股票代號：6690

安碁資訊股份有限公司
Acer Cyber Security Inc.

——三年度年報

刊印日期：民國一一四年三月二十九日
年報查詢網址：http://mops.twse.com.tw
公司網址：https://www.acercsi.com/

一、本公司發言人、代理發言人姓名、職稱、聯絡電話及 e-mail：

發言人	譚百良	財務長	(02)8979-6286	ir@acercsi.com
代理發言人	凌秋玉	總監	(02)8979-6286	ir@acercsi.com

二、總公司、分公司、工廠之地址及電話：

單位	地址	電話
總公司	台北市115南港區南港路三段9號13樓	(02)8979-6286
分公司	無	
工廠	無	

三、股票過戶機構之名稱、地址、網址及電話：

名稱	台新綜合證券股份有限公司股務代理
地址	台北市104建國北路一段96號B1
網址	www.tssco.com.tw
電話	(02)2504-8125

四、最近年度財務報告簽證會計師姓名、事務所名稱、地址、網址及電話：

姓名	趙敏如會計師、張惠貞會計師
事務所名稱	安侯建業聯合會計師事務所
地址	台北市110信義路五段7號68樓
網址	www.kpmg.com.tw
電話	(02)8101-6666

五、海外有價證券掛牌買賣之交易場所名稱及查詢該海外有價證券資訊之方式：

不適用

六、公司網址：

www.acercsi.com

目　錄

壹、 致股東報告書 2

一、 致股東報告書 2

二、 民國 113 年度營業結果 4

三、 民國 114 年度營業計劃 7

貳、 公司治理報告 17

一、 董事、總經理、副總經理、協理、各部門及分支機構主管資料 17

二、 最近年度支付董事、監察人、總經理及副總經理之酬金 26

三、 公司治理運作情形 31

四、 簽證會計師公費資訊 54

五、 更換會計師資訊 55

六、 公司董事長、總經理、負責財務或會計事務之經理人，最近一年內曾任職於簽證會計師所屬事務所或其關係企業之情形 55

七、 最近年度及截至年報刊印日止，董事、監察人、經理人及持股比例超過百分之十之股東股權移轉及股權質押變動情形 55

八、 持股比例占前十名股東，其相互間為關係人或為配偶、二親等以內之親屬關係之資訊 55

九、 公司、公司之董事、經理人及公司直接或間接控制之事業對同一轉投資事業之持股數， 並合併計算綜合持股比例 56

參、 募資情形 58

一、 公司資本及股份 58

二、 公司債（含海外公司債）辦理情形 62

三、 特別股辦理情形 62

四、 海外存託憑證之辦理情形 62

五、 員工認股權憑證辦理情形 62

六、 限制員工權利新股辦理情形 62

七、 併購或受讓他公司股份發行新股辦理情形 64

八、 資金運用計畫執行情形 65

肆、 營運概況 67

一、 業務內容 67

二、 市場及產銷概況 98

三、 最近二年度及截至年報刊印日從業員工資料 107

四、 環保支出資訊 107

五、 勞資關係 108

六、 資通安全管理 109

七、 重要契約 112

伍、 財務狀況及財務績效之檢討分析與風險事項之評估 114

一、 財務狀況（合併財報） 114

二、 財務績效（合併財報） 115

三、 現金流量 115

四、 最近年度重大資本支出對財務業務之影響 116

五、 最近年度轉投資政策、其獲利或虧損之主要原因、改善計畫及未來一年投資計畫 116

六、 最近年度及截至年報刊印日止風險事項之分析評估 116

七、 其他重要事項 122

陸、 特別記載事項 124

一、 關係企業相關資料 124

二、 最近年度及截至年報刊印日止，私募有價證券辦理情形 124

三、 其他必要補充說明事項 124

柒、 附錄一 126

一、 公司董事兼任其他公司職務一覽表 126

壹、致股東報告書

壹、 致股東報告書

一、致股東報告書

各位股東：

安碁資訊（股票代號：6690）自 108 年 10 月 30 日在證券櫃檯買賣中心上櫃已經 5 個年頭，在現有的數位雲端類股產業中，安碁資訊仍是唯一一家專注於資訊安全服務的上櫃公司。隨著資安生態系的快速發展，越來越多雲端服務公司與系統整合商加入上櫃行列，促進了資安產業的成長，並強化企業在營運中的資安防護能力。

113 年因國際地緣政治與國內詐騙事件頻傳，資訊安全的重要性更加凸顯。特別是引用中俄領土爭議的「璦琿條約」事件，引發親俄駭客發動大規模 DDoS 攻擊，讓國家安全與公司治理中的資安需求進一步提升。從國安層級到董事會治理，資訊安全的落實成為必要措施。近年個資外洩，國內詐騙之社會新聞成為矚目焦點，上市櫃公司開始正視機敏資料與個資曝露的風險，因個資外洩企業受罰不僅是資安重訊，對企業商譽也造成嚴重的損害。

根據 113 年的營收數據，安碁資訊表現亮眼，全年的合併營收較去年成長 16%，達到 2146 佰萬元，優於 IDC 預測的台灣資安市場未來五年 11.9%的複合成長率。其主要成長動能來自於資訊安全委外監控（SOC 7x24）、營運不中斷服務，以及資安檢測的顯著貢獻。特別是在 SOC 服務領域，安碁資訊已具領先優勢，並成功拓展至製造業客戶群。

此外，因應金管會推動的行動資安 2.0 攻防演練及國家關鍵基礎設施的演習需求，資安檢測業務需求大增。而資安事件頻發也帶動了鑑識服務的需求，使其成為開發新客戶的重要切入點。這些因素共同促成了安碁資訊在 113 年的穩健成長，並奠定了其在資安市場中的領導地位。

安碁資訊在 114 年的營運策略中，將以提升毛利與擴大市場為核心目標，並聚焦於 AI 與雲端相關領域的發展。針對核心業務 SOC，安碁資訊已展開營運最佳化計畫，目前服務約 300 個 B2B 客戶，每月新增日誌量超過 4000 億筆。未來將致力於提升日誌收集與分析的效率，並在委外監控架構上進行改良，以降低設備建置成本並加強弱點防護。同時，透過既有工具的研發基礎，推出創新產品與服務，進一步提升 SOC 服務的毛利與競爭力。

此外，安碁資訊也積極擴增資安檢測人力，強化紅隊演練服務能力。目前政府公部門已將紅隊演練納入共同供應契約，而 BAS（入侵與攻擊模擬演練）及 MDR（威脅偵測應對服務）已建立穩定客戶基礎。未來將持續擴大團隊規模，以抓住更多商機，進一步提升毛利並擴展市場佔有率。

以雲端技術提供服務的子公司宏碁雲架構（Acer eDC）113 年度再度以 Cloud SOC 創新技術取得年度最佳微軟 Azure Security 最佳合作夥伴，在雲端服務的三大主軸包括：

一、持續專注雲端維運服務，提供企業與政府單位建置日常維運一站式的資安監控服務解決方案，特別是 7x24 Cloud SOC 監控服務，確保資訊安全操作（SecOps）的高效運行。同時派任雲端服務顧問提供日常維運與雲端建置顧問服務，協助上雲安全。

二、提供零信任以及備援備份加密分持方案，提供與現有雲端服務商的差異化服務，並可進一步與市場上的雲端服務商做出結盟，提供客戶最佳選擇。

三、提供 AI 助手的顧問服務，藉由 CSP（Cloud Service Provider）原生方案將工具轉化為日常維運，該顧問服務的導入將使既有日常維運事半功倍，並提供雲端資安檢測服務，持續擴大雲端服務管理多樣性。

以培育資安人才的子公司安碁學苑在資安教育領域的努力與成果令人印象深刻。除了提供常態性開課的 ICO27001 LA 及轉版課程外，113 年新增的雲端安全證照 CCSK 課程，進一步擴大了學員的選擇範圍。學苑累積的 100 多個課程模組，不僅能靈活設計短時長課程，還適時安排週末班，方便學員兼顧工作與學習需求。此外，兩次新人三週訓練結合理論與實務操作，幫助學員更有信心進入資安領域。

另一方面，安碁資訊在技術服務與人力培訓上持續精進，填補現今大學資安課程的不足，並密切關注 AI 與 GPT 等新技術的應用及相關資安威脅。透過新科技提升自動化分析、報告產出等效能，為客戶提供更全面的資訊安全保障，展現出其對未來趨勢的前瞻性與專業性。

董事長  經理人  會計主管 

二、民國 113 年度營業結果

（一）營業成果

1. 合併財務報表資訊

單位：新台幣仟元

年度 項目	最近五年度財務資料				
	109年	110年	111年	112年	113年
營業收入	803,373	852,427	1,603,216	1,844,558	2,146,434
營業毛利	321,209	361,849	642,489	733,332	890,329
營業損益	100,449	104,232	185,451	232,997	293,491
營業外收入及支出	977	4,387	2,005	(803)	(10,636)
稅前淨利	101,426	108,619	187,456	232,194	282,855
繼續營業單位本期淨利	82,154	86,853	155,366	190,587	225,763
停業單位損失	-	-	-	-	-
本期淨利（損）	82,154	86,853	155,366	190,587	225,763
本期其他綜合損益（稅後淨額）	(2,367)	(1,111)	(6,574)	(6,058)	4,350
本期綜合損益總額	79,787	85,742	148,792	184,529	230,113
淨利歸屬於母公司業主	82,154	86,853	155,366	190,587	225,763
淨利歸屬於非控制權益	-	-	-	-	-
綜合損益總額歸屬於母公司業主	79,787	85,742	148,792	184,529	230,113
綜合損益總額歸屬於非控制權益	-	-	-	-	-
每股盈餘（虧損）(元)	4.83	5.11	7.92	8.66	10.13

