營業秘密之保護——兼論於生技／醫藥產業之運用

李毓華 *

壹、前言

貳、生技產業領域營業秘密之重要性

一、營業秘密遭侵害之比例

二、生技之合作模式及涉營業秘密侵害之高額賠償金

三、營業秘密隱藏之鉅額利益

四、產業實務、技術運作之必要性

參、營業秘密管理應注意之問題及原則

一、營業秘密管理應思考之問題

二、資訊保護之基本要素及原則

肆、風險管理概念運用於營業秘密議題

一、有效管理機制及風險管理概念之運用

二、風險管理概念之簡介

三、具體運用方式

四、運用於生技領域應注意之事項

五、營業秘密之稽核機制

伍、結論

* 作者現為新竹地方法院法官，取得國際專案管理師 PMP 證照（2007 年～迄今）。
本文相關論述僅為一般研究探討，不代表本局及任職單位之意見。

摘要

生技產業因其特殊性（技術複雜度高、研發成本高、研發時間長、常需跨國合作），以營業秘密保護部分核心技術乃屬常見。此外，因產業合作及人員流動快，如何避免、降低、轉化「營業秘密外洩、被盜用」及「不當使用他人營業秘密」之風險，是生技產業應重視之議題，本文認為處理營業秘密議題最有效的方式乃結合法律思維及管理架構進行預防措施，此措施更勝於事件發生後的訴訟補救。又因公司每日所產出之資訊量多，故透過具系統性、整合性、易執行、易追蹤之風險管理機制處理生技／醫藥產業之營業秘密管理，較有效益且符合管理成本，本文將試圖以風險管理架構介紹營業秘密之保密（管理）措施、稽核制度，此制度除可降低風險外，更可能藉此整合公司營業秘密及其他智慧財產權，是生技／醫藥產業強化競爭力值得投入之管理方向。

關鍵字：生技、營業秘密、合理保密措施、風險管理、稽核制度
Biotechnology、trade secrets、reasonable measures to maintain secrecy、risk management、audit system

壹、前言

2018 年 Genentech 控訴前員工在職期間洩漏該公司重要的暢銷生物相似藥之配方給我國之喜康生技（JHL Biotech），在該案中，遭竊取之機密文件是透過員工將公司機密資訊（如研發技術報告、穩定性報告、驗證報告等）下載至公司配發之筆電、提供諮詢等方式外洩給喜康生技[1]，該案後來以和解收場[2]；2019 年則有 Eli Lilly 與 Adocia 二家分屬美國及法國之生技公司間有關營業秘密侵害之仲裁案[3]。此外，國內葡萄王生技員工洩漏秘密配方案件[4]及臺灣臺中地方法院 107 年智訴字第 16 號刑事判決（生技公司員工離職後，未經公司授權重製供應商合約、產品成本攤提表等資料）等。由上開國內外事件可見，營業秘密外洩案件在生技／醫藥領域中有增長之趨勢，且外洩事件對於公司之損害甚大，故如何運用有效率之管理措施，保護具有核心競爭力之營業秘密是生技公司需要關注之重要議題。

貳、生技產業領域營業秘密之重要性

營業秘密之於生技產業之重要性，可由幾方面說明之：

一、營業秘密遭侵害之比例

營業秘密侵害之威脅不僅來自於國內之競爭者，亦有來自於國外市場情報蒐集之研究機構、私人企業、學術或研究機構及個人，此乃因生技／醫藥領域有技術複雜度高、研發成本高、研發時間長、常需跨國合作等特質，部分公司欲以不法獲取他人營業秘密之方式以減少研發成本及縮短研發時程之故。美國研究者曾在 2007 至 2009 年間，對 24 個產業技術領域、超過 5,000 家業者進行問卷調查，高達 98% 受訪企業表示在中國大陸曾經歷過營業秘密侵害情事，其中 30.9% 乃化

---

1 Genentech, Inc. v. JHL Biotech, Inc., (No. C 18-06582 WHA).

2 李林瓊，喜康被控竊密與 Genentech 和解，環球生技月刊，https://www.gbimonthly.com/2019/09/52735/（最後瀏覽日：2020/1/26）。

3 Xavier Grange, *Eli Lilly Wins US Trade Secret Arbitration*, ICLG.com, https://iclg.com/news/10057-eli-lilly-wins-us-trade-secret-arbitration（last visited Feb. 12, 2020）

4 蔡依珍，前後任員工洩漏秘密配方葡萄王損失數億，中時電子報，https://www.chinatimes.com/realtimenews/20170420002599-260405?chdtv（最後瀏覽日：2020/1/16）。

學製造業，尤以醫藥及藥品製造業為主[5]。另外，由於近年來與生技／醫藥有關之營業秘密訴訟案件有增加趨勢[6]，均顯示營業秘密保護議題於生技、醫藥領域需特別重視。

二、生技之合作模式及涉營業秘密侵害之高額賠償金

隨著生技和醫藥領域之緊密技術合作，合資、合作、外包在此領域十分常見，而員工工作流動亦屬頻繁，在這種廠商互動及人員高度流動之下，因此生技、醫藥公司涉及營業秘密侵害之可能性便增加。

此外，營業秘密侵害事件之賠償金額有越來越高之趨勢，生技、醫藥公司除需知道如何保護自我的營業秘密外，還必須了解涉及營業秘密侵害索賠事件應如何攻防[7]，故生技公司對於營業秘密之管理是不可忽視的環節。

