|  |  |  |  |
| --- | --- | --- | --- |
| 系統名稱 |  | | |
| 廠商名稱 |  | 業務單位 |  |
| 業務經辦 |  | 會議日期 |  |

請系統廠商於架構會議前詳閱下列注意事項及詳填本表單，並於本表單填寫完成後再行約定「系統架構會議」時間，各項欄位不足填寫時，請自行擴增欄位，本表單內各項目須確實填寫，若無需求、不須採購或使用本行現有設備…等，請於表單欄位上註明。

1. 依據本行「IS2005-應用系統安全管理規範」，本行得於規劃、採購、建置AP應用系統前，邀集相關系統廠商、系統業務負責人等召開「系統架構會議」，其系統架構及規格、系統開發生命週期(SDLC)管理及該專案所涉及之資訊安全議題等，均須遵循本規範辦理。
2. 本「系統架構會議前置表單」為「系統架構會議」使用表單；系統廠商應確實填寫本「系統架構會議前置表單」內之各項資訊，填寫前請先參考本表單附件一~三、(C01) AP應用系統開發配合事項、(D01)資料庫系統開發配合事項 等說明，若有填寫上問題可先洽詢。
3. 雙方於架構會議上，若對於系統架構、軟/硬體規格有疑慮時，雙方得當場協商並確認其系統架構、軟/硬體規格，若無法當場協商並確認其系統架構、軟/硬體規格、本表單內各項資訊填寫不完整、系統架構及規格未經雙方確認、經雙方確認後但又再變更系統架構或規格者、於架構會議確認系統架構及規格後半年才啟動專案者，本行得再次召開「系統架構會議」討論。
4. 廠商如有使用其他Java軟體，應確認軟體授權與使用限制等問題；若有使用Open Source軟體，請於表單內詳細說明。
5. 經「系統架構會議」確認系統架構、規格及本表單內各項資訊後，廠商得依雙方決議事項執行，若於系統安裝設定或上線階段，歸因廠商未於「系統架構會議」上或「系統架構會議前置表單」內未充分揭露各項資訊或本案使用軟(硬)體採購、授權數量不足額，而造成單一或部分軟體與設備缺漏而造成該系統無法正常運行、系統效能不足等相關問題，廠商得負補足軟(硬)體採購、授權數量責任；廠商報價單內之各項資訊內容，得經廠商或原廠技術部門審核。
6. 資料庫主機不得安裝其他應用程式、不開放網路芳鄰、分享資料夾及使用者直接連線；內部Server禁止直接連線Internet；DMZ區主機對內部主機僅限開放80、443、20、21、SMTP等Port。
7. 作業系統、資料庫、AP應用系統等系統軟體，本行均建議使用64位元版本，若非使用64位元版本須說明原因；資料庫字元集建議使用unicode，若非使用unicode請先說明。
8. 禁止使用Administrator、root、oracle等高權限帳號安裝AP應用系統軟體，避免造成日後因帳號納管及密碼變更造成應用系統異常，如有特殊需求請先提出討論。
9. 本專案使用之軟、硬體廠商應保證至少有7年使用及維護年限，並說明如無法達到使用及維護年限的處理方式及補償機制。
10. 除資料庫管理員，禁止使用者透過連線軟體或工具直接連線資料庫系統，如有特殊需求請先提出討論。
11. 依金融機構資通安全防護基準要求，應符合下列要求  
    第九條  
    核心資通系統、第一類電腦系統之營運環境容量管理應符合下列要求：

一、 應依據資源使用狀況及容量需求，亦須考量軟體更新、生命週期、軟硬體運作相容性等因素，評估採用多重備援或冗餘配置(Redundancies)等方式，適時進行資源調整及擴充。

二、 應定期評估核心資通系統是否有單點故障風險(Single Point of Failure)，並導入高可用性或高可靠度的措施（如Active Active、Active Standby或Disaster Recovery），避免因單點故障造成整體異常之情形。

三、 應依業務性質及設備功能等對核心資通系統訂定相關負載量要求，以強化系統穩定性，確保業務持續運作不中斷。

四、 應針對核心資通系統特性、風險因素及所需效能，設定監控項目(如效能，容量空間，負載量、頻寬等)、規則(如警示種類)、程序或規範。

五、 應定期將監控結果適時通知相關權責單位，於完成相關處理及應變後，留存紀錄由權責單位核示。

第十四條

系統生命週期管理應符合下列要求：

一、 應訂定資訊系統開發設計規範並落實執行。

二、 應監督委外開發之應用軟體，並確保其有效遵循本基準規定。

三、 應確保系統軟體和應用軟體安裝最適安全修補程式。

四、 應針對系統架構重大變更或異動時，訂定復原程序，並於上線前進行程序演練或實際演練。

五、 應分別從技術、功能、情境等建立測試案例並進行端點對端點測試。

六、 對於測試用之機敏資料，應先進行資料遮蔽處理或管制保護。

七、 於開發階段起至營運階段，應遵循變更控制程序處理並留存相關紀錄；營運環境變更（如執行、覆核）應由二人以上進行，以相互牽制。

八、 系統軟硬體變更應先進行技術審查並測試；套裝軟體不應自行異動，並應先進行風險評估。程式不應由開發人員自行換版或產製比對報表，應建立程式原始碼管理機制，以符合職務分工及牽制原則。

第十六條  
供應商管理應符合下列要求：  
一、 核心資通系統及各類電腦系統應具備以下管理機制:

