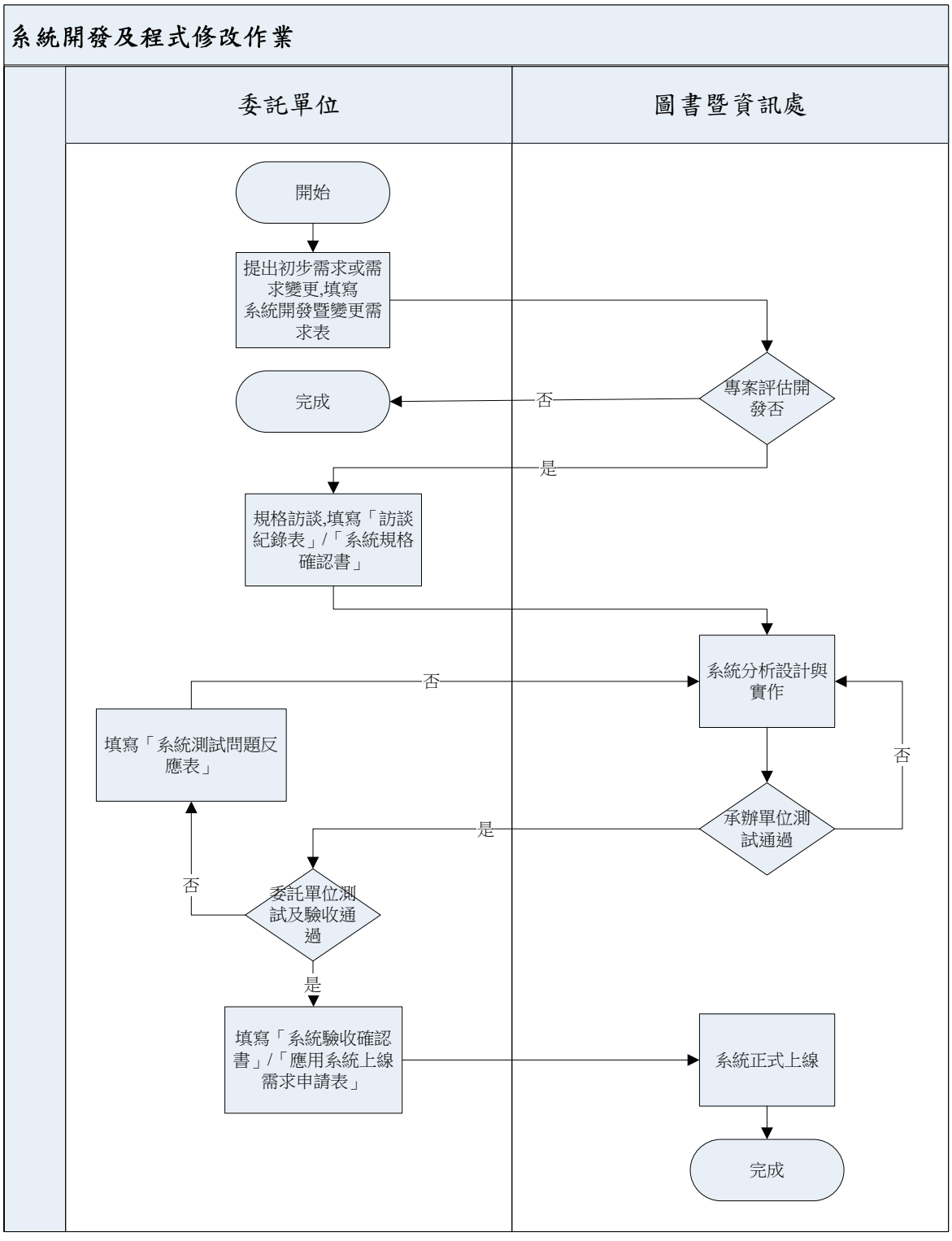
(七)資訊處理事項：

◎系統開發及程式修改作業

1. 流程圖：



2. 作業程序：

2.1. 委託單位提出「系統開發暨變更需求表」時，應一併提出所有相關工作業務手冊、業務流程、相關法令、施行細則、報表等各項詳細文件。

2.2. 本處收到委託單位提出「系統開發暨變更需求表」後，得依需求表之內容進行專案評估。若資料不齊，立即請委託單位補全。若不適開發，需詳述理由並回覆委託單位。若適合開發之專案，由本處與相關單位之承辦人員進行「需求訪談」階段。

2.3. 本處與委託單位相關人員必須進行實質訪談，並填寫「訪談記錄表」。確認相關需求後，依訪談彙集資料導出系統功能及需求關係，經委託單位於「系統規格確認書」上簽章確認後方得進行系統分析與實作。

2.4. 系統完成後，本處需先進行內部測試。若測試結果有問題則回至系統分析與實作階段。若測試結果無誤則交付委託單位測試。

2.5. 委託單位測試及驗收：系統通過本處測試後，交由委託單位於規定期限內進行測試。測試結果若需修正系統，委託單位應提交「系統測試問題反應表」予本處校務資訊組處理。測試結果若無誤，委託單位應交付「系統驗收確認書」予本處校務資訊組，完成系統驗收程序。