三、營業秘密隱藏之鉅額利益

2009 年著名藥廠輝瑞（Pfizer）以 680 億美元併購另一知名藥廠惠氏（Wyeth），輝瑞除了想彌補核心暢銷產品因專利即將到期而造成的營收損失，與搶占市場版圖等主因外，另一項因素與惠氏藥廠當時擁有之一項北美市占率最高的更年期婦女荷爾蒙治療藥物（Premarin）有關。惠氏藥廠從懷孕母馬尿液提煉製造出藥物的關鍵雌激素從未申請專利，全都透過營業秘密形式保護，這項營業秘密也是輝瑞要併購惠氏主要原因之一[8]。此外，如前所述，2019 年 Eli Lilly 與 Adocia 二家之生技公司間有關營業秘密侵害之仲裁案金額高達 13.9 億美元。由以上事件均可見，與生技、醫藥產業相關之營業秘密背後隱藏鉅額之利益。

---

[5] US ITC, *China: Effects of Intellectual Property Infringement And Indigenous Innovation Policies on The U.S. Economy*, Investigation No. 332-519, at 3-16, 3-43, http://www.usitc.gov/publications/332/pub4226.pdf (last visited Jan. 13, 2020).

[6] Tara Nealey, Ronald M. Daignault, Yu Cai, *Trade Secrect in Life Science And Pharmaceutical Companies*, Cold Spring Harbor Perspectives in Medicine, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4382727/ (last visited Feb. 12, 2020).

[7] Nealey, Tara et al., *Trade Secrets in Life Science And Pharmaceutical Companies*, vol. 5, 4 a020982. 20 Cold Spring Harbor Perspectives in Medicine, (2014).

[8] 吳毅勛，商業秘密保護在企業發展中可以創造哪些價值？，每日頭條，https://kknews.cc/finance/pv8938e.html（最後瀏覽日：2020/1/18）。

四、產業實務、技術運作之必要性

在生技、醫藥產業中，部分資訊雖不符合可專利之要件，但因具有重要地位，故可透過營業秘密保護之。舉例而言，培養細菌過程中特定營養素之數量或順序變動可能會顯著改善、影響細胞之成長，增加蛋白質產品之產量，但數量或順序的變動、調整可能會被認為是「顯而易見」的，因此不符合申請專利之要件[9]，尤其有關分離流程（separation processes）、純化流程（purification processes）及培養組織之技術（culturing techniques to grow organisms）等，藉由營業秘密之方式保護通常是首選[10]。再者，有研究發現許多國際大型生物醫藥企業逐漸採用「專利－營業秘密」交叉保護方式保護研發成果[11]。

參、營業秘密管理應注意之問題及原則

一、營業秘密管理應思考之問題

進行營業秘密管理應思考之問題有：其一，海量資訊之有效分類及管理：公司隨時有新的資訊產生，如：研發型公司，實驗數據時刻產出，數量之大，如何妥善分類（機密與非機密或第一等級、第二等級……以此類推），並給予相應之管理非常重要。其次，資訊藏身各部門，若各部門對於營業秘密之處理、判斷標準不一，易生防護上之漏洞。其三，因資訊量多，應擇定並區分需要保密及不需保密者，切勿將所有資訊均納入營業秘密管理範疇，因過度保密管理及全面保密等同於沒有管理，且也不合管理成本及效益。其四，營業秘密通常區分為技術性及非技術性二種，前者通常包含與研發、製造、方法相關者，至於非技術類型乃

---

9 Howard G. Zaharoff, Morse, Barnes-Brown & Pendleton, PC, Waltham, PROTECTING PROPRIETARY INFORMATION, Advising a Massachusetts Business(Chapter 2) 2-10, Massachusetts Continuing Legal Education, Inc.(2011).

10 Rochelle C. Dreyfuss, Katherine J. Strandburg, The Law and Theory of Trade Secrecy 250 (2011), See also Robert W. Payne, *The Emergence of Trade Secret Protection in Biotechnology,* 6 Nat. Biotechnol 130 (1988).

11 朱鏡義、曲凱、范東升、馬秋娟，談生物醫藥領域技術秘密與專利保護模式的選擇，中國醫藥生物技術 9 卷 3 期，頁 239 ，2014 年 6 月。

指與商業活動及公司客戶相關者，有時這二種類型會有重疊的情況，但此分類並不影響所給予之保護措施等級[12]。保護措施等級仍應以該客體之屬性、價值而定。

二、資訊保護之基本要素及原則

以下逐一介紹有關資訊保護之基本要素及原則，因生技、醫藥產業與一般產業資訊保護有相通處，故以下部分注意要點可通用，然本文會於生技／醫藥產業可特別注意之處簡略提出參考意見。

有美國學者主張有效率之資訊保護之基本要素有六點：「1、 Limit access to information to only those who need it（最少接觸原則）2、Place legends on documents and files（標示管理） 3、Implement an information tracking system（實施訊息追蹤管理）4、Dispose of information properly（資訊處理之管理）5、Regulate information that must leave the company（攜出資訊之管理）6、Encourage reporting of violations and investigate and punish violators（鼓勵舉報違法、調查及處罰）」[13]，僅簡要說明該六點原則並提出由實務觀察值得注意之點[14]：

（一）最少接觸原則（有限度接觸原則）

接觸機密之人數與機密被洩漏、盜取之機率成正比，故應視員工工作內容及權限之需要給予相應之資訊接觸範圍，並應適時依員工工作狀態、職位、職務內容之變動，調整員工得接觸資訊之範圍、內容及權限，即員工更換新工作內容時，得接觸到舊工作範圍之權限亦應隨之取消，其具體實踐方式可透過讓員工簽署容許使用方針（Acceptable Use Policy），即依員工工作內容及職務給予相應的電腦系統使用權限[15]。

---

[12] Magdalena Kolasa, Trade Secrect and Employee Mobility 75(2018).

