

從遠銀遭駭事件看有效的風險管理作業 與內部控制三道防線

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 的觀網
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)

兼任講師

總經理

常務理事暨專業發展委員會主任委員

理事暨會員發展與服務委員會主任委員

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





遠東銀行遭駭盜轉18億元案發至今，雖然超過9成9的款項都已追回，但對企業IT部門、銀行CIO或資安圈而言，更重要的是找出駭客入侵銀行的手法，才能從中學到教訓，避免自己成為下一家的受害企業。但是，駭客如何入侵遠銀的細節，刑事警察局還沒有透露更多細節，而臺灣參與調查的資安公司也因保密協定，而拒絕透露更多處理過程。

倒是，國外資安公司McAfee剛在台灣銀行搶案中的角色分析，

在台灣銀行搶案中的角色分析，從程式碼中進一步入侵SWIFT系統的關鍵之一。發表這篇分析的是McAfee首席網路安全部門院士兼副總裁的不明人士，將一支惡意程式碼本

刑事警察局早在10月5日傍晚等，13日時透露，已經從11個簡單描述這批惡意程式的功能。內部電腦，也會蒐集相關情資。局以偵案不公開為由，只有簡單入侵遠東銀行的管道也三緘其口。

反倒是根據McAfee最初接獲的入侵的起點，是一封附件藏有後

張載圖，一張是釣魚郵件要求受害者打開一個偽造的「DocuSign文件」存取網頁，另一個則是偽裝成一個加密PDF線上文件的開啟連結，但這些附件連結都是假冒的，只要受害者點選連結來開啟文件，都會轉向到一個惡意程式網站，來下載一個不明檔案到受害者的電腦中。McAfee透露了這個惡意網址是 hxps://jobsbankbd.com/maliciousfilename.exe (資安公司已經將惡意程式檔名隱匿)。

若透過全球WHOIS查詢這個網址，註冊這個網址是位於孟加拉國首都達卡的一家公司，也就是2016年2月知名SWIFT遭駭事件案主孟加拉央行的所在地。不過，McAfee沒有透露這個網址是駭客所有，或者又是駭客所入侵的另一個跳板網站，不過，若瀏覽這個網站，就會看到一個偽造的Yahoo登入畫面，反映出這個網站可能目前這是一個釣魚網站。

上周金管會也公布了派員進駐遠銀的初步調查結果，發現在權限管理上，遠銀沒有符合最小授權原則，而是給予最高權限。再加上遠銀的SWIFT伺服器也沒有落實實體隔離，可能基於作業方便與其他的電腦連結，雖然負責個人電文放行的工作站有隔離，但因主機沒有做好實體隔離，成為駭客入侵的管道。

綜合金管會和McAfee的分析，可以推測，正因駭客取得最高權限的帳密，又能連線到沒有採取實體隔離的SWIFT伺服器，攻擊者才能進一步控制SWIFT系統。這2組帳號正是這次遠銀遭駭盜轉事件的關鍵。

這支惡意程式還特別會排除三種語系，俄羅斯語系、烏克蘭語系和白俄羅斯語系，遇到這三種語系的系統就不會入侵，但這也可能是駭客故佈疑陣。另外McAfee發現，駭客所用的Hermes勒索加密軟體還只是一個開發中的版本，而不是原始的Hermes軟體。

件，將惡意木馬下載到電腦後，罪者存取銀行內受害者的電腦系統，進一步取得系統的帳號密碼，找到了攻擊者手上的2組

意程式的檔名，包括了M_HERMS.A之外，另外三支(ZTEJ-A病毒)。

而McAfee分析的這支惡

遠銀事件攻擊者取得兩個帳號，程式會在這駭電腦中，建立了運作。資安軟體一般不會將此視

為惡意行為，但這卻是攻擊者用來找出銀行內部防病毒軟體的部署情況，才能進一步刪除系統防病毒服務，瓦解系統資安預警機制。

McAfee從反組譯惡意程式所找到的2組遠銀系統管理帳號，也反映出，駭客為了入侵遠銀內部系統而量身打造了這個專用惡意程式，還不斷利用這兩組帳號密碼來測試遠銀的其他系統，是否可以用同一組密碼入侵。

銀行內部控制三道防線實務守則

四、執行風險管理程序並維持有效的內部控制。

五、當流程及控制程序不足時，應立即提出改善計畫。

第一道防線應定期或不定期就前項內容辦理自我評估，以確保風險有被適當管。

第八條

第二道防線的功能係在訂定整體政策及建立管理制度，協助及監督第一道防線管理風險與自我評估執行情形。依照不同的功能性質，第二道防線之權責包含協助辨識及衡量風險、定義風險管理角色及責任、提供風險管理架構及定期將風險管理結果呈報高階管理階層。說明如下：

- 一、風險管理單位負責建立獨立有效的風險管理機制，以評估及監督整體風險承擔能力、已承受風險現況、決定風險因應策略及風險管理程序遵循情形。
- 二、法令遵循單位負責法令遵循制度之規劃、管理及執行，訂定法令遵循之評估內容與程序，並督導各單位定期辦理法令遵循自行評估及綜理法令遵循事務。
- 三、其他專職單位，包含但不限於財務控制、人力資源、法務等。

第九條

內部稽核單位係第三道防線，負責查核與評估第一道及第二道防線所設計並執行之內部控制與風險管理制度之有效性，並適時提供改進建議。

第四章 三道防線間之協調

第十條

險現況，並向董（理）事會或高階管理階層報告風險管情形。

各銀行的組織架構雖然不盡相同，惟仍須依風險管理及控制架構中各道防線所扮演之角色功能進行協調，運作之原則如下：

- 一、風險管理及控制流程的建構應遵循三道防線模式。
- 二、各道防線均應本於其角色定位及職掌，確實執行及管理相關業務。
- 三、各道防線應互相協調，以促進效率及效率。
- 四、各道防線之風險管理及控制功能運作結果，應互相分享知識與資訊，以協助所有功能更有效完成其職責。

