

使用電腦輔助查核技術與工具 提升查核品質

淺談 如何偵測虛擬交易 與 導入CAATTs查核之
案例分享

主講人: 莊盛祺

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

大綱

- 一. 為什麼要使用電腦輔助查核技術與工具(CAATTs)
- 二. 資料分析能力對內部稽核的重要性
- 三. 風險評估和持續性稽核與監控作業
- 四. 個案探討

為什麼要使用電腦輔助查核技術與工具 (CAATTs)

何謂 CAATs vs CAATTs

- Computer Aided Audit Techniques and Tool (電腦輔助稽核技術與工具)
 - Performing audits without using information technology is hardly an option. When all the information needed for doing an audit is on computer systems, how can one carry out an audit without using the computer? While the audit world will likely grow out of using this terminology, for the purpose of this article, the term CAAT refers to the use of certain software that can be used by the auditor to perform audits and to achieve the goals of auditing.
- 是執行電腦稽核作業重要的工具之一
- 包含很多型態的工具與技術，像是通用稽核軟體、公用程式、測試資料、應用軟體追蹤與圖示法，及稽核專家系統

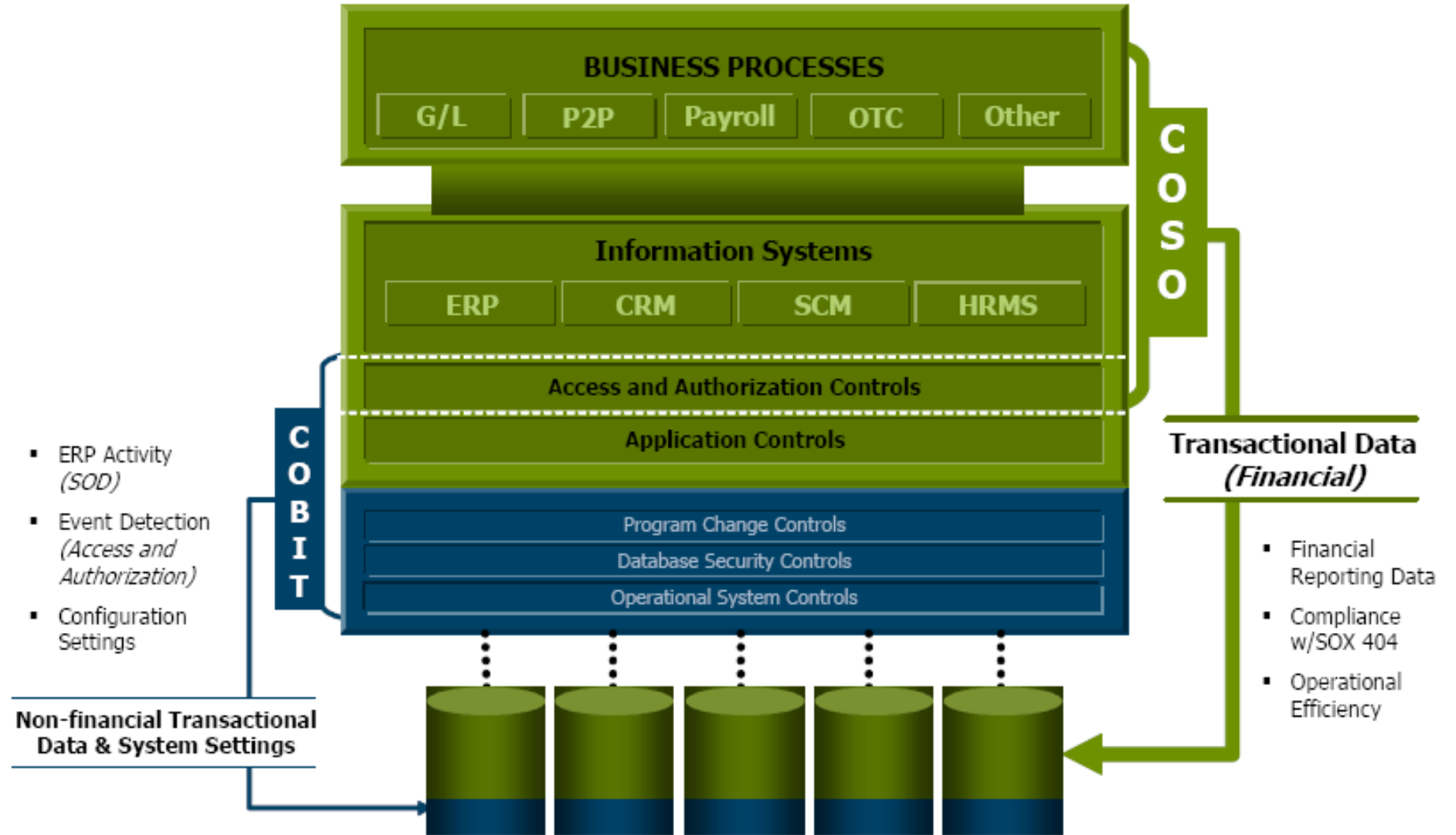


Using CAATs to Support IS Audit

S. Anantha Sayana, CISA, CIA

IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals

Transaction Monitoring for Controls Assurance



CAATs 的使用時機

- 需要與資料庫核對以驗證報表或書面資料，如帳齡表測試
- 需要對以電腦處理之作業流程進行瞭解，如存戶利息計算
- 需要對系統中之交易審計軌跡進行追蹤，如遵行測試
- 人工查核無效果或無效率，如資料量龐大而計算複雜

CAATs 的應用範圍

- 交易明細資料及餘額的測試
- 分析性複核程序驗證作業 (analytical review procedures)
- 一般資訊控制環境 (IS general controls) 遵行測試
- 應用資訊系統控制 (IS application controls) 遵行測試
- 滲透測試 (penetration testing)

電腦輔助查核技術的優點

- 降低審計風險程度
- 較不需依賴受查單位人員
- 較廣泛及一致的稽核範圍
- 資料可以更快速利用
- 改善例外之識別
- 執行時間較有彈性
- 更有機會將內部控制的弱點量化
- 加強抽樣
- 節省成本

採用 CAATs 的注意要點

- 採用CAATs進行測試，所產生的查核證據力較強，使用者必須儘到專業上的注意。
- 使用 CAATs，並**不限定**要是電腦稽核人員，任何人覺得有需要，皆可以運用。

執行**CAATs** 的程序與方法

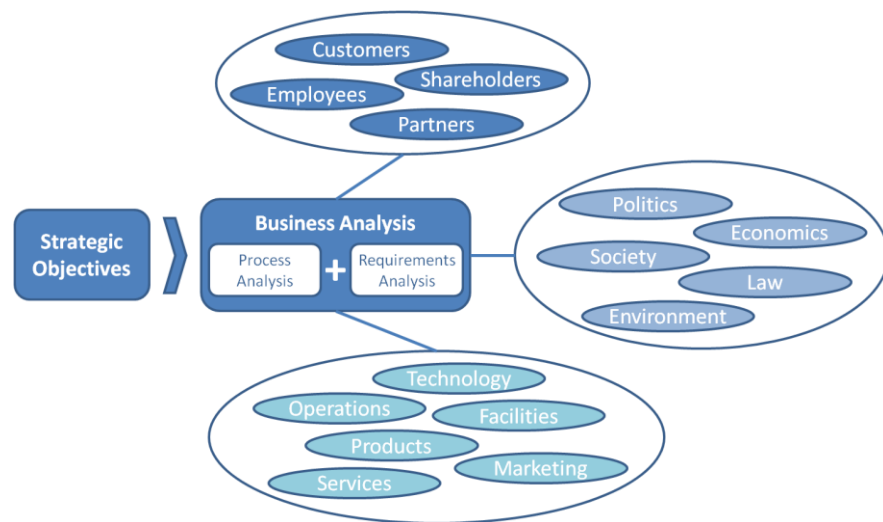
- A. 規劃 (Planning)
- B. 稽核工作的執行 (Performance of audit work)
- C. CAATs文件管理 (CAATs Documentation)
- D. 報告 (Reporting)

資料分析能力對內部稽核的重要性

營運分析的目標

The Goal of Business Analysis

- 及時減少浪費和快速完成專案
- 確認營運需求的正確性與必要性
- 改善專案執行效率

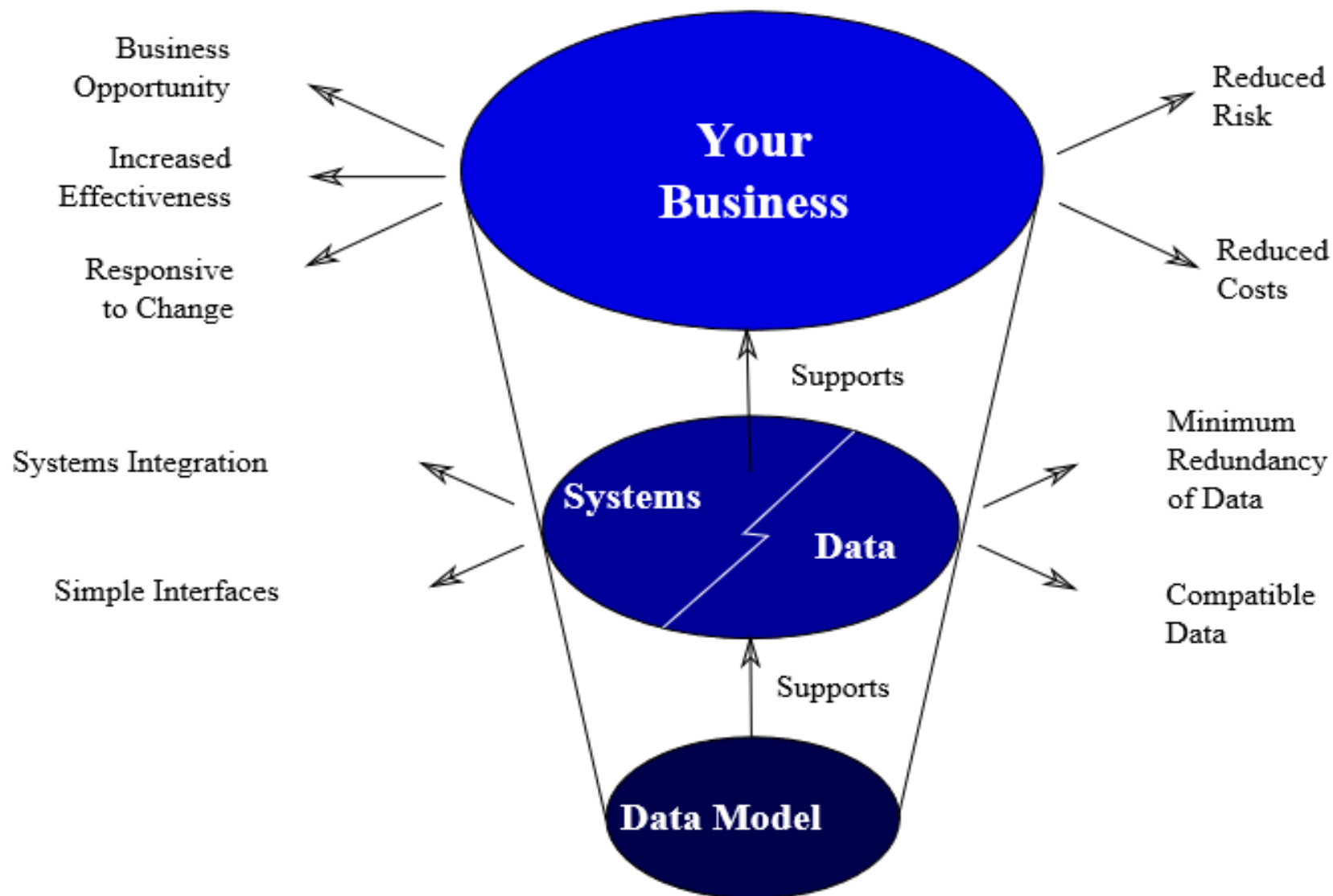


<http://www.onyxinterweb.com/2012/09/business-analysis/>

營運分析 (Business analysis) 是一種辨別營運需求與決定營運問題解決方式的研究過程，它經常包含系統發展要件，也涵蓋作業流程的改善、組織變更或是策略規劃和政策擬定。

- **策略規劃** — 決定企業組織營運需求
- **營運模式分析** — 決定企業組織政策和行銷方式
- **流程設計** — 將企業組織流程標準化
- **系統分析** — 配合資訊作業將營運規則與需求系統化

Data Model Support Your business



Data Analysis - 資料分析

- **資料分析(Analysis of data)** 是以發現有用資訊、建議具體結論及支持決策的目標所進行檢視、清理、格式轉換、和模組化資料的作業流程，數據資料分析具有多重面向和方法，在不同商業、科技和社會科學領域裡，各種名目之下涵蓋不同的技術。
 - 資料採礦(Data Mining)是一種特定的資料分析技術，專注於模組化及知識發現上，做為預測而不是純粹描述性的目的。
 - 商業智慧(Business Intelligent)含蓋很大程度上依賴彙集、重心放在業務訊息上的資料分析。
 - 在統計應用中，有些人劃分的資料分析為描述性統計(Descriptive Statistics)、探索性資料分析(EDA, Exploratory data analysis)及證實性資料分析(CDA, Confirmatory data analysis)，EDA專注於發現資料中新的特性(New Features)，而CDA則是在進行證實或否定已知的假設
 - 預測分析(Predictive Analytics)側重於統計或結構模型的應用以進行預測或分類。
 - 文字分析(Text Analytics)應用統計、語言和結構技術，從文字敘述來源或非結構化資料中擷取及分類資訊。
- **資料整合(Data Integration)**是資料分析的先行步驟和資料分析是緊密地與資料數據可視化與資料傳遞相連，因此資料分析一詞有時候被當作資料建模的同義詞。

分析、監控、報告和及時回應

報表名稱(Report Title): DOMAIN USERS PASSWORD EXPIRY INFORMATION

報表說明(Report Description): 此張報表列示出所有有啟用[密碼永久有效]設定的網域主控站(Domain Controller)使用者帳戶

報表日期(Report Date):2014/3/25 下午 02:25

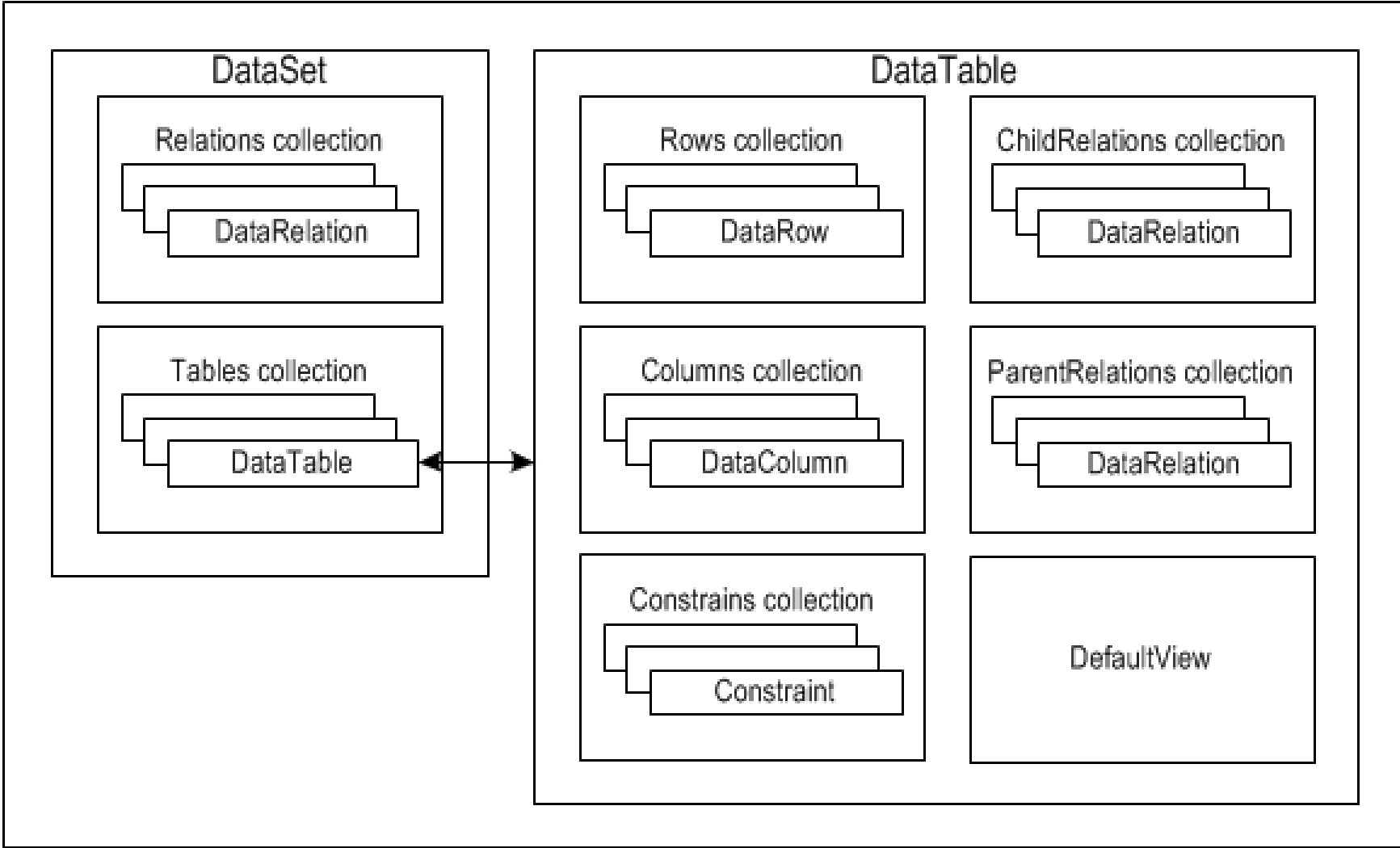
PasswordExpires	Description	Domain	Name	LocalAccount	PasswordChangeable	PasswordRequired	SID	Status	ServerIPAddress
False	專案服務部-顧問	UPROFIT	mia	False	True	True	S-1-5-21-2096861050-3069218562-966048004-1113	OK	192.168.10.1
False	專案服務部-資深顧問	UPROFIT	perry	False	True	True	S-1-5-21-2096861050-3069218562-966048004-1117	OK	192.168.10.1
False	業務部-業務	UPROFIT	eric	False	True	True	S-1-5-21-2096861050-3069218562-966048004-1118	OK	192.168.10.1
					False	True	S-1-5-21-2096861050-3069218562-966048004-2104	OK	192.168.10.1
					False	True	S-1-5-21-2096861050-3069218562-966048004-2105	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原則的套用，密碼永久無須變更。

