1	機關檔案管理人力不足，無法妥善管理檔案							
2	機關檔案管理人員專業知能不足，影響檔案管理品質							
3	檔案銷毀前後處置失當，致應銷毀檔案遭棄置、遺失或外流							
4	機關辦理機密檔案管理作業不當，造成機密外洩，影響民眾權益及國家安全							
5	檔案立案編目品質不佳，影響檔案鑑定、清理及開放應用							
6	機關檔案庫房設置位置失當，因水患造成檔案毀損							
7	機關檔案庫房安全措施未完善，造成檔案失竊或遭破壞							
8	機關檔案因庫房溫溼度控制不良，加速檔案損壞							
9	檔案原件提供檢調應用，造成檔案原件損毀或遺失							
10	文書檔案資訊系統故障，中斷機關行政及內部管理運作							
11	系統遭遇病毒、駭客或惡意程式等外部攻擊，致檔案資料被竊取或竄改							

編號	風險項目	發生機率 等級			影響程度 等級			不適用
		1	2	3	1	2	3	
12	電子檔案儲存設備過時，致資料無法讀取							
【B】 自行增列	(機關自行增列)……							
	……							
	……							

註：

1. 風險項目經評估確定不會發生，亦不會產生任何影響者，即勾選「不適用」。
2. 共通風險項目發生機率及影響程度之判斷標準依本局所訂之等級敘述選定之（詳如附表 2-1，屆時由系統輔助顯示）。

附表 2-1 共通風險項目發生機率及影響程度等級判斷標準

編號	共通風險項目	「發生機率」等級 判斷標準		「影響程度」等級 判斷標準	
		等級	判斷標準	等級	判斷標準
1	機關檔案管理人力不足，無法妥善管理檔案	等級 1	$\frac{\text{近 1 年實際辦理檔案管理人數}}{\text{機關檔案管理合理員額}} \geq 1$	等級 1	未於年度內完成檔案清查工作。
		等級 2	$0.5 \leq \frac{\text{近 1 年實際辦理檔案管理人員}}{\text{機關檔案管理合理員額}} < 0.7$	等級 2	未於每月辦理檔案立案編目。
		等級 3	$\frac{\text{近 1 年實際辦理檔案管理人數}}{\text{機關檔案管理合理員額}} < 0.5$	等級 3	未於每週辦理檔案點收作業。
2	機關檔案管理人員專業知能不足，影響檔案管理品質	等級 1	近 1 年 80%機關檔案管理人員已完成檔案局提供之檔案管理「基礎實務」及「專業進階」培訓課程。	等級 1	能規劃機關檔案管理業務，以及進行工作成效評估及提出改善建議，但尚未能輔導機關同仁與所屬。
		等級 2	近 1 年 80%機關檔案管理人員已完成檔案局提供之檔案管理「基礎實務」培訓課程，但完成「專業進階」培訓課程者未達 80%。	等級 2	能規劃機關檔案管理業務，但尚未能進行工作成效評估及提出改善建議，以及輔導機關同仁與所屬。
		等級 3	近 1 年所有機關檔案管理人員已完成檔案局提供之檔案管理「基礎實務」培訓課程者未達 80%。	等級 3	無法規劃機關檔案管理業務、進行工作成效評估及提出改善建議，以及輔導機關同仁與所屬。

編號	共通風險項目	「發生機率」等級 判斷標準		「影響程度」等級 判斷標準	
3	檔案銷毀前後處置失當，致應銷毀檔案遭棄置、遺失或外流	等級 1	近 1 年核准銷毀檔案於半年內始完成銷毀作業。	等級 1	應銷毀檔案遭棄置、遺失或外流，致檔案內容資訊外洩，但無新聞媒體負面報導。
		等級 2	近 1 年核准銷毀檔案於半年至 1 年內始完成銷毀作業。	等級 2	應銷毀檔案遭棄置、遺失或外流，引起新聞媒體負面報導或網路傳播。
		等級 3	近 1 年核准銷毀檔案超過 1 年始完成銷毀作業。	等級 3	應銷毀檔案遭棄置、遺失或外流，引起社會大幅負面討論與批評。
4	機關辦理機密檔案管理作業不當，造成機密外洩，影響民眾權益及國家安全	等級 1	近 1 年有歸檔案件未依規定使用機密檔案專用封套彌封及簽章，但有專人管理且存放於安全場所管理。	等級 1	機關內與該業務無關人員知悉一般公務機密或機敏資訊，但無新聞媒體負面報導。
		等級 2	近 1 年有歸檔案件依規定使用機密檔案專用封套彌封及簽章，但無專人管理或未存放於安全場所管理。	等級 2	一般公務機密或機敏資訊外流，使機關外部人員知悉，引起民眾陳情或抗議。
		等級 3	近 1 年有歸檔案件未依規定使用機密檔案專用封套彌封及簽章，且無專人管理及未存放於安全場所管理；或檔案局評鑑或主管機關考評發現機關機密檔案管理作業不當。	等級 3	一般公務機密或機敏資訊外流，引起新聞媒體負面報導或網路傳播。