2. 個體財務報表資訊

單位：新台幣仟元

年度 項目	最近五年度財務資料				
	109年	110年	111年	112年	113年
營業收入	803,373	852,427	905,003	1,031,866	1,153,350
營業毛利	321,209	361,849	375,433	408,014	455,693
營業損益	100,449	106,506	68,372	77,501	70,650
營業外收入及支出	977	2,113	102,442	132,383	171,480
稅前淨利	101,426	108,619	170,814	209,884	242,130
繼續營業單位本期淨利	82,154	86,853	155,366	190,587	225,763
停業單位損失	-	-	-	-	-
本期淨利（損）	82,154	86,853	155,366	190,587	225,763
本期其他綜合損益（稅後淨額）	(2,367)	(1,111)	(6,574)	(6,058)	4,350
本期綜合損益總額	79,787	85,742	148,792	184,529	230,113
淨利歸屬於母公司業主	82,154	86,853	155,366	190,587	225,763
淨利歸屬於非控制權益	-	-	-	-	-
綜合損益總額歸屬於母公司業主	79,787	85,742	148,792	184,529	230,113
綜合損益總額歸屬於非控制權益	-	-	-	-	-
每股盈餘（虧損）(元)	4.83	5.11	7.92	8.66	10.13

（二）財務收支及獲利能力分析

1. 合併財務報表資訊

單位：新台幣仟元

	項目	民國112年度	民國113年度
財務收支	營業收入	1,844,558	2,146,434
	營業毛利	733,332	890,329
	稅後淨利	190,587	225,763
獲利能力	資產報酬率（%）	8.33%	6.61%
	股東權益報酬率（%）	15.23%	10.49%
	純益率（%）	10.33%	10.52%
	每股盈餘（元）	8.66	10.13

2. 個體財務報表資訊

單位：新台幣仟元

	項目	民國112年度	民國113年度
財務收支	營業收入	1,031,866	1,153,350
	營業毛利	408,014	455,693
	稅後淨利	190,587	225,763
獲利能力	資產報酬率（%）	11.76%	8.64%
	股東權益報酬率（%）	15.23%	10.49%
	純益率（%）	18.47%	19.57%
	每股盈餘（元）	8.66	10.13

三、民國 114 年度營業計劃

（一）本年度營業計畫概要

1. 發展主動式資安監控中心（Intelligent SOC）

主動式資安監控中心（Intelligent SOC, iSOC）成為企業資安的新標準，結合 AI 分析、自動化回應、威脅情報整合，提供更快、更準確的威脅偵測與應變能力。運用多種 AI 模型進行日誌分析，涵蓋 IT、OT、雲端等三大環境，針對不同客戶和各種不同設備進行多面向分析，從監控服務客戶端的日誌來源，找出異常的行為，挖掘潛藏資安威脅，實現自動化的偵測、判斷與回應，到整合外部威脅情資來源，提升事前日誌監控分析的精準度。在事中、事後階段方面，與 SOC 整合的事件調查、鑑識服務、SOAR，以及惡意威脅狩獵分析服務也是重點。

2. Cloud SOC 雲端及地端資安監控整合服務

本公司是國內唯一完整整合雲原生資安監控平台與 7x24 資安監控維運服務的資安服務廠商。面對現今企業多採混合雲布局的主流趨勢，安碁資訊更可協助客戶導入雲地整合監控與聯防服務機制，整合多雲與地端的資安監控機制於單一監控服務平台，確保企業資安治理與資安維運的完整性與一致性。透過宏碁雲架構，將微軟 Azure 雲端設備日誌與資料整合平台 API 串接，結合既有 ACSI SOC 核心技術能量，並由安碁資訊專家進行關聯規則建立，監控雲端各種資安設備被刺探的行為，將監控的日誌資料所觸發的「事件」進行彙整，再將「事件」遞送轉交給地端的安全監控中心（SOC）進行關聯分析，進而比對雲、地所發生的資安事件關聯，雲端日誌不落地，節省大量日誌下載的網路傳輸費用，建立雲地監控中心混合互相回饋

循環機制。安碁資訊能夠協助企業由單一環境無痛整合至混合雲，提供更安全可靠的雲端服務，使得企業在雲端服務上的共享資源，擁有更大的彈性與靈活性，捍衛雲地 IT / OT 安全，實現企業永續營運的韌性。

3. 發展雲端資安監控中心服務（Cloud SOC）

   是專門為雲端環境設計的資安事件監控與應變平台，負責監測、分析、應對雲端環境中的各種安全威脅與攻擊。Cloud SOC 的核心目標是透過自動化、安全分析、AI 與零信任技術，確保企業的雲端基礎設施、應用、數據免受網路攻擊的威脅。

4. 發展雲端資安監控基準

   隨著企業向雲端遷移，確保雲端環境的安全變得至關重要。傳統資安監控方法已無法滿足動態、分散的雲端架構，因此需要建立雲端資安監控基準（Cloud Security Monitoring Baseline），確保從基礎架構到應用層的全面防護。雲端資安監控基準涵蓋身分與存取、網路安全、應用程式與工作負載、資料保護、安全日誌與事件管理（SIEM）、威脅偵測與回應（MDR）等領域。

5. 發展雲端健診服務

   主要目的是幫助企業評估其雲端環境的安全性，識別潛在的漏洞與風險，並提供改進建議。這樣的服務應結合自動化掃描工具、最佳實踐標準、合規要求及威脅情報，確保雲端架構的完整性和安全性。

6. 推動雲端資安治理解決方案

雲端組態、雲端監控、雲端健診、雲端鑑識與雲端備份（資料加密分持）等五項雲端資安治理解決方案，協助企業在數位轉型提升營運績效之際，共同打造雲端安全的防護力。隨著企業上雲的應用趨勢，整合多雲安全防護也更加重要，安碁資訊在政府、金融、高科技製造業已具備雲地監控整合經驗，從雲端部署、維運監控至雲地兩端關聯分析與情資分享，為客戶在搬遷上雲兼顧雲端安全，提供最佳化的解決方案。

7. 發展紅隊演練服務

紅隊演練（Red Teaming）是一種模擬真實攻擊者的資安測試技術，目標是評估組織的資安防禦能力。核心技術涵蓋情報蒐集、滲透測試、橫向移動、數據竊取、持久化存取，目的是找出組織的資安弱點，提升資安應變能力。

8. 發展入侵及攻擊模擬 BAS（Breach and Attack Simulation）服務

BAS（Breach and Attack Simulation, 入侵及攻擊模擬）是一種自動化攻擊模擬技術，可以持續測試組織的資安防禦能力，並識別安全弱點。BAS 主要模擬真實攻擊者的行為，但不會影響業務運作，BAS 更具自動化、持續性、可量化分析的優勢。

9. 發展零信任架構導入服務

零信任架構（Zero Trust Architecture, ZTA）是一種「永不信任，持續驗證」的安全策略，旨在防止內部與外部威脅。與傳統安全模式不同，零信任不假設內部網路是可信的，而是對每個存取請求進行驗證，確保只有合法用戶與設備能夠存取資源。

10. 整合營運不中斷解決方案

因應駭客勒索黑色產業日益茁壯，復原與備援服務已成為優化與完善本公司提供客戶資安服務所必需，故將整合營運不中斷服務納入資訊安全服務架構，即事前預防-資料與系統備份備原服務、事中偵測-備援演練、事後應變-啟動緊急備援，執行災變復原程序，使整體資安服務架構更為完整，進而強化公司競爭力。

11. 積極拓展上市櫃公司資安服務市場

配合證交所及櫃買中心所公佈的上市上櫃公司資通安全管控指引，要求落實依期程導入國際資安標準並通過驗證及辦理系統滲透測試、資安健診等強化資安防護措施;

並結合通路夥伴，持續擴增在中、南部區域的銷售，擴大對上市上櫃公司業務範圍。

12. 提升安碁學苑在培訓資安人員的課程以及量能

安碁學苑已通過勞動部 TTQS 人才發展品質系統認證，將持續加速職訓機構的設立，以利推動相關資安職能教育訓練，在現有通過的職訓課程中，資安教育訓練成為亮點，也將擴大線上課程以外的實體上課以及企業包班的開課規模，提升人才培育與資安職能教育訓練的服務量能。

13. 積極拓展東南亞海外市場

已於泰國設立營運機構，強化落地資安技術服務，並提供託管式偵測及回應（Managed Detection and Response, MDR），針對客戶端點偵測與回應（Endpoint Detection and Response, EDR）提供解決方案及資安檢測服務，並持續深化與當地夥伴合作，朝向資安區域聯防的目標前進。

（二）未來公司發展策略

1. 發展主動式資安監控中心（Intelligent SOC）

主動式監控智能中心（Intelligent SOC, iSOC）成為企業資安的新標準，結合 AI 分析、自動化回應、威脅情報整合，提供更快、更準確的威脅偵測與應變能力。

2. 發展 Cloud SOC 雲端及地端資安監控整合

本公司是國內唯一完整整合雲原生資安監控平台與 7x24 資安監控維運服務的資安服務廠商。面對現今企業多採混合雲布局的主流趨勢，安碁資訊更可協助客戶導入雲地整合監控與聯防服務機制，整合多雲與地端的資安監控機制於單一監控服務平台，確保企業資安治理與資安維運的完整性與一致性。透過宏碁雲架構，將微軟 Azure 雲端設備日誌與資料整合平台 API 串接，結合既有 ACSI SOC 核心技術能量，並由安碁資訊專家進行關聯規則建立，監控雲端各種資安設備被刺探的行為，將監控的日誌資料所觸發的「事件」進行彙整，再將「事件」遞送轉交給地端的安全監控中心（SOC）進行關聯分析，進而比對雲、地所發生的資安事件關聯，雲端日誌不落地，節省大量日誌下載的網路傳輸費用，建立雲地監控中心混合互相回饋循環機制。安碁資訊能夠協助企業由單一環境無痛整合至混合雲，提供更安全可靠的雲端服務，使得企業在雲端服務上的共享資源，擁有更大的彈性與靈活性，捍衛雲地 IT / OT 安全，實現企業永續營運的韌性。

