行政院所屬各機關因公出國人員出國報告書

（出國類別：赴國外實習）

參加美商花旗銀行稽核課程研習報告

報 告 人：金管會檢查局　施秘書宜君

金管會銀行局　戴稽核美英

金管會銀行局　鄭稽核雅文

金管會檢查局　王專員俊傑

金管會銀行局　楊專員斐堯

出國期間：94 年 5 月 31 日至 6 月 9 日

出國地點：美國紐約市

參加美商花旗銀行稽核課程研習報告

【目　錄】

肆、附件

附表一：GlOBAL TECHOLOGY AUDIT CO-ORDINATION

附表二：Project Review Process：Project Risk Scorecard（PRS）

附表三：Project Risk Assessment

課程講義資料

壹、目的及過程：

本次訓練之目的，係金管會為提升我金融監理人員之能力，爰洽請國際監理機關及世界知名金融機構，為本會同仁安排專業訓練課程希望藉由同仁實地見習業務運作，汲取先進金融機構之管理理念及經驗，以為我國金融監理制度改進之參考依據。

此次金管會遴派銀行局、檢查局共五位同仁赴美商花旗銀行總行，參加其專為金管會監理人員舉辦有關風險導向之稽核方法論訓練，訓練期間為5月31日至6月9日， 地點為位於美國紐約市花旗總行，該訓練課程係由花旗銀行內部稽核部門負責統籌安排，講師部分則由該部門所轄各功能組別之資深人員輪流對我參訓同仁講解稽核方法之內容，並就我同仁所提之問題作深入討論，以期能於短期內能使我同仁對該行之稽核功能有全面性之瞭解。

第一天首先由該行總稽核 Ms. Bonnie Howard 向我參訓同仁致歡迎辭，並對該行之稽核目標、策略、組織等作簡報，並稽核暨風險查核部門（ARR）之資訊系統暨基礎結構建置組(Technology & Infrastructure)人員介紹稽核方法。其後第二天至第五天分別由策略暨支援組(Strategy & Support) 、企業暨投資銀行組(Corporate & Investment Bank)、消費金融組(Global Consumer)等人員授課。最後 3 天則由負責該行海外分支機構稽核之資深人員，講解該行實際之稽核作業。（餘國際業務組(International)、人力資源及訓練發展組（HR/Learning＆Development）、政策法令遵循組（Policy Compliance Group）及投資服務組(Investor Services)業務因受限於上課時間僅二星期，未含於受訓內容，故不在以下報告陳述）

貳、美商花旗銀行風險導向稽核方法論介紹

第一章 稽核暨風險查核部門（ARR, Audit and Risk Review）介紹

第一節 ARR 之角色

一、ARR 的章程

1.嚴格的實施集團風評估及控制環境，並有效遵守法令、規則及政策。

2.傳遞改善行動的問題及狀況，以確保可即時有效解決問題。

3.致力於在全球金融服務產業中，成為風險評估、控制評估及內部稽核等實務的領導者。

4.提供強調執行控制及風險管理實務之工作環境。

5.注意並發展稽核暨風險查核部門及花旗集團良好能力。

二、ARR 的組織概況

ARR 部門共有約 800 位稽核人員，配置在全球 14 個國家，密切配合花旗組織管理架構，以追求效率最大化。

ARR 附加價值在於透過精密且獨立的評估風格，提供即時建議，以強化控制環境；並經由持續監控各項業務的主要風險控制點及問題採取即時的改善措施、辨識緊急風險及趨勢，俾助於花旗集團成為金融服務產業中最佳風險管理及控制的公司，進而成為最受尊重的全球金融服務業。

ARR 的組成係由獨立性及客觀性、以風險為基礎的查核範圍、人員、溝通、組織及關係等六大要素所構成，謹就各項要素的主要內容，說明如次：

1.獨立性及客觀性（Independence and Objectivity）：

ARR 係直接向稽核暨風險管理委員會（Directors Audit and Risk Management Committee，DAC）報告並負責，該部門有專屬預算及資

源支應 ARR 部門的人員及稽核工具，且被充分授權去設計並執行廣泛的內部稽核計畫並自由且不受限制的接近所有營業據點、業務功能、紀錄、財產及人員。

2.以風險為基礎的查核範圍(Risk-based coverage)：

由各業務經理人員責任確認業務風險並建立控制點，以維持有效監控並確保可及時更正已確認的缺失。ARR 應預先聚焦並辨識緊急風險及趨勢，有效說明並承擔管理上已發現缺失，並負責稽核、監控所採取改正措施，向稽核暨風險管理委員會及稽核工作小組報告稽核結果及趨勢，與業務經理人員共同努力以強化控制環境。

3.人員（people）：

人員應具備良好訓練並具積極進取的工作態度，透過分派具挑戰性工作，訓練人員成為新世代領導人，並藉由業務單位與 ARR 部門人員的輪調，使稽核人員達到並維持稽核人員水準，管理階層應瞭解員工心聲、尊重員工並分派均衡工作量。

4.溝通（communication）：

ARR 部門應本於清楚、簡潔、即時及透明化原則，與集團內業務、經營階層領導者、遵循法令主管及外部稽核等人員充分溝通，並提供一致且即時的風險與控制評估報告。

5.組織（organization）：

建立與各項業務密切結合的組織架構，強化以風險為基礎之分析、一致性、達到好成果及工作團隊之必要性；由全球合作部門（Global Liaison）支應每項查核專門技術；並藉重來自業務部門的客座稽核人員（Guest Reviewer），成為整體稽核評估團隊中的一部分。

6.關係（relationship）：

ARR 除應與稽核暨風險管理委員會、業務部門及簽證會計師持續維持良好關係外，亦與遵守法令主管維持獨立且即時的溝通，培養溝通的透明度。

三、ARR 部門稽核人員之主要功能

風險導向稽核人員編制，設置有區域主管（regional director）綜理地區別之稽核業務，對受檢單位的個別業務均設有**計畫經理人（Program Director）**，並依據該業務之程序或功能指派**領隊稽核（lead reviewer）**。

計畫經理人（Program director，PD），通常一位 PD 負責領導二到三個查核團隊，並負責整合所轄之查核計畫並指定查核領隊。其為整個 ARR 注入價值，包括價值觀念的溝通及領導，確保工作團隊能依 ARR/CITI 的價值觀、道德標準行事，並以身作則及監督、確認每一個人能做對的事。身為 PD 必須對業務單位的專業知識充分了解，可以發揮稽核效率、獲得更多的尊重及與主管單位溝通對話。PD 也要確

認受檢單位提供的產品、服務、組織架構、檢查範圍，分派領隊稽核，掌握檢查計劃與目前擁有的人力去配合檢查頻率等。在整套稽核方法（Audit Approach）中，每一階段 PD 扮演非常重要的角色，簡而言之，如：

- 價值觀的建立：如何將花旗的理念融入稽核計畫之規劃？
- 稽核計畫之管理：如何讓查核工作無所遺漏？定義受查單位（評估受查單位是否有分割、合併或取消之必要）、及為受查單位訂定適當的查核計畫、指定領隊稽核。
- 查核流程之管理：如何確保查核工作及持續監督作業之品質？對於專案查核（project review），確認其關鍵風險及控制程序。對於持續性地業務監控計畫，測試其程序以確保計畫之可行與及時更新。
- 公共關係之管理：與受查單位及內部及外部人士之溝通 －與董事會之稽核與風管委員會、外部會計師及主管機關溝通。

領隊稽核（lead reviewer）係實際負責稽核小組與受檢單位的主要聯絡事宜，主要任務為規劃稽核內容、指揮稽核小組、依據受檢單位自我查核結果，評估受檢單位之營運情形。因 ARR 是獨立於營業單位之外，爲讓整個稽核團隊與營業單位保持更緊密的溝通聯繫，也促使營業單位的人員願意且信任地公開討論與分享任何資訊，領隊稽核扮

重要的溝通橋樑。他們知道如何對受檢單位提出問題，熟悉稽核方法、並瞭解如何稽核及如何才能對整個稽核團隊有益。主要責任是擬定檢查計劃、帶隊檢查及透過持續性地業務監控計畫（business monitoring program）對受檢單位作評估。領隊稽核具有以下的特質：

- 領導統馭能力
- 決策能力
- 出類拔萃的特質
- 瞭解風險及如何控制風險
- 有效的溝通能力
- 人際關係管理能力（Program director 與業務單位管理階層之間的關係管理）
- 瞭解及應用有效的稽核方法
- 設法完成賦予的期望

客座稽核人員（Guest Reviewer）是由來自花旗集團營業單位人員，成為檢查團隊的一員參與檢查。他們提供實務上有關風險和產品的專業知識。反之，他們也從參與查核工作得到獨一無二且良好的訓練經驗。一般而言，一年內約有 400 到 500 個客座稽核人員參與 ARR 的檢查。

第二節 ARR之組織分工

ARR部門是花旗集團稽核及風險控管的核心，配合其集團業務別ARR部門分為8個組，分別是企業暨投資銀行組、消費金融、資訊系統與基礎結構建置組、策略暨支援組、全球合作組、國際組、投資服務組及政策遵循組等，各小組為一相互合作之關係，當查核團隊需要某一專業人才時，即可向其他業務/功能組尋求支援。以下僅就受訓課程中提及之各小組分別介紹其功能。