編號	共通風險項目	「發生機率」等級 判斷標準		「影響程度」等級 判斷標準	
5	檔案立案編目品質不佳，影響檔案鑑定、清理及開放應用	等級 1	近 1 年發生 1 次檔案銷毀或移轉目錄無法判定遭檔案局退件或民眾反映檔案目錄著錄資訊與檔案內容不符情形。	等級 1	需進行 1 個年度之檔案目錄修正，始能辦理檔案鑑定、清理及開放應用。
		等級 2	近 1 年發生 2 至 3 次檔案銷毀或移轉目錄無法判定遭檔案局退件或民眾反映檔案目錄著錄資訊與檔案內容不符情形。	等級 2	需進行 2 至 3 個年度之檔案目錄修正，始能辦理檔案鑑定、清理及開放應用。
		等級 3	近 1 年發生超過 3 次檔案銷毀目錄或移轉無法判定遭檔案局退件，或民眾反映檔案目錄著錄資訊與檔案內容不符情形；或檔案局評鑑或主管機關考評發現機關立案編目品質不佳。	等級 3	需進行超過 3 個年度之檔案目錄修正，始能辦理檔案鑑定、清理及開放應用。
6	機關檔案庫房設置位置失當，因水患造成檔案受損	等級 1	檔案庫房設置於 2 樓以上。	等級 1	保存年限未達 30 年且無機敏資訊之檔案受損。
		等級 2	檔案庫房設置於 1 樓或地下室，但有完善防水措施(如警示、阻絕、抽排水設備及水損搶救計畫等)。	等級 2	保存年限 30 年以上且無機敏資訊之檔案受損。
		等級 3	檔案庫房設置於 1 樓或地下室，且缺乏完善防水措施。	等級 3	具機敏資訊之檔案受損。
7	機關檔案庫房安全措施未完善，造成檔案	等級 1	檔案庫房位於機關內，有門禁管制措施或錄影監視系統；或位於機關	等級 1	保存年限未達 30 年且無機敏資訊之檔案失竊或遭破壞。

編號	共通風險項目	「發生機率」等級 判斷標準		「影響程度」等級 判斷標準	
	失竊或遭破壞		外但有人看管，有門禁管制措施或遠端監控錄影監視系統。		
		等級 2	檔案庫房位於機關內，無門禁管制措施及錄影監視系統；或位於機關外但有人看管，無門禁管制措施及遠端監控錄影監視系統。	等級 2	保存年限 30 年以上且無機敏資訊之檔案失竊或遭破壞。
		等級 3	檔案庫房位於機關外無人看管，且無遠端監控錄影監視系統；或近 1 年檔案局評鑑或主管機關考評發現機關檔案庫房安全措施未完善。	等級 3	具機敏資訊之檔案失竊或遭破壞。
8	機關檔案因庫房溫溼度控制不良，加速檔案受損	等級 1	檔案庫房設有溫溼度控制設備，近 1 年有定期記錄，但曾發生溫溼度異常情形。	等級 1	保存年限未達 30 年且無機敏資訊之檔案受損。
		等級 2	檔案庫房設有溫溼度控制設備，近 1 年無定期記錄。	等級 2	保存年限 30 年以上且無機敏資訊之檔案受損。
		等級 3	檔案庫房無設置溫溼度控制設備；或近 1 年檔案局評鑑或主管機關考評發現機關檔案庫房溫溼度控制不良。	等級 3	具機敏資訊之檔案受損。
9	檔案原件提供檢調應用，造成檔案原件毀損或遺失	等級 1	近 1 年以原件提供檢調應用之檔案，占所有檢調件數 20%(不含)以下。	等級 1	保存年限未達 30 年且無機敏資訊之檔案毀損或遺失。
		等級 2	近 1 年以原件提供檢調應用之檔案，占所有檢調件數 20%~50%。	等級 2	保存年限 30 年以上且無機敏資訊之檔案毀損或遺失。