3. 發展 AI 在資安領域的應用與技術發展

(1) 威脅檢測與回應

AI 能即時監控網路和系統，分析大量數據以快速偵測和回應威脅。這包括識別異常行為模式，預測潛在攻擊，並自動化威脅回應。

(2) 惡意程式偵測

AI 演算法可以分析檔案特性和行為模式，偵測惡意程式。這些演算法能夠比傳統方法更快、更準確地識別新型惡意軟體。

(3) 行為分析

AI 能分析使用者和系統的行為，發現可能意味著資安威脅的異常情況，從而提前預防攻擊。

(4) 自動化資安工作

AI 可以自動化例行性資安工作，如威脅偵測和事件回應，讓資安人員專注於更複雜的任務。

(5) 漏洞挖掘

AI 技術被用來發現和修補軟體漏洞，提升軟體開發的安全性。例如，AI 可以幫助

縮小漏洞範圍，並加速漏洞修補過程。

(6) 深度偽造防護

AI 技術也被用來識別和防止利用假視頻和音頻進行的詐騙和身份冒充。

4. 發展雲端資安監控技術

是確保雲端環境中資料、應用和基礎設施的安全性，對於企業保護其雲端基礎設施免受各類攻擊與威脅至關重要。隨著企業將更多業務遷移到雲端，這些監控技術需要有針對性地涵蓋不同層級的資安防禦，並具備強大的即時偵測與反應能力。雲端資安監控的核心技術如下：

- 監控層次與技術
- 資安事件監控
- 威脅偵測與異常行為識別

5. 發展威脅情資 AI 分析平台（ATHENA）

透過每月蒐集的高達 4,000 億筆資料，可結合機器學習(ML)、自然語言處理(NLP)與威脅情報(Threat Intelligence, TI)技術，打造自動化、精準的資安威脅分析系統。以下是關鍵技術架構與發展方向：

(1) 威脅情資收集與解析

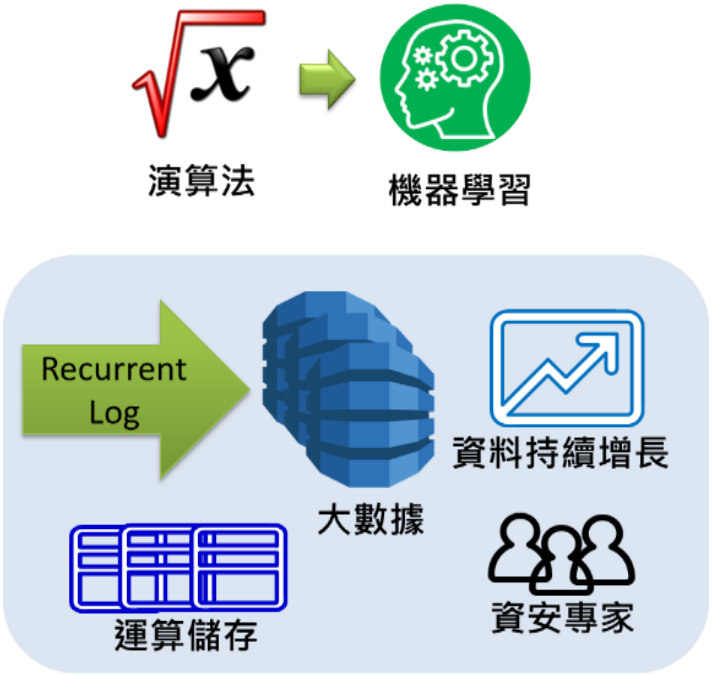
- 多來源情報整合
- NLP 驅動情報解析

(2) AI 驅動威脅分析

- 機器學習偵測

  攻擊預測模型（Attack Prediction Models）：基於 MITRE ATT&CK 框架建立攻擊預測模型。
- 自動化關聯分析

發展威脅情資 AI 分析平台（ATHENA）



（三）受到外部競爭環境、法規環境及總體經營環境之影響

上市（櫃）公司及證券商之資通安全攸關投資大眾權益，金融監督管理委員會（下稱金管會）積極配合推動國家資通安全政策完成相關資通安全措施，已督導證交所及櫃買中心組成資安相關跨部門任務型專案小組，並完成「公開發行公司年報應行記載事項準則」、「公開發行公司建立內部控制制度處理準則」、「上市上櫃公司資通安全管控指引」、「建立證券商資通安全檢查機制」等相關法規修正及指引，提醒上市（櫃）公司及證券商自 111 年起應依相關規定辦理。

上市（櫃）公司及證券商應建立適當內部控制以降低資通安全風險，除應建立適當資通安全作業，並應配置適當人力資源及設備進行資訊安全制度之規劃、監控及執行。金管會已請證交所修正公司治理評鑑指標，完成導入國際資安標準並取得外部驗證之上市（櫃）公司，將於公司治理評鑑時加分，並請證交所及櫃買中心發布上市上櫃公司資通安全管控指引，提供上市（櫃）公司執行內部控制措施時之參考。另證券商部分，符合一定條件之證券商應指派副總經理以上或職責相當之人兼任資訊安全長。證券商並應依證交所資通安全檢查機制分級防護應辦事項，依期程導入國際資安標準並通過驗證及辦理系統滲透測試、資安健診等強化資安防護措施。

另為強化上市（櫃）公司資通安全資訊公開，上市（櫃）公司除應於股東會年報中敘明資通安全政策、具體管理方案及投入資通安全管理之資源等資訊外，如遇發生重大

資通安全事件，應即時發布重大訊息說明發生緣由、可能損失、改善情形及因應措施，並於損失達一定金額以上時，召開重大訊息記者會對外說明，及於股東會年報中揭露所遭受之損失、可能影響、因應措施等資訊。

本公司對這些相關的法規，如何落實在商業、製造業的運用都密切注意中，隨時調整服務類別以及產業應用顧問的訓練，相關的維運經驗以及大數據 AI 發掘也都會透過維運團隊跟研發的互相學習而得到好的成果發展，進而產生新的服務項目跟深化對客戶服務滿意度的目標。在面對全球驟變競爭激烈的環境中，唯有走在資安技術服務的前端，對於資安事件的預防能力再提升，才是領先同業競爭者最大的競爭優勢。

貳

、公司治理報告

貳、 公司治理報告

一、董事、總經理、副總經理、協理、各部門及分支機構主管資料

(一) 董事

1. 董事之基本資料

日期：114 年 3 月 29 日；單位：股

職稱	國籍或註冊地	姓名	性別年齡	選(就)任日期	任期	初次選任日期	選任時持有股份		現在持有股數		配偶、未成年子女現在持有股份		利用他人名義持有股份		主要經(學)歷	目前兼任本公司及其他公司之職務	具配偶或二親等以內關係之其他主管、董事或監察人			備註
							股數	持股比率	股數	持股比率	股數	持股比率	股數	持股比率			職稱	姓名	關係	
董事長	中華民國	宏碁(股)公司	-	111.5.27	3 年	90.4.6 (註1)	10,971,018	63.63%	15,561,992	51.87%	0	0	0	0	-	-	-	-	-	-
	中華民國	代表人：施宣輝	男 51-60歲	111.5.27	3 年	107.06.13	0	0	0	0	7,973	0.03%	0	0	宏碁雲端科技事業群總經理特別助理 美國南加大電機博士	其他兼任職務詳(註2)	-	-	-	-
董事	中華民國	宏碁(股)公司	-	111.5.27	3 年	90.4.6 (註1)	10,971,018	63.63%	15,561,992	51.87%	0	0	0	0	-	-	-	-	-	-
	中華民國	代表人：蔡傑智	男 41-50歲	111.5.27	3 年	112.5.12	0	0	0	0	0	0	0	0	國立陽明交通大學資訊科學碩士 宏碁股份有限公司智慧移動事業處長	其他兼任職務詳(註2)	-	-	-	-
董事	中華民國	宏碁(股)公司	-	111.5.27	3 年	90.4.6 (註1)	10,971,018	63.63%	15,561,992	51.87%	0	0	0	0	-	-	-	-	-	-
	中華民國	代表人：陳怡如	女 61-70歲	111.5.27	3 年	107.03.30	0	0	38,681	0.13%	0	0	0	0	美國洛杉磯加州大學安德森管理學院企業管理碩士 宏碁(股)公司全球資金總處主管	其他兼任職務詳(註2)	-	-	-	-

日期：114 年 3 月 29 日；單位：股

職稱	國籍或註冊地	姓名	性別年齡	選(就)任日期	任期	初次選任日期	選任時持有股份		現在持有股數		配偶、未成年子女現在持有股份		利用他人名義持有股份		主要經(學)歷	目前兼任本公司及其他公司之職務	具配偶或二親等以內關係之其他主管、董事或監察人			備註
							股數	持股比率	股數	持股比率	股數	持股比率	股數	持股比率			職稱	姓名	關係	
獨立董事	中華民國	童至祥	女 61-70歲	111.5.27	3 年	107.12.13	0	0	0	0	0	0	0	0	特力集團執行長 台灣IBM總經理 台灣大學外國語文學系	展籐有限公司董事長 矽力杰(股)公司董事	-	-	-	-
獨立董事	中華民國	龍惠施	女 61-70歲	111.5.27	3 年	111.5.27	0	0	0	0	0	0	0	0	宏碁(股)公司全球財務總部 財務資訊總處總處長 國立政治大學企業管理學士	祥龍投資有限公司董事長 曜揚科技股份有限公司董事長 建碁股份有限公司獨立董事 達運精密工業股份有限公司獨立董事 葳天科技股份有限公獨立董事	-	-	-	-
獨立董事	中華民國	蔡東峻	男 61-70歲	111.5.27	3 年	111.5.27	0	0	0	0	0	0	0	0	國立成功大學交通管理科學學系主任 國立成功大學國際企業研究所所長 國立成功大學EMBA/AMBA執行長 美國伊利諾大學香檳校區企業管理博士	財團法人宏碁基金會董事 財團法人莊漢開教授文教基金會董事	-	-	-	-
獨立董事	中華民國	李紀珠	女 61-70歲	111.5.27	3 年	111.5.27	0	0	0	0	0	0	0	0	臺灣銀行暨臺灣金控董事長 中華民國行政院金融監督管理委員會副主委 中華民國立法委員 中華郵政公司董事長 國立政治大學經濟系所專任教授 新光銀行副董事長 新光金控暨新光人壽副董事長 美國哈佛大學經濟系訪問學者 美國史丹佛大學經濟系訪問學者 國立台灣大學經濟學博士	中華產經發展協會理事長 國立政治大學兼任教授 保利馬公司監察人 台灣玉山科技協會榮譽理事長 國際金融論壇(IFF)理事 東亞經濟協會副理事長	-	-	-	-

