

ARBUTUS 資料分析與稽核系統介紹

主講人: 莊盛祺 舞弊稽核師(Certified Fraud Examiner,CFE)
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

現任：

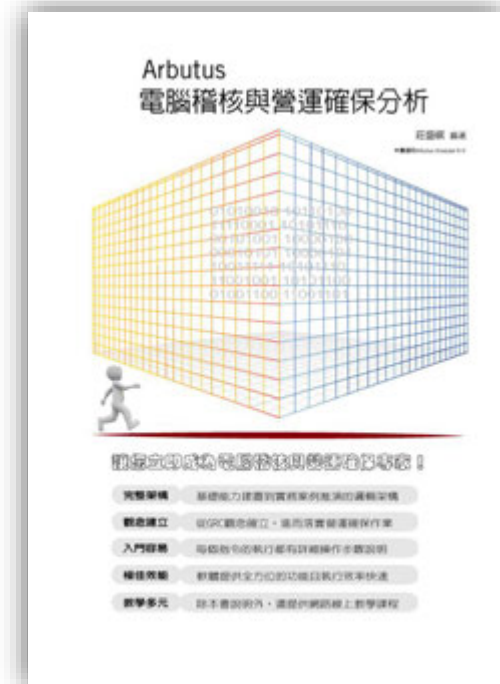
台北大龍峒扶輪社

理事暨節目委員會主任委員

眾信聯合會計師事務所

財務主任

Arbutus電腦稽核與營運確保分析



數位環境

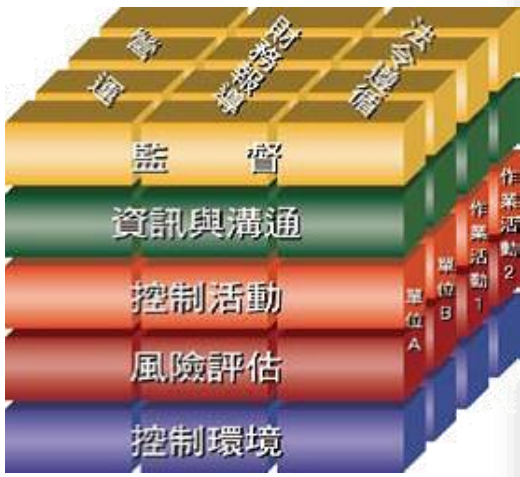


你真得信賴您資訊系統中
所處理的資料及交易記錄的
完整性與正確性嗎



- 資訊管理
- 營運風險
- 市場
- 違法/違約
- 策略性風險
- 財務危機
- 舞弊
- 人力資源
- 信譽

服務範圍



Target Vertical Markets

ePlatform Products

eAutomation Products

- | | |
|---------------------|------------------------------------|
| Network Appliances | Environmental Monitoring |
| Internet Security | Factory Automation |
| Medical/Healthcare | Building Automation |
| Entertainment | Intelligent Transportation Systems |
| eHome/eBuilding | Machine Automation |
| Transportation | Automatic Test Equipment |
| Broadcasting | |
| Facility Management | |

Customization Services

Premier D&MS
(Premier Design & Manufacturing Service)
BTOS
(Build to Order Service)
DTOS
(Design to Order Service)

x86 Embedded Computing	RISC Embedded Computing	Display Solutions	Medical Computing	Applied Panel Computing
Industrial Computing	CompactPCI	Network Appliances	Digital Signage	eVideo Solutions
Automation Controller & Software	Distributed I/O Modules	Industrial I/O	Industrial Communication	Human Machine Interface

Global Manufacturing Centers (China/Taiwan)

內部稽核焦點的轉變

The 20th-century internal audit model

Controls assurance based on cyclical or routine audit plans

週期性內控稽核

Today's typical internal audit model

Controls assurance based on risk-based internal audit plan

風險導向內控稽核

The risk-centric internal audit model of tomorrow

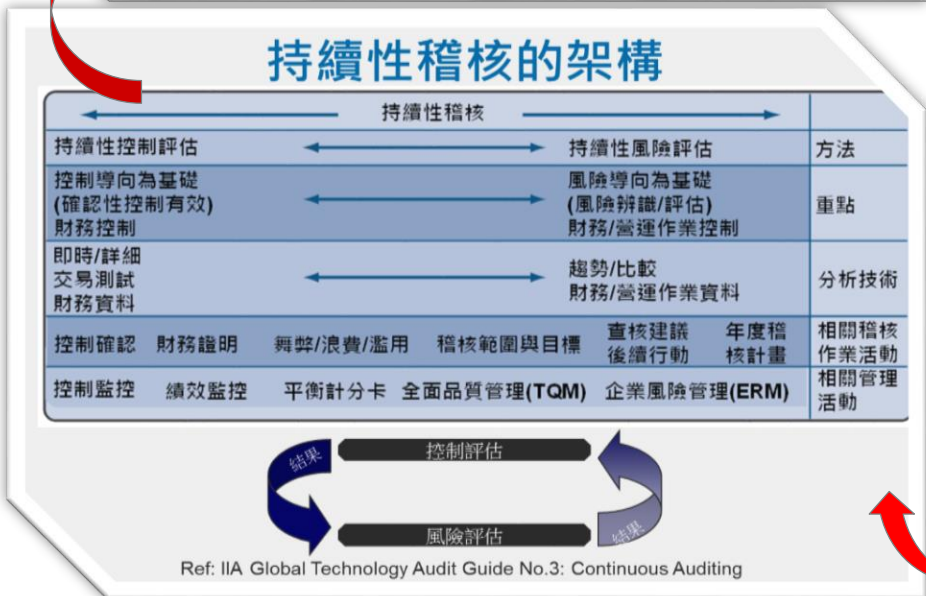
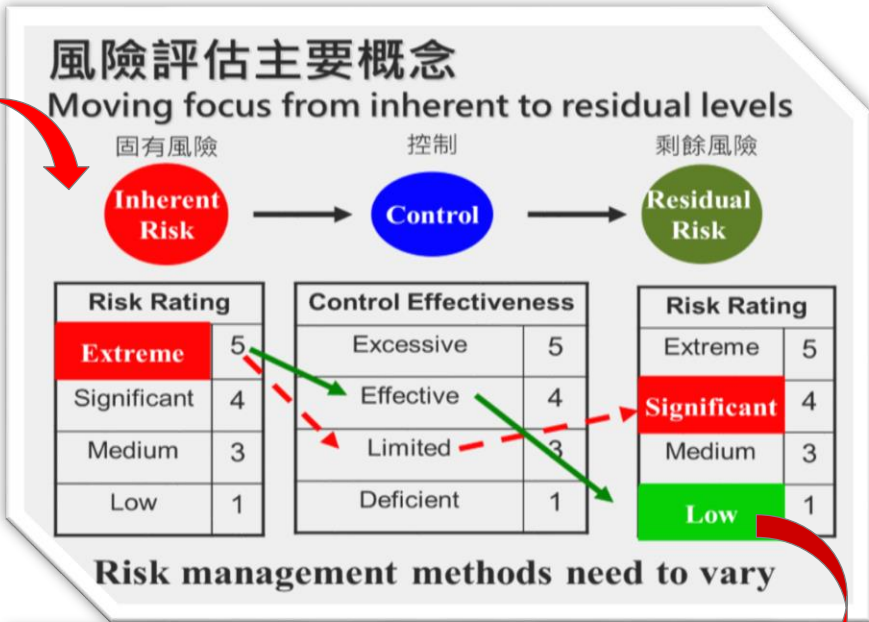
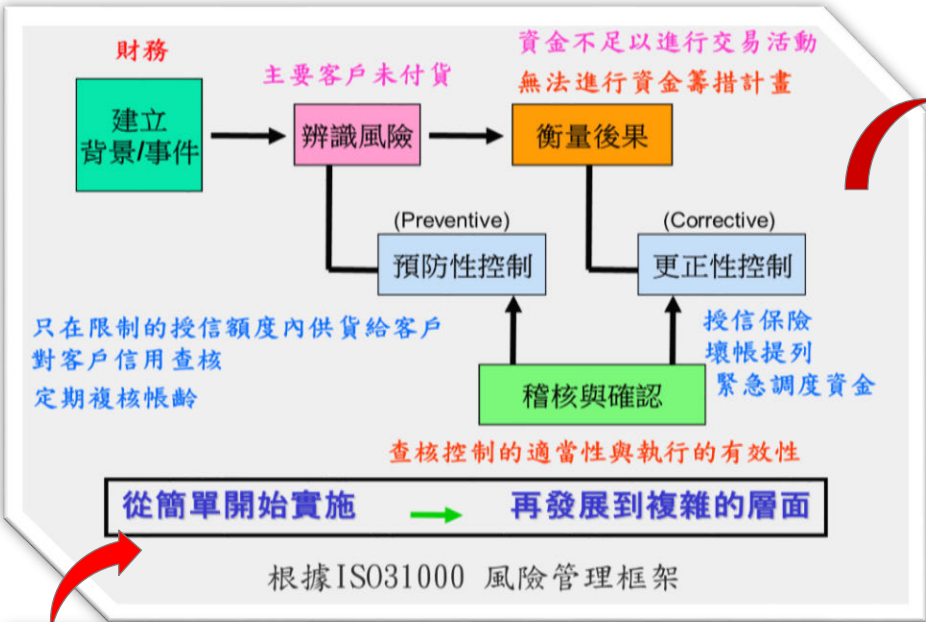
Assurance on the effectiveness of risk management in addition to controls assurance

除內控稽核外，
確認風險管理的有效性

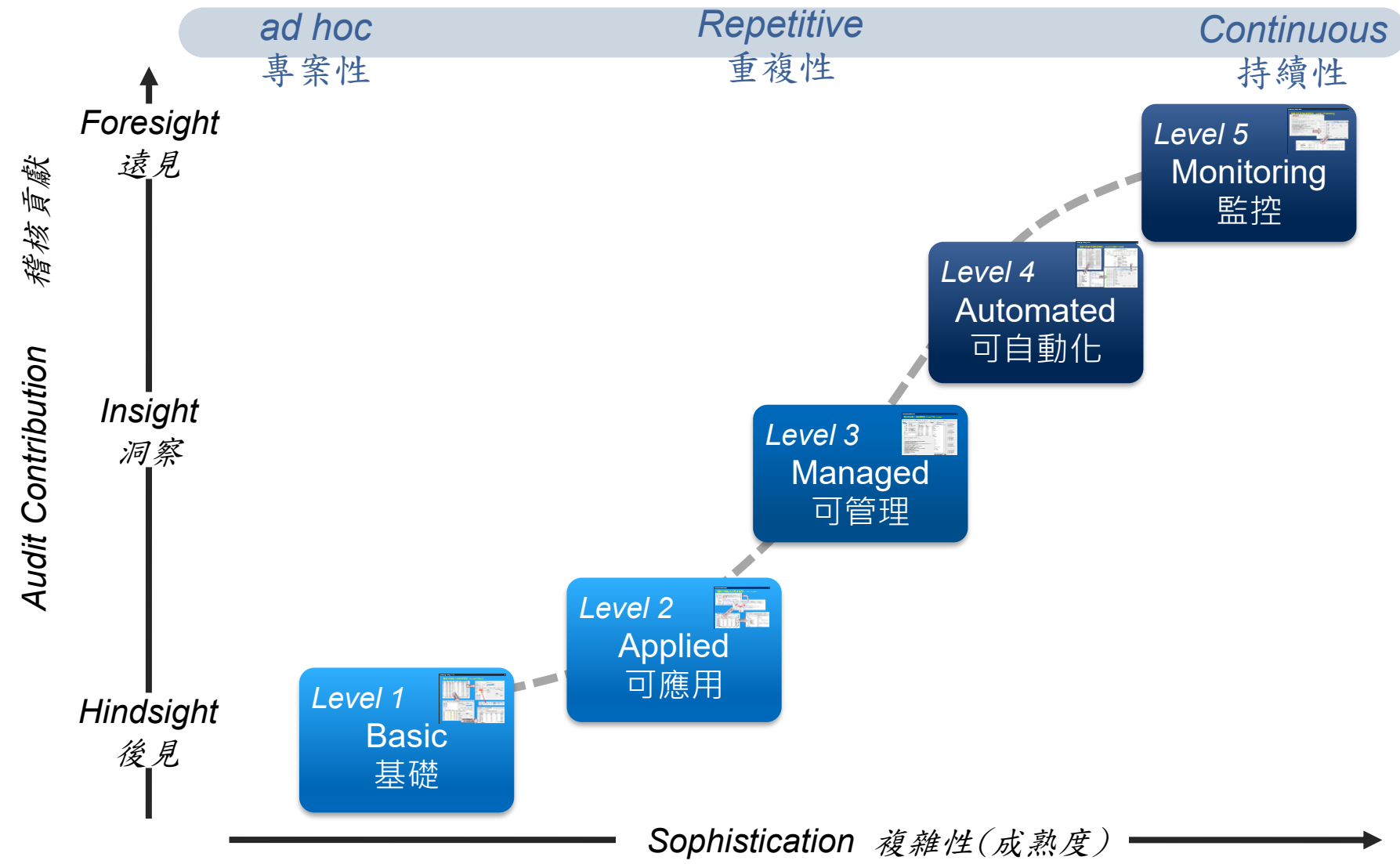
Adapted from PricewaterhouseCoopers Advisory Services, "Internal Audit 2012," © 2007