[13] Darin W. Snyder & David S. Almeling, Trade Secret Law and Corporate Strategy 71 (2018).

[14] *Id*.at 69-81.（說明：部分要點及內容歸納自前揭書籍，詳見各要點內說明及引註，另有部分係作者參考相關要點並藉由實務觀察所提出。）

[15] *Id*.at 71.

（二）標示管理

在相關之機密文件及電子檔上依機密等級給予相應之標示，標示之目的有三：「1、對接觸者提出警示、警告。2、舉證之用：此項標示也可用於訴訟中，舉證證明文件確屬機密文件。3、可藉此循線找出不法盜取之源頭。」[16]

標示之方式應視公司規模大小而有差異，規模小的公司可分為非機密類型（No restriction）及機密類型（Confidential）二種，前者乃指公司不介意對外揭露之資訊，而判斷是否需予以機密處置可藉由網路測試法（Website Test），亦即若資訊適於揭露於網路上者，則無須機密對待；反之，則應歸為機密資訊[17]。至於規模較大之公司可視公司需求及狀況訂出分類標準，但本文認為基於管理成本考量，分類切勿過多。

（三）實施訊息追蹤管理

所謂追蹤管理乃是記錄曾接觸過欲保護資訊之人、時間及作為，其目的在於：「其一，調查用途：可依循相關之紀錄追查盜用及洩漏之過程及人。其二，舉證之用：在盜取及洩漏營業秘密事件中，紀錄可供作證據使用。實際之建置方式可透過軟體系統為之，如：在影印機上設置稽核裝置以便判別使用者複印之內容。」[18]

（四）資訊處理之管理

啟動定期強制刪除機制，亦即除非基於某些特定目的（如訴訟使用、法令要求、政府稽查之必要等）需保存者，若資料或文件無留存之必要性，應定期刪除之，刪除客體包括電子郵件[19]。此外，刪除、銷毀及處理文件應謹慎，應視資訊所儲存之方式給予妥適之處理方式。

---

[16] *Id*.at 72.
[17] *Id*.at 72-73.
[18] *Id*.at 74.
[19] *Id*.at 76.

（五）攜出資訊之管理

避免機密資訊之攜出，若有需要攜出亦應在公司知悉且已進行充分保護下（如簽署保密協議）為之。常見因疏忽而將機密資訊攜出之情況有：「1、在技術展場、演說場合中，隨著宣傳文件、演說內容（稿）或其他相關資料而不慎流出。2、不慎上傳公司或其他網站。3、員工不慎在公眾場合流出，例如在電梯、餐廳、飛機、搭車等，因員工間交談或在電話交談中流出。4、因使用公共無線網路而不慎流出：員工使用公共無線網路接觸公司機密資訊容易被駭客入侵、監控，產生外洩之風險，因此應透過公司政策或者教育訓練，鼓勵或強制員工於公司外部工作使用私人網路，若必須使用公共無線網路，亦應注意可能外洩之風險，避免透過公共無線網路接觸公司機密資訊[20]。」

（六）鼓勵舉報違法、調查及處罰

讓有權處理者及早知悉並察覺違反資訊安全之事件是避免及降低風險之最佳方法，故可透過鼓勵員工向主管、人資或法務部門進行舉報。另外，一旦知悉違規事件，便應立即啟動內部調查及處罰流程，並依違反情節重大與否採取相應之處罰機制，可產生嚇阻效果，並藉由該次個案建立補強漏洞、再次強化員工之教育訓練及保護機密之公司文化[21]。

（七）差異處理原則及定期更新檢視

不同規模公司、產業之資訊保護措施並不相同，應予以差異化處理，此差異取決於：公司規模大小、組織複雜度、競爭環境（含競爭對手、面臨之已知威脅、產業成熟度等）、公司之產業別（如：生技產業、傳統產業、文化產業、資訊科技產業、食品產業）、產業成熟度（成熟、中度發展、新興產業）、欲保護之資訊態樣及形式（如紙本、電子、實驗數據）、資訊內容之價值高低、預期保密期間之長短等因素，依此差異做出符合成本考量之保護措施。

---

[20] *Id*.at 76 -77.
[21] *Id*.at 77 -78.

此外，最基本用作保護密度區別的標準是「資訊價值之高低」，亦即資訊價值高時採取之高密度保護；反之，則採較低保護密度，此乃基於管理成本考量。最後，隨著機密資訊之保護期間進展，公司應定期追蹤、評估保密措施之妥適性、成效性，並視情況做出修正及調整。

而在生技、醫藥產業領域中，不同公司類型亦應有不同的保護措施。依經濟部對生技產業市場分為：藥品、醫療、農業生技、再生醫學、數位醫療[22]，以及智慧醫療等市場，因應不同產業類型之市場所需要保護之核心營業秘密客體亦有所不同。舉例而言，在數位醫療及智慧醫療市場領域，因該領域乃是資訊科技在醫療及健康領域之應用，藉由網際網路及相關技術，以提供或強化健康服務與資訊[23]，因其重點在於資訊科技於醫療領域之應用，因此，相關資訊保護之重點、核心還是圍繞著資訊科技相關技術，至於藥品市場及醫療市場中，相關試驗之數據及試驗方式對於生技、醫藥公司之重要性較高，針對該等資訊自需強化保護。