2.6. 系統負責人應於預定進行系統變更日前，請需求單位填妥「應用系統上線需求申請表」，並經主管簽核同意後，始得上線提供服務。

3. 控制重點：

3.1. 委託單位是否填寫系統開發暨變更需求表，並經主管簽核同意。

3.2. 開發人員是否填寫需求訪談紀錄表，並經委託單位承辦人簽核確認。

3.3. 系統規格確認書是否經委託單位和開發單位主管簽核同意。

3.4. 若委託單位測試未通過是否填寫系統測試問題反應表交校務資訊組。

3.5. 驗收後委託單位是否交付系統驗收確認書，並經主管簽核同意。

3.6. 系統正式上線前委託單位是否提交「應用系統上線需求申請表」，並經主管簽核同意。

4. 使用表單：

4.1. 系統開發暨變更需求表。

4.2. 訪談紀錄表。

4.3. 系統規格確認書。

4.4. 系統測試問題反應表。

4.5. 系統驗收確認書。

4.6. 應用系統上線需求申請表。

5. 依據及相關文件：

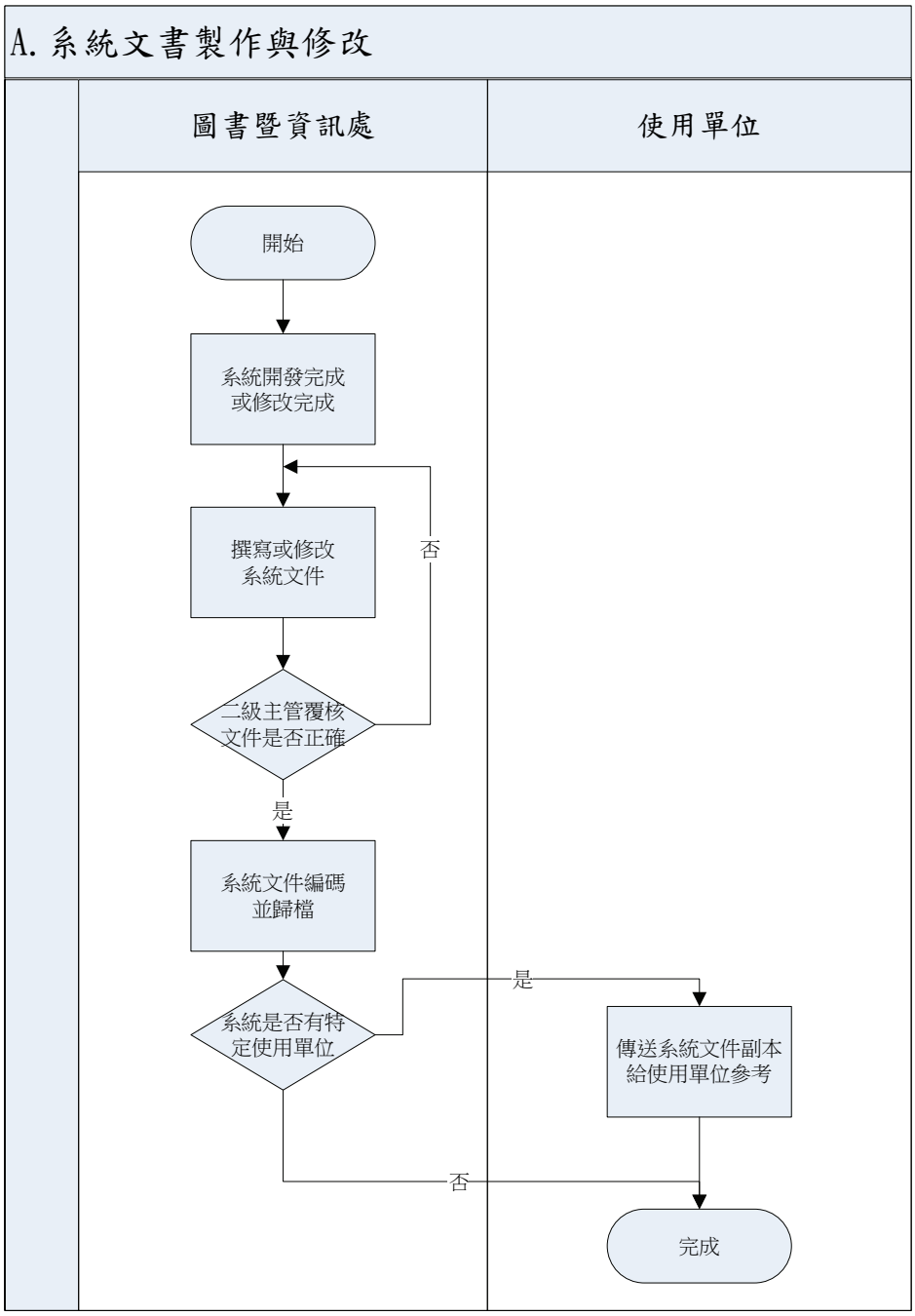
5.1. 佛光大學資訊系統開發暨變更作業要點。

5.2. 佛光大學應用系統安全管理辦法。

◎系統文書編製作業—本項作業分為二部分，依次為：A.系統文書製作與修改、B.系統文書管理。

A.系統文書製作與修改

1. 流程圖：



2. 作業程序：

2.1. 系統文件應統一規定使用相同語言及編碼。

2.2. 系統文件應經二級主管覆核。

2.3. 系統開發單位應將完成之各項資料歸檔備查。

2.4. 系統修改時，文件應隨之修改，並註明修改時間及版本編號。

2.5. 若系統為特定單位使用，應傳送系統文件副本予使用單位參考。

3. 控制重點：

3.1. 是否依規定製作系統文件。

3.2. 是否依規定覆核系統文件。

3.3. 是否依系統修改而修正系統文件。

4. 使用表單：

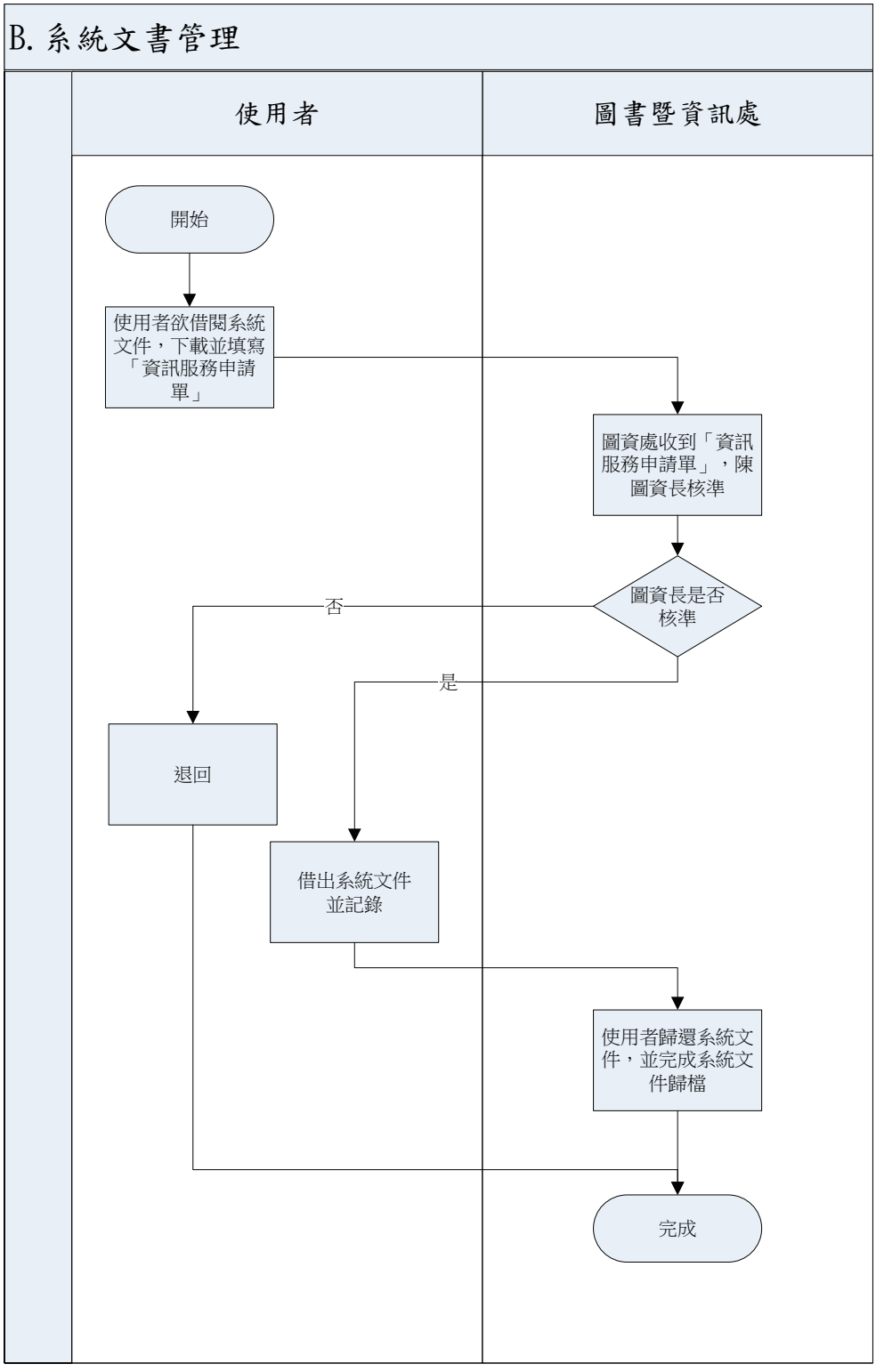
無。

5. 依據及相關文件：

5.1. FGU-IS-02-02 資訊安全文件暨紀錄管理辦法。

B. 系統文書管理

1. 流程圖：



2. 作業程序：

2.1. 系統文件應詳細分類編號統一歸檔。

2.2. 系統文件應備份存放於安全處，並由專人負責保管。

2.3. 借閱系統文件資料時，需填具「資訊服務申請單」，經圖資長核准，始得借閱。

3. 控制重點：

3.1. 系統文件是否確實由專人負責分類管理。

3.2. 各類系統文件是否定期更新管理。

3.3. 系統文件之借閱是否確實提出借閱申請，經權責主管核准。

4. 使用表單：

4.1. 佛光大學資訊服務申請單。

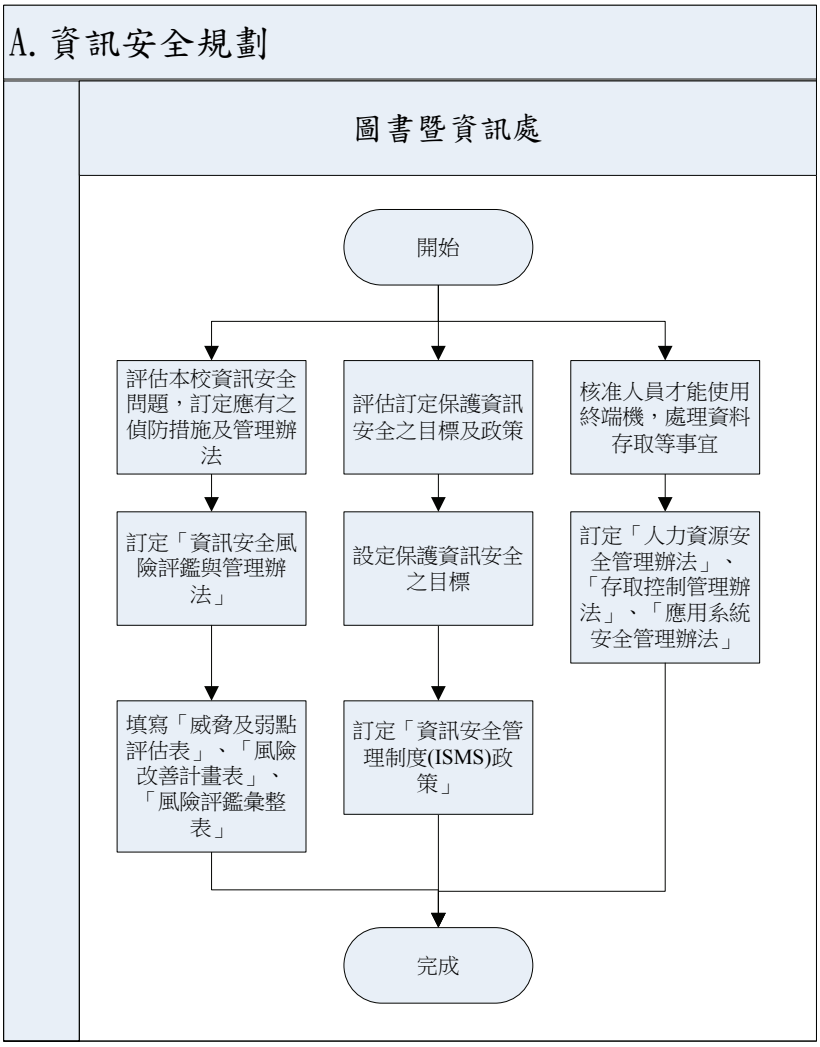
5. 依據及相關文件：

5.1. FGU-IS-02-02 資訊安全文件暨紀錄管理辦法。

◎程式及資料之存取作業—本項作業分成四部分，依次為：A.資訊安全規劃、B.使用者權限管理、C.程式及資料檔案存取、D.程式管理。

A.資訊安全規劃

1. 流程圖：



2. 作業程序：

2.1. 圖書暨資訊處應負責評估本校資訊安全問題，訂定應有之偵防措施及管理辦法。訂定「資訊安全風險評鑑與管理辦法」。填寫「威脅及弱點評估表」、「風險改善計畫表」、「風險評鑑彙整表」。