第五章 附則

第十一條

本守則經本會理事會通過，並報請金融監督管理委員會核備後施行；修正時亦同。

整體內部控制制度有效性及出具內部控制制度聲明書之依據。

第 15 條

銀行業內部稽核單位對國內營業、財務、資產保管及資訊單位每年至少應辦理一次一般查核及一次專案查核，對其他管理單位每年至少應辦理一次專案查核；對各種作業中心、國外營業單位及國外子行每年至少辦理一次一般查核；對國外辦事處之查核方式可以表報稽核替代或彈性調整當地查核頻率。

銀行業稽核單位應將營業單位辦理信託業務、財富管理及金融商品銷售業務有無不當行銷、商品內容是否充分揭露、相關風險是否充分告知、契約是否公平及其他依法令或自律規範應負之義務之執行情形，併入對營業單位之一般查核或專案查核辦理。

金融控股公司內部稽核單位每年至少應辦理一次一般業務查核；每半年至少應對金融控股公司之財務、風險管理及法令遵循辦理一次專案業務查核；另辦理一般業務查核如已涵蓋專案業務查核之項目及範圍，且查核結果無重大缺失事項並於內部稽核報告敘明者，該半年度得免辦理專案業務查核。

內部稽核單位應將法令遵循制度之執行情形，併入對業務及管理單位之一般查核或專案查核辦理。

第 15-1 條

本國銀行得向主管機關申請核准採行風險導向內部稽核制度。主管機關得視銀行之資產規模、業務風險及其他必要情況，請本國銀行申請採行風險導向內部稽核制度。

本國銀行申請採行風險導向內部稽核制度，應符合下列條件：

- 一、最近一次申報自有資本與風險性資產比率，符合銀行資本適足性及資本等級管理辦法第五條之規定。
- 二、以最近一次金融檢查及最近一期經會計師查核簽證之財務報表為基準，均無備抵呆帳及各項準備提列不足。
- 三、最近一季逾期放款比率未超過百分之一。
- 四、已具備有效之內部控制制度，且最近一年內部控制執行無重大缺失，或缺失已具體改善。

本國銀行經採行風險導向內部稽核制度者，不適用前條第一項查核頻率之規定。

第 16 條

金融控股公司及銀行業應依子公司業務風險特性及其內部稽核執行情形，

History of Internal audit...

Late 1990s - 2002 ('risk based auditing'):

- ☐ Increasing integration of risk into audits
- ☐ COSO 'Ent. Risk Mgt. – Integrated Framework'*

2003 - ...2006 (the 'SOX years'):

- ☐ Sarbanes-Oxley Act (2004)
- ☐ Focus on internal controls on fin. rptg. (ICFR)

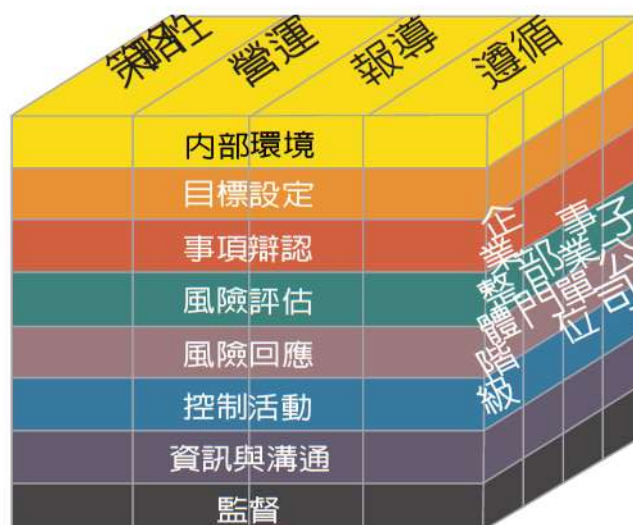
...2007 – 2008 (return to risk?):

- ☐ Focus on entity and process-level controls
- ☐ Integration of risk mitigation/risk treatments

* A bit late in the day (2004), post SOX...