(一) 應先對受託廠商進行適當之安全評估，並依據最小權限及資訊最小揭露原則進行安全管控設計。

(二) 應定期針對可存取銀行內部網路之駐點廠商人員，辦理電子郵件社交工程教育訓練。

二、 核心資通系統及第一類電腦系統之委託契約或相關文件中，應明確約定下列內容：

(一) 應要求受託廠商遵守本基準及其他適當資訊安全國際標準要求，確保資料安全。

(二) 應與受託廠商就服務品質、水準、效能等方面訂定服務要求。

(三) 應依本基準內容對受託廠商進行適當監督。

(四) 當發生資安事故時，受託廠商應主動、即時通知委託人。

(五) 應確保交付之系統或程式無惡意程式及後門程式，其放置於網際網路之程式應通過程式碼掃描或黑箱測試。

**12：廠商報價單內容應包含各項軟、硬體交貨期限等資訊。**

**(A01)** **系統使用單位**

|  |  |  |  |
| --- | --- | --- | --- |
| 項目 | | 說明 | 預估(尖峰)使用人數 |
| 客戶及本行內部人員使用 | **○** |  |  |
| 僅本行內部人員使用 | **○** | ○全行使用  ○總行部室  ○部分、單一部室使用 |  |
| AP應用系統每秒可承受之最大User數 | |  | |
| AP應用系統每一交易之平均執行時間 | |  | |
| AP應用系統每秒/每小時之交易筆數 | |  | |
| 營運衝擊等級分類(註) | | 高○ 中○ 低○ | |
| 資安評估分類(註) | | 第一類○ 第二類 ○第三類○ 不適用○ | |

註：請依據 IS2005-02-系統架構建置資安風險評估表 填寫。

**(A02)** **系統復原目標時間RTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 系統復原目標時間RTO | | 系統備援需求 | | 備註 |
| 同地 | 異地 |
| 2小時 | ○ | ● | ● | 金管會新聞稿要求為2小時 |
| 8小時 | ○ | ○ | ○ |  |
| 夜間批次前 | ○ | ○ | ○ | 請評估是否需同、異地備援 |
| 隔日開業前 | ○ | ○ | ○ | 請評估是否需同、異地備援 |
| 一周內 | ○ | ○ | ○ | 單機 |
| 一周以上 | ○ | ○ | ○ | 單機 |

註1：正式環境RTO為2小時，則必須建立同、異地備援機制。

註2：若有特殊需求請提出討論。本表若有●紅點為必備條件(含以下各項)。

**(A03) 系統架構圖**

須包含應用系統各伺服器角色(WEB、AP、DB、核心主機、其他等)，一般使用者連線方式，維護人員連線方式，區分正式、測試、整測、DMZ環境，所使用TCP/UDP Port，連線方向，各項硬體設備(網路、伺服器、磁碟機等)，連線本行其他外圍系統，本行提供之基本服務(如AD、SMTP、TFS)，**請特別標示本案採購項目**。

**(提供24小時服務、對外服務之系統，其資料庫系統應規劃為獨立使用之資料庫系統，若使用本行集中化資料庫，應配合本行停機維護作業時間)**

**(A04)應用系統之主機清單暨作業系統、資料庫**(依系統架構圖需採購主機數量填寫)

PS：台數為該項目所有主機數量；Core數及RAM為單一台主機所需數量。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | WEB主機 | | | AP主機 | | | DB主機 | | | 其他( ) | | | 其他說明事項(版本中/英文) |
| 作業系統廠牌/版本 | |  | | |  | | |  | | |  | | | 以下core數、RAM大小均為每一台規格 |
| 資料庫廠牌/版本 | | 無 | | | 無 | | |  | | |  | | | 若DB採用集中化主機，請參考(D01)資料庫系統開發配合事項 |
| 正式環境 | | ○實體 ○VM | | | ○實體 ○VM | | | ○實體○VM○集中 | | | ○實體 ○VM | | |  |
| 主機數量/CPU Core/RAM | | 台數 | Core數 | RAM | 台數 | Core數 | RAM | 台數 | Core數 | RAM | 台數 | Core數 | RAM |  |
| 正式主機 | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 本地備援主機 | |  |  |  |  |  |  |  |  |  |  |  |  | 本地備援主機規格同正式主機 |
| 異地備援主機 | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 待版/整測主機 | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 其他主機 | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 測試環境 | | ○實體 ○VM | | | ○實體 ○VM | | | ○實體○VM○集中 | | | ○實體 ○VM | | |  |
| 主機數量/CPU Core/RAM | | 台數 | Core數 | RAM | 台數 | Core數 | RAM | 台數 | Core數 | RAM | 台數 | Core數 | RAM |  |
| 測試主機 | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 其他主機 | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 主機數量總計： | |  | | |  | | |  | | |  | | |  |
| CPU Core數總計： | |  | | |  | | |  | | |  | | |  |
| 授權計算方式： | |  | | |  | | |  | | |  | | |  |
| OS License採購數量總計： | |  | | |  | | |  | | |  | | |  |
| DB License採購數量總計： | | 無 | | | 無 | | |  | | |  | | |  |
| 硬體額外需求 | Raid Card/數量 | ○否 ○是/ | | | ○否 ○是/ | | | ○否 ○是/ | | | ○否 ○是/ | | | 規格： |
| HBA卡/數量 | ○否 ○是/ | | | ○否 ○是/ | | | ○否 ○是/ | | | ○否 ○是/ | | | 規格： |
| 網卡/por數量 | ○否 ○是/ | | | ○否 ○是/ | | | ○否 ○是/ | | | ○否 ○是/ | | | 規格： |
| 是否儲存個資 | | ○否 ○是/ | | | ○否 ○是/ | | | ○否 ○是/ | | | ○否 ○是/ | | | 選”是”請說明儲存方式，如Log、File、DB |
| 其他說明事項：  1.採購之作業系統及資料庫授權數量需足夠，作業系統及資料庫需皆為64位元版本，並請填除版本編號及標準版/企業版等資訊；  2.作業系統若為Windows，版本請填 標準版 / Data Center；非Windows作業系統，版本請填作業系統版本編號。  3.若需多個測試環境請註明可共用或不可共用主機，共用主機台數可寫1台，但請考量系統承載量，非共用主機則請依實際數量填寫，。  4.本行虛擬化環境標準規格為4 Core vCPU + 8GB 記憶體，最大規格為8 Core vCPU + 32GB 記憶體，超過此規格無法再增加CPU及記憶體請考量採用實體機。  5.本行虛擬化環境CPU為共用運算資源，無法提供獨立CPU運算資源；若使用虛擬主機，需考慮系統承載量，勿為虛擬化而虛擬化。  6.考慮硬體承載量，本行均建議AP與DB不為同一台主機。  7.需考慮3~5年之交易成長量，記憶體建議至少為32GB(含)以上，硬碟轉速至少需1萬轉(含)以上，DB主機記憶體建議128GB(含)以上。  8.若有備份需求，Server主機至少需要有獨立的 1 GB 1 Port的網卡1張，線上交易與備份作業需使用不同網卡。  9.DB測試機使用內部硬碟作為存放資料庫或備份空間。DB正式機使用內部硬碟作為存放備份空間，至少2張(RAC環境至少3張 ) 各4 Port Gigabit網卡，至少2張HBA卡。 | | | | | | | | | | | | | | |