2.2. 圖書暨資訊處應評估訂定保護資訊安全之目標及政策。設定保護資訊安全之目標。訂定「資訊安全管理制度(ISMS)政策」。

2.3. 經核准人員才能使用終端機，處理資料存取等事宜。訂定「人力資源安全管理辦法」、「存取控制管理辦法」、「應用系統安全管理辦法」。

3. 控制重點：

3.1. 資訊安全規劃，是否訂定相關偵防措施及管理辦法。

4. 使用表單：

4.1. FGU-IS-04-10 威脅及弱點評估表。

4.2. FGU-IS-04-12 風險改善計畫表。

4.3. FGU-IS-04-11 風險評鑑彙整表。

5. 依據及相關文件：

5.1. 佛光大學資訊安全政策。

5.2. FGU-IS-02-05 資訊安全風險評鑑與管理辦法。

5.3. FGU-IS-02-03 資訊安全管理制度(ISMS)政策。

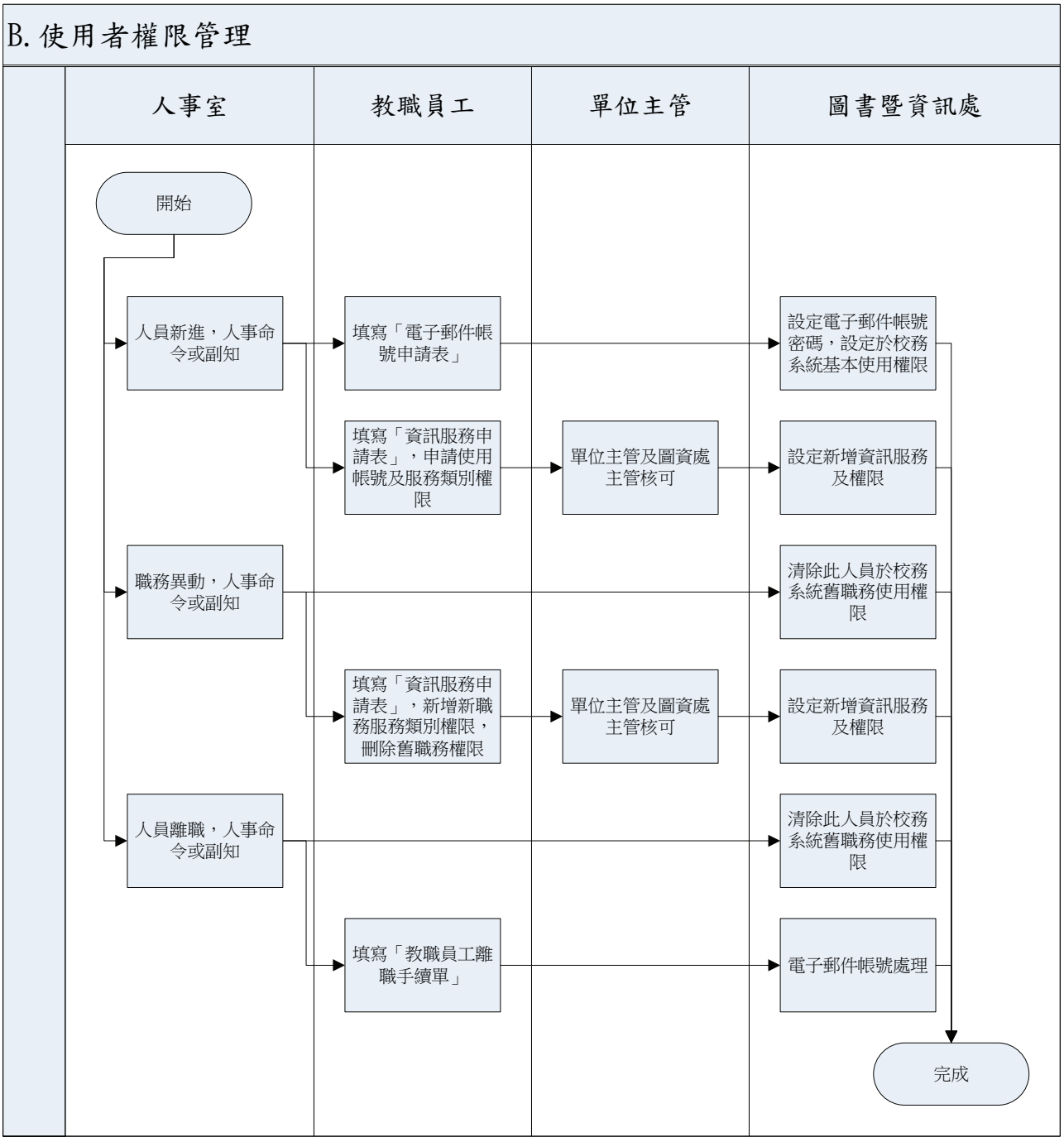
5.4. FGU-IS-02-06 人力資源安全管理辦法。

5.5. FGU-IS-02-10 存取控制管理辦法。

5.6. FGU-IS-02-11 應用系統安全管理辦法。

B.使用者權限管理：

1. 流程圖：



2. 作業程序：
   2.1. 圖書暨資訊處於各項系統資源使用授權時，以規範使用者辨識碼及使用者權限之維護程序及責任。
   2.2. 新進人員應填寫「電子郵件帳號申請表」，由人事室轉交圖書暨資訊處承辦人員設定。
   2.3. 職務異動人員人事命令副知圖書暨資訊處承辦人員後，即刪除該人員舊職務使用權限。
   2.4. 新進人員及職務異動人員應填寫「資訊服務申請表」，註明設定權限，陳權責主管核可後，始送交圖書暨資訊處資訊處承辦人員設定。
   2.5. 人員離職時之使用者權限應刪除，並填寫「教職員工離職手續單」知會圖書暨資訊處處理。

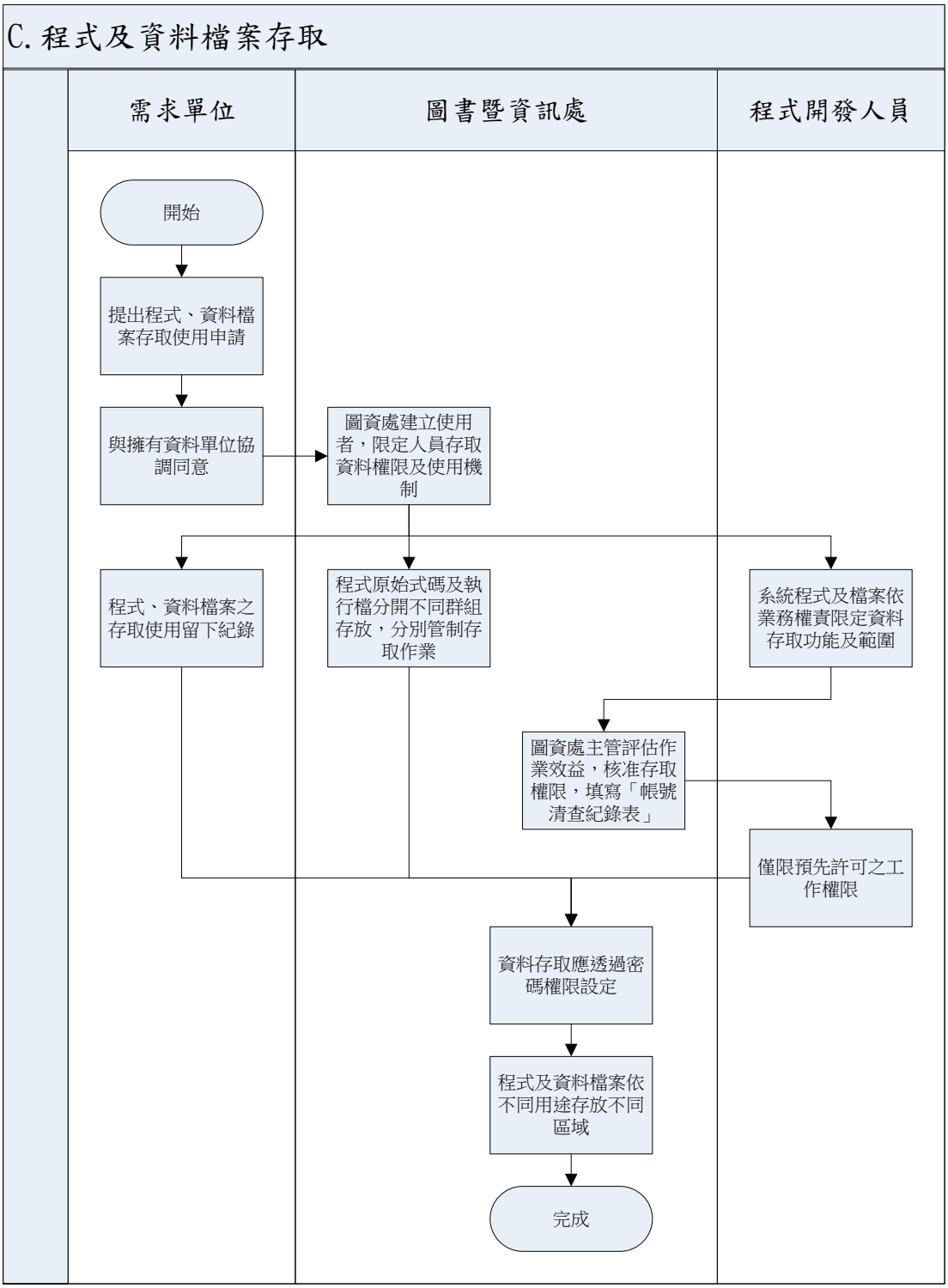
3. 控制重點：
   3.1. 是否訂定資訊安全程序。
   3.2. 使用者登錄系統辨識碼及使用權限之維護程序是否依規定辦理。
   3.3. 本校人員離職或調職時，是否於規定日期內註銷或更新使用者帳號、密碼權限。

4. 使用表單：
   4.1. 電子郵件帳號申請表。
   4.2. FGU-IS-04-17 資訊服務申請表。
   4.3. 教職員工離職手續單。

5. 依據及相關文件：
   5.1. 佛光大學電子郵件帳號申請、使用與管理辦法。

C.程式及資料檔案存取

1. 流程圖：



2. 作業程序：

2.1. 程式、資料檔案之存取使用，由需求單位提出使用申請，經需求單位主管簽核，並與擁有資料單位協調同意後，轉圖書暨資訊處辦理。

2.2. 程式、資料檔案之存取使用，均需留下紀錄。

2.3. 程式之原始式碼及執行檔應分開不同群組存放，且其存取作業亦應分別管制。

2.4. 系統程式應依業務權責限定程式設計人員之資料存取功能及範圍(如：程式之讀、寫)，並由圖書暨資訊處主管評估其作業效益及核准其存取權限，填寫「帳號清查紀錄表」。資料檔案存取，應僅限預先許可之工作權限。

2.5. 資料存取應透過密碼權限設定，以杜絕未經授權之存取發生。

2.6. 程式及資料檔案應依不同用途存放不同區域。

2.7. 資料為各使用單位所擁有，若其他單位需調取資料，經雙方單位協調同意，並設定使用者權限，限定資料之存取權限後，方能讀取資料。

3. 控制重點：

3.1. 是否確實掌握教職員工及學生使用電腦系統程式及資料檔案之存取權限。

3.2. 經授權使用之個人帳號、密碼權限表格是否特別予以列管保護。

3.3. 系統維護人員之程式、資料檔案存取權限是否明確界定並經核准；於作業時即依授權範圍存取之。

3.4. 程式、資料檔案之存取使用是否留下紀錄，是否定期核驗。

3.5. 程式原始碼及執行檔是否分開存放。

3.6. 資料存取方式是否適當，無不當之操作程序。

3.7. 系統資料調取管理，是否以使用者密碼限定資料之存取權限。

4. 使用表單：

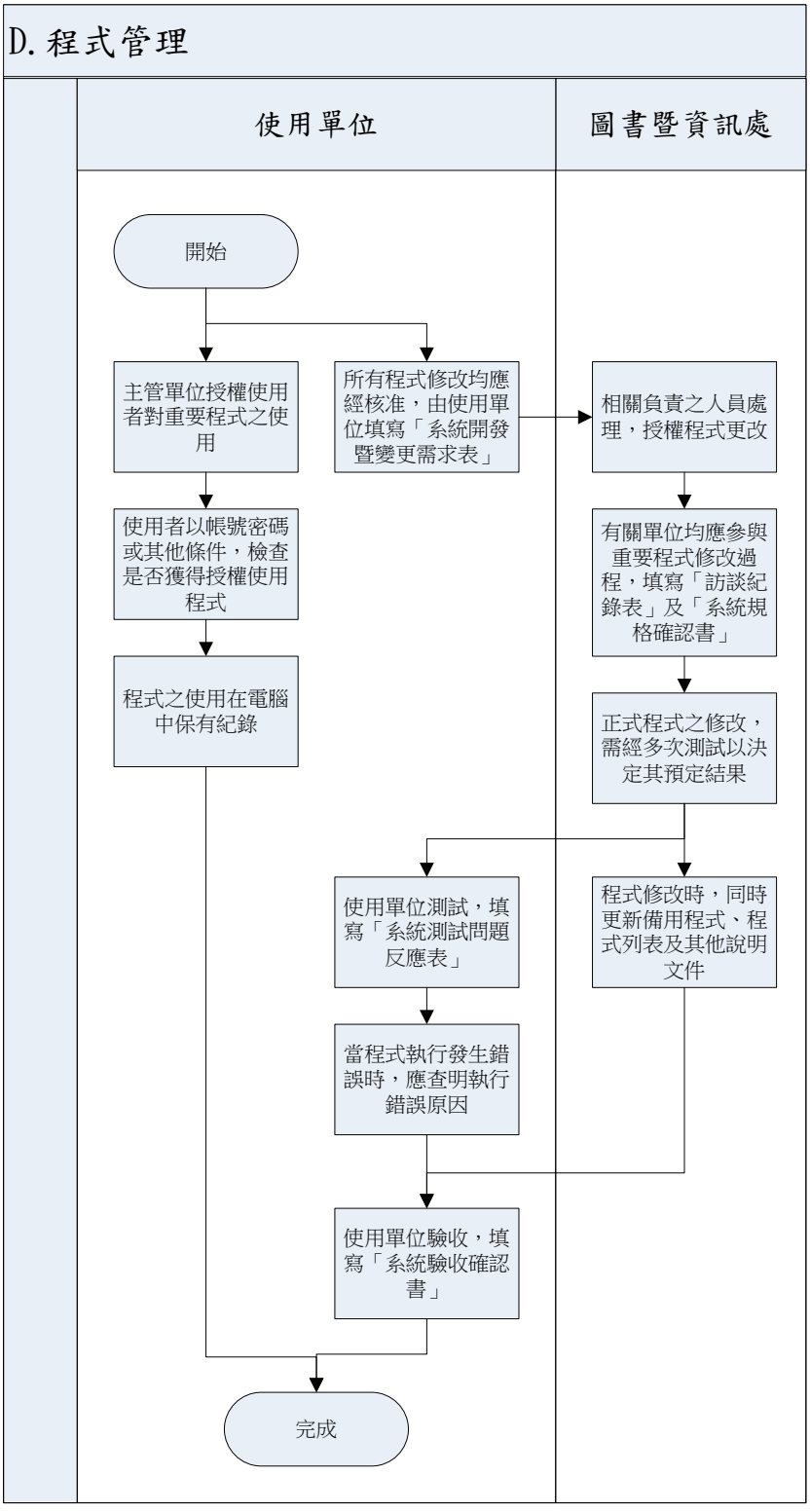
4.1. FGU-IS-04-18 帳號清查紀錄表。

5. 依據及相關文件：

5.1. FGU-IS-02-10 存取控制管理辦法。

D.程式管理

1. 流程圖：


D.程式管理
使用單位
圖書暨資訊處
開始
主管單位授權使用者對重要程式之使用
所有程式修改均應經核准，由使用單位填寫「系統開發暨變更需求表」
相關負責之人員處理，授權程式更改
使用者以帳號密碼或其他條件，檢查是否獲得授權使用程式
有關單位均應參與重要程式修改過程，填寫「訪談紀錄表」及「系統規格確認書」
程式之使用在電腦中保有紀錄
正式程式之修改，需經多次測試以決定其預定結果
使用單位測試，填寫「系統測試問題反應表」
程式修改時，同時更新備用程式、程式列表及其他說明文件
當程式執行發生錯誤時，應查明執行錯誤原因
使用單位驗收，填寫「系統驗收確認書」
完成