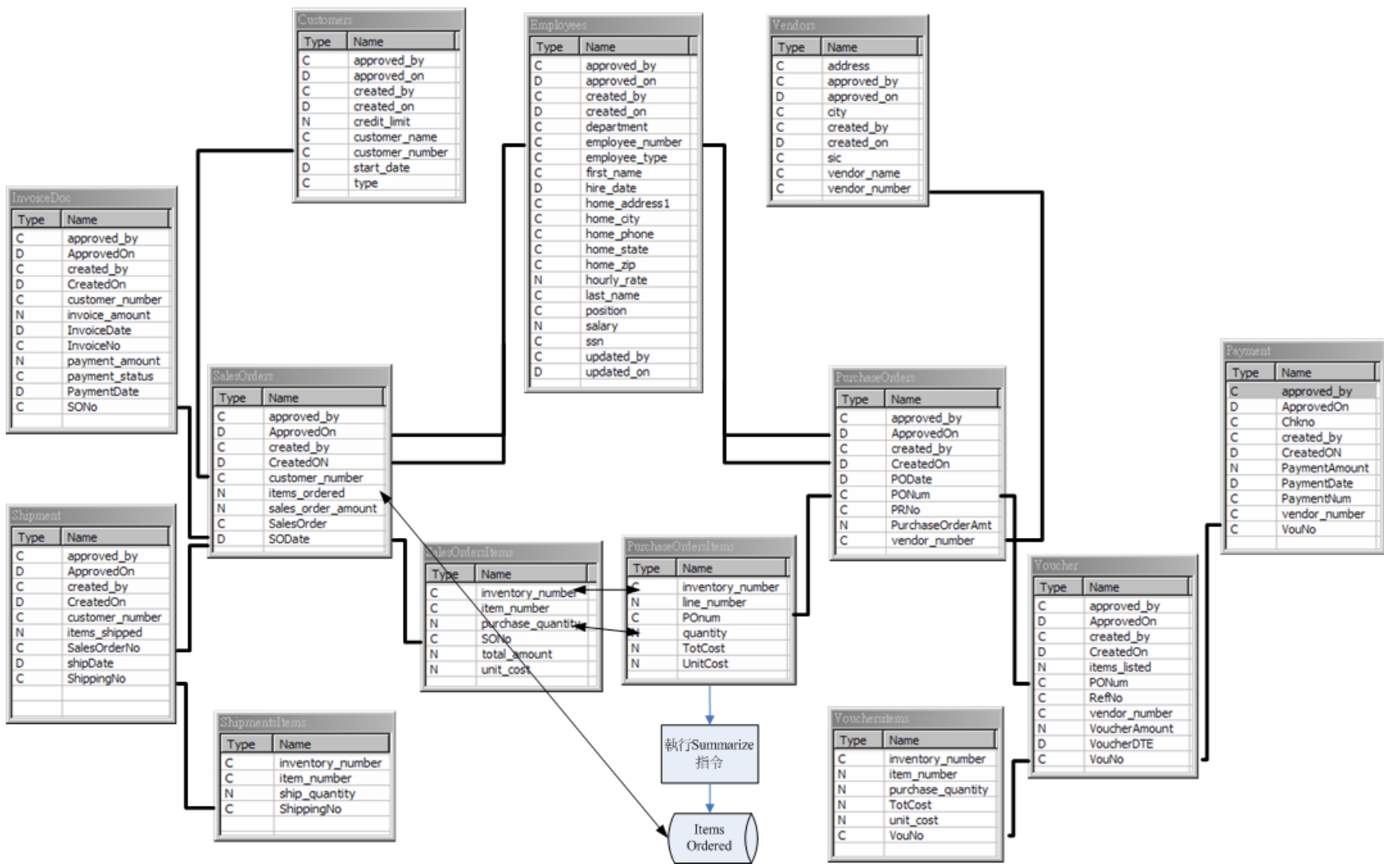


	A	B	D	E	F	G	H	I	J	K	L	M	N	O	P
1															
2	Forecast 2001 & Budget 2002 & Plan 2003 to 2006														
3	Profit & Loss Statement - Total Portfolio														
4															
5	Key drivers - Base case NCA = 91 k														
6															
7	(NTD)	remarks	Actual	Ref only	Ref only	Ref only	Ref only	Ref only	Ref only	Ref only	Ref only	Ref only	Ref only	Ref only	Ref only
8	Day count	actual / forecast	Dec-00	Jan-01	Feb-01	Mar-01	Apr-01	May-01	Jun-01	Jul-01	Aug-01	Sep-01	Oct-01	Nov-01	Dec-01
9		input	31	31	28	31	30	31	30	31	31	30	31	30	31
10	NPCA	per SAS / NCA	9,040	6,288	4,907	7,898	8,929	7,201	7,169	5,172	5,001	4,048	4,145	3,078	2,582
11	Ending Account	per APS / ECOM+NCA	138,750	144,276	148,073	154,171	161,556	166,952	172,547	175,746	178,535	180,733	182,935	184,297	184,974
12	Account Change (2-mth avg)	per F3 / ECOM+NCA	134,448	141,513	146,175	151,122	157,884	164,284	169,770	174,147	177,141	179,534	181,834	183,616	184,598
13	Attributed	calculated	7,206	6,306	6,936	12,858	11,076	12,858	11,126	12,326	14,626	12,166	12,616	11,076	12,116
14	# of Account attr'd	per F3 / ECOM+NCA	835	762	1,110	1,800	1,504	1,805	1,614	1,973	2,212	1,850	1,943	1,716	1,805
15	Active Account	per APS / ECOM+NCA	133,794	140,127	144,182	149,588	156,562	161,878	167,770	175,744	177,946	180,731	182,933	176,266	176,152
16	Activation % (Blended)	calculated	96.4%	97.1%	97.4%	97.4%	96.9%	96.9%	97.2%	100.0%	99.7%	100.0%	100.0%	95.6%	95.2%
17															
18	NPCA	per SAS / NCA	9,833	6,678	5,137	8,200	9,250	7,460	7,373	5,408	5,204	4,238	4,217	3,203	2,678
19	Ending CIF	per APS / ECOM+NCA	154,834	160,683	164,578	170,742	178,311	183,760	189,327	192,587	195,403	197,654	199,760	201,106	201,707
20	Average CIF (2-mth avg)	calculated	150,380	157,759	162,631	167,660	171,036	186,544	190,957	193,995	196,529	198,707	200,473	201,407	
21	Attrition rate	calculated	7.11%	6.16%	6.89%	6.89%	14.14%	11.22%	12.99%	11.34%	13.24%	14.49%	11.93%	12.55%	10.86%
22	# of Card attr'd	per F3 / ECOM+NCA	562	629	636	1,011	862	1,011	862	1,283	1,185	827	865	769	869
23	Active CIF	per APS / ECOM+NCA	149,203	156,062	160,263	165,660	172,756	178,132	184,055	192,585	194,758	197,862	199,768	192,343	192,087
24	Activation % (Blended)	calculated	96.4%	97.1%	97.4%	97.0%	96.9%	96.9%	97.2%	100.0%	99.7%	100.0%	100.0%	95.6%	95.2%
25															
26	Total credit limit (NTD '000)		29,364,478	21,656,172	22,245,065	22,934,261	23,979,966	24,798,062	25,580,484	26,841,242	27,604,043	27,802,317	28,593,694	29,129,894	28,668,733
27	Credit limit Growth %		6.34%	2.72%	3.10%	4.56%	3.41%	3.10%	4.63%	2.84%	0.72%	2.85%	1.80%	1.58%	
28	Total Credit limit - Installment Loan (NTD '000)									197,212	272,779	100,102	157,761	124,557	134,859
29	Total credit limit - Excl. Install Loan(NTD '000)	APS / ECOM+NCA	29,364,478	21,656,172	22,245,065	22,934,261	23,979,966	24,798,062	25,383,272	26,068,463	26,513,871	26,644,556	27,378,137	27,815,036	27,282,409
30	Average credit limit (NTD)	calculated	131,525	134,776	135,164	134,321	134,484	134,948	134,071	135,359	135,688	134,804	137,060	138,310	135,258
31	Total active credit limit - Incl. Install Loan (NTD '000)		19,637,015	21,033,374	21,660,475	22,262,447	23,232,508	24,038,574	24,877,583	25,840,917	27,516,524	27,802,047	28,593,419	29,127,810	27,957,585
32	Total active credit limit - Excl. Install Loan (NTD '000)	CM / ECOM+NCA	19,637,015	21,033,374	21,660,475	22,262,447	23,232,508	24,038,574	24,877,583	25,840,917	26,513,871	26,644,556	27,378,137	27,815,036	26,921,911
33	Average credit limit per card(NTD)		134,776	135,164	134,321	134,484	134,948	135,133	135,372	141,267	141,267	140,662	143,140	144,845	142,131
34	Credit limit Growth %			#DIV/0!	0.29%	-0.62%	0.12%	0.35%	0.12%	3.15%	1.36%	-0.43%	1.76%	1.19%	-1.89%
35	To calculate AR components :														
36															
37	Average @ CM Retail Sales (NTD)		12,582	10,863	9,481	11,791	10,404	11,644	9,861	11,681	10,108	7,296	9,125	8,119	7,638
38	Total Billing for Ending AC		1,691,558	1,537,289	1,385,856	1,781,893	1,642,638	1,913,081	1,674,121	1,929,656	1,790,495	1,310,596	1,659,245	1,489,191	1,410,218
39	SUR - Total Billing / Tot Active Cr Im		8.61%	7.31%	6.40%	8.01%	7.07%	7.96%	6.78%	7.40%	6.78%	4.92%	6.06%	5.06%	5.43%
40	Average @ CM Retail Sales (NTD)		4,873	4,833	4,637	4,446	3,718	4,030	3,502	3,547	4,013	2,772	3,411	3,280	3,127
41	Retail Sales for Ending AC		655,158	684,002	677,880	671,813	587,089	662,089	594,475	617,736	718,378	497,962	620,326	602,248	577,343
42	SUR - Total Sales / Tot Active Cr Im		3.34%	3.25%	3.13%	3.02%	2.53%	2.75%	2.41%	2.73%	2.78%	2.78%	2.78%	2.23%	2.29%
43	Average @ CM Premium (NTD)		1,262	1,774	686	1,568	1,717	2,544	1,263	1,612	1,238	1,261	1,522	1,533	1,569
44	NS Premium for Ending AC		168,396	251,060	144,158	235,383	271,151	417,977	219,574	280,681	219,250	226,539	276,805	281,488	289,623
45	SUR - Premium / Tot Active Cr Im		0.86%	1.19%	0.67%	1.05%	1.17%	1.74%	0.89%	1.03%	0.83%	0.85%	1.01%	1.06%	1.11%
46	Average @ CM AC - Bear Fee (NTD)		1,184	970	1,184	1,761	1,728	1,544	1,544	1,648	1,516	1,762	1,655	1,686	1,487
47	Key drivers - Base Case - Key drivers - Retail	Key drivers - NSPSE	Key drivers - NSPSE	Key drivers - NSPSE	Key drivers - NSPSE	Key drivers - NSPSE	Key drivers - NSPSE	Key drivers - NSPSE	Key drivers - NSPSE	Key drivers - NSPSE	Key drivers - NSPSE	Key drivers - NSPSE	Key drivers - NSPSE	Key drivers - NSPSE	Key drivers - NSPSE

資料來源(Data Source) - 資料集(Data Set)



資料表結構及關係圖(Table Layout & Relation)



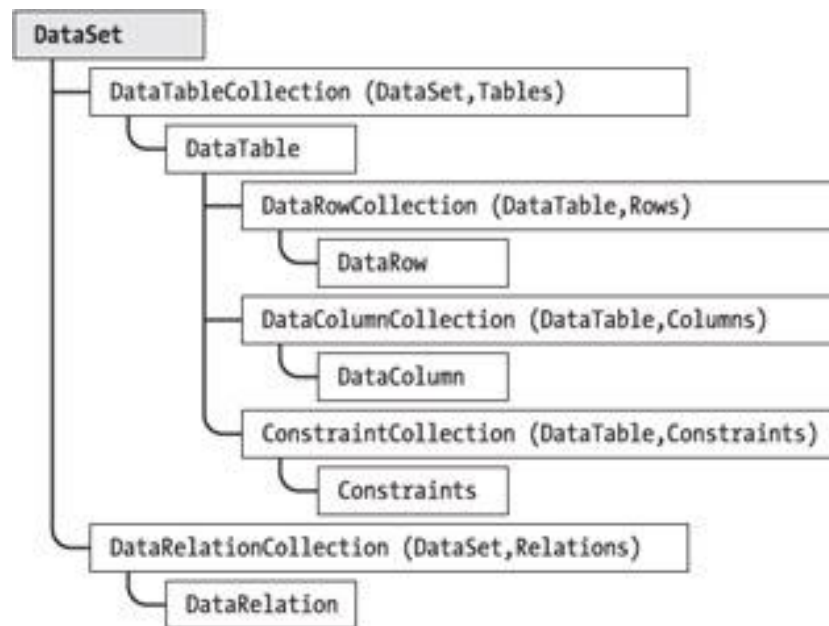
建立資料集(Data Set) — 檢視(View)/查詢(Enquiry)

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

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

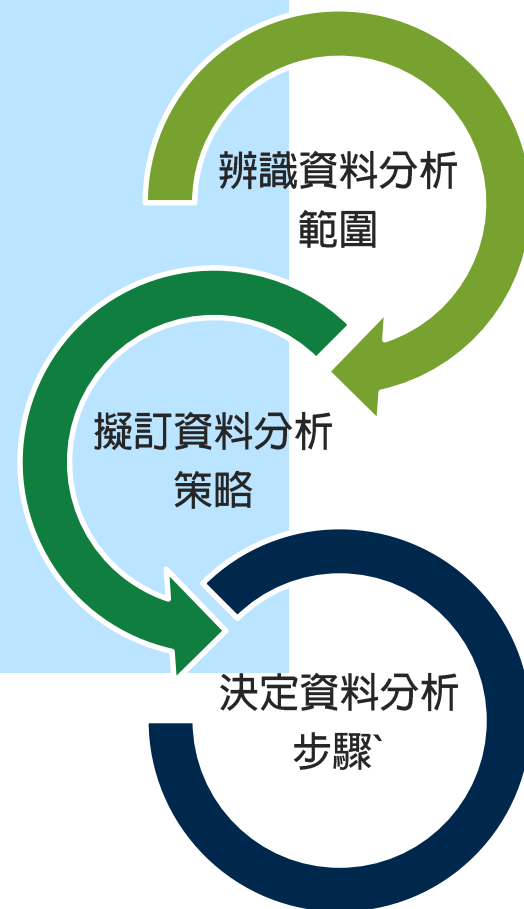
分析目標的訂定-決定資料分析的策略與步驟

分析目標訂定的時間點：

- 事前
- 事中
- 事後

資料分析需求：

- Reporting
- Operational Analysis
- Data-mining
- Fraud Detection
- Continuous Monitoring
- External / Internal Auditing
- Data Migration
- Data Harmonization



訂定查核及分析的目的

Data Analysis Cycle – Planning

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
1-2. 客戶付款金額與發票不符	1. 定期覆核客戶付款差異，以確認無超出允差範圍	1. 驗證系統防止客戶付款差異超出允差範圍的有效性，以及依客戶別分析付款差異的重大性與頻率。
1-3. 應收帳款與總帳科目未做調節	1. 定期執行總帳與應收帳款明細帳之調節	1. 測試總帳與應收帳款明細帳的一致性
1-4. 會計入帳之明細資料不完整	1. 執行檢核，以確保所有的客戶帳單均已及時拋轉至財務系統	1. 驗證帳單是否已適當拋轉至財務系統
1-5. 發票重複開立	1. 針對已開立發票之帳單，系統無法在對其再開立發票	1. 驗證系統是否無法在對已開立發票之帳單開立發票

查核測試是否有拆單分割採購之情形？

1. 開啓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

Purchase_orders			
po_number	C	12	
po_date	D	8	
vendor_number	C	17	
po_amount	N	14	
created_by	C	10	
created_on	D	8	
approved_by	C	10	
approved_on	D	8	

Purchase_orders_items			
po_number	C	12	
line_number	N	12	
inventory_number	C	16	
quantity	N	8	
unit_cost	N	10	

Vendors (Parent)	
Type	Name
C	address
C	approved_by
D	approved_on
C	city
C	created_by
D	created_on
C	sic
C	vendor_name
C	vendor_number

Vouchers			
voucher_number	C	12	
voucher_date	D	8	
vendor_number	C	17	
po_number	C	12	
reference_number	C	12	
items_listed	N	4	
voucher_amount	N	12	
created_by	C	10	
created_on	D	8	
approved_by	C	10	
approved_on	D	8	

Vouchers_items			
voucher_number	C	12	
line_number	N	12	
inventory_number	C	16	
purchase_quantity	N	6	
unit_cost	N	10	

Employees			
employee_number	C	10	
first_name	C	20	
last_name	C	25	
ssn	C	12	
department	C	30	
position	C	30	
employee_type	C	2	
hire_date	D	10	
home_phone	C	15	
home_address1	C	50	
home_city	C	20	
home_state	C	2	
home_zip	C	5	
hourly_rate	N	8	
salary	N	10	
created_by	C	10	
created_on	D	10	
approved_by	C	10	
approved_on	D	10	
updated_by	C	10	
updated_on	D	10	

Authorizations			
employee_number	C	10	
system	C	2	
process	C	2	
create	C	1	
approve	C	1	
modify	C	1	
delete	C	1	
limit	N	16	

Payments			
payment_number	C	12	
payment_date	D	8	
payment_amount	N	14	
vendor_number	C	17	
check_number	C	12	
voucher_number	C	12	
created_by	C	10	
created_on	D	8	
approved_by	C	10	
approved_on	D	8	

尋找資料的態樣(Data Pattern)或發生錯誤的地方

- 辨別問題傾向、精確地確認差異、突顯潛在風險區域
- 依照使用者作業準則，藉由比較分析檔案資料的方式，找尋錯誤及可能舞弊的地方
- 重新計算及確認餘額
- 確認各流程控制點及確保各作業準則之遵循
- 可對應收、應付帳款及任何時間敏感性交易進行帳齡分析
- 藉由對重複付款、帳單號碼缺漏或未發帳單的測試，回復其多支出或所損失的金額
- 可測試出未授權員工與廠商間的關係

Find Abnormal Trend/Exceptional Record/Error

依各分析群組辨別問題傾向、精確地確認差異、突顯潛在風險區域

- Classify
- Summarize
- CrossTabulate
- Stratify
- Age
- Benford

比對資料

- Join Unmatch & Match
- Compare
- Relate Table

異常資料分割與匯出

- Extract
- Export

資料排序

- Sort
- Index

重複/缺漏

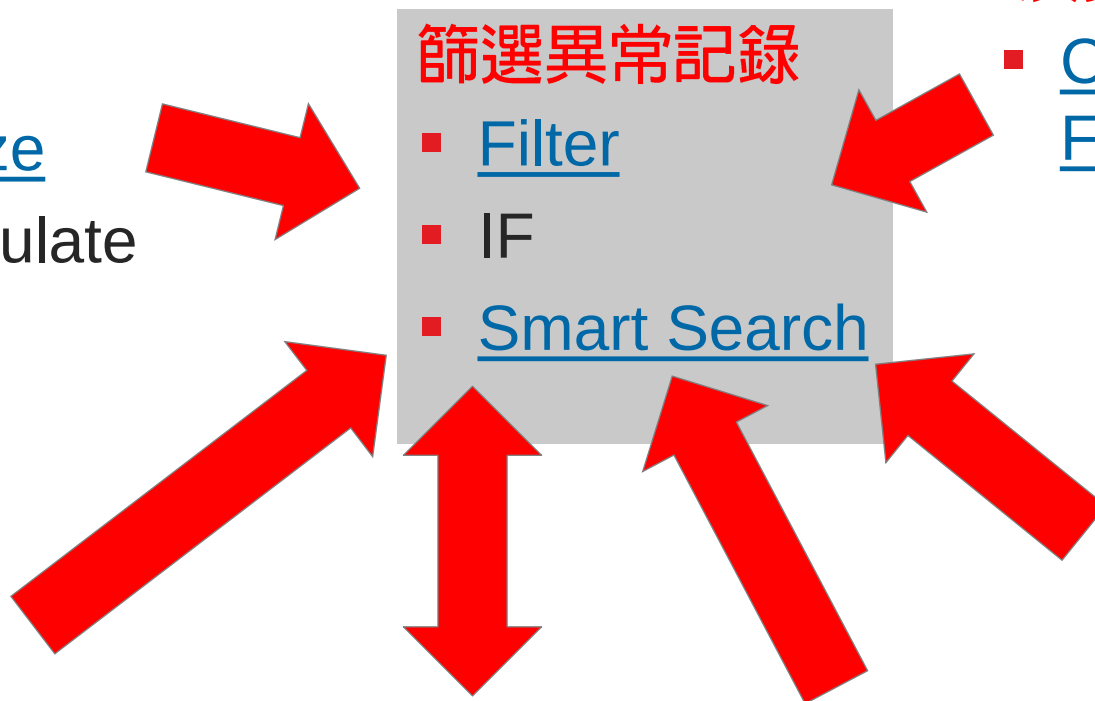
- Duplicate
- Gap

演算欄位

- Computed Field Exc

篩選異常記錄

- Filter
- IF
- Smart Search

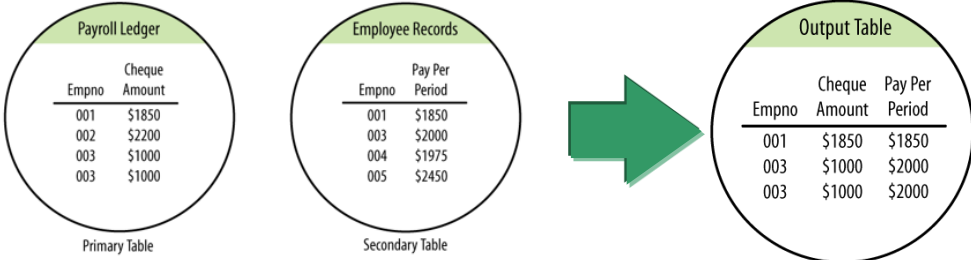


資料分析與測試

Data Analysis Cycle –Data Analysis

合併比較與聯結

聯結比對/Join



關聯/Relation

This screenshot shows a software interface for selecting join types. It features a list of join types on the left and their corresponding Venn diagrams on the right. The join types include: '選擇聯結類型', '與主要資料表紀錄相符', '主要關鍵欄位', '選擇(C)...', '次要關鍵欄位', '選擇(H)...', '與主資料表相符及所有主要資料表紀錄', '與主資料表相符及所有次要資料表紀錄', '與主資料表相符及所有主和次要資料表紀錄', '與主要資料表紀錄不相符', '與主要資料表相符的多對多紀錄', and '包含所有主要和次要資料表的多對多紀錄'. The Venn diagrams show the intersection of two sets, P and S, with different shading patterns representing the join results. Red checkmarks are placed next to the first, fourth, fifth, and sixth diagrams.

This screenshot shows a software interface with a list of relations on the left and a table of data on the right. The list of relations includes 'AR (父欄)', 'amount (N)', 'date (D)', 'DD', 'due (D)', 'Included_Tax (N)', 'MM', 'no', 'Period', 'ref', 'type', 'VAT (N)', and 'TY'. The table of data has columns 'Empno', 'Cheque Amount', and 'Pay Per Period' with data rows (001, \$1850, \$1850), (003, \$1000, \$2000), and (003, \$1000, \$2000). The interface also includes buttons for '資料表(A)', '完成(F)', and '說明(H)'.

This screenshot shows a software interface with a list of relations on the left and a table of data on the right. The list of relations includes 'AR (父欄)', 'amount (N)', 'date (D)', 'DD', 'due (D)', 'Included_Tax (N)', 'MM', 'no', 'Period', 'ref', 'type', 'VAT (N)', and 'TY'. The table of data has columns 'Empno', 'Cheque Amount', and 'Pay Per Period' with data rows (001, \$1850, \$1850), (003, \$1000, \$2000), and (003, \$1000, \$2000). The interface also includes buttons for '資料表(A)', '完成(F)', and '說明(H)'. A red box highlights the text 'Arbutus Compare / 比較'.

