德明財經科技大學

稽核管理規定

機密等級：一般

文件編號：Takming-ISMS-B-013

版　次：V 1.2

初版日期：107.12.25

修 訂 紀 錄

版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	107.12.25	N/A	執行小組	初版
1.1	108.09.11	2，3，4	執行小組	“稽核查檢表”改”稽核檢查表”
1.1	108.09.11	4	執行小組	“矯正與預防處理單”改”觀察、建議及回覆紀錄表”
1.2	114.02.28		推動小組	“分組”改”小組”，”組長”改”召集人”，”組別”改”單位”

1. 目的

建立德明財經科技大學(以下簡稱本校)管理制度獨立稽核之規範，以判斷本校各項作業的控制目標、措施、流程及程序是否符合法規、規範、標準及組織之資訊安全要求。

2. 適用範圍

適用於本校管理系統各項作業流程之稽核作業。

3. 名詞定義

3.1. 管理系統稽核

係一種有系統且獨立的檢查，以決定各項活動及相關結果是否與所計劃的安排相符，此等安排是否有效執行及達成目標。

3.2. 稽核類別

3.2.1. 內部稽核

由各稽核小組針對作業程序之安全控制、風險評估、營運持續計劃...等，進行定期查核，以確保其成效。

3.2.2. 外部稽核

由外部單位所進行的資訊安全稽核。

3.2.3. 專案稽核

針對資訊安全事件、資訊系統的重大變更申訴案件等，特定目的的稽核。專案稽核得視稽核之特定目的需求，以不定期專案方式進行。

4. 權責

4.1. 資訊安全稽核小組召集人

4.1.1. 指派稽核員。

4.1.2. 負責督導稽核作業。

4.1.3. 稽核業務依本作業程序書確實執行。

4.1.4. 規劃稽核作業。

4.1.5. 稽核所需資源。

4.1.6. 小組準備會議。

4.1.7. 召開稽核啟始、結束會議。

4.1.8. 執行並整合稽核作業

4.1.9. 報告稽核執行情形及成果。

4.1.10. 列管「內部稽核報告」及所附相關查核資料。

4.2. 資訊安全稽核小組

4.2.1. 辦理稽核作業相關事宜。

4.2.2. 稽核缺失定期追蹤改善情形並加以記錄。

5. 要求事項

5.1. 政策、標準及要求的定期審查與範圍

5.1.1. 組織以定期執行內部稽核的方式，進行管理系統文件落實的遵循性審查。

5.1.2. 管理系統內部稽核範圍應包含核心業務與營運流程或系統，與高安全等級之資訊系統。

5.2. 法規要求之符合性

5.2.1. 整體管理系統之規劃、設計、建置及實施，均須遵循政府頒布之相關法令規章。

5.2.2. 各管理者應確保在其責任範圍內的所有安全程序是被正確地執行，並且應定期審查相關作業，以確保符合各管理系統政策及相關作業規範要求。

5.3. 內部稽核頻率

5.3.1. 每年至少執行一次內部稽核作業。

5.3.2. 視需要不定期執行專案稽核。

5.4. 內部稽核人員之要求

5.4.1. 稽核小組人員由資訊安全稽核小組召集人指派，為確保稽核過程的客觀性與獨立性，稽核作業應由非受稽核單位之稽核人員擔任。

5.4.2. 稽核人員資格須參與過相關稽核教育訓練課程者。

5.4.2.1. 資訊安全稽核人員應具有受過資訊安全稽核相關教育訓練。

5.4.2.2. 可聘請外部資訊安全顧問擔任稽核人員。

5.4.3. 內部稽核人員應定期參加資訊安全/個人資訊教育訓練，以持續加強資訊安全/個人資訊專業能力與查核技巧。

5.5. 內部稽核計劃與準備

5.5.1. 為達稽核之有效性，稽核小組召集人應事前規劃並編製「內部稽核計畫」，以作為執行稽核指導綱要，內容應包括：稽核依據、範圍、程序、人員、項目、預定時程等，陳請「資訊安全稽核小組」核准後執行。