PRICEWATERHOUSECOOPERS 

風險管理方法 – 以風險為導向的內部控制與稽核作業

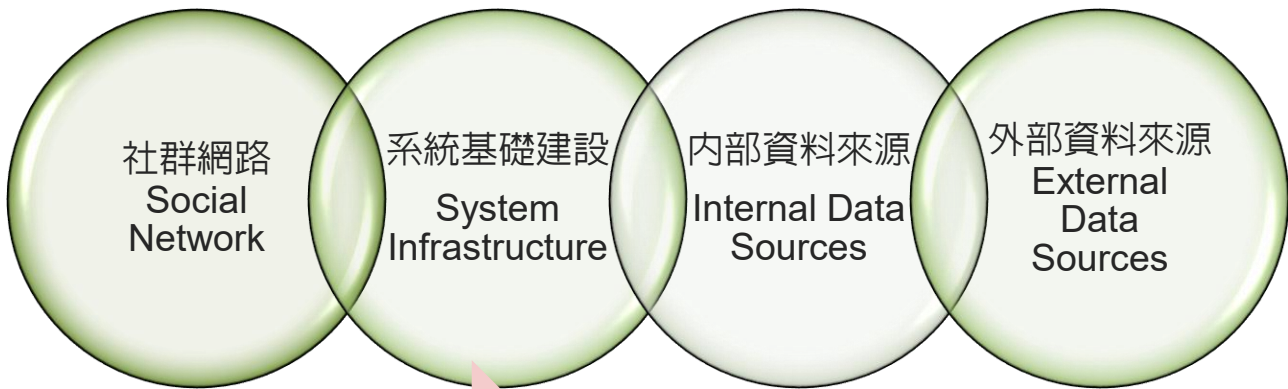


稽核分析能力成熟度模型



我們現在的『稽核分析能力』在哪裡？

資訊來源
Information Sources



擷取,轉換,
和載入
ETL



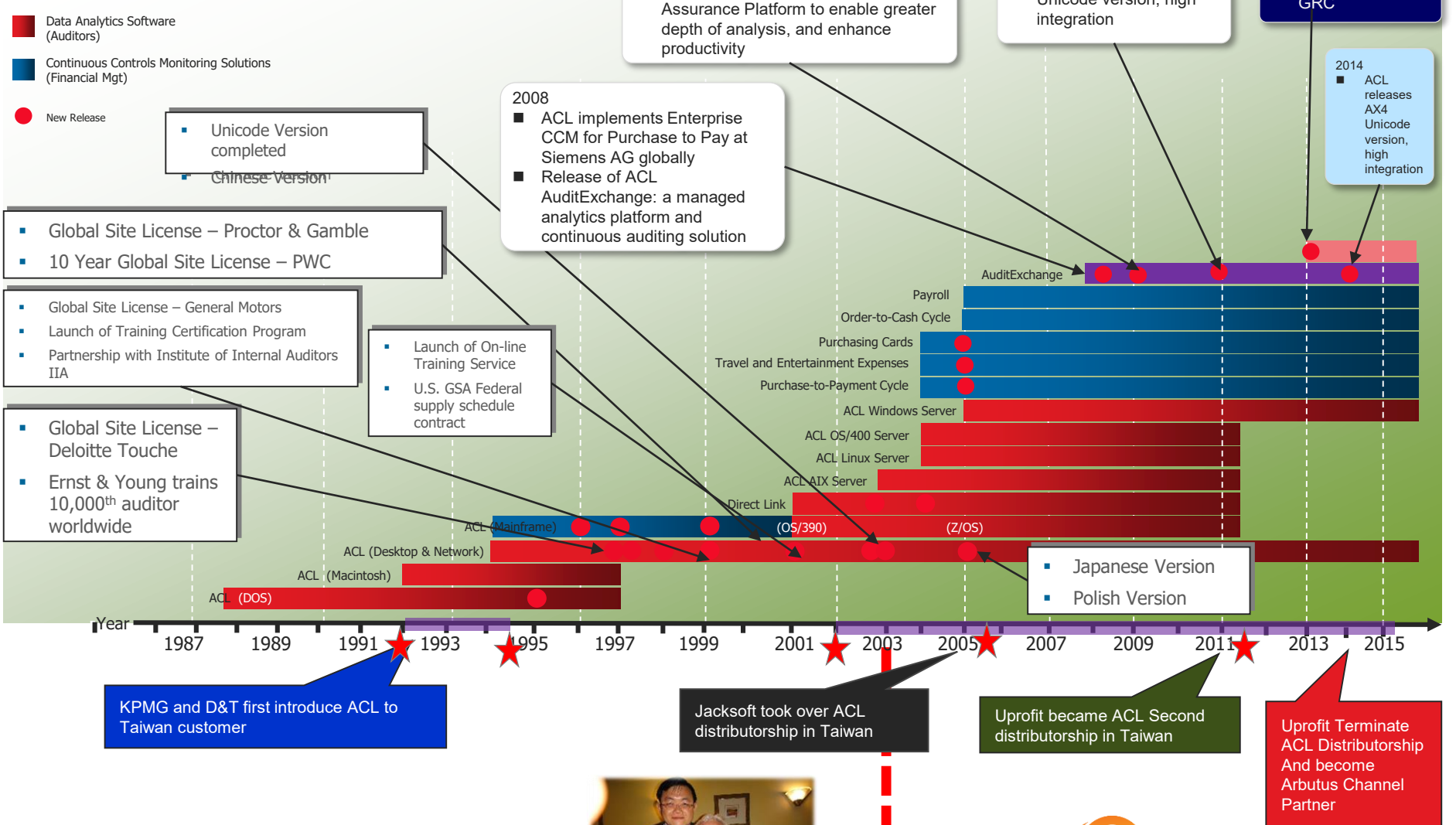
分析方案
Analytics Solutions



要求洞察
Required Insights



ACL in Taiwan



David's 的奇幻之旅



兆益數位正式與Arbutus公司合作，全面進行稽核系統中文化界面的研發，引進先進資料分析技術與即時資訊倉儲觀念

AuditTest - Arbutus Analyzer

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

新增專案(N) Ctrl+N
開啟專案(O) Ctrl+O
關閉專案(C)
儲存檔案(S) Ctrl+S
另存新檔(A)...
頁面設置(T)...
列印(P) Ctrl+P
列印專案文件(D)...
關閉(X)
1 ACL105 Found
2 ArbutusDemoP
3 Clientlist
4 Sample Data
還原(U)
剪下(T)
複製(C)
貼上(P)
資料表格格式(T)...
篩選器(L)...
變數(V)...

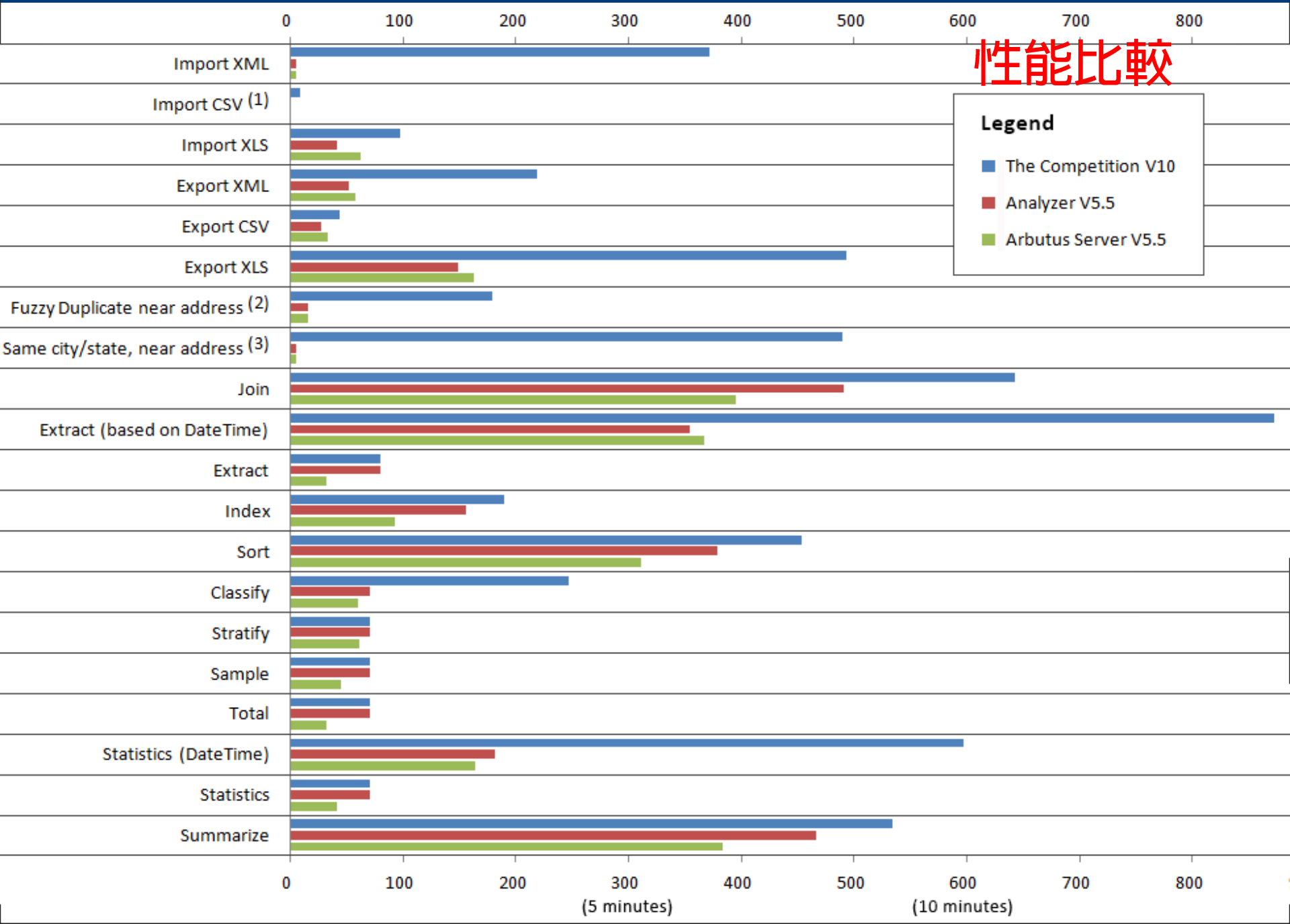
關聯(R)...
報告(P)...
萃取(T)...
匯出(X)...
彙總(S)...
排序(O)...
索引(I)...
聯結(J)...
合併(M)...
比較(C)...
樣本數(I)...
抽樣(S)...
評估(E)...
SQL(Q)...
新增伺服器資料(N)
新增本機資料(L)

驗證(V)...
計算筆數(C)...
總和(T)...
統計(S)...
剖析(P)...
分層(R)...
分類(L)...
帳齡(A)...
交叉分析(U)
班佛分析(B)...
順序(Q)...
缺漏(G)...
重複(D)...
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)

排程(S)
已連接的使用者(C)
開啟指令日誌(C)
顯示/隱藏變數(V)
字體大小(F)
關閉(L) Ctrl+W
伺服器設定檔(P)...
伺服器日誌檔(A)
連線(C)...
中斷連線(D)...
瀏覽(E)...
關於企業伺服器(B)

評論(C)...
卸載(D)...
隨機(R)...
搜尋(E)...
資料表歷史紀錄(H)
從歷史記錄中建立程序(Y)
執行程序(P)...
排程程序(C)...
開啟錄製器(S)
清除日誌檔案(L)...
電子郵件通知(N)...
程序保護(P)...
自訂(U)...
偏好設定(O)...

帳單號碼	日期	產品編號	產品類別	數量	金額	等級
1	12852	01/02/2000	052530155 05	36	1.08	平價
2	12853	01/02/2000	052530155 05	3	0.09	平價
3	12854	01/02/2000	090504761 09	1	6.17	平價
4	12855	01/02/2000	080102630 08	54	907.20	平價
5	12856	01/02/2000	034255003 03	7	2.80	平價
6	12857	01/02/2000	040240664 04	1		
7	12858	01/02/2000	010803760 01	1		
8	12859	01/02/2000	080102630 08	1		
9	12860	01/02/2000	080935428 08	1		
10	12861	01/02/2000	024130572 02	1		
11	12862	01/02/2000	034255003 03	1		
12	12863	01/02/2000	093788411 09	1		
13	12864	01/02/2000	080935428 08	1		
14	12865	01/02/2000	024130572 02	1		
15	12866	01/02/2000	034255003 03	1		
16	12867	01/02/2000	093788411 09	1		
17	12868	01/02/2000	090081001 09	1		
18	12869	01/02/2000	030412903 03	1		
19	12870	01/02/2000	010102710 01	1		
20	12871	01/31/2000	080126308 08	1		
21	12872	02/09/2000	090504761 09	1		
22	12873	02/10/2000	052530155 05	1		
23	12874	02/11/2000	080126308 08	1		
24	12875	02/12/2000	010134420 01	1		
25	12876	02/13/2000	090501551 09	1		
26	12877	02/14/2000	040240284 04	1		
27	12878	02/15/2000	010803760 01	1		
28	12879	02/15/2000	010155170 01	1		
29	12880	02/16/2000	034255003 03	1		
30	12881	02/16/2000	024128812 02	1		
31	12882	02/16/2000	090585322 09	1		
32	12883	02/17/2000	080126308 08	1		
33	12884	02/19/2000	024128932 02	1		
34	12885	02/20/2000	090501551 09	1		
35	12886	02/22/2000	052210545 05	1		
36	12887	02/23/2000	024128712 02	1		
37	12888	02/25/2000	080938748 08	1		
38	12889	02/26/2000	010631190 01	1		
39	12890	02/28/2000	024128712 02	1		
40	12891	12/31/2000	080126008 08	1		



Arbutus 主要顧客群



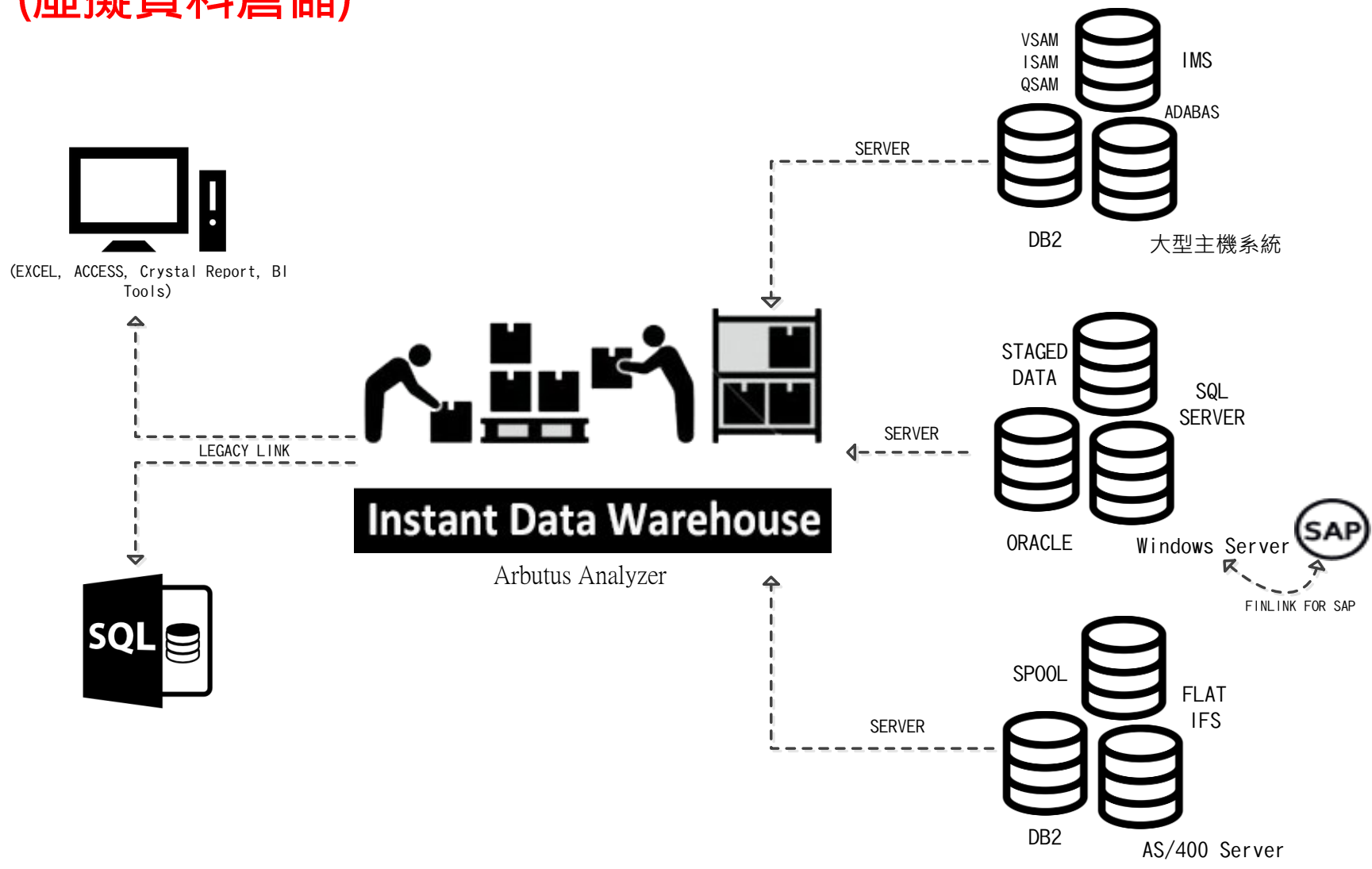
Arbutus Customers

Here are just some of the companies that are licensed users of Arbutus technology:



