計網中心內部控制作業項目

國立金門大學計算機與網路中心業務內部控制作業

一、計算機與網路中心作業職掌:

計算機與網路中心(以下簡稱本中心)主要任務為推展計算機與網路之教學與研究、促進校務行政電腦化、整合全校電腦與網路資源、規劃與維護校園網路、提升資訊處理事項之營運效能及資訊資產安全等。

計算機與網路中心作業目標:

強化資訊安全管理,確保所屬之資訊資產的機密性、完整性及可用性,提供本校資訊化業務得以持續運作之高效環境,並符合相關法規之要求,使其免於遭受內、外部的蓄意或意外之威脅性。

二、風險評估:

(一) 針對全校性合法使用的電腦、網路及資訊系統之機密性、完整性與可用性,進行相關管理作業,監控相關系統服務狀況,做好風險管理、備援規劃,以保障資產安全,避免服務失效可能性及外部因素造成的干擾與損害。

(二) 建立資訊安全管理規範,協助校務行政作業符合法令規定,強化網路及資訊系統運作之穩定與可靠性,降低校園網路與資訊服務系統維運風險,維護組織服務品質與作業效能。

三、選定業務項目:

目前選定網路管理、資訊安全管理、資安事件通報與應變、電子郵件帳號管理、計算機與網路中心電腦教室管理、校務系統資料庫及伺服器主機復原計畫及測試、數位教學平台資料庫及伺服器主機復原計畫與測試等7項重要作業項目,研訂內部控制相關作業。

四、控制作業:

本校各項計算機與網路控制作業,係為確保各項業務活動皆可有效運作,相關控制重點已併入各項業務活動之作業流程中設計。

本中心依據前述作業目標及風險評估結果,訂定對下列業務項目之控制作業:

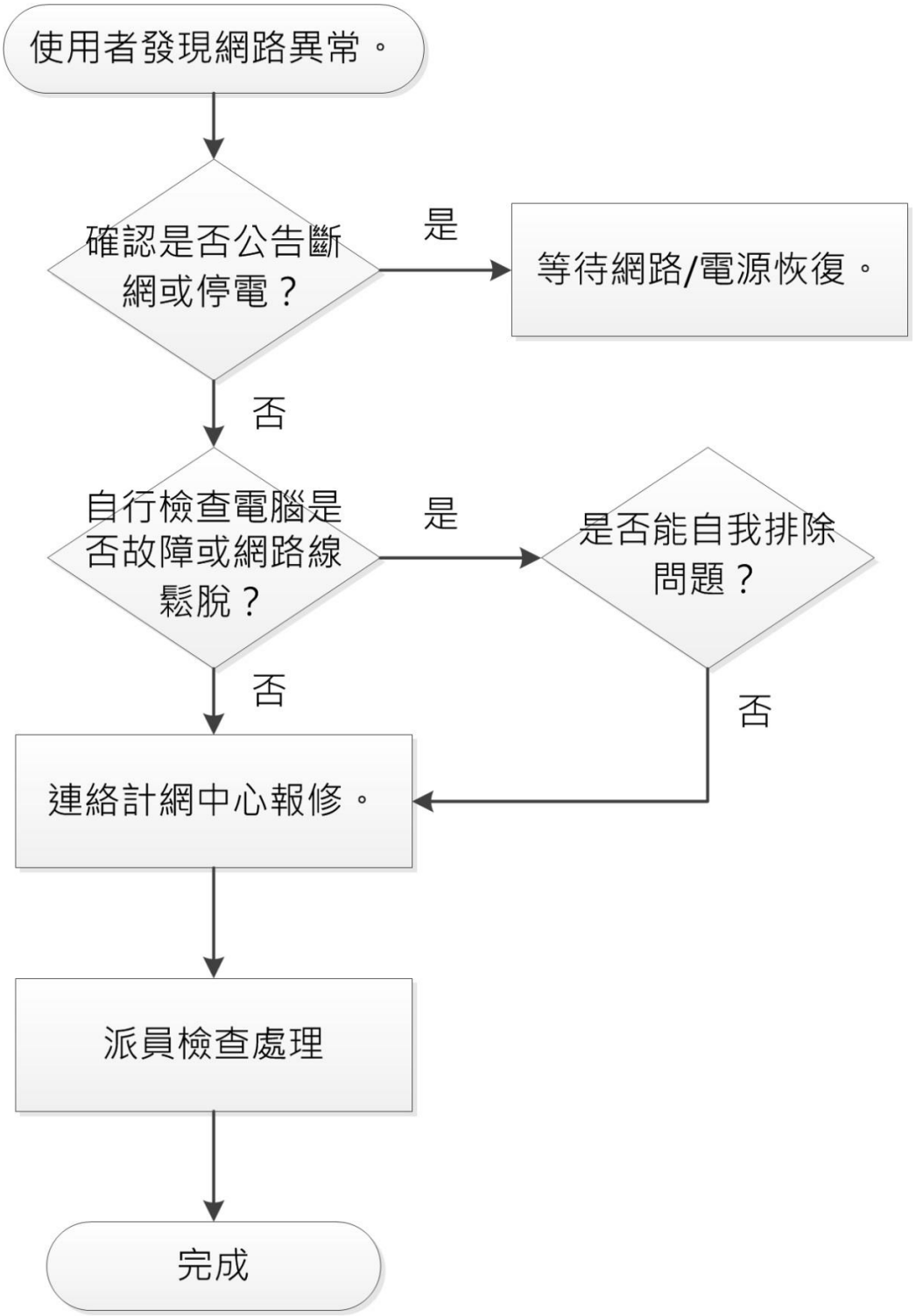
項目編號	訂定作業項目
AI0101	國立金門大學網路管理作業
AI0102	國立金門大學資訊安全管理作業
AI0103	國立金門大學資安事件通報與應變作業
AI0104	國立金門大學電子郵件帳號管理作業
AI0201	國立金門大學計算機與網路中心電腦教室管理作業
AI0202	國立金門大學校務系統資料庫及伺服器主機復原計畫與測試作業
AI0203	國立金門大學數位教學平台資料庫及伺服器主機復原計畫與測試作業

國立金門大學計算機與網路中心作業程序說明表

項目編號	AI0101
項目名稱	網路管理作業
承辦單位	計算機與網路中心 資訊網路組
相關單位	全校各單位
作業程序說明	一、 組態管理： (一) 為維護網路骨幹正常運作，必須定時備份網路骨幹設備組態檔。 (二) 網路設備除網路線連接後，還須進行設備內部組態檔設定，才能符合校園網路需求而正常運作，備份組態檔的用意在於當設備故障或更換設備時，可以迅速載入設備讓網路斷線的時間縮短。 (三) 每三個月定期將現有網路骨幹設備組態設定檔備份一次，以防變動時設備故障可以迅速回復原狀。 二、故障管理： (一) 依據網路管理作業流程辦理。 (二) 使用者發現自己網路不通後應立即檢查自己設備，是否為個人操作問題。 (三) 如非個人操作問題請聯絡本中心資訊網路組協助檢查。 三、效能管理： (一) 依據「國立金門大學校園網路流量管理辦法」辦理。 (二) 本校師生欲使用校園有線網路及無線網路服務者，應依規定辦理申請。 (三) 設定每部設備每日下載之網路流量總合，超過者依「國立金門大學校園網路流量管理辦法」辦理。 四、固定 IP 位址申請： (一) 依據校園網路 IP 申請表辦理申請。 (二) 應確實填寫申請表所需資料。 (三) 詳細閱讀其辦法規則，並予以遵守。 (四) 長官核准後即可送出申請表。 (五) 由本中心核准後發給固定 IP 位址並予以記錄做為日後查詢依據。 五、網域名稱申請： (一) 依據網域名稱申請表辦理。 (二) 應確實填寫申請表所需資料。 (三) 詳細閱讀其辦法規則，並予以遵守。 (四) 無固定實體 IP 位址者，應先行申請。 (五) 長官核准後即可送出申請表。

	(六) 由本中心核准後發給後予以設定並做紀錄供日後查詢依據。 六、無線網路： (一) 於校園內提供本校教職員生無線上網服務。 (二) 以電子郵件帳號做為上網之資訊安全管控措施。 (三) 支援全國學術網路無線漫遊服務。 (四) 無線網路連線設定，請參照本中心網頁「無線網路相關資訊」。
控制重點	每三個月備份一次校園網路骨幹設備組態檔。
法令依據	一、 國立金門大學校園網路流量管理要點。 二、 國立金門大學校園網路使用規範。 三、 國立金門大學 P2P 管理辦法。
使用表單	一、網路節點 IP 位址申請。 二、NQU-ISMS-4-021 系統與網路檢查紀錄表。 三、NQU-ISMS-4-022 防火牆進出規則申請表。 四、NQU-ISMS-4-025 營運持續運作計畫。 五、NQU-ISMS-4-038 域名解析服務申請異動表。 六、NQU-ISMS-4-039 外對內連線服務申請表。

