

持續性內部控制與風險評估

莊盛祺 CFE, 舞弊稽核師

台北商業大學會計資訊系兼任講師

兆益數位股份有限公司總經理

David Chuang の觀網
blog.uprofit-tw.com

兆益數位 Uprofit Digital Ltd.,

2

個人簡介

莊盛祺

現任：

台北商業大學會計資訊系
兆益數位股份有限公司
中華民國電腦稽核協會
台灣舞弊防治與鑑識協會(ACFE TW)
中華民國內部稽核協會
台北大龍峒扶輪社理事

兼任講師
總經理
常務理事暨專業發展委員會主委
理事
理事
理事暨資訊委員會主委

歷任：

傑克商業自動化股份有限公司
行政院風險管理研習班講師/風險管理服務團顧問
中華民國電腦稽核協會
安侯建業會計師事務所
友邦信用卡股份有限公司
安麗日用品股份有限公司
眾信聯合會計師事務所

總經理
秘書長
協理
財務經理
財務經理
財務主任

著作：

Arbutus電腦稽核與營運確保分析



兆益數位訊息網 - Uprofit Connection
@UprofitDigital

首頁
服務內容
評論
商店
優惠
相片
影片
貼文
活動
關於
社群
工作機會
Forum

搜尋

瀏覽廣告中心

已讚 追蹤中 分享

發送訊息

20170831 利用系統工作日誌 (System Log)分析存取記錄
170 次觀看 · 2017年8月31日

認識洗錢
89 次觀看 · 2017年8月30日

前後期主檔(Master File)異動資料查核
79 次觀看 · 2017年8月29日

分析資料前的資料整合介紹
61 次觀看 · 2017年8月28日

電腦稽核人才培育
122 次觀看 · 2017年8月25日

安運確保分析
101 次觀看 · 2017年8月24日

應用系統控制下假催核准採購的適當性與合理性
73 次觀看 · 2017年8月23日

查核銀行貸放授權合理性-多檔案資料表關聯與核對
76 次觀看 · 2017年8月22日

相關聯資料聯結與比對差異 Part II
88 次觀看 · 2017年8月21日

淺談政府風險管理與內部控制制度推動成效
105 次觀看 · 2017年8月16日

相關聯資料聯結與比對差異
78 次觀看 · 2017年8月17日

Analytics & Insight - 分析與洞察
131 次觀看 · 2017年8月16日

稽核自動化與持續性稽核
102 次觀看 · 2017年8月15日

介紹Arbutus基本分析功能
13 次觀看 · 2017年6月13日

情

焦點



討論議題

- 一. 風險思維(Risk-Based Thinking)
- 二. 數位化的挑戰和機會
- 三. 持續性控制與風險評估發展模式
- 四. 導入持續性稽核與監控作業的成功要素

風險思維 (Risk-Based Thinking)



ISO 9001 : 2015 其中兩大核心變化：

- 提出「風險思維 (Risk-based thinking) 」在過程方法 (Process approach)中的應用。
- 領導力 (Leadership) 取代了管理 (Management) ，前者注重行為(Behavior) ，後者注重流程 (Process) 。

建立以風險為基礎的方法，能消弭組織以往被動的預防措施，取而代之的是前瞻性的眼光及積極的行為：以「預先行動來改變」 (Proactive) 替代「對變化作出的被動反應」 (Reactive) ，在以風險為基礎的管理系統中，建立的預防措施將自動觸發。

參考擷錄自ISO顧問職人網頁: <https://isoleader.blogspot.com/2016/08/iso-90012015risk-based-thinking.html>

企業永續經營的目標



Enterprise Risk Management Framework: Integrating with Strategy and Performance

ENTERPRISE RISK MANAGEMENT



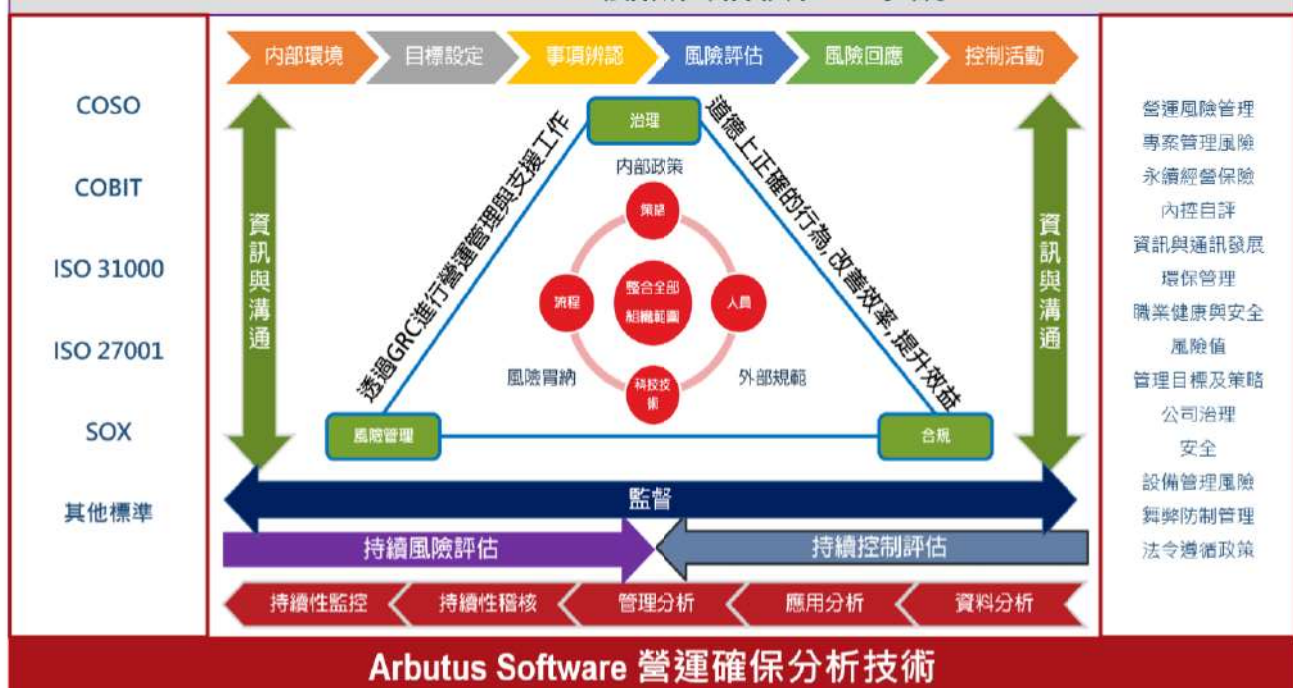
20 key principles within each of the five components