2. 作業程序：

2.1. 對重要程式非經授權不得使用。由主管單位授權使用者對重要成式之使用。

2.2. 程式之使用在電腦中均應保有紀錄。使用者以帳號密碼或其他條件，檢查是否獲得授權使用程式。

2.3. 所有程式修改均應經核准，由使用單位填寫「系統開發暨變更需求表」。並有相關負責之人員，以杜絕程式未經授權而遭更改之情形。

2.4. 有關單位均應參與重要程式修改過程，填寫「訪談紀錄表」及「系統規格確認書」。

2.5. 正式程式之修改，需經多次測試以決定其預定結果。使用單位測試，填寫「系統測試問題反應表」。使用單位驗收，填寫「系統驗收確認書」。

2.6. 程式修改時，備用程式、程式列表及其他說明文件亦應隨同更新。

2.7. 當程式執行發生錯誤時，應查明執行錯誤原因。

3. 控制重點：

3.1. 程式設計人員是否針對程式錯誤加以修改，相關之系統程式是否亦一併修改。

4. 使用表單：

4.1. 系統開發暨變更需求表。

4.2. 訪談紀錄表。

4.3. 系統規格確認書。

4.4. 系統測試問題反應表。

4.5. 系統驗收確認書。

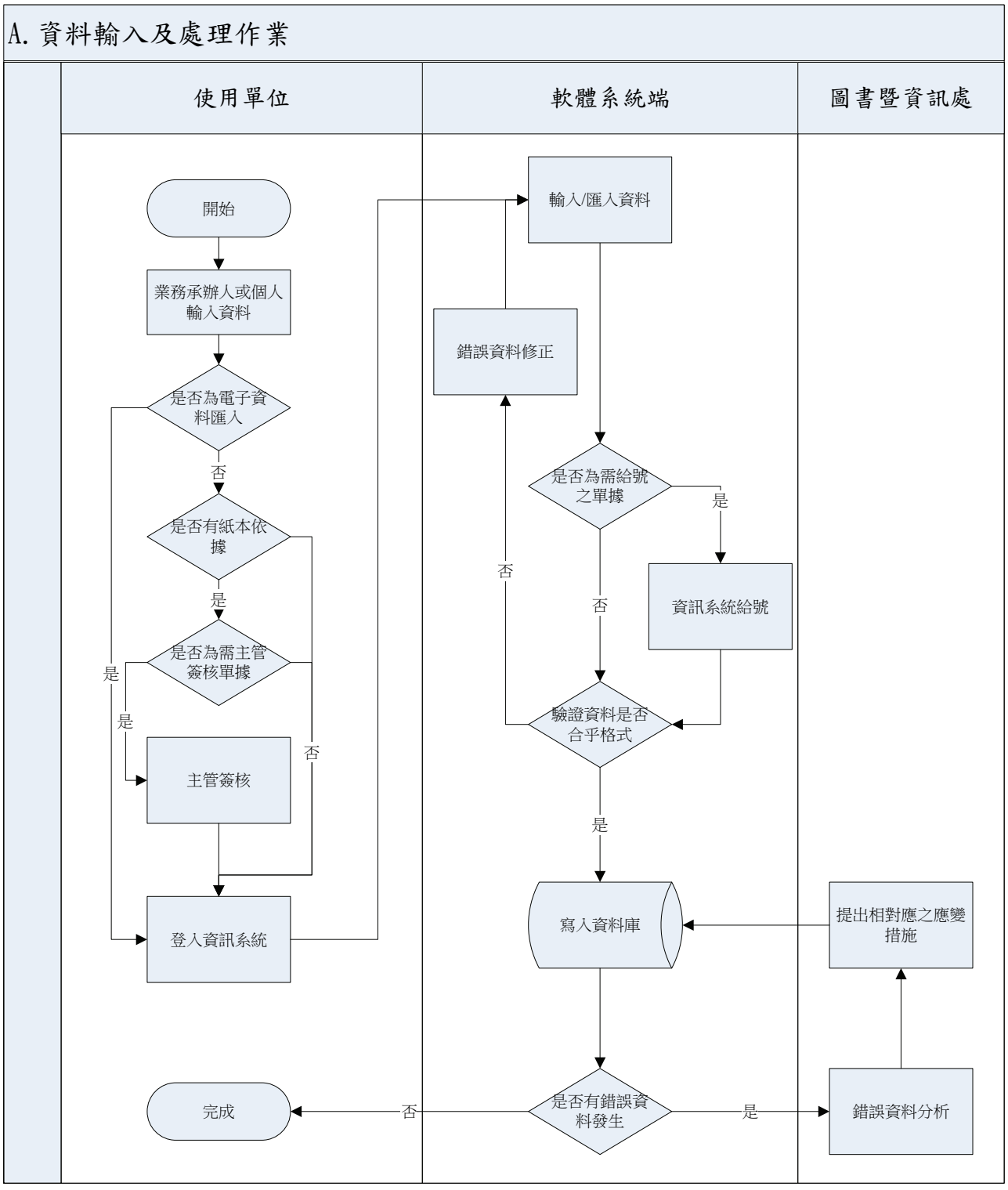
5. 依據及相關文件：

5.1. 佛光大學資訊系統開發暨變更作業要點。

◎資料輸出入及處理作業—本項作業分成二部份，依次為：A.資料輸入及處理作業、B.資料輸出及處理作業。

A.資料輸入及處理作業

1. 流程圖：



2. 作業程序：

2.1. 依據各系統之原始單據執行資料輸入處理。

2.2. 資料輸入單據或由系統產生之單據應以流水編號加以控管如遇有漏號，應即通知相關單位追蹤處理，以確保資料之完整性。

2.3. 資料允許輸入方式：

2.3.1.使用單位將資料依設計的輸入格式輸入。

2.3.2.將備份資料回存至主機。

2.4. 各單位於執行輸入作業前，應先行審核資料內容是否經權責主管簽核，始可輸入，以確保輸入資料之適法性。

2.5. 應用程式應設定自動檢核功能，如：資料屬性、數值正負號檢查、檢查號核對等。

2.6. 資料輸入處理應留下可供確認之紀錄。

2.7. 錯誤資料之更正執行應指派業務所屬單位授權之專人負責。

2.8. 應針對經常發生錯誤資料之發生原因進行追蹤分析，以期改善，並減少錯誤發生。

2.9. 當發生錯誤時，應先分析是屬於資料本身錯誤、或主檔錯誤、或程式錯誤，並追究其原因，取不同應變措施。

2.10.備份資料回存後，須統計資料之完整性及正確性。

3. 控制重點：

3.1. 各項資料之輸入是否評估其工作範圍、權責後，始授權執行輸入作業。

3.2. 對於具影響性之系統操作功能，是否設定使用者權限。

3.3. 資料輸入人員於收到原始單據時，是否審核資料內容經權責主管簽核，始可輸入。

3.4. 應用程式是否設定自動檢核功能。

3.5. 關鍵性資料輸入處理是否留下紀錄。

3.6. 當資料輸入發生錯誤時，是否立即追查原因並處理之。

3.7. 錯誤資料更正是否依既定程序分析錯誤屬性。

4. 使用表單：

無。

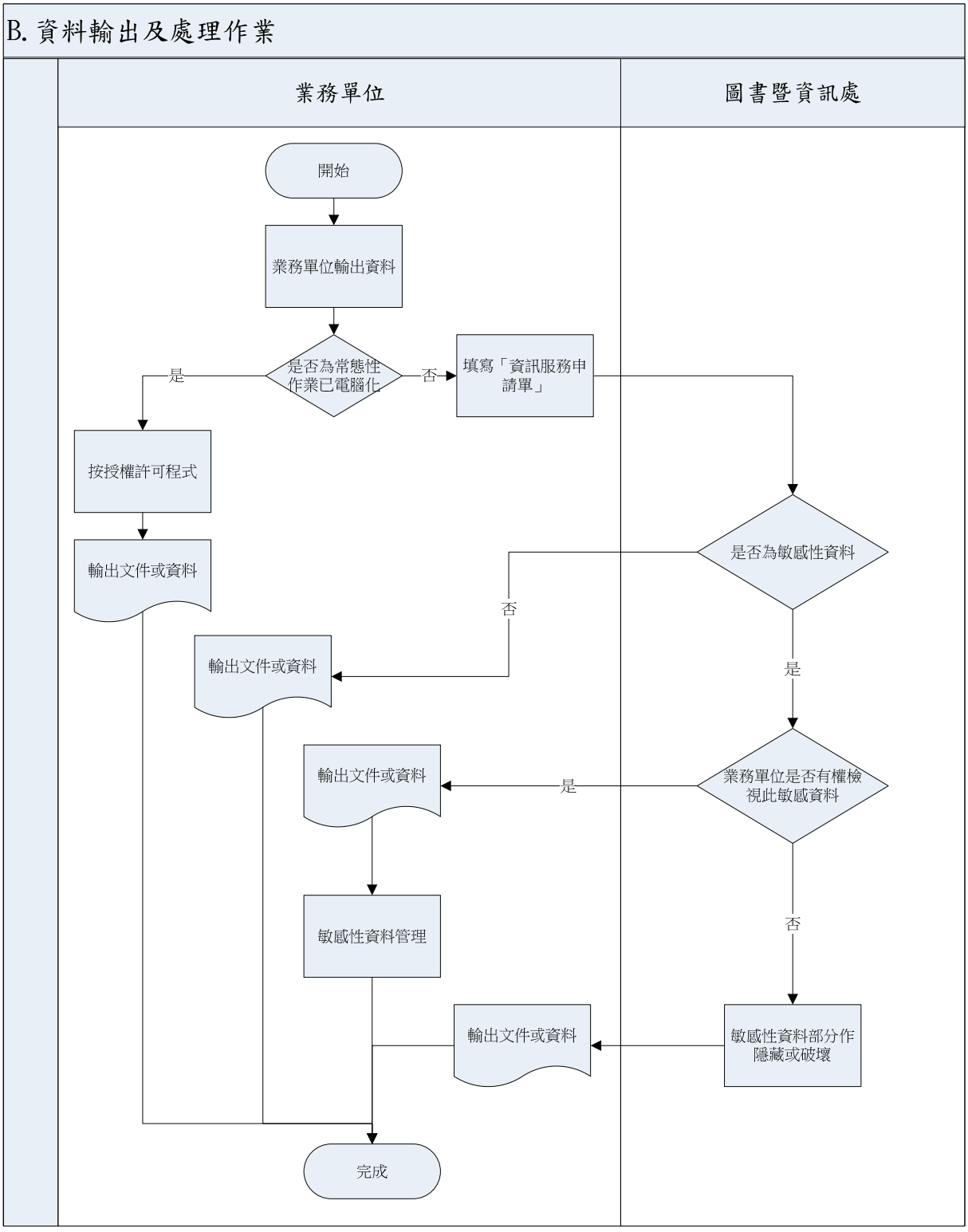
5. 依據及相關文件：

5.1. FGU-IS-02-04 資訊資產管理辦法。

5.2. FGU-IS-03-06 備份管理作業規範。

B. 資料輸出及處理作業

1. 流程圖：



2. 作業程序：

2.1. 機密性或敏感性資料之輸出，依本校資訊資產管理辦法做適當管制。

2.2. 非常態性報表輸出，業務單位需填寫「資訊服務申請單」，圖資中心相關業務人員於工作權限內始進行資料輸出作業。

2.3. 輸出資料使用後若無保存需要，應經適當銷毀處理。

2.4. 重要資料之查詢功能皆有系統權限及帳號密碼須經申請核准後，始得進行之。

2.5. 輸出資料若發現錯誤，應做必要更正，並重新執行資料處理作業。

3. 控制重點：

3.1. 資料輸出是否經過適當之核決程序處理。

3.2. 資料輸出及其輸出份數是否經適當管制。

3.3. 輸出資料保存是否妥當。

4. 使用表單：

4.1. 資訊服務申請單。

5. 依據及相關文件：

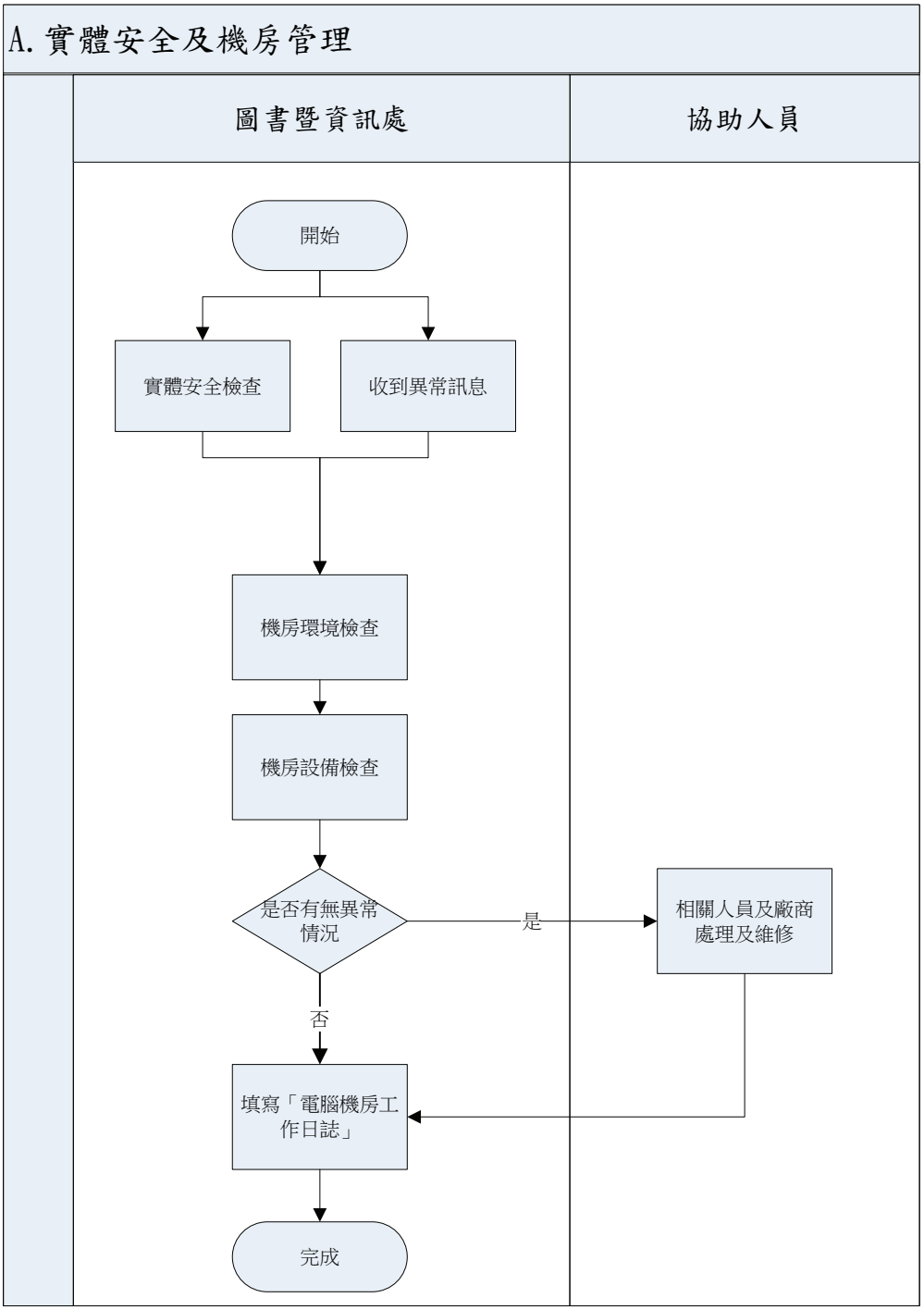
5.1. FGU-IS-02-04 資訊資產管理辦法。