國立金門大學網路管理作業流程圖



國立金門大學內部控制制度控制作業自行評估表

○○年度

評估單位：計算機與網路中心

作業類別(項目)：網路管理作業

評估期間：○○年○○月○○日至○○年○○月○○日

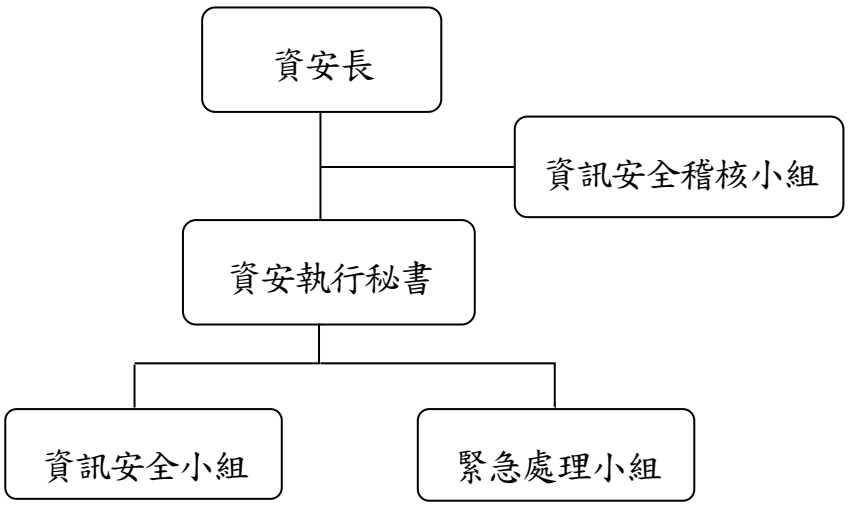
評估日期：　年　月　日

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、每三個月備份一次校園網路骨幹設備組態檔。						
填表人：　　複核：						

註：

1. 機關得就1項作業流程製作1份自行評估表，亦得將各項作業流程依性質分類，同1類之作業流程合併1份自行評估表，將作業流程之控制重點納入評估。
2. 各機關依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「不適用」或「其他」；其中「不適用」係指評估期間法令規定或作法已修正，但控制重點未及配合修正者；「其他」係指評估期間未發生控制重點所規範情形等，致無法評估者；遇有「部分落實」、「未落實」或「不適用」情形，於改善措施欄敘明需採行之改善措施。

國立金門大學計算機與網路中心作業程序說明表

項目編號	AI0102
項目名稱	資訊安全管理作業
承辦單位	計算機與網路中心
相關單位	全校各單位
作業程序說明	一、建立資訊安全管理制度 (一) 界定資訊安全管理制度之範圍。 (二) 依實際業務需求，訂定資訊安全政策。 (三) 定義風險評鑑方法。 (四) 識別各項風險。 (五) 分析與評估各項風險。 (六) 識別並評估風險處理之選項作法。 (七) 選擇控制目標及控制措施以處理風險。 (八) 取得管理階層對所提議之剩餘風險的核准。 (九) 取得管理階層對實施和運作資訊安全管理制度的授權。 (十) 擬定一份適用性聲明書。 二、 實施與運作資訊安全管理制度 (一) 成立資訊安全管理委員會，運作資訊安全管理制度。 資訊安全管理委員會架構如下圖所示：  (二) 制訂並實施風險處理計畫，以達成所識別的各項控制目標。 (三) 實施所選擇的控制措施，以符合控制目標。 (四) 定義如何量測所選擇的控制措施之有效性，並規定如何使用這些量測去評鑑控制措施的有效性，以產生可比較的結果。 (五) 實施教育訓練與認知計畫。 (六) 實施能夠偵測並回報安全事故的程序及其他控制措施。

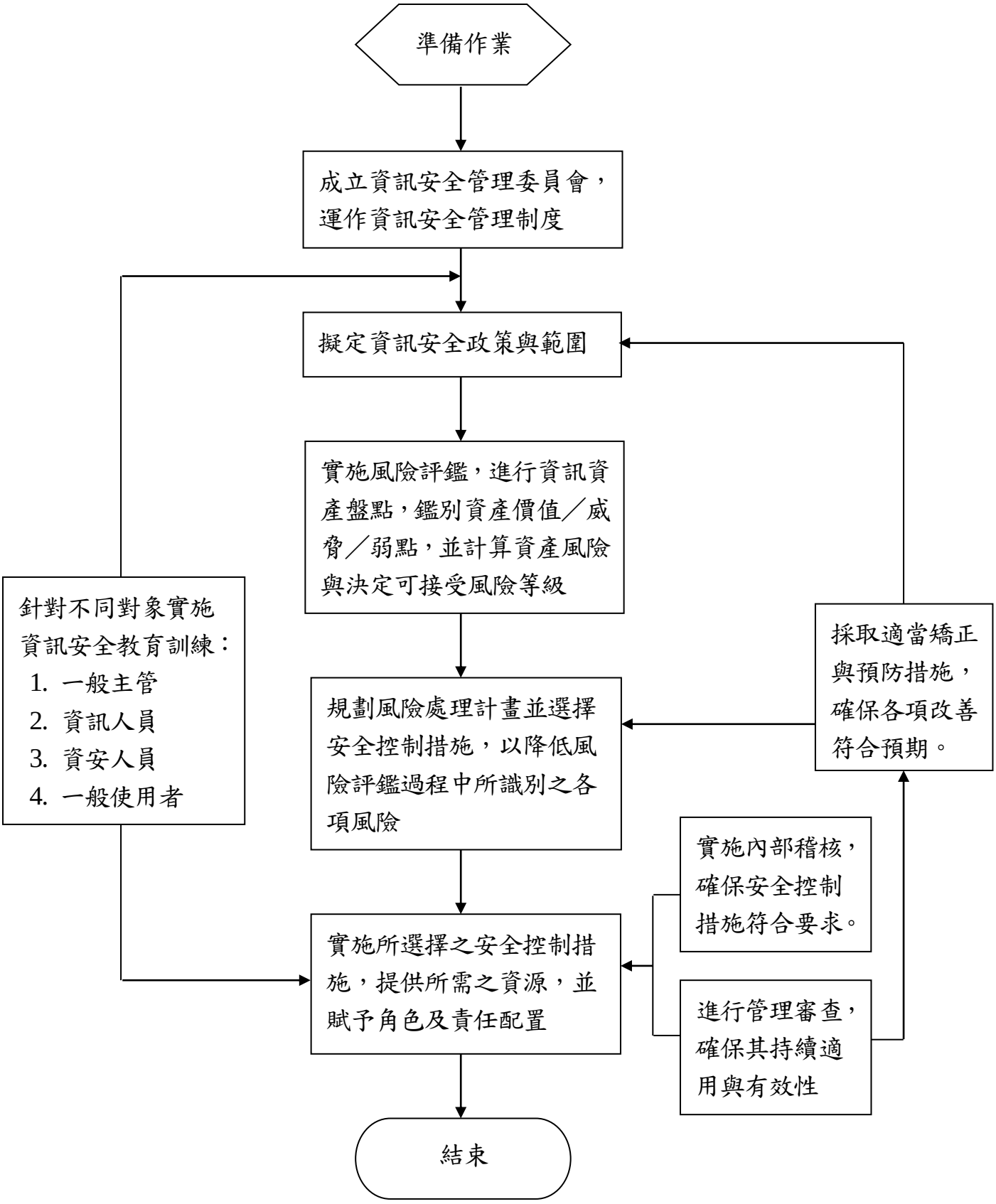
	三、 監督與審查資訊安全管理制度 (一) 執行監督與審查程序及其他控制措施。 (二) 定期審查資訊安全管理制度的有效性(包括是否符合資訊安全政策與目標，以及安全控制措施的審查)，並將安全稽核、事故、有效性測量,以及來自所有利害相關者之建議與回饋的結果納入考量。 (三) 量測控制措施的有效性，以查證已符合各項安全要求。 (四) 依照規劃之期程，定期審查風險評鑑，並審查剩餘風險的等級與已識別的可接受風險。 (五) 依照規劃之期程，實施資訊安全內部稽核。 (六) 定期執行資訊安全之管理階層審查，以確保其範圍之適當性，且資訊安全管理過程之各項改善措施均已識別。 (七) 考量監督與審查活動的發現，以更新安全計畫。 (八) 記錄對資訊安全管理制度有效性或績效產生衝擊之措施與事件。 四、 維持與改善資訊安全管理制度 (一) 實施已識別之資訊安全管理制度各項改善措施。 (二) 採取適當的矯正與預防措施,並由其他機關及本中心之資訊安全經驗中學習。 (三) 與所有利害相關者就各項改善措施進行溝通。 (四) 確保各項改善措施可達到預期目標。 五、 資訊安全管理制度文件化 文件化應包括管理階層決策的紀錄，確保各項措施可追溯至管理階層決策及政策,並確保所記錄的結果是可再產生的(reproducible)。 文件化的項目包括： (一) 資訊安全政策、目標與範圍。 (二) 支援資訊安全管理制度的各項程序及控制措施。 (三) 風險評鑑方法。 (四) 風險評鑑報告。 (五) 風險處理計畫。 (六) 描述如何量測控制措施的有效性所需之文件化程序。 (七) 資訊安全管理制度中所要求之各項紀錄。 (八) 適用性聲明書。
控制重點	一、 是否成立資訊安全組織，以運作資訊安全管理制度。 二、 是否已規劃並定義出資訊安全管理制度之適用範圍。 三、 是否訂定資訊安全政策，並由管理階層核准與正式發布。