一、企業暨投資銀行組(Corporate & Investment Bank)

該行依法人金融業務之特性，將對法人金融之稽核業務區分為三大區塊：（1）Global Banking；（2）Global Markets；（3）Global Transaction Services。Global Banking業務主要對象為大規模企業、金融機構、各國政府等，服務範圍包括提供有關購併、重整、放款、外匯交易、帳款管理、股權、債務及衍生性商品之策略及顧問服務等；Global Markets係對企業、金融機構及個人提供各類有價證券之承銷及交易撮合等之交易平台及技術。至Global Transaction Services主要係對跨國企業或持有各國資產之政府機構為提供帳款管理、財務管理、貿易融資、保管清算之統籌呈報及管理。

二、消費金融組(Global Consumer)

稽核範圍，包含個人金融暨投資（Retail Banking and

Investments）、一般放款（住宅、車貸等）、信用卡、小額借貸、以及保險等，受檢單位（entity）之設置係以國別為主，如國家查核（country review，花旗於台灣之業務即設為一受檢單位），較大國家則以主要風險、辦理程序或銷售管道等為設置受檢單位標準，如信用（Credit，如風險管理、放款、備抵呆帳管理等）、營運（operation，如發卡業務、支票處理等）、法令遵循（Compliance，如內部稽核等）、個人金融（分行個人金融營運）、會計帳務管理（financial control，如會計及報表製作呈報）、其他銷售管道等（other Channels，如網路銀行、電話行銷等）。

就 ARR 角度而言，消費金融所隱含的風險有下列各項，不同的營業模式（Different business Models）、多重行銷通路（Multiple Delivery Channels）、銷售程序（Acquisition Process）、營業項目的複雜性（Wide-Spread Operations）、跨產品別的風險管理（Multi-Product Risk Management）、人員組織、法令遵循、內部稽核控制等。

該行對消費金融服務與客戶的分類及配對，係依據客戶資產、教育程度、職業等區分為 A、B1、B2、C1、C2、C3、D1、D2、E 後，再依據客戶屬性銷售適當產品。

有關行銷及服務通路，該行行銷工具可區分為郵件、登門拜訪、雜誌電視廣告、email 等，客戶取得服務方式可區分為直接（direct

retail），如分行直接提供服務；虛擬（direct virtual），如電話行銷；委外行銷（direct agents）；跨業結盟(third party alliances)。另基本業務及服務平台區分為二種：分行（retail branches）及區域中心（centralized operations）。

有關消費金融的風險及控制的評量（Risk and Control Evaluation）方面，謹說明該行所採用工具如下：

1.風險評量表（Risk Appraisal Profile，RAP 另設第三章詳述）：

該紀錄係藉由例行業務監控稽核（business monitoring and auditing）之結果，對現有風險及控制環境作持續性評量紀錄。其具體程序為，首先該行將各受檢單位（entity）之風險依風險因子家族（risk family）分類為：Strategic/Franchise, Legal, Financial reporting, Staffing/Organization, Credit, Market, Insurance, Cross Border, Operational, Systems/Technology 等十種基本型態，受檢單位經評估其各種風險因子之固有風險（inherent risk）之高低程度後，再依受檢單位所採行之控制因子（control factors）妥適性，將沖抵固有風險後所得之殘餘風險（residual risk）區分為高、中或低，最後合併各風險因子之殘餘風險得出全面性評量結果（overall risk assessment），並將此結果與受檢單位之管理人員討論。該結果將決定實地查核之頻率（review frequency）。

2.消費金融標準稽核程序（Consumer Standard Audit Program）：

為加強稽核作業一致性，該行對消費金融相關業務擬定標準之稽核程序，其主要涵蓋範圍有策略及營業計畫（Strategy & Business Plan）、個人金融相關業務（Retail, branch banking, Investments）、法令遵循（Compliance：一般法規遵詢、防制洗錢、資訊保護等）、財務控制及報告（Financial Control & Reporting）、作業管理（Operations）、授信業務（Credit: Commercial Business, Consumer Bank Lending, Consumer Finance）、資訊系統等。

3.業務監控計畫（business monitoring/planning）:

該計畫係依據風險評量表中，最近一次有關受檢單位的風險程度及控制程序及經營績效等稽核結果而設計，該計畫之實行頻率，原則上對風險評量表中風險因子評估結果為高（High）之業務內控程序，需每季加以評估（Quarterly Review），評估範圍包括依據最近一次受檢結果所擬缺失改善措施（Corrective Action Plans）執行情形，受檢單位自我查核結果及考評等。此外該計畫之執行結果亦須納入風險評量表，以利下一次稽核之查核所需。

該計畫之優點，主要為可加強稽核工作與受檢單位管理人員之往來及溝通，使受檢單位能持續評估其內控之有效性，稽核人員能有效驗證受檢單位採行之缺施改善計畫，辨識評估潛在風險等。

4.稽核程序（Audit Process）：

有關量身訂做的檢查計劃（TRP; Tailored Review Program）部分，係針對特定受檢單位所擬具，利用工具如：標準稽核程序（SAP）、風險評量表、業務監控計畫及其後續規劃等組合而成之查核計畫，其範圍包括：風險評量表及例行業務監控計畫 Business Monitoring 所辨識之特定風險，對內控程序的測試（controls to be tested），有關測試之步驟為：觀察、評估政策及程序、抽查（samples for tests）、回測（retrievals）、資訊系統報表等。

上述有關測試之抽查部分，以風險管理為例，其範圍如下：先就受檢單位所具備之資源及經驗，判斷其風險管理之合適性；對例行業務監視計畫中檢測之內控措施，查核其異常狀況並測試（review derivations and test）；有關分行、區域中心授信權限之查核（delegating credit authority）；例外管理情形的查核（exceptions management process）、對信用評分表的查核（credit scores），有關轉銷呆帳及備抵提列相關規定之查核等。

稽核程序中有關稽核結果之歸類及呈報等，該行係將檢查時所發現之下列異常情形（issuing findings）列為初步稽核缺失：

- 業務面（business）政策及程序之異常情形。
- 組織面（corporation）政策及程序之異常情形。
- 當地法律及規定遵循之異常情形。

- 控制程序的潛在缺點（control weaknesses），尤其是可能影響商譽、或法令遵循、財報正確性、企業策略及營運績效等。

上述所發現缺失，依其對受檢單位之商譽或營運績效等之影響程度，並經適當整合後，可分類如下：

- 重大缺失（Major Business Issue，MBI）-具有重大負面影響
- 一般缺失（Business Issue，BI）-負面影響
- 底稿評註（Workpaper Comment）-輕微缺失

5.稽核報告（Audit Reports）：

稽核報告主要為對受檢單位內部控制環境予以評等，其主要依據為：重要的控制程序及業務辦理程序的有效性；所發現缺失的重要性有關受檢單位缺失改進程序的執行能力之評估。

上開稽核報告之評等，區分為：滿意（Satisfactory）；須改進（Needs Improvement）；不滿意（Unsatisfactory）。

- 滿意：係指受檢單位內部控制及業務執行情形正常且有效，稽核時並無發現任何重大缺失（substantial negative impact on the entity）。
- 需要改進：某些內部控制程序及業務執行情形需要改進始能有效執行，意即稽核時曾發現任何重大缺失。
- 不滿意：大部分內部控制程序及業務執行無法有效執行。意即所發

現之缺失需要管理人員立即的改進措施，以將風險降低至可接受之程度。

6. 風險暨內部控制之自我評估（Risk and Control Self-Assessment，RCSA）：

前述稽核報告亦包含有關受檢單位之風險與內部控制之自我評估執行情形的評等，該自我評估標準係整合於花旗集團之自我評估及營運風險整體架構，風險及控管自行評估有關之主要缺失或一般缺失將會影響整體報告之評等，該評等係依據以下四項標準之評估結果而得：

- 基本內控程序（Control Foundation）：

主要係評估主要風險有無有效辨識，是否有無妥適之內控程序，如風險計算衡量、控制程序之執行及紀錄，有無控制程序之補救措施等。

- 控制程序的評估（Control Assessment）：

主要係評估控制程序有無經妥適測試，如定期評估及紀錄主要風險及控制程序，如對主要風險來源之控制程序的定期測試等。

- 缺失改善措施之有效性（Corrective Action）：

缺失改進措施是否及時且完整，如內控缺失發現時，所採取之缺失改進改進是否及時且完整。

- 資訊呈報系統之妥適性（Reporting）：

有無妥適的資訊管理系統（MIS）及缺失呈報體系，如對受檢單位的內部控制狀態及內控程序及執行品質評估之有效性。

依據上述四個標準，風險與內部控制之自我評估之執行結果可分為下列三種評等（Risk and Control Self-Assessment Rating）：

- 有效（Effective）：無任何異常狀況發現。
- 不完全有效（Not Fully Effective）：有一般缺失情形（Business Issue），如該標準未能被有效的執行，受檢單位未能有效保證其內控程序之健全等。
- 薄弱 （Weak）:有重大缺失情形（Major Business Issues），如該自我評估程序未能有效執行等。