**(A05)應用系統主機備援機制需求**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 主機 | 本地備援採用方式 | | | | 異地備援採用方式 | | 說明事項 |
| Cluster | VMware vMotion | F5 NLB | 其他方式 | 單機 | VMware vMotion |
| WEB | ○Y ○N | ○Y ○N | ○Y ○N |  | ○Y ○N | ○Y ○N |  |
| AP | ○Y ○N | ○Y ○N | ○Y ○N |  | ○Y ○N | ○Y ○N |  |
| DB | ○Y ○N | ○Y ○N | ○Y ○N |  | ○Y ○N | ○Y ○N | 若選VMware vMotion為僅建置在VM主機上之DB主機 |
| 其他 | ○Y ○N | ○Y ○N | ○Y ○N |  | ○Y ○N | ○Y ○N |  |
| 其他說明事項：  1.本表之填寫需參考「(A06) 應用系統相關主機是否可建置於VM 環境或實體伺服器」填寫內容。  2.若為Cluster運作，需注意是否需採購Cluster軟體。  3.DB備援方式請依左列方式填入其他方式欄位：磁碟底層抄寫。Oracle DB：DataGuard、RAC、GoldenGate。IBM DB：HADR。微軟DB：SQL Always On可選擇，但須注意軟體授權數量。  4.備援方式需對應到磁碟空間需求表格填寫。 | | | | | | | |

**(A06)主機磁碟空間需求 (GB)**

1.為本專案總需求空間，需預估系統上線後5年內之成長量，AP應用系統與資料庫系統需有House Keeping機制。若有異地備援需求，須注意磁碟空間。

2.若採虛擬化方式建置，正式環境與異地備援總空間須加計25%空間作為快照及備份使用。

3.除正式(同地備援) ONLINE交易資料庫系統之磁碟保護採用RAID-10保護外，其餘均為採用RAID-5保護，若有特殊需求請提出。

4.AP應用系統程式、交易紀錄檔與AP應用系統LOG等，需區分不同磁碟空間或不同Mount Point存放，設備規格資料可由本行提供，廠商再提供報價。

5.資料庫系統與資料庫備份檔需區分不同磁碟空間或不同Mount Point存放。設備規格資料可由本行提供，廠商再提供報價。

6.DB系統ORACLE為使用 DB或Table Export及RMAN備份：MS SQL為使用資料庫備份方式；為每日執行Full+Transaction(Archive) Log備份；均為先備份至磁碟再上磁帶，故需考慮DB備份使用之磁碟空間；測試DB均不作備份，若有特殊需求請提出。

7.測試環境資料庫一律使用測試環境集中化資料庫，AP人員無Create Database權限，若有特殊需求請另外提出。

8.SQL Server測試環境資料庫若有需使用正式環境資料當作測試資料，需使用測試環境集中化資料庫環境，並建立去識別化機制，否則另需採購主機及SQL Server軟體授權。

**(A06-1)主機磁碟空間需求-WEB主機 (GB)**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 環境別 | | A | B | C | D | E | F | G | H | 說明/計算公式說明  (請務必填寫) |
| 作業 系統 | WEB 系統程式 | 每年資料成長量 | | | 資料 備份量 | 5年 成長量 | 5年 需求 總計 |
| 目前資 料量 | 交易 紀錄 | 其他 |
| 100 | 100 | 10 | 10 | 0 | 20 | 100 | 300 | 我是範例 |
| 正式  環境 | 正式主機 |  |  |  |  |  |  |  |  |  |
| 本地備援主機 |  |  |  |  |  |  |  |  | 本地備援若採用Cluster、VMwarev Motion機制，本項B~H欄位不用填寫 |
| 異地備援主機 |  |  |  |  |  |  |  |  |  |
| 待版/整測主機 |  |  |  |  |  |  |  |  |  |
| 其他主機 |  |  |  |  |  |  |  |  |  |
| 測試  環境 | 測試主機 |  |  |  |  |  |  |  |  |  |
| 其他主機 |  |  |  |  |  |  |  |  |  |
| 各使用空間統計： | |  |  |  |  |  |  |  |  |  |
| 其他說明事項：  1.若需多個測試環境請註明可共用或不可共用主機，共用主機台數可寫1台，但請考量系統承載量；非共用主機則請依實際數量填寫，但使用空間請加倍計算。  2.作業系統(A)均為100Gb，若有特殊需求請提出。  3.WEB系統程式(B)若需備份則為每周或每月備份一次，若有特殊需求請提出。  4.資料備份量F (系指每日應備份資料) =C+D+E；5年成長量G=F\*5；5年需求總計H=A+B+G；若WEB系統程式會增長應一併加入計算。  5.本地備援主機及異地備援主機磁碟空間與正式主機一致。 | | | | | | | | | | |