	四、 是否實施風險評鑑，並針對評鑑結果規劃適當的風險處理計畫。 五、 是否已建立及使用有效性量測指標。 六、 是否定期實施內部稽核，以確保各項安全控制措施符合要求。 七、 資訊安全管理制度所需之文件與紀錄，是否已文件化並受到適當的保護。 八、 管理階層是否定期審查資訊安全管理制度，以確保其持續的適用及有效性。
法令依據	一、 行政院及所屬各機關資訊安全管理要點。 二、 行政院及所屬各機關資訊安全管理規範。 三、 資通安全管理法。 四、 資通安全管理法施行細則。 五、 資通安全責任等級分級辦法。 六、 教育體系資通安全暨個人資料管理規範。 七、 資通安全事件通報及應變辦法。 八、 國立金門大學資通安全事件通報及應變管理程序。 九、 國立金門大學資通安全維護計畫。 十、 NQU-ISMS-1-001 資訊安全政策。 十一、 NQU-ISMS-1-002 適用性聲明。 十二、 NQU-ISMS-2-001 資訊安全組織程序書。 十三、 NQU-ISMS-2-002 文件管理程序書。 十四、 NQU-ISMS-2-003 資訊資產管理程序書。 十五、 NQU-ISMS-2-004 風險評鑑與管理程序書。 十六、 NQU-ISMS-2-005 人員安全與教育訓練程序書。 十七、 NQU-ISMS-2-006 實體安全管理程序書。 十八、 NQU-ISMS-2-007 通信與作業管理程序書。 十九、 NQU-ISMS-2-008 存取控制管理程序書。 二十、 NQU-ISMS-2-009 系統開發與維護程序書。 二十一、 NQU-ISMS-2-010 委外管理程序書。 二十二、 NQU-ISMS-2-011 安全事件管理程序書。 二十三、 NQU-ISMS-2-012 營運持續運作管理程序書。 二十四、 NQU-ISMS-2-013 資訊安全稽核作業程序書。 二十五、 NQU-ISMS-2-014 矯正及預防管理程序書。 二十六、 NQU-ISMS-3-001 資訊資產管理說明書。 二十七、 NQU-ISMS-3-002 網路及系統安全管理說明書。 二十八、 NQU-ISMS-3-003 電子郵件帳號管理說明書。

	二十九、 NQU-ISMS-3-004 帳號及通行密碼管理說明書。 三十、 NQU-ISMS-3-005 資訊備份管理說明書。 三十一、 NQU-ISMS-3-006 系統開發與維護作業說明書。 三十二、 NQU-ISMS-3-007 惡意軟體防護管理說明書。
使用表單	一、 NQU-ISMS-4-001 資訊安全組織成員表。 二、 NQU-ISMS-4-002 外部單位聯絡清單。 三、 NQU-ISMS-4-003 ISMS 有效性量測表。 四、 NQU-ISMS-4-004 文件調閱申請單。 五、 NQU-ISMS-4-005 文件修訂建議表。 六、 NQU-ISMS-4-006 資訊安全管理文件列表。 七、 NQU-ISMS-4-007 外來文件一覽表。 八、 NQU-ISMS-4-008 資訊資產清單。 九、 NQU-ISMS-4-009 威脅弱點評估表。 十、 NQU-ISMS-4-010 風險評鑑彙整表。 十一、 NQU-ISMS-4-011 風險改善計畫表。 十二、 NQU-ISMS-4-012 風險評估報告。 十三、 NQU-ISMS-4-013 保密切結書。 十四、 NQU-ISMS-4-014 離職人員帳號停用查核表。 十五、 NQU-ISMS-4-015 資訊安全教育訓練簽到表。 十六、 NQU-ISMS-4-016 人員職掌清冊。 十七、 NQU-ISMS-4-017 年度教育訓練計劃。 十八、 NQU-ISMS-4-018 人員資訊安全守則。 十九、 NQU-ISMS-4-019 人員進出機房登記表。 二十、 NQU-ISMS-4-020 設備進出紀錄表。 二十一、 NQU-ISMS-4-021 系統與網路檢查紀錄表。 二十二、 NQU-ISMS-4-022 防火牆進出規則申請表。 二十三、 NQU-ISMS-4-023 資訊安全事件通報單。 二十四、 NQU-ISMS-4-024 業務流程衝擊分析表。 二十五、 NQU-ISMS-4-025 營運持續運作計畫。 二十六、 NQU-ISMS-4-026 營運持續運作計畫演練活動紀錄。 二十七、 NQU-ISMS-4-027 資訊安全內部稽核計畫。 二十八、 NQU-ISMS-4-028 資訊安全內部稽核表。 二十九、 NQU-ISMS-4-029 資訊安全內部稽核報告。 三十、 NQU-ISMS-4-030 矯正與預防處理單。 三十一、 NQU-ISMS-4-031 設備異動申請單。

	三十二、 NQU-ISMS-4-032 系統變更申請單。 三十三、 NQU-ISMS-4-033 軟體清冊。 三十四、 NQU-ISMS-4-034 權限帳號檢視申請紀錄單。 三十五、 NQU-ISMS-4-035 校務系統使用者帳號功能模組申請表。 三十六、 NQU-ISMS-4-036 校園入口網管理帳號申請異動表。 三十七、 NQU-ISMS-4-037 網頁空間使用申請異動表。 三十八、 NQU-ISMS-4-038 域名解析服務申請異動表。 三十九、 NQU-ISMS-4-039 外對內連線服務申請表。 四十、 NQU-ISMS-4-040 電子郵件帳號申請異動單。 四十一、 NQU-ISMS-4-041 系統使用權限管理名冊。 四十二、 NQU-ISMS-4-042 資訊系統管理帳號申請異動單。 四十三、 NQU-ISMS-4-043 備份資料測試紀錄單。 四十四、 NQU-ISMS-4-044 新應用系統開發維護申請單。 四十五、 NQU-ISMS-4-045 應用系統維護申請單。 四十六、 NQU-ISMS-4-047 系統測試資料申請單。 四十七、 NQU-ISMS-4-048 會議記錄。 四十八、 NQU-ISMS-4-050 安全等級評估表 四十九、 NQU-ISMS-4-051 資訊系統清冊 五十、 NQU-ISMS-4-052 電子公文系統帳號新增移轉處理單 五十一、 NQU-ISMS-4-053 利害相關者與議題一覽表 五十二、 NQU-ISMS-4-054 政策.目標與評量對應表 五十三、 NQU-ISMS-4-055 內外部溝通或傳達一覽表。 五十四、 NQU-ISMS-4-056 資通安全維護計畫 五十五、 NQU-ISMS-4-057 雲服務專案管理表 五十六、 NQU-ISMS-4-058 組態安全管理表

國立金門大學資訊安全管理作業流程圖



國立金門大學內部控制制度控制作業自行評估表

○○年度

評估單位：計算機與網路中心

作業類別(項目)：資訊安全管理作業

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期：　年　月　日

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、是否成立資訊安全組織，以運作資訊安全管理制度。						
二、是否已規劃並定義出資訊安全管理制度之適用範圍。						
三、是否訂定資訊安全政策，並由管理階層核准與正式發布。						
四、是否實施風險評鑑，並針對評鑑結果規劃適當的風險處理計畫。						
五、是否已建立及使用有效性量測指標。						
六、是否定期實施內部稽核，以確保各項安全控制措施符合要求。						
七、資訊安全管理制度所需之文件與紀錄，是否已文件化並受到適當的保護。						
八、管理階層是否定期審查資訊安全管理制度，以確保其持續的適用及有效性。						
填表人：　　複核：						