註 1：原法人股東宏碁電腦公司於 91.3.27 併入宏碁股份有限公司。

註 2：兼任該集團之其他子公司職務詳如附錄一。

2. 法人股東之主要股東

日期：114 年 3 月 29 日

法人股東名稱	法人股東之主要股東	持股比
宏碁股份有限公司	元大台灣高股息基金專戶	5.23%
	台北富邦商業銀行股份有限公司受託保管復華台灣科技優息ＥＴＦ證券投資信託基金專戶	3.65%
	宏榮投資股份有限公司	2.42%
	臺灣中小企業銀行股份有限公司受託保管大華銀台灣優選股利高填息３０ＥＴＦ證券投資信託基金專戶	1.85%
	渣打國際商業銀行營業部受託保管先進星光基金公司之系列基金先進總合國際股票指數基金投資專戶	1.33%
	渣打國際商業銀行營業部受託保管梵加德集團公司經理之梵加德新興市場股票指數基金投資專戶	1.21%
	施振榮	1.15%
	合作金庫商業銀行股份有限公司	1.15%
	花旗（台灣）銀行託管ＡＣＥＲ海外存託憑證	0.90%
	融欣管理顧問股份有限公司	0.75%
	榕安管理顧問股份有限公司	0.75%

3. 法人股東之主要股東屬法人者其主要股東

日期：114 年 3 月 29 日

法人股東名稱	法人股東之主要股東	持股比
宏榮投資股份有限公司	施宣輝	26.09%
	葉紫華	20.13%
	施宣榕	17.25%
	施宣麟	17.16%
	施芳程	8.93%
	葉庭宇	8.84%
	財團法人智榮文教基金會	1.60%
合作金庫商業銀行股份有限公司	合作金庫金融控股股份有限公司	100%
融欣管理顧問股份有限公司	施宣麟	54.57%
	施芳程	22.71%
	施儀佳	22.71%

日期：114 年 3 月 29 日

法人股東名稱	法人股東之主要股東	持股比
榕安管理顧問股份有限公司	施宣榕	43.58%
	葉庭宇	18.81%
	葉珈瑄	18.81%
	葉秉學	18.81%
	施宣麟	0%

註：財團法人智榮文教基金會之捐助者為施振榮先生，捐助比率 100%。

4. 董事專業資格及獨立董事獨立性資訊揭露

條件 姓名	專業資格與經驗	獨立性情形	兼任其他公開發行公司獨立董事家數
施宣輝	1. 施宣輝先生為安碁資訊(股)公司及智聯服務(股)公司董事長。宏碁(股)公司於2011年併購雲端服務公司iGware，施宣輝正式加入宏碁(股)公司擔任其總經理特別助理，為雲端服務開發奠定基礎。2014年起雲端服務轉為宏碁(股)公司自建雲事業群，由施宣輝擔任總經理協助宏碁進行全方面的轉型。 2. 施宣輝先生具有電機工程博士學位，過去曾從事IC設計、多媒體影/音訊號處理技術、圖像分析及平板電腦的軟體設計。 3. 專長於資訊科技領域，且未有公司法第30條各款情事。	1. 除本人兼任部分宏碁集團公司董事、宏碁雲架構董事長、智聯服務公司董事長及兼任部分宏碁集團公司董事外，其父親(施振榮)亦兼任部分宏碁集團公司董事，配偶或二親等以內親屬則未有擔任集團公司董事、監察人或受僱人之情事。 2. 本人未持有本公司股份，其配偶及未成年子女則持有股份共計7,973股(0.03%)。 3. 本人及其配偶或二親等以內親屬均未有擔任與本公司有特定關係公司之董事、監察人或受僱人，亦無提供集團公司商務、法務、財務及會計等服務之情事。	0
陳怡如	1. 陳怡如女士在財務專業領域擁有30年以上經驗，並於2017年7月接任宏碁(股)公司全球財務長至今。 2. 陳怡如女士在1999年加入宏碁(股)公司，歷任全球及區域資金部主管職務，2002年至2004年擔任亞太地區資金部主管，自2005年起擔任全球資金業務部門處長，至2017年升任為全球財務長。在陳怡如的領導之下整合宏碁全球財務狀況，成功簡化全球一百多間子公司的財務流程。在進入宏碁之前，陳怡如曾任職於花旗銀行。 3. 陳怡如女士擁有台灣大學經濟系學士，並具有美國加州大學洛杉磯分校安德森	1. 除本人為宏碁(股)公司全球財務長，並兼任部分宏碁集團公司董事外，配偶或二親等以內親屬未有擔任集團公司董事、監察人或受僱人之情事。 2. 本人持有38,681股(0.13%)，其配偶或二親等以內親屬則未持有本公司股份。 3. 本人及其配偶或二親等以內親屬均未有擔任與本公司有特定關係公司之董事、監察人或受僱人，亦無提供集團公司商務、法務、財務及會計等服務之情事。	0

條件 姓名	專業資格與經驗	獨立性情形	兼任其他公開發行公司獨立董事家數
	管理學院企業管理碩士學位。 專長於企業財務、資金與風險管理等領域，且未有公司法第30條各款情事。		
蔡傑智	1. 蔡傑智先生為宏碁(股)公司智慧移動事業處長。蔡傑智先生2002年加入宏碁，歷經筆電、智慧型手機、智慧家庭等創新產品研發與管理，於2011年加入宏碁雲端擔任產品管理主管。2022年擔任宏碁集團董事長技術助理，2023年接任智慧移動新事業負責人。 2. 蔡傑智先生具有資訊科學碩士學位，曾從事嵌入式系統開發、智慧型手機軟體管理及多項雲端應用管理。另管理碩士在職專班畢業。 3. 專長於資訊科技領域，且未有公司法第30條各款情事。	1. 除本人為宏碁(股)公司智慧移動事業處長外，配偶或二親等以內親屬未有擔任集團公司董事、監察人或受僱人之情事。 2. 本人及其配偶或二親等以內親屬均未持有本公司股份。 3. 本人及其配偶或二親等以內親屬均未有擔任與本公司有特定關係公司之董事、監察人或受僱人，亦無提供集團公司商務、法務、財務及會計等服務之情事。	0
龍惠施	1. 龍惠施女士曾任宏碁(股)公司全球財務總部財務資訊總處總處長，擁有豐富的財務相關經驗。現任為祥龍投資有限公司董事長及曜揚科技股份有限公司董事長等。 2. 龍惠施女士擁有國立政治大學企業管理學士學位。 3. 專長於企業財務與投資等領域，且未有公司法第30條各款情事。	1. 除本人為建碁(股)公司獨立董事外，配偶或二親等以內親屬未有擔任集團公司董事、監察人或受僱人之情事。 2. 本人及其配偶或二親等以內親屬均未持有本公司股份。 3. 本人及其配偶或二親等以內親屬均未有擔任與本公司有特定關係公司之董事、監察人或受僱人，亦無提供集團公司商務、法務、財務及會計等服務之情事。	3
童至祥	1. 童至祥女士曾任IBM台灣第一任女性總經理並於特力集團擔任執行長長達11年，現為展藤有限公司董事長及矽力杰(股)公司董事。 2. 專長於企業經營管理、國際貿易與行銷等領域，且未有公司法第30條各款情事。	1. 本人及其配偶或二親等以內親屬未有擔任集團公司董事、監察人或受僱人之情事。 2. 本人及其配偶或二親等以內親屬均未持有本公司股份。 3. 本人及其配偶或二親等以內親屬均未有擔任與本公司有特定關係公司之董事、監察人或受僱人，亦無提供集團公司商務、法務、財務及會計等服務之情事。	0
蔡東峻	1. 蔡東峻先生曾擔任國立成功大學交通管理科學學系主任、國立成功大學國際企業研究所所長及國立成功大學EMBA/AMBA執行長。現任財團法人宏碁基金會董事及財團法人莊漢開教授文教基金會董事。	1. 除本人為財團法人宏碁基金會董事外，配偶或二親等以內親屬未有擔任集團公司董事、監察人或受僱人之情事。 2. 本人及其配偶或二親等以內親屬均未持有本公司股份。 3. 本人及其配偶或二親等以內親屬均未有	0

條件 姓名	專業資格與經驗	獨立性情形	兼任其他公開發行公司獨立董事家數
	2. 蔡東峻先生擁有美國伊利諾大學香檳校區企業管理博士。 3. 專長於企業管理及行銷管理等領域，且未有公司法第30條各款情事。	擔任與本公司有特定關係公司之董事、監察人或受僱人，亦無提供集團公司商務、法務、財務及會計等服務之情事。	
李紀珠	1. 李紀珠女士現任中華產經發展協會理事長、國立政治大學兼任教授及保利馬公司監察人等。曾任臺灣銀行暨臺灣金控董事長、中華民國行政院金融監督管理委員會副主委、中華民國立法委員、國立政治大學經濟系所專任教授、中華郵政公司董事長、新光金控暨新光人壽副董事長、新光銀行副董事長等職。於金融及經濟領域經驗十分豐富。 2. 李紀珠女士為台灣大學經濟學博士，並為美國哈佛及史丹佛大學經濟系訪問學者。 3. 專長於財務金融及企業管理等領域，且未有公司法第30條各款情事。	1. 本人及其配偶或二親等以內親屬未有擔任集團公司董事、監察人或受僱人之情事。 2. 本人及其配偶或二親等以內親屬均未持有本公司股份。 3. 本人及其配偶或二親等以內親屬均未有擔任與本公司有特定關係公司之董事、監察人或受僱人，亦無提供集團公司商務、法務、財務及會計等服務之情事。	0

5. 董事會多元化及獨立性

(1) 董事會多元化

A. 董事會多元化之政策

本公司隸屬宏碁集團成員之一，一向注重公司治理，並於「公司治理實務守則」第三章「強化董事會職能」訂有董事會成員多元化方針。本公司之董事會應指導公司策略、監督管理階層、對公司及股東會負責，其公司治理制度之各項作業與安排，應確保董事會依照法令、公司章程之規定或股東會決議行使職權。

本公司之董事會結構，應就公司經營發展規模及其主要股東持股情形，衡酌實務運作需要，決定五人以上之適當董事席次。董事會成員組成應考量多元化，除兼任公司經理人之董事不宜逾董事席次三分之一外，並就本身運作、營運型態及發展需求以擬訂適當之多元化方針， 宜包括但不限於以下二大面向之標準：