至於有關消費金融的風險及控制評估的呈報及溝通程序方面，與其他主要業務相同，原則上均由發現缺失（issues）、缺失改善措施追蹤（Corrective Action Tracking）、稽核工作小組會議（Audit Work Groups）、稽核委員會暨所屬委員會（ Directors Audit Committee and Audit Subcommittees）等程序完成稽核之呈報及溝通。

三、資訊系統暨基礎結構建置組(Technology & Infrastructure)

完整稽核方法應包括資訊風險（Technology Risk）的評估，資訊風險包括：

- 資訊安全性

- 資料保密性
- 法令遵循
- 應用及系統有效性（Availability of applications and systems）
- 資料取得、完整性及被竊取（acquisition、integration divestiture）
- 委外機構管理
- 電子業務及網路應用
- 業務恢復及連續性（recovery continuity）
- 新系統發展
- 公司治理

電腦稽核的稽核方法包括資訊基礎建設（Technology Infrastructure）、專案查核（Application review）、計畫風險查核（Project Risk Review）及發展部門之查核（Development Unit Review）。以花旗集團為例，資訊業務最大特色在於有大約 3 萬位資訊人員及超過 45 萬台資訊設備，其全球的電腦稽核分別在北美、拉丁美洲、墨西哥、歐洲及中東、亞洲（日本）等 5 個區域執行稽核工作，每個區域所執行的電腦稽核均應包括資訊運用查核（Application review）、計畫風險查核（Project Risk Review）及資訊基礎建設（Technology Infrastructure）等三大要素（詳附表 1），其主要內容摘要如次：

1.資訊運用查核（Application review）：

與產品稽核人員一起執行完整的稽核查核產品專案功能及控制全球查核的現況：目前有 55 位專案稽核人員配置在全球 5 大地區，依據標準稽核程序進行風險評估、測試程序及提報應改進缺失，稽核範圍包括：

- 運用控制（Application Controls）：包括自資料投入、處理、產出、稽核軌跡及功能。
- 資料安全評估：自風險評等、資料分類、剩餘風險、改善措施及授權管理等方面評估資料安全性；對於資料安控稽核則包括自業務開始至結束資料處理程序之安全管理、存取權限是否與人員工作責任相當，及每半重新檢視授權妥適性等評估使用者資料存取權限。
- 業務持續性（Continuity of Business）：稽核種點包括業務恢復計畫及測試計畫之核心處理程序、意外事故發生時備援場所。

2.計畫風險查核（Project Risk Review）：

針對具有高風險及有高度影響的業務及初次採用的資訊技術進行查核，包括新系統設計、現行系統重置、系統發展生命週期及計畫改變、遷移及合併等。計畫風險查核方法反應受法規、競爭環境、投資人或客戶、技術發展等內部及外部威脅等因素持續影響。查核程序包括（詳附

表 2）：

- 定義計畫（project Identification）：可藉由參予業務及資訊部門年度計畫或預算編制過程，以瞭解各部門重要的策略、計畫組合預測；或業務及資訊管理系統功能、稽核與風險查核部門相互影響者。
- 開始查核（Review Initiation）：以風險為基礎來分析計畫查核之優先秩序，採用計畫風險計分卡（Project Risk Scorecard，PRS），以風險評分結果排列優先秩序。

  ※評分的風險種類 category：計畫成本、策略排列（strategic alignment）、業務影響（包括交易風險、信用或市場風險、法令或信譽風險）、計畫複雜性、業務或計畫管理、外部風險（產業環境、經濟環境、策略聯盟者或合作夥伴等風險）。
- 實地查核及評估（Fieldwork and Assessment）：
  - 計畫查核特色：在於執行較每季所規劃且結合軟體發展生命週期為長的查核循環，分別就計畫開始、定義、設計、架構、核准、執行及發出執行查核（Post Implementation Review）等進行查核。
  - 查核程序：利用計畫風險評估，對集團策略風險、業務風險、計畫管理風險暨基礎工程及支持風險等評估整體風險趨勢，評估

後與計畫管理小組討論，在檢查及向資深經理人報告前，對所有活動計畫應出具季報。

- 計畫風險評估（Project Risk Assessment, PRA's，詳附表 3）：

  目的在依據整體計畫評估及狀況、計畫風險及問題、發現及建議、緩和活動等維持管理機制。計畫成功主要因素：

  - ✧ 集團策略風險：計畫應與公司或業務之策略及目的一致。
  - ✧ 業務風險：評估項目包括計畫地位、資源管理、業務條件及管理等。
  - ✧ 計畫管理：規劃及觀察、風險管理、財務處理、軟體工程、品質保證及營運準備。
  - ✧ 基礎工程及支持風險（Infrastructure and Support）：資料安全性、委外機構管理、法規、資料中心及業務持續性。

- 結束查核及報告：當計畫查核已經達到重要執行目標及業務目的時即可完成，沒有尚未解決計畫問題，查核報告應摘要計畫歷史問題等級及業務效率等。

3.資訊基礎建設（Technology Infrastructure）：

評估及控制主要產品之資訊基礎設備，例如資料中心、當地及各地區網路及聲音系統；稽核範圍包括產品營運過程、系統架構、電腦系統連線、業務連續性及設備，以確保符合花旗集團資訊技術管理策略

及準則、法令及最佳實務作法；稽核及風險評估部門也執行未被列入查核的重要建設專案（non-rated reviews of strategic infrastructure projects）包括資料中心整合、主要基礎建設發展、平台標準化、自動化及新興的技術等。

四、策略暨支援組(Strategy & Support)

對 ARR 員工提供準則、回應及協助；確保 ARR 部門品質；協助 ARR 管理廣泛資料並分析；維持或支持稽核委員會程序；與法務人員及簽證會計師合作。依功能別旗下設有稽核委員會、策略規劃、報告、品質保證及標準等 5 個室：

1. 委員會委員資格應具備獨立性、專業知識及經驗，審核財務報告及控制財務報告。
2. 策略規劃：對稽核暨風險查核部門員工提供準則、回應及協助。
3. 報告：將 ARR 報告資料轉入花旗集團管理資訊，稽核報告轉入資料庫→當地稽核工作小組→團體稽核工作小組→稽核暨風險管理委員會。主要職掌係為稽核暨風險管理委員會彙總有關 ARR 工作狀況，俾利其向總稽核報告；為 ARR 管理經理人準備該部門每月管理資訊系統之資料；協調年度稽核計畫。
4. 品質保證（quality assurance）：首席稽核經理人應建立且維持品質保證計畫，以評估內部稽核部門之運作，並達到內部稽核專業實

務之標準。目標包括：

- 跨越稽核暨風險查核部門（ARR）達到稽核品質一致性：透過不斷地測量、點對點的評估及對主要稽核程序之評估。
- 維持高標準稽核品質。
- 遵守最佳實務及稽核標準。
- 提供建議及解決方案以改進稽核品質、效率及一致性。

5. 準則：維持及傳達稽核暨風險查核部門之稽核方法論；定義及發展以改變稽核與風險查核部門之策略及程序；管理稽核計畫準則之書庫。

五、全球合作組（Global Liaison）

全球合作部門是 ARR 部門的特色之一，為避免眾多稽核人員對於稽核報告之表達產生重大差異，必需有一個小組負責整合各地區對所缺失事項認知的差異。全球合作組的主要任務為確保稽核之品質及一致性，特別是受檢單位業務性質複雜，涉及全行風險評估、缺失呈報及歸類等，或是有關於如何辨識、歸納全行性的問題等。當有關的產品和功能是廣泛的且要求充分聚焦在下述幾點時，即需要全球合作部門介入：

- 風險評估（risk assessment），檢查意見，全球一致性地檢查報告與評等。

- 總體檢查意見的確認、分級及宣傳。
- 與業務經理人員，法規遵循人員，外部稽核人員及主管機關培養關係。

第2章　控制與風險評估方法論（Control and Risk Assessment Methodology）

於第一章已依受訓日程介紹過大致的稽核方法，在本章再將「控制與風險評估方法論」作整合性的內容介紹，並將於第三章專章介紹稽核方法的精髓-風險評量表(RAP)。

一、風險評估（Risk Assessment）

1.花旗集團的所有業務均列入稽核範圍，並依國別或業務所蘊含之主要風險分割受查單位（audit entity），係為管理稽核活動提供一種有別於法律個體之查核架構。

2.受查單位已被評價且現行風險與控制環境簡要概況已被紀錄(Captured)。

3.衡量固有風險以預防 RAP 每個 ARR 的風險要素的風險，包括策略與商譽風險（Strategic/Franchise）、法令遵循風險、財務報告風險、人員配置與組織風險、信用風險、市場風險、保險風險、跨國風險、作業風險及系統資訊等。

4.辨識控制因素，以減緩固有風險。

5.保持風險綜合評估表 （Risk Appraisal Profile, RAP）之持續有效（Live）：

- 風險綜合評估檔不是一個靜態的檔案，稽核部門必須瞭解業

務部門活動、公司政策及相關風險的第一手訊息，讓RAP檔是一個及時反映最新風險資訊的檔案。

- 稽核部門必須隨時注意所有的消息來源：經濟報告、信評公司訊息、競爭力分析、MIS系統資料、部門自行評估、ARR專家等等。並隨時與業務單位、區域主管或其他部門來的同事（客座稽核人員Guest Reviewer）討論。