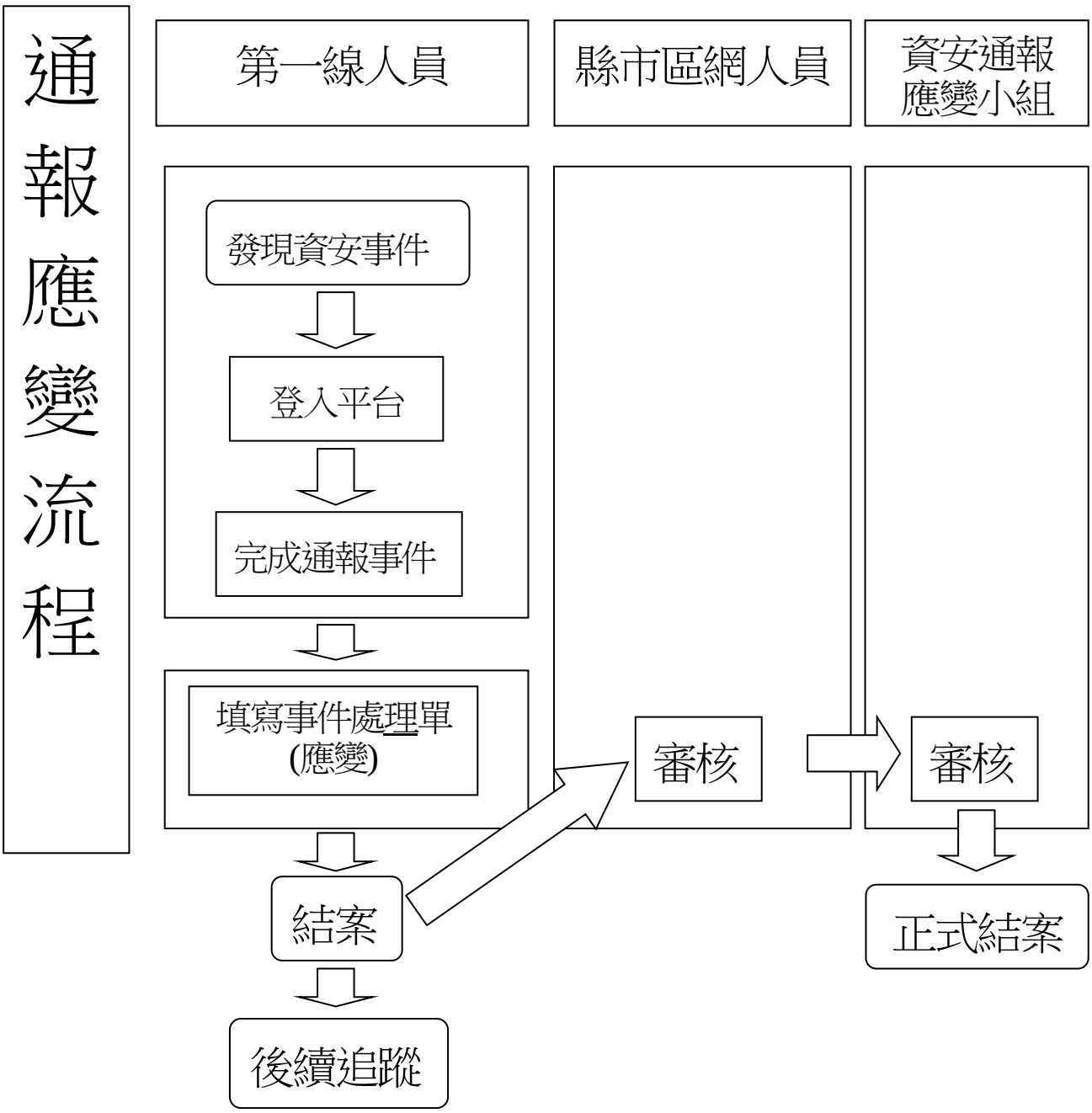
註：

1. 機關得就1項作業流程製作1份自行評估表，亦得將各項作業流程依性質分類，同1類之作業流程合併1份自行評估表，將作業流程之控制重點納入評估。
2. 各機關依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「不適用」或「其他」；其中「不適用」係指評估期間法令規定或作法已修正，但控制重點未及配合修正者；「其他」係指評估期間未發生控制重點所規範情形等，致無法評估者；遇有「部分落實」、「未落實」或「不適用」情形，於改善措施欄敘明需採行之改善措施。

國立金門大學計算機與網路中心作業程序說明表

項目編號	AI0103
項目名稱	資安事件通報與應變
承辦單位	計算機與網路中心 資訊網路組
相關單位	全校各單位
作業程序說明	一、 接受通報 (一)經由使用者以各種管道(電話、Email、書面)通報訊息。 (二)經由資安設備 Log 得知之訊息。 (三)經由教育部資安事件通告。 二、 判斷及處理 (一)接收到之訊息需判斷是否為資安事件，及其嚴重度與處理難度為何。 (二)記錄通報訊息（資訊安全事件通報單)。 (三)若處理難度低者（表示使用者可自行處理者，如用防毒軟體清毒即可者)，告知單位資安負責人，請其自行處理。 (四)若嚴重度高或是處理難度高者，依「資訊安全事件通報單」前往處理。 (五)若研判可能影響層面大者，不管是否可處理完成皆須往上通報（國家資通會報、教育部）並考量發訊息至全校。 三、 往上通報 經判斷需往上通報者，依其通報管道往上通報。 (一)所屬縣市網路中心。 (二)教育機構資安通報平台。 https://info.cert.tanet.edu.tw/ (三)國家資通安全通報應變網站。 https://www.ncert.nat.gov.tw/
控制重點	一、 事件級別為 1、2 級資安事件需於 72 小時內處理完成並結案。 二、 事件級別為 3、4 級資安事件因影響範圍擴大，因此需於 36 小時內處理完成並結案。
法令依據	一、 資通安全事件通報及應變辦法。 二、 國立金門大學資通安全事件通報及應變管理程序。
使用表單	國立金門大學資訊安全事件通報單

國立金門大學資安事件通報與應變流程圖



國立金門大學內部控制制度控制作業自行評估表

○○年度

評估單位：計算機與網路中心

作業類別(項目)：資安事件通報與應變管理作業

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期：　年　月　日

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、事件級別為 1、2 級資安事件需於 72 小時內處理完成並結案。						
二、事件級別為 3、4 級資安事件因影響範圍擴大，因此需於 36 小時內處理完成並結案。						
填表人：　　複核：						