編號	共通風險項目	「發生機率」等級 判斷標準		「影響程度」等級 判斷標準	
		等級 3	近 1 年以原件提供檢調應用之檔案，占所有調件數 50%(不含)以上。	等級 3	具機敏資訊之檔案毀損或遺失。
10	文書檔案資訊系統故障，中斷機關行政及內部管理運作	等級 1	近 1 年內曾服務中斷次數在 1 次以下。	等級 1	系統服務需於中斷後 1 小時內始能恢復正常運作
		等級 2	近 1 年內曾服務中斷次數在 2 次至 3 次。	等級 2	系統服務需於中斷後超過 1 小時至 2 天內始能恢復正常運作。
		等級 3	近 1 年內曾服務中斷次數在 4 次以上。	等級 3	系統服務需於中斷後超過 2 天始能恢復正常運作。
11	系統遭遇病毒、駭客或惡意程式等外部攻擊，致檔案資料被竊取或竄改	等級 1	近 1 年內被竊取或竄改次數在 1 次以下；或現行檔案資料具有防火牆及防毒軟體保護者。	等級 1	造成少於 10 萬元之財產損失；或內含保存年限 10 年以下而無實體原件之檔案。
		等級 2	近 1 年內被竊取或竄改次數在 2 次至 4 次；或現行檔案資料僅有防火牆保護者。	等級 2	造成 10 萬元以上，未達 50 萬元之財產損失；或內含保存年限超過 10 年，未達 20 年而無實體原件之檔案。
		等級 3	近 1 年內被竊取或竄改次數在 5 次以上；或現行檔案資料無防火牆保護；或尚無專人檢查病毒碼即時更新。	等級 3	造成 50 萬元以上之財產損失；或內含保存年限超過 20 年而無實體原件之檔案。
12	電子檔案儲存設備過時，致資料無法讀取	等級 1	近 1 年內有 1 件以下電子檔案無法讀取；或現行使用之儲存媒體製造時間均在近 3 年以內，但未實施每年辦理電子檔清查作業者。	等級 1	無法讀取之電子檔案有保存年限 10 年以下者。

編號	共通風險項目	「發生機率」等級 判斷標準		「影響程度」等級 判斷標準	
		等級 2	近 1 年內有 2 件以上電子檔案無法讀取；或現行使用之儲存媒體中有製造時間迄今超過 3 年者；或近 3 年未曾辦理電子檔案清查作業。	等級 2	無法讀取之電子檔案有保存年限超過 10 年且未達 20 年者。
		等級 3	近 1 年內有超過 5 件電子檔案無法讀取；或現行使用之儲存媒體中有製造時間迄今超過 5 年者；或近 5 年未曾辦理電子檔案清查作業；或有電子檔案已無讀取設備或軟體界面但仍未轉置者。	等級 3	無法讀取之電子檔案有保存年限超過 20 年者。

註：

1. 實際辦理檔案管理人數之計算，專辦人員計列 1 人，兼辦人員依其工作項目中檔案管理所占比重計列(如 0.5 人)；以上人員含正式公務人員、約聘僱人員、派遣人員、臨時人員等。
2. 機關檔案管理合理員額，係指依機關檔案管理作業手冊第 6 章表 6-1「機關檔案管理人員員額配置計算方式」核算之員額。

附表 3 風險分布及風險等級判斷基準

影響程度 等級	風 險 分 布		
3	<u>風險值 3</u> 中高度風險，必須 明定管理階層權責 並強化監督	<u>風險值 6</u> 高度風險，必須研 訂處置方案	<u>風險值 9</u> 極度風險，應即刻 採取行動
2	<u>風險值 2</u> 中度風險，必須指 定專人持續監控	<u>風險值 4</u> 高度風險，必須研 訂處置方案	<u>風險值 6</u> 高度風險，必須研 訂處置方案
1	<u>風險值 1</u> 低度風險，以一般 步驟處理	<u>風險值 2</u> 中度風險，必須指 定專人持續監控	<u>風險值 3</u> 中高度風險，必須 明定管理階層權責 並強化監督
	1	2	3
	發 生 機 率 等 級		

附表 4 機關檔案風險評估及處理表(參考範例)

序次	風險項目	風險分析		風險值 (發生機率) * (影響程度)	因應措施
		發生機率等級	影響程度等級		
1	A9. 檔案原件提供檢調應用，造成檔案原件損毀或遺失	2	2	4	1. 針對高使用率之檔案原件優先辦理複製儲存作業。 2. 未辦理複製儲存之檔案原件，如有檢調應用需求，以影本提供之。
2	A12.	3	1	3	
3	B1.	2	3	6	
4	B2.	1	3	3	