● 基本條件與價值：性別、年齡、國籍及文化等。
● 專業知識與技能：專業背景 (如法律、會計、產業、財務、行銷或科技)、專

業技能及產業經歷等。

董事會成員組成應普遍具備執行職務所必須之知識、技能及素養。為達到公司治理之理想目標，董事會整體應具備之能力如下：

- 營運判斷能力。
- 會計及財務分析能力。
- 經營管理能力。
- 危機處理能力。
- 產業知識。
- 國際市場觀。
- 領導能力。
- 決策能力。

B. 董事會成員多元化之具體管理目標

董事會成員多元化有助於董事會功能有效發揮，本公司董事會成員之提名與遴選係遵照公司章程之規定，並採用候選人提名制，以確保董事成員之多元性及獨立性，並已遴選具有不同之專業知識之技能之董事，提供不同角度思維與貢獻，以進一步強化董事會職能。本公司已達成獨立董事過半及每一性別佔董事會席次 1/3（含）以上之具體管理目標。

C. 董事會成員多元化之落實情形

截至民國 113 年底，有 1 位董事年齡在 40～50 歲，有 1 位董事年齡在 50～60 歲，有 5 位董事年齡在 60 歲以上；有 4 位女性董事，3 位男性董事；且均為本國籍董事。各董事之專長及多元化背景如下：

- 專長於雲端服務及 IC 設計：施宣輝 先生
- 專長於財務、資金與風險管理等專業領域：陳怡如 女士
- 專長於雲端應用管理、資訊科技及經營管理等專業領域：蔡傑智 先生
- 專長於財務會計、投資與經營策略管理等專業領域：龍惠施 女士
- 專長於資訊系統、企業經營管理、國際貿易等專業領域：童至祥 女士
- 專長於企業經營管理、行銷管理以及學術研究等專業領域：蔡東峻 先生
- 專長於財務金融及經營管理等專業領域，並曾任立法委員等公職：李紀珠 女士

姓名	性別	國籍	類別	年齡			經營策略與管理	資訊服務/AIoT	雲端服務	國際貿易	IC設計	行銷	投資	學術研究	財務金融	會計
				41~50	51~60	61以上										
施宣輝	男	中華民國	法人董事代表人		V		V	V	V		V		V			
陳怡如	女	中華民國	法人董事代表人			V							V		V	V
蔡傑智	男	中華民國	法人董事代表人	V			V	V	V		V					
龍惠施	女	中華民國	獨立董事			V							V		V	V
童至祥	女	中華民國	獨立董事			V	V	V		V			V			
蔡東峻	男	中華民國	獨立董事			V	V					V		V		
李紀珠	女	中華民國	獨立董事			V	V						V		V	

(2) 董事會獨立性

本公司共有七席董事，其中四席為獨立董事，獨立董事之佔比為 57%。由於獨立董事佔董事席次之半數，確能發揮其功能監督公司運作並保護股東權益，其專業觀點均能獨立於管理層或其他董事，彰顯董事會獨立性。

本公司之董事間，除施宣輝先生、陳怡如女士及蔡傑智先生係由宏碁股份有限公司所指派外，其餘之董事 (含獨立董事) 間，並無配偶或二親等以內之親屬關係，故未有違反證券交易法第 26 條之 3 第 3 項。

本公司依法設置審計委員會以替代監察人，故不適用證券交易法第 26 條之 3 第 4 項規定。

(二) 總經理、副總經理、協理及各部門與分支機構主管

日期：114 年 3 月 29 日；單位：股

職稱	國籍	姓名	性別	選(就)任日期	持有股份		配偶、未成年子女持有股份		利用他人名義持有股份		主要經(學)歷	目前兼任其他公司之職務	具配偶或二親等以內關係之經理人			備註
					股數	持股比率	股數	持股比率	股數	持股比率			職稱	姓名	關係	
總經理	中華民國	吳乙南	男	107/06/13	242,003	0.81%	0	0	0	0	SUN Microsystems, Taiwan 業務協理 BMC, Taiwan 業務協理、台灣區總經理 IBM Taiwan 系統工程師、產品經理、行銷經理 美國Syracuse University電腦資訊科學碩士	宏碁雲架構服務(股)公司 董事兼總經理 安碁學苑(股)公司 董事長	-	-	-	-
副總經理	中華民國	楊旭平	男	107/06/13	67,875	0.23%	0	0	0	0	誠旭企業 副理 華康科技公司 經理 金氏電腦 經理 復興工專電機科	-	-	-	-	-
副總經理	中華民國	黃瓊瑩	男	107/06/13	76,939	0.26%	0	0	0	0	NSOC 國家級資訊安全營運中心建置案 技術長 異康(股)公司安全技術部 專案經理、協理 資訊工業策進會系統安全中心 分項計畫主持人 英國曼徹斯特科技大學資訊工程研究所碩士	安碁學苑(股)公司 董事	-	-	-	-
財務及會計主管	中華民國	譚百良	男	107/06/13	104,000	0.35%	0	0	0	0	宏碁(股)公司電子化服務事業群 財務處資深處長 元碁資訊(股)公司 經營分析副理 財團法人中國生產力中心 專案經理 眾信會計師事務所 審計員 東吳大學會計系學士	宏碁智通(股)公司 監察人 安圖斯科技股份有限公司 監察人 宏碁智雲服務(股)公司 監察人 宏碁雲架構服務(股)公司 監察人 安碁學苑(股)公司 監察人 宏碁健康(股)公司 監察人 ACER CLOUD TECHNOLOGY (US), INC. 董事 宏碁雙智(重慶)有限公司 監察人	-	-	-	-
稽核室經理	中華民國	金珊如	女	107/06/13	6,961	0.02%	0	0	0	0	宏碁(股)公司電子化服務事業群 財務主任 勤業眾信會計師事務所 副領組 英國肯特大學國際會計及財務研究所碩士 東吳大學會計系學士	-	-	-	-	-
副總經理及資安長(註1)	中華民國	顧寶裕	男	107/06/13	0	0	0	0	0	0	異康 (股)公司安全系統部 協理 經濟部科技專案 研發工程師及專案經理 資訊工業策進會系統安全中心 專案經理、資深工程師 交通大學資訊科學研究所碩士	-	-	-	-	-

註 1.顧寶裕於 113 年 4 月 30 日辭任，凡解任或辭任者持有股數皆以 0 表示。

二、最近年度支付董事、監察人、總經理及副總經理之酬金

（一）最近會計年度（113 年）支付董事、總經理及副總經理之酬金

1. 董事之酬金

單位：新台幣仟元

職稱	姓名	董事酬金								A、B、C及D等四項總額及占稅後純益之比例		兼任員工領取相關酬金								A、B、C、D、E、F及G等七項總額及占稅後純益之比例		領取來自子公司以外轉投資事業或母公司酬金
		報酬(A)		退職退休金(B)		董事酬勞(C)		業務執行費用(D)				薪資、獎金及特支費等(E)		退職退休金(F)		員工酬勞(G)						
																本公司		財務報告內所有公司				
		本公司	財務報告內所有公司	本公司	財務報告內所有公司	本公司	財務報告內所有公司	本公司	財務報告內所有公司	本公司	財務報告內所有公司	本公司	財務報告內所有公司	本公司	財務報告內所有公司	現金金額	股票金額	現金金額	股票金額	本公司	財務報告內所有公司	
董事長	宏碁(股)公司 代表人：施宣輝	900	900	0	0	0	0	90	90	總額 990 比例 0.44%	總額 990 比例 0.44%	0	0	0	0	0	0	0	0	總額 990 比例 0.47%	總額 990 比例 0.47%	36,749
董事	宏碁(股)公司 代表人：蔡傑智 宏碁(股)公司 代表人：陳怡如																					
獨立董事	龍惠施 童至祥 蔡東峻 李紀珠	1,400	1,400	0	0	2,170	2,170	120	120	總額 3,690 比例 1.63%	總額 3,690 比例 1.63%	0	0	0	0	0	0	0	0	總額 3,690 比例 1.63%	總額 3,690 比例 1.63%	0

1.請敘明獨立董事酬金給付政策、制度、標準與結構，並依所擔負之職責、風險、投入時間等因素敘明與給付酬金數額之關聯性：

(1)本公司給付獨立董事酬勞決策，乃根據本公司之公司章程規定，由薪酬委員會提出報告，經董事會決議通過後，依法提報股東常會報告。

(2)訂定酬金之程序，亦依據公司章程及獨立董事固定報酬給付標準與金額訂定之。

(3)本公司之獨立董事酬勞乃依公司章程規定，公司年度如有獲利，於預先保留彌補累積虧損之數額後，另得提撥不高於0.8%為董事酬勞，並同考量公司未來面臨之營運風險及其與經營績效之正向關聯性，以謀永續經營與風險控管之平衡。

2.除上表揭露外，最近年度公司董事為財務報告內所有公司提供服務（如擔任非屬員工之顧問等）領取之酬金：無。

酬金級距表

給付本公司各個董事酬金級距	董事姓名			
	前四項酬金總額（A+B+C+D）		前七項酬金總額（A+B+C+D+E+F+G）	
	本公司	財務報告內所有公司	本公司	母公司及所有轉投資事業
低於1,000,000元	宏碁（股）公司、施宣輝、蔡傑智、陳怡如、龍惠施、童至祥、蔡東峻、李紀珠	宏碁（股）公司、施宣輝、蔡傑智、陳怡如、龍惠施、童至祥、蔡東峻、李紀珠	宏碁（股）公司、施宣輝、蔡傑智、陳怡如、龍惠施、童至祥、蔡東峻、李紀珠	宏碁（股）公司、龍惠施、童至祥、蔡東峻、李紀珠
1,000,000元（含）～2,000,000元（不含）	-	-	-	-
2,000,000元（含）～3,500,000元（不含）	-	-	-	-
3,500,000元（含）～5,000,000元（不含）	-	-	-	蔡傑智
5,000,000元（含）～10,000,000元（不含）	-	-	-	-
10,000,000元（含）～15,000,000元（不含）	-	-	-	施宣輝
15,000,000元（含）～30,000,000元（不含）	-	-	-	陳怡如
30,000,000元（含）～50,000,000元（不含）	-	-	-	-
50,000,000元（含）～100,000,000元（不含）	-	-	-	-
100,000,000元以上	-	-	-	-
總計	8人	8人	8人	8人