即時資料倉儲 - Instant Data Warehouse

(虛擬資料倉儲)



THE INSIGHT ADVANTAGE TO YOUR BUSINESS

如何提高你的洞察力

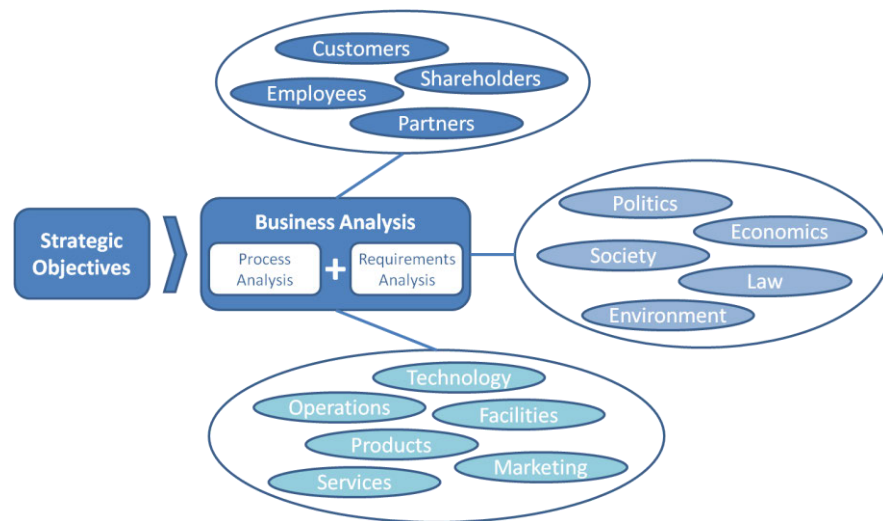
Insight = Catalyst(催化劑), Analyses(分析), and Assessments(評估).



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

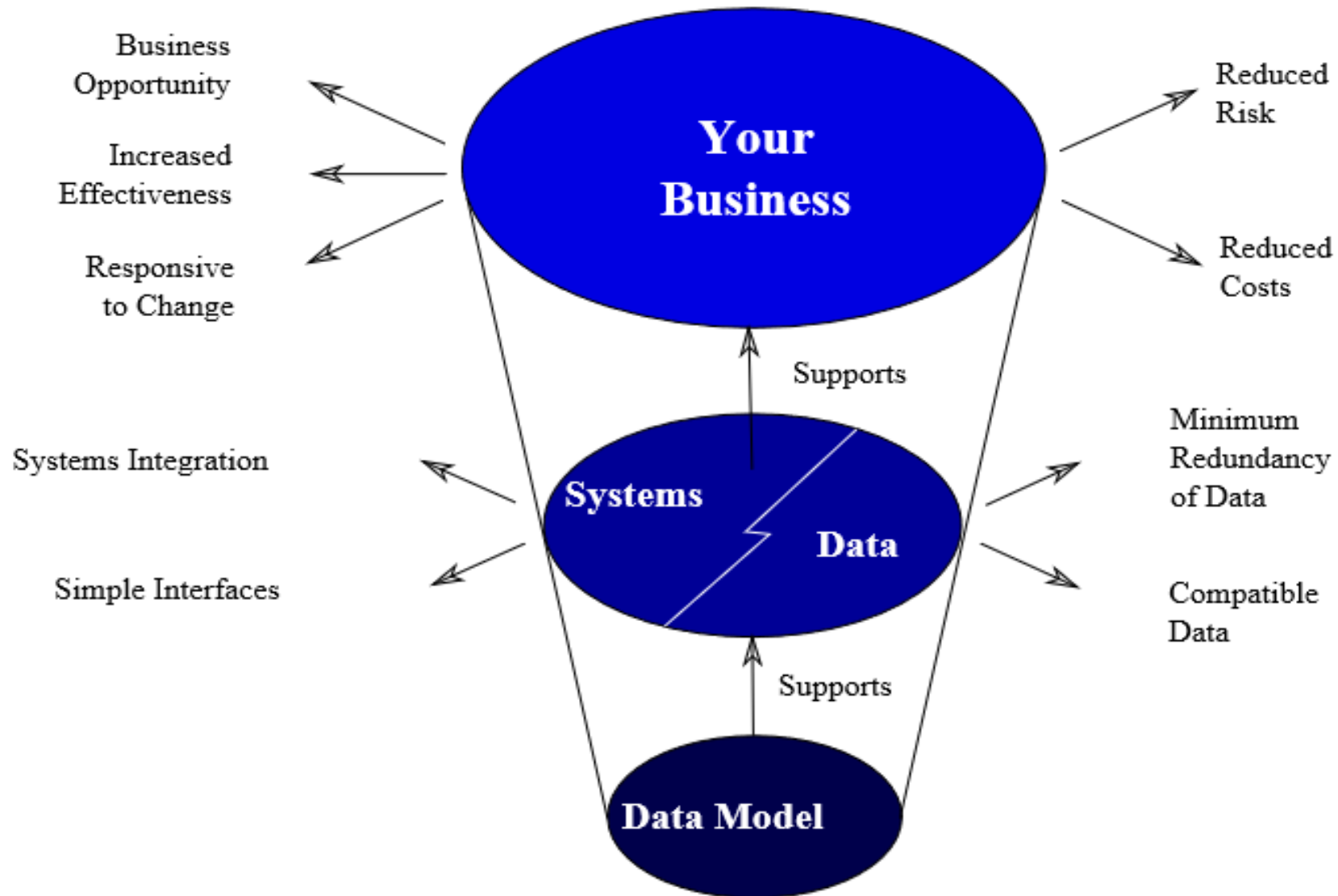


<http://www.onyxinterweb.com/2012/09/business-analysis/>

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。

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

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

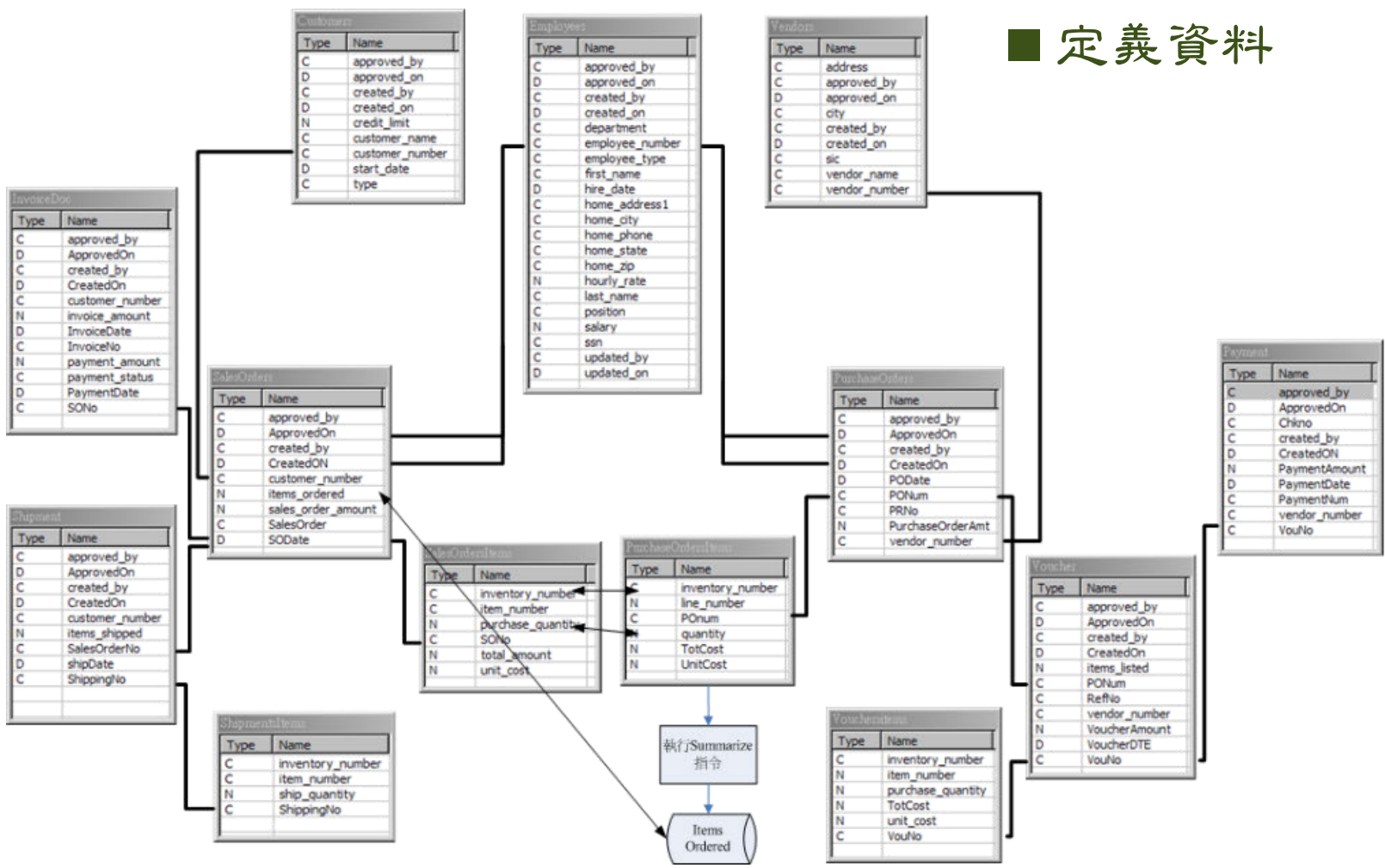
稽核分析能力(二) – 知道選定查核目標範圍的能力

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

稽核分析能力(三) – 知道取得資料源的能力

資料表結構及關係圖 (Table Layout & Relation)

- 找尋查核資料位置
- 取得資料
- 定義資料



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](#) [SQL](#)

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	10155180	28	9.93
10025	237936	01/31/2000	56,767.20	80102618	3,379	16.80
10025	232195	11/14/2000	965.77	80930990	323	2.99
10101	4517604	10/30/2000	154.00	93788411	110	1.40

報表檔(Report file)

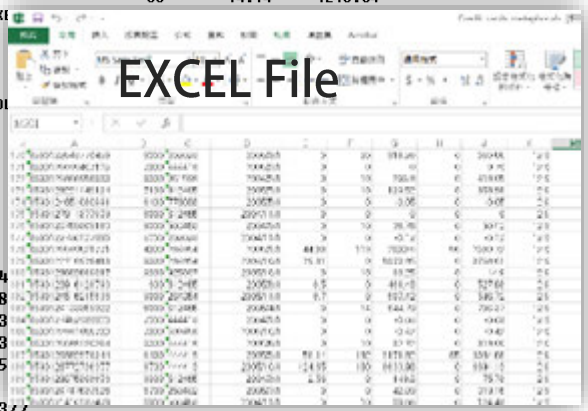
01/08/01
09:44:42

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 HINCER	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:			

EXCEL File



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

Delimited File

```
"employee_number","Name","ID","department","Position","Address","manager","BankAccount","Expense_claim_report_amount"  
"00183","李明云","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","基隆市仁愛區光二一路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","邱建成","E294347311","Training","Manager, Personnel","新竹市香山區五福路3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
```



ims

稽核分析能力(四) – 知道搜尋與推演資料的能力

篩選異常記錄

- Filter
- IF
- Smart Search

	Cust Number	Invoice Date	Due Date	Ref No	Trans Type	Trans Amount
2	795401	10/15/2000	11/14/2000	206300	IN	225.87
3	795401	02/04/2000	03/05/2000	207137	IN	180.92
4	516372	02/17/2000	03/18/2000	211206	IN	1,610.87
7	784647	05/21/2000	06/20/2000	212297	IN	737.36
9	501657	06/30/2000	07/30/2000	212824	IN	1,524.32
11	230575	07/28/2000	08/27/2000	213057	IN	2305.75
21	836004	08/17/2000	09/16/2000	213116	IN	2131.16
22	836004	08/17/2000	09/16/2000	213116	IN	2131.16
23	812465	08/21/2000	11/29/2000	213227	IN	2132.27
24	836004	08/27/2000	09/26/2000	213241	IN	2132.41
25	478504	08/28/2000	09/27/2000	213255	IN	2132.55
38	376505	09/03/2000	10/03/2000	213301	IN	2133.01
39	501657	09/03/2000	10/03/2000	213327	IN	2133.27
40	501657	09/03/2000	03/02/2000	213327	IN	3,633.40
41	501657	09/03/2000	12/02/2000	213326	IN	945.40
42	501657	09/03/2000	03/02/2000	213325	IN	4,426.14
43	925007	09/03/2000	12/02/2000	213318	IN	1,418.09
44	925007	09/03/2000	03/02/2000	213317	IN	2,188.09