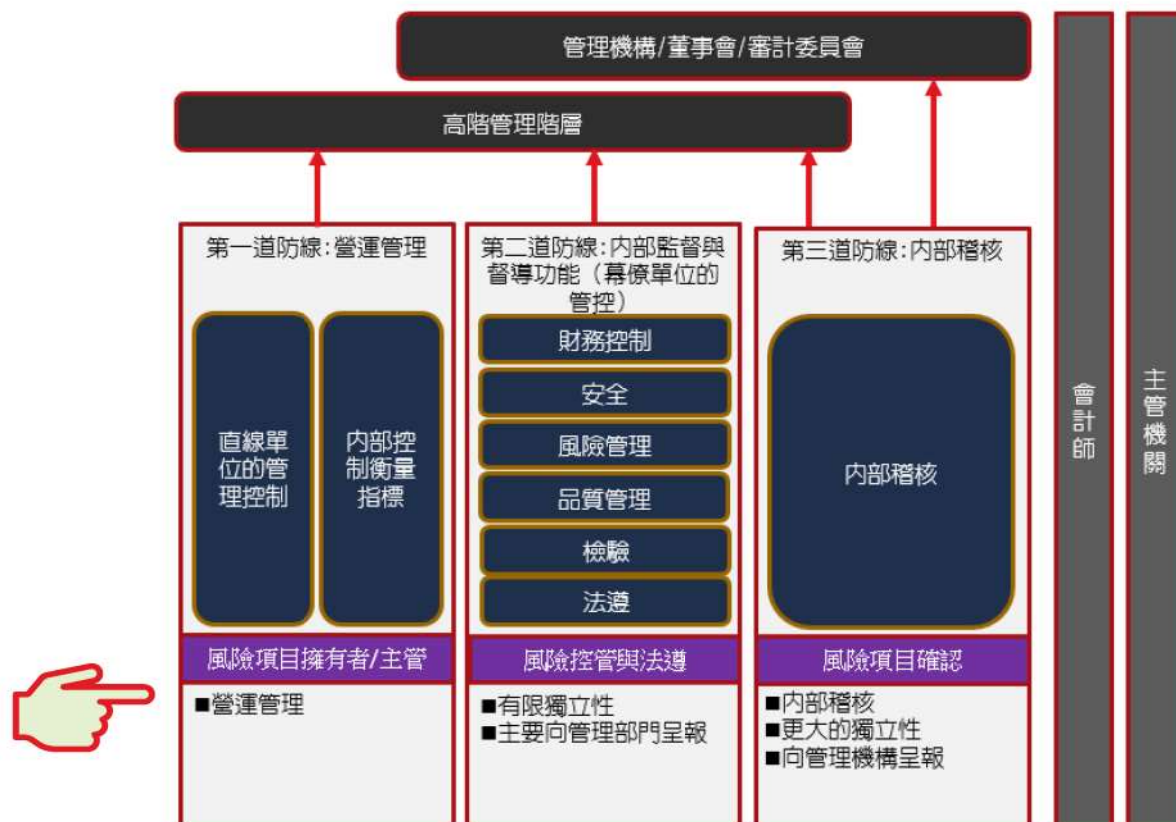
COSO-ERM企業風險管理整合架構

立方體之上方所標示者，為四類目標(策略性、營運、報導及遵循)；立方體之前方則標示八個組成要素，右方則描述企業之單位，此種表達方式顯示可著眼於企業風險管理之整體，或著眼於某一類目標、某一個組成要素、某個企業單位，甚或更小之組成單位。

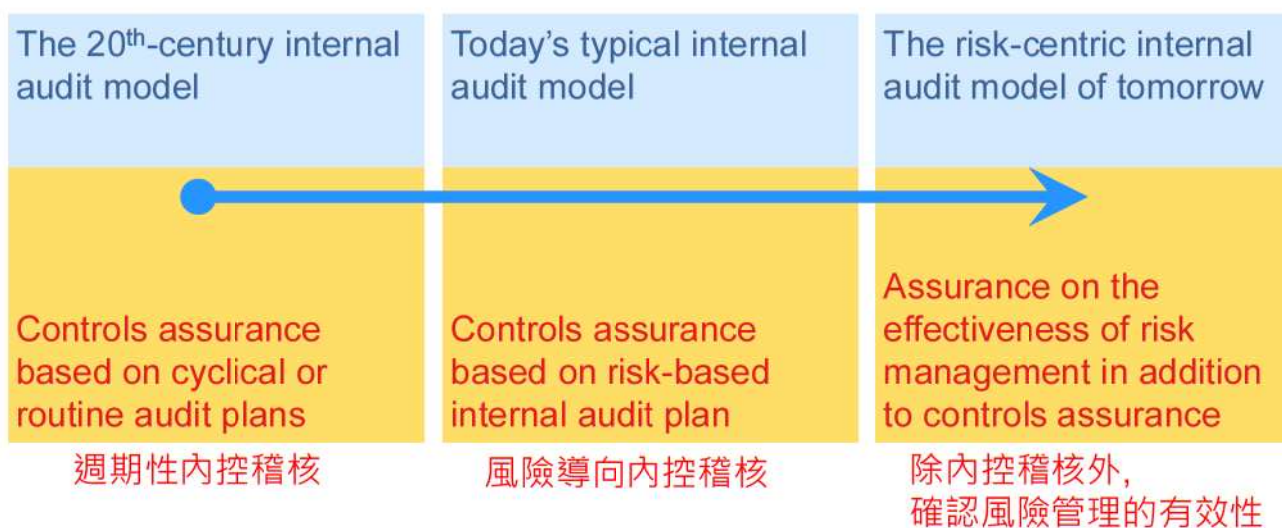


Source: *COSO Enterprise Risk Management – Integrated Framework*, 2004. COSO. 及企業風險管理－整合架構：馬秀如博士等譯