擷取自The Committee of Sponsoring Organizations of the Treadway Commission

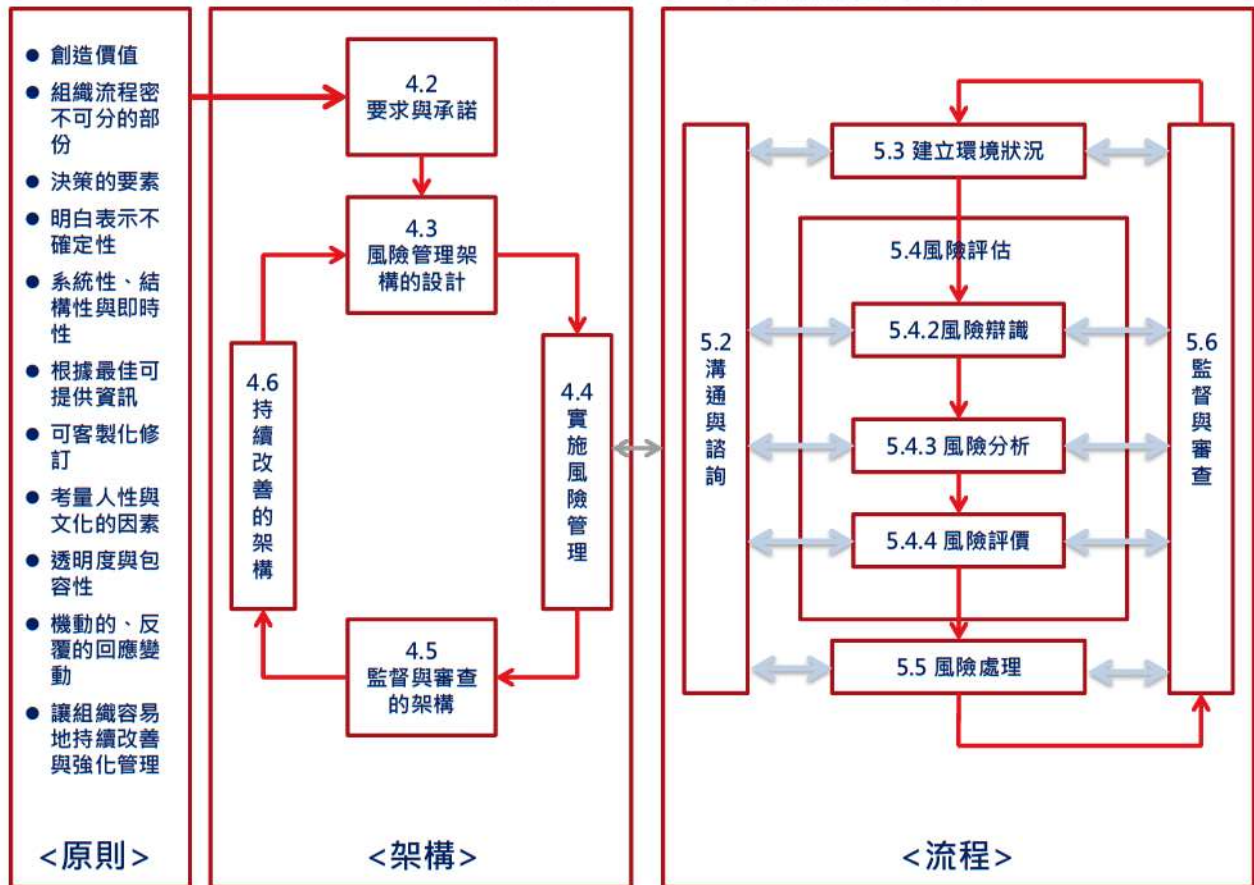
治理、風險管理、合規性及營運確保科技解決方案

eGRC & Business Assurance Technology Solution

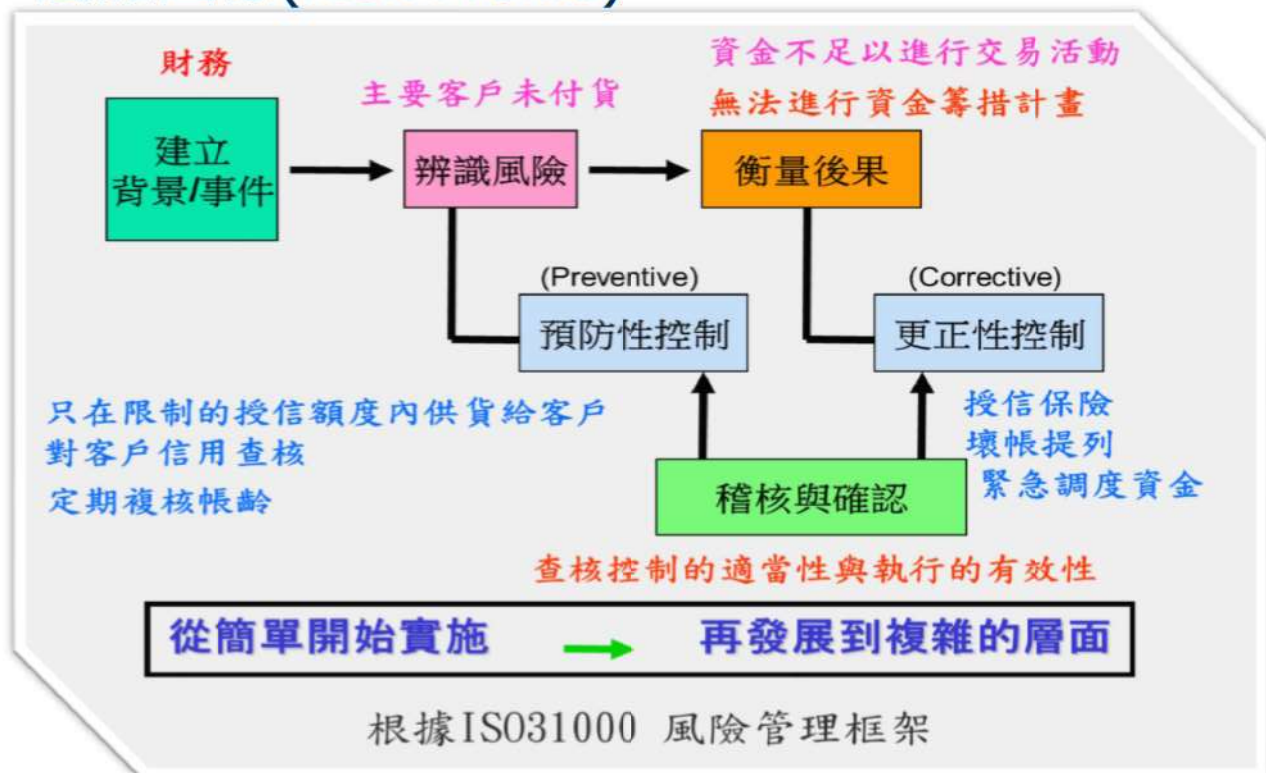
Pentana Vision 風險與稽核管理系統



ISO31000:2009風險管理原則、架構和流程關係圖



風險圖像(Risk Profile)



風險評估-Risk Assessment

風險背景

標識風險

風險背景

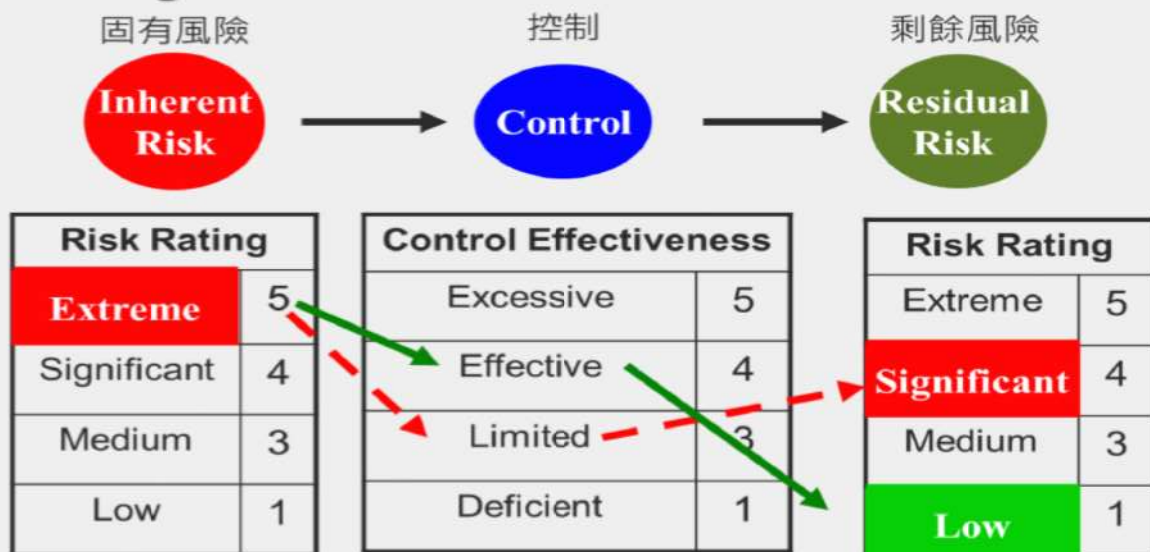
固有風險評估

後果影響

The screenshot displays the KnowRisk Enterprise software interface. The left sidebar shows a tree view of risk profiles. The main window is divided into several sections: 'Risk Profiles' (listing various risk categories like '02. 選辦會96年度風險'), 'Profile Risks' (showing a table of risks with columns for 'Risk Rating', 'Control Effectiveness', and 'Residual Risk'), and 'Profile Consequences (Impacts)' (showing a table of consequences for specific risks). Red arrows point from the labels to the corresponding sections in the software interface.

風險評估主要概念

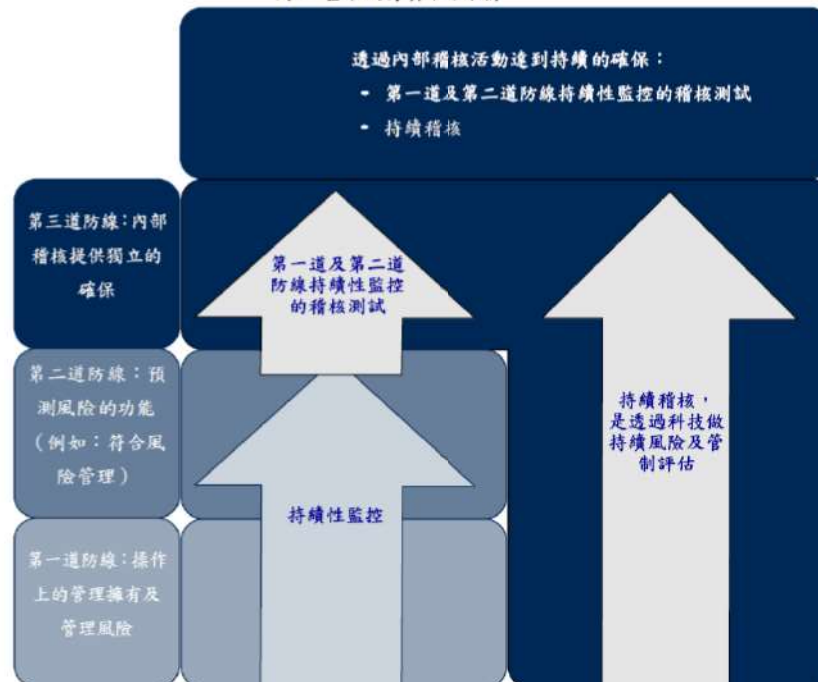
Moving focus from inherent to residual levels





