

控制、風險與 治理個案實戰

CONTROL, RISK AND GOVERNANCE
CASE STUDIES

蘇淑美、陳錦烽 著

37個

引人矚目的真實故事

智勝
BEST-WISE

Control, Risk and Governance
Case Studies

Case

控制、風險與治理



蘇淑美、陳錦烽 著

智勝文化

控制、風險與治理個案實戰

Control, Risk and Governance Case Studies

國家圖書館出版品預行編目資料

控制、風險與治理個案實戰 / 蘇淑美, 陳錦烽著.

-- 初版.-- 臺北市: 智勝文化, 2013.04

面; 公分

ISBN 978-957-729-921-5(平裝)

1. 企業管理 2. 內部控制 3. 風險管理 4. 個案研究

494

102006128

作者/蘇淑美、陳錦烽

發行人/紀秋鳳

出版/智勝文化事業有限公司

地址/台北市 100 館前路 26 號 6 樓

電話/(02)2388-6368

傳真/(02)2388-0877

郵撥/16957009 智勝文化事業有限公司

登記證/局版臺業字第 5177 號

出版日期/2013 年 4 月初版

定價/300 元 (平裝)



ISBN 978-957-729-921-5 (平裝)

Control, Risk and Governance Case Studies

by Shumei Su and Jinfeng Chen

Copyright 2013 by Shumei Su and Jinfeng Chen

Published by BestWise Co., Ltd.

智勝網址: <http://www.bestwise.com.tw>

本書之文字、圖形、設計均係著作權所有，若有抄襲、模仿、冒用情事，依法追究。
如有缺頁、破損、裝訂錯誤，請寄回本公司調換。

為尊重著作權及符合「合理使用」原則，
若有本書 PPT 及各章授權使用需求，請與本公司版權部門洽詢。

自序

這 16 年來，筆者積極地參與內部稽核協會及公司治理協會的活動，且榮幸地能夠有機會接觸許多國內外從業人員與文獻。有感於內部控制與公司治理的專業書籍大多以教科書或研究成果的樣態呈現，但因公司治理、風險管理與內控內稽都是企業營運過程的嚴肅課題，似乎也無可厚非。因為嚴肅，有時讓人覺得沉重，就怕文字論理太生硬，讓人讀了不易消化，因此，繼上一本工具書《內部稽核新紀元》出版之後，一直想以個案分析的方式來探討內部控制、風險管理與公司治理的議題，自忖也許在真實的故事中能發現不同角度的思維。

本書在寫作進行中，國內外企業也有幾項重大事件發生，牽涉到的是內部控制、風險管理與公司治理各項問題。鑑於讀者未必了解其來龍去脈，特別寫下來，以做為企業界管理階層之參考。

本書以說故事的方式，敘述每一個案的前因後果，希冀以各種不同面向與角度來探索前述三大嚴肅議題：內部控制、風險管理與公司治理。書中個案有些依據新聞報導加以深入分析並撰寫，有些則是由企業界朋友轉述得知，相當具有參考價值。

全書分為三大篇。第一篇之「內部控制」分為三種行業別：「銀行業」共涵蓋九個個案，「其他產業」有八個個案，「政府機關」則收錄了四個個案。其中，個案如「錢在網銀內消失了」、「有發票沒機器」、「利用 FEDI 偷錢」、「業績壓力的縫隙」、「賭場的內控」、「都是親信惹的禍」等，提出問題思考或問題剖析、指出法令遵循情況，且提出解決問題方案；少數個案則引述國際內部稽核專業實務架構，並針對國際之作法稍加探討；有些個案則輔以控制流程圖，讓讀者更清楚關鍵控制點何在。此外，臺灣即將開拓博弈觀光，而美國政府對賭場內控之要求，也值得我方借鏡。

第二篇「風險」涵蓋六個個案，大多是國外個案，例如：「都是風控長的錯？」、「臉書上市」、「自我感覺良好」等，每個個案敘述前因後果或敘述整體企業事件、闡明風險何在，並探討如何降低或轉移風險。

第三篇「公司治理」涵蓋 10 個個案，例如：「薪酬委員會可以瘦肥貓嗎？」、「經營權之爭」、「股東會紀念品」、「決策品質」等，每個個案探討不同的公司治理原則。依據經濟合作暨發展組織（OECD）提出之公司治理