演算欄位

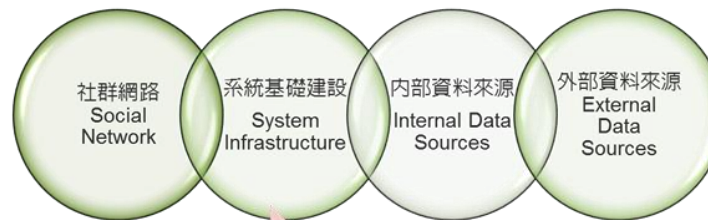
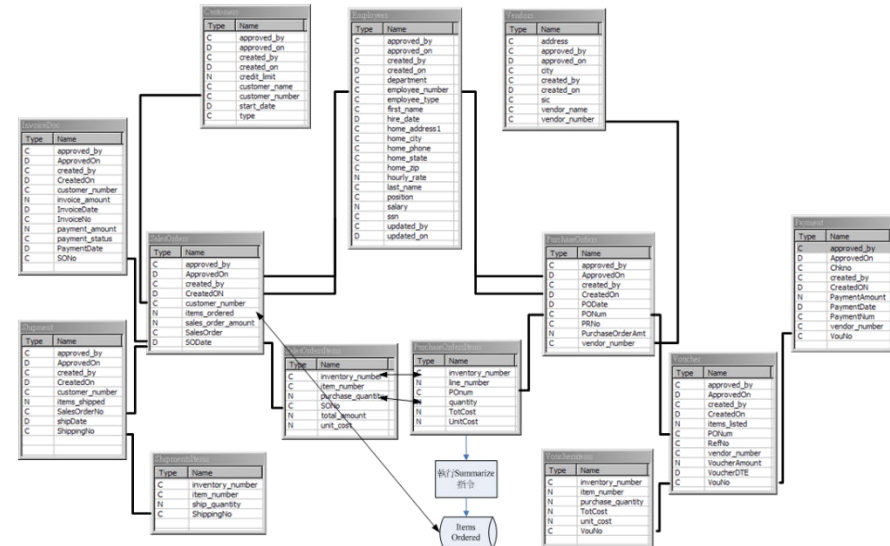
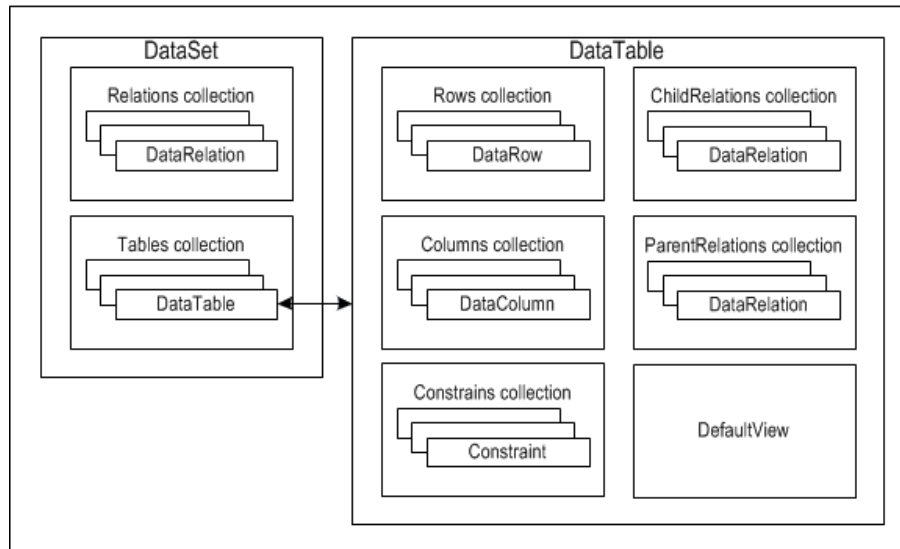
- Computed Field Exc

	Cust Number	Invoice Date	Due Date	Ref No	Trans Type	Trans Amount	VAT Period	NewDue	ChangeDue	Risk
1	795401	08/20/2000	09/19/2000	205505	CN	(474.75)	-23.74	200009	09/19/2000	Low Level
2	795401	10/15/2000	11/14/2000	206300	IN	225.87	11.29	200011	11/14/2000	Mid Level
3	795401	02/04/2000	03/05/2000	207137	IN	180.92	9.05	200003	03/05/2000	Mid Level
4	516372	02/17/2000	03/18/2000	211206	IN	1,610.87	80.54	200003	03/18/2000	Mid Level
5	516372	04/30/2000	03/18/2000	211206	TR	(1,298.43)	-64.92	200003	03/18/2000	Low Level
6	516372	05/21/2000	06/20/2000	212334	CN	(12.23)	-0.61	200006	06/20/2000	Low Level
7	784647	05/21/2000	06/20/2000	212297	IN	737.36	36.87	200006	06/20/2000	Mid Level
8	516372	06/10/2000	07/10/2000	212592	CN	(37.15)	-1.86	200007	07/10/2000	Low Level
9	501657	06/30/2000	07/30/2000	212824	IN	1,524.32	76.22	200007	07/30/2000	Mid Level
10	222006	07/17/2000	01/01/2000	43614X	PM	539.97	27.00	200001	01/01/2000	Mid Level
11	230575	07/28/2000	08/27/2000	213057	IN	2305.75			08/27/2000	Low Level
12	516372	08/17/2000	09/16/2000	213116	IN	2131.16			09/16/2000	Low Level
13	516372	08/17/2000	09/16/2000	213116	IN	2131.16			09/16/2000	Low Level
14	516372	08/17/2000	09/16/2000	213116	IN	2131.16			09/16/2000	Low Level
15	516372	08/17/2000	09/16/2000	213116	IN	2131.16			09/16/2000	Low Level
16	516372	08/17/2000	09/16/2000	213116	IN	2131.16			09/16/2000	Low Level
17	516372	08/17/2000	09/16/2000	213116	IN	2131.16			09/16/2000	Low Level
18	516372	08/17/2000	09/16/2000	213116	IN	2131.16			09/16/2000	Low Level
19	516372	08/17/2000	09/16/2000	213116	IN	2131.16			09/16/2000	Low Level
20	516372	08/17/2000	09/16/2000	213116	IN	2131.16			09/16/2000	Low Level
21	836004	08/17/2000	09/16/2000	213116	IN	2131.16			09/16/2000	Mid Level
22	836004	08/17/2000	09/16/2000	213116	IN	2131.16			09/16/2000	Mid Level
23	812465	08/21/2000	11/29/2000	213227	IN	2132.27			11/29/2000	High Level
24	836004	08/27/2000	09/26/2000	213241	IN	2132.41			09/26/2000	Mid Level
25	478504	08/28/2000	09/27/2000	213255	IN	2132.55			09/27/2000	Mid Level
26	665004	09/03/2000	10/03/2000	213301	IN	2133.01			10/03/2000	Mid Level
27	516372	09/03/2000	10/03/2000	213327	IN	2133.27			10/03/2000	Mid Level
28	262001	09/03/2000	12/02/2000	213304	IN	1,215.54	69.78	200012	12/02/2000	Mid Level
29	262001	09/03/2000	12/02/2000	213304	IN	614.78	30.74	200012	12/02/2000	Mid Level
30	262001	09/03/2000	12/02/2000	213304	IN	614.78	30.74	200012	12/02/2000	Mid Level
31	262001	09/03/2000	12/02/2000	213304	IN	614.78	30.74	200012	12/02/2000	Mid Level
32	665004	09/03/2000	10/03/2000	213301	IN	2133.01			10/03/2000	Mid Level
33	665004	09/03/2000	10/03/2000	213301	IN	2133.01			10/03/2000	Mid Level
34	6414	09/03/2000	10/03/2000	213301	IN	2133.01			10/03/2000	Mid Level
35	262001	09/03/2000	12/02/2000	213304	IN	614.78	30.74	200012	12/02/2000	Mid Level
36	262001	09/03/2000	12/02/2000	213304	IN	614.78	30.74	200012	12/02/2000	Mid Level
37	925007	09/03/2000	12/02/2000	213318	IN	1,418.09			12/02/2000	Mid Level
38	376505	09/03/2000	10/03/2000	213301	IN	2133.01			10/03/2000	Mid Level

稽核分析能力(五) – 知道驗證資料完整性的能力

- 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

資料表結構及關係圖 (Table Layout & Relation)



載入

Data Warehouse

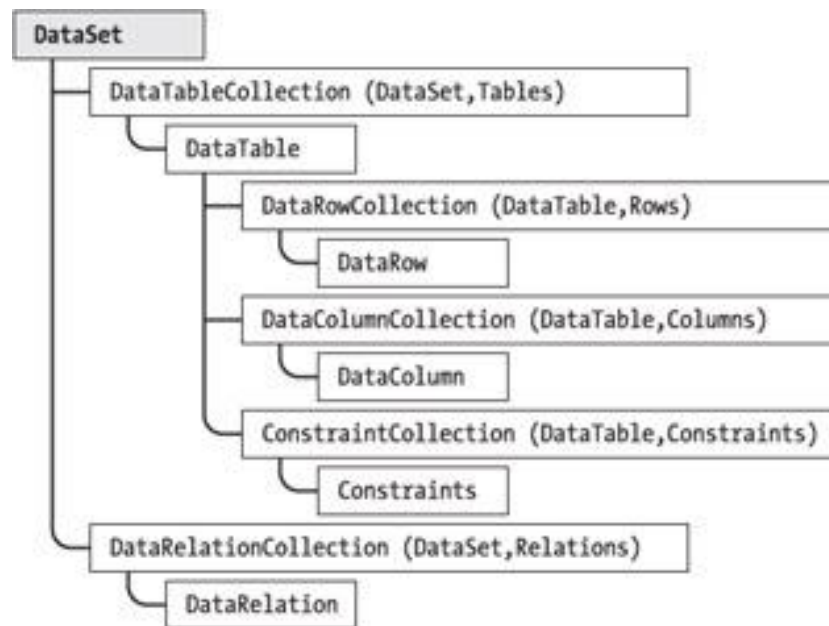
建立資料集(Data Set) — 檢視(View)/查詢(Enquiry)

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

稽核分析能力(七) – 知道找出異常態樣資料的能力

- 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

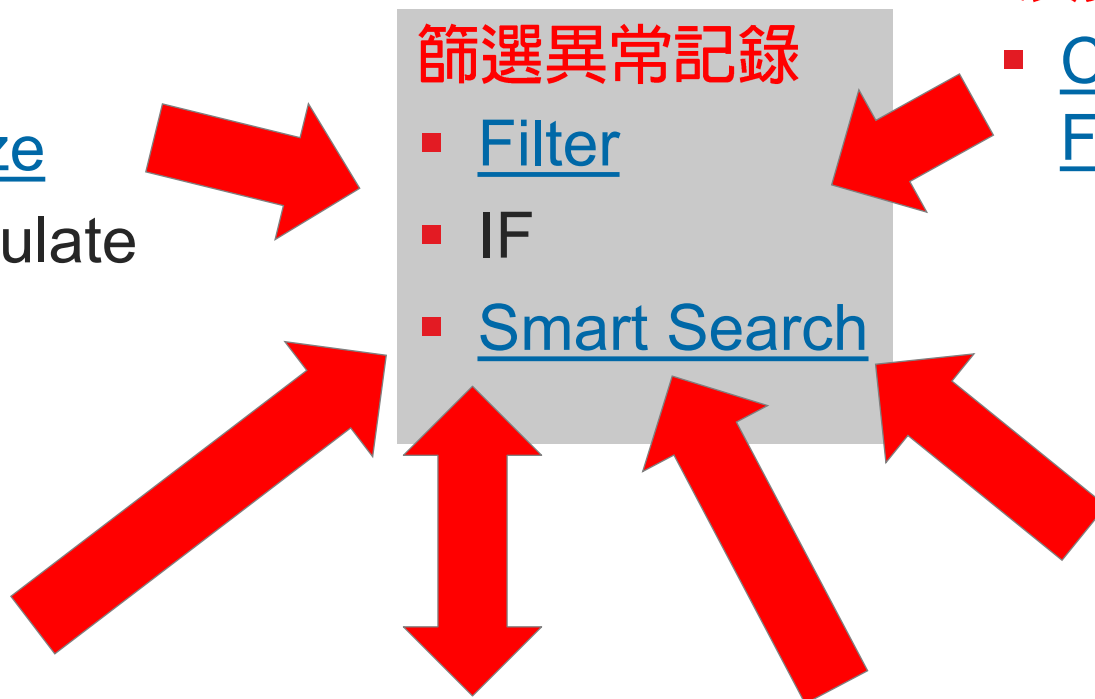
- Duplicate
- Gap

演算欄位

- Computed Field Exc

篩選異常記錄

- Filter
- IF
- Smart Search

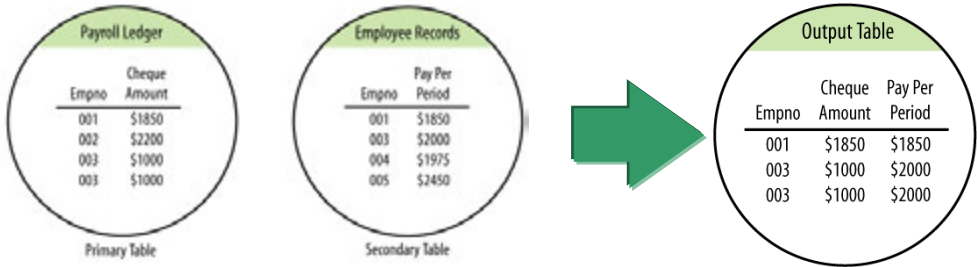


稽核分析能力(八) – 知道多檔案資料分析比對能力

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 lists five options, each with a visual representation of the join and a '選擇(H)...' button. Red checkmarks are placed next to the first, fourth, and fifth options.

- 選擇聯結類型: 與主要資料表紀錄相符 (Visual: Venn diagram with intersection shaded)
- 選擇聯結類型: 與主資料表相符及所有主要資料表紀錄 (Visual: Venn diagram with intersection shaded)
- 選擇聯結類型: 與主資料表相符及所有次要資料表紀錄 (Visual: Venn diagram with intersection shaded)
- 選擇聯結類型: 與主資料表相符及所有主和次要資料表紀錄 (Visual: Venn diagram with intersection shaded)
- 選擇聯結類型: 與主要資料表紀錄不相符 (Visual: Venn diagram with intersection unshaded)
- 選擇聯結類型: 與主要資料表相符的多對多紀錄 (Visual: Venn diagram with intersection shaded)
- 選擇聯結類型: 包含所有主要和次要資料表的多對多 (Visual: Venn diagram with intersection shaded)

This screenshot shows a 'Relations' window with two tables: 'AR (父值)' and 'AR_Sort'. The 'AR (父值)' table has columns: amount (N), date (D), DO, true (D), Included_Tax (N), MM, no, Period, ref, Rank, type, VAT (N), YY. The 'AR_Sort' table has columns: amount (N), date (D), Included_Tax (N), MM, no, Period, ref, Rank, type, VAT (N), YY. A line connects the 'AR (父值)' table to the 'AR_Sort' table.