（八）對於電子資訊之保護措施

隨著科技之進步，資訊、數位方式儲存機密資訊成為未來趨勢，因此，許多營業秘密之洩密事件常因筆電遺失、竊取筆電（或硬碟）、不當下載筆電或其他載體（如 USB 等）、在網站上傳、透過電子郵件等方式為之，如本文一開始所提及之案例，故此部分之保護措施有越顯重要的趨勢。

一般而言，公司保護資訊之方式可藉由最平常的密碼控管至複雜的入侵偵測系統（heuristic intrusion detection）、生物辨識（biometrics）、深度內容檢測（deep content inspection）等[24]。針對不同的資訊設備可提供之資訊防護措施分別簡述如下：「1、網路：可藉由防火牆、使用 user IDs、監控點、網路攻擊即時警示系統、防毒軟體等措施。2、檔案文件：藉由實

[22] 2019 生技產業白皮書，經濟部工業局，第 9 頁，https://www.biopharm.org.tw/images/2019/Biotechnology-Industry-in-Taiwan-2019.pdf（最後瀏覽日：2020/1/25）。
[23] 魏于翔，全球智慧醫療發展趨勢，農業生技產業季刊 56 期，頁 1 ，2018 年。
[24] Darin W. Snyder & David S. Almeling, *supra* note 13, at 78.

踐最低程度接觸原則，以避免某些危害行為（如複製、修改、刪除或電子郵寄）。另外，如密碼保護、文件管理系統等。3、資料備份：定期自動備份資料可避免駭客挾持資料向公司勒索高額款項。4、設備安全防護：此乃針對筆電、PDAs 及其他員工所使用之載體進行之管制。對具有機密性之資訊應拒絕讓其得以儲存在任何可以攜離公司之載體中。5、物聯網（Internet of Things，IoT）：隨著物聯網技術成熟以及運用快速成長，個人、商業甚至政府資訊在網路上串流量大，因此資訊安全保護也越來越重要。而防護之方法可透過定期更新密碼、加密等措施。6、電子郵件之監控：電子郵件最主要用於商業往來，且亦為盜用營業秘密之常見方式之一，絕大多數的公司對於電子郵件也有一定程度之加密措施。」[25]

（九）對他人所有之營業秘密管理保護措施

公司需謹慎處理及妥善保管他人（如：合作廠商、客戶）的機密資訊，否則可能會違反與他人契約內容、協議，而正確之態度便是將之視同自己公司之機密處理。有合作關係的雙方可藉由建立營業秘密清冊之方式進行管理，此一清冊建立主要功能在於讓合作雙方必要相關人知悉，並要求保密與擬定相對應之侵權懲罰[26]。

再者，營業秘密管理除了防止自身營業秘密遭外洩或盜用外，蒐集他人資訊之合法性也是營業秘密管理之範疇，因若員工不法獲取之他人營業秘密亦會使得公司陷入侵害他人權利之風險中。申言之，公司必須教育員工避免不法、不當取得競爭公司及合作夥伴之機密資訊，蒐集相關資訊應透過正當管道（如網路上或其他已公開發表之文件、期刊等）。

（十）定期、適時調整管理措施

公司之保護措施並非一成不變，隨著公司規模變化、公司所在產業結構變化（如從新興邁向中度成熟，或中度成熟進入高度成熟）、資訊

[25] *Id*. at 78-81.

[26] 徐嘉謙，智慧財產權與營業秘密之發展，營業秘密管理體制之創建，獨享數位文化股份有限公司，頁 25 ，2018 年 5 月。

技術發展、新競爭對手出現及新產出之重要機密量及內容，公司應與時俱進的調整並做出相應之保護措施。

肆、風險管理概念運用於營業秘密議題

公司營業秘密之管理必須透過跨部門整合管理之方式進行，法律、研發、業務、財務、人資、資訊等各部門均有屬於各自之重要機密資訊需進行管理，而營業秘密管理之重要性除了預防之外，另具有妥善之營業秘密管理流程可於訴訟中當作公司已實施「合理保密措施」之有力證據。本文認為，良好的營業秘密管理制度低標應達到法律要求的保護措施要求，若透過管理制度可進一步達到整合公司內部營業秘密及其他智慧財產權，藉此強化公司之競爭力，乃是管理制度所欲達到之高標效應。

另有學者主張企業機密保護最大之效果應該由法律面切入，至於營業秘密之切入則以結合完善的管理體系方法論以及企業核心業務流程，所產出之管理效果方能最大化[27]。此外，研發型企業核心技術點通常都集中在一、二個部門，因此得以識別出這些核心營業秘密並加以妥適之管理方案方屬於具有效率之管理制度[28]。

如前所述，在生技領域中，不同市場屬性之公司其核心技術亦不同，各不同類型之公司應視其公司屬性找出核心技術（即重點保護客體）及部門（重點部門）並給予妥善管理措施。舉例而言，對 CRO[29] 代理試驗類型之生技公司而言，與試驗技術相關之資訊，以及受託試驗之研究相關數據均屬於核心之機密事項。至於在數位醫療、智慧醫療市場其重點乃在於將資訊科技運用於醫療用途，故應注意與相關核心資訊技術有關之資訊保護，該相關資訊部門便是應予重點管理之部門。另外，藥品、醫療及再生醫學市場則側重於相關試驗數據及試驗方式之保護，因此，有關試驗部門則是應強化管理之部門。