原則為：確保股東權益、股東公平待遇、保障利害關係人利益、揭露與透明化及強化董事會責任。而這十個個案依上述五大原則來探討問題，並提出公司治理之建議。

此際，政府正致力於強化各機關之內部控制，因此，筆者也舉四例以供政府機關參考。原先所寫為基層員工涉及之舞弊事件，然而，管理階層之採購弊端可能危及人民生命財產之安全，比起基層員工之舞弊，影響更為深遠，豈可輕忽？

控制與風險是一體的兩面，事先疏於預防控制，往往導致企業承受重大之風險；而內部控制制度之建立及執行是強化公司治理制度之基礎。治理階層若善盡善良管理人之注意義務，一定會督導機構內部控制制度之落實執行，且能有效管理機構之各種風險；反之，機構若無良善之公司治理制度，則將缺乏良好的經營方向與決策品質，其內控與風險也疏於督導，而機構終將衰頹。

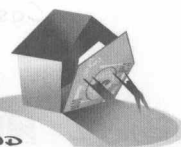
蘇淑美 陳錦烽

目錄

CONTENTS

CONTROL, RISK AND

GOVERNANCE CASE STUDIES



Part 1 內部控制

- Case 1 錢在網銀內消失了 3
- Case 2 積少成多，聚沙成塔 9
- Case 3 定期存單質借 13
- Case 4 貸超所值 19
- Case 5 金庫大盜之謎 23
- Case 6 有發票沒機器 27
- Case 7 人頭冒貸 31
- Case 8 家賊難防 35
- Case 9 利用 FDI 偷錢 41
- Case 10 隻手遮天 45
- Case 11 魔鬼藏在細節裡 51
- Case 12 業績壓力的縫隙 55
- Case 13 賭場的內控 61

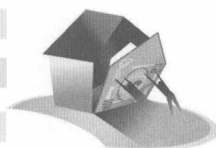
- Case 14 雅痞的採購 65
- Case 15 人資管理系統 75
- Case 16 都是親信惹的禍 83
- Case 17 疏忽的代價 87
- Case 18 虛擬薪資帳戶 89
- Case 19 故意遺失檔案嗎？ 93
- Case 20 攸關國之存續 97
- Case 21 坑殺人民血汗錢 101

Part 2 風險個案 105

- Case 22 退休金保險公司 107
- Case 23 都是風控長的錯？ 113
- Case 24 K 賣場的風險 123
- Case 25 臉書上市 133
- Case 26 守成不易 141
- Case 27 自我感覺良好 147

Part 3 公司治理個案 151

- Case 28 薪酬委員會可以瘦肥貓嗎？ 153
- Case 29 經營權之爭 159
- Case 30 當東方遇見西方 165
- Case 31 勞工的血淚 169
- Case 32 問題只在存貨嗎？ 177
- Case 33 百年老店的考驗 181
- Case 34 股東會紀念品 189
- Case 35 是副總或門神？ 195



Case 36 決策品質 199

Case 37 又見掏空 203



PART

1

內部控制

銀行業

Case 1 ~ Case 9

其他產業

Case 10 ~ Case 17

政府機關

Case 18 ~ Case 21

Case 1

錢在網銀內消失了

壹、銀行開戶

2012年，原本在臺北上班、50歲的張太太，因為經濟不景氣，又逢歐債危機，公司縮編裁員，高齡高薪的她，又碰上公司某一副總非常歧視高齡女性，因而在第一波裁員潮中遭到資遣。於是，張太太帶了一些現金來到美國西岸探視兒子。兒子平時忙著上班，晚上和假日則忙著進修學分及參加活動。在美國，銀行的營業時間雖然是週一至週五早上九點至晚上七點，以及週六的早上九點至下午兩點，但張太太的兒子一時之間還抽不出時間陪她去銀行。張太太心想，手邊帶了3萬元的旅行支票及8,000元的現鈔，放在屋子裡也不是挺安全，又曾聽兒子提起某家銀行經營績效較佳，自恃英文程度不錯的她，因此自行前往該銀行開戶。櫃檯人員聽說她要開戶，趕緊介紹服務台一位專責開戶之行員Richard協助她開戶。Richard非常熱心且殷勤，不僅幫忙填表格，還遞上一杯咖啡請她喝。張太太開了兩個帳戶，一個是儲蓄存款帳戶，另一個是支票存款帳戶。完成開戶後，張太太拿到兩張存款的收據，此時，她突然想到自己此行只能待三個月，三個月後就必須回臺灣處理一些事務，因此詢問了Richard有關網路銀行開戶的事。Richard很熱心地表示，直接在他桌上的那台電腦開戶即可，並且詳細詢問了張太太的使用者名稱、密碼及三個問題的答案，包括：1.你第一個寵物的名字；2.你最喜歡的城市名字；3.你母親的婚前姓氏。