註：

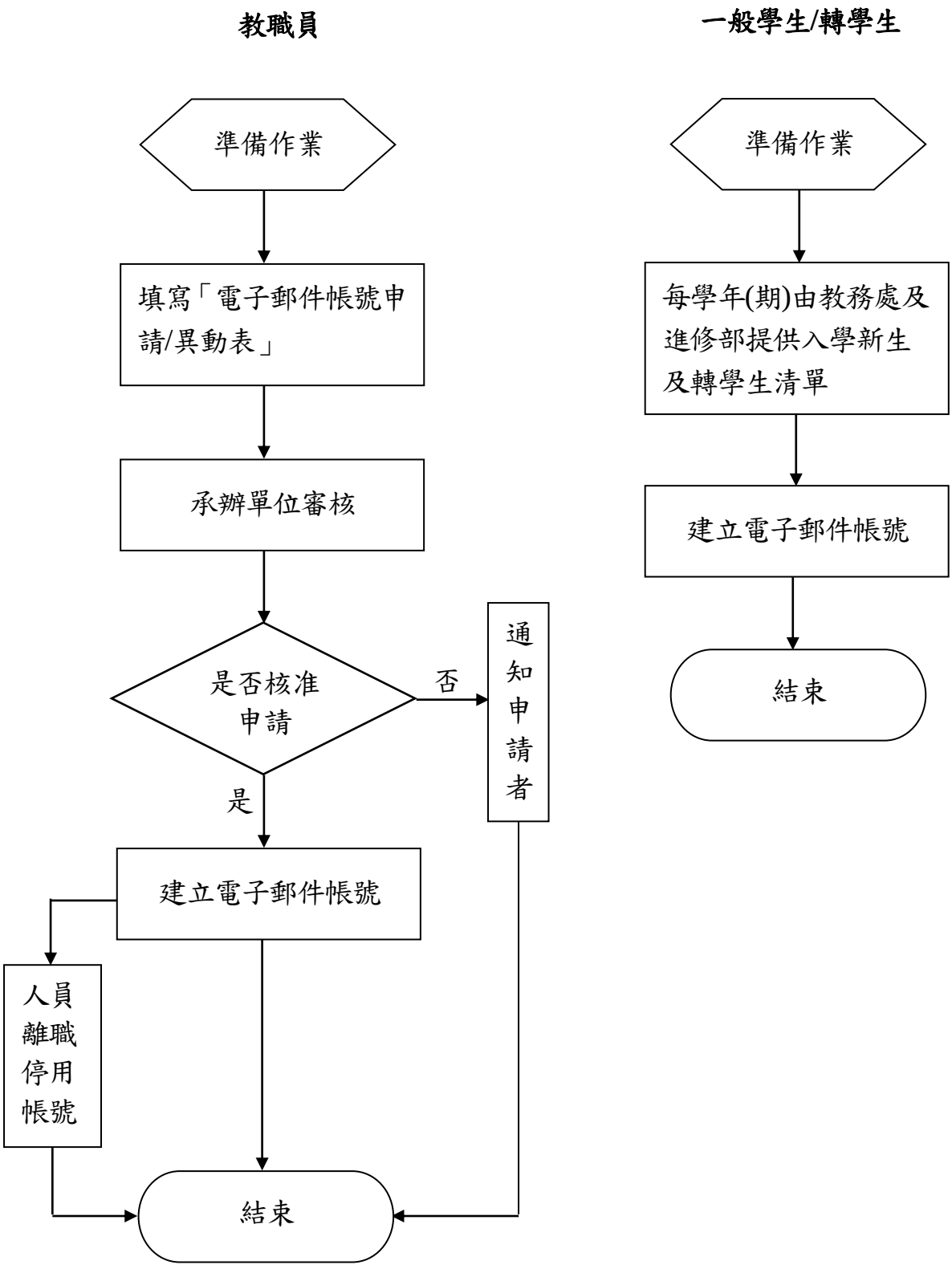
1. 機關得就1項作業流程製作1份自行評估表，亦得將各項作業流程依性質分類，同1類之作業流程合併1份自行評估表，將作業流程之控制重點納入評估。
2. 各機關依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「不適用」或「其他」；其中「不適用」係指評估期間法令規定或作法已修正，但控制重點未及配合修正者；「其他」係指評估期間未發生控制重點所規範情形等，致無法評估者；遇有「部分落實」、「未落實」或「不適用」情形，於改善措施欄敘明需採行之改善措施。

國立金門大學計算機與網路中心作業程序說明表

項目編號	AI0104
項目名稱	電子郵件帳號管理
承辦單位	計算機與網路中心
相關單位	全校各單位
作業程序說明	一、電子郵件帳號設定原則 (一) 教職員(Webmail)電子郵件帳號設定原則： [username] @nqu.edu.tw (二) 教職員(Gmail)電子郵件帳號設定原則： [username] @email.nqu.edu.tw (三) 學生(Webmail)電子郵件帳號設定原則： [username] @stu.nqu.edu.tw (103 學年度起新生入學不提供此服務) (四) 學生(Gmail)電子郵件帳號設定原則： [username] @ student.nqu.edu.tw (103 學年度起新生入學提供此服務) 二、電子郵件帳號申請 (一) 教職員工：填寫「電子郵件帳號申請/異動表」，經核准後由本中心系統管理人員設定。 (二) 一般學生/轉學生：每學年(期)由教務處及進修部提供入學新生及轉學生清單開通之。 三、電子郵件預設通行密碼於使用者第一次登入系統時，必須立即更改通行密碼。 四、停止使用權： (一) 本校官方電子郵件(Webmail)：教職員離職後保留 1 個月、兼任教師聘期終止後保留 3 個月、退休人員保留 3 年，逾保留期限者，本校得刪除該使用者帳號及所有資料。 (二) 本校 Gmail：教職員離職後保留 1 個月、兼任教師聘期終止後保留 3 個月、退休人員保留 3 年、學生畢業後轉為校友 Gmail，逾保留期限或半年未登入者，本校得刪除該使用者帳號及所有資料、退學生於退學後即停止使用權。 五、為配合本中心維持全校電子郵件之正常運作，各電子信箱之擁有人有配合本中心提出之電子郵件相關規定之義務。 六、本校之教職員生應親自開啟電子信箱，並正確使用該信箱。基於使用權責任歸屬問題，任何人都不得將個人的帳號借予他人使用。

	七、信箱擁有者應定期清理其過期郵件，以確保整個電子郵件和該信箱之正常運作和順暢。使用磁碟機容量以不超過帳號所在電子郵件系統之規定為原則。 八、個人電腦中必須安裝防毒軟體，並隨時更新病毒碼，以避免外來含毒信件。 九、使用收信軟體須取消[信件預覽]功能，且不開啟來路不明信件及附件檔案。 十、公開性之文件中如有煽動性或毀謗性文字，經查屬實，則將發生情節依校方規範給予懲處，於調查期間停止電子信箱之使用權利。 十一、 禁止以校內帳號傳遞或散播不實或不當之言論，違者依校方規範給予最嚴厲之懲罰。 十二、 本校提供之電子郵件信箱應只於公務上使用。 十三、 為防範因使用者帳號被刪除或其他不可抗拒之因素而導致資料遺失，重要資料應自行備份，本中心不負任何保管及賠償責任。
控制重點	一、是否依規定申請電子郵件帳號。 二、是否依規定停止電子郵件帳號使用權。
法令依據	一、國立金門大學電子郵件帳號管理說明書。 二、國立金門大學電子郵件帳號管理規範。
使用表單	一、國立金門大學電子郵件帳號申請/異動表。 二、國立金門大學離職人員帳號停用查核表。

國立金門大學電子郵件帳號管理作業流程圖



國立金門大學內部控制制度控制作業自行評估表

○○年度

評估單位：計算機與網路中心

作業類別(項目)：電子郵件帳號管理作業

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期：　年　月　日

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、是否依規定申請電子郵件帳號。						
二、是否依規定停止電子郵件帳號使用權。						
填表人：　　複核：						

註：

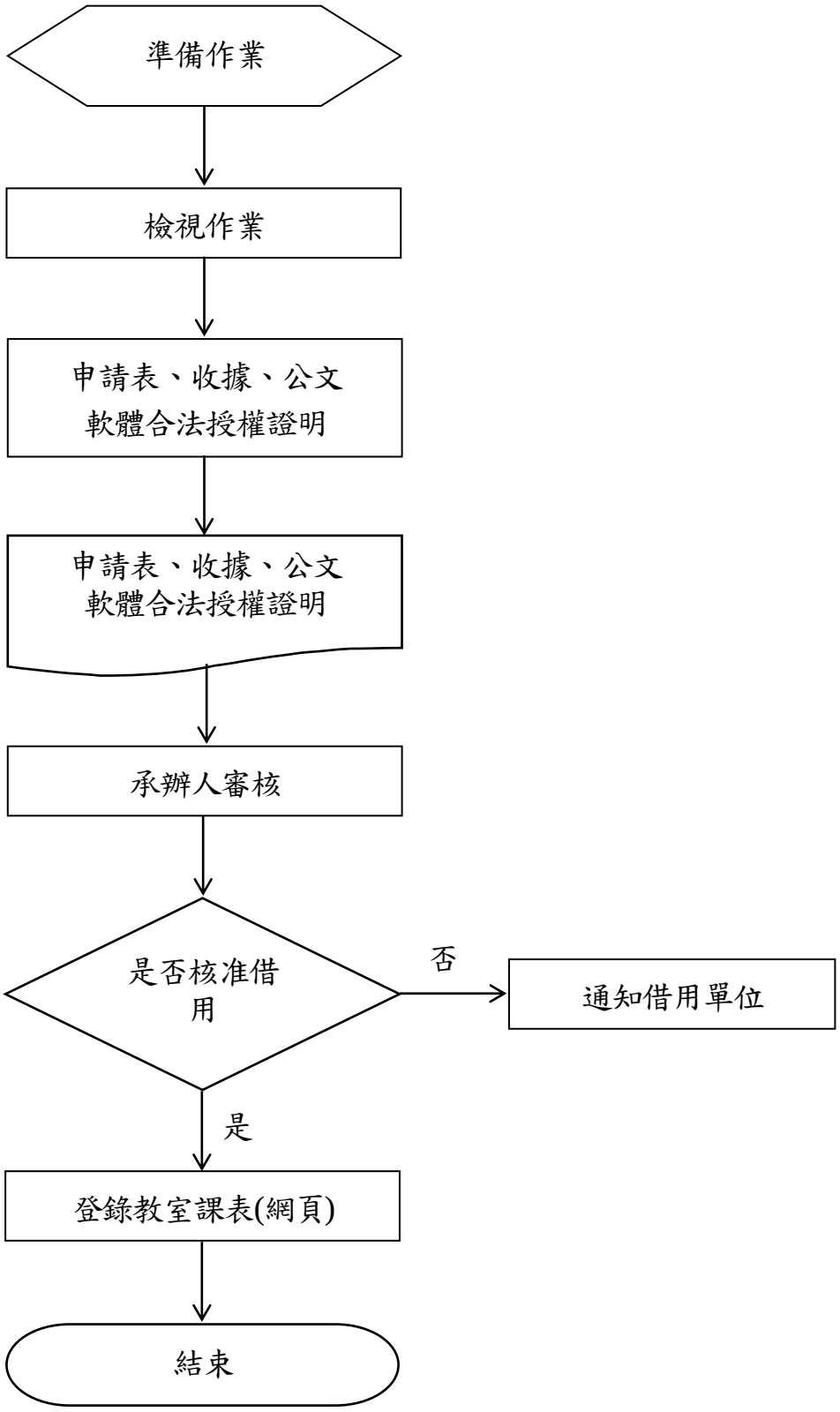
1. 機關得就1項作業流程製作1份自行評估表，亦得將各項作業流程依性質分類，同1類之作業流程合併1份自行評估表，將作業流程之控制重點納入評估。
2. 各機關依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「不適用」或「其他」；其中「不適用」係指評估期間法令規定或作法已修正，但控制重點未及配合修正者；「其他」係指評估期間未發生控制重點所規範情形等，致無法評估者；遇有「部分落實」、「未落實」或「不適用」情形，於改善措施欄敘明需採行之改善措施。