2. 最近年度（113 度）支付總經理及副總經理之酬金

單位：新台幣仟元

職稱	姓名	薪資（A）		退職退休金（B）		獎金及特支費等等（C）		員工酬勞金額（D）				A、B、C及D等四項總額及占稅後純益之比例（%）		領取來自子公司以外轉投資事業或母公司酬金
		本公司	財務報告內所有公司	本公司	財務報告內所有公司	本公司	財務報告內所有公司	本公司		財務報告內所有公司		本公司	財務報告內所有公司	
								現金金額	股票金額	現金金額	股票金額			
總經理	吳乙南	8,797	8,797	360	360	7,641	7,641	1,996	0	1,996	0	總額 18,794 比例 8.32%	總額 18,794 比例 8.32%	0
副總經理及資安長（註1）	顧寶裕													
副總經理	楊旭平													
副總經理	黃瓊瑩													

註 1.顧寶裕於 113 年 4 月 30 日辭任。

酬金級距表

給付本公司各個總經理及副總經理酬金級距	總經理及副總經理姓名	
	本公司	財務報告內所有公司
低於1,000,000元	顧寶裕	顧寶裕
1,000,000元（含）~2,000,000元（不含）	-	-
2,000,000元（含）~3,500,000元（不含）	楊旭平	楊旭平
3,500,000元（含）~5,000,000元（不含）	黃瓊瑩	黃瓊瑩
5,000,000元（含）~10,000,000元（不含）	吳乙南	吳乙南
10,000,000元（含）~15,000,000元（不含）	-	-
15,000,000元（含）~30,000,000元（不含）	-	-
30,000,000元（含）~50,000,000元（不含）	-	-
50,000,000元（含）~100,000,000元（不含）	-	-
100,000,000元以上	-	-
總計	4人	4人

本表所揭露酬金內容與所得稅法之所得概念不同，故本表目的係作為資訊揭露之用，不作課稅之用。

3. 分派員工酬勞之經理人姓名及分派情形

日期：113年12月31日；單位：新台幣仟元

	職稱	姓名	股票金額	現金金額	總計	總額占稅後純益之比例
經理人	總經理	吳乙南	0	2,096	2,096	0.93%
	副總經理	楊旭平				
	副總經理	黃瓊瑩				
	財務及會計主管	譚百良				
	稽核室經理	金珊如				

（二）分別比較說明本公司及合併報告所有公司於最近二年度支付本公司董事、總經理及副總經理酬金總額占個體或個別財務報告稅後純益比例之分析並說明給付酬金之政策、標準與組合、訂定酬金之程序及與經營績效及未來風險之關聯性

1. 最近二年度支付本公司董事酬金總額及占稅後純益比例之分析

單位：新台幣仟元

項目	112年度		113年度	
	本公司	合併報表	本公司	合併報表
董事酬金總額	3,200	3,200	3,690	3,690
董事酬金總額及占稅後純益比例	1.68%	1.68%	1.63%	1.63%

(1) 給付酬金之政策、標準與組合

本公司給付獨立董事酬勞之決策，乃根據本公司之公司章程規定，由薪酬委員會提出報告，經董事會決議通過後，依法提報股東常會報告。

(2) 訂定酬金之程序

本公司之獨立董事酬勞乃依公司章程規定，公司年度如有獲利，於預先保留彌補累積虧損之數額後，另得提撥不高於 0.8%為董事酬勞，且其分配辦法將由薪資報酬委員會提報董事會決定後，並於股東會報告之。

(3) 與經營績效及未來風險之關聯性

本公司之董事酬勞乃依公司章程規定，且非固定部份乃依照公司年度獲利情形支給，故其與公司經營績效相關。且薪酬委員會亦定期評估並檢討董事會之薪資報酬，將相關結果呈報董事會討論，以確認其與公司永續經營成果平衡。

2. 最近二年度支付本公司總經理及副總經理酬金總額占稅後純益比例分析

單位：新台幣仟元

項目	112年度		113年度	
	本公司	合併報表	本公司	合併報表
總經理及副總經理酬金總額	21,496	21,496	18,794	18,794
總經理及副總經理酬金總額占稅後純益比例	11.28%	11.28%	8.32%	8.32%

(1) 給付酬金之政策、標準與組合

本公司給付經理人之酬勞主要分為固定薪資及變動獎金；固定薪資為每年度與員工約定之月發放薪資，變動獎金則為達成目標績效表現之酬勞。固定薪資乃指公司依據同仁之工作職掌、業界整體環境及市場水準等因素，訂定與工作績效相關

之薪資報酬；變動獎金乃考量當年度績效與貢獻，由薪酬委員會提報經董事會核准後，依公司年度獎金發放公告辦理。

(2) 訂定酬金之程序

員工酬勞乃依據公司章程規定辦理。員工酬勞實際分派之數額由董事會議定並報告股東會，員工酬勞之發放總金額須符合董事會通過之年度預算。

(3) 經營績效及未來風險之關聯性

員工酬勞乃依據法規及當年度經營結果辦理，其發放標準、結構及制度亦將隨時視實際營運狀況及相關法規變動適時檢討調整之。本公司之薪酬委員會亦定期評估經理人之薪資報酬現況，並提供建議予董事會參考及討論，以確認整體報酬之合理性。

三、公司治理運作情形

（一）董事會運作情形

最近年度（113 年 01 月 01 日至 113 年 12 月 31 日）董事會開會 7 次（A），董事出列席情形如下

職稱	姓名	實際出席次數（B）	委託出席次數	實際出席率（B/A）	備註
董事長	宏碁股份有限公司 代表人：施宣輝	7	0	100%	
董事	宏碁股份有限公司 代表人：陳怡如	7	0	100%	
董事	宏碁股份有限公司 代表人：蔡傑智	7	0	100%	
獨立董事	童至祥	7	0	100%	
獨立董事	龍惠施	7	0	100%	
獨立董事	蔡東峻	7	0	100%	
獨立董事	李紀珠	7	0	100%	

其他應記載事項：

1. 董事會之運作如有下列情形之一者，應敘明董事會日期、期別、議案內容、所有獨立董事意見及公司對獨立董事意見之處理：

(1) 證券交易法第 14 條之 3 所列事項：本公司已依證券交易法規定設置審計委員會，故不適用證券交易法第 14 條之 3 規定，有關證券交易法第 14 條之 5 所列事項之說明，請參閱本年報審計委員會運作情形。

(2) 除前開事項外，其他經獨立董事反對或保留意見且有紀錄或書面聲明之董事會議決事項：無。

2. 董事對利害關係議案迴避之執行情形

董事會 日期及期別	議案內容	董事對利害關係議案迴避之執行情形
113.2.27 113年 第二次董事會	第一案 民國112年度董事酬勞案	本案涉獨立董事酬勞，故全體獨立董事因自身利害關係依公司法第206條及相關法令之規定迴避參與討論與表決，經主席徵詢獨立董事以外之其他出席董事一致無異議通過。

3. 當年度及最近年度加強董事會職能之目標與執行情形評估

本公司董事會藉各功能委員會分工合作，如薪酬委員會及審計委員會等，以協助董事會履行其監督職責，積極強化董事會職能落實公司治理。

（二）董事會評鑑執行情形

本公司 113 年度董事會評鑑結果已於 114 年 2 月 24 日董事會會議中進行報告，說明董事會評鑑的執行情形、評鑑結果分析及相關改進措施，以提升董事會運作效能並確保公司治理品質。

評估週期	每年執行一次		
評估期間	自113年1月1日至113年12月31日之績效進行評估		
評估範圍	董事會績效評估、個別董事成員績效評估、功能性委員會績效評估		
評估方式	董事會內部自評、董事成員自評、同儕評估		
評估內容	董事會自我評鑑 1.對公司經營之參與程度 2.提升董事會決策品質 3.董事會組成與結構 4.董事之選任與持續進修 5.內部控制	董事會成員自我評鑑 1.公司目標與任務之掌握 2.董事職責認知 3.對公司營運之參與程度 4.內部關係經營與溝通 5.董事之專業及持續進修 6.內部控制	功能性委員會自我評鑑 1.對公司營運之參與程度 2.功能性委員會職責認知 3.提升功能性委員會決策品質 4.功能性委員會組成及成員選任 5.內部控制

（三）審計委員會運作情形

113 年 01 月 01 日至 113 年 12 月 31 日審計委員會開會次數合計 6 次，獨立董事出列席情形如下：

職稱	姓名	實際 出席次數	委託 出席次數	實際出席率	備註
召集人	龍惠施	6	0	100%	
獨立董事	童至祥	6	0	100%	
獨立董事	蔡東峻	6	0	100%	
獨立董事	李紀珠	6	0	100%	

審計委員會成員專業資格與經驗	
成員	**專業資格與經驗**
龍惠施	龍惠施女士曾任宏碁全球財務總部財務資訊總處總處長，擁有豐富的財務相關經驗。現任為祥龍投資及曜揚科技（股）公司董事長。
童至祥	童至祥女士曾擔任台灣IBM總經理及特力集團執行長，現同時兼任展藤(限)公司董事長及矽力杰（股）公司董事。
蔡東峻	蔡東峻先生曾擔任國立成功大學交通管理科學學系主任、國立成功大學國際企業研究所所長及國立成功大學EMBA/AMBA執行長，在學術界擁有豐富的資歷。現任財團法人宏碁基金會董事及財團法人莊漢開教授文教基金會董事。
李紀珠	李紀珠女士現任中華產經發展協會理事長、保利馬公司監察人、台灣玉山科技協會榮譽理事長、國際金融論壇（IFF）理事、東亞經濟協會副理事長及國立政治大學兼任教授。曾任臺灣銀行暨臺灣金控董事長、中華民國行政院金融監督管理委員會副主委、立法委員、政治大學經濟系所專任教授、中華郵政公司董事長、新光金控暨新光人壽副董事長等職。於金融及經濟領域經驗十分豐富。