Richard將張太太的回答一一鍵入電腦後，告訴她網路銀行已經開戶完成，她可以即刻使用網路銀行，而金融卡會在10天後寄到她所填寫的住址。

時值春夏之際，鬱金香盛開，處處美景。張太太每天和兒子共進早餐，等兒子上班後，收拾好家裡便四處逛逛，有時搭公車至市區博物館、美術館，日子過得怡然自得。因為兒子孝順，一星期總會給她一些現金，雖然銀行金融卡寄來了，卻不曾使用，也沒想到要上網看一下銀行帳戶。

過了春天，夏天更是熱鬧，街上繁花盛開，湖上白帆點點，藍天碧湖，美不勝收。一晃眼，三個月過去了。張太太回到臺灣，和兒子 Skype 完後，才想到從未上網查看過自己在美國的銀行帳戶，此時，她才將自己當初在銀行記下帳戶名稱及密碼的小筆記本拿出來，上網看一下自己的帳戶餘額。一看之下，張太太非常震驚，因為她儲蓄存款帳戶裡的餘額竟然只剩幾十元。張太太趕緊利用 Skype 打電話至當初開戶的分行要找 Richard，可是，Richard 已經離職，其他行員則只能上銀行的資料庫查她的餘額。不甘心自己的錢莫名其妙不見了，張太太再次上網查交易紀錄，結果發現，除了當初開的兩個帳戶外，自己還多了一個帳戶，而儲蓄存款帳戶的錢分四次轉進這多出來的帳戶，而且一再地從 ATM 被提領出去。張太太找來當初的存款收據，怎麼看，總共也只開了兩個帳戶，怎麼會憑空多了一個帳戶？

最後，張太太致電銀行網頁中的 1-800 電話，電話那端的工作人員也只能告訴她，她當初總共開了三個帳戶，其中兩個帳戶有金融卡，她在開戶申請書中註明一張金融卡寄到兒子的地址，另一張金融卡會親自至開戶所在分行領取，她也簽收領取了該張金融卡。

貳、問題思考

1. 網路銀行的開戶作業，如何確保客戶之存款安全？
2. 網路銀行控制的弱點為何？

參、問題剖析

一、臺灣網路銀行之開戶作業模式

在臺灣，若銀行要求開啟網路銀行，一般都是請客戶填寫網路銀行申請書及同意書，申請完畢，銀行會給客戶一份彌封的密碼，辦理網路銀行開戶的行員看不到客戶的密碼，而且客戶在開啟彌封之密碼時，封面皆會有一行紅字提醒客戶：進入網路銀行後，請立即更新密碼。較敬業的行員也會再次提醒：回家後要更改密碼。若客戶在一個月內未上網登錄並更新密碼，則該客戶之網路銀行將會被鎖碼。

二、美國網路銀行之開戶作業模式

在美國，銀行一般的開戶非常簡便，無須客戶親臨銀行櫃檯，可直接在銀行官網上開啟新帳戶。新帳戶一旦開啟成功後，不論是到 ATM 存錢或親臨櫃台存錢皆可。若為金額較大之定存或特殊期限之定存，或購買 CDS 等，銀行在客戶網路開戶後，會寄送相關同意書至客戶所留的通訊地址，請客戶臨櫃親簽，開戶才算完成。