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
 - » 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

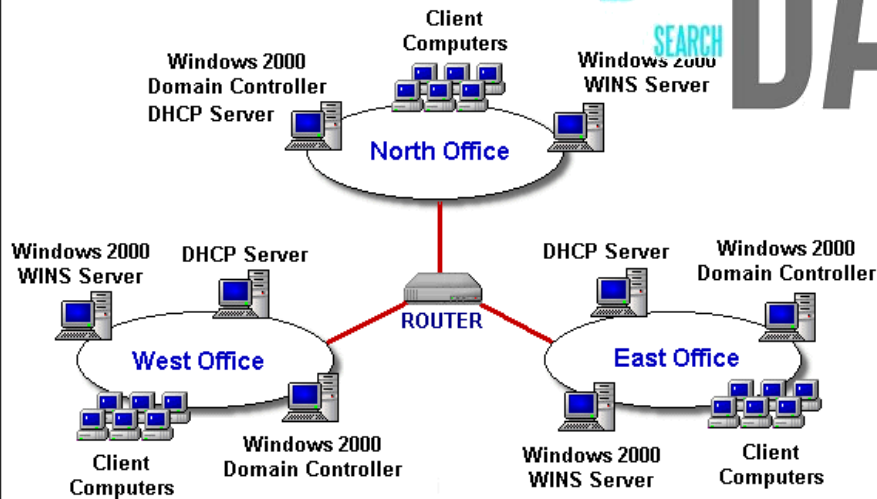
Cost of Revenues

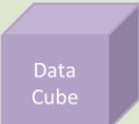
Gross Margin

Investments

Operating Income

Word cloud terms: COMPLEX ANALYTICS, BIOLOGICAL, HUNDREDS, WORKS, CAPACITY, USED, NEW, DIRECT, BIBER, HUBS, PROCESS, SET, USE, CONTINUES, F

[illegible]

企業資訊系統	ETL工具	資料管理	BI應用	使用者
			 數位儀錶板 動態報表	營運策略 

擷取與定義原始資料能力

Data Analysis Cycle – Data Access

文字檔(Text File)

010102840 PRESSURE COOKER	123	49.95	39.95	21.07
010119040 BLANCHER	72	27.00	24.95	15.50
010134420 VEGETABLE STEAMER	67	19.95	14.95	9.87
010135060 192 OZ DUTCH OVEN	75	29.95	26.50	22.00
010155150 STEP-ON CAN	24	14.95	9.95	6.50
010155160 1 SHELF BREADBOX	97	27.50	24.95	18.00

資料庫(dBase, Oracle, Sybase) - ODBC

Vendor Number	Invoice Number	Invoice Date	Invoice Amount	Product Number	Quantity	Unit Cost
10025	234056	09/30/2000	486.00	10228620	45	10.80
10025	230592	09/30/2000	850.58	10102710	142	5.99
10025	239215	09/30/2000	278.04	10155160	28	9.93
10025	237936	01/31/2000	56,767.20	80102618	3,379	16.80
10025	232195	11/14/2000	965.77	80930898	323	2.99
10101	4517604	10/30/2000	154.00	93788411	110	1.40

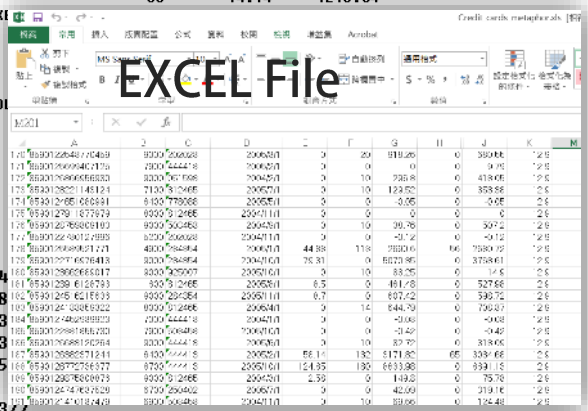
報表檔(Report file)

01/08/01
09:44:42

Inventory Valuation Report
As At December 31, 2000

Page 1

	Quantity	Unit Cost	Total Cost
Product Class: 01 - Housewares			
010102710 ALUMINUM TEAPOT 8 CUP	144	5.99	862.56
010102840 PRESSURE COOKER 8QT	400	39.40	15760.00
010119040 BLANCHER	190	8.00	1520.00
010134420 VEGETABLE STEAMER	50	3.12	156.00
010135060 192 OZ DUTCH OVEN	230	27.60	6348.00
010155150 STEP-ON CAN	132	8.40	1108.80
010155160 1 SHELF BREADBOX	56	9.93	556.08
010155170 4 PC CANISTER SET	96	7.05	676.80
010207220 NAPKIN & RELISH HOLDER	212	3.22	682.64
010226620 CAKE DECORATING SET	48	10.80	518.40
010310890 HINCR	86	14.14	1216.04
010311800 PASTA NOODLE MAKER			
010311990 DIET SCALE			
010551340 DISH DRAINER			
010631140 CAKE PAN			
010631190 LOAF PAN			
010803760 7 PC KITCHEN TOOL			
Class Totals:			



Web Log File

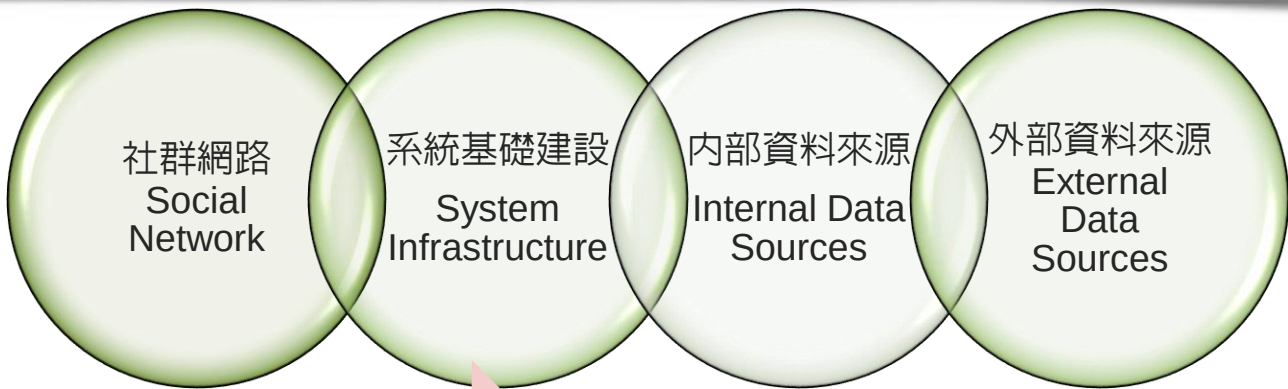
193.63.247.66 - - [24/Apr/2000:03:02:45 -0800] "GET /globlnav.gif HTTP/1.0" 200 1739 D= 3304
203.80.120.148 - - [13/Mar/2000:00:39:46 -0800] "GET /index.html HTTP/1.0" 200 12449 D= 1098
203.30.7.130 - - [12/May/2000:02:18:13 -0800] "GET /wh_text.gif HTTP/1.0" 200 1797 D= 285573
194.98.47.110 - - [19/Nov/2000:05:17:29 -0800] "GET /getacro.gif HTTP/1.0" 200 909 D= 129883
193.45.187.5 - - [25/Sep/2000:04:11:39 -0800] "GET /press.10.gif HTTP/1.0" 200 11256 D= 2265
198.82.152.48 - - [19/Apr/2000:05:23:58 -0800] "GET /banner3.gif HTTP/1.0" 304 72 D= 307523
196.26.83.226 - - [16/Jul/2000:01:22:57 -0800] "GET /10yr_lgo.gif HTTP/1.0" 200 2258 D= 213377
202.45.188.25 - - [16/Nov/2000:02:11:33 -0800] "GET /sitemap.gif HTTP/1.0" 200 1891 D= 58304
195.75.80.131 - - [15/Oct/2000:03:58:44 -0800] "GET /wh_text.gif HTTP/1.0" 200 1821 D= 160623
210.132.194.198 - - [13/May/2000:05:03:34 -0800] "GET /globlnav.gif HTTP/1.0" 200 1763 D= 90719
194.92.216.111 - - [11/Nov/2000:02:12:09 -0800] "GET /demo/acl_english.exe HTTP/1.0" 200 1700893 D= 181912
196.29.32.113 - - [27/Dec/2000:04:09:04 -0800] "GET /globlnav.gif HTTP/1.0" 200 1763 D= 118259



```
"employee_number","Name","ID","department","Position","Address","manager","BankAccount","Expense_claim_report_amount"  
"010183","李明月","E192340929","Development","Specialist, Development","竹北市三民路548號3樓","000476","1620519223405",0  
"000184","姚學雲","G193594110","Consulting","Specialist","基隆市中正區中正路330號","000375","6020519335905",50553  
"000190","陳曉紋","D193167898","Consulting","Consultant","基隆市仁愛區仁二路19號","000375","1010519331605",0  
"000193","李瑞婷","B296949123","Consulting","Consultant","基隆市仁愛區光二路1號","000375","2110529669405",0  
"000195","陳佩珊","H193541316","Consulting","Senior Consultant","基隆市安樂區樂利三街261號","000375","2120519335405",0  
"000196","邱建豪","E294347311","Training","Manager, Personnel","新竹市香山區五福路2段707號","000634","2050529443405",0  
"000198","顏子豪","E198761637","Support","Cashier","桃園縣中壢市私立中原大學內","000324","2500519887605",0  
"000200","李宜昆","D199492729","Development","Specialist, Development","新竹市經國路一段442巷9號","000476","6110519994905",0  
"000201","張威隆","G192386669","Support","Sales Support","桃園縣中壢市元化路2段126號","000324","5490519223805",0
```

Delimited File

資訊來源
Information Sources



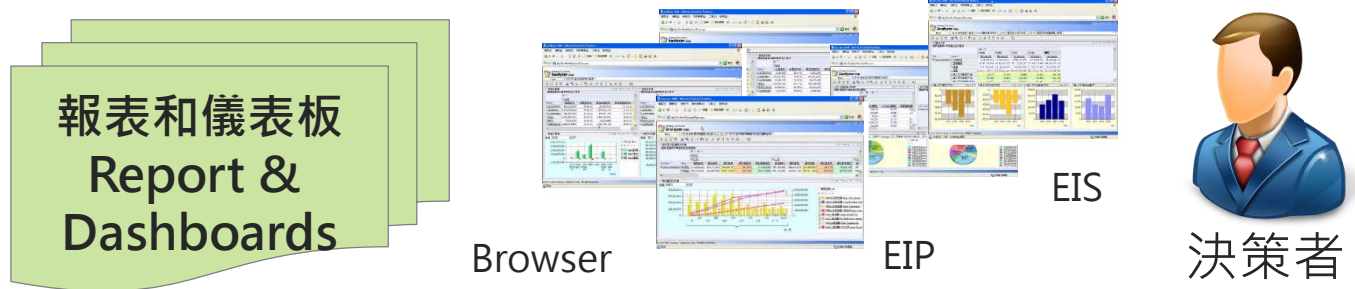
擷取,轉換,
和載入
ETL



分析方案
Analytics Solutions



要求洞察
Required Insights





決策者

收集那麼多資料給我做什麼？

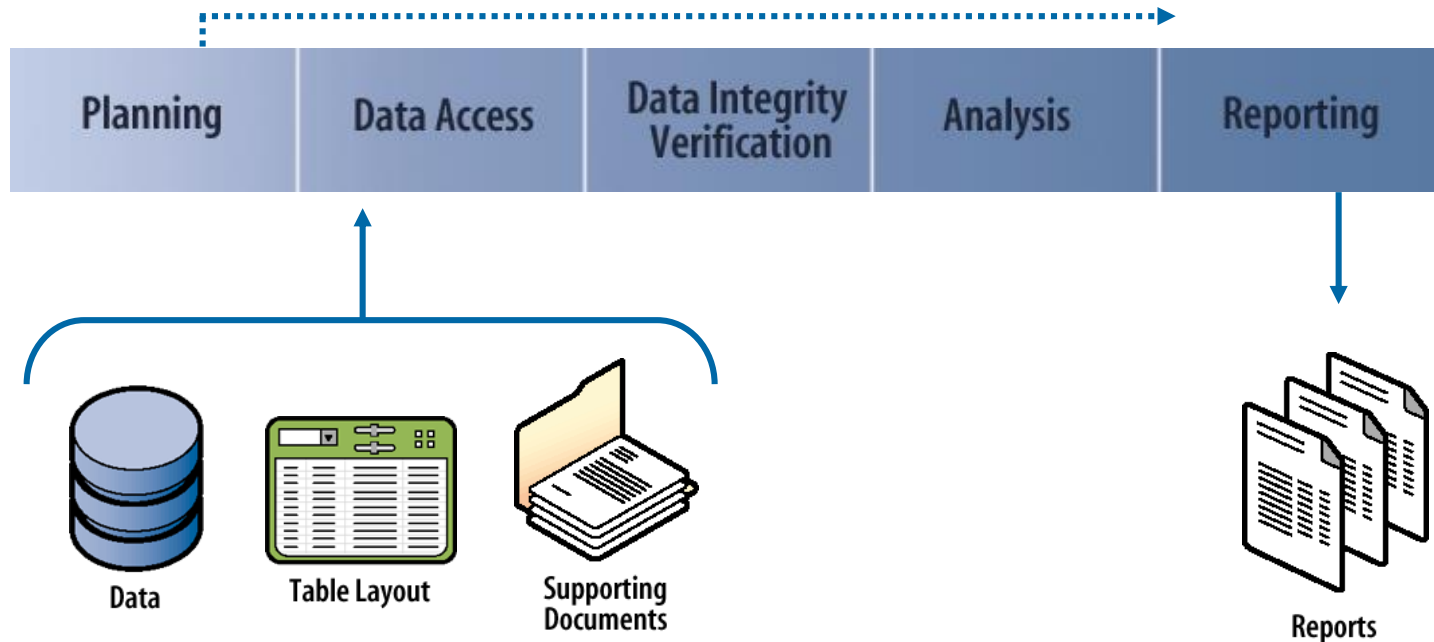
Create Value/創造價值

- Reporting/向上級報告
- Monitoring/營運監控
- Data Quality Assurance/資料品質確保
- Compliance and Audit Assurance/合規與稽核確認

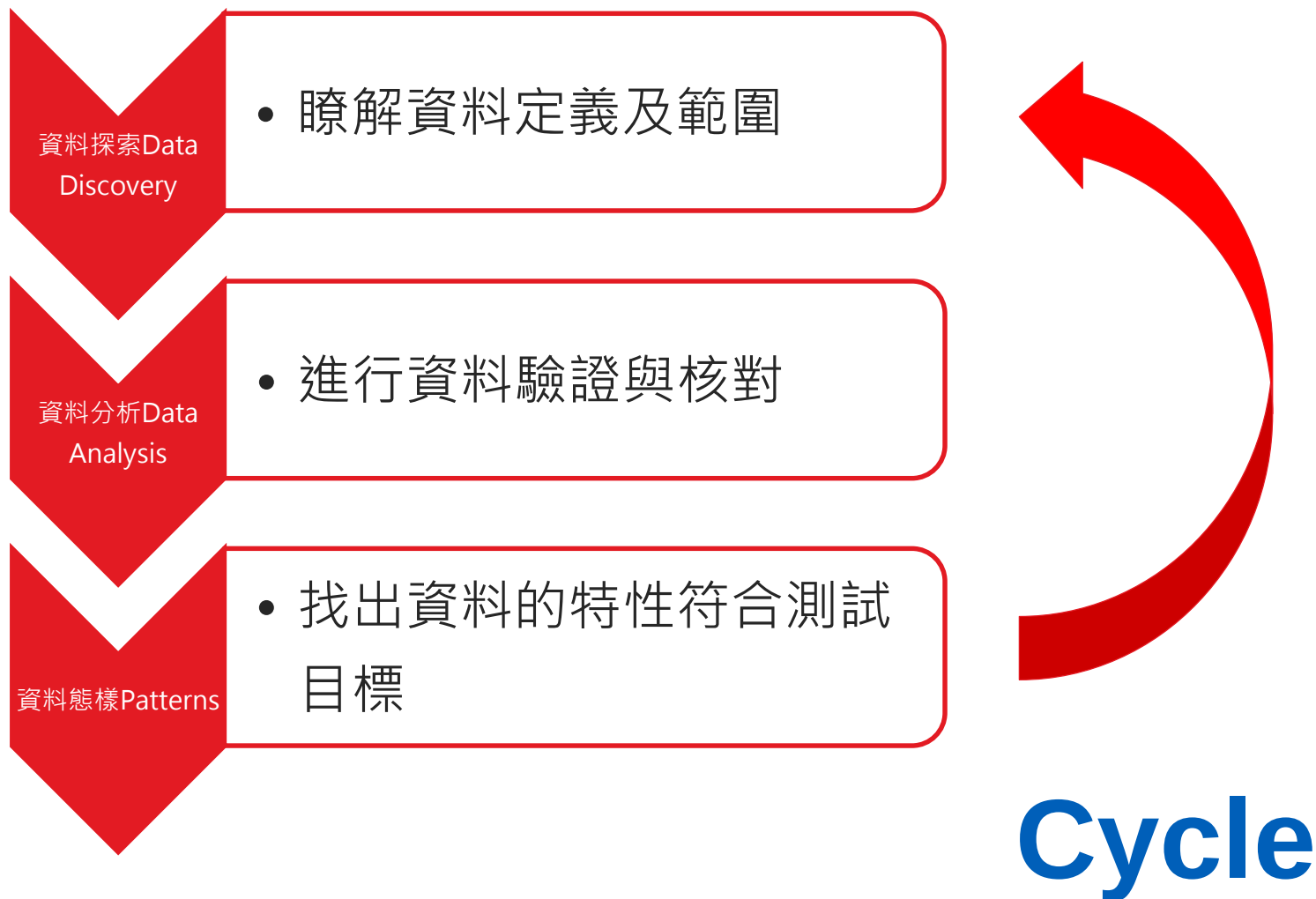


資料分析循環(The Data Analysis Cycle)

- 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)



Data Analysis Roadmap



Data Analysis – Critical for Your Audit Function



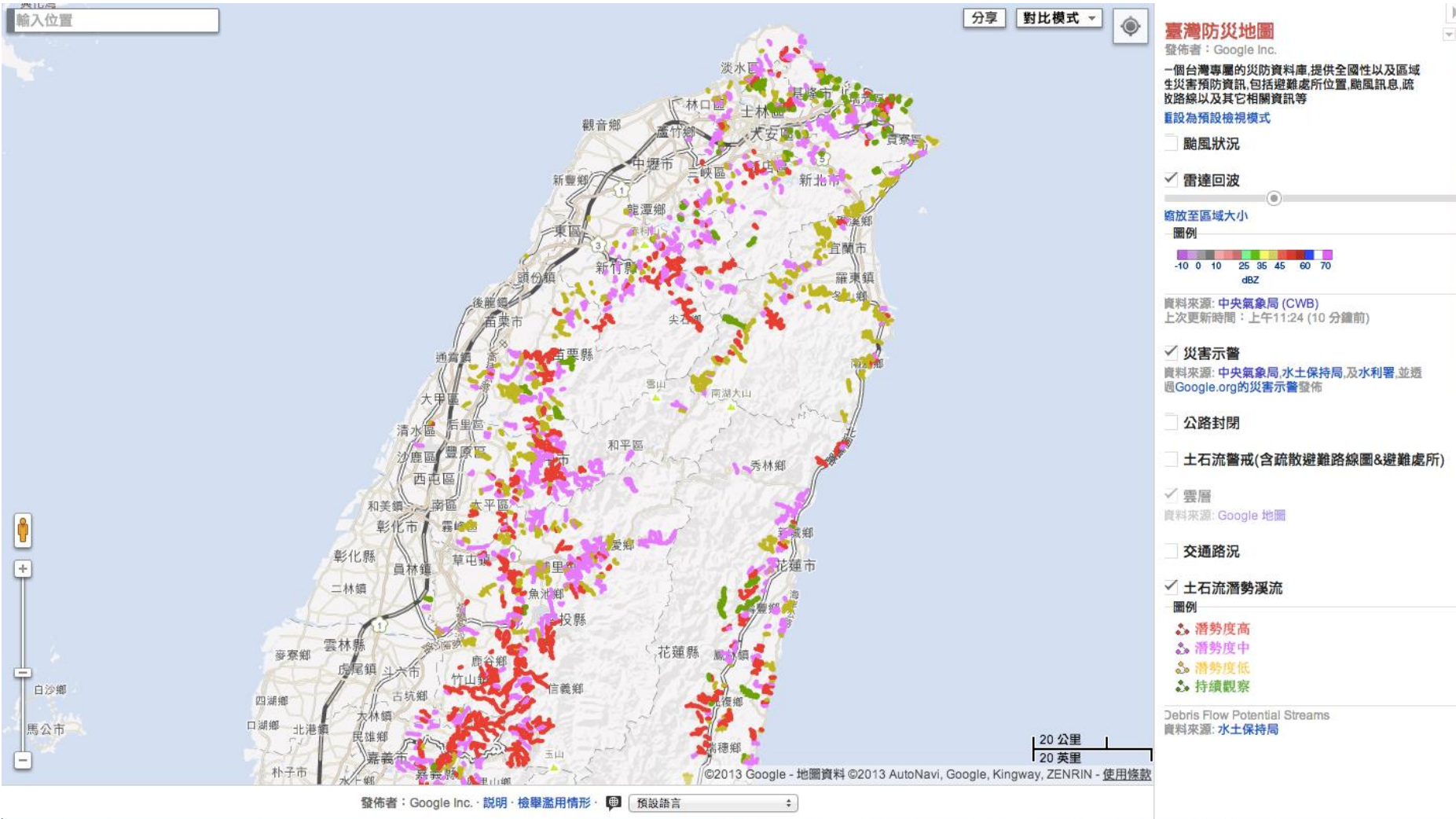
Internal audit's data analytic capabilities, instrumental to effectively examining the large volumes of data readily accessible through ERP systems for anomalies and other fraud indicators, are now even more critical.