5.2. FGU-IS-02-10 存取控制管理辦法。

◎檔案及設備之安全作業—本項作業分成二部份，依次為：A.實體安全及機房管理、B.備份及備援管理。

A.實體安全及機房管理

1. 流程圖：



2. 作業程序：

2.1. 應訂定「實體安全管理辦法」，以確保資訊資產及周邊環境設施之安全，避免因環境問題所引發的風險實體安全。

2.2. 應訂定「電腦機房安全管理作業規範」，並明確訂定機房環境標準，如溫度、濕度、防火設備、門禁管制等。

2.3. 重要電腦設備及通訊設備應放置於電腦機房防護，對於人員的進出，亦應以門鎖及錄影設備控管，未經授權者不得擅自進入。

2.4. 電腦機房應有不斷電系統(且有發電機支援)與環境監控設備，並定期進行維護。

2.5. 電腦機房內不應放置易燃或爆裂物等危險物品；且須設置滅火設備，並定期檢測其有效使用期間。

2.6. 圖書暨資訊處操作人員須每日檢查機房設備運作情形，並填寫「電腦機房工作日誌」。

2.7. 若電腦機房環境超過標準或設備故障，應通知相關人員進行處理及維修，並填寫「電腦機房工作日誌」。

3. 控制重點：

3.1. 是否制定「實體安全管理辦法」。

3.2. 是否制定「電腦機房安全管理作業規範」。

3.3. 實體安全是否依據「實體安全管理辦法」妥善管理。

3.4. 電腦機房是否依據「電腦機房安全管理作業規範」妥善管理。

3.5. 電腦機房是否具不斷電系統(且有發電機支援)與環境監控設備，並定期進行維護。

3.6. 電腦機房是否嚴禁擺置易燃或爆裂物等危險物品；滅火設備是否定期檢測有效使用期間。

3.7. 重要電腦及通訊設備是否特別防護；人員進出電腦機房之控管，是否亦經核准。

3.8. 每日機房設備運作情形，是否確實檢查並記錄於「電腦機房工作日誌」。

3.9. 電腦機房環境或設備發現異常時，是否於「電腦機房工作日誌」上記錄發生原因及排除方法。

4. 使用表單：

4.1. FGU-IS-04-15 電腦機房工作日誌。

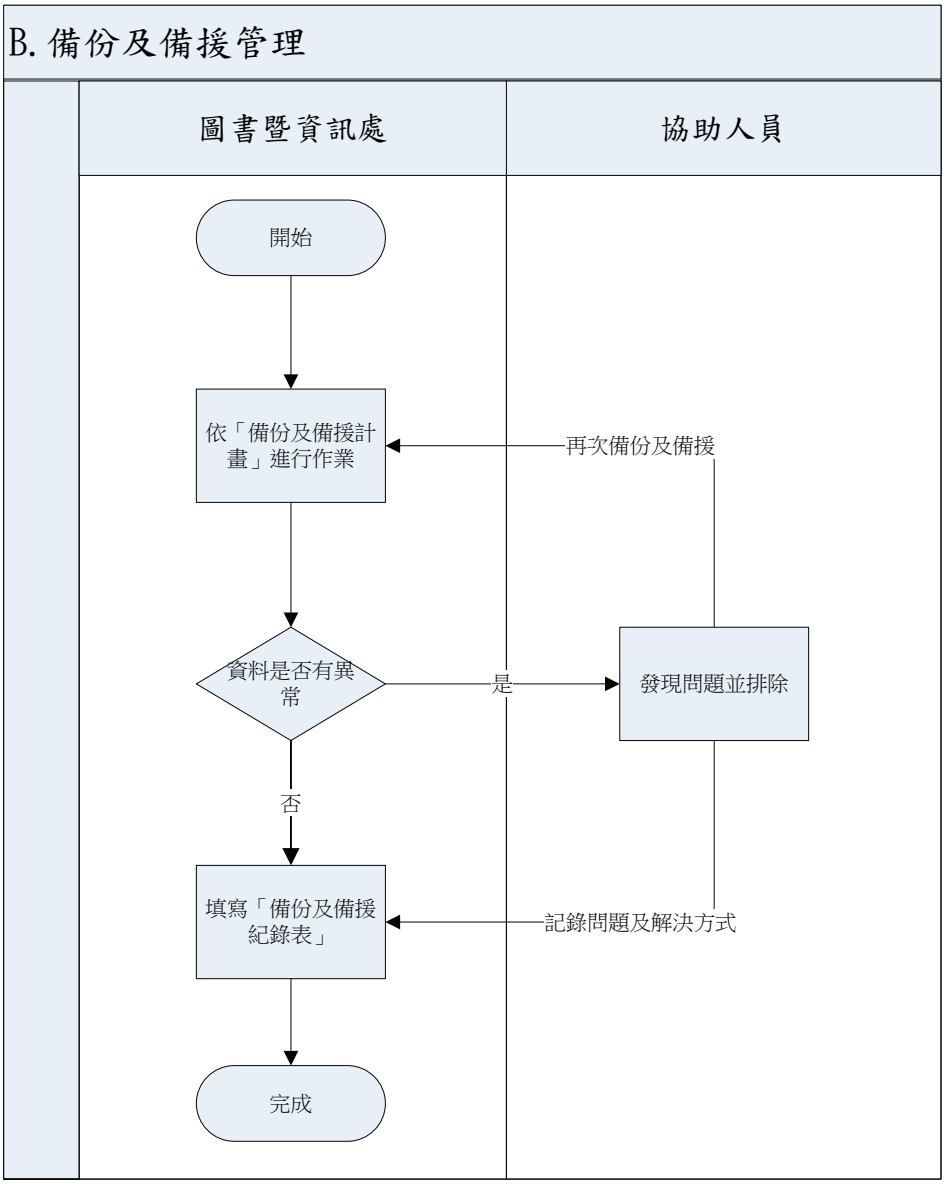
5. 依據及相關文件：

5.1. FGU-IS-02-07 實體安全管理辦法。

5.2. FGU-IS-03-01 電腦機房安全管理作業規範。

B. 備份及備援管理

1. 流程圖：



2. 作業程序：

2.1. 應根據「營運衝擊分析表」，訂定重要工作之「備份及備援計畫」，並於「備份及備援紀錄表」做紀錄，以確認備份及備援是否完整。

2.2. 備份及備援過程中發現異常，應於「備份及備援紀錄表」上記錄發生原因及排除方法，並再次依「備份及備援計畫」進行相關作業。

2.3. 備份及備援資料，應異地存放於安全且獨立之處所。

2.4. 備份及備援資料，應依「系統復原計畫及測試作業」測試其回復後之可用性。

3. 控制重點：

3.1. 是否確實記錄於「備份及備援紀錄表」。

3.2. 作業發現異常時，是否於「備份及備援紀錄表」上記錄發生原因及排除方法。異常排除後，是否再次進行備份及備援作業。

3.3. 備份及備援資料是否有異地存放安全且獨立之處所。

3.4. 備份及備援資料是否測試其回復後之可用性。

4. 使用表單：

4.1. FGU-IS-04-40 營運衝擊分析表。

4.2. 備份及備援紀錄表。

5. 依據及相關文件：

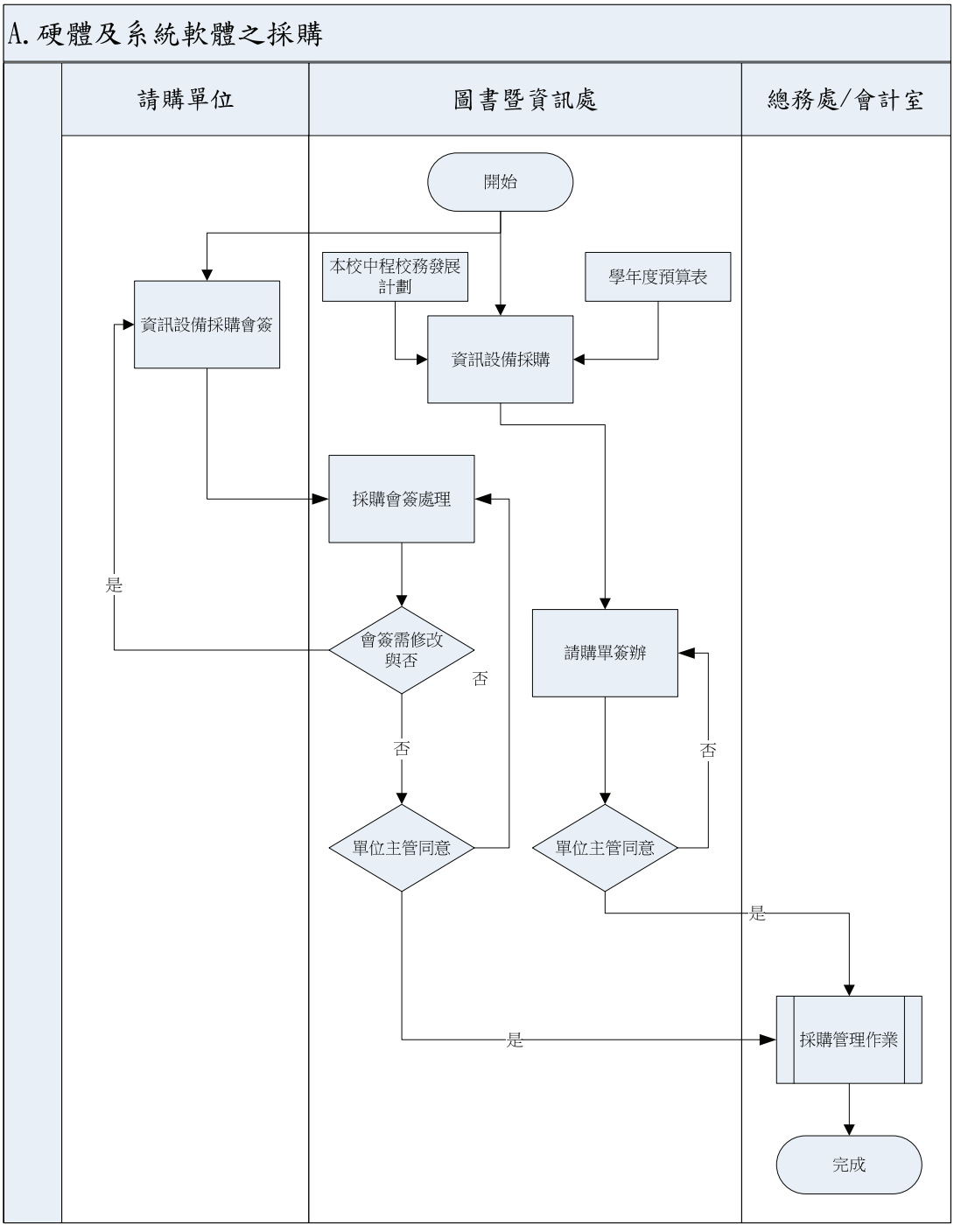
5.1. 備份及備援計畫。

5.2. 系統復原計畫及測試作業。

◎硬體及系統軟體之使用與維護作業—本項作業分成三部分，依次為：A.硬體及系統軟體之採購、B.硬體及系統軟體之維護、C.智慧財產權之管理。

A.硬體及系統軟體之採購

1. 流程圖：



2. 作業程序：

2.1. 電腦設備之採購以預先編列之學年度預算為標準。
2.2. 電腦設備採購應考慮本校整體短、中、長期策略與發展方向。
2.3. 電腦軟硬體之採購方法，應遵循本校採購作業要點流程。
2.4. 採購電腦軟硬體設備應由圖書暨資訊處及使用單位共同進行效益評估及規格調整。

3. 控制重點：

3.1. 電腦軟硬體採購是否編列學年度預算。
3.2. 電腦軟硬體採購是否考慮本校整體短、中、長期策略與發展方向。
3.3. 電腦設備採購是否依據本校採購作業要點程序辦理，並經圖書暨資訊處及使用單位共同進行效益評估及規格調整。