有效風險管理與內部控制三道防線



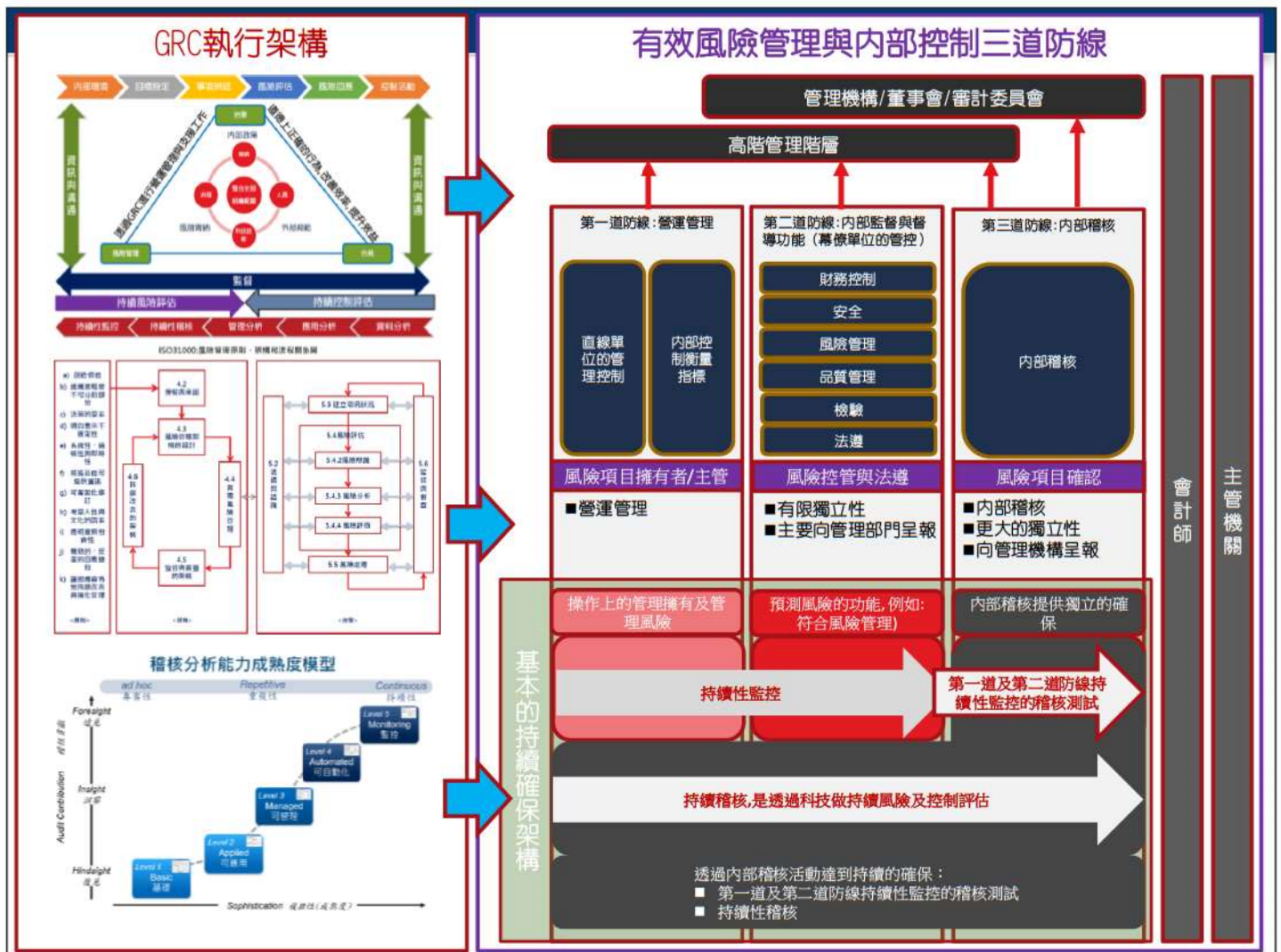
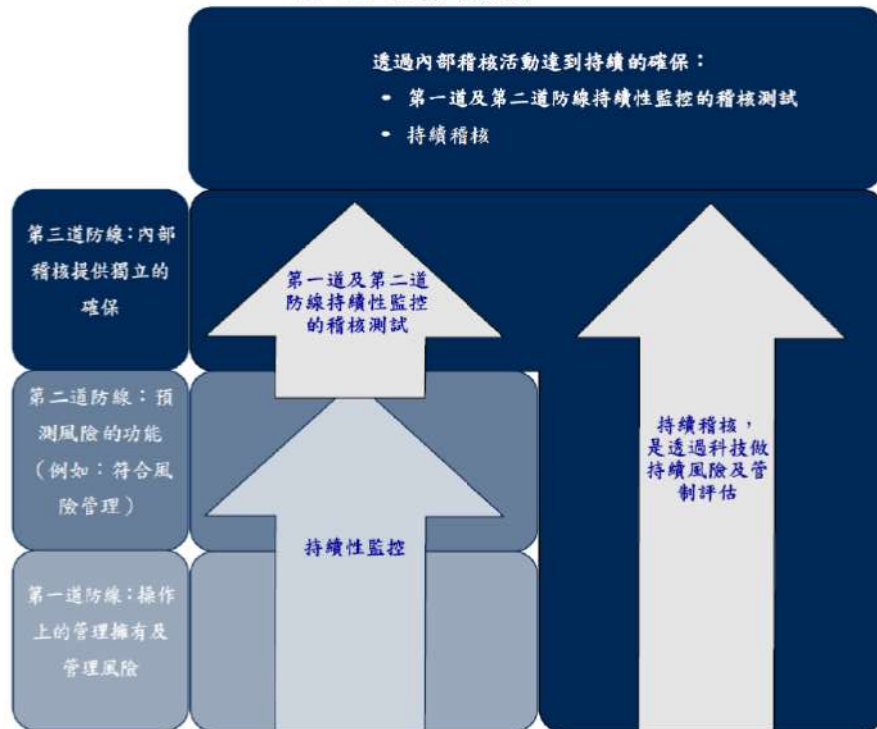
內部稽核焦點的轉變



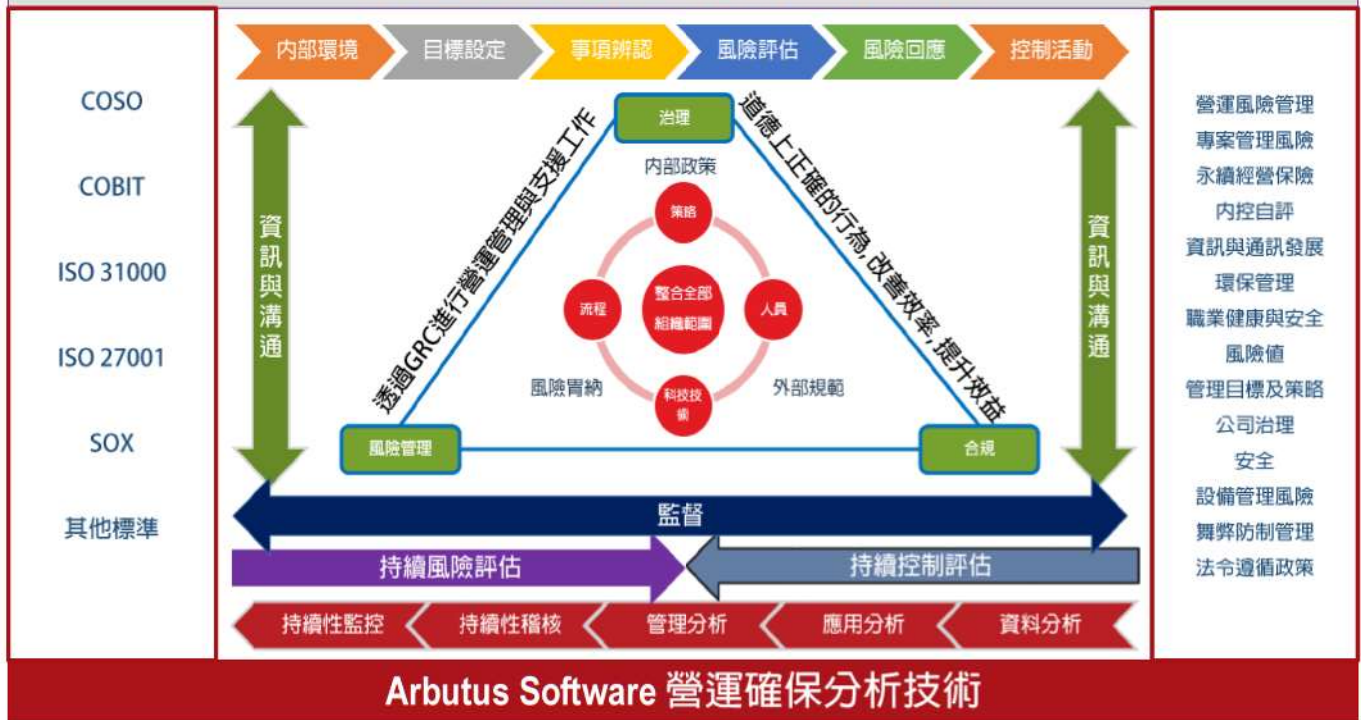
Adapted from PricewaterhouseCoopers Advisory Services, "Internal Audit 2012," © 2007