State of the Internal Audit Profession Study
2009

風險評估和持續性稽核與監控作業

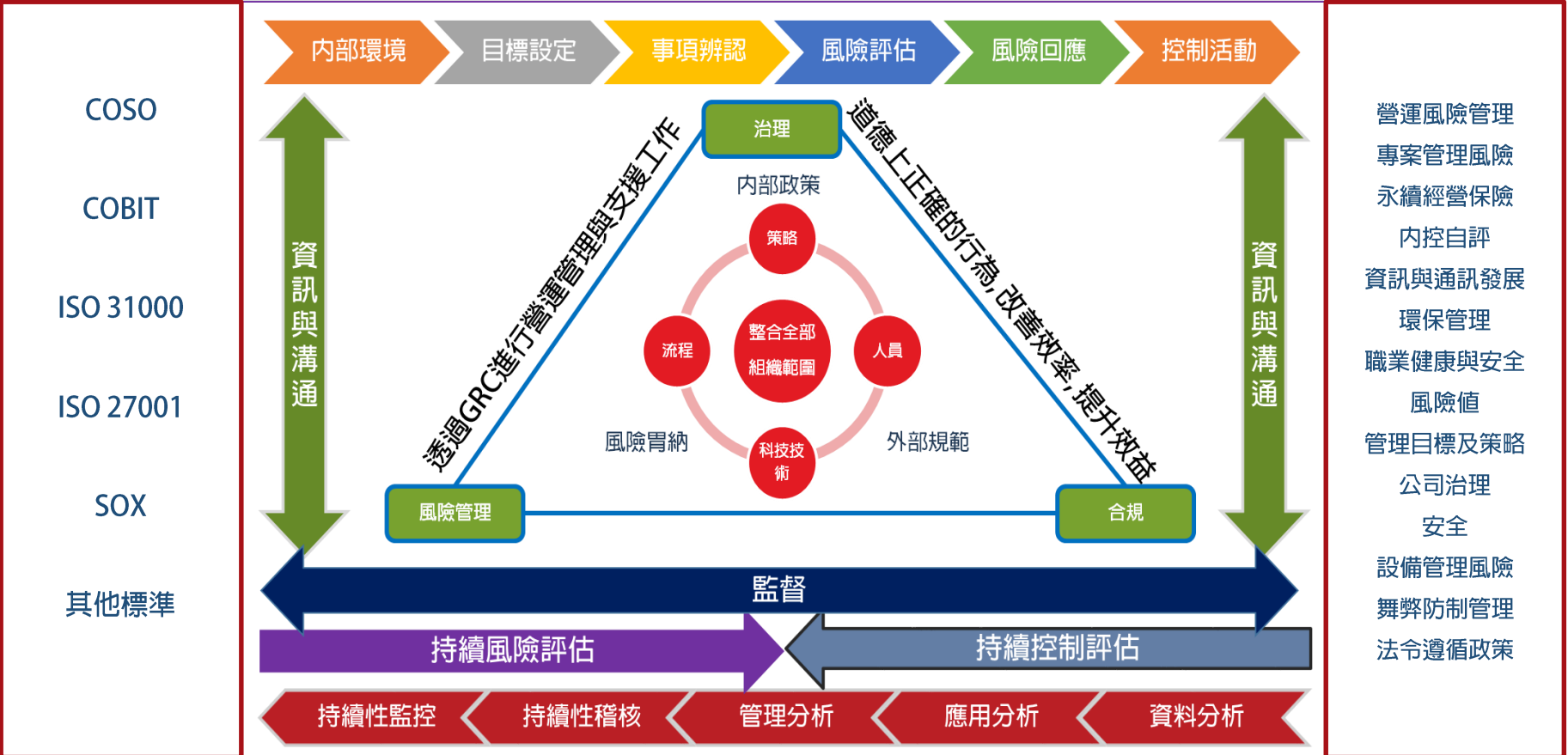
Where are your risk area?



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

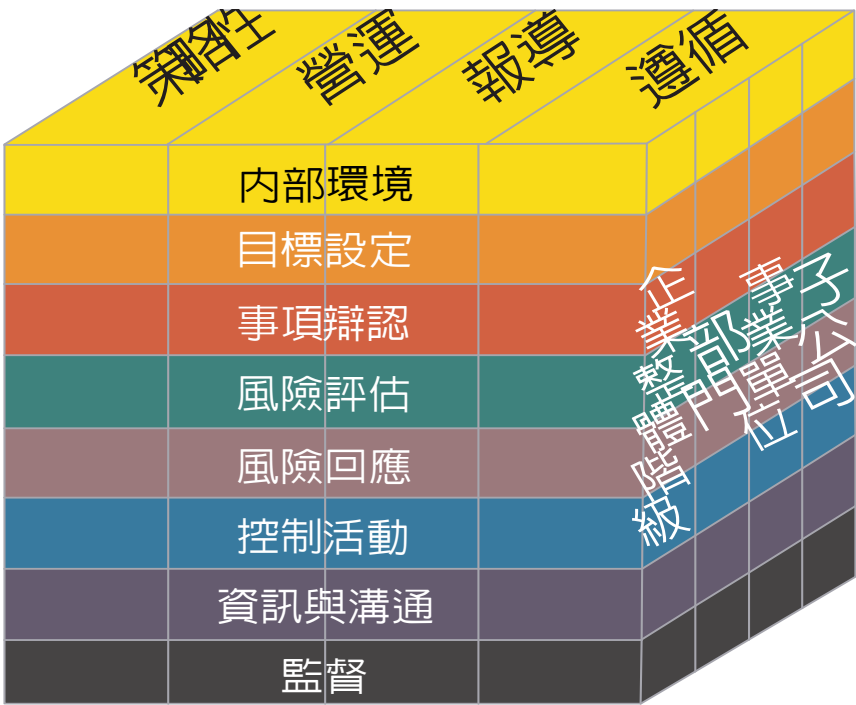
Pentana Vision 風險與稽核管理系統



Arbutus Software 營運確保分析技術

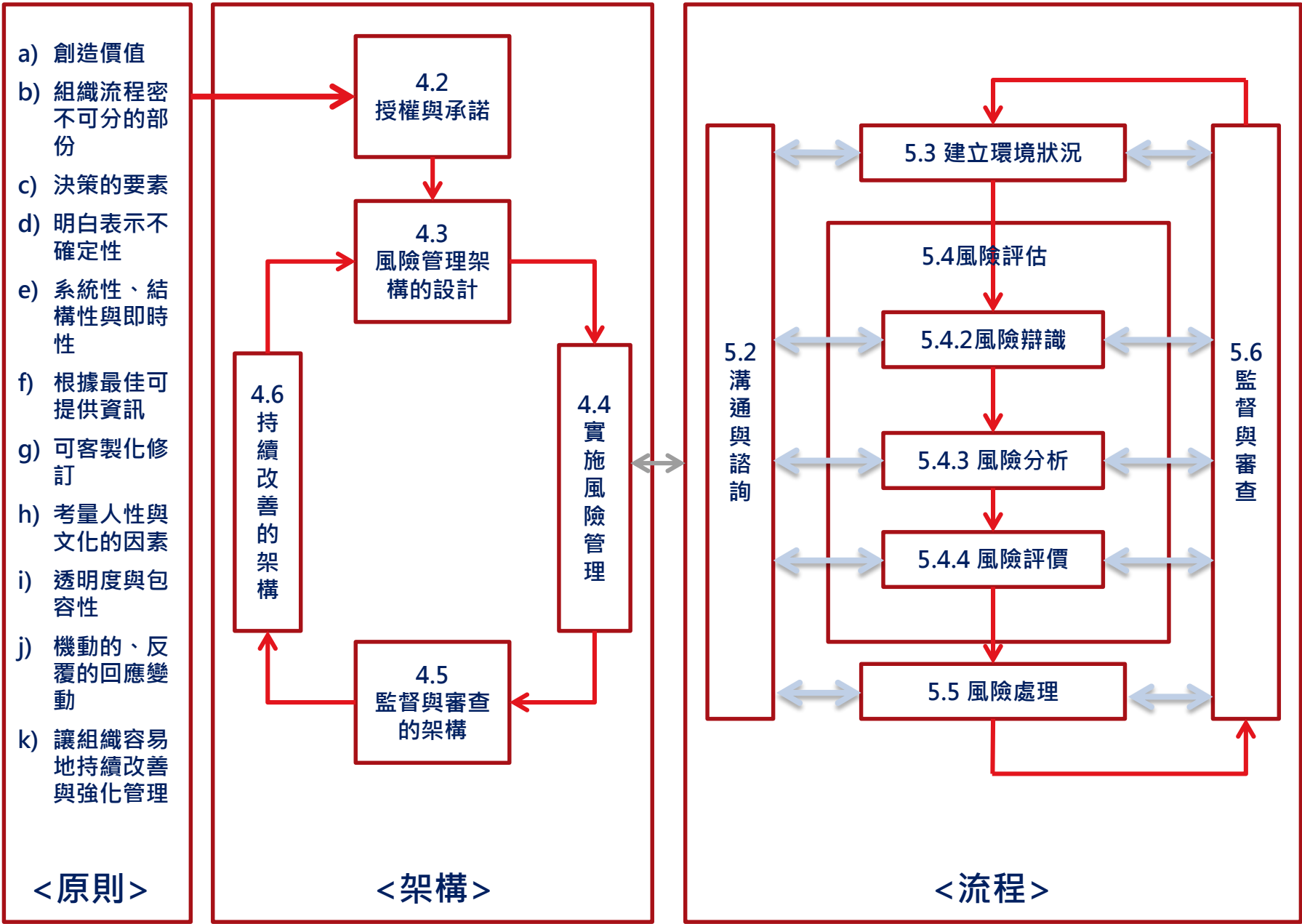
ERM企業風險管理整合架構(COSO)

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。

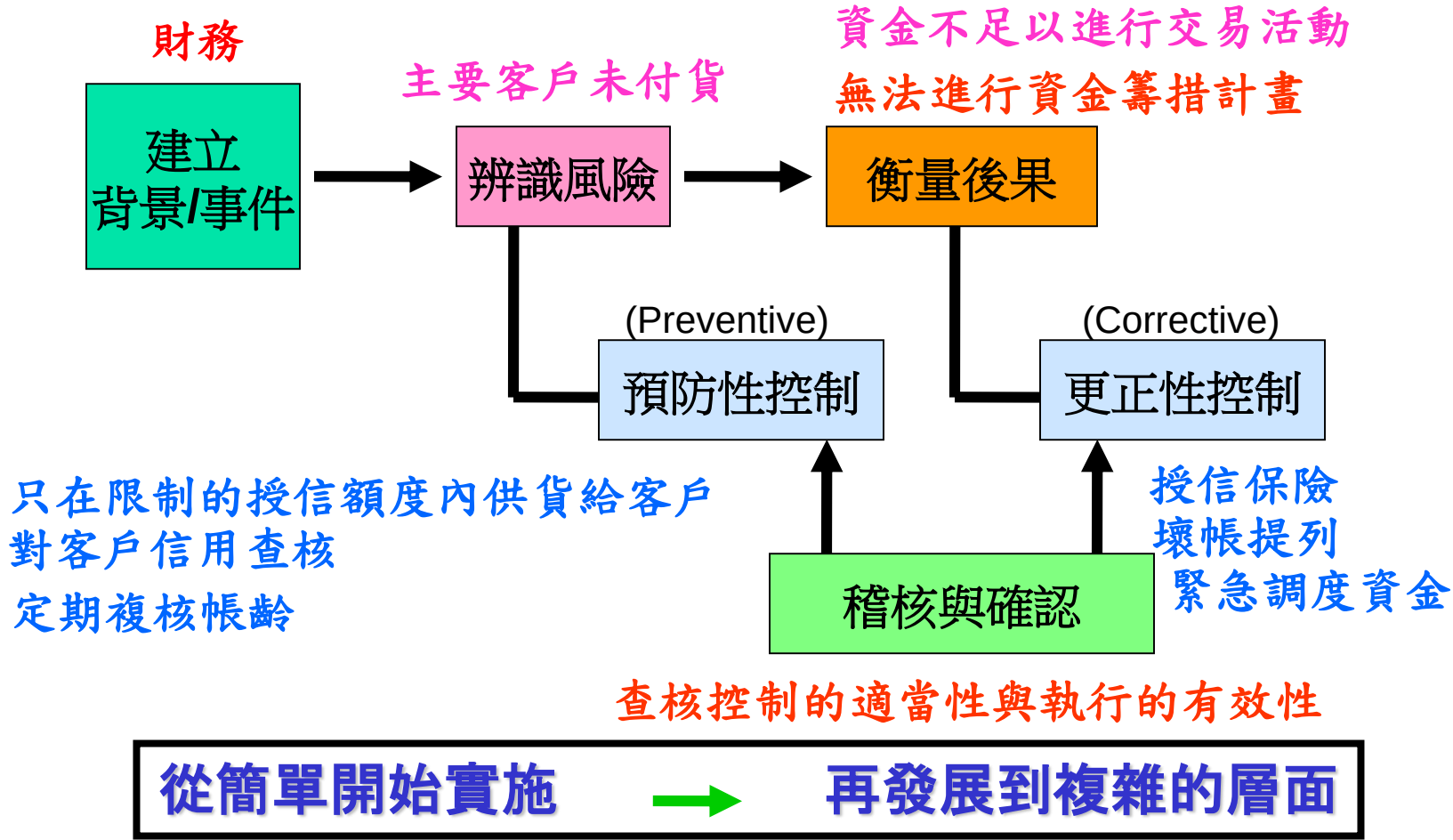


Source: COSO Enterprise Risk Management – Integrated Framework, 2004. COSO. 及企業風險管理－整合架構：馬秀如博士等譯

ISO31000:風險管理原則、架構和流程關係圖



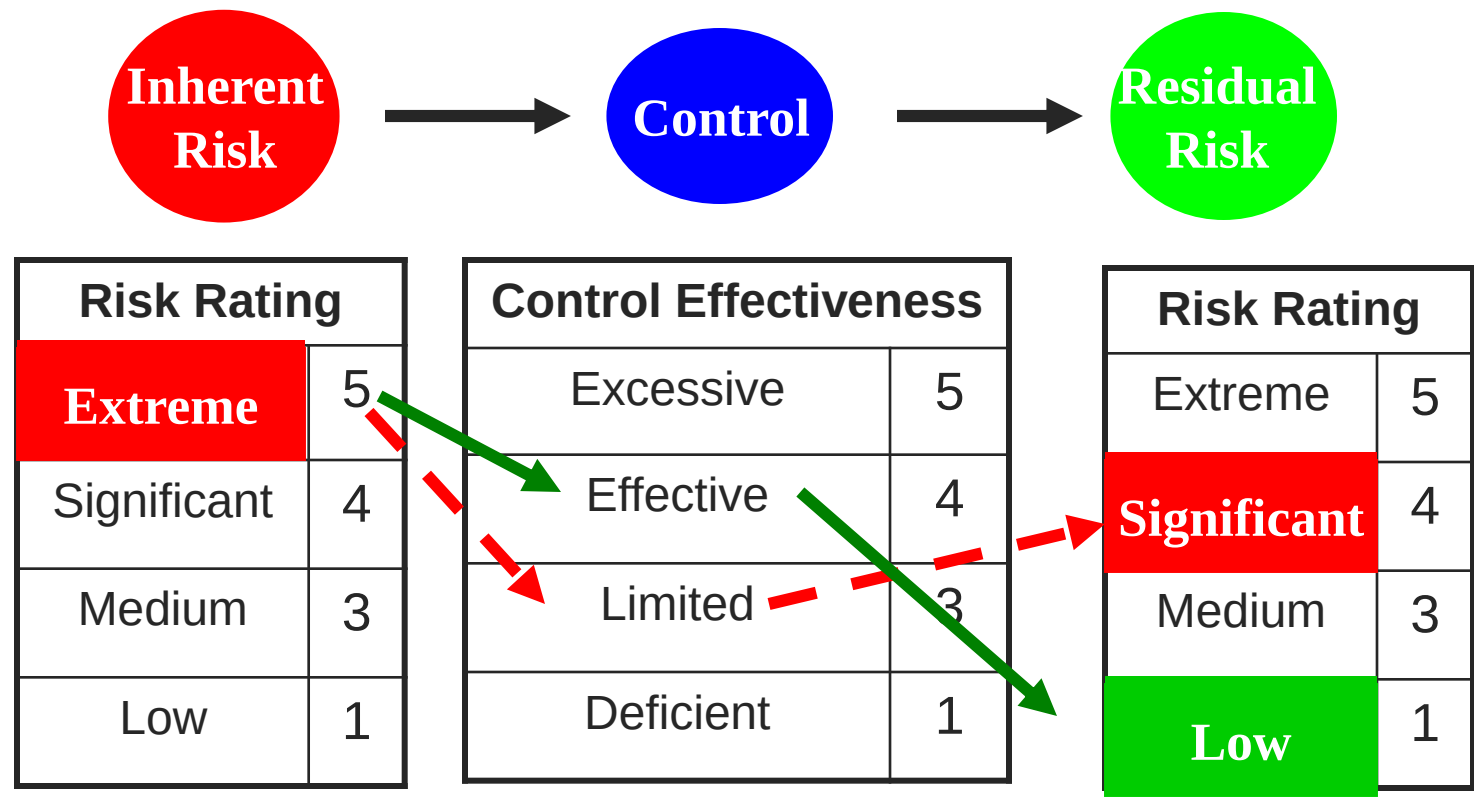
風險管理方法



根據澳洲/紐西蘭 AS/NZ 4360 風險管理框架

Key Concepts.....

Moving focus from inherent to residual levels

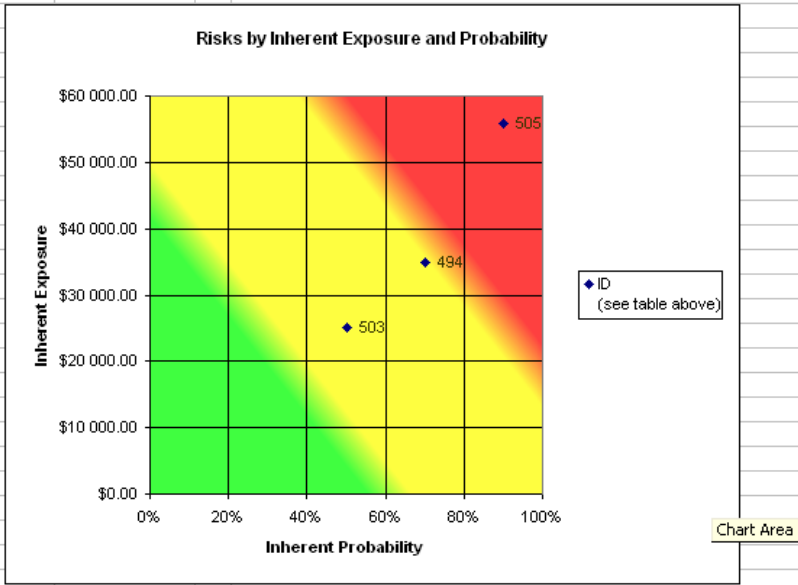


Risk management methods need to vary

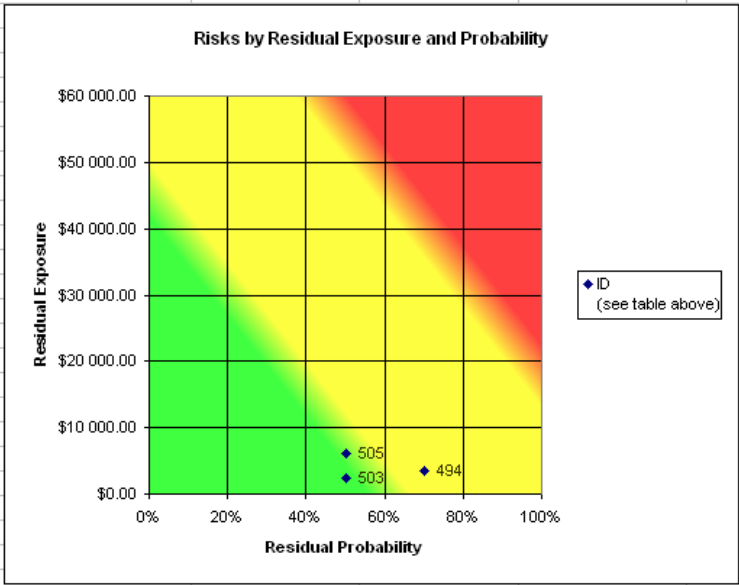
Key Concepts.....

Risk Grid Report Before & After Controls

Risk Category	ID	Risk Description	Inherent Probability	Inherent Exposure	Residual Probability	Residual Exposure
Banking Risks	505	Passwords have been compromised in settlements by being obtained in an unlawful/unauthorised manner	90%	\$55 800.00	50%	\$6 200.00
Banking Risks	503	Inaccurate and/or incomplete information is provided to the credit system.	50%	\$25 000.00	50%	\$2 500.00
Cashflow/Liquidity	494	Key customer who owes us money (i.e. a debtor) fails	70%	\$35 000.00	70%	\$3 500.00



before controls



after controls

Items in the red area require immediate attention.