肆、全面解決問題之方案

一、網路安全防護

在臺灣，銀行開啟網路銀行的方式是半自動化作業，因此，對於網路安全防護知識不足的客戶仍有相當的保護作用；而美國則已進入自動化的時代，要開啟網路銀行，只需至銀行網頁登錄即可。至於密碼、帳戶名稱及其他安全通關密語，最好是無人知曉，因為這是最安全的模式。而且帳戶名稱及密碼應該定時更新，才不易被網路高手盜取。

張太太在銀行辦事員 Richard 的電腦裡留下帳號名稱、密碼及安全防護的三個問答，完全沒有設防，很容易被動手腳。在這種情況下，張太太應該立即回家，在自家電腦裡更改帳戶名稱及密碼，那麼行員就算知道她所有的個人基本資料，也無法動到她任何一分錢。

二、銀行的安全控管機制

網路銀行應對行員設限，就算再怎麼自動化，也應對臨櫃客戶申請網路銀行之程序，設下安全控管機制。臺灣的銀行針對客戶申請網路銀行的程序實在值得美國的銀行效法。此外，新開戶客戶之各式金融卡及信用卡，應強制直接寄到客戶的通訊地址，而非由客戶至分行領取。

三、職能分工

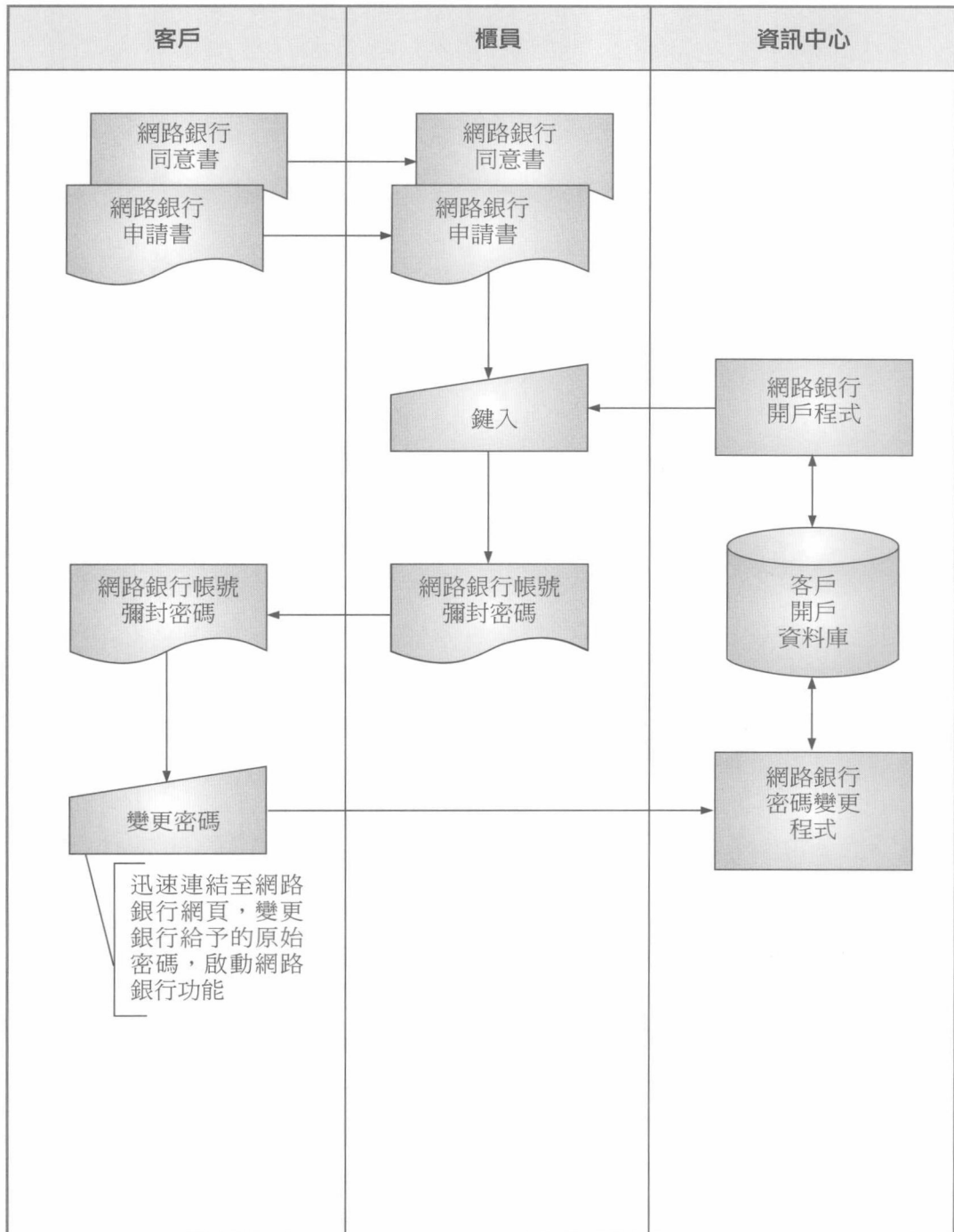
內部控制中一項非常重要的元素就是職能分工，因此，在這個案例裡面，輸入資料、授權資料、處理資料和檢查資料的職責均應加以區隔。就內部控制