**(A06-2)主機磁碟空間需求-AP主機 (GB)**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 環境別 | | A | B | C | D | E | F | G | H | 說明/計算公式說明  (請務必填寫) |
| 作業 系統 | AP應用 系統程式 | 每年資料成長量 | | | 資料 備份量 | 5年 成長量 | 5年 需求 總計 |
| 目前資 料量 | 交易 紀錄 | 其他 |
| 100 | 100 | 10 | 10 | 0 | 20 | 100 | 300 | 我是範例 |
| 正式  環境 | 正式主機 |  |  |  |  |  |  |  |  |  |
| 本地備援主機 |  |  |  |  |  |  |  |  | 本地備援若採用Cluster、VMwarev Motion機制，本項B~H欄位不用填寫 |
| 異地備援主機 |  |  |  |  |  |  |  |  |  |
| 待版/整測主機 |  |  |  |  |  |  |  |  |  |
| 其他主機 |  |  |  |  |  |  |  |  |  |
| 測試  環境 | 測試主機 |  |  |  |  |  |  |  |  |  |
| 其他主機 |  |  |  |  |  |  |  |  |  |
| 各使用空間統計： | |  |  |  |  |  |  |  |  |  |
| 其他說明事項：  1.若需多個測試環境請註明可共用或不可共用主機，共用主機台數可寫1台，但請考量系統承載量；非共用主機則請依實際數量填寫，但使用空間請加倍計算。  2.作業系統(A)均為100Gb，若有特殊需求請提出。  3.AP應用系統程式(B)若需備份則為每周或每月備份一次，若有特殊需求請提出。  4.資料備份量F (系指每日應備份資料) =C+D+E；5年成長量G=F\*5；5年需求總計H=A+B+G；若AP應用系統程式會增長應一併加入計算。  5.本地備援主機及異地備援主機磁碟空間與正式主機一致。 | | | | | | | | | | |

**(A06-3)主機磁碟空間需求-DB主機(GB)**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 環境別 | | A | B | C | D | E | F | G | H | I | 說明/計算公式說明  (請務必填寫) |
| 作業 系統 | DB 系統程式 | 每年資料成長量 | | | 資料 備份量 | 5年 成長量 | DB 備份 空間 | 5年 需求 總計 |
| 目前資 料量 | 交易 紀錄 | 其他 |
| 100 | 100 | 10 | 50 | 0 | 60 | 300 | 750 | 500 | 我是範例(H與I分開計算) |
| 正式  環境 | 正式主機 |  |  |  |  |  |  |  |  |  |  |
| 本地備援主機 |  |  |  |  |  |  |  |  |  | 使用OS Cluster、單機本欄不需填寫。 |
| 異地備援主機 |  |  |  |  |  |  |  |  |  | 同正式主機 |
| 待版/整測主機 |  |  |  |  |  |  |  |  |  |  |
| 待版/整測倒檔空間需求 |  |  |  |  |  |  |  |  |  | 若需DB全部倒檔，則為正式主機資料庫G欄空間1/2 |
| 測試  環境 | 測試主機 |  |  |  |  |  |  |  |  |  |  |
| 倒檔空間需求 |  |  |  |  |  |  |  |  |  | 若需DB全部倒檔，則為正式主機資料庫G欄空間1/2 |
| 各使用空間統計： | |  |  |  |  |  |  |  |  |  |  |
| 其他說明事項：  1.若需多個測試環境請註明可共用或不可共用主機，共用主機台數可寫1台，但請考量系統承載量；非共用主機則請依實際數量填寫，但使用空間請加倍計算。  2.作業系統(A)均為100Gb，若有特殊需求請提出。  3. DB系統程式(B)為每月備份一次，若有特殊需求請提出。  4. DB備份空間H(Windows)、/backup(UnixBase)，為產生資料庫備份檔所需空間，Oracle資料庫約需2.5倍空間H=G\*2.5；SQL Server資料庫約需1.25倍空間H=G\*1.5。  5.資料備份量F (系指每日應備份資料) =C+D+E；5年成長量G=F\*5；5年需求總計I=A+B+G。  6.Oracle RAC DB主機若採用ASM保護機制， DB磁碟空間最少為2倍。Oracle DG及MS SQL Always On 2台DB主機磁碟空間為2倍，每增加一台主機空間增加1倍。  7.本地備援主機及異地備援主機磁碟空間與正式主機一致。 | | | | | | | | | | | |

**(A06-4)主機磁碟空間需求-其他主機(GB)**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 環境別 | | A | B | C | D | E | F | G | H | 說明/計算公式說明  (請務必填寫) |
| 作業 系統 | 系統  程式 | 每年資料成長量 | | | 資料 備份量 | 5年 成長量 | 5年 需求 總計 |
| 目前資 料量 | 交易 紀錄 | 其他 |
| 100 | 100 | 10 | 10 | 0 | 20 | 100 | 300 | 我是範例 |
| 正式  環境 | 正式主機 |  |  |  |  |  |  |  |  |  |
| 本地備援主機 |  |  |  |  |  |  |  |  | 本地備援若採用Cluster、VMwarev Motion機制，則B~H欄位不用填寫 |
| 異地備援主機 |  |  |  |  |  |  |  |  |  |
| 待版/整測主機 |  |  |  |  |  |  |  |  |  |
| 其他主機 |  |  |  |  |  |  |  |  |  |
| 測試  環境 | 測試主機 |  |  |  |  |  |  |  |  |  |
| 其他主機 |  |  |  |  |  |  |  |  |  |
| 各使用空間統計： | |  |  |  |  |  |  |  |  |  |
| 其他說明事項：  1.若需多個測試環境請註明可共用或不可共用主機，共用主機台數可寫1台，但請考量系統承載量；非共用主機則請依實際數量填寫，但使用空間請加倍計算。  2.作業系統(A)均為100Gb，若有特殊需求請提出。  3.AP應用系統程式(B)若需備份則為每周或每月備份一次，若有特殊需求請提出。  4.資料備份量F (系指每日應備份資料) =C+D+E；5年成長量G=F\*5；5年需求總計H=A+B+G；若AP應用系統程式會增長應一併加入計算。  5.本地備援主機及異地備援主機磁碟空間與正式主機一致。 | | | | | | | | | | |