Risk Assessments

稽核

風險註冊

目標設定

風險事項辨識

控制項目

風險評估

查核測試作業

控制有效性評估

稽核工作

稽核詳細資訊

指定 Staff

工作計畫

風險註冊

風險矩陣

控制矩陣

全域

分析

稽核工作

資料庫

管理員

Pentana

Pentana Vision (Standalone) - Built 13/01/2012 11:36 PM

目標

風險

控制項

顯示

評估

增加 審查

增加 Point

設定為 In Scope

設定為 Out Of Scope

目標

OTC1 - 銷售作業 (4 items)

出貨作業 (Shipping) (1 item)

OTC1-4 - 履行客戶訂單的需求

OTC1-4-1 - 出貨時不正確地記錄與入帳, 以致帳上難以沖轉

OTC1-4-1-1 - 僅經授權人員依核准之出貨文件入帳

56 - 檢視系統權限, 評估出貨人帳權限成員的設定是否適當

57 - 驗證系統是否僅針對具有相關核准文件之出貨才能入帳

OTC1-4-2 - 送到客戶端的貨品不符合訂單要求之規格

OTC1-4-2-1 - 依客戶訂單內容直接產生檢貨單, 且其檢貨明細無法自行更改

58 - 驗證檢貨單內容是否自動從客戶訂單帶出, 無法自行更改

59 - 檢視檢貨文件類型與訂單之參照設定是否適當

OTC1-4-2-2 - 檢查已檢貨及裝箱的貨品, 以確保其一致

OTC1-4-3 - 客戶沒收到貨

OTC1-4-3-1 - 於系統中設定出貨確認程序, 當客戶收到貨則進行出貨的確認與結清

61 - 檢視與評估系統出貨確認程序是否有效設定與執行

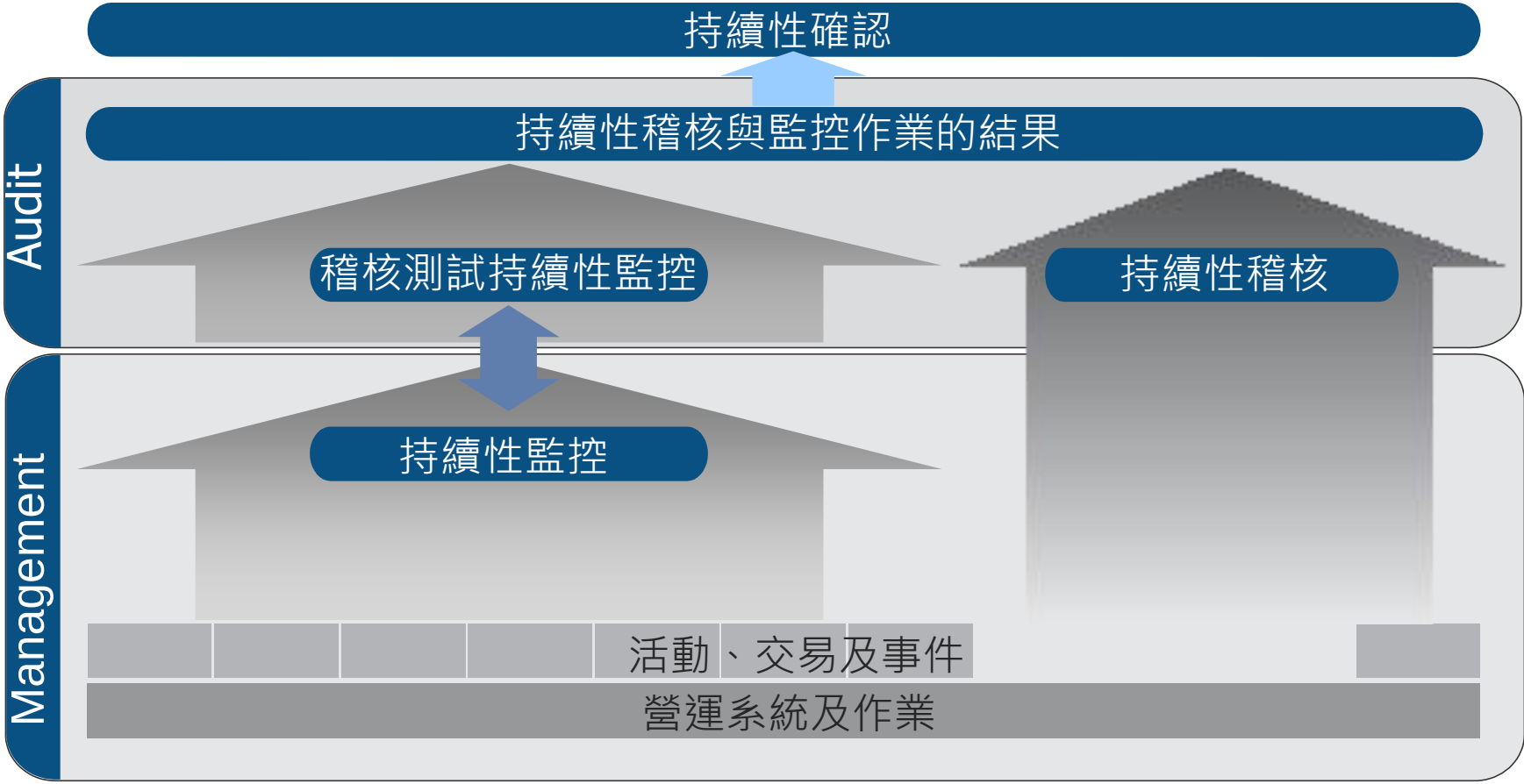
OTC1-4-3-2 - 檢查裝箱的貨品, 以確保提出貨商品已正確裝箱

OTC1-4-4 - 客戶訂單的修改無法即時反應

負責	類別	範圍	資料
Possible(可能)	Severe	High	
Adequately Designed	Partially Operating	Partially	
Probable(很可能)	Severe	High	
Well Designed	Fully Operating	Effective	
Well Designed	Partially Operating	Partially	
Very Probable(非常可能)	Severe	Very High	
Well Designed	Partially Operating	Partially	
Probable(很可能)	Moderate	Medium	

持續性監控、稽核與確認

Continuous Monitoring、Continuous Auditing、and Continuous Assurance



持續稽核、監控與確認(概念模式)

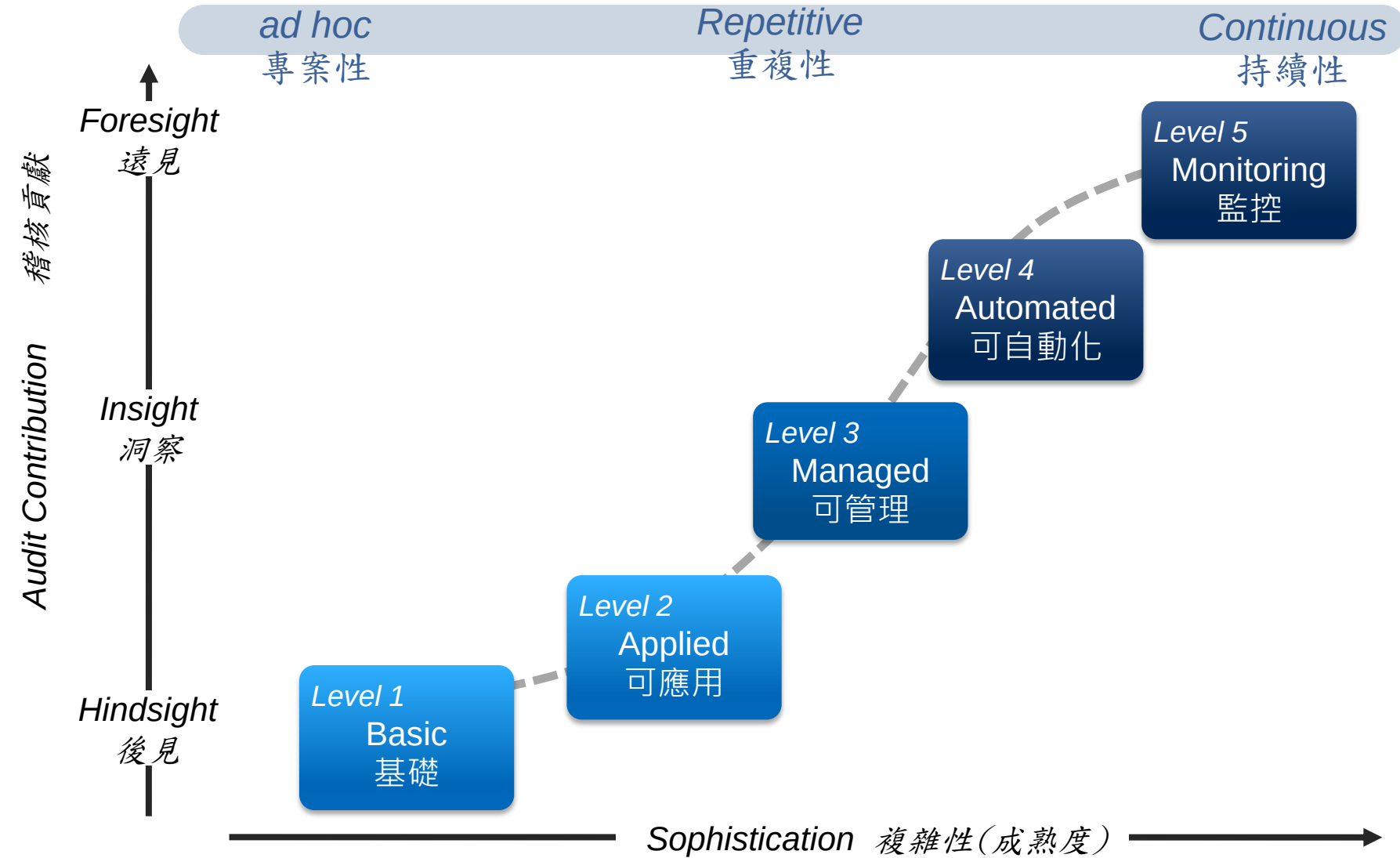
Ref: IIA Global Technology Audit Guide No.3: Continuous Auditing

持續性稽核的架構

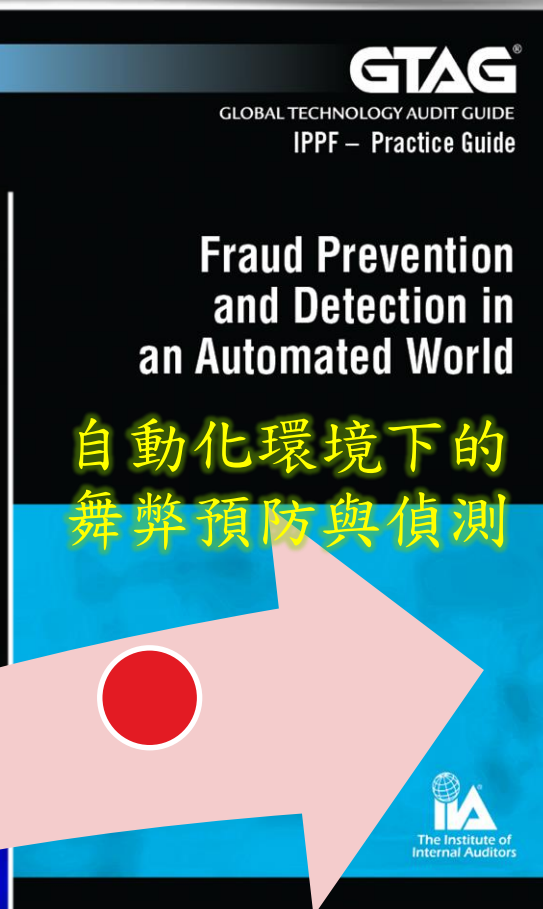
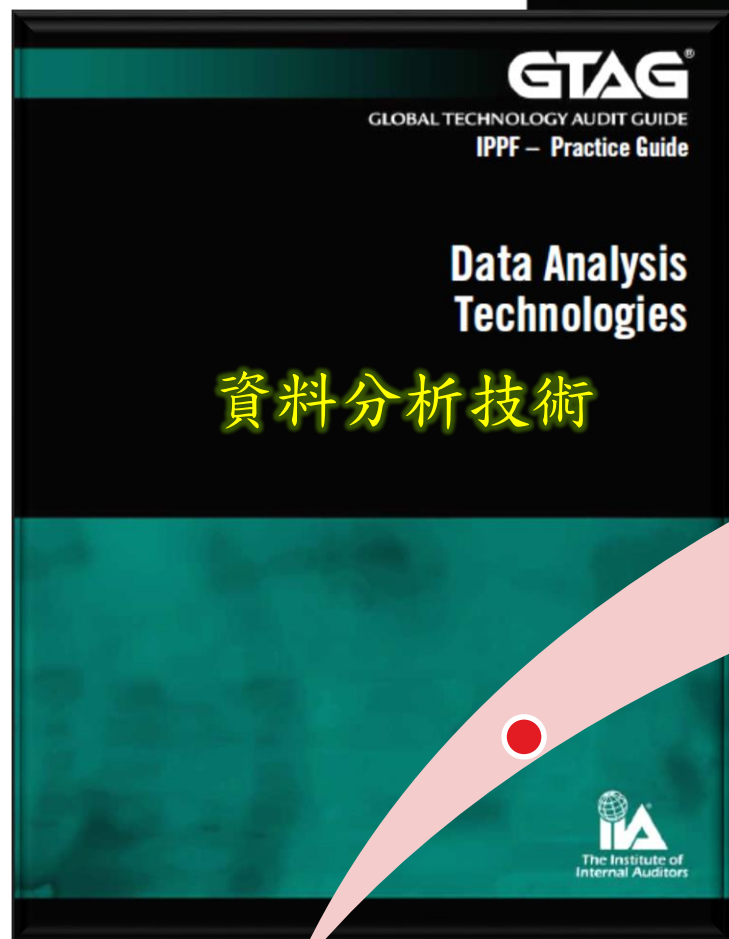
持續性稽核						
持續性控制評估		持續性風險評估				方法
控制導向為基礎 (確認性控制有效) 財務控制		風險導向為基礎 (風險辨識/評估) 財務/營運作業控制				重點
即時/詳細 交易測試 財務資料		趨勢/比較 財務/營運作業資料				分析技術
控制確認	財務證明	舞弊/浪費/濫用	稽核範圍與目標	查核建議 後續行動	年度稽 核計畫	相關稽核 作業活動
控制監控	績效監控	平衡計分卡	全面品質管理(TQM)	企業風險管理(ERM)		相關管理 活動



稽核分析能力成熟度模型



IIA GTAG全球科技查核指引



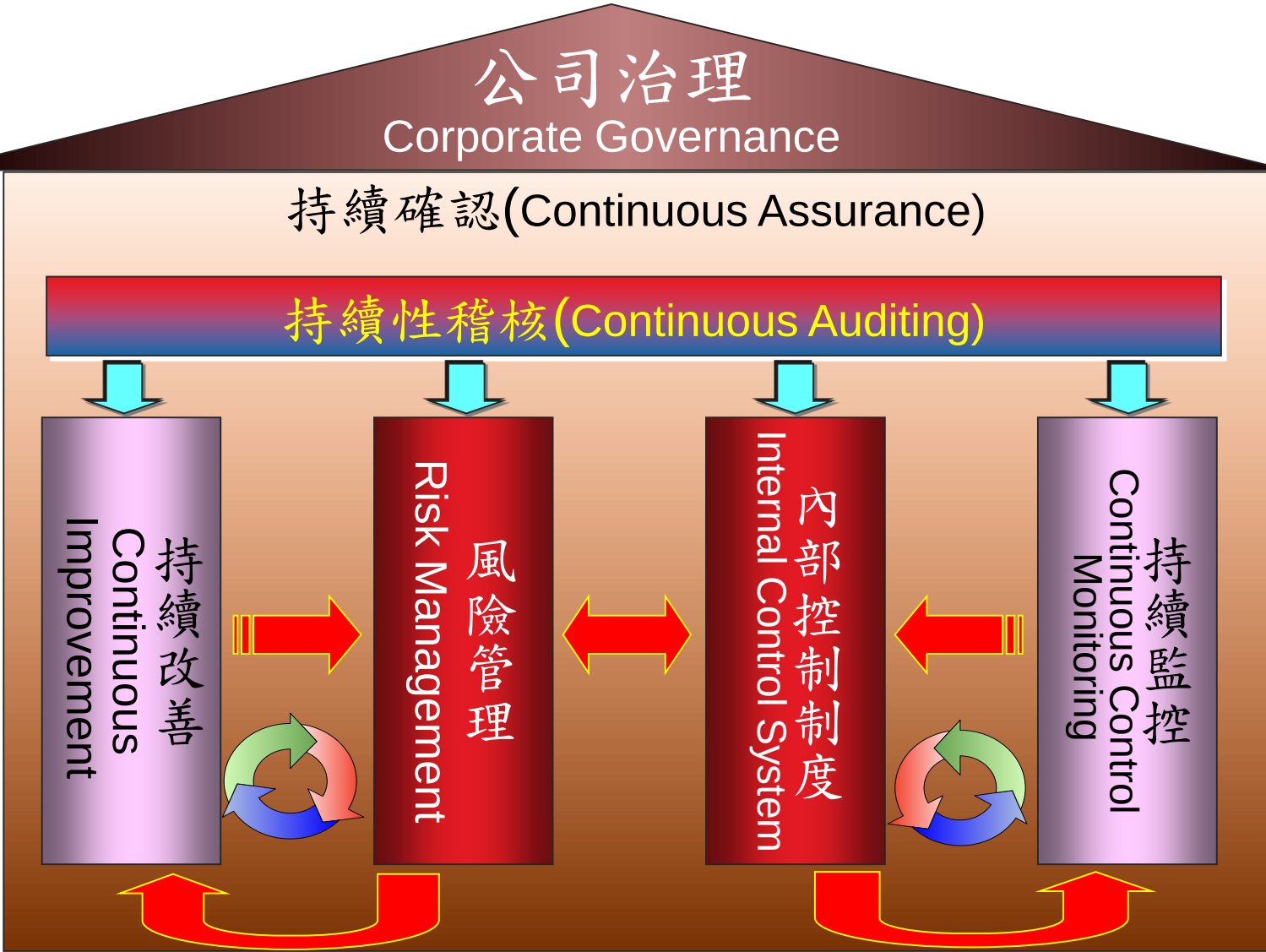
What do you **THINK** your current
'audit analytic capability' is?

你們認為：

你們現在的『稽核分析能力』在哪裡？

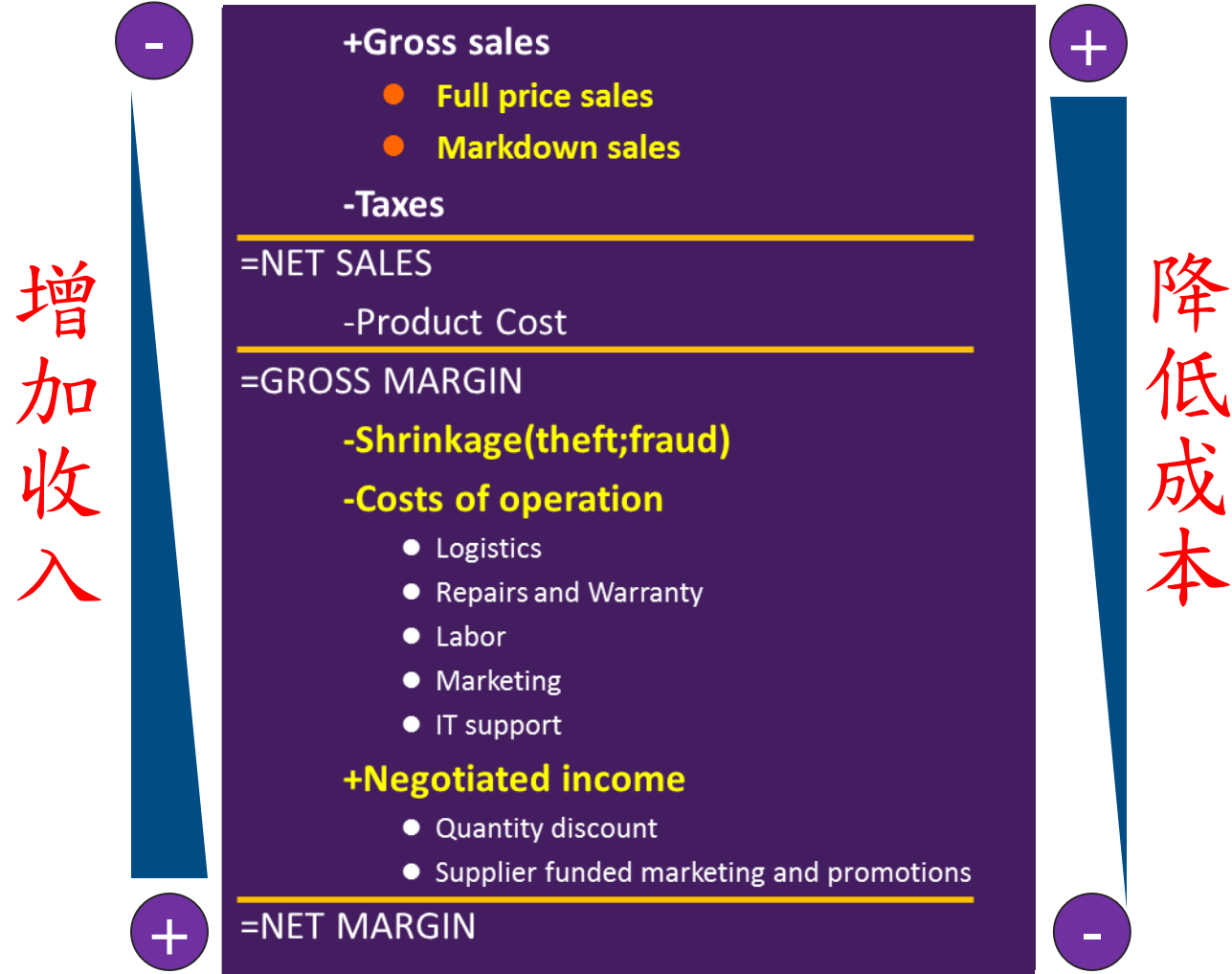
我們共同的目標

營運確保架構



Business Assurance

營運確保的目的



營運確保的實行重點 – Financial Value and Internal Control

Processes/ Operations

- ✓ Accounts Payable
- ✓ Audit
- ✓ Operations Costing
- ✓ Strategic Sourcing
- ✓ Supplier Management
- ✓ Category Profitability
- ✓ Inventory Management
- ✓ Transportation Management
- ✓ Reverse Logistics
- ✓ Promotion Evaluation
- ✓ New Product Evaluation
- ✓ Item/Category Profitability
- ✓ Channel Management
- ✓ Customer Profitability
- ✓ Service Level Pricing