5.5.2. 稽核小組召集人應研擬規劃「稽核檢查表」，並召開小組準備會議，提示稽核要點、協調分工及排定時程。

5.5.3. 稽核小組召集人需於查核前通知受稽核單位。

5.5.4. 受稽核單位於接獲稽核通知後，應配合準備稽核所需相關資料。

5.6. 稽核執行要求與技巧

5.6.1. 稽核執行要求事項

5.6.1.1. 稽核人員於稽核時，應依抽樣之原理收集足夠之客觀證據，以研判該稽核項目是否符合相關規範。

5.6.1.2. 稽核時應保存適當的稽核軌跡。

5.6.1.3. 稽核人員依「稽核檢查表」執行稽核，逐項填寫稽核結果；「稽核檢查表」若須增修時，需經稽核小組召集人同意，以更新「稽核檢查表」。

5.6.1.4. 受稽核單位應尊重及支持稽核員，誠實答覆稽核員所提問題，並接受調閱有關紀錄、報告及文件。

5.6.2. 稽核執行技巧

5.6.2.1. 將稽核查驗項目記錄於工作底稿。

5.6.2.2. 了解查核重點。

5.6.2.3. 記錄稽核過程中所發現之結果，並於整理後列入稽核報告。

5.6.2.4. 透過紀錄/文件資料之查核、人員訪談及現場查驗以驗證安全措施實施之有效性。

5.6.2.5. 文件/紀錄查核：確認相關文件/紀錄之關連性。

5.6.2.6. 人員訪談：確認不同階層的人員對同一事物的說法的一致性。

5.6.2.7. 現場查驗：確認員工是否遵守標準作業程序；硬體設施是否符合規定/標準。

5.6.2.8. 採用開放式問題，避免使用封閉式問題。

5.6.2.9. 銳利之觀察力：觀察受訪人員之肢體語言、面部表情、姿勢動作及談話內容。

5.6.2.10. 詳細查證：查核結論必須基於足夠有效的客觀查核證據。

5.6.2.11. 執行內部稽核所需之技術資源應於事前明確界定，並準備妥當。稽核作業應於測試區域執行，且於稽核作業完成後立即消除相關資料，如需存取軟體及資料者，應儘量以唯讀方式為之。

5.6.2.12. 執行內部稽核時，對於相關系統之存取，應予以監督並留下紀錄，以備日後查考。

5.7. 內部稽核報告

5.7.1. 內部稽核符合度判定標準如下：

5.7.1.1. 不適用：凡該查核項目不包含於現行個人資訊管理制度範圍內者。

5.7.1.2. 不符合：查核過程中該項目發現任何缺失，或稽核人員提出需改進事項者，該項目即評為不符合。

5.7.1.3. 符合：該查核項目未發現任何缺失者，該項目即評為符合。

5.7.2. 稽核人員應於內部稽核結束後，進行小組內部會議討論並彙整稽核發現後提交稽核小組召集人。

5.7.3. 稽核小組召集人應於稽核完成後，召開稽核結束會議報告稽核發現，並對稽核發現疑義進行澄清，稽核報告應請受稽單位代表簽名。

5.7.4. 稽核小組召集人並應將稽核報告彙整提報「資訊安全執行小

組」管理審查會議。

5.7.5. 受稽單位於接獲稽核報告後，應依據「矯正管理規定」之規定，於約定時間內將該單位之缺失分析原因及擬採行之矯正措施填列於「觀察、建議及回覆紀錄表」內，並經主管核定後回覆各稽核小組。

5.8. 資訊系統稽核控制措施

5.8.1. 系統稽核工具(例如入侵偵測系統(Intrusion Detection System, IDS)等)之存取應由授權的人員於授權範圍內操作，並留有存取、操作記錄，以防止任何可能的誤用或破解。

5.8.2. 系統稽核工具應存放於獨立系統及安全的地點內，防止不當操作造成其他系統之損害。

6. 參考文件

6.1. 文件暨紀錄管理規定。

6.2. 外來文件一覽表。

6.3. 內部稽核計畫。

6.4. 稽核檢查表。

6.5. 矯正管理規定。

6.6. 內部稽核報告。

6.7. 觀察、建議及回覆紀錄表。