**(A06-5) 主機磁碟總空間統計(GB)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 正式環境 | | | | | 測試環境 | 使用空間總計 | 說明事項 |
| 正式  主機 | 本地備援  主機 | 異地備援  主機 | 待版/整測  主機 | DB 備份空間 | 測試主機 |  |  |
| WEB主機 |  |  |  |  |  |  |  |  |
| AP主機 |  |  |  |  |  |  |  |  |
| DB主機 |  |  |  |  |  |  |  |  |
| 其他主機 |  |  |  |  |  |  |  |  |
| 請將A06-1~4項H欄(DB含I欄)內資料填入相對應欄位! | | | | | | | | |

**(A07)資料備份需求可於架構會議上做確認**

○ 配合本行使用Veritas NetBackup備份軟體做備份。(續填本表 備份項目、備份週期、備份資料量)

○ 需另外採購備份軟體，名稱： 。(續填本表各項目)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 備份主機 | 備份項目 | License數量 | 備份週期(日/週/月) | 備份資料量 | 備註 |
| WEB | * O.S. ○ File ○ DB |  |  |  |  |
| AP | * O.S. ○ File ○ DB |  |  |  |  |
| DB | * O.S. ○ File ○ DB |  |  |  | ○依照以下其他說明事項2作業方式 |
| 其他 |  |  |  |  |  |
| 其他說明事項：  1.本行所有備份均以file方式做備份，每日備份保留2週，每週備份保留2個月，每月備份保留15年，若有特殊需求請提出。如有特殊需求請提出。  2.DB系統Oracle為使用 Table Export及DB RMAN備份方式；MS SQL為使用資料庫備份方式。備份均為先備份至磁碟再上磁帶，故需考慮DB備份使用之磁碟空間；測試DB均不作備份，若有特殊需求請提出。  3.備份及有倒檔需求之主機請注意是否都需要各一個License。  4.需要備份之主機至少需要有獨立的 1 GB 1 Port 網卡1張，線上交易與備份作業需使用不同網卡。  5.本行正式環境之虛擬機為每兩周備份一次，若有特殊需求請提出。 | | | | | |

**(A08)AP應用系統伺服器安裝使用軟體(含Open Source)** (AP應用系統所需之系統軟體均需詳列，包含內附及需採購項目)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 應用系統伺服器安裝使用軟體 | | | | | |
| 廠牌、軟體名稱 |  |  |  |  |  |
| 自行開發/套裝軟體 |  |  |  |  |  |
| 版本(32/64bit) |  |  |  |  |  |
| 本行需採購 | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N |
| 提供本行Source Code | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N |
| 本行可修改Source Code | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N |
| 使用情境及授權考量 | | | | | |
| 系統使用 | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N |
| 外部使用 | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N |
| 內部使用 | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N |
| 程式使用 | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N |
| 授權方式 |  |  |  |  |  |
| 維護方式 | | | | | |
| 本行自行維護 | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N |
| 委外廠商維護 | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N | ○Y ○N |
| 安全更新機制 |  |  |  |  |  |
| 數量 |  |  |  |  |  |
| 備註 |  |  |  |  |  |
| 其他說明事項：  1.如使用Websphere、JBoss、Tomcat、Apache等，應注意採購Java軟體授權。  2.如使用Weblogic，無需再另採購Oracle JDK。(註：Oracle Java SE(EE)-包含JDK,JRE,JavaFX Runtime 和 JRockit JDK)。  3.使用各項軟體含Open Source應注意軟體合法授權使用。  4.開發廠商使用Open Source軟體，如情資發出重大弱點，日後需完整負責相關修補及修補後確認應用程式可正常運作。(例：Struts 2、Spring Framework、Apche Log4j…) | | | | | |

**(A09) 個資保留說明**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **伺服器角色** | **正式環境** | | | | **測試環境** | **保留年限** | **清除方式** | **備註說明** |
| 正式主機 | 本地備援主機 | 異地備援主機 | 待版/整測主機 | 測試主機 |
| WEB主機 |  |  |  |  |  |  |  |  |
| AP主機 |  |  |  |  |  |  |  |  |
| DB主機 |  |  |  |  |  |  |  |  |
| 其他主機 |  |  |  |  |  |  |  |  |

**(A10) 設備置放資訊機房需求**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ○本案設備置放於 北瓦 資訊機房 | | | ○本案設備置放於 北瓦及備援 資訊機房 | | | | |
| ○本案設備置放於 備援 資訊機房 | | | ○本案設備需置放於 北瓦(備援)資訊機房 以外區域 | | | | |
| 設備名稱 | 存放位置 | 使用機架容量  (座/U) | 電力規格 | 電流/瓦數 | 插頭規格 | 電力迴路 | 備註 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 其他說明事項：  1.本案設備不管置放北瓦資訊機房(含備援機房)與否，廠商均需包含網路配線、配電及提供排插。 | | | | | | | |

**(A11)** **軟、硬體使用及維護年限、EOS日期說明**

請列出本案採購之軟、硬體項目其使用年限、EOS日期等資訊。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 項目 | 分類 | 使用/維護年限 | EOS日期 | EOS處理方式 | 備註說明 |
|  | ○軟體○硬體 |  |  |  |  |
|  | ○軟體○硬體 |  |  |  |  |
|  | ○軟體○硬體 |  |  |  |  |
|  | ○軟體○硬體 |  |  |  |  |

**(B01)使用者工作站軟、硬體需求**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 使用者工作站安裝應用系統軟體需求 | | | | | | | | | | |
| 工作站 | 是否  安裝 | | 廠牌、系統  軟體名稱 | | 版本 | 32/64bit | 自行開發/  套裝軟體 | 本行是否  需採購 | 用途 | 備註 |
| 一般使用者 | ○Y ○N | |  | |  |  |  | ○Y ○N |  |  |
| 系統開發人員 | ○Y ○N | |  | |  |  |  | ○Y ○N |  | 資訊區塊開發人員 |
| 使用者工作站建議硬體規格 | | | | | | | | | | |
| 工作站 | | CPU時脈、Core | | 記憶體 | | 硬碟容量 | OS版本 | 瀏覽器版本 | 用途 | 備註 |
| 一般使用者 | |  | |  | |  |  |  |  |  |
| 系統開發人員 | |  | |  | |  |  |  |  | 資訊區塊開發人員 |
| 其他說明事項：  1.目前本行個人工作站作業系統為：Win 10 (LTSC及SAC) 32/64 bit、RAM 8GB。  2.如需採購Client端(使用者)主機，應以本行現行規格為主。  3.系統開發瀏覽器請以Google Chrome & Microsoft Edge為主要核心。  4.禁止使用IE 11及Adobe Flash Player。 | | | | | | | | | | |