BUSINESS AREAS



FINANCE

BUSINESS ASSURANCE

- Control Bill Backs Collection
- Control execution of payments terms
- Invoice Validation
- Control of utilities usage (communication s: energy: mobile phones)



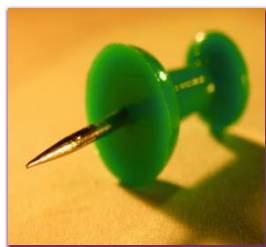
BUY

- Supplier Service levels
- Contract control
- Cost & Deal Management



SUPPLY CHAIN MARKETING

- Product Traceability
- Shrinkage visibility
- Measure employee productivity
- Out-of-stock



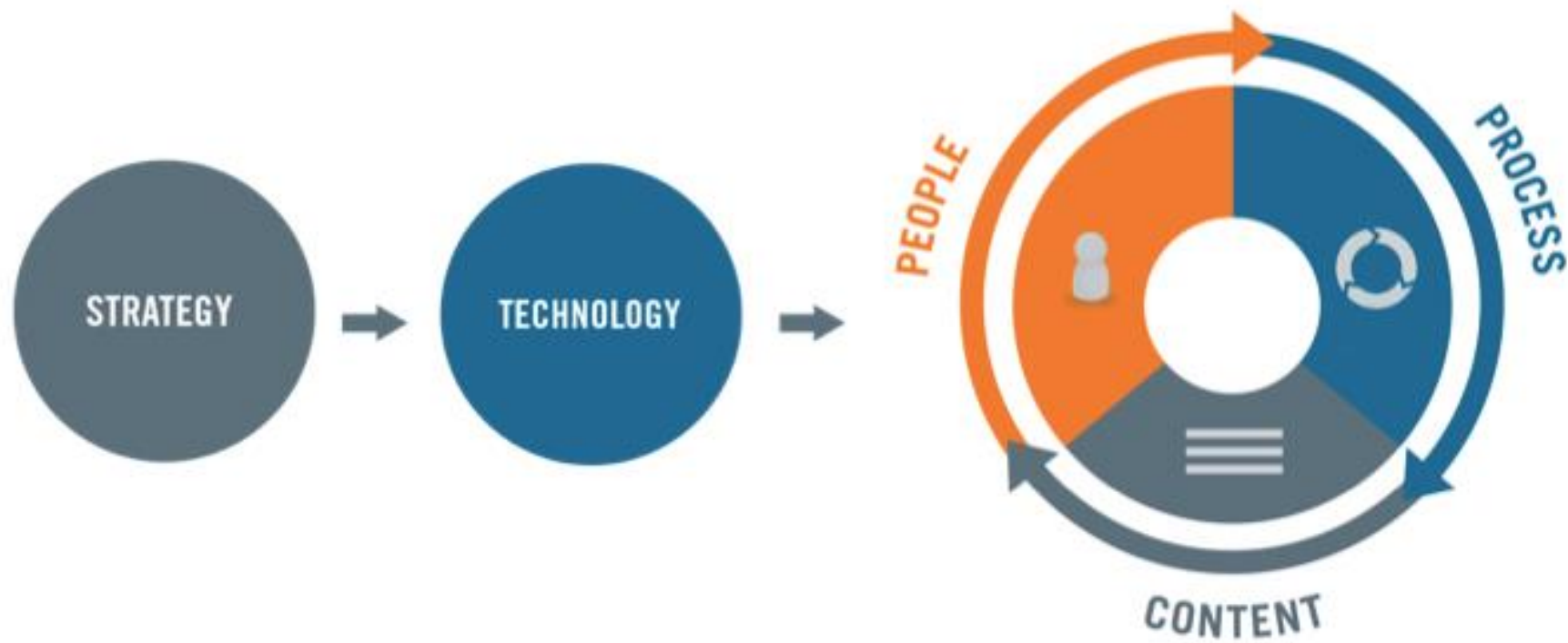
- Item lifecycle (de-listing control)
- Control Price Execution effectiveness
- Control execution of clusters of Assortment



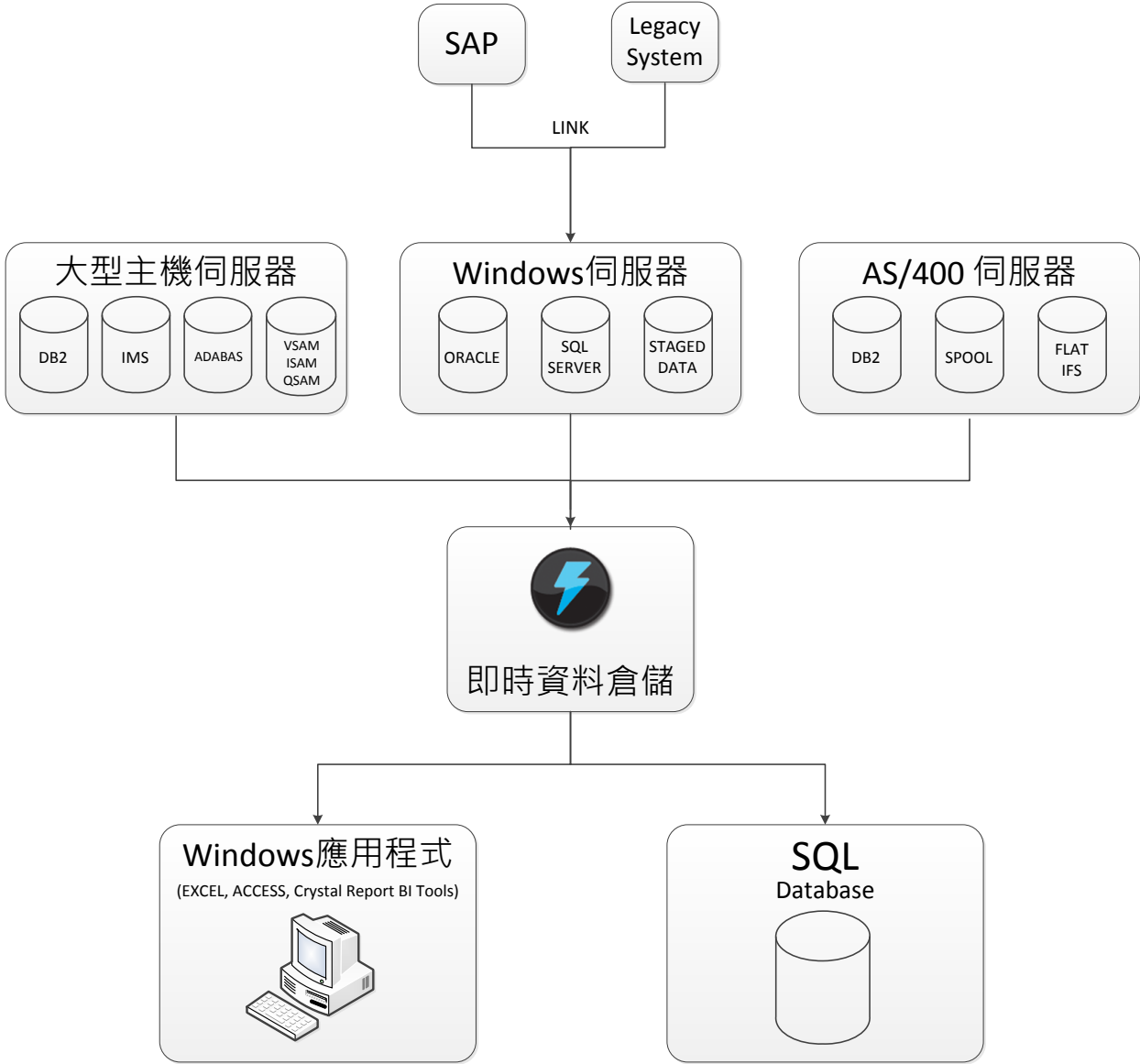
SALES

- Planogram execution
- Measure Cashier productivity
- Sales Analysis

持續性稽核實行步驟



即時資料倉儲 - Instant Data Warehouse



專案概觀

- UPGeneral [D]
- Accounts
- AP_trans
- Vendor
- Accounts_r
- AR2
- Badfile
- Custom
- Demo
- Duplica
- Trans
- Data
- Data Folder
- Inventory_review
- Payroll_analysis
- Empmast
- Payroll

MODCASE

- OS_Window_Hardening_Auditing
 - A00_Main_Script
 - A01_Set_Value
 - C00_DataAnalysis
 - C01_Q1_延遲返國、差旅費計算
 - C02_Q2_請購合理驗證
 - C03_Q3_採購合理性
 - C04_Q4_報表依權責發生制入帳
 - C05_Q5_資產管理有效性
 - C06_Q6_付款金額的正確性
 - C07_Q7_供應商主檔資料重複建立
 - C08_Q8_無對應供應商的採購資料

Vendor Number	Invoice Number	Invoice Date	
11663	5981807	11/17/2000	
13808	2275301	11/17/2000	
12433	6585673	11/17/2000	
11663	5983947	11/17/2000	
12130	589134	11/17/2000	
13411	49545947	10/30/2000	
12433	6585951	10/30/2000	
10721	123196	10/30/2000	
12433	6585880	10/30/2000	
13411	49540141	10/30/2000	
10787	591533	05/31/2000	
12	10534	58720114	05/31/2000
13	14913	8457230	05/31/2000
14	10534	58720114	05/31/2000

專案概觀

- UPGeneral [D]
- Accounts
- AP_trans
- Vendor2
- Accounts_receivable_audit
- AR2
- Badfile
- Customer
- Demo
- Duplicate_Train
- Trans
- Data
- Data Folder
- Inventory_review
- Payroll_analysis
- Empmast
- Payroll

MODCASE

- OS_Window_Hardening_Auditing
 - ProdServer
 - Purchase_to_Payment

E01_Requisition_Limits
E02_Split_Requisitions
E03_Unauthorized_Requisitions
E04_Requisition_Data_Validity
E05_Requisition_SOD
E06_Single_Purchase_Order
E07_Split_Purchase_Order
E08_Unauthorized_Purchaser
E09_Purchasing_Data_Validity
E10_PO_SOD_Approver
E11_PO_SOD_Vendor
E12_Receiving_2Way_Match
E13_Receiving_Data_Validity
E14_Receiving_SOD
E15_Single_Invoice_Limits
E16_Split_Invoice_Limits
E17_Retroactive_PO
E18_Invoice_2Way_Match
E19_Invoices_Data_Validity
E20_Payables_SOD_PO
E21_Payables_SOD_Receipt
E22_Prohibited_Vendors
E23_Vendor_Address_Match
E24_Vendor_Name_Match
E25_Unusual_New_Vendor
E26_One_Time_Vendors
E27_GR_Without_Invoice
E28_Invoices_After_Period_End
E29_Payments_2Way_Match
E30_Duplicate_Payments
E31_Dup_Payments_Similar_Amt
E32_Dup_Payments_Diff_Dates
E33_Dup_Payments_Patterns
E34_Duplicate_Payments_EFT
E35_Payables_Data_Validity
E36_Payments_SOD_PO
E37_Manual_Payments
E38_Missing_Vendor_Info

WINDOWS Hardening

☐要匯入所有WMI Tool產生的原始稽核資料，請勾選此選項

☐如果您在WMI Tool中有勾選收集檔案(Include Files)權限清單，請勾選此選項

選擇想要執行之稽核模組

☐01-1. 檢核目前所有網域及本機所有使用者及其權限(The Privileges)，群組(Group)和使用狀態(Status)

☐01-2. 檢核所有無效/停用/久未使用(Inactive/Stall)的使用者帳號

☐01-3. 檢核來賓帳號(Guest Account)是否有被停用(Disable)

☐02-1. 檢核目前所有網域及本機所有資料夾及檔案的存取權限及所有權，進行各種異常使用狀態的統計與交叉比對

☐02-2. 檢核是否有任何資料夾被分享，並取得存取預設權限

☐02-3. 檢核所有隱藏系統檔案及它們的存取權限

☐03-1. 檢核系統安裝之防毒軟體，已將軟體版本以及病毒碼更新至最新版本

☐04-1. 檢核Windows排程(Scheduled Tasks)權限設定

☐05-1. 檢核稽核日誌(Audit Policy)記錄作業有遵循相關資訊安全標準

☐06-1. 檢核帳號與密碼安全設置/配置中，密碼政策(Password Policy)與帳戶鎖定政策有遵循標準

☐06-2. 檢核帳號安全設置遵循標準 (Security Options Policy)

☐06-3. 檢核未啟動不必要的程式或服務(System Startup Programs and Services)

☐06-4. 檢核系統重要檔案(System Critical File Information)及資料夾之權限設定

☐06-5. 檢核群組原則政策設定(Group Policy Settings)

☐06-6. 檢核系統修補程式(System Patch Update)更新狀態

☐執行所有的稽核模組

OK

Cancel

查核專案管理

稽核程式自動化/Procedure

專案概觀

- Payroll_analysis
 - Empmast
 - Payroll
 - Sales_reps
 - Work_depts
- Result
 - Results
 - source
 - Source_Folder
 - Work_Folder
- E01_ReqLimits
- E02_SplitReqs
- E03_UnauthReqs
- E04_ReqValidity
- E05_ReqSOD
- removeTempTable1
- DemoServer
- MODCASE
- OS_Window_Hardening_Auditing
- ProdServer
 - Data
 - Result
 - Script_Folder
 - A00_Main_Script
 - A01_Set_Value
 - C00_DataAnalysis
 - C01_Q1_延遲返國、差旅費計算
 - C02_Q2_請購合理驗證
 - C03_Q3_採購合理性
 - C04_Q4_報表依權責發生制入帳
 - C05_Q5_資產管理有效性
 - C06_Q6_付款金額的正確性
 - C07_Q7_供應商主檔資料重複建立
 - C08_Q8_無對應供應商的採購資料
- Source_Folder
- Work_Folder
- Purchase_to_Payment
 - 個人排程輸出：DemoServer
 - 個人排程輸出：PRODServer

指令日誌

AP_trans

C01_Q1_延遲返國、差旅費計算 x

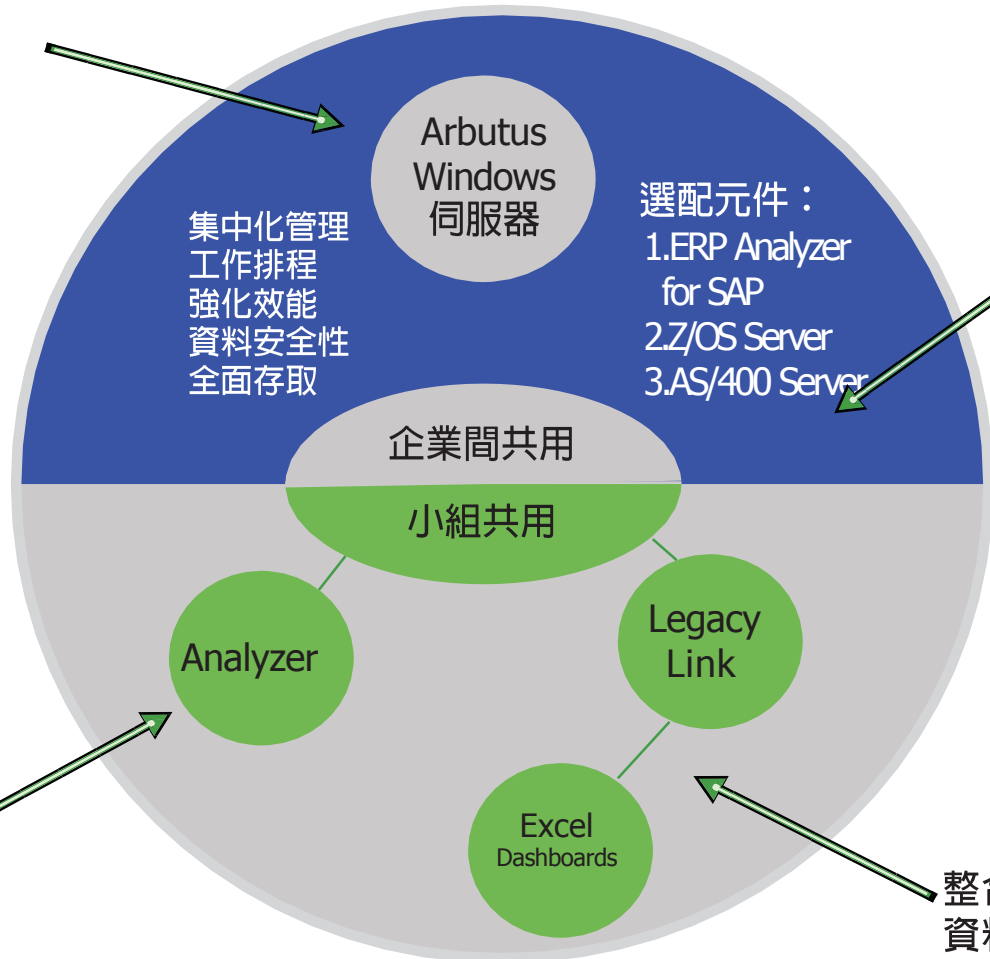
```
20
21
22
23 *****
24 ** 篩選出差費用支付無主檔申請 (Q1_Abnormal_NoFormNo), 出差報告沒有事前申請記錄 (Q1_Abnormal_NoLeaveNo)
25 *****
26
27
28 OPEN LEAVE_APPLICATIONS_XLSX_W
29
30 DELETE FIELD LEAVE_STARTDATE OK
31 DEFINE FIELD LEAVE_STARTDATE COMPUTED CTOD(SUBSTR(START_DATE,1,4)+SUBSTR(START_DATE,6,2)+SUBSTR(START_DATE,9,10), "YYYYMMDD")
32
33 DELETE FIELD LEAVE_ENDDATE OK
34 DEFINE FIELD LEAVE_ENDDATE COMPUTED CTOD(SUBSTR(END_DATE,1,4)+SUBSTR(END_DATE,6,2)+SUBSTR(END_DATE,9,10), "YYYYMMDD")
35 SET FOLDER /Work_Folder/C01
36 INDEX ON LEAVE_NUM TO "LEAVEAPP_on_LEAVENO"
37
38
39 SET FOLDER /Work_Folder/C01
40 OPEN FTEMASTER_W
41 DELETE FIELD txtNew_LeaveNo OK
42 DEFINE FIELD txtNew_LeaveNo COMPUTED SUBSTRING(ALLTRIM(LEAVENO), 1, 12)
43 INDEX ON FORMNO TO "FTEMASTER_on_FORMNO"
44
45 OPEN FTEXPENSES_W
46 DEFINE RELATION FORMNO WITH FTEMASTER_W INDEX FTEMASTER_on_FORMNO
47 DEFINE RELATION FTEMASTER_W.txtNew_LeaveNo WITH LEAVE_APPLICATIONS_XLSX_W INDEX LEAVEAPP_on_LEAVENO
48
49
50
51
52 Set Exact off
53 SET FOLDER /Work_Folder/C01
54 EXTRACT FIELDS ALL FTEMASTER_W.ERPNO AS "ERPNO" FTEMASTER_W.FORMNO AS "HEADER_FORMNO" FTEMASTER_W.CENTER AS "CENTER" FTEMASTER_W.CENTERID AS "CENTERID"
FTEMASTER_W.APPLICANTNAME AS "APPLICANTNAME" FTEMASTER_W.PLAN_Memo AS "PLAN" FTEMASTER_W.REASON AS "REASON" FTEMASTER_W.LEAVENO AS "WF_LEAVENO"
LEAVE_APPLICATIONS_XLSX_W.LEAVE_NUM AS "LEAVE_NUM" LEAVE_APPLICATIONS_XLSX_W.EMP_NAME AS "EMP_NAME" LEAVE_APPLICATIONS_XLSX_W.LEAVE_STARTDATE AS
"LEAVE_STARTDATE" LEAVE_APPLICATIONS_XLSX_W.LEAVE_ENDDATE AS "LEAVE_ENDDATE" IF (BETWEEN(FTEDATE, _BDate, _EDate) AND (FTEMASTER_W.ERPNO <> "-") AND (NOT
```

102 筆記錄 D:\Arbutus\Sample Files\Course Data\UP10General\Data Folder\AP_trans.dat

小組/企業間共用系統架構

集中化的資料管理：

- 易用性
- 可承受性
- 高效能



集中化管理
工作排程
強化效能
資料安全性
全面存取

Arbutus
Windows
伺服器

選配元件：
1.ERP Analyzer
for SAP
2.Z/OS Server
3.AS/400 Server

使用企業間共用以及
小組共用，能簡易地
與組織內成員共同使
用與分享資料

企業間共用

小組共用

Analyzer

Legacy
Link

Excel
Dashboards

利用Analyzer提高
稽核分析能力

整合稽核分析軟體
資料至Excel與儀表板
(Dashboard)軟體

Arbutus Shared Folders

共用資料夾

個人共用



在本機多個專案中共同使用資料表、程序、檢視(View)及其他物件，降低管理成本

小組共用



利用網路芳鄰功能，與小組成員共同分享資料表、程序、檢視(View)及其他物件

企業間共用



透過Arbutus Windows Server進行資料集中化管理並加強資料安全性，使用排程功能達到持續性監控的目的

Arbutus Shared Folders

共用資料夾



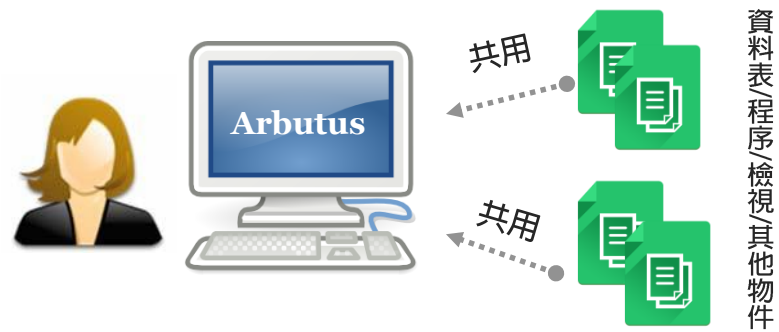
如何利用Arbutus 企業共用資料夾
功能管理產出的稽核結果？

Arbutus Shared Folders

共用資料夾 — 個人共用

案例情境

台北所稽核人員—Mia想在本機多個專案中分享稽核結果



共用(S) 工具(T) 應用程式(A) 伺

管理共用資料夾(M)...