---

27 吳毅勛，營業秘密管理框架總論，營業秘密管理體制之創建，獨享數位文化股份有限公司，頁 78 ，2018 年 5 月。

28 同前註，頁 83。

29 CRO（Contract Research Organization，委託研究機構），也有稱之為（Clinical Research Organization，臨床研究機構），即接受藥廠或生技公司委託進行研究服務之機構。

本文認為在處理營業秘密之議題中，可將「營業秘密洩漏之可能性及危害」及「不當侵害他人營業秘密」當成公司之「風險」，並透過風險管理之架構達到降低風險產生之機率及對公司產生之危害，以下將分別介紹有關風險管理之概念，並進一步將之具體運用於營業秘密之管理。

一、有效管理機制及風險管理概念之運用

有效的管理機制須符合統一性、系統化、易執行、易追蹤，及符合管理成本等要求，而適當之管理架構必須能整合上開基本原則並考量企業類型差異，做出符合個別公司及企業之營業秘密管理架構。本文認為，風險管理架構是一套具清楚可操作步驟（辨識、分析、應對、監控）、整合性、易執行及追蹤，且符合成本之管理模式，而此套機制已成功運用於處理許多新興科技及法律議題中，如金融法令遵循風險管理及監控[30]，及食品安全管理[31]等領域，因此非常適合藉其優點處理資料量繁雜之營業秘密管理議題。

二、風險管理概念之簡介

專案管理中所謂「風險管理」乃包括風險規劃、風險識別、風險分析、風險應對及風險監控等步驟，透過以上步驟對要處理之顯在及潛在風險進行妥適之管理措施。而各該步驟之主要內涵說明如下：（一）在風險規劃階段乃本於事業環境、組織，擬定適合、可實施之風險管理計畫。（二）風險識別乃在於將可能產生風險之因子找出並記錄之。在風險識別階段，經常使用之蒐集資訊方式有德爾菲技術（是一種結構化的決策支持技術，它的目的是在訊息收集過程中，通過多位專家獨立地反覆主觀判斷，獲得相對客觀的訊息、意見和見解）、訪談、根本原因識別、SWOT 分析法等方式[32]。（三）風險分析包括定性風險分析及定量風

---

[30] 孫欣、章友馨，金融機構法令遵循風險評估與法規資料庫，KPMG，https://home.kpmg/tw/zh/home/insights/2018/01/law-compliance-risk-assessment-and-regulations-database.html（最後瀏覽日：2020/1/13）。

[31] 口述／資料提供：姜至剛，採訪／撰稿：鍾旻園，食品安全風險分析與重要性，台大醫院健康電子報 109 期，2016 年 12 月，https://epaper.ntuh.gov.tw/health/201612/PDF/%E9%A3%9F%E5%93%81%E5%AE%89%E5%85%A8%E9%A2%A8%E9%9A%AA%E5%88%86%E6%9E%90%E8%88%87%E9%87%8D%E8%A6%81%E6%80%A7.pdf（最後瀏覽日：2020/1/18）。

[32] 項目管理協會著，盧有杰、王勇譯，項目管理知識體系指南，頁 206，電子工業出版社，2007 年 1 月第 10 刷。

險分析二方面，主要乃針對各風險產生之機率及可能產生之影響進行評估，並將各風險因子進行排序。（四）風險應對規劃，亦即針對已識別出之風險進行降低或避免風險產生之應對策略，亦即依各該營業秘密之屬性（如價值高低、所屬部門之差異性等）給予相應之管理措施。（五）風險監控乃追蹤、監測已識別之風險、殘餘風險，並繼續識別新風險，續而進行應對措施。以上步驟均需持續更新、調整，並予以逐步完善之。

圖 1　風險管理流程圖

三、具體運用方式

有學者提出營業秘密之風險管理是從營業秘密侵害防護之角度，透過風險辨識、風險分析、風險評估與風險處理等程序，降低營業秘密遭竊取、外洩可能對公司產生之危害[33]。

本文認為處理營業秘密首要之事項便是識別出「營業秘密」。其次，就所識別出之營業秘密進行分類及評估該項秘密是否有妥善之防護措施。最後，提出報告將建議修正之管理措施具體說明之。其中風險識別、分析、評估等階段透過稽核方式十分有效，此部分具體內容詳本文後述。

本文認為可將風險管理之概念用以下具體之步驟實踐之：（一）擇定管理及稽核團隊：有關管理及相關稽核組成人員可視公司規模之大小做相應之規劃，並

[33] 賴弘捷，營業秘密管理與風險分析，營業秘密管理體制之創建，獨享數位文化股份有限公司，頁 117-178，2018 年 5 月。

納入各部門之人員，並擇定稽核程序之最高負責、協調者。（二）風險管理規劃階段：此階段主要之功能在稽核團隊訂出主要之管理、稽核之原則、方針。（三）風險識別：本文認為此一階段主要目的在於識別出公司之營業秘密，其中首要目標更在於識別出核心營業秘密。（四）風險分析：包括定性及定量分析，此階段應將所識別出之營業秘密依其價值高低進行等級排序。（五）風險應對：可能產生之應對方式分為降低風險、避免風險、轉移風險及接受風險等四種。此外，透過稽核程序並將各風險應處置之方式列出。（六）風險監控：對於識別出之風險或潛在風險進行監控。