國立金門大學計算機與網路中心作業程序說明表

項目編號	AI0201
項目名稱	計算機與網路中心電腦教室管理作業
承辦單位	計算機與網路中心 軟體系統組
相關單位	全校各教學單位及行政單位
作業程序說明	一、排課及借用： (一) 計算機與網路中心(以下簡稱本中心)電腦教室依「國立金門大學計算機與網路中心電腦設備及教室借用辦法」規定以支援全校師生教學與研究使用及校外單位電腦訓練課程。 (二) 教室使用以每學期排定課程優先使用，其餘時段得依「國立金門大學計算機與網路中心電腦設備及教室借用辦法」開放臨時借用。 (三) 電腦教室借用說明： 1. 至本中心網站查詢電腦教室排程，下載「電腦教室借用申請表」，填妥資料後，於使用前三天提出並送達本中心軟體系統組辦理。 2. 依規定需付費使用時，請至本校總務處事務組及出納組繳交相關費用並領取收據，收費標準請參考本校總務處「國立金門大學場地設備借用收費標準」，憑收據使用電腦教室。 3. 本校老師或社團需不定期借用本中心電腦教室，應以書面於前一週之星期五前向本中心提出申請，本中心將安排閒置教室供教學使用。 4. 借用教室如需加裝軟體，須檢具合法授權證明。 二、設備管理： (一) 電腦教室設備包括電腦主機、印表機、網路、電力、廣播教學系統、投影機、空調及攝影監視系統等。需定期檢測功能是否正常。 (二) 電腦裝有 Phantosys 管理軟體，可設定多重系統選單與即時復原電腦資料，避免電腦教室中毒機會。 (三) 資訊設備由本中心自行維護、電力空調等由總務處維護，其餘設備故障時依廠商報價處理。 三、軟體管理： (一) 作業系統及教學軟體每年寒暑假進行重新安裝及更新版本。 (二) 須按時檢視電腦是否安裝非授權軟體，每部電腦均安裝 Phantosys 管理軟體，可設定多重系統選單與即時復原電腦資料，避免安裝非法軟體。 四、使用管理：

	(一) 學生使用電腦教室需遵守「國立金門大學計算機與網路中心電腦教室使用規則」規定。 (二) Phantosys 管理軟體，控管本中心所有軟體版本及系統更新項目。 (三) 每部電腦使用即時復原設定，避免使用者中毒機會。
控制重點	一、 電腦教室電腦是否安裝非授權軟體。 二、 電腦教室電腦等設備功能是否正常。 三、 電腦教室電腦是否有資訊安全漏洞。 四、 電腦教室電腦硬體是否有故障。
法令依據	一、 國立金門大學計算機與網路中心電腦設備及教室借用辦法。 二、 國立金門大學計算機與網路中心電腦教室管理規則。
使用表單	一、 電腦教室排課需求表。 二、 電腦教室借用申請表。

國立金門大學計算機與網路中心電腦教室管理作業流程圖



國立金門大學內部控制制度控制作業自行評估表

○○年度

評估單位：計算機與網路中心

作業類別(項目)：計算機與網路中心電腦教室管理作業

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期：　年　月　日

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、電腦教室電腦是否安裝非授權軟體。						
二、電腦教室電腦等設備功能是否正常。						
三、電腦教室電腦是否有資訊安全漏洞。						
四、電腦教室電腦硬體是否有故障。						
填表人：　　複核：						

註：

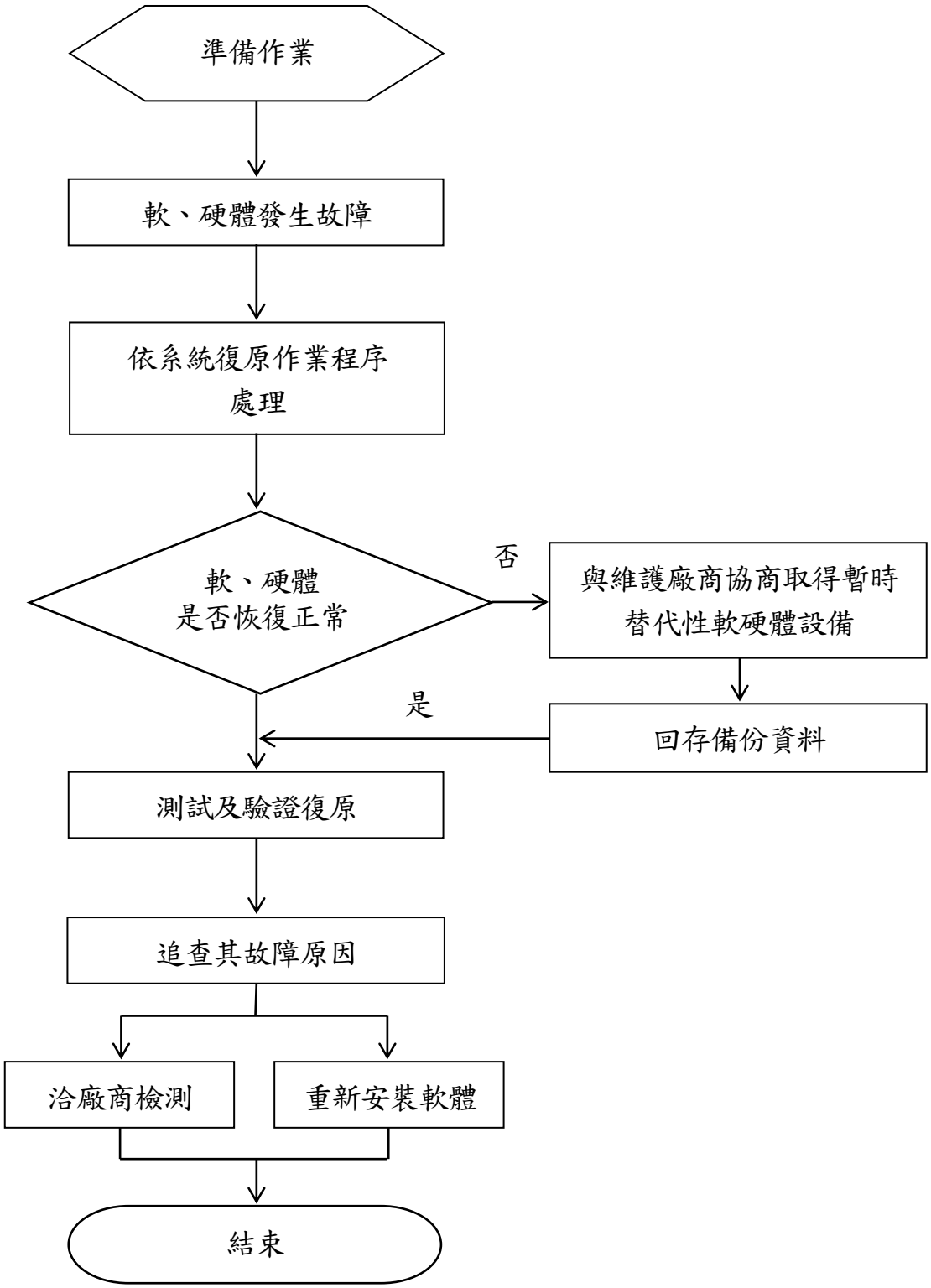
1. 機關得就1項作業流程製作1份自行評估表，亦得將各項作業流程依性質分類，同1類之作業流程合併1份自行評估表，將作業流程之控制重點納入評估。
2. 各機關依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「不適用」或「其他」；其中「不適用」係指評估期間法令規定或作法已修正，但控制重點未及配合修正者；「其他」係指評估期間未發生控制重點所規範情形等，致無法評估者；遇有「部分落實」、「未落實」或「不適用」情形，於改善措施欄敘明需採行之改善措施。