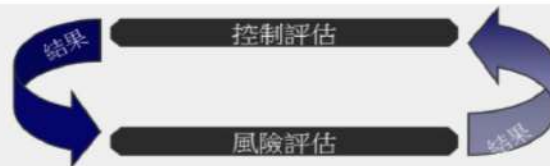
持續性稽核、監控與確保架構

圖1、基本的持續確保架構



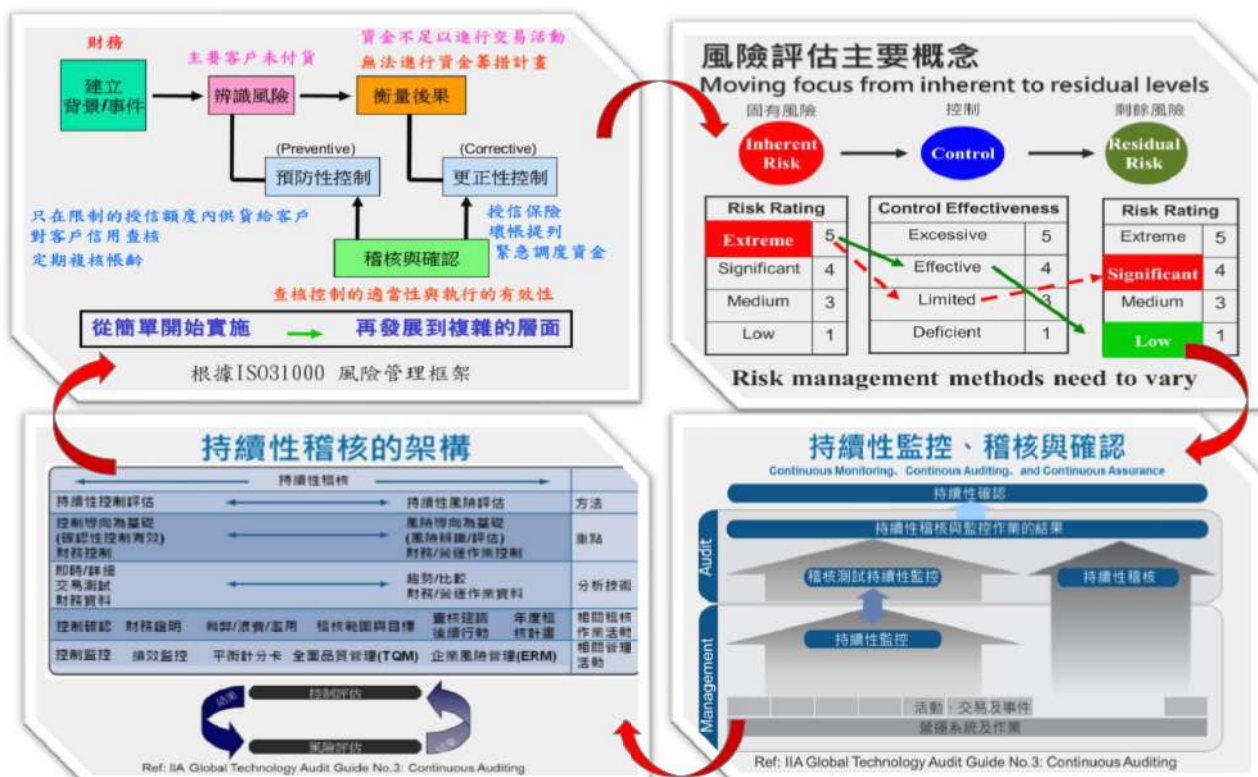
持續性稽核的架構

持續性稽核						
持續性控制評估				持續性風險評估		方法
控制導向為基礎 (確認性控制有效) 財務控制				風險導向為基礎 (風險辨識/評估) 財務/營運作業控制		重點
即時/詳細 交易測試 財務資料				趨勢/比較 財務/營運作業資料		分析技術
控制確認	財務證明	舞弊/浪費/濫用	稽核範圍與目標	查核建議 後續行動	年度稽核計畫	相關稽核 作業活動
控制監控	績效監控	平衡計分卡	全面品質管理(TQM)	企業風險管理(ERM)		相關管理 活動