四、運用於生技領域應注意之事項

在生技產業中運用風險管理架構應注意以下幾點：

（一）組成人員

稽核人員之組成必須有研發、資訊及法務等人員，因生技領域技術複雜度高，專業分工十分細緻，對於系爭技術領域該項資訊之重要程度唯有了解該項技術之人員參與方能識別出其重要性，因此納入不同技術背景之研究人員、主管有其必要性。申言之，在進行生技、醫藥研究過程，實驗設計與指導、實驗室管理、整合實驗及驗證、實驗操作等所需的背景學科知識並不相同，有需要基礎學科為重者（如：微生物學、生物化學、食品科學、醫藥學等），亦有需要工程背景者（如：機械工程、生醫工程等），故稽核組成人員需納入上開不同背景者，至於法務人員可提供法律諮詢。此外，對於各稽核環節及過程中，公司之措施、政策及與員工之協議是否有效防堵公司員工外洩及不當使用他人之營業秘密，此部分亦需透過法務人員之法律專業檢視並提出修正建議。最後，如前所述，因科技進步，許多保護措施需要透過科技、資訊方式進行，故資訊人員也是稽核團隊之組成不可或缺者。

（二）風險識別及風險分析階段具有特別重要性

生技產業特別重視測試、試驗及研發，這一連串環節（測試過程、方法、結果）所產出之相關實驗數據、資料，都可能會是營業秘密保護

之核心標的，故對於上開相關資訊之識別及分析尤其應更細緻、謹慎及有效率。

此外，營業秘密通常區分為「技術性」及「非技術性」二種，有時這二種類型會有重疊的情況，但此分類並不影響所給予之保護措施等級高低[34]。尤其在生技、醫藥領域，研發合作機會甚高，公司之研發資訊同時也可能是合作公司（客戶）之資訊，故於識別及分析營業秘密之階段應予以特別注意。

最後，不同型態之生技公司，所追求技術領域內容亦有不同，對新藥開發類型的生技、醫藥公司而言，越是研發型的公司越是投入很高的資金與資源以追求關鍵技術之自主性；至於 CRO 代理試驗類型之生技公司而言，越高技術自主程度能提供更多的代理試驗服務[35]。因此，二種不同類型公司所要辨識出之核心技術亦不相同。此外，CRO 因為是接受藥廠或生技公司委託進行研究服務的機構，提供新藥開發時所需的非臨床與臨床試驗、數據分析等專業服務。因此，如前所述，對於試驗過程中客戶所交付之研究內容、數據等之資訊保護其等級應納入最高等級之保護範圍。

（三）風險應對策略

在生技、醫藥領域核心配方、實驗方法、製程相較於其他產業領域更顯重要，該等資訊屬核心技術，應予以最高等級之機密保護措施。至於其他部門（如財務、業務、行政等）亦應視各自部門屬性情況訂定不同層級機密分類標準。

（四）參與稽核之人員也須簽署保密協議

蓋進行公司內部之營業秘密盤點時，會因此知悉非其業務範圍之公司機密，而稽核報告更是公司內部營業秘密之整合內容，此份稽核報告

---

[34] Magdalena Kolasa, *supra* note 12.

[35] 劉昱岑，臺灣生物科技公司創新行為之研究，政治大學科技管理研究所碩士論文，頁 165，2004 年。

當然屬於公司內部之最高機密，故參與之人員均必須簽署保密協議。而與稽核相關之內容當然也必須列入最高機密對待之。

五、營業秘密之稽核機制

（一）營業秘密稽核之定義及功能

如前所述，營業秘密管理可透過風險管理之機制加以具體落實，而落實此種機制之方式可透過營業秘密稽核制度，亦即透過擇定一定之組成成員、施以系統化之管理措施，進行系統性、常規性、定期性之稽核程序，降低營業秘密洩漏及被盜用之風險，這便是實施營業秘密稽核制度之目的。

為了避免處於被動之狀態，公司最好的策略是採取主動、預防及事先把關的態度，學者認為最優先的程序就是先篩選出公司具有競爭優勢之的機密訊息、資訊，並評估是否已對該訊息做好充足的保密措施，並稱此種調查為「營業秘密稽核」（trade secret audit）[36]。至於應採取何種密度的審核，本文認為應依公司之規模、屬性（如研發型、受託試驗型等），並考量稽核成本做出最符合各該公司的稽核策略。此外，儘管進行營業秘密審核不代表可以防堵所有可能產生之風險，但可預期會有大幅度降低、轉化風險的功能，因此，公司進行營業秘密審核具有高度必要性。

（二）稽核機制之優缺點

採取營業秘密審核措施之優點有：「1、藉此發掘隱藏於公司內部被忽略具價值之概念（未被察覺、未被評估或未被使用之概念），並促使那些想法有更好的用途及使用在新產品或服務。2、可即時發現安全上的漏洞並適時做出防護措施。3、提升員工對於營業秘密保護之警覺意識，藉此減少因疏忽而洩漏營業秘密之風險產生（經統計超過 80% 之營業秘密洩漏是源自於無知或粗心所造成）。4、可用於訴訟中，證明已採行「合

[36] Darin W. Snyder & David S. Almeling, *supra* note 13, at 145.

理保密措施」之有力證據。5、可藉此向公司的股東及其他利害關係人證明對於資產確實進行妥善的管理措施。」[37]

除了以上優點外，本文認為藉由公司內部稽核制度可同時檢視公司與員工針對相關禁止不法使用他人營業秘密之協議是否周全，如：是否在員工開始受僱之職前訓練、教育訓練、公司政策、僱傭契約及相關與員工之協議等中，有明確規定禁止員工不法、不當使用他人營業秘密之規範，並得用於訴訟中作為抗辯事由。一般而言，營業秘密侵害案件訴訟中，有三個主要之攻防主軸：「1、獨立開發。2、該資訊是公眾知識。3、原告未採取合理保密措施。」[38] 詳言之，在訴訟中可藉由公司內部健全之文件、檔案充分舉證公司確實在未不法使用他人營業秘密之情況下獨立發展相關技術、產品，甚至可能證明在他人營業秘密尚未產生之前公司便已經使用系爭之技術、資訊。