二、稽核計畫：

- 查核的全性面：
  - 瞭解業務：瞭解業務為規劃稽核計劃的第一步，深入瞭解業務可由四個面象來進行：1.法律個體2.技術環境3.稽核及法規延革4.與業務有關之其他組織/部門
  - 對業務的瞭解有助於：1.有效查核業務2.適當定位受查單位3.說服業務部門並提高稽核部門之聲譽4.確認市場、經濟環境及法規變化對業務之影響
  - 瞭解所轄稽核計劃之屬性：
    - ✧ 受查單位之規模及數目
    - ✧ 以風險水準劃分受檢單位
    - ✧ 以稽核評等劃分受查單位
    - ✧ 受查單位原始資料之正確及可靠性

- ✧ 確認受查單位之檢查頻率落點
- ✧ 規劃查核時間

➢ 訂定一個全方位的查核計劃：考慮產品、組織架構、業務規模並找出相互關聯及差異點

➢ 計畫經理人必須指定稽核領隊，並不時評估受查單位之適當性，亦即：

- ✧ 是否須為新的業務成立新的受查單位？
- ✧ 現行受查單位有無分割之必要？
- ✧ 現行受查單位有無合併之必要？
- ✧ 現行受查單位之查核範圍是否需要增刪？

● 查核計劃之規劃：

➢ 擬訂查核計劃時應考慮之因素：

- ✧ 在稽核頻率的時限內平均分配工作
- ✧ 平均領隊稽核的工作量
- ✧ 在考量可用資源及個人發展的情況下規劃查核工作
- ✧ 找出需要請客座稽核人員（Guest Reviewers）協助之專業知能
- ✧ 告知業務部門年度稽核計劃
- ✧ 將重大業務活動列入時程

✧ 在稽核計劃中加入由持續監控得到的訊息

✧ 與其他稽核團隊協調（借調人力）

➢ 查核計劃的變更：

✧ 與原訂查核頻率不同之查核計劃是有可能發生的

✧ 與原查核頻率不同之查核計劃必須說明原因並應顯示於自動檢核（Auto Audit）中

✧ 稽核部門主管及外部稽核、主管機關等會把焦點放在高風險受查單位查核計劃之更動

三、稽核頻率：

主要係以前次控制評等及整體風險評估結果為考量基礎，以風險評量表衡量受檢對象（audit entity）整體風險程度(分高風險、中度風險及低風險)，藉以決定稽核頻率（如下表）。例如高風險業務稽核頻率為 12 個月、中度風險業務則每 24 個月查核一次、低風險業務則 36 個月查核一次，ARR 部門仍應配合業務、產品及作業程序變動的速度，調整稽核頻率。

稽核頻率附表：

	稽核頻率			
綜合風險評等	不滿意	須改進	滿意	未評等
高	12 個月	12 個月	12 個月	12 個月
中	12 個月	12 個月	18-30 個月	12-24 個月
低	12 個月	12 個月	30-42 個月	12-24 個月
未評等	12 個月	12 個月	12 個月	12 個月

為因應業務、產品及作業流程的快速變化，自 2005 年開始，Citi 採取一項加速查核頻率的措施，在 2006 年底前，查核頻率將有以下變革：中級風險單位之查核頻率不超過 24 個月、低級風險單位之查核頻率不超過 36 個月。

四、整合的風險基礎方法（稽核週期）：

1.年度計畫、業務監控→業務評估→業務監控；查核範圍及工作計畫→測試及報告。

2.查核方法：

- 內稽部門的查核主要以兩種方式進行，一為實地查核，一為持續性的業務監控。持續性的監控即在平時即必須瞭解受檢單位、與受檢單位建立良好關係、維護風險綜合評估表、監理規劃、與稽核委員會溝通、缺失事項追蹤、年度查核規劃。
- 實地查核即到受檢單位進行檢查，其程序如下：

查核規劃	**—> 實地查核**	**—> 結束查核**	**—> 事後追蹤**
決定查核團隊	查核開始會議	查核團隊評估	準備查核報告
規劃實地查核	與業務部門會談	檢討會	工作底稿
決定抽樣	草擬缺失事項		風險評估檢討
工作分工	釐清管理部門責任		重新評量 RAP
工作排程	衝突管理		回饋

量身訂做的稽核計畫 溝通

後勤作業

溝通

3.查核缺失之彙整：

- 在提出缺失事項之前，領隊稽核必須瞭解所有的查核缺失（findings）
- 與受檢單位討論以確認缺失事項是否正確表達
- 將查核缺失記入查核工作底稿並註明例外事項
- 評估缺失事項並決定其適當表達（重大缺失、業務缺失或工作底稿附註）
- “敏感性議題”之處理：某些議題可能業務單位主管認為過於”敏感”而不願稽核人員將之揭露於查核報告，如法規遵循、稅務等。遇到這種情況，稽核人員必須將問題反映給 ARR 中的策略支援部門—法規遵循全球合作部，並與業務首席顧問討論，以獲知此一議題之表達方式
- 缺失事項分類，並與全球合作部門討論議題之歸類與處理
- 依據對自行查核之評估完成 RCSA 報告
- 評估缺失事項之嚴重程度

4.查核報告：

- 查核報告之撰寫必須針對報告閱讀者之需求；即高階管理階層
- 適當表達問題之嚴重程度；對缺失事項既不隱瞞也不誇大
- 查核報告主要項目
  - 內容為**五、控制評價**及**六、風險暨控制自我評估**
  - 改善措施
  - 附註：
    - ✧ 控制缺失、建議事項及改善計畫
    - ✧ 業務概述及範圍
    - ✧ 業務主管之態度
- 控制環境之評估，並以三項指標作為該控制可否達成預期效果之評量標準：
  - 控制點與業務是否密切配合
  - 所發現問題的重要程度
  - 業務單位改善缺失的能力
- 查核報告品質管制：同儕覆核，以專業角度進行品質確認
  - 為確保查核報告水準，由稽核部門其他同事針對查核報告整體之關聯性及是否適當表達進行覆核
  - 提供改進的觀察及建議

- 提供建議給領隊稽核及稽核主管

五、控制評價（Control Evaluation）：

1.稽核應包括對受檢對象的信譽或財務有重大影響之缺失進行分類，包括有重大負面影響的重大缺失、有負面影響的一般缺失、及查核工作底稿評註中所列影響較小之缺失。

2.稽核報告應包括對控制環境之評估評等（Assessment rating）結果，評等基礎包括主要控制程序及業務執行的有效性、辨識問題的重要性及評估業務上可易於改善的缺失。評等結果分為滿意（Satisfactory）、須改進（Needs Improvement）或不滿意（Unsatisfactory）。

六、風險暨控制自我評估（Risk and control Self-Assessment Evaluation）：詳 p.13

七、業務監控（Business Monitoring）：

業務監控計畫係以最適的風險評量表及稽核期間所執行工作等所評估出風險與控制為計畫基礎。是一個繼續不斷的程序，稽核部門會為每一個檢單位都擬訂一份持續監控計畫（Business Monitoring Plan），並按季提出報告，以獲得對受檢單位控制是否有效之最新訊息。

1.提供有效控制的持續資訊，以減緩主要的業務風險。

2.藉由管理促進 ARR 確認所採取的改善措施，可解決現行控制問題。

3.使 ARR 可迅速反應內部及外部變動，以調整稽核計畫。

4.有助於 ARR 辨識及瞭解所蘊含的緊急風險及潛在問題，並同意採解決措施。

5.改進稽核的有效性、稽核重點及時間。

6.使 ARR 及管理部門建立強且積極的工作關係。

7.持續監督計畫建架於於風險評估檔（RAP）及實地查核的發現。

※持續監督之 3 項標準文件：

1.持續監督計畫

2.持續監督之季報：每季提出持續監督報告，報告內容包含：

(1)持續監督計畫所述之風險、控制及作業流程

(2)缺失事項的書面改善計畫

(3)標準化是非題

3.持續監督的發現：記錄需要改善措施的重大發現

七、計畫風險性查核（Project Risk Review）及專案查核（Special Reviews）：對於未落入一般 ARR 評等之特殊個案，仍必須進行風險評估及查核，主要有以下兩種方式：

1.計畫風險性查核：針對高風險、影響深遠之業務或科技方案，如：系統開發、業務轉換、業務移轉或合併等專案進行個別之風險評

估。

2.專案查核：針對單一事件或特殊要求，如：

- 購併完成之查核：在完成購併之後的 90 天內，對新併入之企業體作一評估
- 特例查核：因應管理部門之要求或由持續監督中（Business Monitoring）發現，對某一特定業務、流程或地區進行分析及測試

八、報告及溝通（Reporting and Communication）：

1.缺失（Issues）：ARR 應就查得並確認之業務風險及控制之缺失，洽請業務單位採取改善措施。

2.改善措施的軌跡（Corrective Action Tracking）：追蹤所有重大缺失及一般缺失之改善情形，且確定過去的缺失已改善。稽核部門必須確保缺失之改善。所有重大缺失及業務缺失均應追蹤改善情形，對於逾期未改善之缺失事項將提昇報告層級。

3.稽核工作小組（Audit Work Group）：ARR 管理部門每季與集團資深經理人開會討論，內容包括良好的稽核、主要業務發展趨勢或一般性問題、過去缺失之改善情形及專案查核報告。