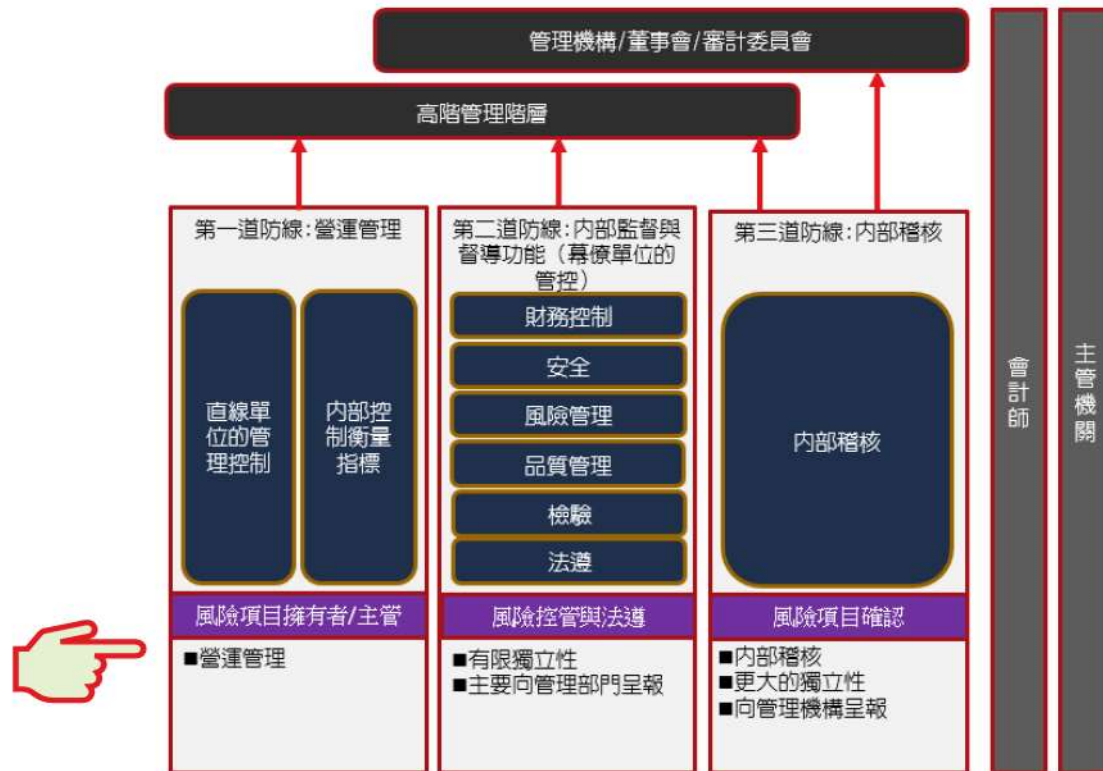


Ref: IIA Global Technology Audit Guide No.3: Continuous Auditing

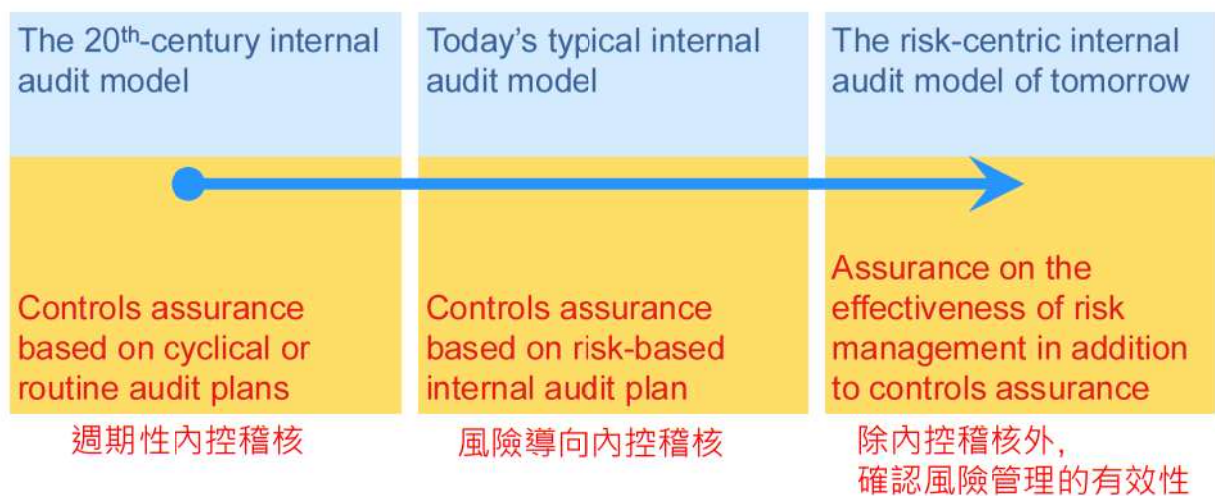
風險管理方法 – 以風險為導向的內部控制與稽核作業



有效風險管理與內部控制三道防線

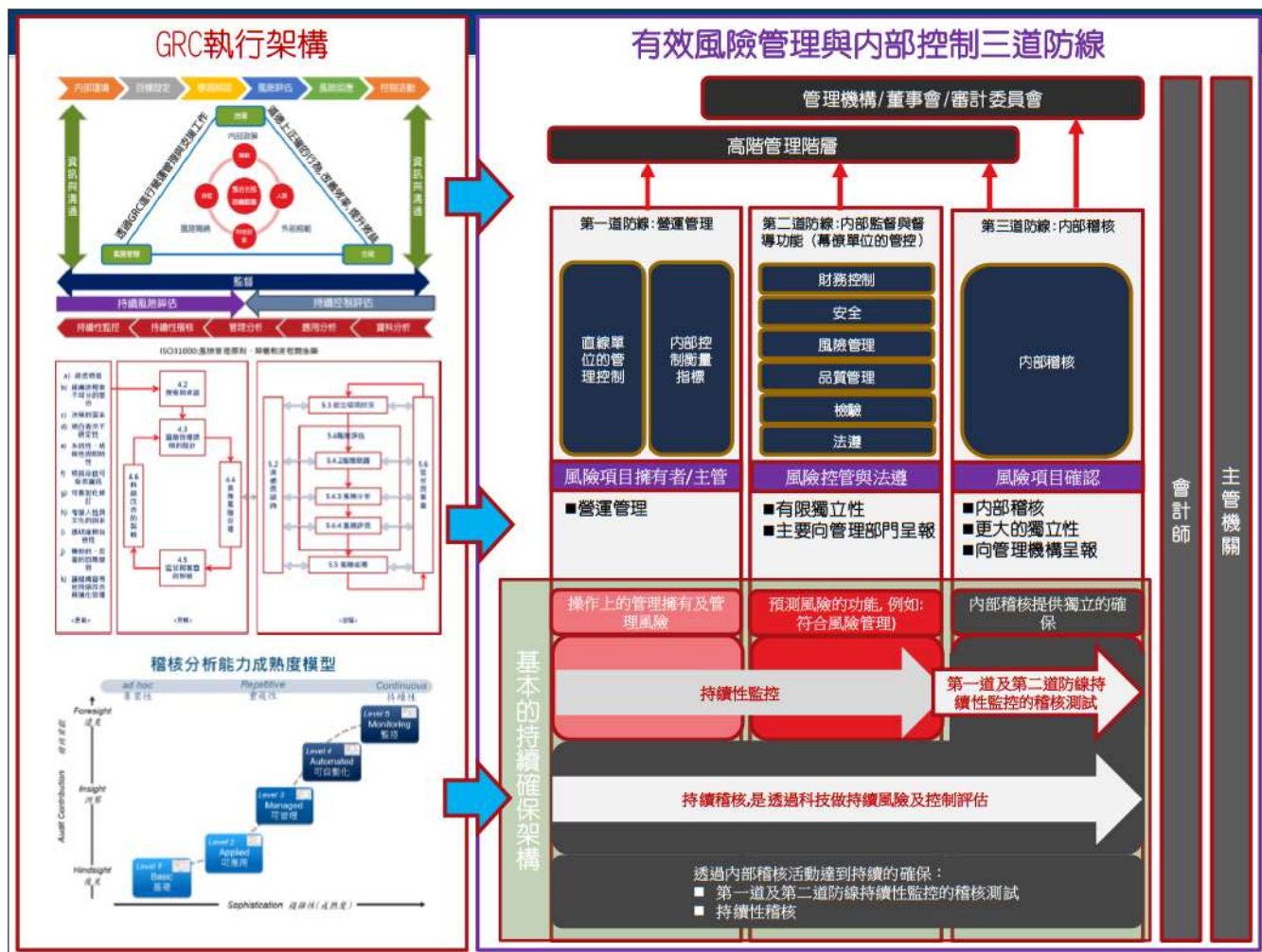


內部稽核焦點的轉變



Adapted from PricewaterhouseCoopers Advisory Services, "Internal Audit 2012," © 2007

PRICEWATERHOUSECOOPERS 



稽核數位化的挑戰與機會

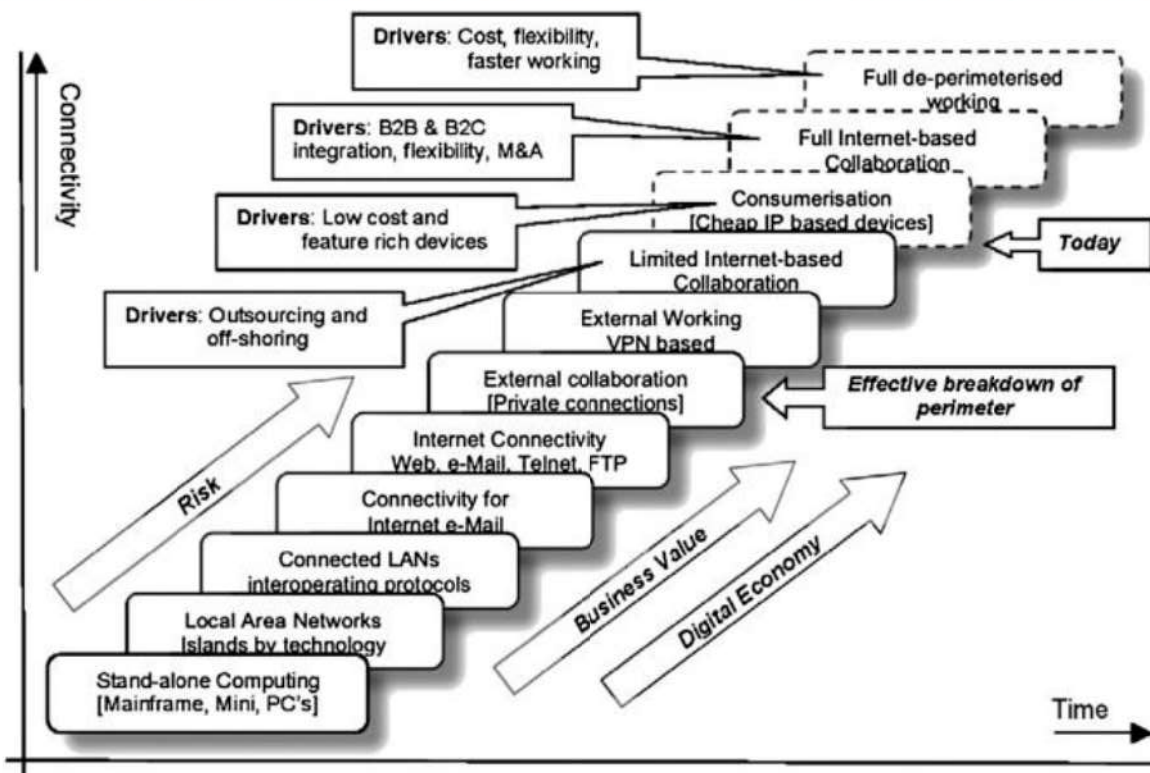


近二十年全球數位化演進時間序

Timeline: Influence of digital on the mainstream



數位經濟與商業價值的轉變 → 風險也逐漸增加



確認性工作的未來 The Future of Assurance

- 技術進步從根本上改變了稽核的性質，稽核人員如何利用最新技術來增強他們**分析資訊**的方式？
- 建構能夠在多重營運作業流程和產業中，提供高品質查核證據和有價值營運洞察力的分析模型並非易事，我們致力應對這些挑戰，以**提供高品質及有價值的查核**。



參考EY-UK Publication: The Future of Assurance, How technology is transforming the audit

Assurance

*Assurance is **necessary** and **sufficient** evidence that information (or **information systems** and **technology**) meet their recipients' (or their users') **knowledge** (or **belief, trust** or **confidence**) requirements in support of **rational action** in one or more **specific contexts**.*

(Will and Whobrey 2003)