4. 使用表單：

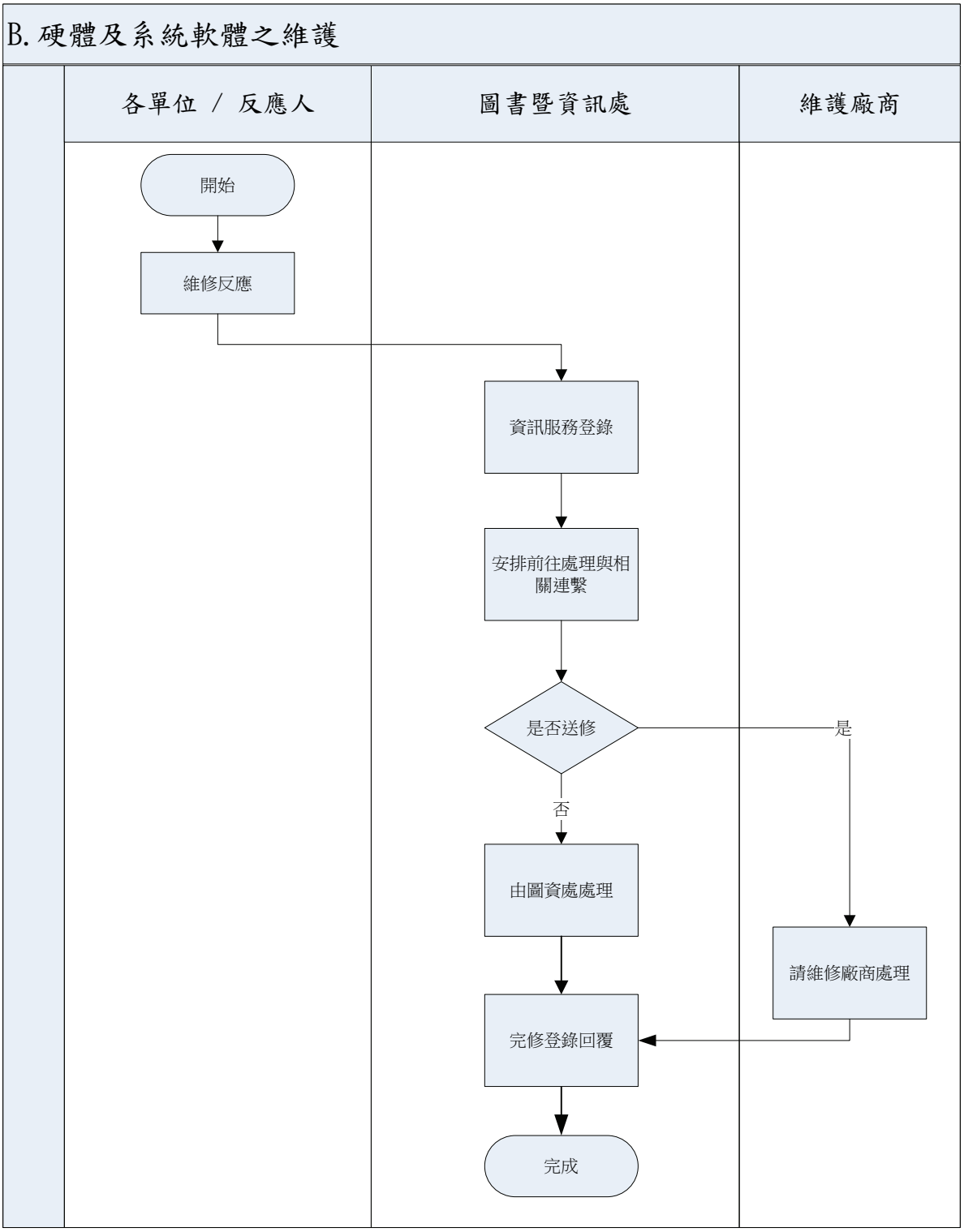
4.1. 請購單（電子表單系統）。

5. 依據及相關文件：

5.1. 學年度預算表。
5.2. 佛光大學中程校務發展計劃。
5.3. 佛光大學採購作業要點。

B. 硬體及系統軟體之維護

1. 流程圖：



2. 作業程序：

2.1. 由各單位叫修反應人向圖書暨資訊處提出「資訊服務」，圖書暨資訊處即進行登錄與安排前往處理事宜。

2.2. 若圖書暨資訊處可完修則盡速完成，並進行完修登錄與回覆反應人。

2.3. 若需送至維護廠商處理，則請維護廠商處理，完成後進行完修登錄與回覆反應人。

3. 控制重點：

3.1. 反應維護項目是否切實完成處理。

4. 使用表單：

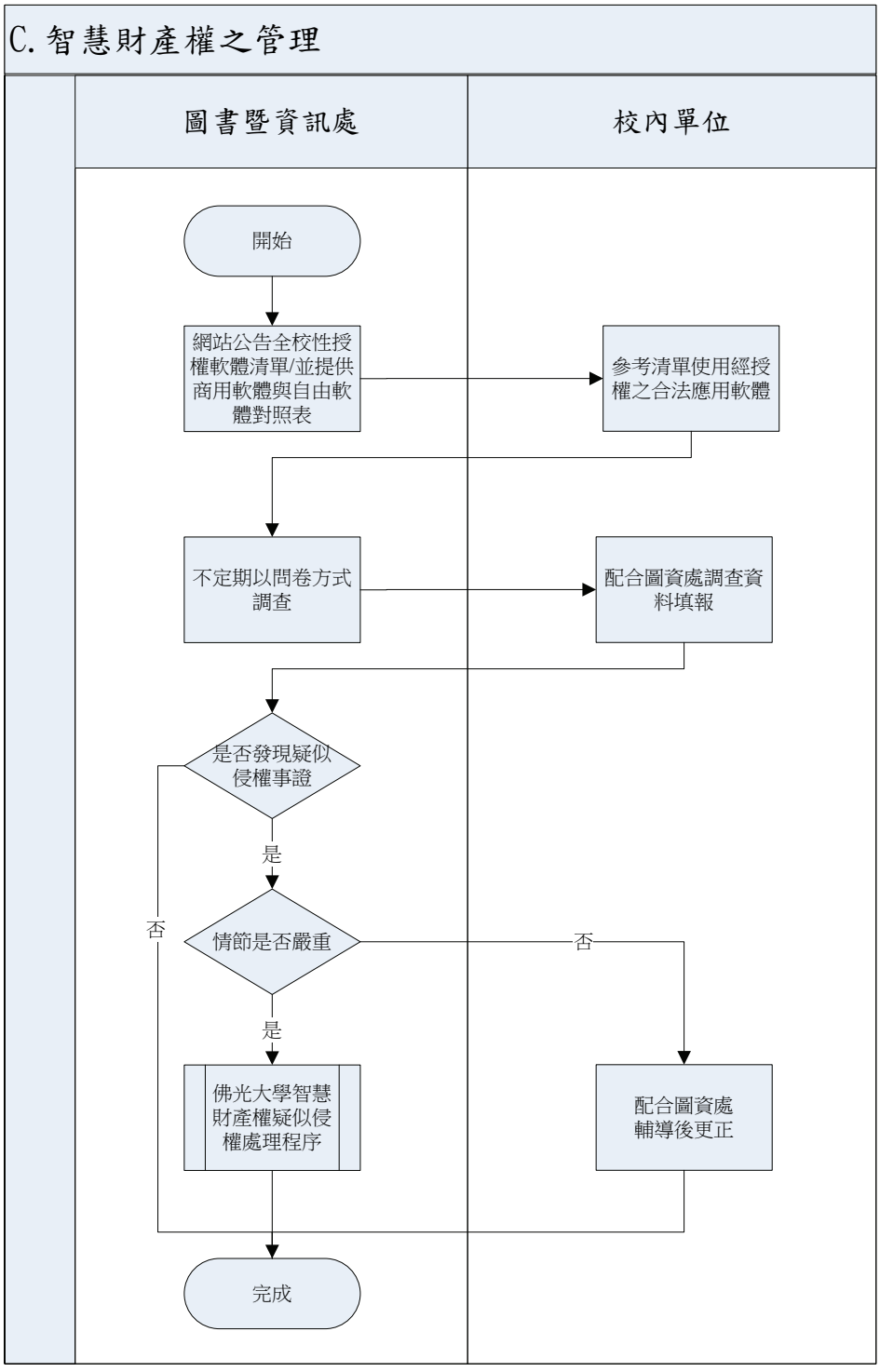
4.1. 圖書暨資訊處資訊網路服務表。

5. 依據及相關文件：

無。

C.智慧財產權之管理

1. 流程圖：



2. 作業程序：

2.1. 本校應使用經授權之合法應用軟體，各單位使用之電腦不得擅自安裝未經授權或非法之軟體。

2.2. 圖書暨資訊處應於網站公告全校性授權軟體清單予各單位參考使用，並提供自由軟體與商用軟體對照表與使用者選擇。

2.3. 圖書暨資訊處應不定期以問卷方式調查單位電腦是否有使用未經授權或非法之軟體。

2.4. 如發現疑似侵權之行為應予以輔導更正情節嚴重者得依本校「佛光大學智慧財產權疑似侵權處理程序」進行處理。

3. 控制重點：