4.稽核暨風險管理委員會暨所屬委員會（Directors Audit and Risk Management Committee（DAC）and Audit Subcommittees）：由

稽核暨風險管理委員會的主管檢視公司的風險管理程序、會計策略及遵守法令程序，ARR 須向稽核暨風險管理委員會報告所查核缺失對於公司營運或主要業務的可能影響。

5.溝通：由各區之稽核團隊（Audit Work Groups）定期（每季）與高階管理階層討論非滿意之查核（less than satisfactory audits）、逾期之改善措施、一般性議題及專案查核。

第三章 風險評量（Risk Appraisal）

第一節 定義及功能

一、定義：

風險（risk）-對業務可能導致反效果之情況或事件

風險評量（risk appraisal）-對於潛在風險所致的影響作出衡量和統整出專業判斷的一套具系統性的過程；所有稽核活動之基礎

固有風險-在無控制或減輕因子下所可能產生的風險

殘餘風險-未能藉由業務控制機制或作業環境之風險減輕因子消除之風險

二、功能：

爲了評估業務或計畫之內控制度的有效性，必須先清楚且徹底的瞭解：

-業務或計畫的活動與目的

-與這些活動或目的相關的風險（即固有風險）

-減輕風險的控制因子或其他因子

-環境在考量風險控制或其他減輕因子後所剩餘之風險（即殘餘風險）

領隊稽核被要求經由對每一個受檢單位依其稽核頻率稽核，完成及維護風險評量表，並以書面方式呈現他們對風險狀況的瞭解。另一個是類似 RAP 的專案檢查計分表，是為對特定的受檢單位作專案檢查而使用，是為確認牽涉新興計畫和初次推行業務的相關風險。

第二節 風險評量表（Risk Appraisal Profile,RAP）

RAP 是會影響到稽核過程的每一個部份，包括從業務監視（business monitoring）到決定實地查核頻率，選擇稽核團隊人員及發

展測試策略以確認應有的內控意見和建議採取的糾正措施。它也是用來與業務單位溝通業務監視與查核主題的有效工具。

一、建立風險評量表

風險評量表是被設計用來對受檢單位所有營運風險為系統性評量的有利工具。ARR 已定義出十種標準的風險組合以之建立區分不同類型風險的共同語言。風險評量可能包含對營運策略和財務操作潛在影響以及立即牽涉到內控層面的觀察。

風險衡量並非是絕對的科學判斷，因它涵蓋了專業的人為判斷。領隊稽核人員必須確認受檢單位所有不同層面活動的關聯性，以對受檢單位的全面性風險作平衡的瞭解。同時，使用一致性的風險衡量矩陣以使吾人能分析在不同時間及不同受檢單位的風險趨勢，也可使稽核資源配置更有效率。

必要的是領隊稽核人員需與 ARR 溝通及協調以確保他們的風險評量能夠併入相關聯的查核知識，另領隊稽核人員會隨時更新 RAP 的內容。如此一來稽核人員就能靠著與管理階層、總體事務聯絡人員、地區經理人及其他 ARR 專家來擴大查核經驗與增加風險衡量的一致性。稽核人員也必須與業務線上的管理階層共同審視衡量結果以確保達到業務風險認知的分享。

二、RAP 的範例：

受檢單位：				
準備人員：				
核准人員：				
日期：				
審視結果：				
風險組合	內生風險等級(高、中、低、無)	實質內生風險水準	控制因子	殘餘風險等級(高、中、低、無)
策略/商譽				
法令/遵循				
財務報告				
人員配置/組織				
信用				
市場				
保險				
跨部門				
作業				
系統/科技				
綜合風險評等	根據：			高、中、低
與 ARR 討論：	姓名：			
與業務單位最終討論	姓名：			日期：

說明：1.審視結果（business overview）是讓讀者對業務引發的風險有簡潔的概念

2.對不同風險種類給予高、中、低或無之等級；另領隊稽核人員需對風險作實質的簡短說明。

3.RAP 要求要應對採取何種方法或控制因子以減輕風險作簡潔說明。

4.領隊稽核人員評估內生控制及風險減輕因子後，決定殘餘風險的等級，所決定的殘餘風險等級是不會比內生風險高。

5.最後領隊稽核人員全面性的衡量所有風險、控制及減輕因子後給予綜合風險評等，並且簡單說明理由及根據，而綜合風險評等將會決定受檢單位被稽核的頻率。

6.最後 RAP 結論將陳閱予 ARR 內負責督導及提供準則的人員及須負責的業務單位經理人員。

- **Business Overview**

是讓讀者對業務單位因業務活動或作業引發的風險有簡單卻高水準的概念。審視結果也在稽核報告的附錄中提供了有關營業單位細項

的描述。而審視結果亦可用 EXCEL 軟體做成的圖表來表達簡短的訊息。

視不同的受檢單位將有不同的描述特徵，如：

-營業規模

-目標市場

-營業所在國家

-法規

-經濟、政治或法令環境

-功能性責任（如：法令遵循，作業管理，財務控制）

-主要業務的產生或改變（如：新系統的完成，規定的改變，架構的重組）

-表現紀錄

-財務目標（如：收入成長，報酬，市場定位）

-特別產品的依賴度、顧客區隔、地域、科技、獨立的合約對象或服務提供商

為了架構以上層面的內涵是需要一些業務統計數字，包括：

收益、報酬率、收益率、顧客群、總人數、成長或變換率、交易量或值、資產及負債、資本額和財務杆桿、財務或風險評等、資產組合、損失，損失預測及損失準備、逾期，協商或其他受損資產、交易期間、交易條件或架構

- **Risk Families**

1. 策略/商譽風險

定義：起因高階業務決策或決策執行帶來的負面結果或影響；營業風險起因於包括國家干擾和負面的大眾意見而使業務無法正常操作

典型來源：

-缺乏對業務策略或風險偏好清楚的定義

-目標市場好高騖遠、高風險或與業務策略或作業環境不一致

-產品組合與策略、競爭/經濟環境或業務單位現有或未來的資源與能一不一致

-潛在報酬不足調整風險水準

-未能遵守產品計劃、政策或程序

-主要市場或顧客偏好的改變

-無法增加收入以彌補損失

-風險管理程序薄弱

-對較大或複雜的交易無法管控風險

-無法維持競爭力

-在既存或新業務快速成長

-國有化或被徵收

-戰爭、暴動

-業務單位與政府機關的關係

-引起傷害公司商譽的潛在原因

標準控制和減輕因子

-清楚並具體表示營運策略

-產品和目標市場與策略、風險偏好、作業環境和可得的資源具一致姓

-強調業務在市場上是或將是一位領導者

-在組織的每一個階層對風險管理都能有強烈的覺醒

-內部控制的監視與追蹤

-良好的統合管理與監督（依產品、地域、功能）

-風險暨資本市場委員會

-獨立的研究分析

-營業策略的覆審（預算與實際執行）

-即時有效的改正紀錄與軌跡

-記錄成功地管理改變

-穩定地市場或消費指標

-精密的情境計畫和壓力測試，包括核熔分析（meltdown analysis）

-在高風險交易、資產組合或產品計劃有行政風險的預防措施

2. 法令/遵循風險

定義：法令遵循風險起因於違反或未能遵守法律、法規或規範，或因規範某產品或顧客行為的法令規定定義不清、未經考驗。會使得公司受

罰款，或導致契約無效。

典型來源：

-未有充足的法令遵循監督

-本地政策及程序與公司標準不一致

-大量的交易與計畫要求內部或外部法定的允准

-業務活動要求具體規範以執行、保護契約或交易權利

-業務活動要求特定揭露（風險、費用、損失的曝險金額等）以避免遭受罰款

-信託關係與信託義務

-外匯交易執行的報告

-洗錢、行賄或可疑交易的可能

-關係人交易的限制

-保密義務與防火牆

-特定證照或資格的要求

-法令環境的變化

-潛在的利益衝突

-產品是否符合消費者的最大利益

-未能依賴法規系統執行契約義務

標準控制和減輕因子

- 精通本國或外國法令規定，有效地風險暨控制自評（Risk and Control Self-Assessment，RCSA）程序

-嚴格的法令遵循監視

-具體規範所有契約和交易

-每日交易確認

-監理審查

-有效地反洗錢計畫

-法規架構與法令要求具一致姓

-清楚的方法以管理防火牆

-有效地認證及註冊程序

-有效的公司治理軌跡紀錄

-穩定的法規環境

3.財務報告風險

定義：財務報告風險起因於未遵循會計政策或主管機關、稅務機關及MIS 對報告的要求，而提交錯誤的資訊或未能及時提交資訊都將導致主管機關或投資大眾或其他主要機關對公司的財務狀況有錯誤的瞭解如此將會造成法規上的懲處或使股票價值減少。其也將誤解造成不適的業務決策和財物損失的原因。