**(B02)一般(含分行、總行)使用者連線交易資料傳輸量評估**(指行內使用者與AP應用系統間連線)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 交易方式 | | 通訊埠 | 用途說明 | 單筆交易資料  傳輸量(Kb) | 預估尖峰時段  交易量(筆數) | 特殊頻寬  需求(\*4) | 備註 |
| Server-Client | ○Y ○N |  |  |  |  | ○Y ○N |  |
| Web Browser | ○Y ○N |  |  |  |  | ○Y ○N |  |
| 其他方式 |  |  |  |  |  | ○Y ○N |  |
| 交易過程是否加密 | 加密方式： | | | | | | |
| 其他說明事項：  1.AP應用系統與資料庫主機不開放網路芳鄰、分享資料夾等通訊埠，資料庫主機且不開放行內使用者直接連線使用。  2.右列TCP Port 若無使用須關閉：21, 22, 23, 25, 80, 110, 443, 1433, 1521, 1526, 3306, 3389, 4100, 5432, 5631, 5800, 5900, 7001, 8080, 8889。  3.應使用Web Browser介面做為各類交易之連線方式，非使用此連線方式均須提出說明；另須提供後台管理人員資料修改介面。  4.目前分行線路頻寬(下行/上行)：ADSL(20M/5M)、專線(8M/8M、忠孝分行(4M/4M))，若有特殊需求請於下方提出說明。 | | | | | | | |
| **特殊頻寬需求說明：** | | | | | | | |

**(C01) 應用系統開發配合事項**

1.不得以本機最高權限綁定或執行相關AP應用系統程式。

2.得建置AP應用系統警示機制(包含Keep Alive、System Error等)、AP應用系統log、系統日誌須配合有異機存放機制。

3.得具備Single sign on Password（請參考附件二說明）。

4.AP得提供使用者完整操作記錄軌跡及記錄異地存放機制。

5.應建立後台資料查詢與修改介面。

6.測試資料庫使用正式環境資料當測試資料，得建立敏感性資料遮罩機制。

7.得建立HouseKeeping機制，以節省磁碟及避免造成系統異常，並提供HouseKeeping程序或程式。(上線前需檢附於電腦主機檢核表)

8.Windows BASE系統之C磁碟空間及Unix BASE系統之根目錄磁碟空間僅可供O.S.開機系統使用，其他AP系統程式、AP系統之LOG、資料庫DATA等均須放在該磁碟空間以外之磁碟空間。

**(C02) DMZ區限制事項**

|  |  |  |
| --- | --- | --- |
| 限制事項 | 確認項目 | 備註 |
| DMZ區伺服器提供檔案上傳功能及其檢核控管機制 | ○提供 ○不提供 | 供外部客戶連線之DMZ區網站伺服器提供檔案上傳功能，檢核控管機制說明如下： |
| DMZ區伺服器不得具備後台管理平台功能 | ○具備 ○不具備 | 僅供外部客戶連線之DMZ區網站伺服器，其後臺管理平台應與客戶使用平台分離 |
| 其他說明事項：  1.DMZ區只開放WEB、SMTP、FTP、DNS等服務。 | | |

**(C03) 管理需求**

|  |  |  |
| --- | --- | --- |
| 管理事項 | 確認項目 | 備註 |
| 納入本行AD系統管理 | ○Y ○N | 內部Windows伺服器均須納入AD管理，DMZ區則不納入AD管理。 |
| 納入本行防毒系統管理 | ○Y ○N | 所有Windows伺服器均須納入管理 |
| 防毒軟體掃毒例外清單 | ○Y ○N | 例外清單： |
| 是否需FTP檔案傳輸 | ○Y ○N | 需使用集中化FTP伺服器將檔案FTP至其他主機或外部單位，並使用SFTP方式進行檔案傳檔，一般伺服器為FTP Client端 |
| 該系統具有敏感性資料 | ○Y ○N | ○WEB ○AP ○DB ○其他： 說明： |
| 電子郵件寄送需求 | ○Y ○N | ○測試(禁止及對外寄送) ○寄送內部 ○寄送外部 ○其他： 說明：需說明電子郵件寄送對象 |
| 微軟安全性更新 | ○Y ○N | ○自動：執行時間：○07：00 ○10：00 ○11：00 ○12：00 ○16：00 ○17：00  ○手動：手動執行時間：請相關負責人員到場協助執行及驗測 |
| 應用系統使用基礎架構服務，應使用非同步模式開發 | ○Y ○N | 說明：應用系統使用基礎架構服務(如SMTP)，應使用”非同步模式”開發，禁止使用”同步模式”開發 |
| 其他說明事項：  1.禁用administrator、root等本機高權限帳號作為服務帳號；Windows平台均須進行微軟安全性更新作業。  2.禁止將個人帳號加入Administrators或RDP群組中。  3.禁止使用者、業務經辦及系統管理人員直接由PC利用RDP方式連線正式環境。 | | |