增加個人共用(P)...

增加小組共用(T)...

增加企

關於共

個人共用資料夾

共用資料夾設定

名稱: MiaShare

資料夾: C:\MiaShare

☐ 僅適用於本專案

確定 取消

Arbutus Shared Folders

共用資料夾 — 小組共用

案例情境

高雄所稽核人員—Brad想利用網路芳鄰與小組成員分享稽核結果



共用(S) 工具(T) 應用程式(A) 伺

管理共用資料夾(M)...

增加個人共用(P)...

增加小組共用(T)...

增加企業間共用(E)...

關於共用資料夾(F)

網路位置 (3)

Tools (\\VIC-PC) (Y:)

共 465 GB

名稱: BradShare

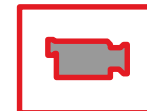
資料夾: Y:\Arbutus

☐ 僅適用於本專案

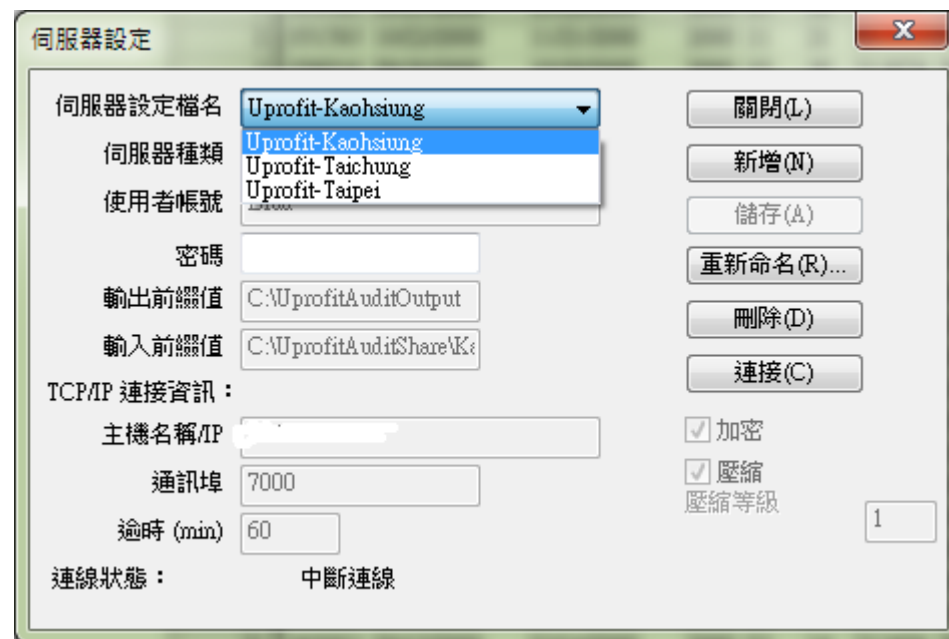
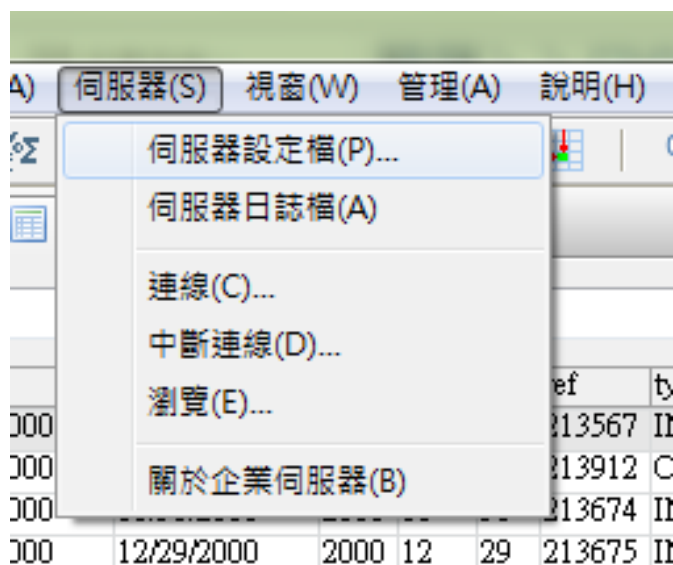
確定 取消

小組共用資料夾

Arbutus Shared Folders 企業間共用資料夾



- Randolph為本次稽核專案負責人，該專案有與台北分公司的Mia合作執行，Randolph想將稽核結果跟Mia分享，但僅授權給Mia讀取權限
- Brad是高雄所稽核人員，沒有任何檢視Randolph稽核專案的權限



Arbutus Shared Folders

共用資料夾 — 企業間共用

案例情境

Randolph想分享稽核結果給Mia，但Brad沒有權限

Brad

Mia

Randolph

沒有權限

完全控制

讀取

資料表/程序/檢視/其他物件

共用(S) 工具(T) 應用程式(A) 伺

管理共用資料夾(M)...

增加個人共用(P)...

增加小組共用(T)...

增加企業間共用(E)...

企業間共用資料夾設置

名稱: TaichungAudit-Randolph

設定檔: Uprofit-Taichung

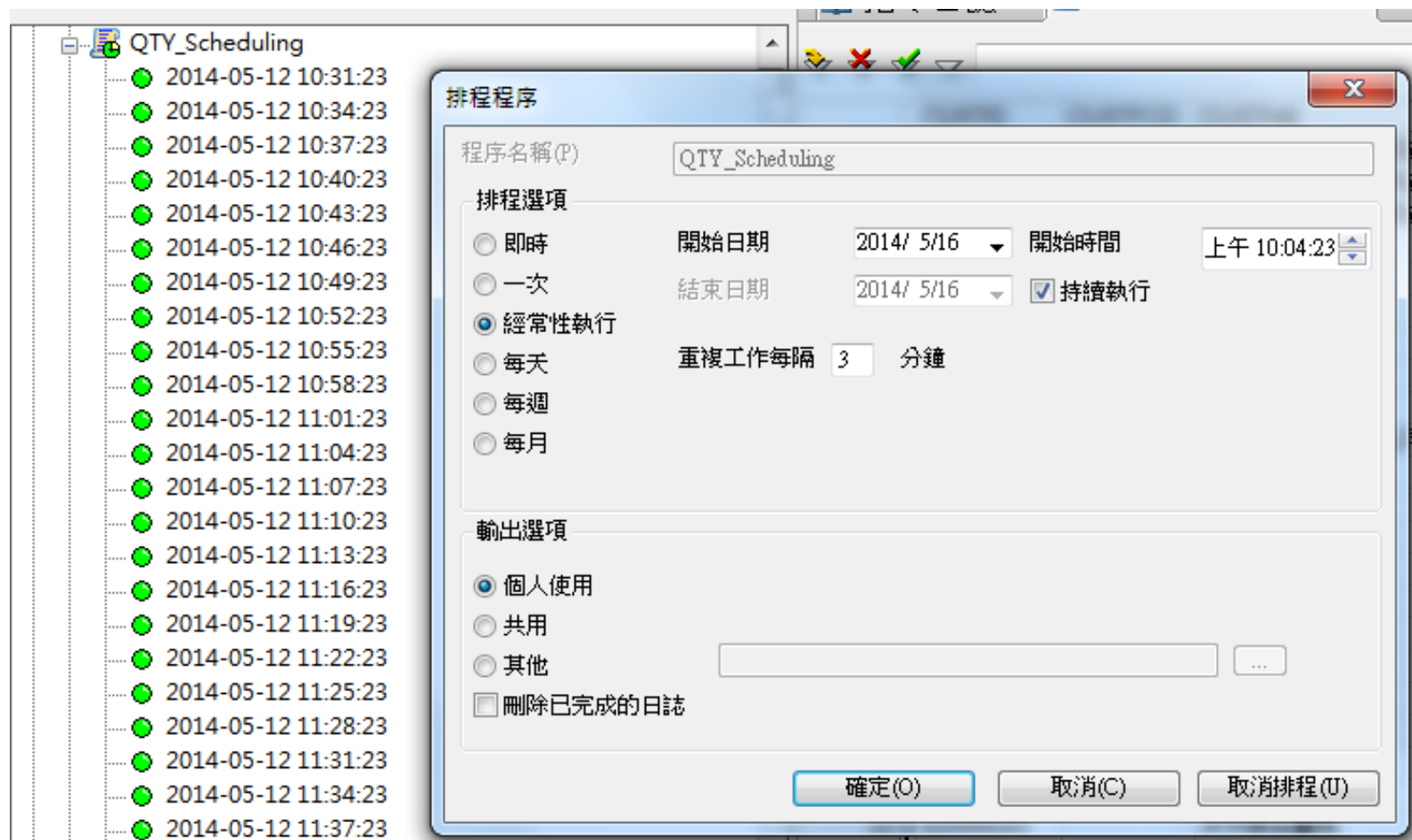
資料夾: C:\TaichungAudit

☐ 僅適用於本專案

確定 取消

企業間共用資料夾

資料排程(Scheduling)

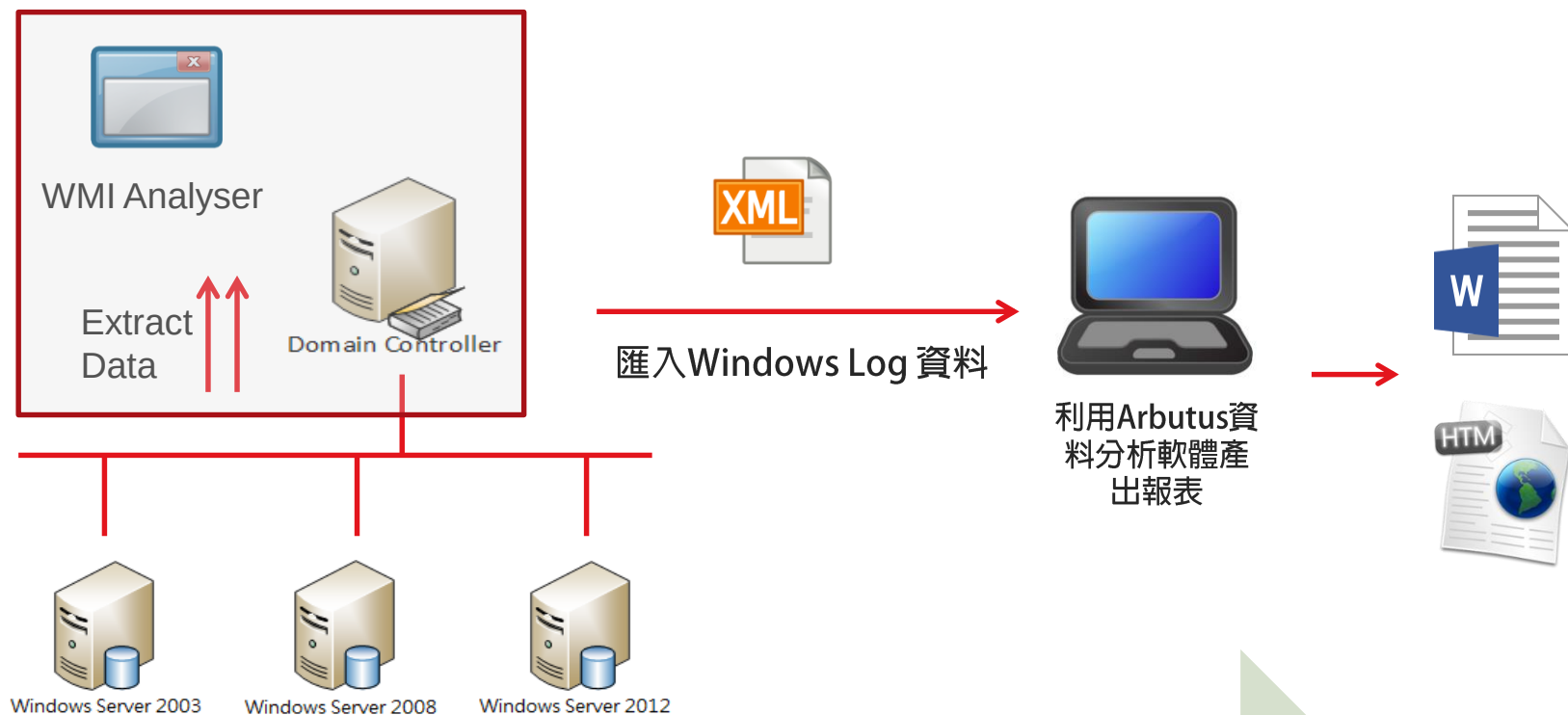


一套專門用來執行 IT 稽核的專案系統

Automated Auditing Program for OS Hardening Compliance (for Windows)

- 檢核管理資安政策及端點安全性
 - 統一檢核各網域伺服器及其所屬伺服器的管理稽核原則及端點安全性
- 縮短執行檢核的時間
 - 可選定所欲檢核的伺服器IP位置，進行自動化檢核
- 一致地驗證規範
 - 可根據主要的產業規範和內部原則進行標準化及客製化
- 檢核系統規範
 - 使用本系統自動化檢核不符合公司政策的系統設定值
- 功能豐富的報告
 - 最新的資料、功能強大的報告

查核模組系統架構與執行步驟



擷取Windows Log
資料

將Windows Log資料
匯入資料分析軟體

利用資料分析軟體分
析Windows Log 資料

匯出報表並作監控

六大查核模組

使用者和權限狀態
稽核模組



磁碟、目錄及檔案使
用權限異常稽核模組



防毒軟體更新異常
稽核模組



排程權限設定
稽核模組



稽核功能(Audit
Policy)異常稽核模組



資訊安全政策異常
稽核模組



六大查核模組功能介紹

使用者和權限狀態稽核模組



- 匯入網域及本機所有使用者(Users)及其權限(Privilege), 群組和使用狀態；密碼永久有效啟用狀態
- 辨別出所有無效(inactive)/停用(stall)/久未使用的使用者帳號
- 判別來賓帳號(Guest account)是否有被關閉使用

Guest - 內容

密碼複寫	撥入	物件	安全性	環境	工作階段
遠端控制	遠端桌面服務設定檔	COM+	屬性編輯器		
一般	位址	帳戶	設定檔	電話	組織
			已發佈的憑證	懸屬於	

使用者登入名稱(U):

使用者登入名稱 (Windows 2000 前版)(W):
UPROFIT\ Guest

登入時段(L)... 登入到(T)...

☐ 解除鎖定帳戶(N)

帳戶選項(O):

- ☐ 使用可還原的加密來存放密碼
- ☒ 帳戶已停用
- ☐ 互動式登入必須使用智慧卡
- ☐ 這是機密帳戶，無法委派

帳戶到期日

☒ 無(V)

☐ 到期日(E): 2014年 5月 7日

確定 取消 套用(A) 說明

Active Directory 使用者和電腦

動作(A) 檢視(V) 說明(H)

Active Directory 使用者和電腦 [DC1.uprofit.test-network.com]

儲存查詢

uprofit.test-network.com

- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- LostAndFound
- Managed Service Accounts
- Program Data
- Resource
 - Account
 - Sharefolder
 - Shareprinter
- System
- Users
- NTDS Quotas
- TPM Devices

名稱

- Administrator
- Allowed RODC Password Replic...
- Cert Publishers
- Cloneable Domain Controllers
- Denied RODC Password Replicat...
- DnsAdmins
- DnsUpdateProxy
- Domain Admins
- Domain Computers
- Domain Controllers
- Domain Guests
- Domain Users
- Enterprise Admins
- Enterprise Read-only Domain C...
- Group Policy Creator Owners
- Guest
- krbtgt
- postgres
- postgres2
- Protected Users
- RAS and IAS Servers
- Read-only Domain Controllers
- Schema Admins
- WinRMRemoteWMIUsers_

Brad - 內容

密碼複寫	撥入	物件	安全性	環境	工作階段
遠端控制	遠端桌面服務設定檔	COM+	屬性編輯器		
一般	位址	帳戶	設定檔	電話	組織
			已發佈的憑證	懸屬於	

使用者登入名稱(U):
brad @uprofit.test-network.com

使用者登入名稱 (Windows 2000 前版)(W):
UPROFIT\ brad

登入時段(L)... 登入到(T)...

☐ 解除鎖定帳戶(N)

帳戶選項(O):

- ☐ 使用者必須在下次登入時變更密碼
- ☐ 使用者不能變更密碼
- ☒ 密碼永久有效
- ☐ 使用可還原的加密來存放密碼

帳戶到期日

☒ 無(V)

☐ 到期日(E): 2014年 5月 7日

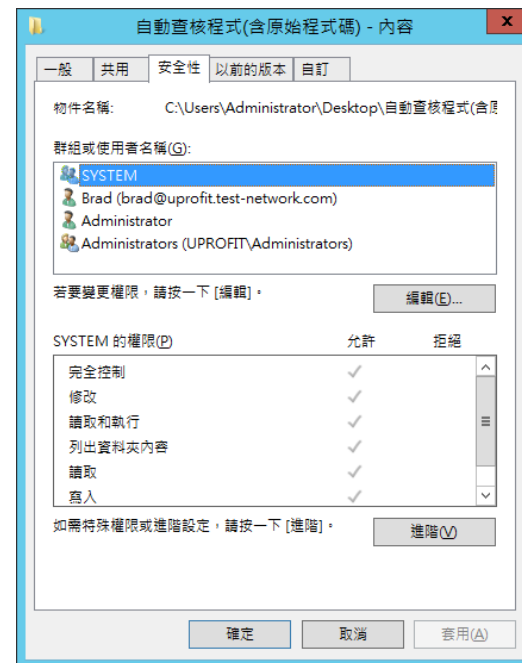
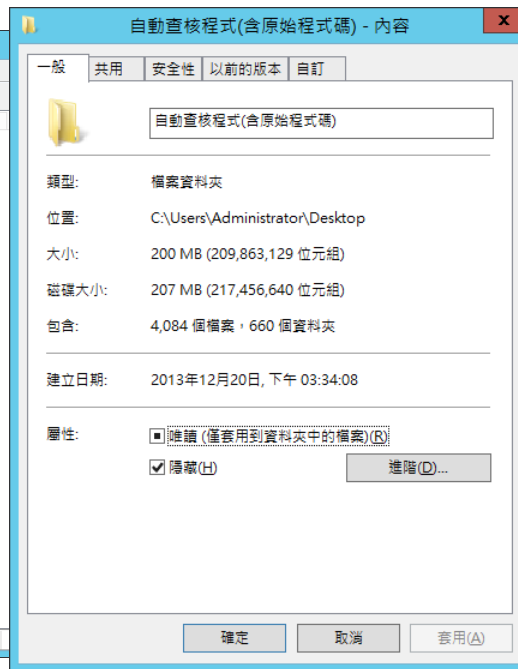
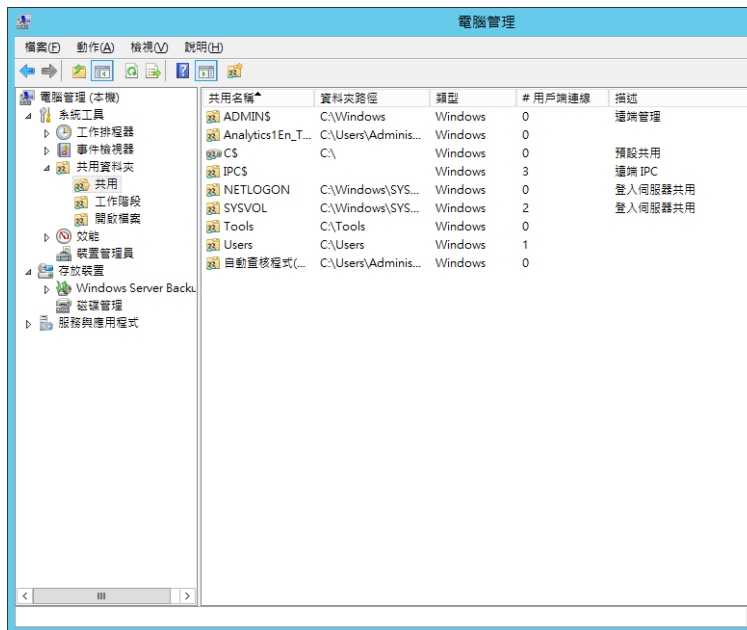
確定 取消 套用(A) 說明

六大查核模組功能介紹

磁碟、目錄及檔案使用權限異常稽核模組



- 匯入磁碟、目錄及檔案使用權限紀錄，並可依需求設定僅需蒐集之項目。
- 確認資料夾及檔案的存取與所有權，以便報告任何存取異常的情況(例如：任何人可寫入之檔案及目錄)
- 確認是否有任何資料夾被分享並取得存取預設權限
- 確認出所有隱藏系統檔案及它們的存取權限，以決定這些資料夾及檔案隱藏的理由