3.1. 各單位使用電腦是否已落實不擅自安裝未經授權或非法之軟體。

3.2. 圖書暨資訊處是否檢查或調查各單位電腦之安裝與使用狀況。

4. 使用表單：

4.1. 佛光大學電腦軟體安裝使用調查表。

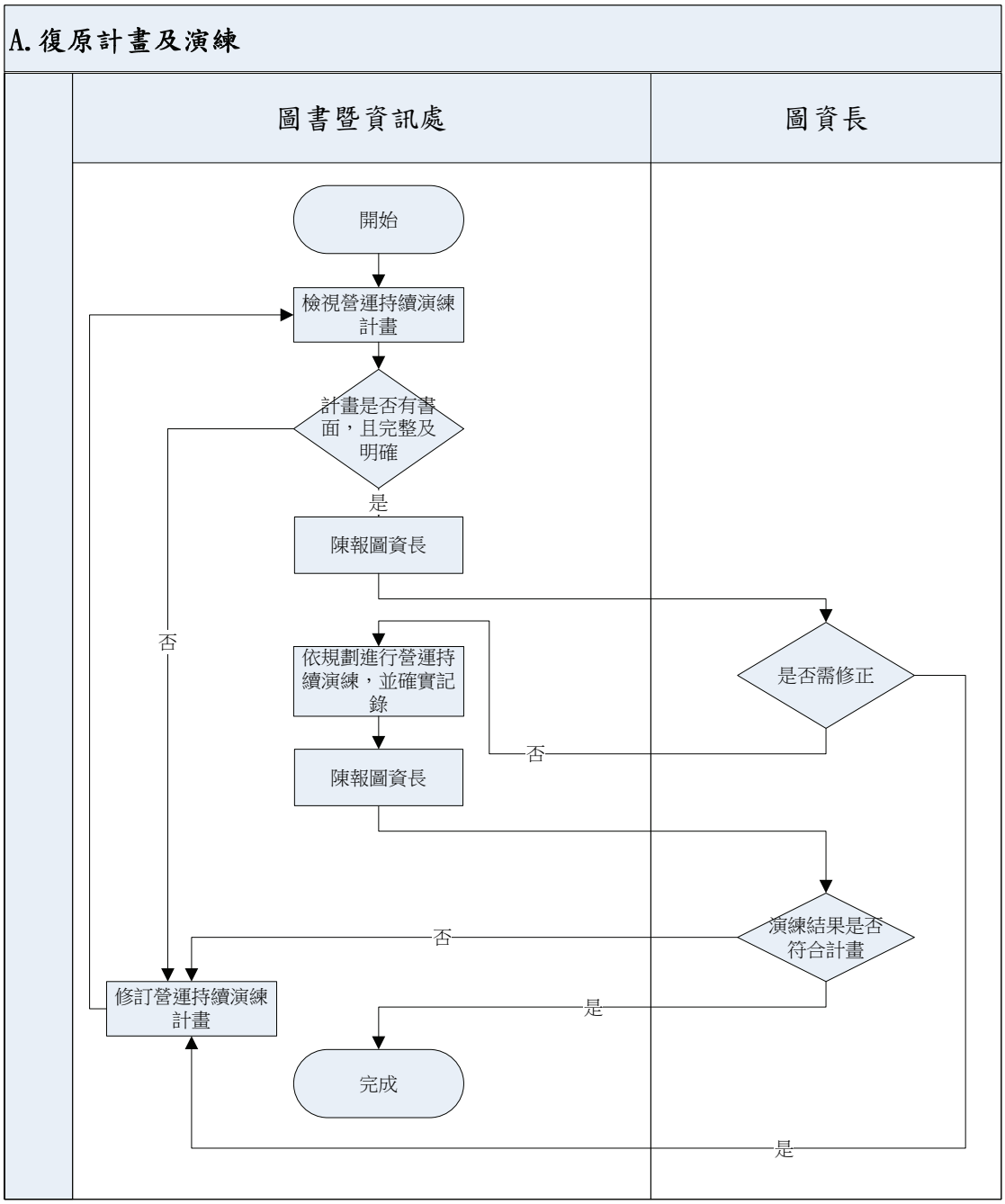
5. 依據及相關文件：

5.1. 佛光大學智慧財產權疑似侵權處理程序。

◎系統復原計畫及測試作業—本項作業分成二部份，依次為：A.復原計畫及演練、B.故障復原及測試。

A.復原計畫及演練

1. 流程圖：



2. 作業程序：
   2.1. 應成立「資訊安全緊急應變處理小組」，並加強訓練其緊急事故應變能力。
   2.2. 應訂定「營運持續演練計畫」，定期進行演練並確實紀錄營運持續處理過程，以確保備援措施之有效性與故障復原之可行性，進而評估災難復原所需之人力、設備與時間。
   2.3. 復原程序應訂明復原工作之優先順序。
   2.4. 各種故障等級，應訂有允許復原時間及報告層級。
   2.5. 對備援設備應不定期檢測，測試其可用性。

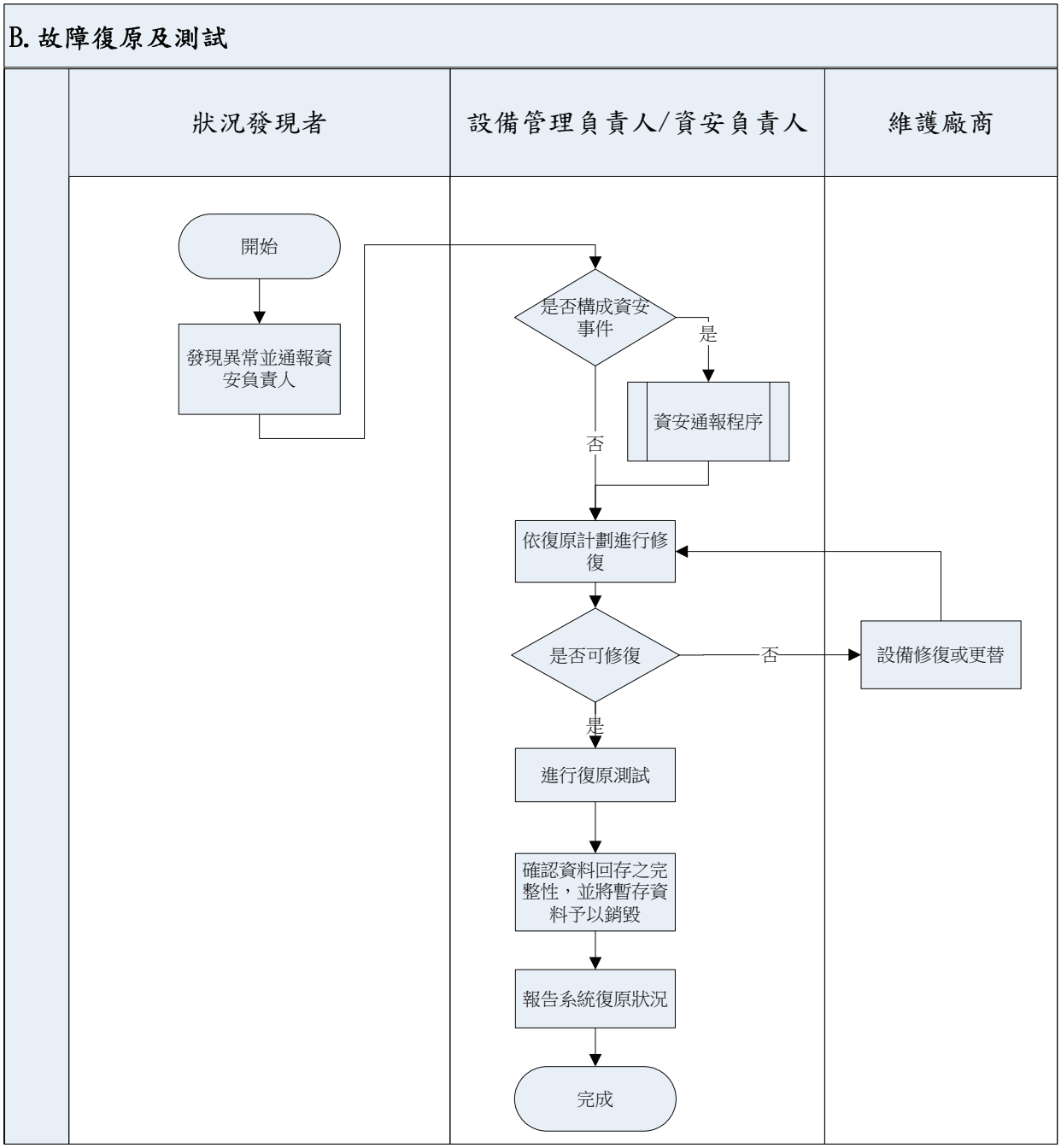
3. 控制重點：
   3.1. 是否成立「資訊安全緊急應變處理小組」，並加強訓練其緊急應變能力。
   3.2. 各種故障等級，是否訂有允許復原時間及報告層級。
   3.3. 復原程序是否訂明復原工作之優先順序。
   3.4. 是否制訂完整且可行之書面「營運持續演練計畫」。
   3.5. 是否測試或演練「營運持續演練計畫」並確實記錄，以確保計畫之適用性及支援運作能力。