至於缺點部分則有：「1、花費時間與金錢，且有可能會干擾公司正常業務之運作。2、可能會因發現以往未察覺的營業秘密損失，而依公司之狀況及會計義務，這些損失情況有可能必須要予以揭露。3、可能顯露公司以往並未採取合理保密措施之缺失，但也因此有進行修補措施之機會。4、稽核進行的不完全，也可能在訴訟中被對手利用。」[39]

（三）審核的組織（團隊）組成及成員

審核團隊的組成、人數及編制應該視公司規模之大小而定，公司規模數十人或未達百人的小型公司或許可以推由一個人進行，然若大型公司、跨國公司等規模較大型者，可能需要一組團隊進行。

至於組成人員部分，具有法律背景的人員、律師應該是必要的成員。此外，資訊部門人員之任務乃在調查過程中可協助分析解讀有關電腦資訊管理系統、伺服器及防火牆等相關資訊運用之相關問題；另外，因為

[37] *Id*. at 146.
[38] Nealey, Tara et al., *supra* note 7.
[39] Darin W. Snyder & David S. Almeling, *supra* note 13, at 146.

許多營業秘密都是透過數位方式進行儲存，而被盜用之方式通常也是藉由數位方式為之，因此，需要透過資訊人員協助擬訂相關防護措施[40]。

再者，既然營業秘密可能遍布每個部門，故每個部門至少應指派一個高階主管參與組成，便於進行更全面及深入之稽核。最後，基於讓此一審核團隊之運作更順暢，公司必須賦予此一稽核團隊充分的權限，讓相關成員於進行審核之工作過程中可以得到公司其他部門及員工之配合[41]。另外，不同公司組織管理架構擇定之部門協調者亦不相同，在屬於分層組織管理架構之公司類型，因各部門的高階主管應知悉或知悉可以協助審核團隊找出機密資訊的人員，該高階主管適合擔任居間協調者；至於屬於扁平化組織類型的公司，則可由產品經理、團隊負責人擔任協調者[42]。

（四）稽核程序之步驟

1、確認屬性（是否屬於營業秘密）、位置（存在公司哪個單位掌管中）、價值及是否已經採取相應的保護措施

盤點營業秘密之工程浩大，因營業秘密的態樣眾多，其分別存在於每個部門，各部門所屬之秘密類型相異，舉例而言，財務部門所掌管的機密資訊多屬與成本、費用及與財物相關者；人資部門則掌管組織結構、薪資、獎金等；銷售部門則有顧客名單、顧客偏好、經銷商、配送等相關訊息；行銷部門則擁有定價、產品發布、廣告行銷計畫等資訊；工程、創意、研發部門擁有程式、配方、原始碼、實驗數據及結果等資訊；製造部門擁有製程、組件、成分、生產計畫、供應商等資訊[43]。

有效率的稽核程序必須兼具「問對人」及「問對問題」二個面向，而進行稽核時問題（問卷）首要需釐清的核心問題有二：公司內部最重要的營業秘密內容為何？哪些營業秘密會為公司帶來競爭優勢？

---

40 *Id*. at 147.
41 *Id*. at 148.
42 *Id*. at 148.
43 *Id*. at 148.

至於，實際進行之步驟有三：清查、價值性判斷及彙整所有經辨識之營業秘密是否有採行保護措施，及該保護措施內容為何。針對第一階段（清查、盤點）應注意之事項為：「（1）盡可能辨識出屬於各該部門之營業秘密：當受訪者無法正確釐清或產生混亂時，可藉由適度提示可能屬於該部門之營業秘密範圍，讓受訪者可以循線回答；（2）儲存位置、接觸權限之釐清：一旦識別出營業秘密時，應立即記錄所儲存之地點、位置及方式（如公司檔案夾、電子郵件、特定電腦等），接著，應識別出有權限接觸該營業秘密之人員，如具有開啟營業秘密文件、檔案之人員有哪些？各該人員之權限範圍？以及是否有任何控管及追蹤使用狀態之措施？」[44]

有關第二階段（價值性判斷）部分可思考以下因素有：「（1）公司為該營業秘密已經投入之成本及資金？（2）該營業秘密對公司之貢獻（所產生之利潤、收入）？（3）該營業秘密之揭露將對公司產生之損失？（4）競爭對手願意為取得該營業秘密之權利支付之金額？」[45]

最後，第三階段（彙整所辨識之營業秘密是否有採行保護措施及該措施內容為何），此階段可藉由下列問題內容釐清之：「（1）公司對該營業秘密目前採取之保護措施為何？例如：該營業秘密是否只允許有權限及工作上必須之人員接觸、該機密訊息可否藉由遠端操控、是否有透過警報、相機、防護鎖等相似之設備管制接觸該營業秘密、針對該營業秘密是否已有任何禁止洩漏之保密條款、現有網路設備是否有對該營業秘密進行防護措施、對該營業秘密是否有限制複製、修改、刪改等使用上之限制措施、對於曾經接觸或使用該營業秘密之人有無追蹤及紀錄之措施、該營業秘密文件上是否有標註機密之警示字樣等。（2）除了目前之保護措施外，是否有其他措施可以保護該項營業秘密。（3）該營業秘密是否有已知之威脅可能存在？如

[44] *Id*. at 149.
[45] *Id*. at 149.