This screenshot shows a software interface for comparing two tables. The title is 'GRC & Business Assurance Analytics Technology'. The main area displays a table with columns: ID, Project, Status, and others. A red box highlights the 'Arbutus Compare / 比較' section.

什麼是模糊重複測試

定義：模糊測試是依據Damerau—Levenshtein distance理論，來演算編輯距離。

以新增、刪除、替代、相鄰，這四種方式演算編輯距離。

可應用在：字元、數字、日期的欄位內容

		1	2	3	4
	0	1	2	3	4
2	1	1	1	2	3
1	2	1	1	2	3
4	3	2	2	2	2
3	4	3	3	2	2

編輯距離：相鄰、新增、新增

編輯距離：相鄰、相鄰

Fuzzy Duplicate(Near)

- (EX:在可能重複採購單中，將輸入日期改為相近)

→ 原始資料熊様

產出結果

<<檔案結束>>

模糊重複-找出特殊符號或外表相似的資料 Fuzzy Duplicate(Similar)

- 某一個欄位中內容存有一些特殊符號，或者相似的資料態樣，使得增加資料驗證的困難度 (EX:採購單單號是否有此類情況)

	REQUISITION_HEADER_ID	ORIGIN	VENDOR_ID	VENDOR_NAME	OPRID_ENTERED_B
1	135427	ACQ	0000000103	PIACREPIT SCREENING SERVICES LI	BMCLAREN
2	135443	ACQ	0000000123	MI	ljmcmill
3	135444	ACQ	0000000123	MI	ljmcmill
4	135446	ACQ	0000000123	MI	ljmcmill
5	135452	ACQ	0000000153	LABOTT LABORATORIES INC	GEFISH
6	135457	ACQ	0000000153	LABOTT LABORATORIES INC	NLHERNAN
7	135460	ACQ	0000000376	PETION PERSONNEL INC	BMCLAREN
8	135461	ACQ	0000000539	PVANCEP MEPICAL SUPPLY LLC	eawillia
9	135462	ACQ	0000000586	MRIFORM INC	sjridge
10	135463	ACQ	0000000590	ROCOM	magordon
11	135464	ACQ	0000000832	ICATEL INTERNETWORKING	sstein
12	135465	ACQ	0000000862	LAERT ALARMS BURGLAR & FIRE PRO	sjridge
13	135466	ACQ	0000000971	YSLEN SYSTEMS GROUP	lvasquez

	REQUISITION_HEADER_ID	REQUISITION_HEADER_ID2
1	135501	135501
2	135540	135540
3	173730	173730
4	186233	186233-
5	186281	186281'
<< 檔案結束 >>		

原始資料態樣

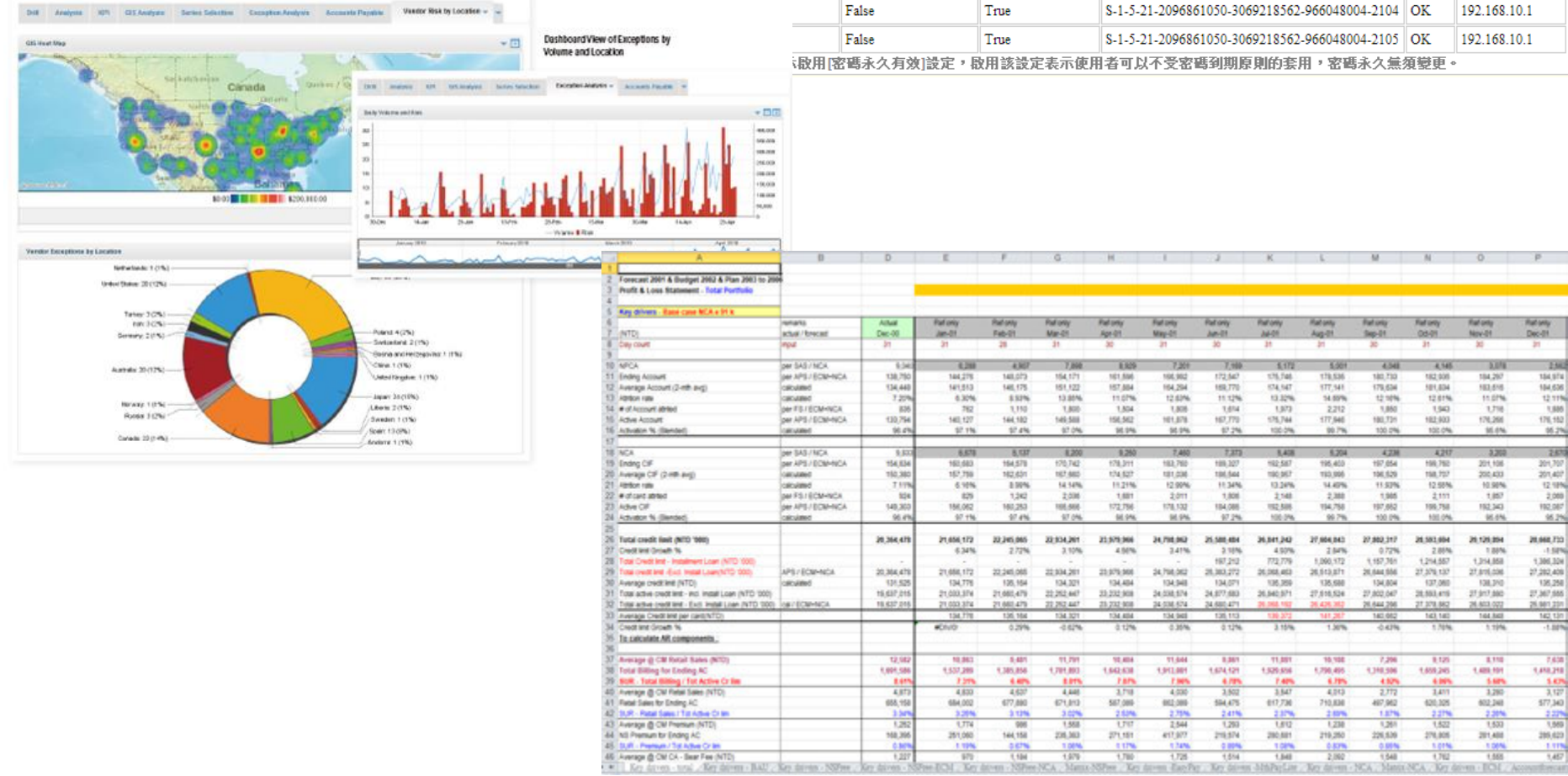
產出結果

稽核分析能力(九) – 知道匯出檔案及報表的能力

報表名稱(Report Title): DOMAIN USERS PASSWORD EXPIRY INFORMATION
報表說明(Report Description): 此張報表列出所有啟用[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	True	S-1-5-21-2096861050-3069218562-966048004-2104	OK	192.168.10.1
				False	True	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。



稽核分析能力(十) – 知道整合分析策略的能力

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
6. 輸出查核報告

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

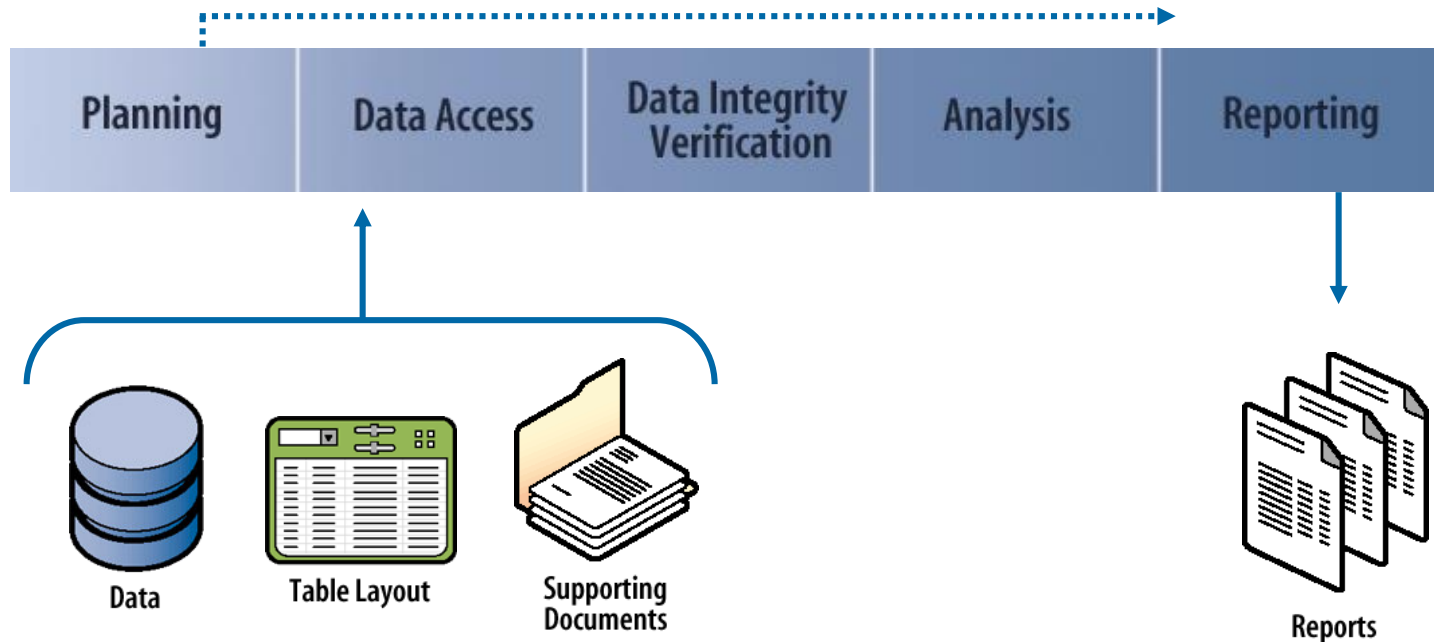
Payments		
payment_number	C	12
payment_date	D	8
payment_amount	N	14
vendor_number	C	17
check_number	C	12
voucher_number	C	12
created_by	C	10
created_on	D	8
approved_by	C	10
approved_on	D	8

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

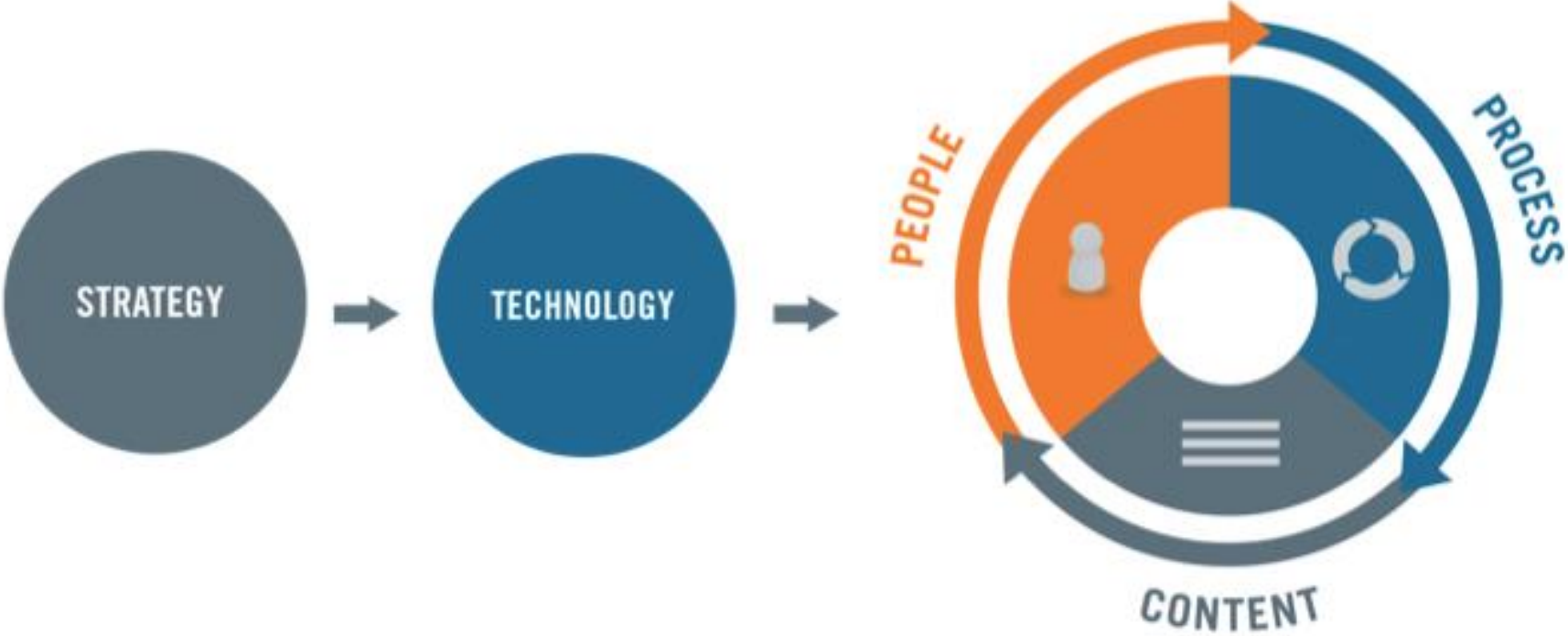
Employees		
employee_number	C	10
first_name	C	20
last_name	C	25
ssn	C	12
department	C	30
position	C	30
employee_type	C	2
hire_date	D	10
home_phone	C	15
home_address1	C	50
home_city	C	20
home_state	C	2
home_zip	C	5
hourly_rate	N	8
salary	N	10
created_by	C	10
created_on	D	10
approved_by	C	10
approved_on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

資料分析循環(The Data Analysis Cycle)