標準來源：

-會計政策和程序不明或與一般公認會計準則、其他適用的會計準則規範或公司標準不一致

-潛在的錯誤、令人誤解或未及時的財務報告都將導致公司的聲譽受損或損害公司的永續經營

-會計政策的濫用導致錯誤的財務報告

-在會計或 MIS 上的歷史資料錯誤

-會計或 MIS 上的資料驗證獨立性不足

-無形資產的錯誤價值判斷

-損失提列不足

-未能以即時及有效的方法調節會計帳

-缺乏可靠的月況、季備忘錄和季執行的報告

-未遵循已建立的程序傳遞財務資訊給公司財務內控單位

-有可能導致主管機關對不正確、誤導或非即時的財務報告的制裁或罰款

標準控制和減輕因子

-清楚且以具體文件表示並和主管機關規定及公司標準一致的會計政策和程序

-強大的 MIS 和管理審查程序

-穩固的月調節及即時的未達帳解決程序和紀錄

-具備強大的內部及外部財務報告規範知識及嚴格的監視是否遵照內外部規範

-經常性地審查及會計調整的批准

-在會計程序上做要求嚴格地檢查及平衡，包括合理的審查，波動分析及年度報告等

-正式的提存審查程序

-對可靠財務報告的簽署

-穩定及良好統合的報告系統及系統進入的限制

4.人員配置/組織風險

定義：員工及組織風險起因於缺乏(1)一套適合及清楚定義的組織架構(2)對員工執行業務有充分及完整的管理和策略(3)道德規範的遵守（無論公司、業界或社會）。若未能維持一個好的管理和控制佳的作業環境皆可能導致業務不能達成目標。

標準來源：

-組織架構與策略或工作程序不一致

-缺乏明顯的分層負責及授權

-未能吸引足夠的適任資格職員留任

-人員流動率高

-過度依賴臨時員工

-未有充足的領導人員

-未能提供員工適合的訓練

-跨階層的資訊分享不足

-責任區份不足或員工有道德風險的可能

-未能有清楚定義責任或要求的委外契約

標準控制和減輕因子

-人員配置與訓練課程與業務策略一致

-依業務活動和程序及組織大小和複雜度有適當的組織架構與監督

-明確的授權與分層負責制度

-適任且具資格的職員

-低流動率

-有效領導

-僱用深度，包括對主要位子有適合的人員備援

-有效地員工同化和訓練進取心

-組織中必要的資訊能充分溝通

-強烈的責任區隔以杜絕利益衝突和確保獨立性

-員工的行為道德標準和利益衝突都能有正式的監視和遵循紀錄

-委外契約清楚定義服務要求與責任

-穩定的營運策略和作業環境

5.信用風險

定義：信用風險起因於借款人、相對人（如：外匯交易或衍生性商品契約等之交易對手）或發行者（如：債或股權之發行）未能及時且完全地依約定履行他的義務，造成對公司的財務上損失。信用風險可能出現在表內或表外，而因違約的損失可能不是發生在交易確定之前就是之後。