『確認』是指資訊能夠符合其接受者（或其使用者）的知識（或信仰、信任或信心）需求，以支援在一或多個特定背景中之合理行為的充份必要證明。

內部稽核的機會



改變的速度和數據的激增為內部稽核創造了新的機會，增加有價值的洞察及見解。

利益關係人對強化洞察的新方式持開放態度。

內部稽核正在尋求建立自己的技能，以便在這個新世界中更有效率地工作，並為組織確保未來的價值。

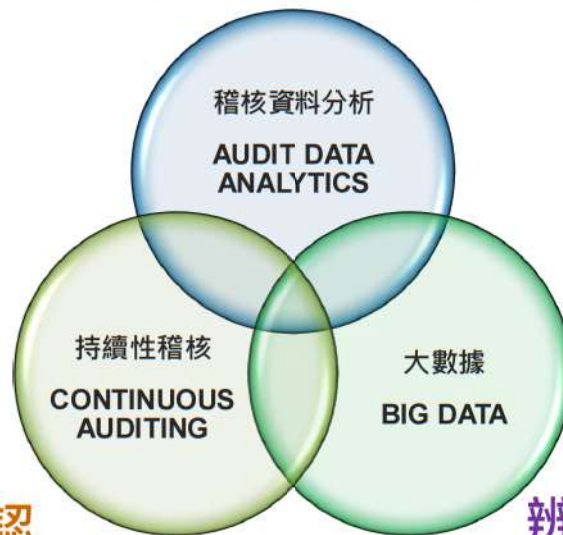
數位化稽核 vs 稽核數位化



圖片擷取參考自<https://www.vozax.com/app-development-strategy/>

轉型中的稽核作業

有效查核與舞弊偵測



持續性確認

辨別多種行為

持續性控制與風險評估發展模式

David Chuang 的觀網
blog.uprofit-tw.com

基本的持續確認架構

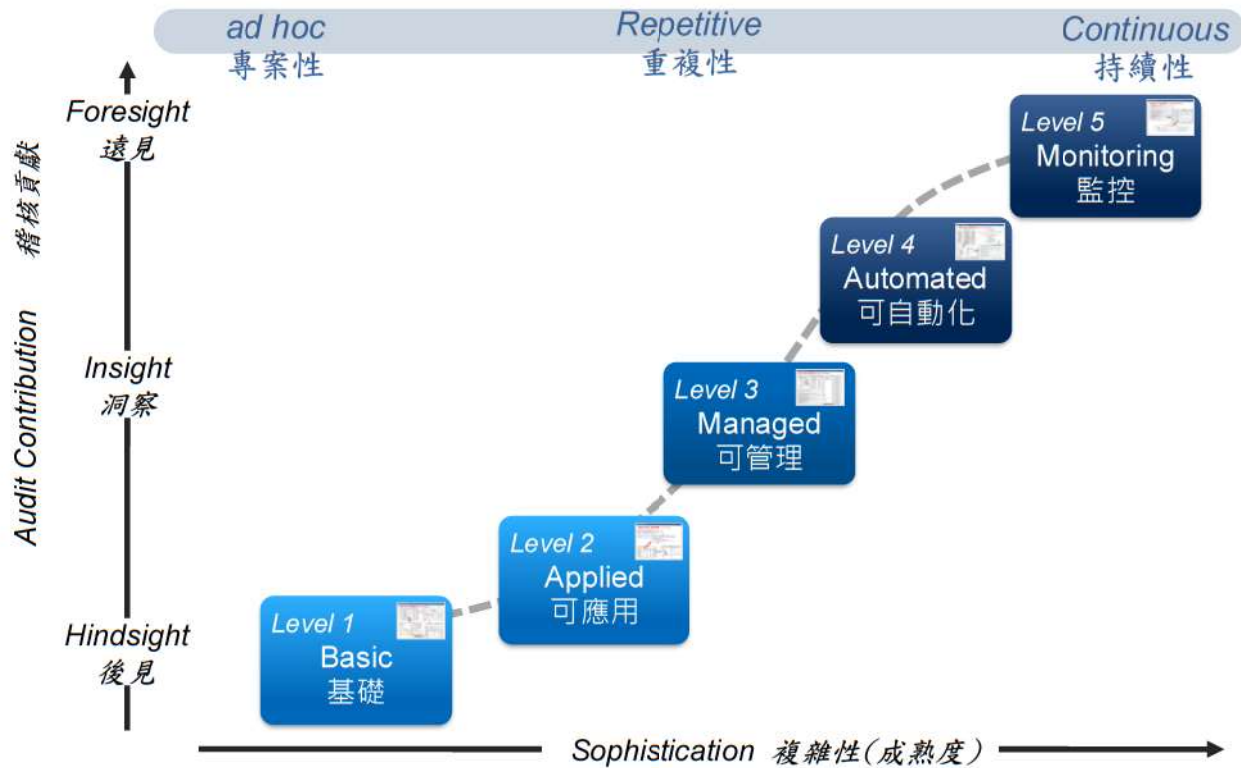


持續性稽核的架構

持續性稽核						
← 持續性控制評估			→ 持續性風險評估			方法
控制導向為基礎 (確認性控制有效) 財務控制			風險導向為基礎 (風險辨識/評估) 財務/營運作業控制			重點
即時/詳細 交易測試 財務資料			趨勢/比較 財務/營運作業資料			分析技術
控制確認	財務證明	舞弊/浪費/濫用	稽核範圍與目標	查核建議 後續行動	年度稽核計畫	相關稽核作業活動
控制監控	績效監控	平衡計分卡	全面品質管理(TQM)	企業風險管理(ERM)		相關管理活動



稽核分析能力成熟度模型



我們現在的『稽核分析能力』在哪裡？

Analytics & Insights

Unlocks the power of your data

我們十力展現

- 稽核分析能力(一) - 知道查核價值的能力
- 稽核分析能力(二) - 知道選定查核目標範圍的能力
- 稽核分析能力(三) - 知道取得資料源的能力
- 稽核分析能力(四) - 知道搜尋與推演資料的能力
- 稽核分析能力(五) - 知道驗證資料完整性的能力
- 稽核分析能力(六) - 知道如何匯整資料的能力
- 稽核分析能力(七) - 知道找出異常態樣資料的能力
- 稽核分析能力(八) - 知道多檔案資料分析比對能力
- 稽核分析能力(九) - 知道匯出檔案及報表的能力
- 稽核分析能力(十) - 知道整合分析策略的能力

稽核分析能力(一) - 知道查核價值的能力

傳統稽核

- 依據既有的控制事項表進行年度查核
- 著重表報隨機抽核(比較表面)
- 人工檢驗表單簽核為主
- 對查核結論的效果有限

現代稽核

- 以為風險基礎的控制項查核
- 著重100%交易資料查核(兼具廣度與深度)
- 以系統作業為基礎的查核
- 查核結論較具體

銷售及收款循環

可能風險	控制種類/重點	查核程序
1-1. 當客戶具有信用額度問題時，仍對其供貨	1. 系統設定凍結信用額度超限之客戶，以免進行進一步的訂單處理	1. 驗證是否客戶信用額度超限，系統即予以凍結，而無法進行訂單作業 2. 評估後續解除凍結之程序是否適當

稽核分析能力(二) – 知道選定查核目標範圍的能力

查核議題	PBC List清單	資料期間
議題1. 驗證付款與發票金額的一致性, 以確保付款交易的準確性和有效性。(標準元件) 控制重點： A. 支票付款總額是否與應付憑單、應付帳款及付款傳票總額一致？ B. 付款天數是否合乎付款規定？ C. 付款對象是否為進貨的供應商？ D. 入帳及付款是否經適當核准？ E. 傳票日期是否有不合理之現象？	參考資料來源： A. 應付憑單檔 B. 應付帳款傳票檔 C. 付款傳票檔 D. 支票or電匯單檔	半年

資料正確性與可靠性 – Data Integrity

- 資料完整性(Data Integrity)就是資料表(Table)包括：
 - 沒有中斷的資料或錯誤的欄位定義 ➤ [Verify](#)
 - » No corrupt data or erroneous field definitions
 - 只有有效的日期 ➤ [Verify](#)
 - » Only validity dates
 - 數值加總和控制數一致 ➤ [Count, Total, & Statistics](#)
 - » Numeric totals that reconcile to controls
 - 遺漏項目 ➤ [Gap](#)
 - » Missing Item or records
 - 只有唯一記錄 ➤ [Duplicate](#) Fuzzy Duplicate([Near](#), [Similar](#))
 - » Only unique records
 - 所有資料及這些都只是你需要的資料 ➤ [Other\(Classify, Filter\)](#)
 - » All the data and only the data you requested
 - 演算欄位包含正確數值 ➤ [Other\(Computed Field, Filter\)](#)
 - » Calculated fields that contain correct values
 - 欄位中的資料符合預期 ➤ [Other\(Classify, Join, Filter\)](#)
 - » Data in fields where it is expected
 - 欄位間的關係是一致的及有邏輯的 ➤ Other(Filter, Classify, Join, ...)
 - » Field relationships that are consistent and logical
 - 資料看起來是合理的 ➤ Other(Filter, Classify, Join, ...)
 - » Data that looks reasonable

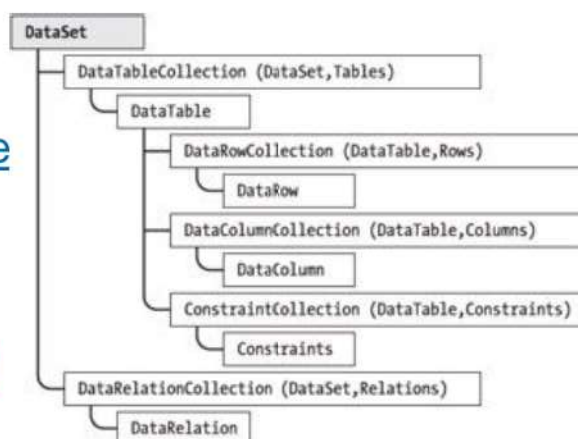
建立資料集(Data Set) – 檢視(View)/查詢(Enquiry)

依不同維度單一或多階層進行分類、分層、分期彙總

- [Classify](#)
- [Summarize](#)
- [CrossTabulate](#)
- [Stratify](#)
- [Age](#)

合併與關聯資料

- [Join](#)
- [Merge](#)
- [Extract Append](#)
- [Relate Table](#)



約束/篩選範圍

- [Filter](#)
- [IF](#)
- [Smart Search](#)

演算欄位

- [Computed Field](#)

資料分割與匯出

- [Extract](#)
- [Export](#)

資料排列優先次序

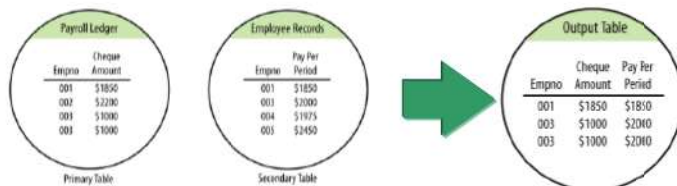
- [Sort](#)
- [Index](#)