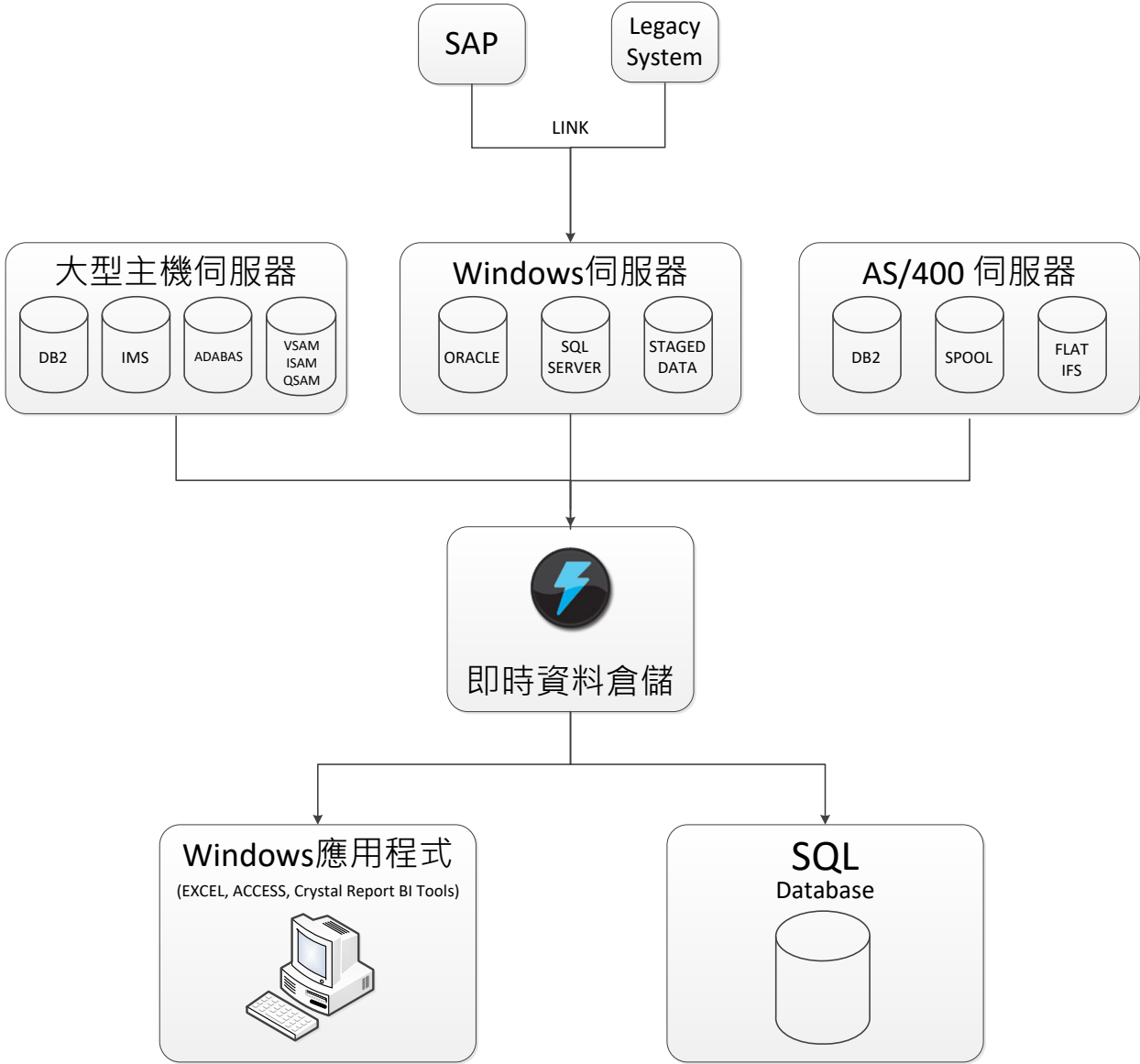
- 規劃(Planning)
- 資料存取(Data access)
- 資料完整性驗證(Data integrity verification)
- 資料分析(Data analysis)
- 查核報告(Reporting results)



持續性稽核實行步驟



即時資料倉儲 - Instant Data Warehouse



稽核程式自動化/Procedure

進階技術能力

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_LEAVEENO"
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_LEAVEENO
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_LEAVEENO"
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

Arbutus Procedure – Advance Function(1)

SKLProj - 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)

Dialog Folder

檔案 常用 共用 檢視

下載 文件 音樂 圖片 影片 OS (C:) Data (D:) SRECYCLE.BIN ACLSoftware Adobe Software Application Files Arbutus Arbutus Data File Brad Business Development Desktop David FFOutput Mail Marketing MSOCache Multimedia Files NORTHWIND OneDrive Pentana Project Library SQL Server 2000 Sample Databases System Volume Information Temp Test Training UprofitDigital Windows OS Hardening 公會會員學術單位 Windows OS Hardening.zip TOSHIBA EXT (E) Active Drive (F:) Vic-D (\\172.16.50.140) (F:) Vic-e (\\172.16.50.140) (U) 27 個項目 已開啟 1 個項目 4.13 KB

名稱 修改日期 類型 大小

Sample	2014/12/1 下午 0...	檔案資料夾	
EmpFilter.aww	2014/12/1 下午 0...	AWW 檔案	1 KB
EmpFilter.fil	2014/12/1 下午 0...	FL 檔案	1 KB
EmpFilter.fmt	2014/12/1 下午 0...	FMT 檔案	2 KB
Employees2.aww	2014/11/27 下午...	AWW 檔案	1 KB
Employees2.fil	2014/11/27 下午...	FL 檔案	4 KB
Employees2.fmt	2014/11/27 下午...	FMT 檔案	2 KB
Employees2OX.aww	2014/12/12 下午...	AWW 檔案	1 KB
Employees2OX.fil	2014/12/12 下午...	FL 檔案	1 KB
Employees2OX.fmt	2014/12/12 下午...	FMT 檔案	1 KB
F01_洗線.pro	2014/12/20 下午...	PRO 檔案	5 KB
F02_新裝.pro	2014/12/22 下午...	PRO 檔案	3 KB
F03_新裝.pro	2014/12/22 下午...	PRO 檔案	3 KB
F04_保養.pro	2014/12/19 下午...	PRO 檔案	3 KB
F05_保養過程.pro	2014/12/19 下午...	PRO 檔案	3 KB
F06_保養報告.pro	2014/12/19 下午...	PRO 檔案	3 KB
F07_保養過程及保養報告.pro	2014/12/19 下午...	PRO 檔案	3 KB
F08_維修.pro	2014/12/19 下午...	PRO 檔案	4 KB
F09_新裝.pro	2014/12/19 下午...	PRO 檔案	3 KB
F12_ETF.pro	2015/3/5 下午 02...	PRO 檔案	3 KB
F13_ETF_CHANGE.pro	2015/3/5 下午 04...	PRO 檔案	3 KB
F14_ETF_ORDER.pro	2015/3/5 下午 04...	PRO 檔案	3 KB
F15_ETF_RISK.pro	2015/3/5 下午 03...	PRO 檔案	3 KB
F16_不動產.pro	2015/3/5 下午 05...	PRO 檔案	3 KB
F17_進程.pro	2015/3/5 下午 05...	PRO 檔案	3 KB
F18_臺北.pro	2015/3/5 下午 05...	PRO 檔案	3 KB
New_Procedure.pro	2014/12/18 下午...	PRO 檔案	1 KB

Arbutus Procedure
以實體檔案存在

DA\Project Library\Sing Kong\SingKongProj\SKLProj\Dialog Folder\F01_洗線.pro - Notepad++

```

40  DescriptE = Alltrim(DescriptE) + ";" + Alltrim(ItemName) + Blanks(60)
41  End
42
43  Open 二階單位
44  Group
45  DescriptF = Alltrim(DescriptF) + ";" + Alltrim(ItemName) + Blanks(60)
46  End
47
48
49  Do Procedure .DialogPro while Postflag
50
51
52
53  Set Safety on
54
55
56
57  Procedure DialogPro
58  Postflag = F
59  CHECKBOX1 = F
60
61  if SelectDept = 1 DIALOG (DIALOG TITLE "洗線防制作業辦理情形之查核 - 服務中心-01" WIDTH 721
HEIGHT 323 ) (BUTTONSET TITLE "確定(60);取消(60)" AT 396 228 DEFAULT 1 MORE ) (DROPDOWN TITLE
"%DescriptA%" TO "DROPDOWN1" AT 396 94 WIDTH 242 DEFAULT 2 ) (CHECKBOX TITLE "是否結束輸入?" TO
"CHECKBOX1" AT 48 239 WIDTH 203 ) (TEXT TITLE "請選擇服務中心別" AT 48 96 ) (TEXT TITLE
"(1).請輸入篩選條件後按下確定進行查詢" AT 36 24 WIDTH 300 HEIGHT 14 ) (TEXT TITLE
"(2).選擇服務中心後請勾選「結束條件輸入」並按下確定即可產出篩選後的報表" AT 36 48 ) (TEXT TITLE
"請輸入申報日期(起) (年(民國).月.日) : " AT 48 132 ) (TEXT TITLE "請輸入申報日期(止)
(年(民國).月.日) : " AT 48 168 ) (EDIT TO "StartDate" AT 396 130 CHAR ) (EDIT TO "EndDate" AT 396
166 CHAR )
62
63
64  if SelectDept = 2 DIALOG (DIALOG TITLE "洗線防制作業辦理情形之查核 - 業務部室-02" WIDTH 725
HEIGHT 415 ) (BUTTONSET TITLE "確定(60);取消(60)" AT 396 324 DEFAULT 1 MORE ) (DROPDOWN TITLE
"%DescriptB%" TO "DROPDOWN1" AT 396 94 WIDTH 242 DEFAULT 2 ) (CHECKBOX TITLE "是否結束輸入?" TO
"CHECKBOX1" AT 48 239 WIDTH 203 ) (TEXT TITLE "請選擇部室別" AT 48 96 ) (TEXT TITLE

```

Normal text file length: 5557 lines: 75 Ln:1 Col:1 Sel:0|0 Doc/Windows Big5 (Traditional) IN5

1 筆記錄 D:\Project Library\Sing Kong\Test\SKLProj\SKLProj\Dialog Folder\EmpFilter.fil

Arbutus Procedure – Advance Function(2)

UPGeneral - 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

UPGeneral [D:\Arbutus\Sample Files\Course Data\UP10General\UPGeneral\Accounts_receivable_audit\Top_Customer_AR_.fil]

Accounts_payable

Accounts_receivable_audit

A123

AR

ARCLF

Customer

Pro_1

Pro_2

SAMPLEfile

Top_Customer_AR_ (Selected)

Top_Customer_AR_

Trans

TRANSTXT

Inventory_review

Payroll_analysis

result

WorkFolder

AllSCH_List

AllSystemFileOwner_Access

AR2

Badfile

Customers

Demo

Invoices

New_Procedure_2

指令日誌

Top_Customer_AR_

Top_Customer_AR_ x

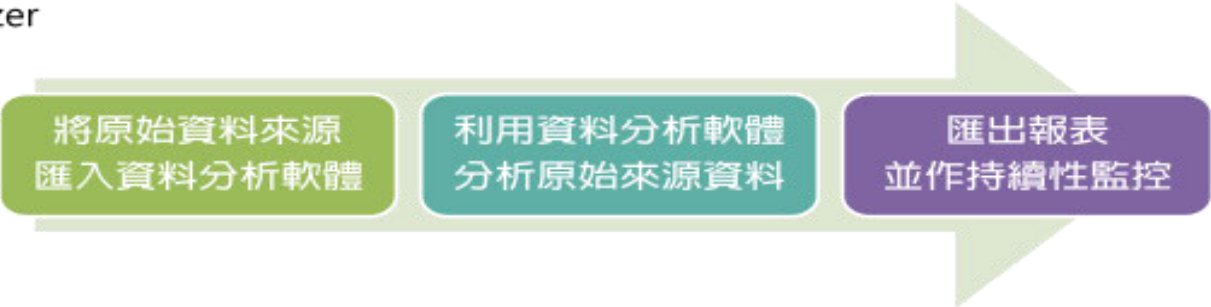
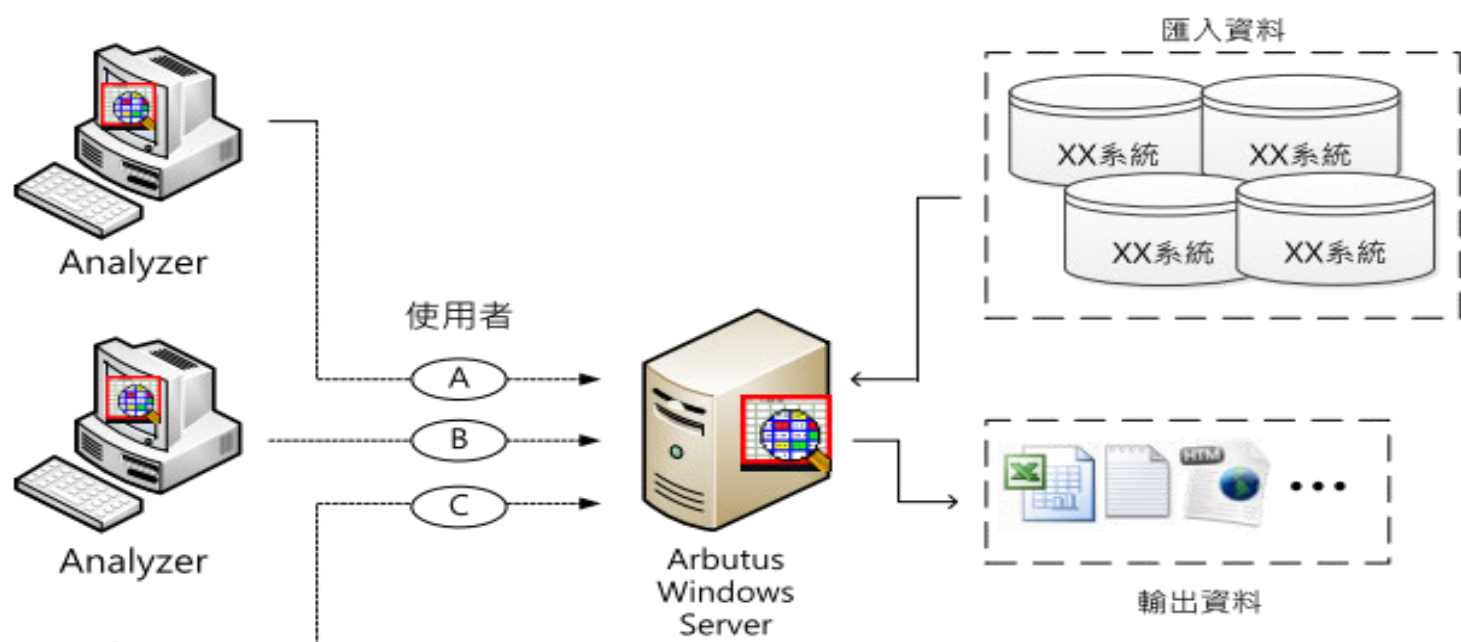
Smart Search

	Cust Number	Count	計數的百分比	欄位的百分比	Trans Amount
1	065003	115	14.90	20.45	95891.01
2	176437	18	2.33	2.73	12805.12
3	262001	101	13.08	9.45	44319.60
4	297397	18	2.33	3.13	14691.12
5	376005	30	3.89	3.10	14537.22
6	501657	52	6.74	4.89	22939.52
7	516372	94	12.18	8.49	39814.86
8	641464	34	4.40	5.82	27266.97
9	811002	55	7.12	7.88	36965.26
10	925007	93	12.05	17.97	84272.93