標準來源：

-投資組合策略不清

-依賴不正確的消費者或相對人資訊或在發展訂價和風險接受程度上有不足的損失經驗

-無效地目標市場及風險接受程度運用

-不當地風險評等及分級

-過度注意借款人、相對人或發行者單一事件等所引發可能無法接受的高額損失（如：企業報酬率下降、區域性經濟衰退、流動性危機、過時的技術）

-資產組合對信用環境改變的敏感性（如：價差縮小、流動性變化、房地產價值的波動）

-擔保品不足

-契約條款含糊不清或無拘束力

-逆選擇（因資訊不完整）

-新業務快數成長

-積極的放款或微弱的監督，尤其在微弱的控制環境下

-依賴過時或不適的模型預測資產組合表現

-對資產組合表現未能有效且及時地監督

-法規限制價格水準及彈性，限制資本使用及基金來源等

-無效地催收、改善管理或追索程序

標準控制和減輕因子：

-產品和目標市場與策略和風險偏好一致

-清楚和合適的風險接受標準

-對資金或資本額有合適的負債評等模型和方法

-模型的定期覆審以確認波動性

-監督層級與分層負責架構與業務規模、複雜性及區域性一致

-高度自動的信用系統以杜絕風險接受準則以外的交易發生

-對投資及產品組合有穩定成熟的可預測損失經驗

-經常性的客戶接觸（透過背景調查及清楚的開戶流程）

-精確的交易文件內容

-對投資組合嚴格地監督操作表現

-對因作業環境改變所做的即時、有效反應都能有軌跡或紀錄

-強大的催收、改善管理或追索程序

6.市場風險

定義：市場風險起因於金融市場環境的改變，包括利率、流動性、訂價和匯率，其是可能導致業務未能善盡義務或招致損失。

標準來源：

-複雜的結構式交易

-高槓桿部位

-造市、交易和部位對金融市場的變化敏感

-大額開放部位，尤其是敏感性資產

-以本國貨幣表示的盈餘或資本受美金升值的侵蝕

-缺乏實際成交市場以致難以評價

-投資組合的價值是由二個或更多的獨立變數決定

-流動性或其他資產特性使得在合理損失下難以符合財務上義務

-過度交易操作或微弱監督，尤其在微弱的控制環境下

-避險部位與持有部位未能相互滿足

-資產和負債到期日非預期的不一致

-過度依賴模型預測市場行為

-潛在的市場操縱

-鉅額且複雜的資負表

標準控制和減輕因子：

-每日監督和市場風險限額報告

-精確的操作監督及對引發管理上即時、健全的反應都能有軌跡或紀錄

-清楚的部位限額與充分的市場區隔能具一致性

-場內且風險獨立的風險限額

-市場風險監視與其他市場管理紀律一致

-風險管理系統能追蹤財產目錄和定價，市場變動對投資組合價值的影響建立模型、交易部位是否低於限額

-正確的交易報告

-避險策略與現存部位一致

-穩固的資本額及不同資金來源

-細密的情境計畫和壓力測試，包括核熔分析

-定期對市場行為及統計模型的預測能力有效性作檢測

-監視層級及分層負責架構與業務規模、複雜性及地域性一致

-穩定的經濟環境

7.保險風險

定義：保險風險起因對顧客的生命、財產或行為承保，在價格上不足以彌補預定可能的損失額，所引起公司的財務損失。可能是因為：

-所承接的業務種類並未滿足特定的承保條件

-未能收取一定足夠的貼水以承擔相關風險

-設定不適的承保準則

標準來源：

-承保分類不清或未能與風險偏好一致

-無效地承保分類

-依賴不正確的客戶資訊、不適的損失經驗或不實際的投資假設

-過度依賴過時或不適的模型預測損失

-過度集中注意客戶的地理區域、年紀、職業或其他可能導致大額損失的單一事件。

-逆選擇

-逆處境模式

-財產價值低估

-無效地再保險

-法規限制價格水準和變動性、要求非自願地市場參與、限制投資選擇或資本的使用等

-依賴第三者的擔保人

-無效地選擇、損失預防和控制或挽救、代位程序

標準控制和減輕因子

-清楚定義的營運策略與目標市場、產品供應和目標市場具一致性

-清楚合適地承保風險、偏好分類

-政策應用資訊具獨立性且經認證

-有效地使用再保險，包括充分的風險分類、成本效益分析和確認再保險商長期的財務生存能力

-強大的資訊管理系統和對執行及作業環境精確地監督

-正式地準備金覆審程序

-精算模型預測能力定期的確認有效性

-建立在穩定、成熟的投資組合、產品組合和顧客上有效的預測損失經驗

-能防止超越準則外交易執行的高度有效地自動承保和政策保險系統

-強大的損失預防、索賠處理和再保險收回架構

8.跨國風險

定義：跨國風險起因於一國內情況（事件）乾擾到業務單位從另一國借款人相對人或發行者收受資金的能力，包含貨幣轉換和跨國匯款轉帳風險。

標準來源：

-國家風險評等（Country Risk Ratings,CCR）一班等同的內生風險等級如下：

CCR	內生風險等級

5	高
4	高
3	中
2	低
1	低

CCR 若是有其他的風險來源（如下），評等是可被調整的：

-與觀察名單的國家交易

-交易的國家曾有銀行倒帳或貨幣移轉限制

-未能遵循跨國風險限額或最大授權額度

-跨國交易未有清楚且強有力的契約

-跨國交易未有充分的擔保品

標準控制和減輕因子

-強大的國家風險覆審程序

-精確的國家曝險監督和對引發管理上即時、健全的反應都能有軌跡或紀錄

-清楚的風險曝額與風險分及級具一致性

-以本國貨幣作業

-跨國交易重分配及減輕，包括聯行間的交易淨額

-具強制力、約束力的外部保證或擔保品

9.作業風險

定義：起因於業務有關對客戶提供產品、服務的程序潛在可能的崩潰，並非只是定義在操作和技術上，是會造成顧客抱怨，且未能達到策略目標，具有財務上的損失的。

標準來源：

-不良設計或監視工作流程，造成無法接受的失誤率、作業損失和資源的無效使用

-程序、設施或設備不足支持工作量或複雜性

-以人工交易的量過高

-產品轉換具複雜性

-不良設計、執行或內部控制程序，包括不足的雙重牽制

-對跨多重功能、區域或組織的管理程序不足，造成處理程序有落差

-不足的品質確保程序

-對公司和顧客資產未有充足的保全程序所造成的損害

-由於規定不清楚、不足的作業準則和程序、不足的風險管理、未具流動性、或未能履行契約義務等造成支付系統的錯誤以致結果未如預期

-個人或群體有關的內部或外部交易弱點所引發的舞弊行為

-薄弱的客戶管理功能，包括無效率或未及時地問題解決功能

-客戶抱怨或交易取消率高

-對委外過度依賴或無效率地管理， 包括重要或高風險功能的委外或者是委外並不能達到業務上的要求

標準控制和減輕因子

-穩定、整合性佳的作業程序與內部控制

-程序、設施與業務策略、工作量或複雜性具一致性

-有效地業務永續經營計畫和高水準的員工熟悉管理

-有效的落差管理，包括期間程序覆審和流程分析

-交易人員和檢核人員的控制

-獨立的交易再確認過程

-精確及及時的管理報告紀錄

-強大的監視程序且能有持續性改善的承諾

-強大的品質確保計畫

-充足、有效且可信賴的支付系統

-強大的顧客抱怨解決程序及相關的程序改善

-成功留住客戶的軌跡或紀錄

-強大的資產維護和安全程序

-良好的委外篩選、控制和監視程序

10.系統/技術風險

定義：起因於不足和不善的控制系統及軟體應用。不足的電腦設備或

程式可能干擾或減少自動流程的效率，造成服務中斷、不適的業務決策、過度的作業成本或錯誤。

標準來源：

-系統策略、平台、架構或應用與業務計畫及公司標準間不具一致性

-系統功能不足以達到目標

-複雜的作業及資料庫管理系統和產品

-薄弱的計畫管理

-複雜的遷移或具整合性的整併計劃

-薄弱的計畫或執行管理

-不足的應變管理

-不足的流程管理

-需要高水準的資訊安全

-依賴網路或其它介面

-依賴新興技術

-依賴過時的系統或軟體不再被提供商支援

-不足的資訊技術策略和程序

-不足的測試、備援計劃或程式管理

標準控制和減輕因子

-穩定且整合良好的系統

-設備及應用與業務策略、工作量和複雜性具一致性

-明確、設計良好且有效率的系統架構

-不過度依賴網路或其它介面

-明確的應變管理過程且能伴隨較少的安全破壞程度

-強大的備援計劃或程式管理

-制訂清楚的資訊技術政策與流程

-經常性的對技術應用的合適及效率與否作測試及再確認

- **Risk Levels Materiality**

Low-低度風險是認為這些風險的影響並不會改變公司在主要業務或地區上活動的生存或前景。這並是意謂低風險不值得去控制它，即時它可能只是一個非重要的控制失誤所導致的結果。

Medium-中度風險是認為這些風險的影響會使公司在主要業務或地區上活動的生存或前景有負面影響。這時是需要盡可能及時的更正及採取行動，然而，即時在最糟的情況下，公司在主要業務或地區上活動的生存或前景還不會受到大大的傷害。

High-高度風險是認為這些風險會使公司在主要業務或地區上活動的生存或前景有不可挽回的負面影響，這將撼動公司的市場地位並須耗費成本及面臨挑戰去恢復原狀的。

要給予何種風險是需要靠累積經驗、借用總體事務聯絡人員按其他 ARR 專家來判斷，並沒有其他速成的規則，尤其是遇到未曾遇過

的風險時。

- **綜合風險評等（Composite Risk Rating）**

綜合風險評等係 ARR 在對受檢單位提出一個整體性的風險評估。它是一種專業的判斷，而不是依賴任何數學公式。即使風險組合中只有一 個風險是高的，其他風險都屬低或中度風險，領隊稽核人員也可能在整體考量後給予高風險的綜合風險評等。

參、心得與建議

金融市場的蓬勃發展殿基於健全的金融機構與先進的金融監理，面對金融業務一日千里的創新，各國金融主管機關莫不致力提昇金融監理人員能力，以期在國際金融市場上取得一席之地。本次蒙長官安排至世界知名金融機構研習，心中感激之情難以言喻，研習中不僅獲得第一手之金融新知，亦將台灣金融監理委員會之措施與未來展望分與會人員，雙方交流融洽。為提昇金融監理之效能與加強雙方金融交流建議未來對於此類交流應繼續辦理。另就本次研習內容彙整建議事項如下。

花旗集團的目標是”成為世界上最有聲望的金融服務集團”，為了達成這個目標，花旗列出了五要點之計畫，包括：加強訓練、提升智能及發展、平衡的績效考評、充分溝通及加強控制。其先進的風險導向稽核制度為該集團達成內部控制的主要方式，該項制度建置以來不僅重新調整集團資源配置，也提升集團整體風險管理之水準。整體制度有許多值得目前我國金融機構及主管機關借鏡之處，如：

一、充沛的人力資源及分工：

對受檢單位之查核計畫及實地查核，皆有計畫經理人、領隊稽核、客座稽核人員等多人參與，可對受檢單位之風險進行充分評估，並同時確

保稽核報告之品質。尤其客座稽核人員之參與（通常在一年內會有 400 到 500 個客座稽核人員參與 ARR 查核，與稽核人員比例約 5:5），不僅使 ARR 部門得到專業人才之支援，同時也培養業務部門同仁稽核及風險管理之概念，對於整體營運之提升有莫大助益。另 ARR 部門之領導級人員（如計畫經理人）皆有豐富之金融從業經驗（多爲 15 年以上），對業務及作業流程均可充分掌握。

二、集團內部觀念統合 － 全球合作組：

全球合作組負責整合 ARR 語言，並將某一地區發生的事件及時週知 ARR 部門，讓稽核報告維持全球一致的品質及呈現。如此一來，除可避免對同一事件不一致之表達外，更重要的是讓稽核人員可以瞭解其他地區發生的狀況並預為準備。透過全球資訊的交流，稽核人員不再只瞭解自己所轄地區之業務，更可以擴大視野以全球一致的觀點，來探討稽核事件的輕重及對整個集團的影響。其也確保 ARR 稽核品質的一致性，並特別注意：

1. 風險評估、缺失、報告及評分的全球性一致性

2. 定義、歸類及宣導全球性議案

3. 與業務單位、法令遵循、外部稽核及主管機關維繫關係

三、風險評量表：

風險評量表是花旗集團風險導向稽核制度的核心，透過對風險的

充分掌握以分配有限的稽核資源，以風險評量表決定稽核頻率並作為持續監督計畫之基礎，不僅有效資源配置，同時也提升集團風險管理之能力。為了讓風險評量表發揮最大效用，計畫經理人必須同時注意內部外部環境的變化，隨時更新內容，一旦有新的經濟、金融事件即隨時更新風險評量表內容。

四、業務持續監督：

藉由不間斷的監督程序，稽核部門會為每一個受檢單位都擬訂一份持續監督計畫（Business Monitoring Plan）並按季提出報告，以獲得對受檢單位控制是否有效之最新訊息，瞭解業務部門是否採取適當措施改善內控之缺失且幫助 ARR 找出並瞭解逐漸升高的風險或潛在的議題，俾儘速回應，增進查核效率、焦點及時效。

五、稽核計畫之管理：

針對受檢單位訂定一個全方位的查核計劃，考慮產品、組織架構、業務規模並找出相互關聯及差異點（identify interdependence and gap），量身訂製稽核計畫，並對計畫執行之差異進行分析。其有兩項特點值得借鏡：

1.查核的全性面：

瞭解業務為規劃稽核計劃的第一步，係由（1）法律個體（2）技術環境（3）稽核及法規延革（4）與業務有關之其他組織/部門來進

行瞭解。以風險水準/稽核評等劃分受檢單位，瞭解受檢單位之規模及數目、受檢單位原始資料之正確及可靠性、確認受檢單位之檢查頻率落點及規劃查核時間。

對業務的瞭解將有助於有效查核業務、適當定位受檢單位（是否須為新的業務成立新的受檢單位、現行受檢單位有無分割/合併之必要、查核範圍是否需要增刪等）、說服業務部門並提高稽核部門之聲譽及確認市場、經濟環境及法規變化對業務之影響。