國立金門大學計算機與網路中心作業程序說明表

項目編號	AI0202
項目名稱	校務系統資料庫及伺服器主機復原計畫與測試作業
承辦單位	計算機與網路中心
相關單位	軟體系統組
作業程序說明	一、 備援措施： (一) 在主要的硬體或軟體發生故障時，或暫時性或永久性的設備損壞時，應有備援計劃以處理關鍵性工作。 (二) 資料庫每周一、二、三、四、六、日執行差異性備份；每周五執行完整備份，且保留至少近三十日備份版本。 (三) 校務資訊系統伺服器主機系統備份每週應執行完整備份，且保留近二次備份版本。 (四) 備援計劃應包括具體的備份資料及系統程式以重建現有之校務資訊系統。 (五) 應定期測試備援計劃以確定其可行並評估災難復原測試結果。 (六) 備援人員應定期接受備援訓練，以熟悉備援業務。 (七) 重要軟體及文件、清冊應抄錄備份於安全場所。 二、 故障復原： (一) 由單位內人員參加成立緊急應變小組，並加強訓練其緊急事故應變能力。 (二) 復原程序應訂明復原工作之優先順序。 (三) 硬體或軟體發生故障異常時，立即檢查維修，並保留維修紀錄。 (四) 系統經外力破壞造成無法運作或損毀時，應立即通知配合廠商進行修復。 (五) 硬體或軟體發生嚴重故障損壞無法回復正常運作時，應請原購置廠商提供應急用之支援設備暫時使用，回存本校備份資料，以利硬體或軟體設備能正常運作。 (六) 硬體或軟體發生嚴重故障損壞進行暫時性應變措施時，相關人員應立即進行硬體或軟體復原工作，如損壞程度已無法修復，相關人員應隨即採購相容性高的硬體或軟體設備，並儘速復原設備至正常運作狀態。 (七) 判定硬體或軟體故障原因。如是硬體設備發生問題，應洽廠商進行檢測維修，並於修復完成後，針對復原之硬體設備進行測試驗收；如是軟體設備發生問題，應與相關單位探討問題發生原因，並追查是否屬人為疏失，必要時應洽維護廠商或計算機與網路中心人員重

	新安裝軟體。 (八) 對備援設備應每年一次(含以上)，測試其可用性。 三、 復原結果測試： (一) 重置後之硬體或軟體，於執行測試控制作業程序後，應將暫存於其他系統之資料回存；於完成回存作業，並確認資料回存之完整性後，須將暫存資料予以銷毀。 (二) 計算機與網路中心人員應將測試結果詳述說明，併同測試資料及程式規範送交計算機與網路中心主任核示後建檔。
控制重點	一、備援措施： (一) 覆核是否制定書面之備援計劃。 (二) 備援計劃是否完整及明確。 二、故障復原： (一) 是否規劃由單位內人員參加成立緊急應變小組，並加強訓練其緊急應變能力。 (二) 是否制訂完整且可行之書面復原計劃。 (三) 是否不定期測試及演練復原計劃，以確保硬體或軟體復原計劃之適用性及支援運作能力。 (四) 當硬體或軟體發生異常時，計算機與網路中心人員是否依系統復原作業程序處理。 (五) 硬體或軟體復原後，是否追查其故障原因，研討解決之道，避免類似狀況發生。 (六) 對於人為破壞或不可抗力因素所造成之系統毀損，是否立即與廠商協商，取得暫時替代性軟、硬體供即時性資料處理之用，避免本校系統運作中斷。 三、復原結果測試： (一) 重置後之硬體或軟體，是否依測試控制作業程序執行測試。 (二) 重置後之硬體或軟體，是否已將暫存於其他系統之資料回存；於完成回存作業後，是否確認資料回存之完整性，並將暫存資料予以銷毀。 (三) 計算機與網路中心人員是否詳述說明測試結果，併同測試資料及程式規範送交中心主任核示後建檔。
法令依據	一、NQU-ISMS-4-025 營運持續運作計畫。 二、NQU-ISMS-4-027 資訊安全內部稽核計畫。
使用表單	校務系統資料庫及伺服器主機備援及緊急災害應變計劃。

國立金門大學校務系統資料庫及伺服器主機復原計畫與測試作業流程圖



國立金門大學內部控制制度控制作業自行評估表

○○年度

評估單位：計算機與網路中心

作業類別(項目)：校務系統資料庫及伺服器主機復原計畫與測試作業

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期：　年　月　日

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、備援措施： (一)覆核是否制定書面之備援計劃。 (二)備援計劃是否完整及明確。						
二、故障復原： (一)是否規劃由單位內人員參加成立緊急應變小組，並加強訓練其緊急應變能力。 (二)是否制訂完整且可行之書面復原計劃。 (三)是否不定期測試及演練復原計劃，以確保硬體或軟體復原計劃之適用性及支援運作能力。 (四)當硬體或軟體發生異常時，計算機與網路中心人員是否依系統復原作業程序處理。 (五)硬體或軟體復原後，是否追查其故障原因，研討解決之道，避免類似狀況發生。 (六)對於人為破壞或不可抗力因素所造成之系統毀損，是否立即與廠商協商，取得暫時替代性軟、硬體供即時性資料處理之用，避免本校系統運作中斷。						
三、復原結果測試： (一)重置後之硬體或軟體，是否依測試控制作業程序執行測試。 (二)重置後之硬體或軟體，是否						

已將暫存於其他系統之資料回存；於完成回存作業後，是否確認資料回存之完整性，並將暫存資料予以銷毀。 (三)計算機與網路中心人員是否詳述說明測試結果，併同測試資料及程式規範送交中心主任核示後建檔。						
填表人：　　複核：						