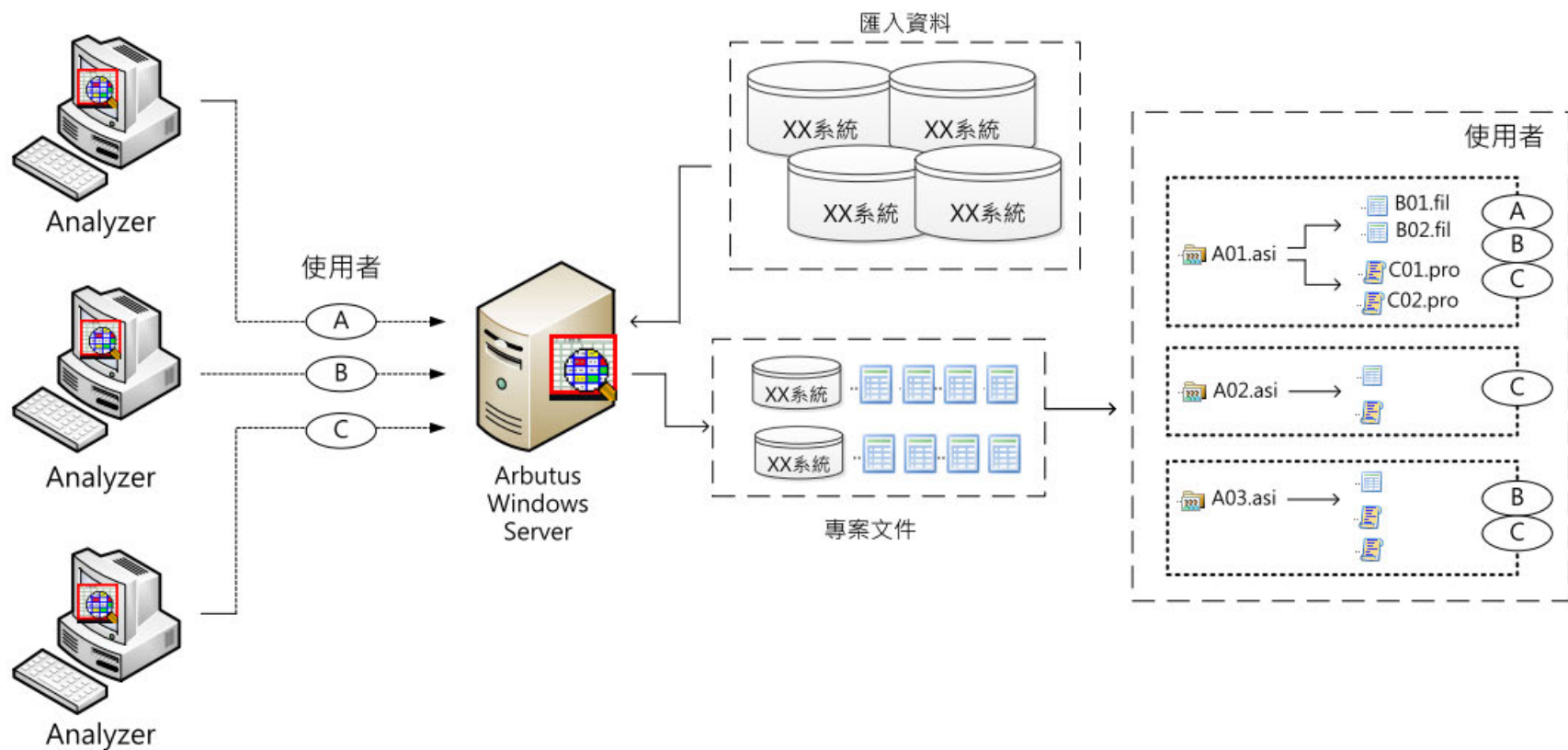
<< 檔案結尾 >>

Open Table with auto run procedure

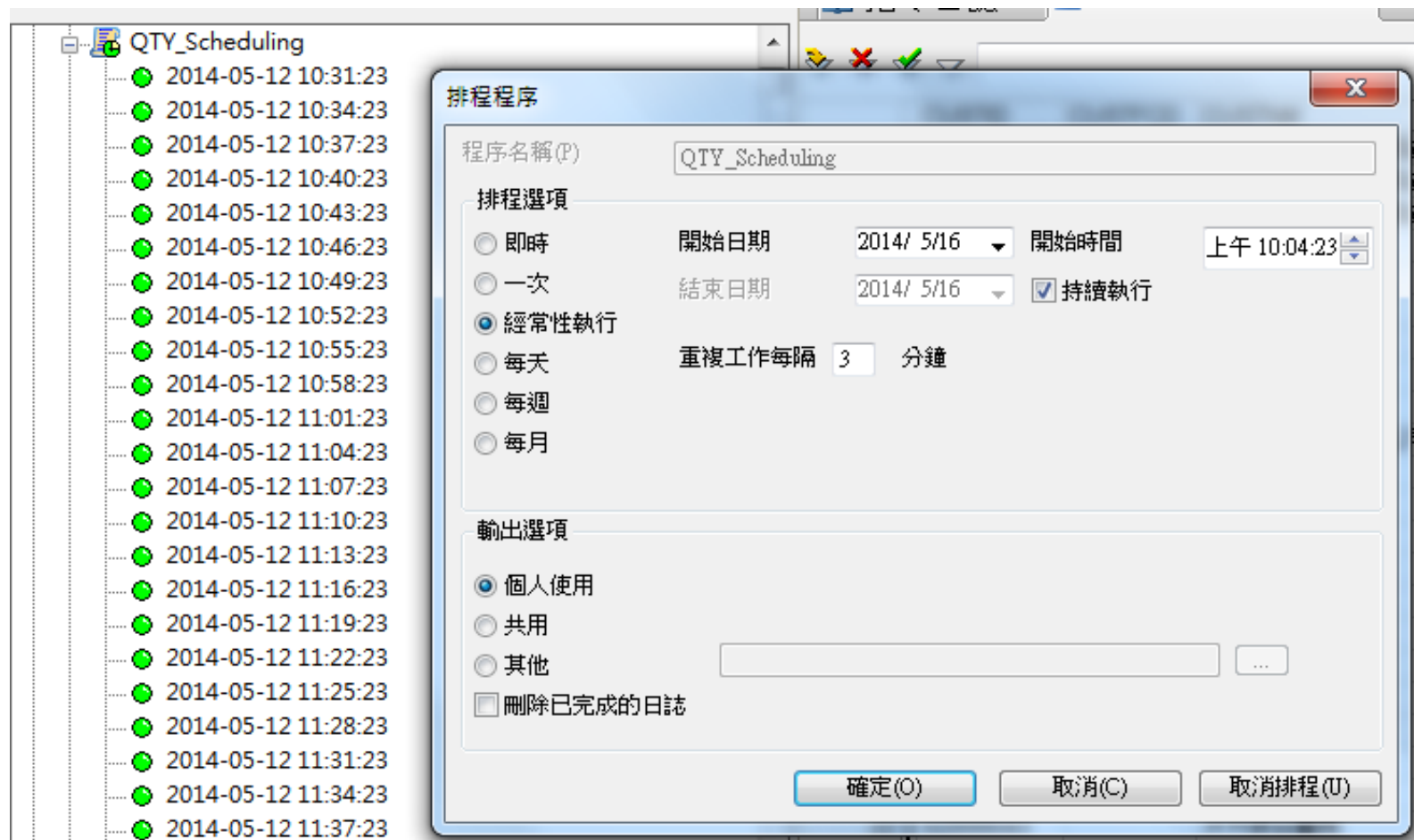
10 筆記錄 D:\Arbutus\Sample Files\Course Data\UP10General\UPGeneral\Accounts_receivable_audit\Top_Customer_AR_.fil



Arbutus Server 系統管理員可依據企業資安政策，可參照實際情境控管存取等級，防止不必要的資料存取。



資料排程(Scheduling)



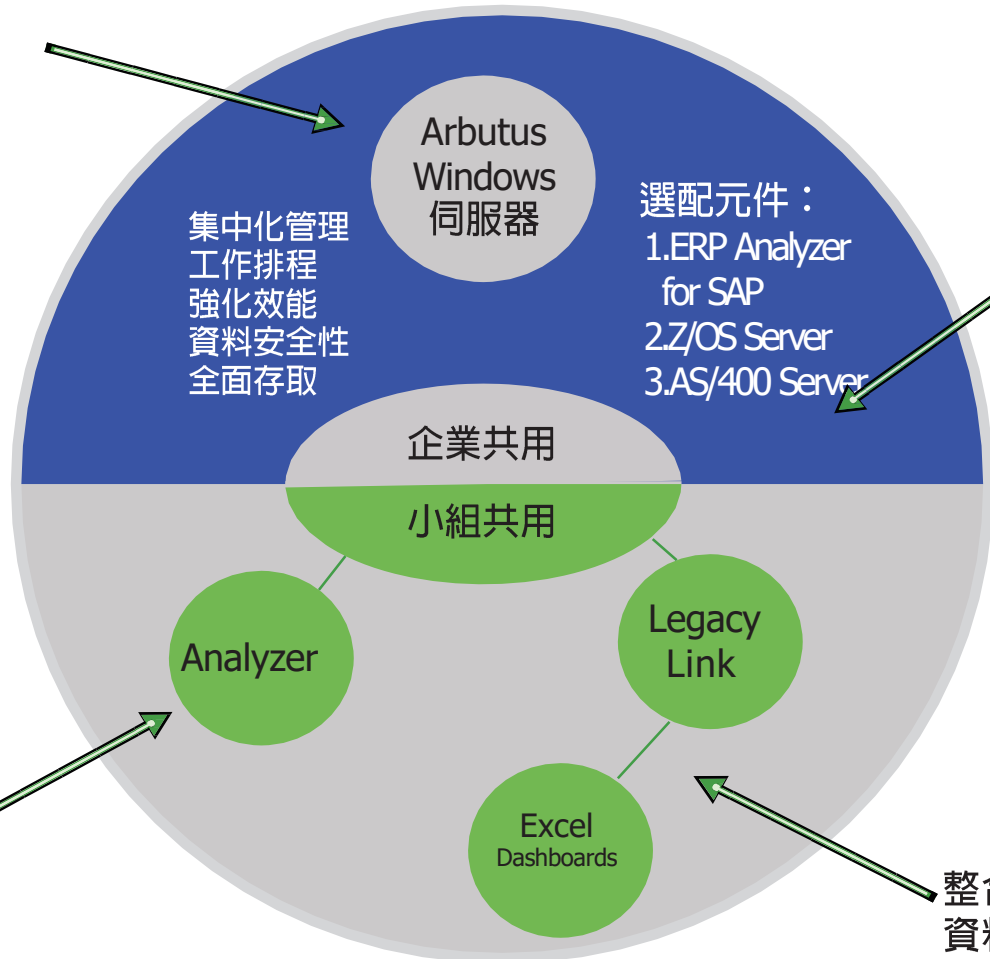
系統及資料安全

- 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。

小組/企業共用系統架構

集中化的資料管理：

- 易用性
- 可承受性
- 高效能



使用企業共用以及小組共用，能簡易地與組織內成員共同使用與分享資料

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



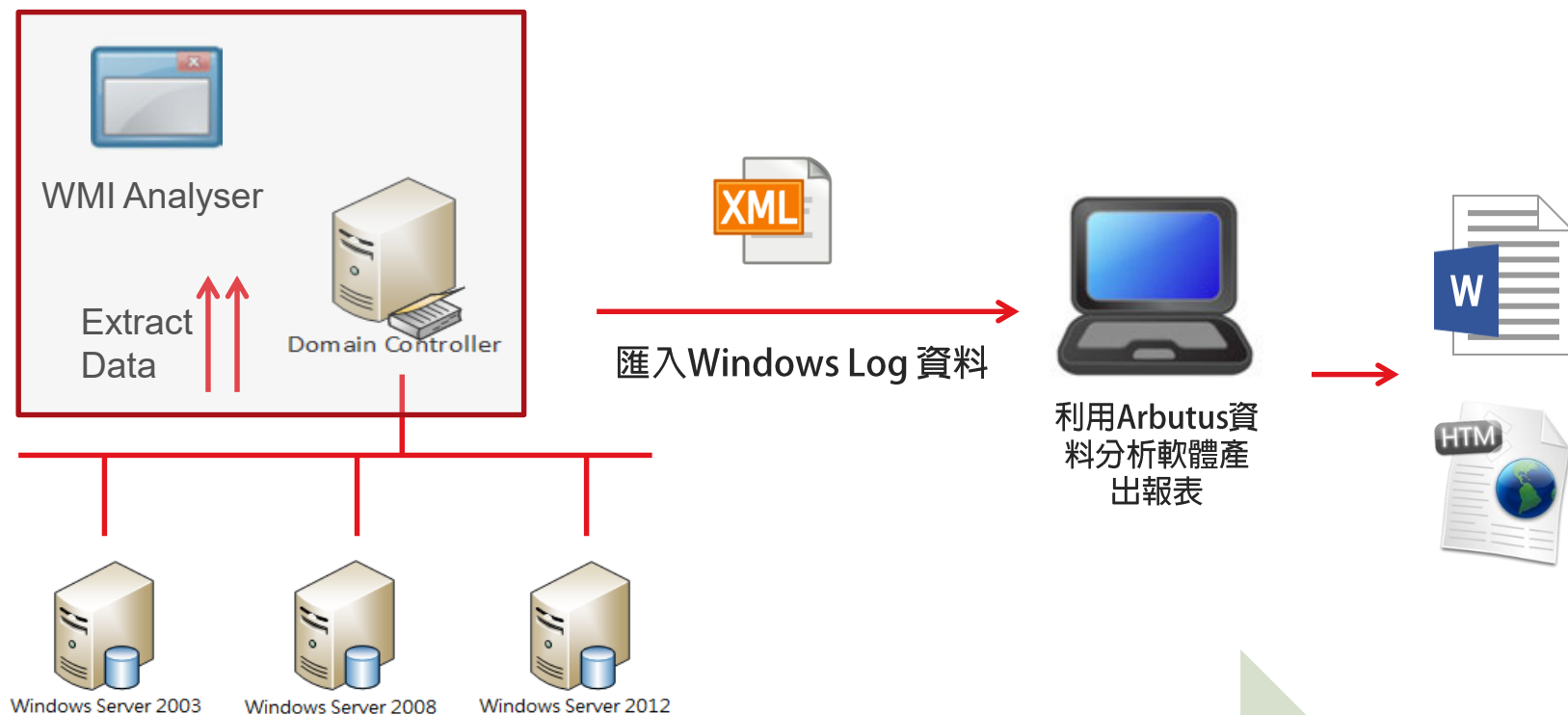
透過Arbutus Windows Server進行資料集中化管理並加強資料安全性，使用排程功能達到持續性監控的目的