**(C04)應用系統使用之內外部網路通訊埠及檔案交換需求**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 分類 | | 使用通訊埠/服務 | 用途 | | | | 備註 |
| 一般使用者 | |  |  | | | |  |
|  |  | | | |  |
| 系統管理員  與開發人員 | |  |  | | | |  |
|  |  | | | |  |
| 應用  系統 | 內部連線 |  | F5需求 | ○Y ○N |  | |  |
|  | F5需求 | ○Y ○N |  | |  |
| 外部連線 |  | F5需求 | ○Y ○N |  | |  |
|  | F5需求 | ○Y ○N |  | |  |
| 檔案  交換  需求 | 分類 | 使用通訊埠/服務 | 系統/外部單位名稱 | | | 交換之內部伺服器IP/伺服器目錄/對外網址/對外IP/其他 | 交換方式 |
| 內部系統 |  |  | | |  |  |
| 外部單位 |  |  | | |  |  |
| 其他 |  |  | | |  |  |
| 其他說明事項：  1.此為AP與DB、Web與DB、Client與DB、基本認證及通知服務等之間連線。  2.通訊埠/服務包含一般使用者、系統管理與開發人員、對內連線(WEB、AP、DB、FTP、SMTP、DMZ..etc)、對外連線(Internet)所需之相關資訊。  3.一般使用者係指使用該系統之非資訊區塊作業人員，應提供Web Browser介面做為各類交易之連線方式，另須提供後台管理人員資料修改介面。  4.系統維護操作，人員均須透過VDI進行遠端管理，上線前未列出的通訊埠將關閉不使用。  5.請AP人員以此列出之通訊埠開通防火牆。  6.右列TCP Port 若無使用須關閉：21, 22, 23, 25, 80, 110, 443, 1433, 1521, 1526, 3306, 3389, 4100, 5432, 5631, 5800, 5900, 7001, 8080, 8889  7.資料庫系統主機不提供存放內/外部單位檔案交換檔，若係為系統監控管理之用則須提出說明。  8. 測試環境禁止連線其他環境。  9. 因F5 Load Balance有5分鐘、ASA防火牆有60分鐘Session Idle Timeout機制，故AP應用系統一定要有Keep Alive機制。  10.禁止置於同一F5下之設備，使用F5之VIP作為設備互相連線之方式。  11.系統有對外連線之Web (80 & 443)服務，請申請於WAF之下保護，否則無法上線。 | | | | | | | |

**(C05)應用系統服務帳號需求**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 伺服器角色 | 需申請服務帳號 | 用途 | 帳密壓碼方式 | 加解密方式 | 備註 |
| WEB | ○Y ○N |  |  |  |  |
| AP | ○Y ○N |  |  |  |  |
| DB | ○Y ○N |  |  |  |  |
| 其他 | ○Y ○N |  |  |  |  |
| 其他說明事項：  1.請說明應用系統服務帳號用途、壓碼及加解密機制。  2.禁用administrator、root等本機高權限帳號作為服務帳號。 | | | | | |

**(C06)應用系統各功能執行方式及執行權限**

|  |  |  |  |
| --- | --- | --- | --- |
| 執行方式 | 用途 | 所需權限 | 備註 |
| 網頁 |  |  |  |
| Windows / UnixBase排程 |  |  |  |
| Windows / UnixBase服務 |  |  |  |
| Windows / UnixBase常駐程式 |  |  |  |
| 其他 |  |  |  |
| 其他說明事項：  1.請說明應用系統執行方式及所需權限，原則上不給予高權限執行相關服務。  2.請說明應用系統是否有綁定安裝帳號之需求。  3.請說明應用系統是否有跨伺服器讀取資料之需求。  4.禁用administrator、root等本機高權限帳號作為服務帳號。 | | | |

**(C07)應用系統資料儲存機制**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 伺服器角色 | 檔案格式 | 存檔方式 | 預估單一目錄檔案數量/單一資料庫大小 | 備註 |
| WEB |  |  |  |  |
| AP |  |  |  |  |
| DB |  |  |  |  |
| 其他 |  |  |  |  |
| 其他說明事項：  1.請說明應用系統資料儲存機制，相關資料以資料庫或檔案方式儲存，並預估單一目錄檔案數量及資料庫大小避免效能問題。 | | | | |

**(C08)應用系統資料分級存放機制及Log清除作業執行方式**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 分類 | 執行方式 | 執行時間 | 所需權限 | 機制說明 | 備註 |
| 資料分級存放機制 |  | ○日 ○周 ○月 ○季 ○半年 ○年 |  |  |  |
| Log清除作業 |  | ○日 ○周 ○月 ○季 ○半年 ○年 |  |  |  |
| 其他說明事項：  1.應用系統應規畫資料分級存放機制，超過一定年限之資料存放應由Level(1)、Level(2)磁碟機轉存至低階Level(3)磁碟機或規畫備份至磁帶。  2.應用系統應包含資料分級存放後之資料機制。  3.說明應用系統資料分級存放機制及Log清除作業執行方式及所需權限，原則上不給予高權限執行相關服務。  4.禁用administrator、root等本機高權限帳號作為服務帳號。 | | | | | |

**(D01)資料庫系統開發配合事項**

1.禁止項目：禁止使用Server本機或資料庫最高權限帳號作為資料庫連線帳號；禁止一般使用者申請連線資料庫系統；除系統管理員外其餘人員禁止登入資料庫本機作業。

2.為符合ISO 27001及主管機關相關規定，AP應用系統須建立資料庫系統連線警示(Alert)及Housekeeping機制(含資料生命週期)，HouseKeeping需提供HouseKeeping程序或程式。

3.AP應用系統應建立後台資料查詢與修改介面及建立資料庫存取紀錄；含有個人敏感性資料之資料庫應納入DAM系統。

4. 5.Windows BASE系統，C磁碟空間僅可供O.S.開機系統用，其他AP系統程式、AP系統之LOG、資料庫DATA等均須放在C磁碟空間以外。

5.Unix BASE系統，/root磁碟空間僅可供O.S.開機系統用，其他AP系統程式、AP系統之LOG、資料庫DATA等均須放在/root磁碟空間以外。

6.正式區ONLINE交易資料庫系統檔案之磁碟應以RAID-10做保護(若有其他需求請另外說明)。

7.磁碟陣列機組應佈建HOT SPARE DISK 以增加多一層資料保護機制及減少磁碟機因故障需更換之風險。

8.測試、整測環境資料庫一律使用集中化資料庫，AP人員無Create Database權限，若有特殊需求請另外提出。

9.測試環境資料庫若有需使用正式環境資料當作測試資料，需使用測試環境集中化資料庫環境，並建立去識別化機制，否則另需採購主機及資料庫軟體授權。

○ Y、符合以下數據，可使用本行現有集中化**正式環境資料庫**。

**(若該系統上線後造成整體資料庫效能不彰、影響其他資料庫運作等問題，會強制退出SQL Server集中化DB，且廠商要補增購DB主機及DB License。)**

○ N、需採購DB主機，已填寫於(A06)應用系統之主機清單暨作業系統、資料庫

|  |  |
| --- | --- |
| 項目 | 數值 |
| 空間使用量初始值 | < 100GB |
| 每年空間成長量 | <50GB |
| DB Process同時間使用量 | < 500 |
| 存放歷史資料 | < 3年 |
| 單次select 資料量 | <10GB |