六大查核模組功能介紹

防毒軟體更新異常 稽核模組



- 確認系統安裝的防毒軟體有更新病毒碼及程式版本至最新版本

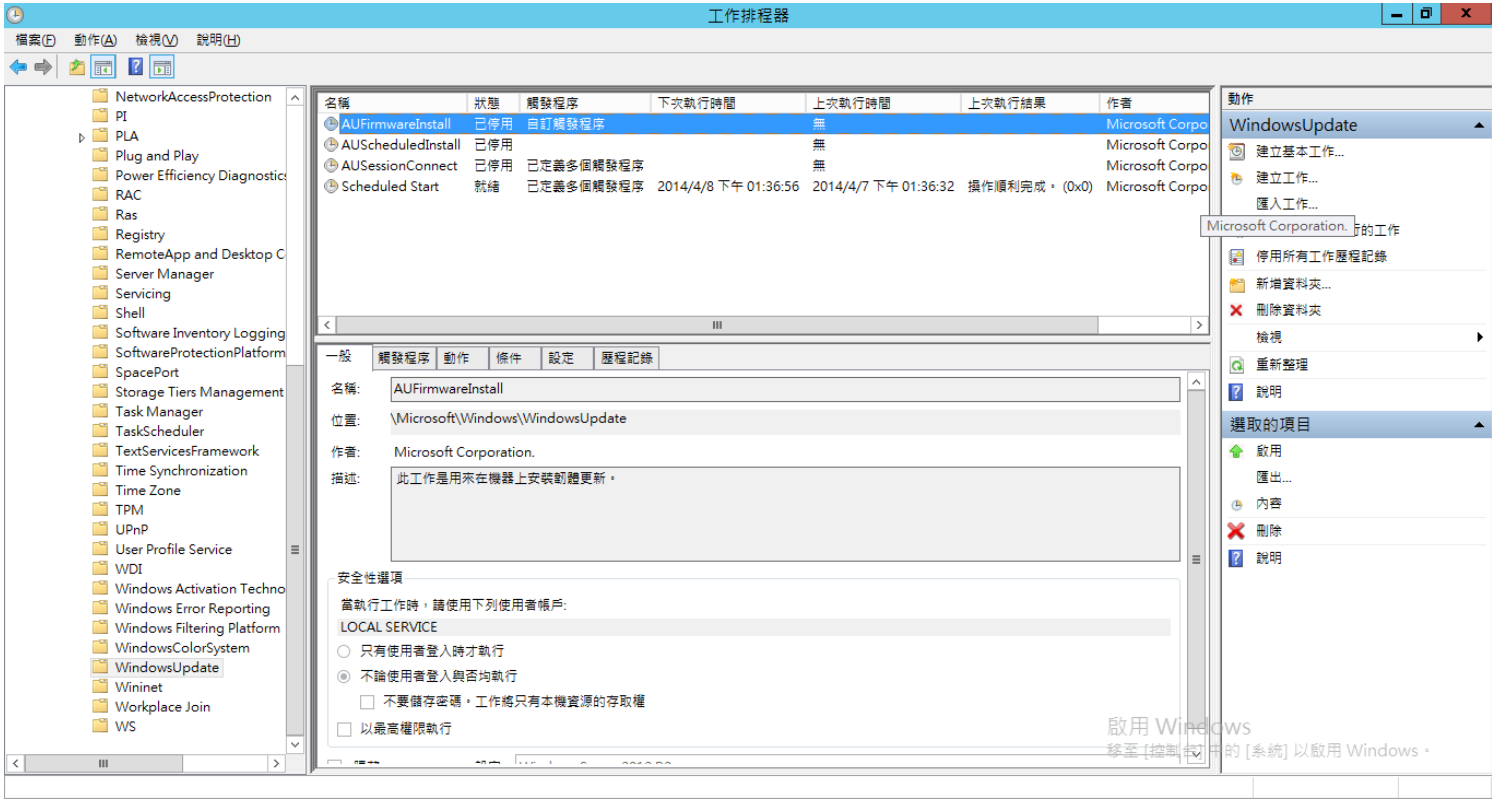


六大查核模組功能介紹

排程權限設定 稽核模組



- 檢核Windows排程權限設定



六大查核模組功能介紹

稽核功能(Audit Policy)異常稽核模組



- 確認稽核日誌功能是否有被啟動
- 確認稽核日誌記錄作業有遵循相關資訊安全標準

原則

稽核目錄服務存取

稽核系統事件

稽核物件存取

稽核原則變更

稽核特殊權限使用

稽核帳戶登入事件

稽核帳戶管理

稽核登入事件

稽核程序追蹤

原則設定

尚未定義

成功

尚未定義

失敗

尚未定義

成功, 失敗

尚未定義

成功, 失敗

成功

群組原則模型

群組原則結果

群組原則管理

Default Domain Policy

領域

詳細資料

設定

委派

Default Domain Policy

資料收集: 2014/4/7 下午 04:19:48

電腦設定 (已啟用)

原則

Windows 設定

安全性設定

帳戶原則/密碼規則

帳戶原則/帳戶鎖定原則

帳戶原則/Kerberos 原則

本機原則/稽核原則

原則

稽核系統事件

稽核原則變更

稽核帳戶登入事件

稽核登入事件

稽核程序追蹤

設定

成功

失敗

成功, 失敗

成功, 失敗

成功

本機原則/安全性選項

公開金鑰原則/加密檔案系統

使用者設定 (已啟用)

沒有設定定義。

啟用 Windows

移至 [控制台] 中的 [

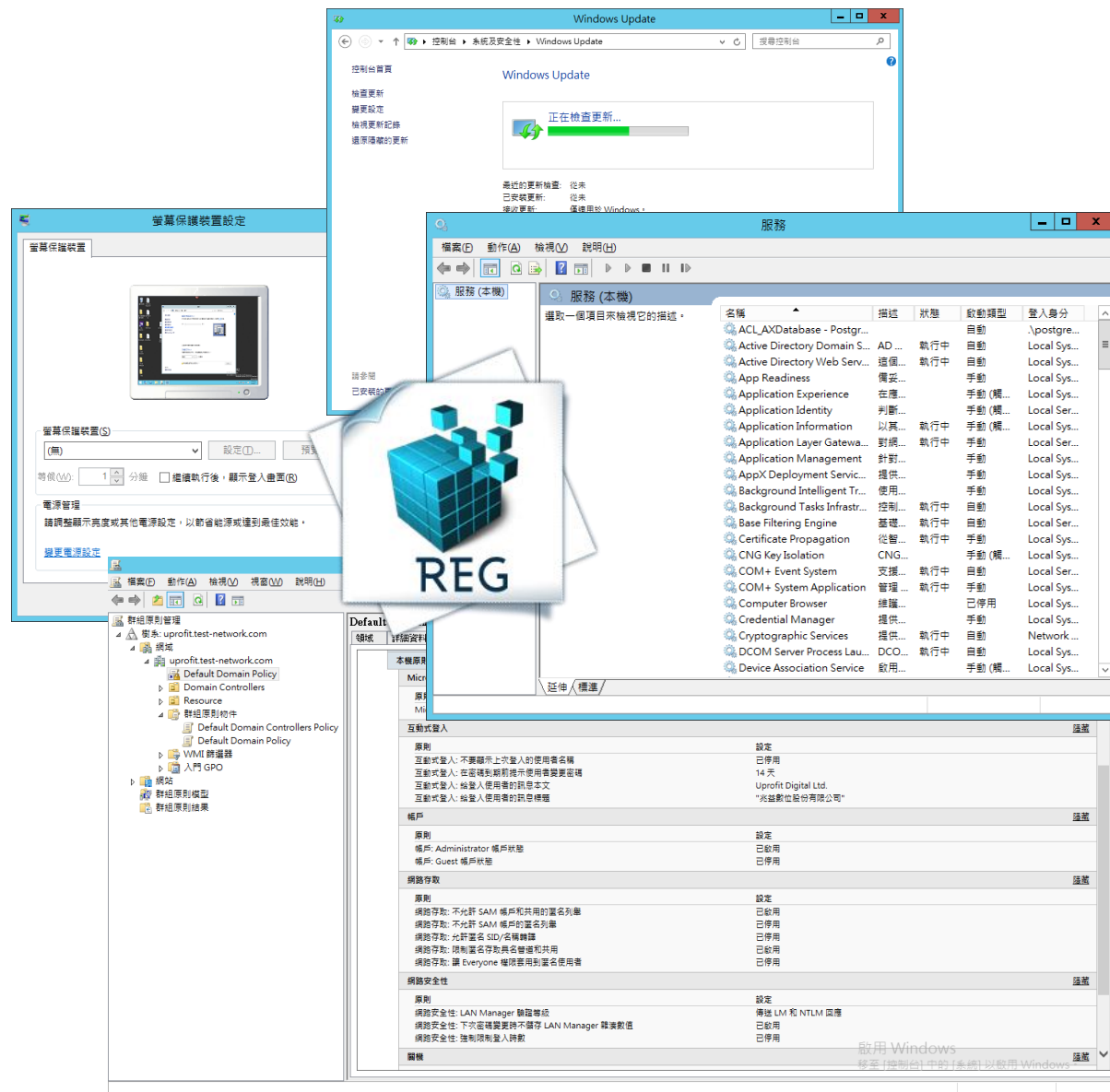
六大查核模組功能介紹

資訊安全政策異常稽核模組



- 依系統特性(Web Server、DB Server、Domain Controller)提供安全設定最佳化之參照標準並定義於Arbutus的比對樣本中，於資料搜集及分析時可供直接套用檢核。
 - 伺服器螢幕保護裝置啟用時間設定檢核
 - 帳號及密碼安全設置/配置 (Security Setting/Configure)的資訊安全政策
 - 確認未啟動不必要的程式或服務
 - 系統重要檔案之權限設定檢核
 - Windows Registry之設定檢核
 - 群組原則政策(Group Policy)檢核
 - 系統修補程式更新檢核

資訊安全政策異常稽核模組



實機操作畫面 — 資料蒐集、彙整、分析



資料蒐集



資料彙整、
分析



實機操作畫面 -- 報告產出

Windows OS Hardening
Audit Report

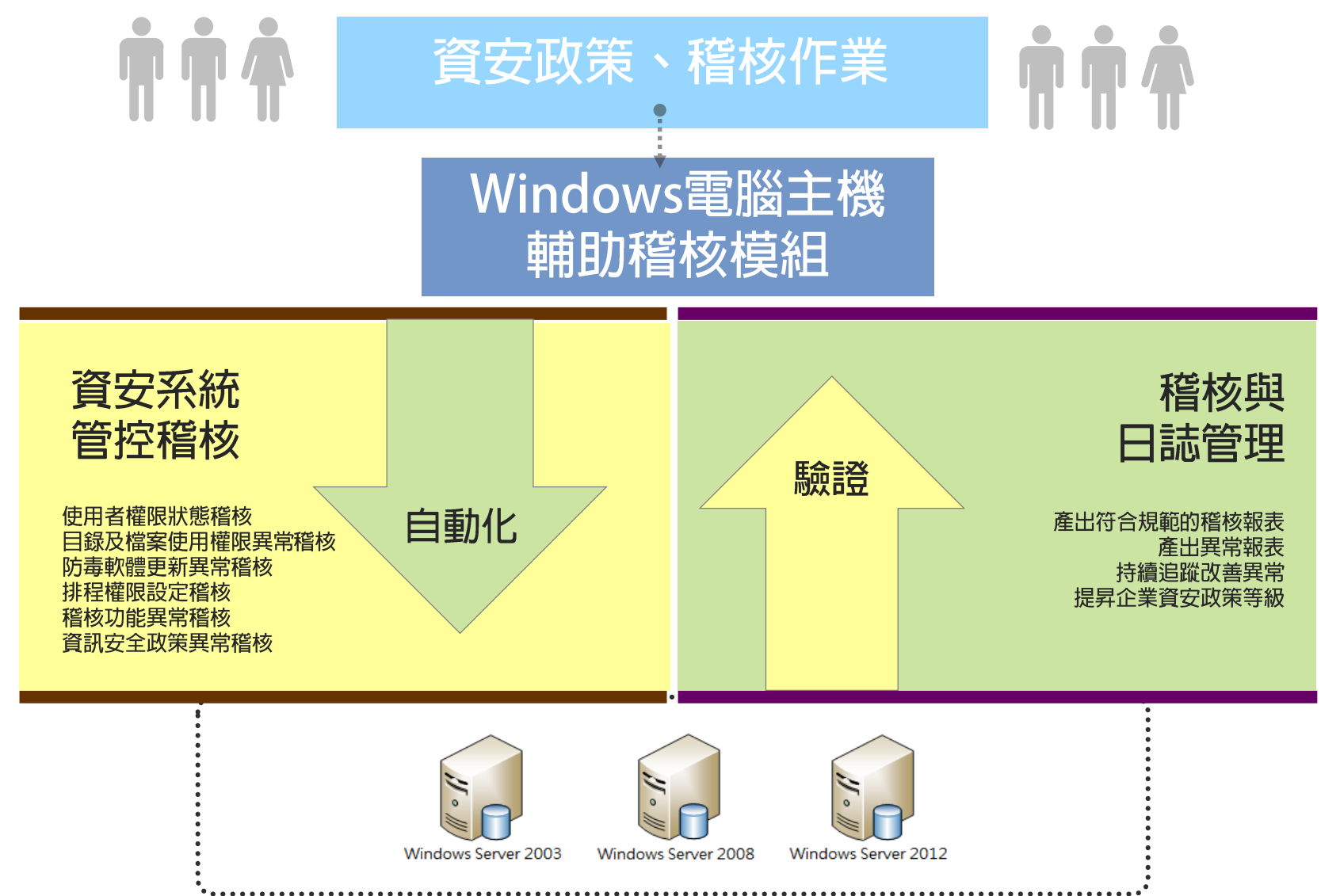
報表名稱(Report Title): **HIDDEN_FOLDERS_REPT**
報表說明(Report Description): 此張報表列出所有被隱藏的資料夾
報表日期(Report Date):2014/7/14 下午 09:42

Hidden	Name	Compressed	CSName	Encrypted	FileType	Path	Readable	System	Writeable	ServerIP Address
True	c:\wmi test\fis	False	DC1	False	File Folder	\wmi test\	True	False	True	192.168.10.1
True	c:\wmi test\fis\output	False	DC1	False	File Folder	\wmi test\fis\	True	False	True	192.168.10.1
True	c:\program files\windowsupdate	False	MS2	False	File Folder	\program files\	True	False	True	192.168.10.20

輔助說明(Comments): 此張報表係比對Hidden欄位的數值，若為True則表示該資料夾為隱藏狀態

欄位名稱	說明
Hidden	若該數值為True，則該檔案為隱藏狀態 若該數值為False，則該檔案為顯示狀態
Name	該檔案完整路徑 Example:c:\winnt\system\win.ini
Compressed	若該數值為True，則該檔案具有壓縮屬性 若該數值為False，則該檔案不具有壓縮屬性
CSName	該檔案所屬主機名稱
Encrypted	若該數值為True，則該檔案具有加密屬性 若該數值為False，則該檔案不具有加密屬性
FileType	檔案類型

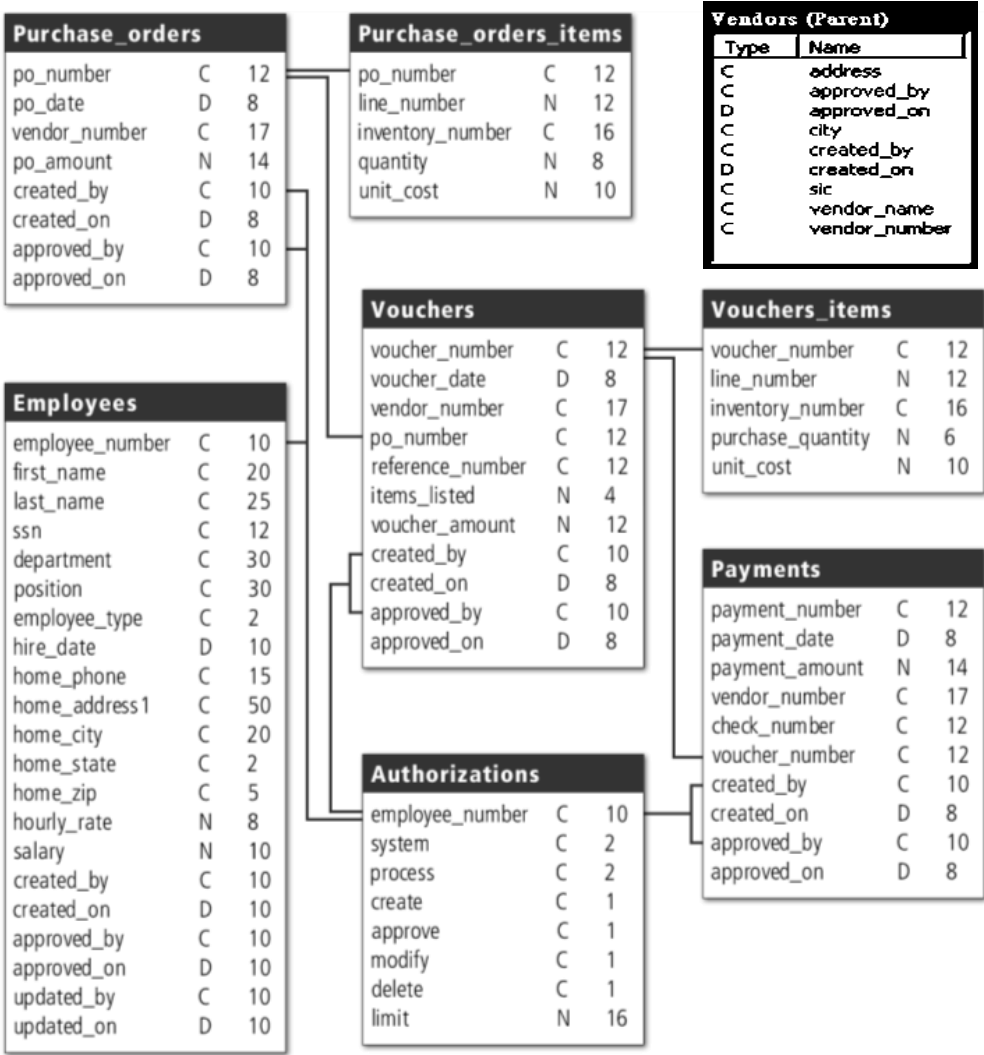
為什麼要選擇Windows 電腦主機輔助稽核模組?



個案探討

範例一:採購付款作業查核

- 一. 授權採購的適當性?
- 二. 付款作業的正確性?



範例二：員工出差申請費用報支查核

- 一. 員工出差申請的適當性與合理性
- 二. 員工出差費用申請的正確性
- 三. 員工出差費用支付的正確性

Travel_Requisition	
欄位名稱	欄位型態
Requisition_number	C
Requisition_date	D
employee_number	C
preauth_amount	N
trip_beg	D
trip_end	D
Approved_on	D
Approved_by	C

Employeeemast	
欄位名稱	欄位型態
employee_number	C
Name	C
ID	C
department	C
Position	C
Address	C
manager	C
BankAccount	C
Limit	C

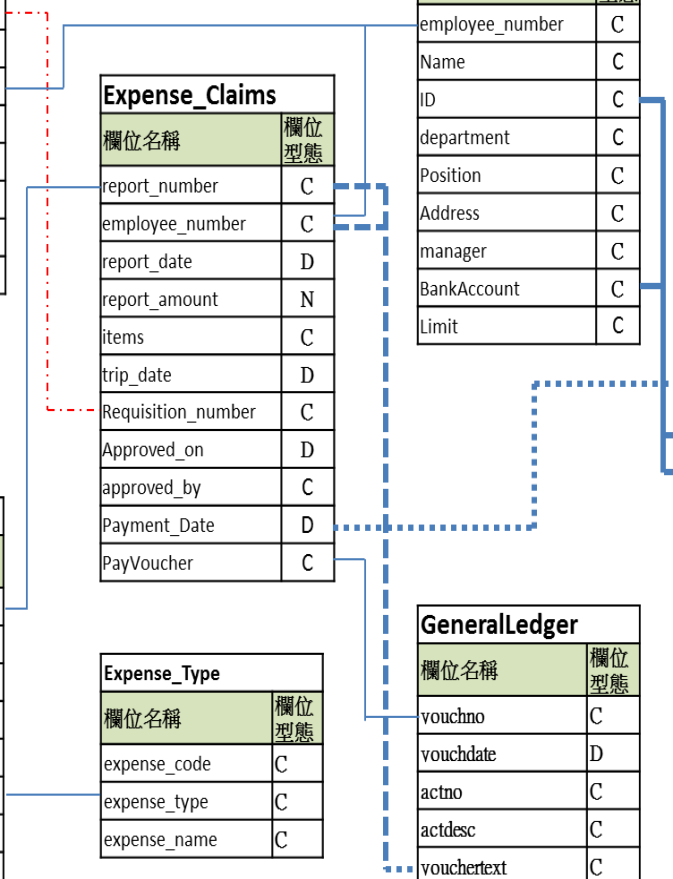
Expense_Claims	
欄位名稱	欄位型態
report_number	C
employee_number	C
report_date	D
report_amount	N
items	C
trip_date	D
Requisition_number	C
Approved_on	D
approved_by	C
Payment_Date	D
PayVoucher	C

BankStatement	
欄位名稱	欄位型態
Payment_Date	D
BankAccount	C
EmployeeID	C
Name	C
report_amount	N

Expense_Detail	
欄位名稱	欄位型態
report_number	C
employee_number	C
merchant_name	C
expense_date	D
expense_amount	N
expense_type	C
payment_type	C
receipt	C

Expense_Type	
欄位名稱	欄位型態
expense_code	C
expense_type	C
expense_name	C

GeneralLedger	
欄位名稱	欄位型態
vouchno	C
vouchdate	D
actno	C
actdesc	C
vouchertext	C
Locamt	N
DC	C



實務交流互動 Q&A



A photograph of a field of yellow flowers, possibly rapeseed, under a clear blue sky. The flowers are in the foreground and middle ground, with some in sharp focus and others blurred. The sky is a deep blue, and there are some dark trees in the background.

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>

ACL資料分析與電腦稽核系統 - <https://www.facebook.com/Uprofit.ACL>

ACL 資料分析與電腦稽核學習網 - <https://www.facebook.com/UprofitDigital>

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

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