其他應記載事項：

1. 審計委員會年度之審議事項主要重點包括：

(1) 審閱財務報表

(2) 評估內部控制制度之有效性

(3) 委任簽證會計師

(4) 修訂內部規章

(5) 通過上櫃相關之議案

(6) 審查年度營運計畫、預算及稽核計畫等

2. 審計委員會之運作如有下列情形之一者，應敘明董事會日期、期別、議案內容、審計委員會決議結果以及公司對審計委員會意見之處理：

(1) 證券交易法第 14 條之 5 所列事項。

(2) 除前開事項外，其他未經審計委員會通過，而經全體董事三分之二以上同意之議決事項。

審計委員會日期及期別	議案內容及後續處理事項（如有）	證券交易法第14條之5所列事項	其他未經審計委員會通過而經全體董事三分之二以上同意之決議事項
113.01.23 113年第一次審計委員會	擬購買南港利百代大樓建物及土地	V	無
	擬向銀行辦理購買南港利百代大樓建物及土地之不動產貸款案	V	無
	審計委員會決議結果：審計委員會全體成員同意通過		
	公司對審計委員會意見之處理：董事會全體出席董事一致同意通過審計委員會提交董事會之議案與意見		
113.02.27 113年第二次審計委員會	提請承認本公司民國112年度財務報表及營業報告書案	V	無
	提請討論本公司民國112年度盈餘分派案	V	無
	擬通過本公司民國112年度內部控制聲明書案	V	無
	委任本公司民國113年度財務報表查核簽證會計師及評估會計師獨立性案	V	無
	訂定註銷本公司收回民國110年第一次限制員工權利新股股份之減資基準日	V	無
	審計委員會決議結果：審計委員會全體成員同意通過		
	公司對審計委員會意見之處理：董事會全體出席董事一致同意通過審計委員會提交董事會之議案與意見		
113.04.30 113年第三次審計委員會	提請同意民國113年第一季經會計師核閱之財務季報告	V	無
	訂定註銷本公司收回民國110年第一次限制員工權利新股股份之減資基準日	V	無
	審計委員會決議結果：審計委員會全體成員同意通過		
	公司對審計委員會意見之處理：董事會全體出席董事一致同意通過審計委員會提交董事會之議案與意見		
113.07.30 113年第四次審計委員會	提請同意民國113年第二季經會計師核閱之財務季報告	V	無
	擬辦理民國113年度第一次現金增資發行新股案	V	無
	本公司內部規章修訂案	V	無
	審計委員會決議結果：審計委員會全體成員同意通過		
	公司對審計委員會意見之處理：董事會全體出席董事一致同意通過審計委員會提交董事會之議案與意見		
113.09.04 113年第五次審計委員會	擬增資子公司宏碁雲架構服務股份有限公司	V	無
	審計委員會決議結果：審計委員會全體成員同意通過		
	公司對審計委員會意見之處理：董事會全體出席董事一致同意通過審計委員會提交董事會之議案與意見		
113.10.29 113年第六次審計委員會	提請同意民國113年第三季經會計師核閱之財務季報告	V	無
	提請同意本公司民國114年度營運計畫暨預算案	V	無
	提請同意本公司民國114年度稽核計畫	V	無
	修訂本公司預先核准非確信服務政策及服務清單案	V	無
	本公司內部規章修訂案	V	無
	審計委員會決議結果：審計委員會全體成員同意通過		
	公司對審計委員會意見之處理：董事會全體出席董事一致同意通過審計委員會提交董事會之議案與意見		

3. 獨立董事對利害關係議案迴避之執行情形：無此情形。

4. 獨立董事與內部稽核主管及會計師之溝通情形

(1) 本公司內部稽核主管除每月向獨立董事彙報內部稽核執行情形外，並定期於每季的審計委員會中單獨與獨立董事進行內部稽核報告，與委員溝通稽核之結果及內控缺失的改善情形。如有特殊狀況時，內部稽核主管將即時向審計委員會委員報告，以確保資訊透明並及時採取必要的應對措施。

(2) 本公司審計委員會與內部稽核主管溝通狀況良好，主要溝通情形摘要如下：

日期	溝通重點	建議及結果
113.02.27 113年第一次 審計委員會	112年第四季公司內部稽核單位之業務暨112年度第三季缺失改善追蹤	經獨立董事詢問報告相關內容與相關細節並由內部稽核主管答覆與說明後，獨立董事並無其他意見
	112年度「內部控制制度聲明書」	經獨立董事詢問報告相關內容與相關細節並由內部稽核主管答覆與說明後，獨立董事並無其他意見
113.04.30 113年第二次 審計委員會	113年第一季公司內部稽核單位之業務暨112年度第四季缺失改善追蹤	經獨立董事詢問報告相關內容與相關細節並由內部稽核主管答覆與說明後，獨立董事並無其他意見
113.07.30 113年第三次 審計委員會	113年第二季公司內部稽核單位之業務暨113年度第一季缺失改善追蹤	經獨立董事詢問報告相關內容與相關細節並由內部稽核主管答覆與說明後，獨立董事並無其他意見
113.10.29 113年第四次 審計委員會	113年第三季公司內部稽核單位之業務暨113年度第二季缺失改善追蹤	經獨立董事詢問報告相關內容與相關細節並由內部稽核主管答覆與說明後，獨立董事並無其他意見
	本公司民國114年度稽核計畫	經獨立董事詢問報告相關內容與相關細節並由內部稽核主管答覆與說明後，獨立董事並無其他意見

(3) 本公司簽證會計師定期於每年第一季及第三季的審計委員會中報告當年度之財務報表查核（或核閱）相關事項，以及其他相關法令要求之溝通事項，若有特殊狀況時，亦會即時向審計委員會委員報告。報告後亦會單獨與獨立董事進行溝通。

(4) 本公司審計委員會與簽證會計師溝通狀況良好，主要溝通情形摘要如下：

日期	溝通重點	建議及結果
113.02.27 113年第一次 審計委員會	獨立性/查核人員查核財務報告之責任/查核範圍、方式及結論/查核發現/相關法令更新報告/事務所品質管理制度之溝通	經獨立董事詢問報告相關內容與相關細節並由簽證會計師答覆與說明後，獨立董事並無其他意見或建議
113.04.30 113年第二次 審計委員會	核閱人員核閱期中財務報告之責任及獨立性/核閱範圍、方式及結論/核閱發現/年度查核規劃/相關法令更新報告	經獨立董事詢問報告相關內容與相關細節並由簽證會計師答覆與說明後，獨立董事並無其他意見或建議

日期	溝通重點	建議及結果
113.10.29 113年第六次 審計委員會	核閱人員核閱期中財務報告之責任及獨立性/核閱範圍、方式及結論/核閱發現/年度查核規劃/相關法令更新報告	經獨立董事詢問報告相關內容與相關細節並由簽證會計師答覆與說明後，獨立董事並無其他意見或建議

（四）公司治理運作情形及其與上市上櫃公司治理實務守則差異情形及原因

評估項目	運作情形			與上市上櫃公司治理實務守則差異情形及原因
	是	否	摘要說明	
一、公司是否依據「上市上櫃公司治理實務守則」訂定並揭露公司治理實務守則？	V		本公司已於民國108年3月1日經董事會通過「公司治理實務守則」。	無重大差異
二、公司股權結構及股東權益 (一)公司是否訂定內部作業程序處理股東建議、疑義、糾紛及訴訟事宜，並依程序實施？	V		(一)為確保股東權益，本公司由發言人及代理發言人專責妥善處理股東建議。	無重大差異
(二)公司是否掌握實際控制公司之主要股東及主要股東之最終控制者名單？	V		(二)本公司確實掌握實際控制公司之主要股東及主要股東之最終控制者名單。	無重大差異
(三)公司是否建立、執行與關係企業間之風險控管及防火牆機制？	V		(三)本公司根據如子公司管理辦法、背書保證作業程序、資金貸與他人作業程度及取得或處分資產處理程序及關係人交易管理等內部相關辦法建立適當風險控管機制及防火牆。	無重大差異
(四)公司是否訂定內部規範，禁止公司內部人利用市場上未公開資訊買賣有價證券？	V		(四)本公司訂有防範內線交易管理辦法，以禁止公司內部人利用市場上未公開資訊買賣有價證券。	無重大差異
三、董事會之組成及職責 (一)董事會是否擬訂多元化政策、具體管理目標及落實執行？	V		(一)本公司目前董事七席，包含四席獨立董事及四席女性董事，已依據多元化政策辦理並擬定具體管理目標，以其專業能力，就公司有關內控制度執行及相關議案，提供董事會良好之建議。	無重大差異
(二)公司除依法設置薪資報酬委員會及審計委員會，是否自願設置其他各類功能性委員會？		V	(二)本公司目前已設置薪資報酬委員會及審計委員會，未來將視法令及實際需求情況設置其他功能性委員會。	未來將視法令及實際需求情況設置
(三)公司是否訂定董事會績效評估辦法及其評估方式，每年並定期進行績效評估，且將績效評估之結果提報董事會，並運用於個別董事薪資報酬及提名續任之參考？	V		(三)本公司已於民國108年11月4日經董事會通過「董事會自我評鑑或同儕評鑑辦法」及其評估方式。每年均定期進行董事績效評估，並於完成評估後向董事會陳報評估結果，評估結果將運用於個別董事薪資報酬及提名續任之參考。114年1月份辦理113年度董事會績效評估，並於114年2月24日董事會向董事陳報評估結果。	無重大差異