資料分析與測試

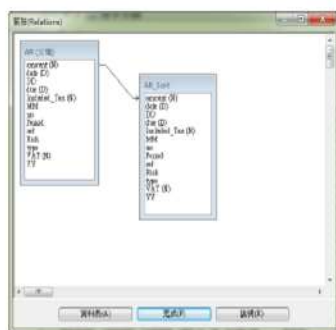
Data Analysis Cycle –Data Analysis

合併比較與聯結

聯結比對/Join



關聯/Relation

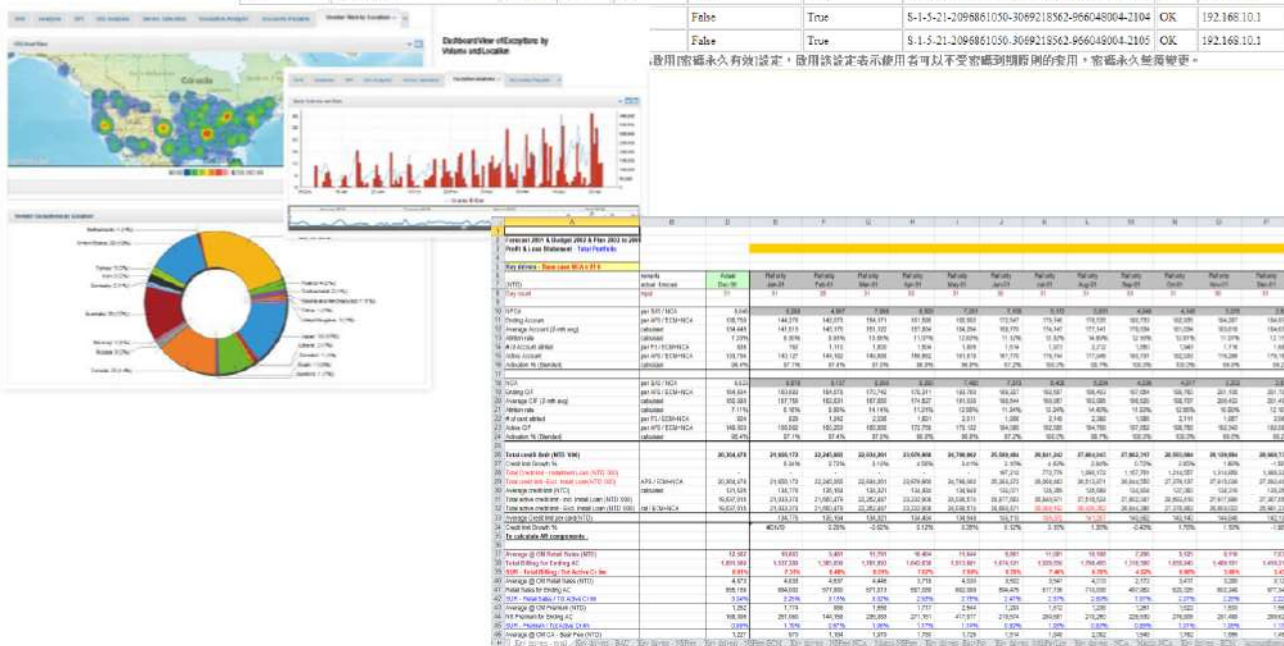


分析、監控、報告和及時回應

報告名稱(Report Title): DOMAIN USERS PASSWORD EXPIRY INFORMATION
報告說明(Report Description): 此報告列出所有有效期限的網域主控站(Domain Controller)使用者帳戶
報告日期(Report Date): 2011/03/28 下午 02:26

PasswordExpires	Description	Domain	Name	LocalAccount	PasswordChangeable	PasswordRequired	SID	Status	ServerIP Address
False	專家服務器訪問	UPROFIT	ntls	False	True	True	S-1-5-21-209681030-3069218362-866048004-1113	OK	192.168.10.1
False	專家服務器訪問	UPROFIT	porty	False	True	True	S-1-5-21-209681030-3069218362-866048004-1117	OK	192.168.10.1
False	專家服務器訪問	UPROFIT	etc	False	True	True	S-1-5-21-209681030-3069218362-866048004-1118	OK	192.168.10.1
False	專家服務器訪問	UPROFIT	etc	False	True	True	S-1-5-21-209681030-3069218362-866048004-2104	OK	192.168.10.1
False	專家服務器訪問	UPROFIT	etc	False	True	True	S-1-5-21-209681030-3069218362-866048004-2105	OK	192.168.10.1

啟用密碼永久有效設定，啟用該設定表示使用者可以不受密碼到期限制的使用，密碼永久無變更。

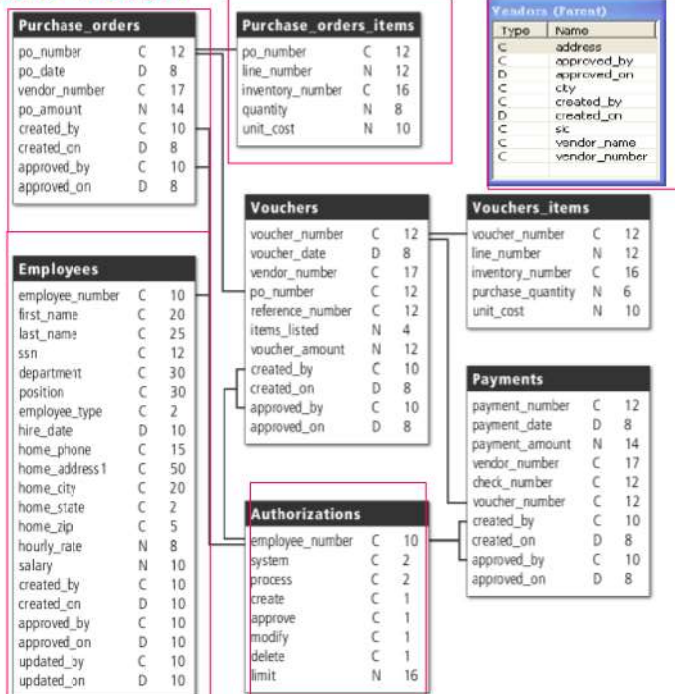


整合分析策略

查核測試是否有拆單分割採購之情形？

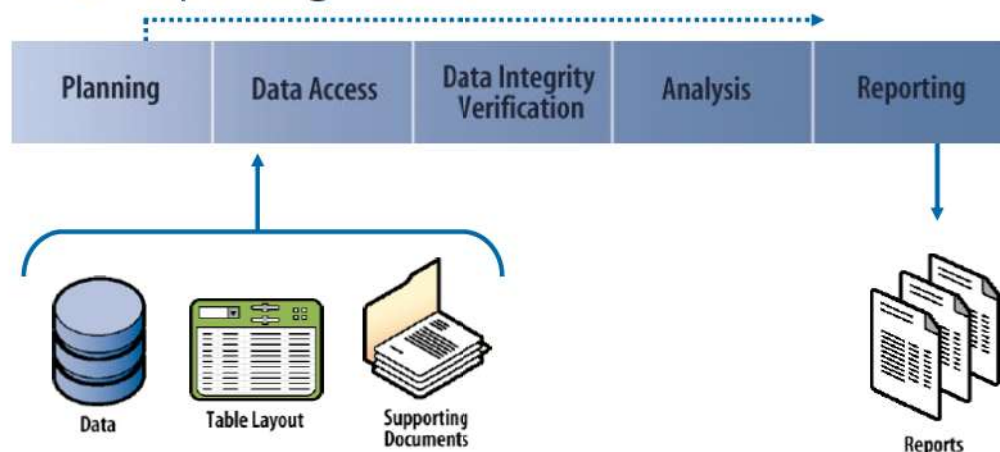
1. 開啟purchase_orders資料表，利用Duplicate指令，將廠商有一筆以上的交易挑選至另一個新資料表。
2. 在新表中，利用Sort指令，依廠商代號及採購日期排序，產生新表。
3. 設立新演算欄位計算同一個廠商與上一次交易的日期天數。
4. 篩選出相隔30天以內，利用Summarize指令，依照廠商別彙總產生新表。
5. 測試是否超過採購授權限額
6. 輸出查核報告