PRICEWATERHOUSECOOPERS 

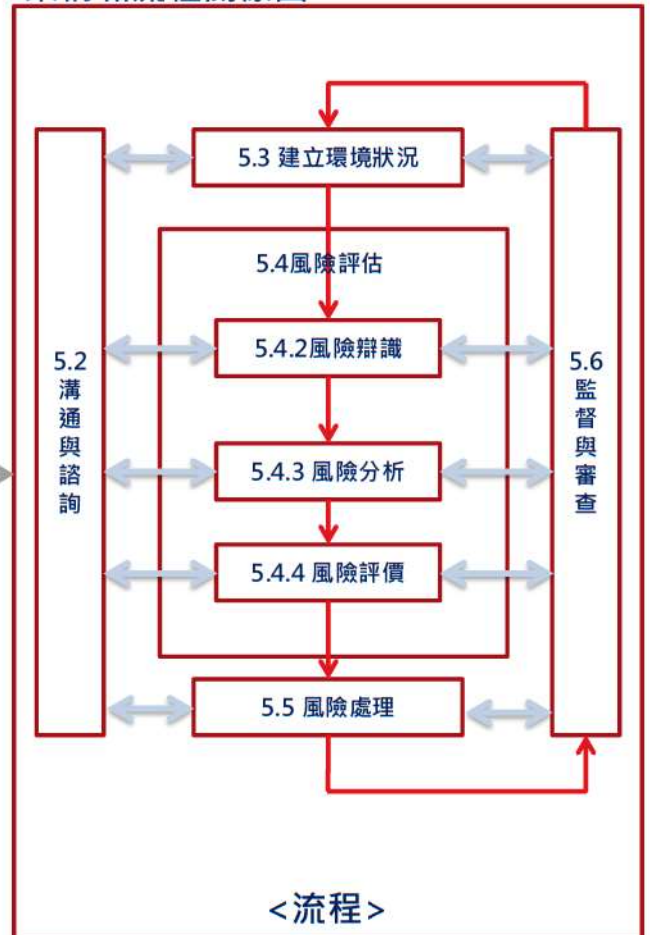
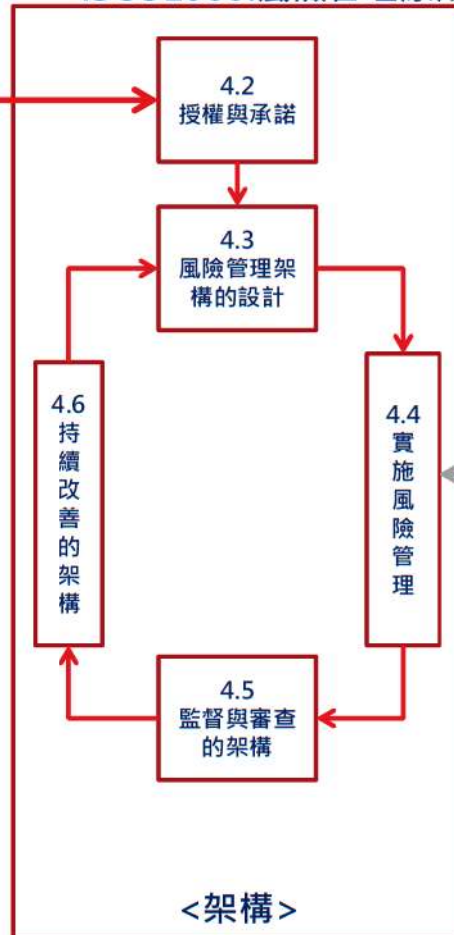
圖1、基本的持續確保架構