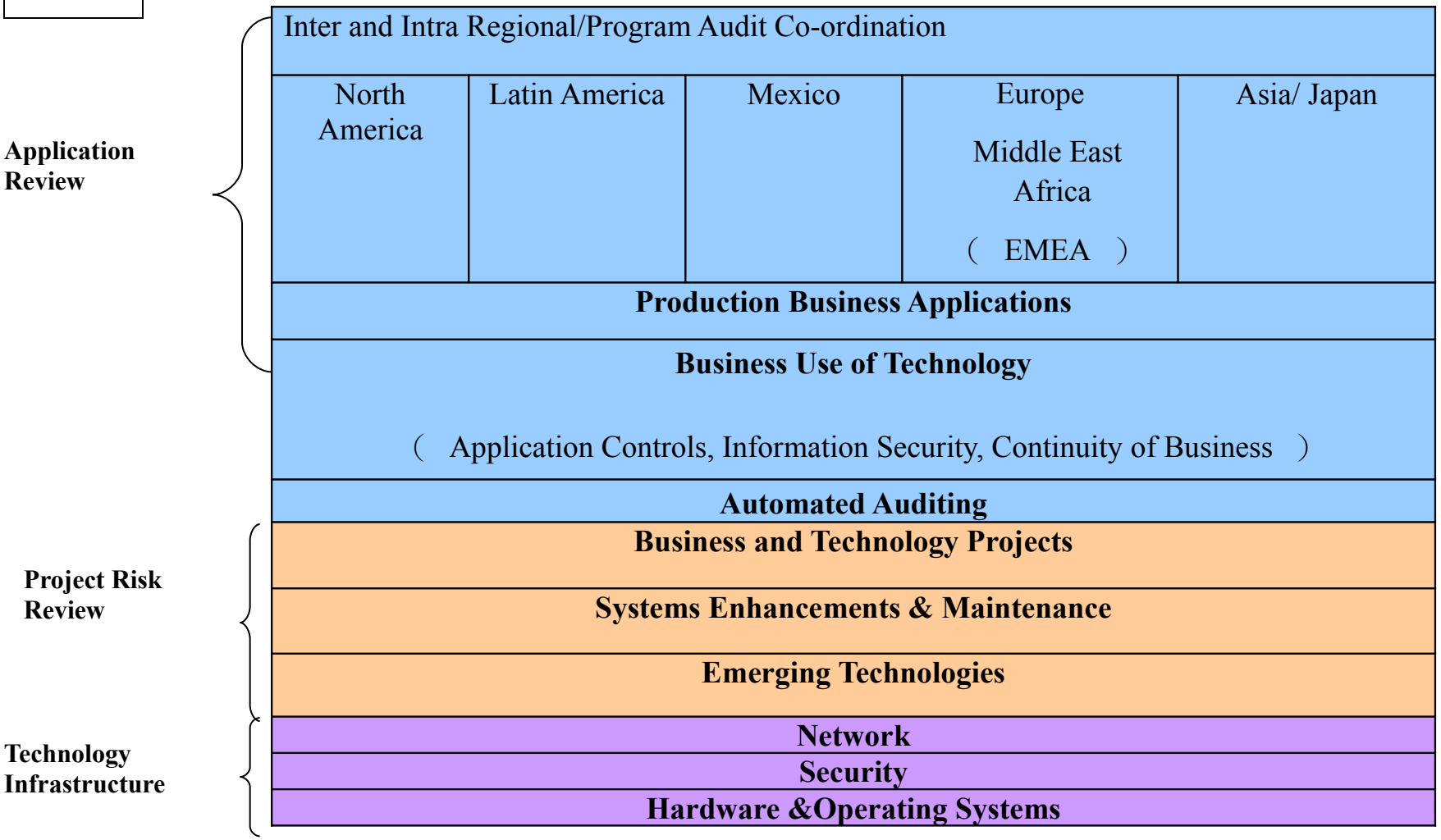
2.查核計劃之規劃：

擬訂查核計劃時考慮（1）在稽核頻率的時限內平均分配工作（2）在考量可用資源及個人發展的情況下規劃查核工作（3）提出需要請客座稽核（Guest Reviewers）協助之專業知能（4）告知業務部門年度稽核計劃（5）將重大業務活動列入（6）在計劃中加入由持續監督得到的訊息（7）與其他稽核團隊協調（借調人力）。

另與原訂查核頻率不同之查核計劃是有可能發生的，隨時能變更查核計劃，與原查核頻率不同之查核計劃必須說明原因，而稽核部門主管及外部稽核、主管機關等特別會把焦點放在高風險受檢單位查核計劃之更動。

附表 1

GlOBAL TECHOLOGY AUDIT CO-ORDINATION



Technology risk is reviewed as part of an integrated audit approach

Project Review Process：Project Risk Scorecard（PRS）

ARR-Project Risk Scorecard				
Project Entity：			**As of date：**	
Description：			**Workdays：**	
Risk Category	**Risk Level**	**weight**	**Risk Score**	**Rationale**
Project Cost Score	Less than $1 MM	10%	0.10	
Strategic Alignment Score	Strong Alignment	10%	0.10	
Business Impact Score		20%	0.30	
Transaction Risk	High transaction volumes/ $ transaction value/ Assets Processed	5%	0.15	
Credit/market Risk	Low	5%	0.05	
Regulatory/ Legal /Reputation Risk	Low	5%	0.10	
Project complexity Score	Medium complexity	20%	0.40	
Business/Project Management Score		20%	0.50	
Business Sponsorship	Strong and Effective Business Sponsorship	5%	0.05	
Project Management Effectiveness	ineffective	15%	0.45	
External Risks		20%	0..60	
Industry Environment Risk	High	5%	0.15	
Economic Environment Risk	High	5%	0.15	
Joint Venture, Partnership and Vendor Risk	High	10%	0.3	
Total weighted Risk Score		100%	2.00	
Composite Risk Rating（H,M,L）			**High**	

Prepared by：		**Date：**	
Approved by：		**Date：**	
Discussed within ARR：		**Date：**	
Last Discussed with line management：		**Date：**	

附表 3

Project Risk Assessment

Project Name ： As entered in Auto Audit

Project Manager （ s ） ： Enter the project manager name （ s ）

Project Description ： Provide a concise project description that gives the reader a clear understanding of the project ； i.e. overall project strategy, objectives, products and services provided. If known, also indicate the target implementation date and estimated overall project costs.

Sponsoring Business ： Enter sponsoring business

AWG Meetings* ： Enter AWG codes from footnote

This project is presently in the phase of** ： Select relevant phase as defined in footnote

As of date ： DD/MM/YYYY

Overall Assessment and Trend*** Some Concerrns **Prior Assessment** ：On Track **Risk Trend** ： Increasing **Date of prior PRA** ： DD/MM/YYYY	**Rationale**： ● In narrative form, explain the rationale for the overall risk assessment so that a reader who is not familiar with the project will clearly understand the related risks and concerns. This text should be suitable for copying directly	**Recommendation/Corrective Action taken**： ● Provide ARR’s recommendation for correcting the project concerns/issues and explain corrective actions satisfactorily completed or pending. For pending CAPs, indicate the scheduled completion date.

	into Audit Work Group materials without editing.	

Key Project Success Factor Assessment and Trend	**Rationale**	**ARR Recommendations/Corrective Action Taken**

Strategic/Franchise Risks	**Rationale：**	**Recommendations/Corrective Action Taken：**
Some Concerns **Risk Trend** ： Decreasing □ Alignment with Citigroup strategy □ Alignment with business strategy □ Alignment with technology architecture □ Ongoing evaluation of business case □ Other	● Explain the rationale for the stated risk assessment and trend. ● Use bullet points to separate multiple concerns and topics. ● For any concerns of issues reported, place an X in the box on the left that best describes the relevant risk factor	● Provide ARR,s recommendation for correcting the stated risks and concerns and explain corrective actions satisfactorily completed or pending. For pending CAP's indicate the scheduled completion date. ● Use bullet points to separate multiple concerns and topics.
Business Risks On Track **Risk Trend** ： Stable □ Project Sponsorship □ Governance □ Active Involvement of all parties □ Resource management □ Other	**Rationale：** ● Explain the rationale for the stated risk assessment and trend. ● Use bullet points to separate multiple concerns and topics. ● For any concerns or issues reported and X in the box on the left that best describes the relevant risk factor.	**Recommendations/Corrective Action Taken：** ● Provide ARR's recommendation for correcting the stated risks and concerns and explain corrective actions satisfactory completion date. ● Use bullet points to separate multiple concerns and topics.

Project Management Risks	**Rationale：**	**Recommendations/Corrective Action Taken：**
At Risk **Risk Trend**：Decreasing □ Project Planning & Overshit □ Risk Management □ Financial Processes □ Software Engineering □ Operational Readiness □ Other	● Explain the rationale for the stated risk assessment and trend. ● Use bullet points to separate multiple concerns and topics. ● For any concerns of issues reported, place and x in the box on the left that best describes the relevant risk factor.	● Provide ARR's recommendation for correcting the stated risks and concerns and explain corrective actions satisfactorily completion date. ● Use bullet points to separate multiple concerns and topics.

Infrastructure & Support Risks	**Rationale：**	**Recommendations/Corrective Action Taken：**
On Track **Risk Trend** ： Stable □ Information Security □ Vendor Mgmt. & Outsourcing □ Legal & Regulatory □ Infrastructure （Data Centers/ Networks ） □ Continuity of Business / Insurance □ Other	● Explain the rationale for the stated risk assessment and trend. ● Use bullet points to separate multiple concerns and topics. ● For any concerns or issues reported, place an x in the box on the left that best describes the relevant risk factor	● Provide ARR's recommendation for correcting the stated risks and concerns and explain corrective actions satisfactorily completed or pending. For pending CAPs, indicate the scheduled completion date. ● Use bullet points to separate multiple concerns and topics.

Prepared by：Responsible Lead Reviewer	**Date**：DD/MM/YYYY
Approved by：Responsible Program Director / Director	**Date**：DD/MM/YYYY
Discussed with line management：Names/ Functional titles of line managers	**Date**：DD/MM/YYYY

*AWG codes ： CIB （ Corporate & Investment Bank ） ,

GC （ Global Consumer ） ,GIM （ Global Investment

Management ） ,INTL （ Citigroup International ） ,O&T （ Global

Operations & Technology and Corporate Infrastructure ）

** The project should be in one of the following six phases ： Initiation,

Definition, Design, Construction, Validation, Implementation.

***Assessments and trends are defined as follows ：

On Track （ Green ） — The project is generally meeting its objectives. Concerns identified have.Satisfactory corrective action plans.

Some Concerns （ Yellow ） — Concerns or project issues identified require corrective action plans.

At Risk （ Red ） — The project is at risk of not meeting key objectives. Significant concerns or issues require immediate management attention and corrective action.