<http://blog.uprofit-tw.com/?p=4625>



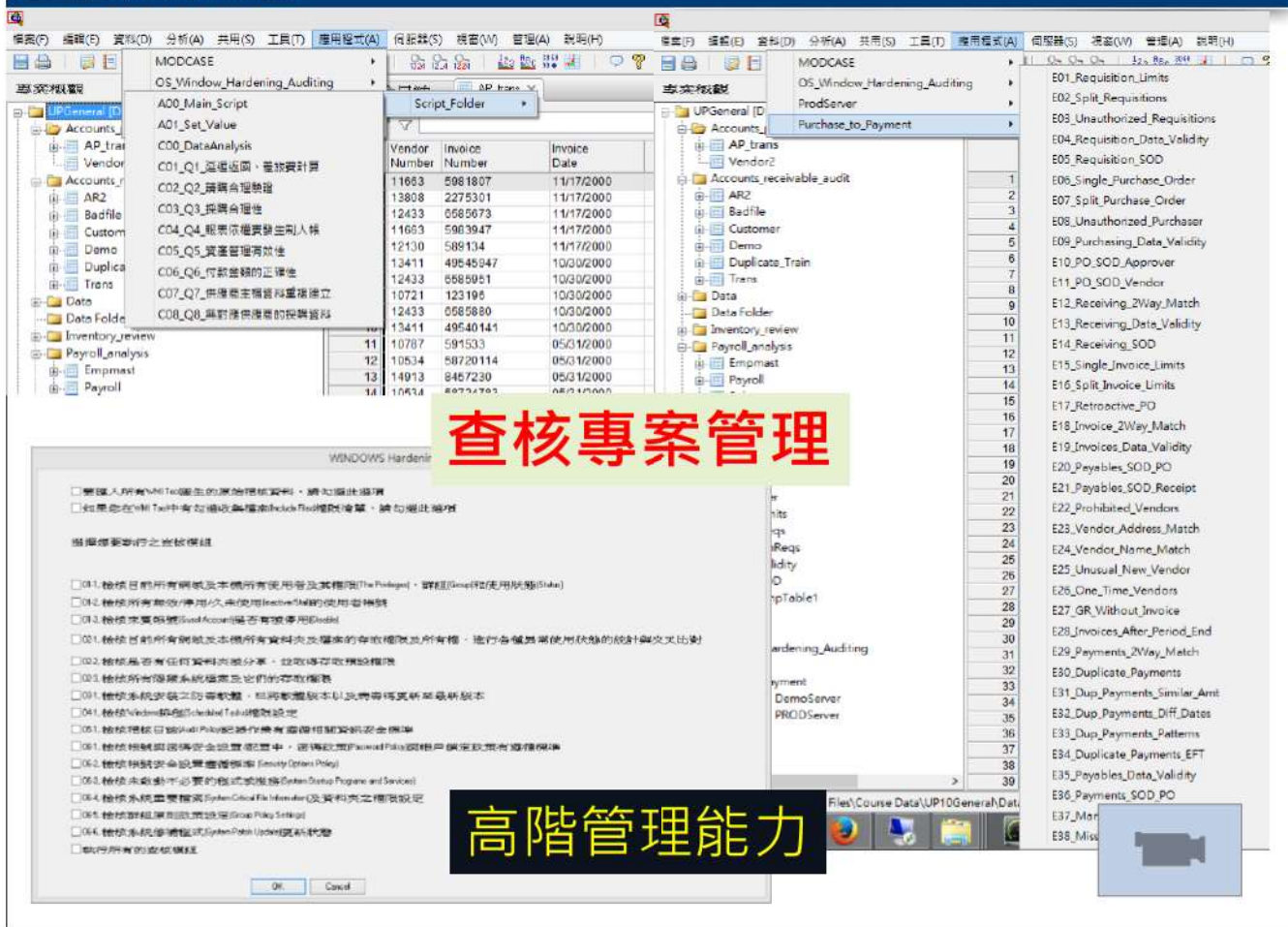
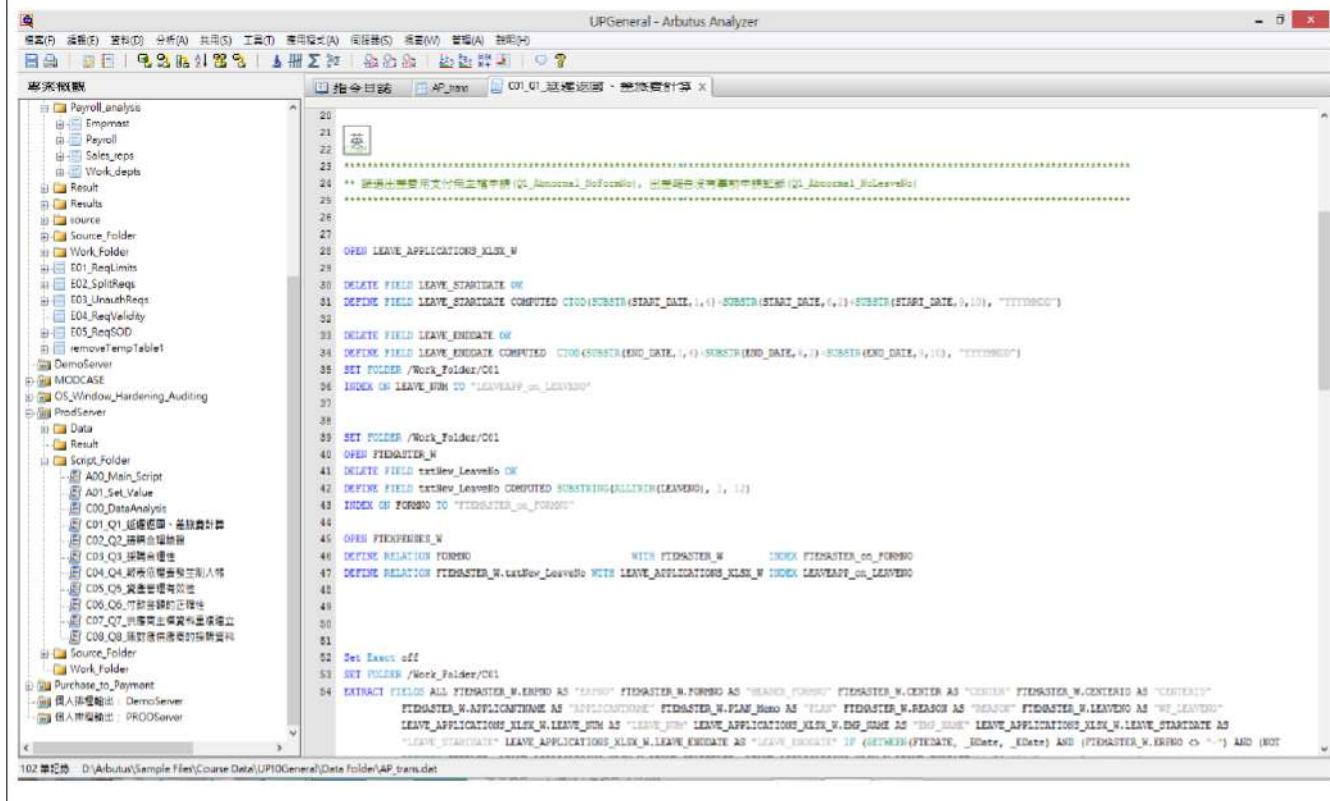
資料分析循環(The Data Analysis Cycle)

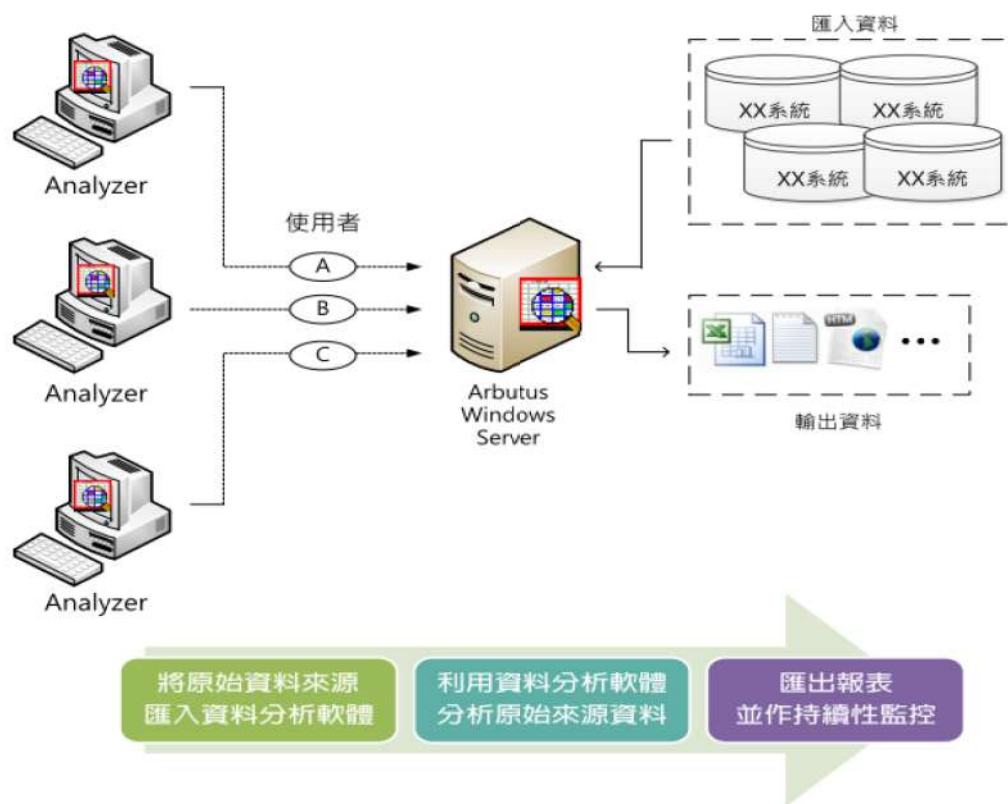
- 規劃(Planning)
- 資料存取(Data access)
- 資料完整性驗證(Data integrity verification)
- 資料分析(Data analysis)
- 查核報告(Reporting results)



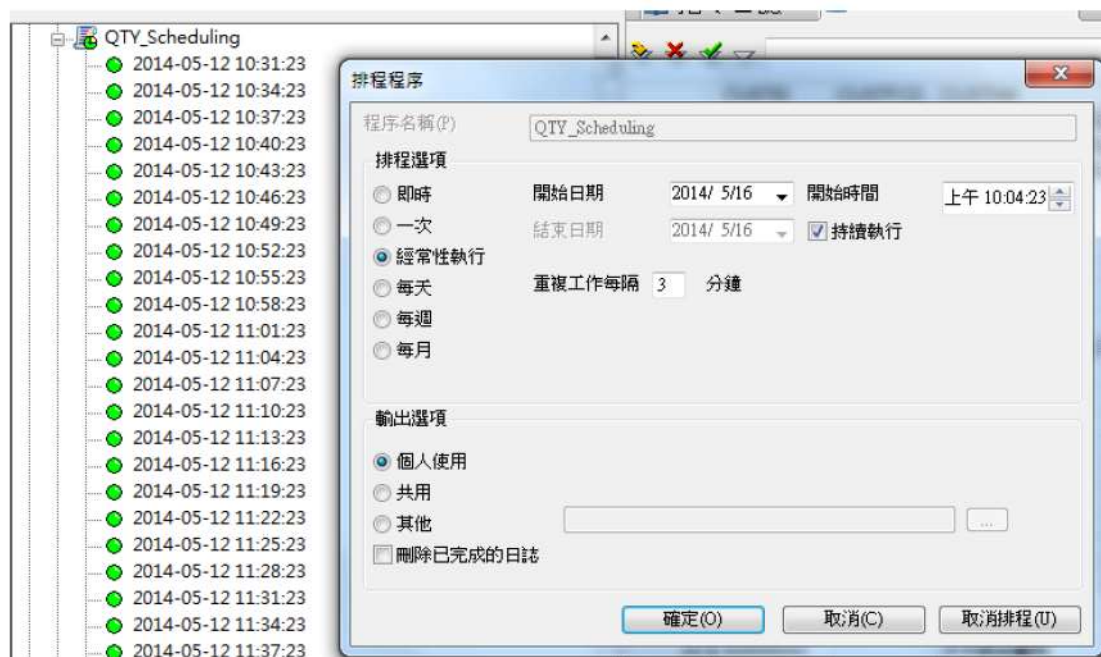
稽核程式自動化/Procedure

進階技術能力





資料排程(Scheduling)