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):

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(U)

☐ 到期日(E):

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(I)

Active Directory 使用者和電腦 [DC1.uprofit.test-n] 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):

使用者登入名稱 (Windows 2000 前版)(W):

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(U)

☐ 到期日(E):

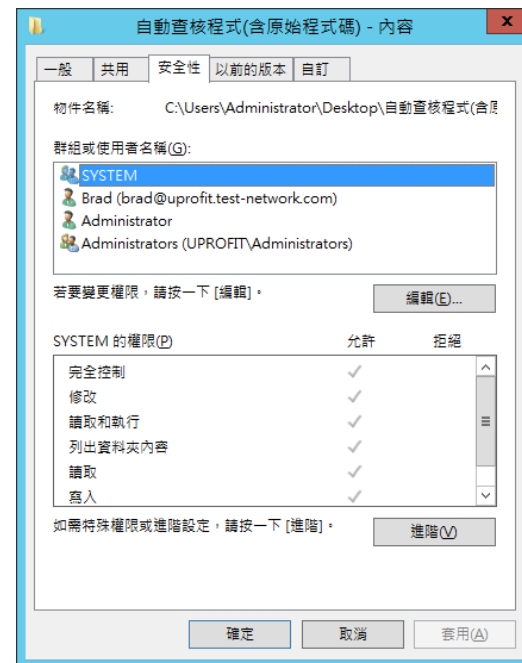
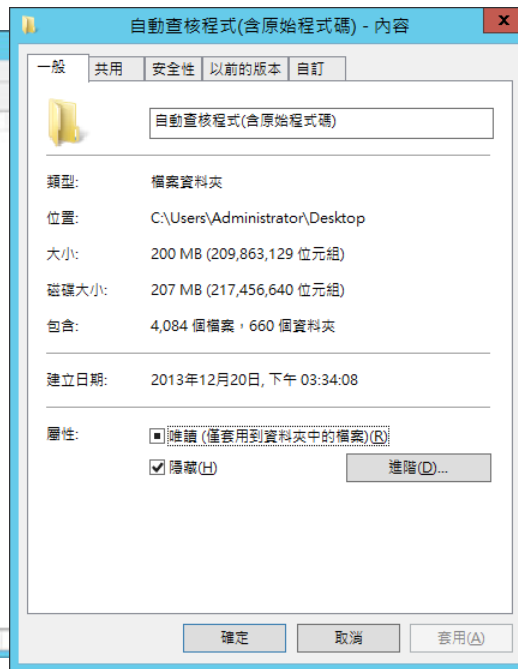
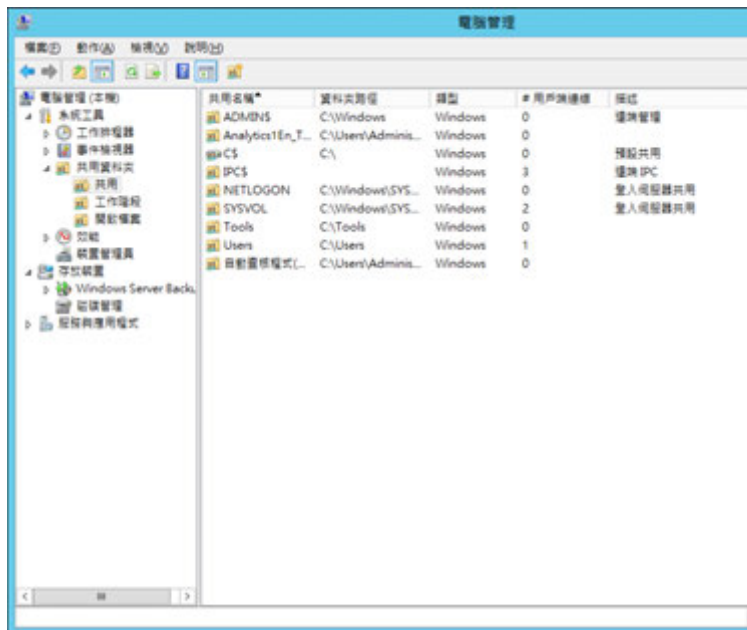
確定 取消 套用(A) 說明

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

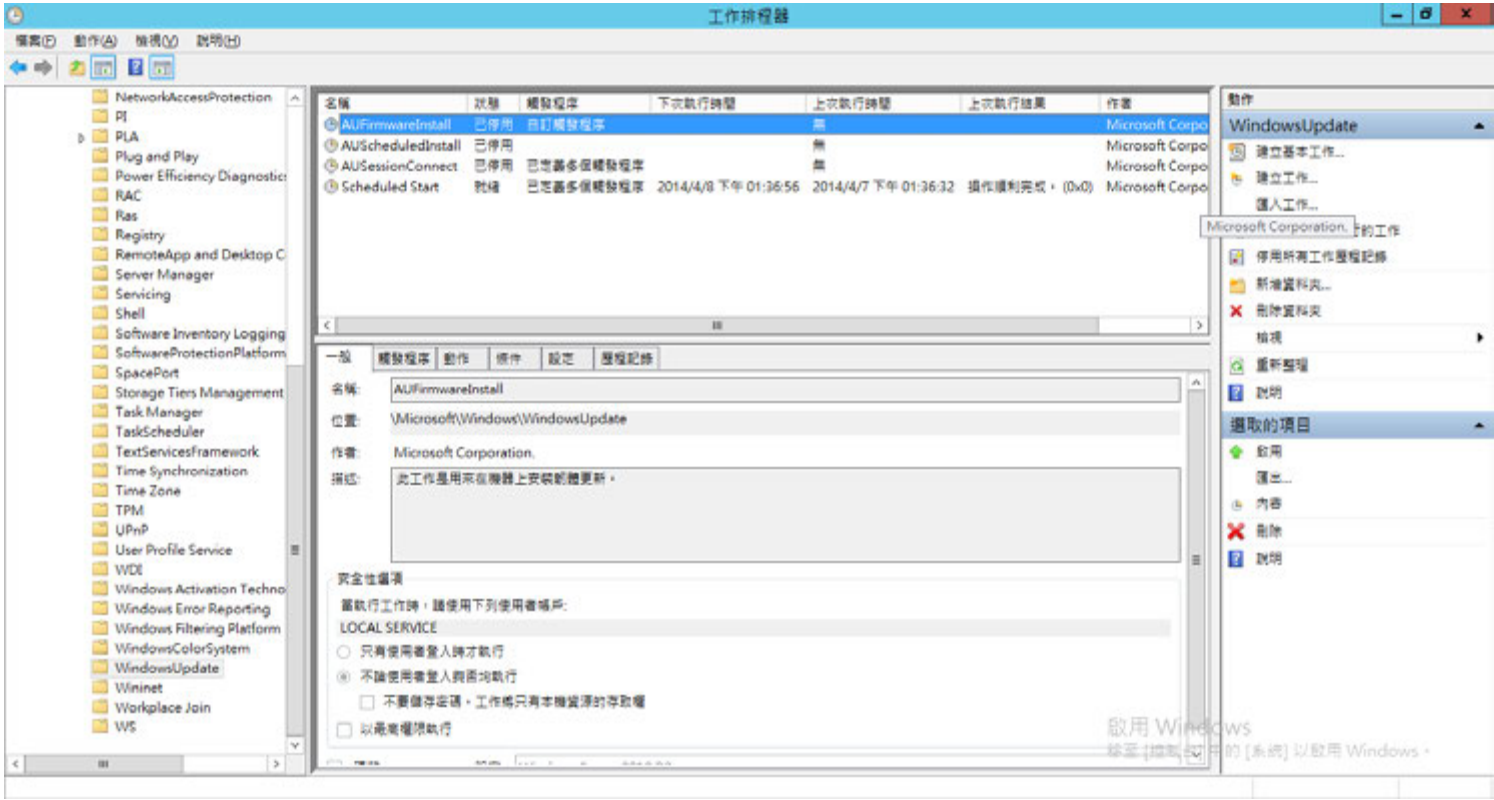


六大查核模組功能介紹

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

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。

全部隱藏

隱藏

顯示

隱藏

顯示

顯示

隱藏

顯示

隱藏

顯示

顯示

隱藏

顯示

顯示

隱藏

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

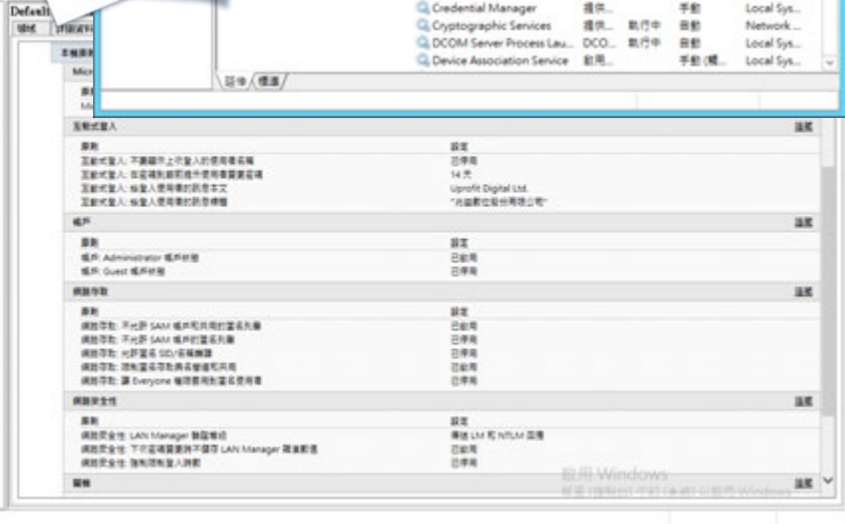


- 依系統特性(Web Server、DB Server、Domain Controller)提供安全設定最佳化之參照標準並定義於Arbutus的比對樣本中，於資料搜集及分析時可供直接套用檢核。
 - 伺服器螢幕保護裝置啟用時間設定檢核
 - 帳號及密碼安全設置/配置 (Security Setting/Configure)的資訊安全政策
 - 確認未啟動不必要的程式或服務
 - 系統重要檔案之權限設定檢核
 - Windows Registry之設定檢核
 - 群組原則政策(Group Policy)檢核
 - 系統修補程式更新檢核

六大查核模組功能介紹

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

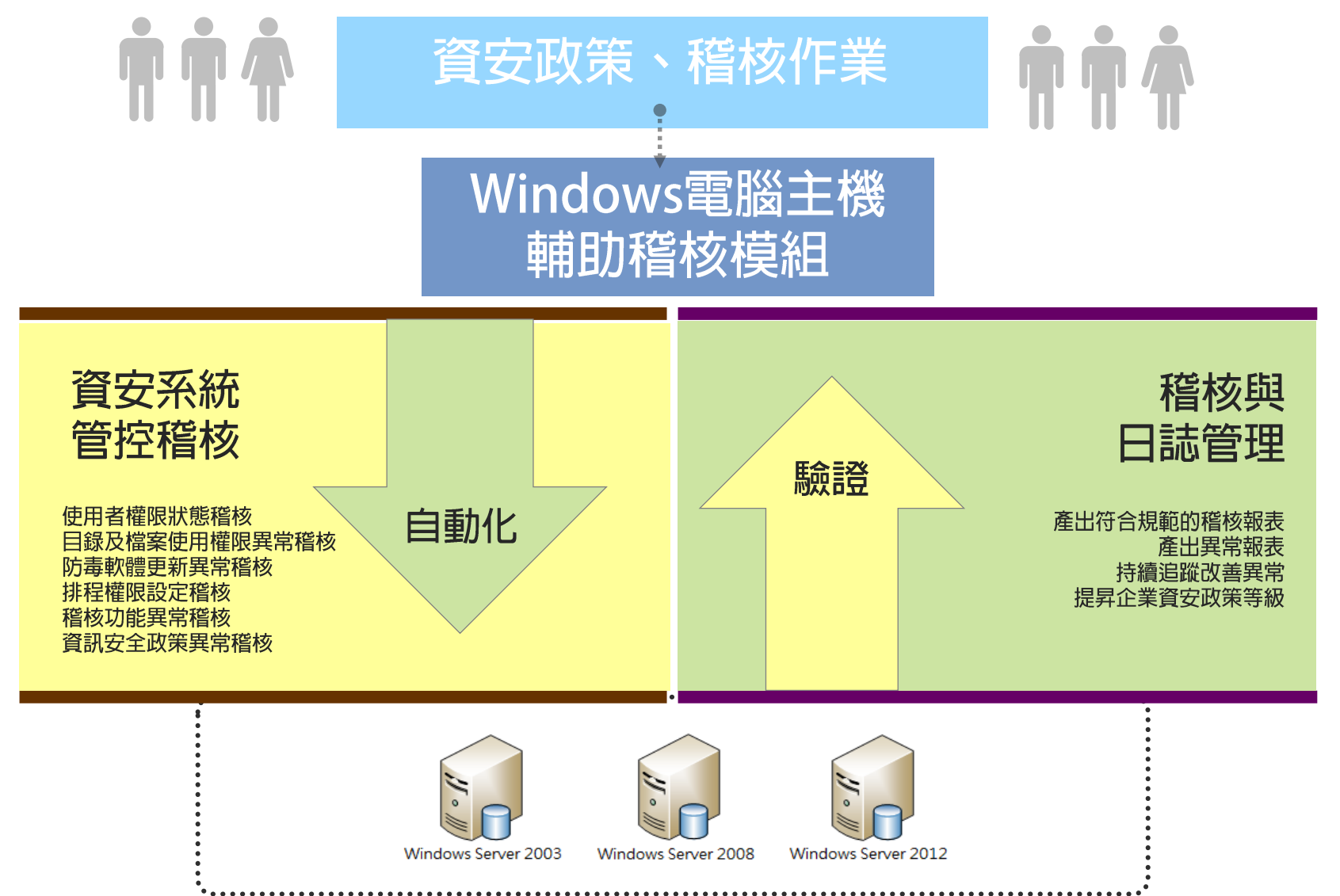
報表名稱(Report Title): **HIDDEN_FOLDERS_REPT**
報表說明(Report Description): 此張報表列出所有被隱藏的資料夾
報表日期(Report Date):2014/7/14 下午 09:42

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?



A scenic landscape photograph showing a green hillside with a blue windmill in the distance, surrounded by trees and mountains under a cloudy sky.

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>