的成本效益來說，職能分工可嵌入流程中加以控制，例如：開啟帳戶由開戶櫃檯處理，其他存款與提款則由一般櫃檯處理，若需開啟網路銀行帳戶，則由客戶自行上網登錄，或填寫網銀申請單，再由系統跑出一組彌封之密碼，並請客戶登錄後更改密碼，同時嚴禁行員幫客戶開啟網路銀行帳戶。

伍、資訊科技稽核之功能

國際內部稽核協會（Institute of Internal Auditors, IIA）出版之《全球科技稽核指引》（*Global Technology Audit Guide*）指出，目前許多企業之主要控制都以科技為基礎，或者設定於業務應用系統內。該書指出，資訊科技控制不是自動的。對於已使用資訊科技超過 50 年的組織而言，控制並不總是為新系統硬體或軟體的預先設定的條件。控制的開發與實施，一般都在系統中已認知的弱點和威脅之後。故以此個案而言，銀行行員具備可存取權限來操作系統，IT 稽核職能應協助確保銀行行員只能存取執行其職責的資料及功能，但不能執行功能性之交易。

陸、網路銀行申請作業流程圖



Case 2

積少成多，聚沙成塔

壹、沒人曾在意小數點後面的兩位數？

在臺灣，如果有一塊錢掉在地上，是不會有人撿的，因為一塊錢實在買不了什麼東西。但是，在美國，幾角幾分經常是交易時跟在小數點後面的魔法數字。例如：超市中的水果售價牌上標示著「2.99/Lb」（一磅 2.99 元）或「3.99/Lb」（一磅 3.99 元）。可是，他們為什麼不乾脆用整數表示，寫成「3/Lb」或「4/Lb」呢？

事實上，大家都知道，超市運用的是「行銷心理學」，售價標示「一磅 2.99 元」就是讓客戶在心理上覺得買的東西是兩塊多的價錢，而不是三塊，感覺上好像便宜多了，但實際上只差 1 美分。由此可見，美元的幾角幾分仍然可以左右買賣的行情。

話說美國大型銀行的客戶人數約達 5,000 多萬人，假如負責維修銀行內部作業程式之軟體工程師，某一天趁無人監管時，在程式中動了手腳，將每個客戶在銀行存款利息的 1 美分每個月自動轉入自己特設的帳戶中，一年所得金額為 $0.01 \times 12 (\text{月}) \times 50,000,000 = 6,000,000$ ，亦即該軟體工程師一年可得手 600 萬美元。

因為每位客戶每人每月的存款利息只被 A 走 1 美分，沒有人會在乎，而且美國存款戶不似臺灣存款戶有自己的存摺，而是定期寄送對帳單（目前已發展到客戶可自行上網查詢存款餘額，只要客戶同意，銀行可以不寄送紙本對帳單）。大多數的人拿到銀行對帳單，頂多只會稍微計算一下，因此，0.01 美元經常會被認為是正常的誤差。而這筆轉帳就在人不知鬼不覺中持續進行。

一年之後，某個敏銳且仔細的客戶拿起計算機計算自己的存款利息，才赫然發現自己的利息每個月都少 1 美分，因此跑去找銀行理論。銀行這才循線追查，最後發現所有客戶的每月存款利息都減少 1 美分，且這 1 美分均被匯入同