系統及資料安全

- Arbutus 稽核查核資料管理系統可以將稽核所需之查核資料集中於統一的伺服器平台，而在進行資料傳輸時，均有對傳輸的資料進行加密。
- 與 Windows Active Directory、Local Account 整合，不需要從外部設定權限，控管方便、管理容易
- 簡易的安裝介面及操作介面，能大幅降低管理複雜度與成本。
- Analyzer 單一軟體介面的方式去存取專案所有資料。相同的操作環境，便於使用者登入操作，並可讓新進人員快速熟悉操作環境。

持續性控制評估



評估基準條件的控制項目(仍然在使用中並且功能有效)
及對後續的變更進行評量，
考量自動控制、資訊一般控制、及人工控制相互間的關係

持續性監控

- 目的：考慮營運目標及關鍵性的成功要素。
- 風險：辨別可能阻礙組織成功的障礙。
- 回應：配合不同來源的資料，來發現及確認新的風險。例如：可重新設定的條件、變更、事件登錄，財務交易及非結構性資料。
- 時機：即時偵測控制問題。。
- 行動(方案)：追蹤控制缺失改善行動。

持續性監控、稽核與確認之關係

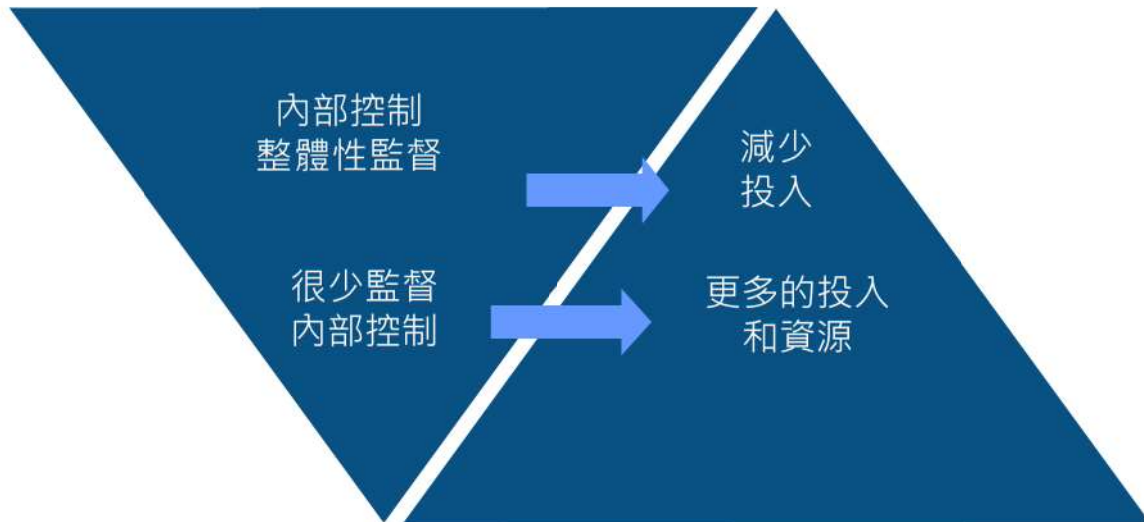
Continuous Monitoring、Continuous Auditing、and Continuous Assurance

- 持續性稽核(Continuous Auditing)
 - 此方法被使用來以連續性的基礎進行稽核相關的作業活動 - 包括控制與風險評估
 - 由內部稽核來執行(第三道防線)
- 持續性監控(Continuous Monitoring)
 - 去確保政策與程序有效運行的作業，且評估控制的妥適性及有效性。
 - 由營運作業／財務管理人員執行(第一道及第二道防線)；稽核是去獨立評估管理作業活動的適當性。(第三道防線)
- 持續性確認(Continuous Assurance)
 - 結合持續性稽核與監控的執行成效

持續性稽核與監控工作投入關係

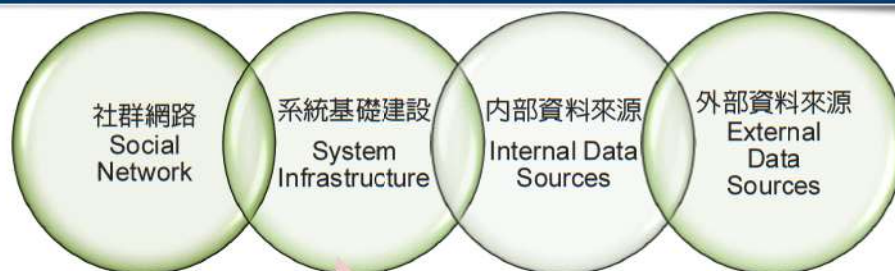
Continuous Monitoring、Continuous Auditing、and Continuous Assurance

管理階層的第一道及第二道防線
持續性監控工作的投入



內部稽核的第三道防線持續性稽核工作的投入

資訊來源
Information
Sources



擷取, 轉換,
和載入
ETL

擷取

轉換

載入



分析方案
Analytics
Solutions

海量資料(BIG DATA)



要求洞察
Required
Insights

報表和儀表板
Report &
Dashboards

Browser



EIP

EIS

決策者



導入持續性稽核與監控作業的成功要素



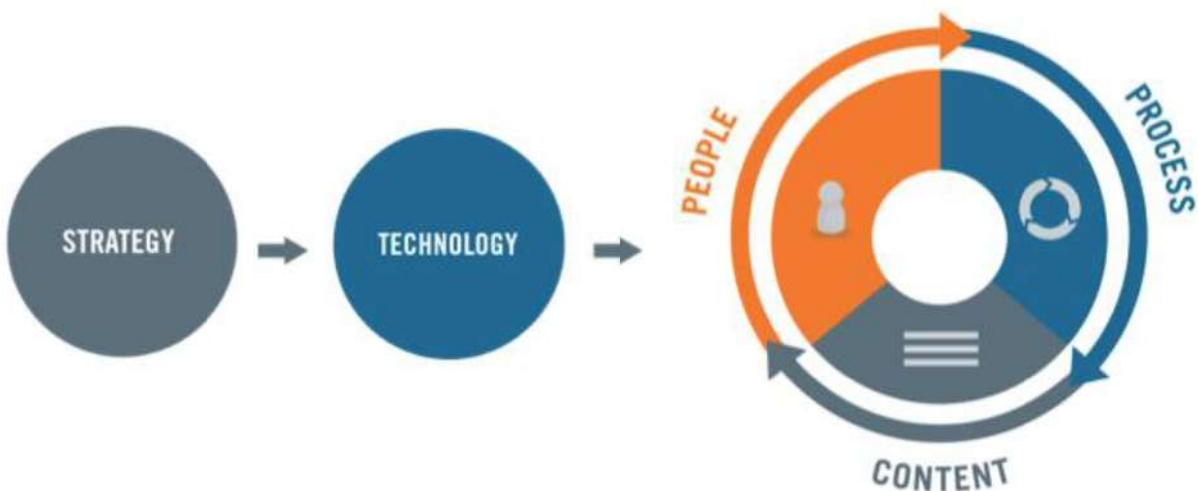
持續性確認的角色及責任

角色	責任
內部稽核主管 (CAE)	- 經由確保內部稽核人員的能力和工具的足夠性，資料安全的安排及預算為持續性稽核作業建立其公信力。 - 教育內部稽核人員、資深管理人員及董事會有關內部稽核作業及管理當局的角色及責任。 - 規劃要做多年的策略以取得利害關係人更多的支持。 - 溝通內部稽核對持續性監控有效性評估的結果。
內部稽核（第三道防線）	- 聯結第一道及第二道防線規劃持續性稽核 - 執行持續性稽核： □ 與企業聲明主張及營運目標連結有關的分析。 □ 配合風險因素及控制活動。 □ 如同可信賴的顧問，透過評估新的企業風險，增加其稽核的價值。 - 執行持續性監控的稽核測試。 - 聯結稽核目標，例如完整性、正確性及安全性等，提供持續確認作業。 - 維護有效的資料安全準備工作。
營運主管（第一及第二道防線）	- 設計與執行持續性監控來評估風險管理及控制的適當性及有效性。 - 提供在風險上流程的專業意見與回應。發展與執行管理方案來解決問題發生的原因。 - 縮短管理行動的時間。

需求目標的明確



持續性稽核實行步驟與關鍵要素





Technology for GRC & Business Assurance

祝福大家
有個美好的一天!
謝謝!

11070 台北市信義區基隆路一段141號9樓之8

TEL:02-27601798 FAX:02-27601797

Mobile phone: 0937054999

E-mail: david_chuang@uprofit-tw.com

Web Site: www.uprofit-tw.com

Facebook 專頁: david.sc.chuang

Facebook 粉絲專頁:

兆益數位訊息網 - <https://www.facebook.com/UprofitDigital>

大衛營 Uprofit Connection - <https://www.facebook.com/Uprofit.Connection>

兆益電腦稽核論壇 - <https://www.facebook.com/UprofitForum>

全國大專院校電腦稽核個案競賽暨專題研討會 - <https://www.facebook.com/ACLAward>

David Chuang の觀網
blog.uprofit-tw.com