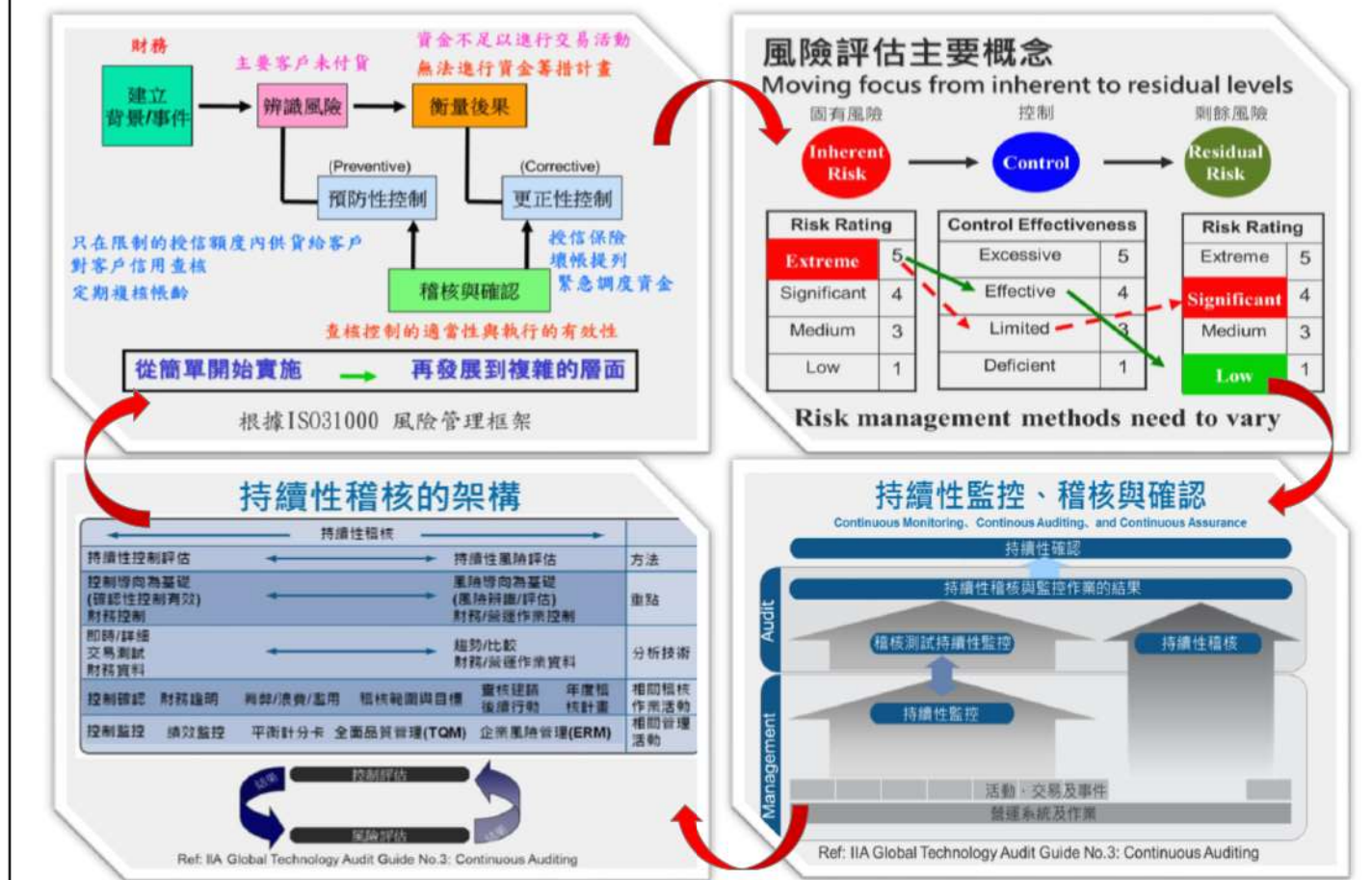
Pentana Vision 風險與稽核管理系統



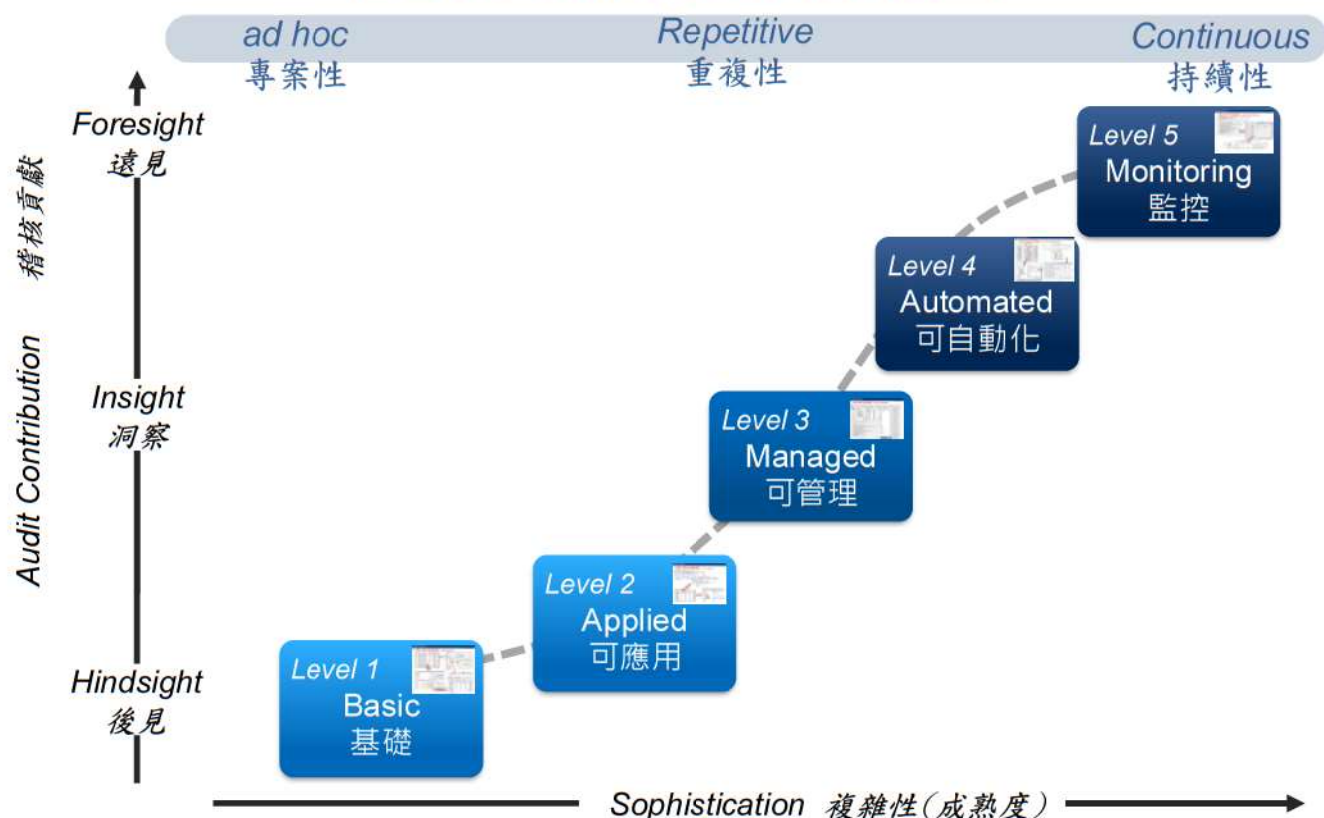
- 創造價值
- 組織流程密不可分的部份
- 決策的要素
- 明白表示不確定性
- 系統性、結構性與即時性
- 根據最佳可提供資訊
- 可客製化修訂
- 考量人性與文化的因素
- 透明度與包容性
- 機動的、反覆的回應變動
- 讓組織容易地持續改善與強化管理