有部門之人員要離開公司至競爭對手公司工作、該訊息是否曾經被不該持有機密之人員向外公開過等。」[46]

此外，在美國，依2016年5月11日通過的營業秘密防護法案（The Defend Trade Secrets Act 2016，簡稱DTSA法案），其中包含「吹哨者免責條款」，該免責條款主要是鼓勵員工向主管機關秘密舉報公司有不當使用營業秘密之行為，舉報人會受到相當之保障，而為了使「吹哨者免責條款」具有實際運用可能性，DTSA法案要求雇主必須於合約中清楚註明「吹哨者免責條款」、並提醒員工有此條款之存在，否則，雇主對不法洩密員工主張侵害營業秘密之損害賠償時，不得請求懲罰性損害賠償及律師費用[47]。在稽核過程同時必須要確認公司相關政策、文件及與員工間之協議中是否包含「吹哨者免責條款」及其他政府主管機關要求之事項。

綜上所述，一個具有效率、精確之稽核需在問對人、問對問題、使用對的方法（用問卷、問出正確的問題）等之下，方才可以盤點出全部屬於公司有價值之營業秘密。

2、審核報告、後續改善及定期檢討程序

審核完成後應製作書面審核報告，其內容應包括以下調查內容：（1）所盤點出之營業秘密內容、各該營業秘密之價值，並依其價值進行重要性排序，並依該營業秘密之生命週期將保密之期間記載（基於成本考量，將已不具有價值、不需保密之客體從保護範圍移除）。（2）保護該等營業秘密之措施，並注意應除舊布新，即建議應將不合時宜的保護措施去除，並新增有效的保護措施。（3）其他建議事項：於查核過程中所發現其他相關問題（含管理措施、法律問題等）。

---

46 *Id*. at 150.

47 The Defend Trade Secrets Act of 2016, S.1890,114th Congress.§2（2016）、章忠信，美國新訂營業秘密保護法案強化民事救濟手段，http://www.copyrightnote.org/ArticleContent.aspx?ID=8&aid=2774（最後瀏覽日：2020/1/30）、曾勝珍，2016年美國營業秘密防衛法修法前後之案例探討（上），全國律師月刊2019年6月號，頁54。

此外，如前所述，此份報告本身也是一個核心之營業秘密，因報告內容蒐集整合了公司內部與營業秘密相關訊息，故這份報告應視為最高等級之營業秘密加以保護。最後，於稽核報告結果出來後，公司便應執行相應的改善措施。而此種稽核程序應該定期執行之（期間視公司規模大小而有區別），原則上最好一年一次，以便了解、更新公司內部營業秘密之最新狀態，適時讓新發現或新產生之營業秘密納入保護範圍，再者，基於成本考量，應將舊的、不需納入保護範圍之營業秘密移出保護清單中。

伍、結論

生技、醫藥產業領域以營業秘密保護核心技術乃屬常見，在產業合作之必要及人員流動快的情況下，如何避免、降低、轉化「營業秘密外洩」、「不當使用他人營業秘密」之風險是生技、醫藥產業應重視之議題。而本文認為透過以風險管理架構為主，輔以法律思維所建立之營業秘密稽核制度，可達成有效率且符合成本之管理措施。

此外，在具體運用營業秘密稽核制度時，建議應注意以下事項：

一、組成人員應來自各相關單位

人員組成須包含研發、資訊及法務，其中研發技術人員部分因專業分工細，故應視各生技公司之情況納入基礎學科背景、機械、生醫工程背景之人員，唯有了解該項技術之人員參與方能識別出資訊內容之屬性並進行分析。至於法務人員可提供法律諮詢並藉由稽核過程，再度檢視公司之措施、政策及檢視公司與員工之協議是否具有有效防堵公司員工外洩及不當使用他人之營業秘密。最後，許多保護措施需要透過科技、資訊方式進行，故資訊人員加入也是稽核團隊組成不可或缺者。

二、風險識別及風險分析階段具有特別重要性

生技產業特別重視測試、試驗及研發，這一連串環節所產出之相關實驗數據、資料，都可能會是營業秘密保護之核心標的，故對於上開資訊之識別及分析尤其應投入更多心力。此外，營業秘密雖然分為「技術性」及「非技術性」二種，唯有時這二種類型會有重疊的情況，故此分類並不影響所給予之保護措施等級，尤其在生技領域研發合作機會甚高，公司之研發資訊同時也可能是合作公司（客戶）之資訊，故於識別及分析營業秘密之階段應予以特別注意。最後，不同型態之生技公司，所追求技術領域內容亦有不同，針對不同類型公司辨識出之重點（核心）保護客體亦不相同，故應注意與核心資訊科技技術相關之資訊保護。

三、風險應對策略

在生技、醫藥領域核心配方、實驗方法、製作流程之相較於其他產業領域更顯重要性，上開資訊均屬與公司產品相關之核心技術應該予以最高等級之機密保護（應對）措施。至於其他部門（如財務、業務、行政等）亦應視各自部門屬性情況訂定不同層級機密分類標準。

四、參與稽核之人員須簽署保密協議

稽核報告是公司內部營業秘密之整合內容，此份稽核報告當然屬於公司內部之最高機密，故而參與之人員均必須簽署保密協議。而與稽核相關之內容當然也必須列入最高機密對待之。

本文認為以上所介紹的稽核、管理措施一方面可避免公司之營業秘密遭外洩，同時也藉此管理機制可避免公司內部使用不法、或不當使用他人營業秘密之情況。此外，藉由定期性、整合性、有系統、具體、易執行、易追蹤之稽核制度更可能達到整合公司營業秘密及其他智慧財產權，強化公司競爭力之效果，在生技產業日漸重要、科技技術越來越進展之未來，若能運用有效之管理、稽核制度管理公司營業秘密也是生技公司取得競爭力之重要方向。