4. 使用表單：
   4.1. FGU-IS-04-41 營運持續演練計畫表。
   4.2. FGU-IS-04-42 營運持續處理紀錄。

5. 依據及相關文件：
   5.1. FGU-IS-02-13 資訊業務持續營運管理辦法。
   5.2. FGU-IS-04-39 營運持續計畫。

B. 故障復原及測試

1. 流程圖：



2. 作業程序：
   2.1. 硬體或軟體發生故障異常時，使用者應立即圖書暨資訊處人員處理；維修人員經適當授權後始執行修復作業，且通知使用者處理情形與修復狀況，並保留維修紀錄。
   2.2. 系統經外力破壞造成無法運作或損毀時，應立即通知維護合約廠商進行修復；備份媒體則由圖書暨資訊處人員修復之。
   2.3. 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。
   2.4. 硬體或軟體發生嚴重故障損壞進行暫時性應變措施時，圖書暨資訊處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，圖書暨資訊處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。
   2.5. 重大事故硬體或軟體復原，應由圖書暨資訊處與電腦廠商簽訂合約。合約內容應包含修護完成交期、保固期間、違約損失賠償罰則及應變方式等條文。
   2.6. 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，必要時應洽廠商或圖書暨資訊處人員重新安裝軟體。
   2.7. 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。
   2.8. 圖書暨資訊處人員應將系統復原狀況與測試結果交圖資長核示後建檔。

3. 控制重點：
   3.1. 當硬體或軟體發生異常時，圖書暨資訊處人員是否依系統復原作業程序處理。
   3.2. 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。
   3.3. 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、硬體供及時性資料處理之用，避免本校系統運作中斷。
   3.4. 重置後之硬體或軟體，是否依測試控制作業程序執行測試。
   3.5. 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。
   3.6. 圖書暨資訊處人員是否詳述系統復原狀況與測試結果，並交圖資長核示後建檔。

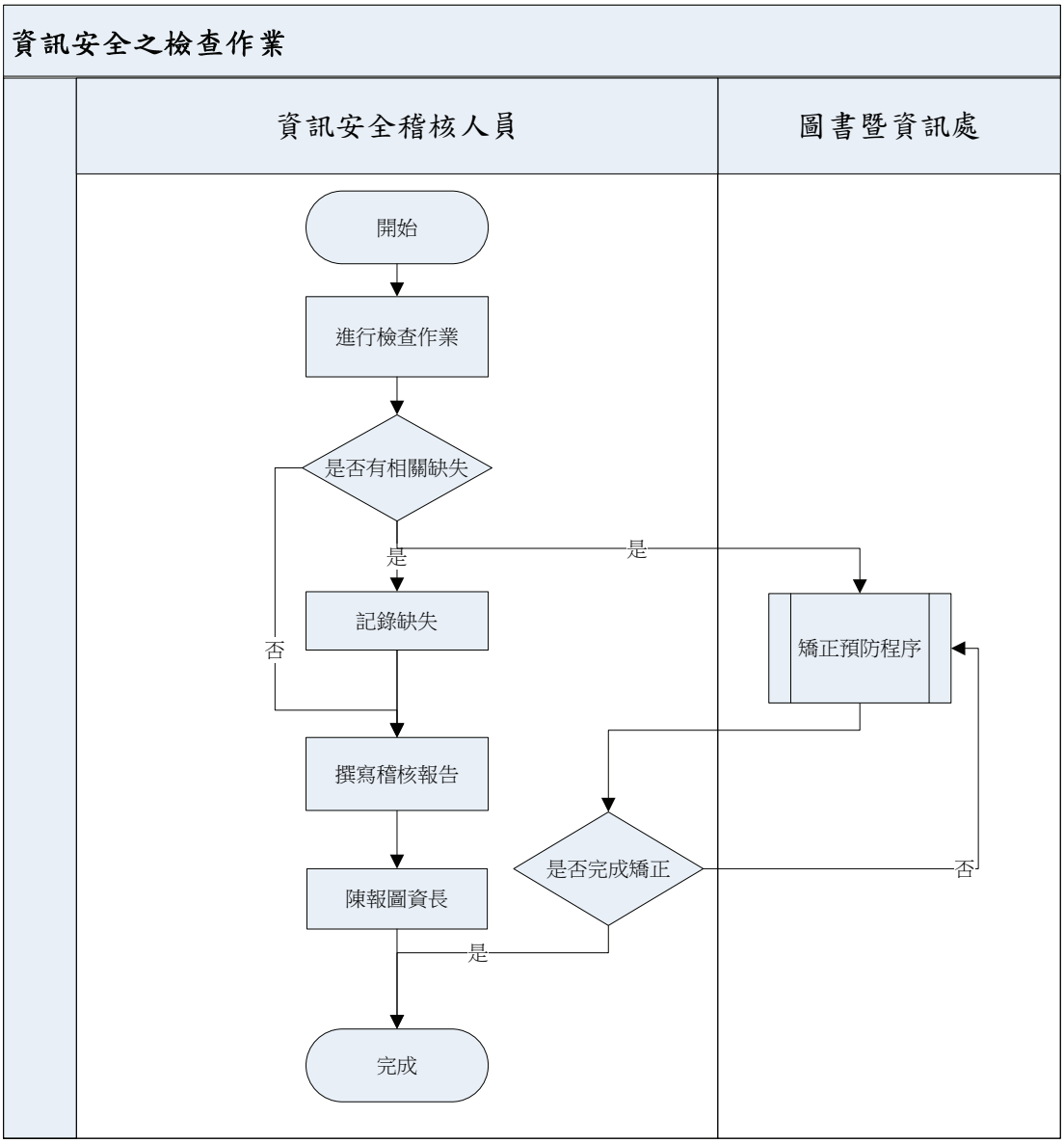
4. 使用表單：
   4.1. FGU-IS-04-41 營運持續演練計畫表。
   4.2. FGU-IS-04-42 營運持續處理紀錄。

5. 依據及相關文件：
   5.1. FGU-IS-02-13 資訊業務持續營運管理辦法。

5.2. FGU-IS-04-39 營運持續計畫。

◎資訊安全之檢查作業

1. 流程圖：



2. 作業程序：

2.1. 圖書暨資訊處應負責資訊安全規範擬訂，執行資訊管理工具之設定與操作，確保系統與資料的安全性與完整性。

2.2. 使用單位電腦及微軟作業系統之伺服器，應具備病毒掃瞄軟體，並且定期掃瞄電腦病毒與更新病毒碼。

2.3. 應建置防火牆及防毒機制，以防止駭客或電腦病毒之侵害。

2.4. 員工非經權責主管授權，禁止將本校相關資料經由電子郵件對外傳送。

2.5. 禁止教職員工及學生透過網路收發或下載與未經授權使用之軟體及其它不當軟體，以避免佔用本校網路資源及電腦病毒感染機會。

2.6. 重要軟體及機密檔案應以予密碼保護或加密處理。

2.7. 重要伺服器之帳號應定期審查。

2.8. 密碼應定期更新，並符合長度與複雜度規定，避免遭挪用或剽竊。

2.9. 使用單位電腦及網路系統資料，應定期備份重要檔案及資料。

2.10. 應定期進行弱點掃瞄，並完成嚴重弱點修復。

3. 控制重點：

3.1. 是否建立資訊安全控管機制，以確保網路傳輸資料的安全性，防止未經授權的系統存取。

3.2. 使用單位電腦及微軟作業系統之伺服器，是否具備病毒掃瞄軟體。

3.3. 是否設置建置防火牆及防毒機制，以防止駭客或電腦病毒之侵害。

3.4. 是否教育教職員工及學生正確使用合法軟體之概念。

3.5. 圖書暨資訊處人員是否定期檢視郵件伺服器上郵件收發情形，若有異常狀況是否陳報權責主管處理。

3.6. 重要軟體及機密檔案是否以予密碼保護或加密處理。

3.7. 重要伺服器之帳號是否定期審查。

3.8. 密碼是否定期更新，並符合長度與複雜度規定。

3.9. 使用單位電腦及網路系統資料，是否定期備份重要檔案及資料。

3.10. 是否定期進行弱點掃瞄，並完成嚴重弱點修復。

4. 使用表單：

4.1. FGU-IS-04-25 軟體使用管理表。

4.2. FGU-IS-04-22 員工保密暨使用合法電腦軟體切結書。

4.3. FGU-IS-04-20 弱點掃描執行申請表。

4.4. FGU-IS-04-21 弱點處理紀錄表。

4.5. FGU-IS-04-28 防火牆規則管制表。

4.6. FGU-IS-04-31 資訊安全稽核計畫。

4.7. FGU-IS-04-32 資訊安全管理制度內部稽核表。
4.8. FGU-IS-04-33 控制措施實施有效性檢查表。
4.9. FGU-IS-04-34 資訊安全內部稽核報告。
4.10. FGU-IS-04-35 資訊安全矯正與預防處理表。

5. 依據及相關文件：

5.1. 佛光大學資訊安全政策。
5.2. FGU-IS-03-07 軟體資產管理作業規範。
5.3. FGU-IS-03-03 主機與伺服器安全管理作業規範。
5.4. FGU-IS-03-04 弱點管理作業規範。
5.5. FGU-IS-03-05 防火牆建置與管理作業規範。
5.6. FGU-IS-03-06 備份管理作業規範。
5.7. FGU-IS-02-14 資訊安全稽核暨矯正預防管理辦法。