**(D02) 資料庫使用者權限管理**

○ 資料庫使用者權限管理，依 (附件三) 資料庫使用者存取權限控管 來作權限管理。

○ 資料庫使用者權限管理，無法依 (附件三) 資料庫使用者存取權限控管 來作權限管理，請填以下表格。

|  |  |  |  |
| --- | --- | --- | --- |
| User name | System Privilege | Object Privilege | 其他說明 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**(E01)帳號管理**

|  |
| --- |
| 宣導事項 |
| 1. 依據「IS3006-帳號權限管理程序」作業系統及資料庫帳號皆須納管並變更密碼。 2. 非系統預設之服務帳號，僅可進行參數設定之作業，並須配合每年變更密碼。 3. 高權限系統帳號及人員維運帳號，請依流程申請與領用。 4. 非必要之帳號須刪除，若無法刪除則須設定為nologin、locked、停用。 |

**(E02)換版自動化**

|  |  |  |
| --- | --- | --- |
| 項目 | 確認項目 | 說明 |
| ○委由廠商開發  ○本行自行開發(跳至第2題)  ○其他(請於說明欄中敍述) |  | 說明： |
| 1.委外開發合約是否會載明交付原始碼(完整或客製化部分) | ○Y ○N | 說明： |
| 2.集中編譯的建置 | ○廠商 ○AP ○不適用 | 說明： |
| 3.部署腳本的提供 | ○廠商 ○AP ○不適用 | 說明： |
| 其他說明事項：  若合約內載明須交付原始碼，請由系統負責人確認與收妥。 | | |

**(E03)程式碼掃描**

|  |
| --- |
| 宣導事項 |
| 1.依據「IS3008-技術脆弱性管理程序」進行程式碼掃描，以確保本行系統程式之機密性、完整性、可用性。須進行程式碼掃描的範圍與情境如後：網際網路應用系統(DMZ)、安裝於客戶端之應用程式(含APP)且有提供線上服務者、ATM系統、各項因法規要求應完成之系統類別、新系統上線前，若適用範疇與情境變更請依本行管理規範作業。  2.申請換版時須檢附基於當下之owasp規範之「源碼檢測安全性評估報告」，報告中不得有【高】、【中】、【低】風險性弱點，方可進行上版申請。 |

**以上所有項目確認無誤後，請於最後一頁 “附件四”列出所有採購清單!!**

注意事項：

1.廠商報價需包含網路配線、電力配電及提供排插。

2.廠商報價需含上線後1年保固及第2年開始至第5年之維護費用。

3.請確認導入使用之軟、硬體設備，是否符合本行IT Policy規定。

4.請確認因執行本專案，本行是否需自行另外採購之設備(含網卡、光纖卡、NBU Client License)。

5.請確認報價是否含O.S.及DB License，數量是否足夠。

6.請確認是否需採購SAN Switch。

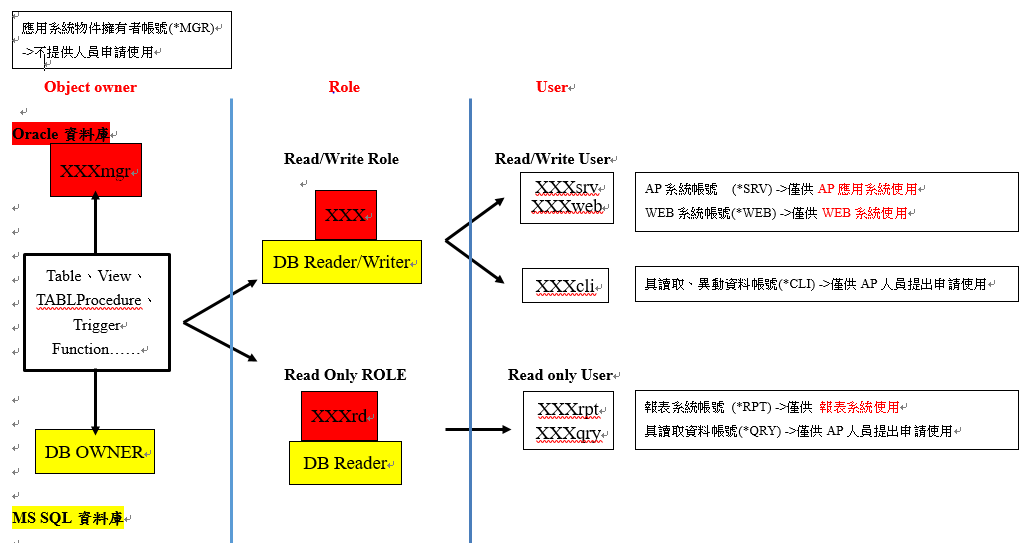
**本表填寫完成應經架構會議討論並確認內容無誤後，連同會議紀錄，留底存查。**

**(附件二) 存取目錄服務(Active Directory, 簡稱AD)程式開發準則**

1. 存取目錄服務時, 請指定本行網域MKTB.com.tw, 勿指定單一伺服器名稱或IP, 以免造成個別伺服器單點失敗(Single Point Failure).

2. 存取目錄服務時, 判斷部門別請以目錄服務中department屬性欄位, 判斷員編請以目錄服務中SAMAccountName屬性欄位.

**(附件三) 資料庫使用者存取權限控管**



**附件四：設備採購清單**

**會議、討論歷程：**