風險管理方法 – 以風險為導向的內部控制與稽核作業



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？

THE INSIGHT ADVANTAGE TO YOUR BUSINESS

如何提高你的洞察力

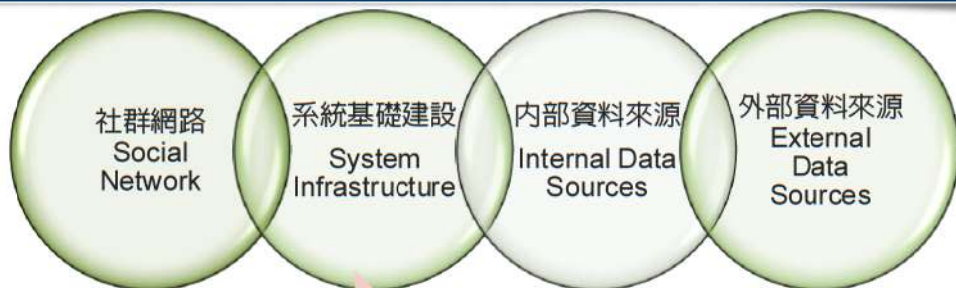
Insight = Catalyst(催化劑), Analyses(分析), and Assessments(評估).



兆益數位 Uprofit Digital Ltd.,

23

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)



資料探索
Data
Discovery

資料分析
Data
Analysis

資料態樣
Patterns

要求洞察
Required
Insights

報表和儀表板
Report &
Dashboards

Browser

EIP

EIS

決策者



安例·疑似洗錢或咨訊六見能樣

Deposits - Arbutus Analyzer

檔案(F) 編輯(E) 資料(D) 分析(A) 共用(S) 工具(T) 應用程式(P) 伺服器(S) 視窗(W) 管理(A) 說明(H)

專案概觀

指令日誌 SelectedRiskAcctTrans

Smart Search

	EndWeekDay	ACCOUNT_NO	TransDate	POSTING_SOURCE	TRANSCODE	DepositAmt	ACCOUNT_NO	EndWeekDay	COUNT	DepositAmt
1	04/15/2017	1228896	04/09/2017	SYSTEM	DEP	55950	1228896	04/15/2017	17	500144
2	04/15/2017	1228896	04/09/2017	SYSTEM	DEP	53193	1228896	04/15/2017	17	500144
3	04/15/2017	1228896	04/10/2017	SYSTEM	DEP	25249	1228896	04/15/2017	17	500144
4	04/15/2017	1228896	04/10/2017	SYSTEM	CHK	5551	1228896	04/15/2017	17	500144
5	04/15/2017	1228896	04/10/2017	SYSTEM	DEP	30714	1228896	04/15/2017	17	500144
6	04/15/2017	1228896	04/11/2017	SYSTEM	SVC	25	1228896	04/15/2017	17	500144
7	04/15/2017	1228896	04/11/2017	SYSTEM	CHK	17609	1228896	04/15/2017	17	500144
8	04/15/2017	1228896	04/11/2017	SYSTEM	CHK	15095	1228896	04/15/2017	17	500144
9	04/15/2017	1228896	04/12/2017	SYSTEM	DEP	59581	1228896	04/15/2017	17	500144
10	04/15/2017	1228896	04/12/2017	SYSTEM	CHK	8578	1228896	04/15/2017	17	500144
11	04/15/2017	1228896	04/12/2017	SYSTEM	CHK	27311	1228896	04/15/2017	17	500144
12	04/15/2017	1228896	04/13/2017	SYSTEM	DEP	37155	1228896	04/15/2017	17	500144
13	04/15/2017	1228896	04/14/2017	SYSTEM	DEP	49040	1228896	04/15/2017	17	500144
14	04/15/2017	1228896	04/14/2017	SYSTEM	DEP	17372	1228896	04/15/2017	17	500144
15	04/15/2017	1228896	04/15/2017	SYSTEM	DEP	33527	1228896	04/15/2017	17	500144
16	04/15/2017	1228896	04/15/2017	SYSTEM	CHK	18075	1228896	04/15/2017	17	500144
17	04/15/2017	1228896	04/15/2017	SYSTEM	DEP	36248	1228896	04/15/2017	17	500144
18	04/08/2017	1314379	04/02/2017	SYSTEM	DEP	32527	1314379	04/08/2017	16	520942
19	04/08/2017	1314379	04/02/2017	SYSTEM	DEP	51208	1314379	04/08/2017	16	520942
20	04/08/2017	1314379	04/02/2017	SYSTEM	DEP	59055	1314379	04/08/2017	16	520942
21	04/08/2017	1314379	04/02/2017	SYSTEM	CHK	12510	1314379	04/08/2017	16	520942
22	04/08/2017	1314379	04/02/2017	SYSTEM	DEP	17211	1314379	04/08/2017	16	520942
23	04/08/2017	1314379	04/02/2017	SYSTEM	DEP	17211	1314379	04/08/2017	16	520942
24	04/08/2017	1314379	04/02/2017	SYSTEM	DEP	17211	1314379	04/08/2017	16	520942
25	04/08/2017	1314379	04/02/2017	SYSTEM	DEP	17211	1314379	04/08/2017	16	520942
26	04/08/2017	1314379	04/02/2017	SYSTEM	DEP	17211	1314379	04/08/2017	16	520942
27	04/08/2017	1314379	04/02/2017	SYSTEM	DEP	17211	1314379	04/08/2017	16	520942
28	04/08/2017	1314379	04/02/2017	SYSTEM	DEP	17211	1314379	04/08/2017	16	520942
29	04/08/2017	1314379	04/02/2017	SYSTEM	DEP	17211	1314379	04/08/2017	16	520942
30	04/08/2017	1314379	04/02/2017	SYSTEM	CHK	12510	1314379	04/08/2017	16	520942
31	04/08/2017	1314379	04/02/2017	SYSTEM	DEP	17211	1314379	04/08/2017	16	520942

接著進行詳查

102 筆記錄 E:\Client Sample Case\APPBanking\Banking - Deposits\Deposits\Work Folder\SelectedRiskAcctTrans.fl