註：

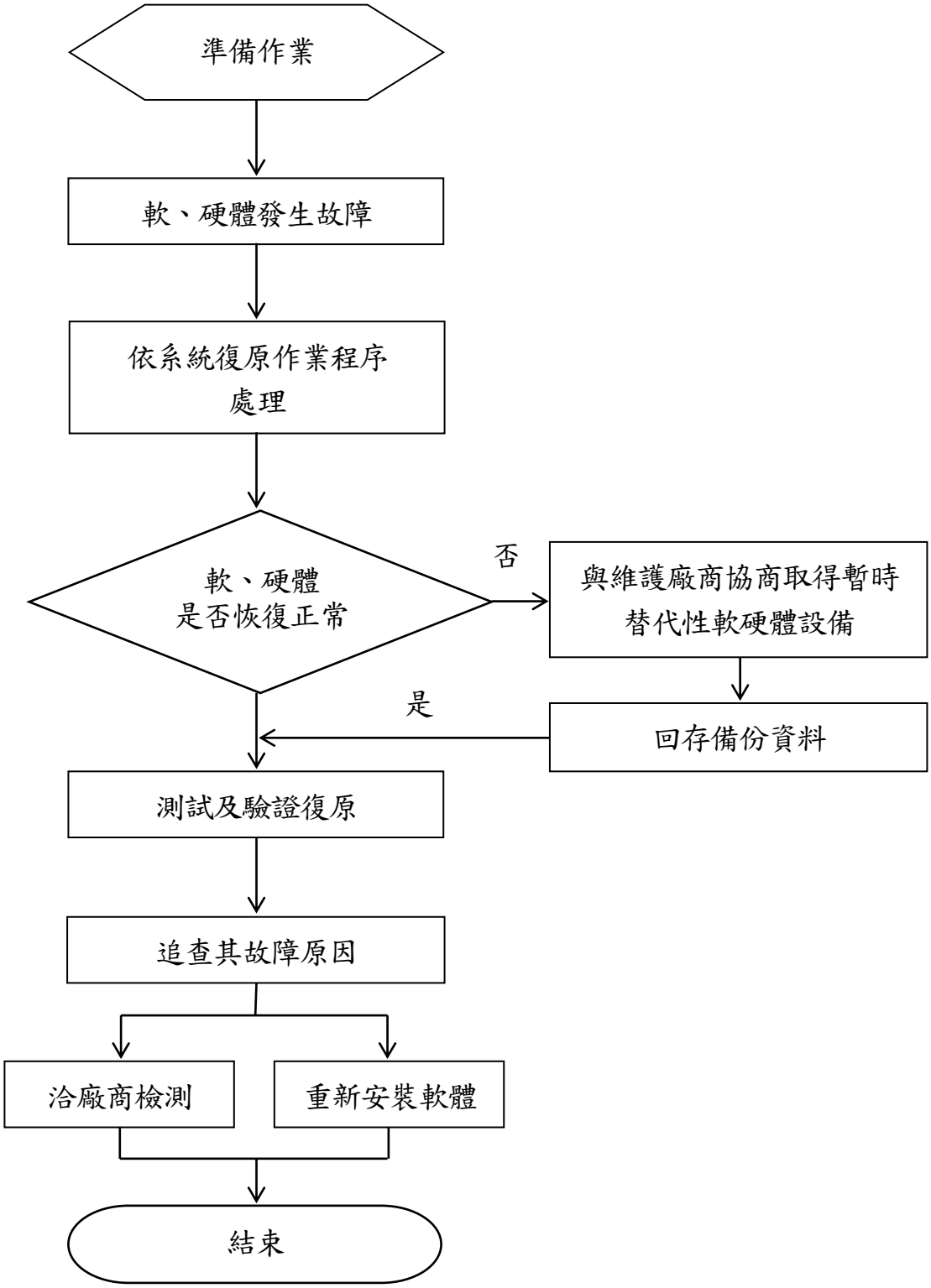
1. 機關得就1項作業流程製作1份自行評估表，亦得將各項作業流程依性質分類，同1類之作業流程合併1份自行評估表，將作業流程之控制重點納入評估。
2. 各機關依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「不適用」或「其他」；其中「不適用」係指評估期間法令規定或作法已修正，但控制重點未及配合修正者；「其他」係指評估期間未發生控制重點所規範情形等，致無法評估者；遇有「部分落實」、「未落實」或「不適用」情形，於改善措施欄敘明需採行之改善措施。

國立金門大學計算機與網路中心作業程序說明表

項目編號	AI0203
項目名稱	數位教學平台資料庫及伺服器主機復原計畫與測試作業
承辦單位	計算機與網路中心
相關單位	軟體系統組
作業程序說明	一、備援措施： (一)在主要的硬體或軟體發生故障時，或暫時性或永久性的設備損壞時，應有備援計劃以處理關鍵性工作。 (二)資料庫每日固定每小時備份。 (三)數位教學平台伺服器主機系統備份每週應執行完整備份，且保留近二次備份版本。 (四)備援計劃應包括具體的備份資料及系統程式以重建現有之校務資訊系統。 (五)應定期測試備援計劃以確定其可行並評估災難復原測試結果。 (六)備援人員應定期接受備援訓練，以熟悉備援業務。 (七)重要軟體及文件、清冊應抄錄備份於安全場所。 二、故障復原： (一)由單位內人員參加成立緊急應變小組，並加強訓練其緊急事故應變能力。 (二)復原程序應訂明復原工作之優先順序。 (三)硬體或軟體發生故障異常時，立即檢查維修，並保留維修紀錄。 (四)系統經外力破壞造成無法運作或損毀時，應立即通知配合廠商進行修復。 (五)硬體或軟體發生嚴重故障損壞無法回復正常運作時，應請原購置廠商提供應急用之支援設備暫時使用，回存本校備份資料，以利硬體或軟體設備能正常運作。 (六)硬體或軟體發生嚴重故障損壞進行暫時性應變措施時，相關人員應立即進行硬體或軟體復原工作，如損壞程度已無法修復，相關人員應隨即採購相容性高的硬體或軟體設備，並儘速復原設備至正常運作狀態。 (七)判定硬體或軟體故障原因。如是硬體設備發生問題，應洽廠商進行檢測維修，並於修復完成後，針對復原之硬體設備進行測試驗收；如是軟體設備發生問題，應與相關單位探討問題發生原因，並追查是否屬人為疏失，必要時應洽維護廠商或計算機與網路中心人員重新安裝軟體。

	(八)對備援設備應每年一次(含以上)，測試其可用性。 三、復原結果測試： (一)重置後之硬體或軟體，於執行測試控制作業程序後，應將暫存於其他系統之資料回存；於完成回存作業，並確認資料回存之完整性後，須將暫存資料予以銷毀。 (二)計算機與網路中心人員應將測試結果詳述說明，併同測試資料及程式規範送交計算機與網路中心主任核示後建檔。
控制重點	一、備援措施： (一)覆核是否制定書面之備援計劃。 (二)備援計劃是否完整及明確。 二、故障復原： (一)是否規劃由單位內人員參加成立緊急應變小組，並加強訓練其緊急應變能力。 (二)是否制訂完整且可行之書面復原計劃。 (三)是否不定期測試及演練復原計劃，以確保硬體或軟體復原計劃之適用性及支援運作能力。 (四)當硬體或軟體發生異常時，計算機與網路中心人員是否依系統復原作業程序處理。 (五)硬體或軟體復原後，是否追查其故障原因，研討解決之道，避免類似狀況發生。 (六)對於人為破壞或不可抗力因素所造成之系統毀損，是否立即與廠商協商，取得暫時替代性軟、硬體供即時性資料處理之用，避免本校系統運作中斷。 三、復原結果測試： (一)重置後之硬體或軟體，是否依測試控制作業程序執行測試。 (二)重置後之硬體或軟體，是否已將暫存於其他系統之資料回存；於完成回存作業後，是否確認資料回存之完整性，並將暫存資料予以銷毀。 (三)計算機與網路中心人員是否詳述說明測試結果，併同測試資料及程式規範送交中心主任核示後建檔。
法令依據	一、NQU-ISMS-4-025 營運持續運作計畫。 二、NQU-ISMS-4-027 資訊安全內部稽核計畫。
使用表單	數位教學平台資料庫及伺服器主機備援及緊急災害應變計劃。

國立金門大學數位教學平台資料庫及伺服器主機復原計畫與測試作業流程圖



國立金門大學內部控制制度控制作業自行評估表

○○年度

評估單位：計算機與網路中心

作業類別(項目)：數位教學平台資料庫及伺服器主機復原計畫與測試作業

評估期間：○○年○○月○○日至○○年○○月○○日

評估日期：　年　月　日

控制重點	評估情形					改善措施
	落實	部分落實	未落實	不適用	其他	
一、備援措施： (一)覆核是否制定書面之備援計劃。 (二)備援計劃是否完整及明確。						
二、故障復原： (一)是否規劃由單位內人員參加成立緊急應變小組，並加強訓練其緊急應變能力。 (二)是否制訂完整且可行之書面復原計劃。 (三)是否不定期測試及演練復原計劃，以確保硬體或軟體復原計劃之適用性及支援運作能力。 (四)當硬體或軟體發生異常時，計算機與網路中心人員是否依系統復原作業程序處理。 (五)硬體或軟體復原後，是否追查其故障原因，研討解決之道，避免類似狀況發生。 (六)對於人為破壞或不可抗力因素所造成之系統毀損，是否立即與廠商協商，取得暫時替代性軟、硬體供即時性資料處理之用，避免本校系統運作中斷。						
三、復原結果測試： (一)重置後之硬體或軟體，是否依測試控制作業程序執行測試。						

(二)重置後之硬體或軟體，是否已將暫存於其他系統之資料回存；於完成回存作業後，是否確認資料回存之完整性，並將暫存資料予以銷毀。 (三)計算機與網路中心人員是否詳述說明測試結果，併同測試資料及程式規範送交中心主任核示後建檔。						
填表人：　　複核：						

註：

1. 機關得就1項作業流程製作1份自行評估表，亦得將各項作業流程依性質分類，同1類之作業流程合併1份自行評估表，將作業流程之控制重點納入評估。
2. 各機關依評估結果於評估情形欄勾選「落實」、「部分落實」、「未落實」、「不適用」或「其他」；其中「不適用」係指評估期間法令規定或作法已修正，但控制重點未及配合修正者；「其他」係指評估期間未發生控制重點所規範情形等，致無法評估者；遇有「部分落實」、「未落實」或「不適用」情形，於改善措施欄敘明需採行之改善措施。