62,445 筆記錄 E:\Client Sample Case\APPBanking\Banking - Deposits\Deposits\Work Folder\Deposit History.fl

	EndWeekDay	ACCOUNT_NO	TransDate	POSTING_SOURCE	TRANSCODE	DepositAmt	ACCOUNT_NO	EndWeekDay	COUNT	DepositAmt
29	12/02/2017	1202488	03/15/2017	SYSTEM	SVC	690	1202488	12/02/2017	16	520942
30	12/02/2017	1202488	03/15/2017	SYSTEM	DEP	690	1202488	12/02/2017	16	520942
31	12/02/2017	1202488	03/15/2017	SYSTEM	DEP	34107	1202488	12/02/2017	16	520942

62,445 筆記錄 E:\Client Sample Case\APPBanking\Banking - Deposits\Deposits\Work Folder\Deposit History.fl

The screenshot displays the Microsoft Access interface. A yellow callout bubble with the text "KYC可疑交易對象" (KYC Suspicious Transaction Object) is positioned over the query results. The query results table, titled "FuzzyDup_Procedure2", contains the following data:

	CustomerID	CompanyName	ContactName	CORPORATE_NAME	NAME	ContactTitle
1	10011	LILA-Supermercado	Carlos Gonzalez	LILA Supermercado	Gonzalez Carlos	Accounting Manager
2	10028	France restauration	Carine Schmitt	restauration France	Carine Schmit	Marketing Manager
3	10057	Berglunds snabbkop	Christina Berglund	Berglunds snabbk	Christina Berglund	Order Administrator

The 'CORPORATE_NAME' and 'NAME' columns are highlighted with a red box. The interface also shows a 'Join' dialog box and a 'FuzzyDup_Procedure2' query design view.

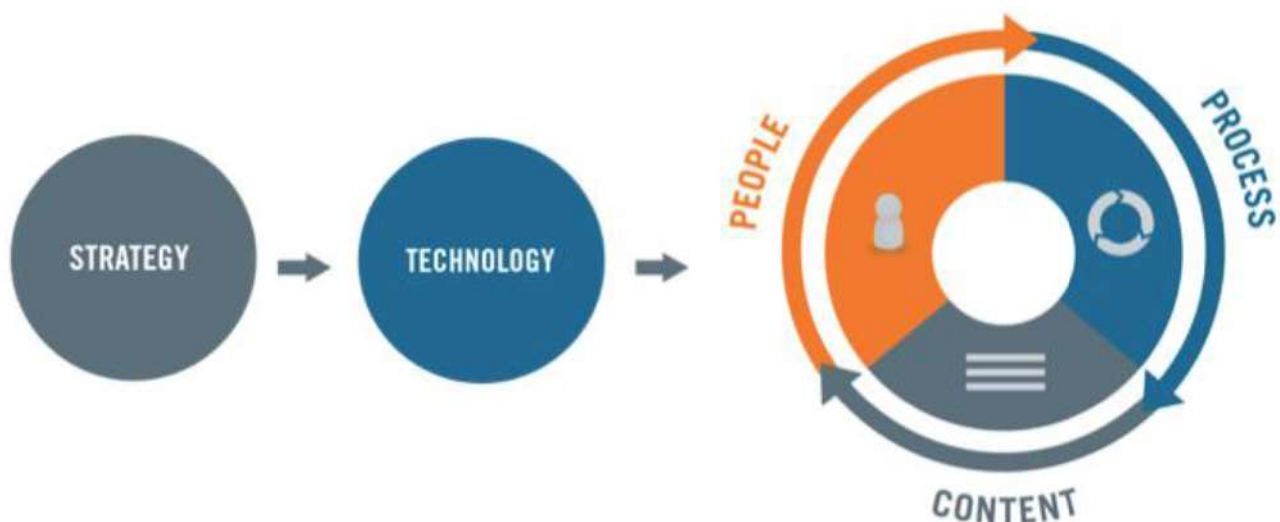
Analytics & Insights

Unlocks the power of
your data

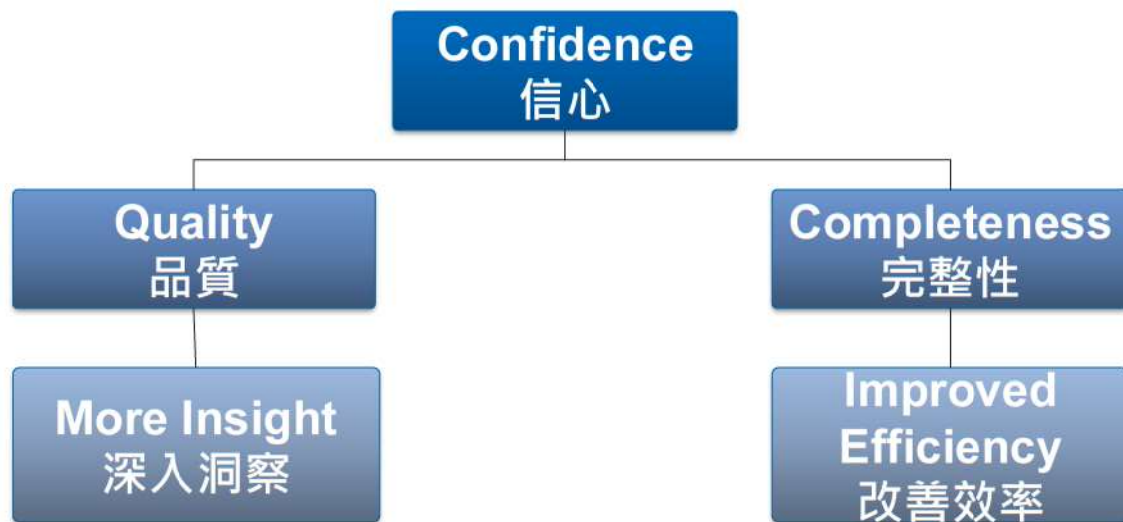
我們十力展現

- 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

持續性稽核實行步驟



Delivering Assurance – Achieving Confidence



免除您心中的疑惑

FREEDOM FROM DOUBT™





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 的觀網
blog.uprofit-tw.com