評估項目	運作情形			與上市上櫃公司治理實務守則差異情形及原因
	是	否	摘要說明	
(四)公司是否定期評估簽證會計師獨立性？	V		(四)評核會計師之資格及獨立性為本公司審計委員會的主要職責之一。財務單位每年定期評估簽證會計師之獨立性，並提報審計委員會及董事會通過。114年度會計師獨立性及適任性評估作業，經參酌安侯建議聯合會計師事務所民國112年審計品質指標Audit Quality Indicators(AQI)資訊，已由財務單位評估完成，並於114年2月24日呈報審計委員會及董事會。 審計委員會係依據會計師所出具之超然獨立聲明書及審計品質指標Audit Quality Indicators (AQI)相關資訊，來進行綜合評估，評估之重要項目如下： 1. 公司管理當局是否尊重簽證會計師所提出之客觀且具挑戰性的查核流程。 2. 簽證會計師所提供之非審計服務是否可能損及其查核之獨立性。 3. 簽證事務所是否有訂定獨立性規範，要求事務所、事務所人員及其他受獨立性規範之人員，依會計師職業道德規範維持獨立性；並禁止任何人員從事內線交易、誤用內部訊息或任何可能造成在證券或資本市場上的誤導行為。 4. 主辦會計師及會簽會計師等承辦期間已達規定之期限者，是否均定期輪調。 5. 審計品質指標Audit Quality Indicators (AQI)。主要係從專業性/品質控管/獨立性/監督/創新能力等五大構面13項指標予以衡量。	無重大差異
四、上市上櫃公司是否配置適任及適當人數之公司治理人員，並指定公司治理主管，負責公司治理相關事務（包括但不限於提供董事、監察人執行業務所需資料、協助董事、監察人遵循法令、依法辦理董事會及股東會之會議相關事宜、辦理公司登記及變更登記、製作董事會及股東會議事錄等）？	V		本公司於112年2月24日董事會通過任命財務長擔任公司治理最高主管，並率領財務、法務、股務及人事等相關功能單位人員共同組成公司治理專責團隊，負責處理事務摘要如下： 1. 研擬規劃適當公司制度，以促進公司的透明度、法令的遵循及內稽內控的落實。 2. 辦理股東會議事務，包括於每年依規定製作並於期限前申報股東會開會通知書、議事手冊及議事錄等。 3. 依法辦理董事會之會議相關事宜及製作董事會議事錄。	無重大差異

評估項目	運作情形			與上市上櫃公司治理實務守則差異情形及原因
	是	否	摘要說明	
			4. 協助董事就任及持續進修。 5. 提供董事執行業務所需之資料。 6. 協助董事遵循法令。 7. 其他依公司章程或契約所訂定之事項等。	
五、公司是否建立與利害關係人（包括但不限於股東、員工、客戶及供應商等）溝通管道，及於公司網站設置利害關係人專區，並妥適回應利害關係人所關切之重要企業社會責任議題？	V		本公司建立發言人制度，定期將重要財務業務及其他相關資訊，公告於公開資訊觀測站，並於公司網站設置利害關係人專區，作為對外與利害關係人之管道，使其利害關係人快速瞭解公司營運狀況，以維持其權益。	無重大差異
六、公司是否委任專業股務代辦機構辦理股東會事務？	V		本公司委託台新綜合證券股務代理部負責處理股東會事務及股務作業。	無重大差異
七、資訊公開 (一)公司是否架設網站，揭露財務業務及公司治理資訊？	V		(一)本公司網站已適度揭露公司財務、業務及公司治理資訊等相關資訊。並於股東會及其他法人投資人說明會時向投資人說明本公司公司治理執行之情形。	無重大差異
(二)公司是否採行其他資訊揭露之方式（如架設英文網站、指定專人負責公司資訊之蒐集及揭露、落實發言人制度、法人說明會過程放置公司網站等）？	V		(二)本公司行銷部門負責蒐集及揭露相關資訊，並已建立發言人及代理發言人制度，亦依規定揭露相關資訊於「公開資訊觀測站」。	無重大差異
(三)公司是否於會計年度終了後兩個月內公告並申報年度財務報告，及於規定期限前提早公告並申報第一、二、三季財務報告與各月份營運情形？	V		(三)本公司113年度財務報告已於114年2月24日完成申報及公告作業。第一、二、三季財務報告與各月份營運情形，均依照主管機關相關規定期限前，完成申報及公告作業。	無重大差異
八、公司是否有其他有助於瞭解公司治理運作情形之重要資訊（包括但不限於員工權益、僱員關懷、投資者關係、供應商關係、利害關係人之權利、董事及監察人進修之情形、風險管理政策及風險衡量標準之執行情形、客戶政策之執行情形、公司為董事及監察人購買責任保險之情形等）？	V		1. 本公司董事除按主管機關規定安排進修外，另參與相關由公司主動安排之進修課程。 2. 本公司於董事會議事規則中明確訂定董事對於其利害相關之議案討論及表決應予以迴避。 3. 本公司已為董事及重要職員購買責任保險。 4. 本公司業已增加獨立董事為四席，且有四名女性董事。 5. 為強化公司治理，本公司已修訂「董事會議事規則」部分條文，涉及公司經營之重大性事項，董事為決策前應有充分之資訊及時間評估，不得以緊急情勢或正當理由以臨時動議提出。 6. 本公司已增訂「內部重大資訊處理作業程序」，以強化重大訊息資訊揭露之品質。	無重大差異

評估項目	運作情形			與上市上櫃公司治理實務守則差異情形及原因
	是	否	摘要說明	
			7. 本公司已修訂「內部控制制度」，以提升本公司對資訊安全之重視及配置適當人力資源及設備，進行資訊安全制度之規劃、監控及執行資訊安全管理作業。 8. 本公司已修訂「防範內線交易管理辦法」，禁止公司董事及內部人於財務業績發布前交易其股票，以強化公司治理及維護股東權益，落實股東平等對待。	

九、就臺灣證券交易所股份有限公司治理中心最近年度發布之公司治理評鑑結果說明已改善情形，及就尚未改善者提出優先加強事項與措施：

1. 本公司已改善項目如下：導入ISO50001並取得第三方驗證。
2. 尚未改善者提出優先加強事項與措施：a.編製113年度永續報告書，並於公告前提報董事會。b.永續報告書編製參考SASB準則揭露相關ESG資訊。

（五）公司如有設置薪資報酬委員會者，應揭露其組成、職責及運作情形

1. 薪資報酬委員會成員資料

身份別	條件 / 姓名	專業資格與經驗	符合獨立性情形	兼任其他公開發行公司薪資報酬委員會成員家數	備註
獨立董事	龍惠施	1.龍惠施女士曾任宏碁全球財務總部財務資訊總處總處長，擁有豐富的財務相關經驗。現任為祥龍投資及曜揚科技（股）公司董事長。 2.專長於企業財務及管理等領域，且未有公司法第30條各款情事。	1.本人及其配偶或二親等以內親屬未有擔任集團公司董事、監察人或受僱人之情事。 2.本人及其配偶或二親等以內親屬均未持有本公司股份。 3.本人及其配偶或二親等以內親屬均未有擔任與本公司有特定關係公司之董事、監察人或受僱人，亦無提供集團公司商務、法務、財務及會計等服務之情事。	3	-
獨立董事	童至祥	1.童至祥女士曾擔任台灣IBM總經理及特力集團執行長，現同時兼任展藤(股)公司董事長及及矽力杰(股)公司董事 2.專長於企業經營管理、國際貿易與行銷等領域，且未有公司法第30條各款情事。	1.本人及其配偶或二親等以內親屬未有擔任集團公司董事、監察人或受僱人之情事。 2.本人及其配偶或二親等以內親屬均未持有本公司股份。 3.本人及其配偶或二親等以內親屬均未有擔任與本公司有特定關係公司之董事、監察人或受僱人，亦無提供集團公司	0	-

身份別	條件 姓名	專業資格與經驗	符合獨立性情形	兼任其他公開發行公司薪資報酬委員會成員家數	備註
			商務、法務、財務及會計等服務之情事。		
獨立董事	蔡東峻	1.蔡東峻先生曾擔任國立成功大學交通管理科學學系主任、國立成功大學國際企業研究所所長及國立成功大學EMBA/AMBA執行長。現任財團法人宏碁基金會董事及財團法人莊漢開教授文教基金會董事。 2.專長於企業管理及行銷管理等領域，且未有公司法第30條各款情事。	1.本人及其配偶或二親等以內親屬未有擔任集團公司董事、監察人或受僱人之情事。 2.本人及其配偶或二親等以內親屬均未持有本公司股份。 3.本人及其配偶或二親等以內親屬均未有擔任與本公司有特定關係公司之董事、監察人或受僱人，亦無提供集團公司商務、法務、財務及會計等服務之情事。	0	-
獨立董事	李紀珠	1.李紀珠女士現任中華產經發展協會理事長、國立政治大學兼任教授及保利馬公司監察人等。曾任臺灣銀行暨臺灣金控董事長、中華民國行政院金融監督管理委員會副主委、中華民國立法委員、國立政治大學經濟系所專任教授、中華郵政公司董事長、新光金控暨新光人壽副董事長、新光銀行副董事長等職。於金融及經濟領域經驗十分豐富。 2.李紀珠女士為台灣大學經濟學博士，並為美國哈佛及史丹佛大學經濟系訪問學者 3.專長於財務金融及企業管理等領域，且未有公司法第30條各款情事。	1.本人及其配偶或二親等以內親屬未有擔任集團公司董事、監察人或受僱人之情事。 2.本人及其配偶或二親等以內親屬均未持有本公司股份。 3.本人及其配偶或二親等以內親屬均未有擔任與本公司有特定關係公司之董事、監察人或受僱人，亦無提供集團公司商務、法務、財務及會計等服務之情事。	0	-

2. 薪資報酬委員會運作情形資訊

(1) 本公司之薪資報酬委員會委員計 4 人。

(2) 本屆委員任期：第三屆薪資報酬委員任期自 111 年 5 月 27 日起至 114 年 5 月 26 日止，本屆委員於最近年度（113 年）薪資報酬委員會共開會 4 次（A），委員資格及出席情形如下：

職稱	姓名	實際出席次數（B）	委託出席次數	實際出席率（%）（B/A）	備註
召集人	童至祥	4	0	100	
委員	龍惠施	4	0	100	
委員	蔡東峻	4	0	100	
委員	李紀珠	4	0	100	

(3) 其他應記載事項

A. 董事會如不採納或修正薪資報酬委員會之建議，應敘明董事會日期、期別、議案內容、董事會決議結果以及公司對薪資報酬委員會意見之處理（如董事會通過之薪資報酬優於薪資報酬委員會之建議，應敘明其差異情形及原因）：無此情形。

B. 薪資報酬委員會之議決事項，如成員有反對或保留意見且有紀錄或書面聲明者，應敘明薪資報酬委員會日期、期別、議案內容、所有成員意見及對成員意見之處理：無此情形。

C. 薪資報酬委員會之討論事項及決議結果

薪資報酬委員會日期及期別	議案內容	薪資報酬委員會決議結果	公司對薪資報酬委員會意見之處理
113.02.27 113年 第一次薪資報酬委員會	民國112年度董事酬勞案	本案因涉及薪酬委員會成員之薪資報酬事項，建議不予討論直接提交董事會討論（本案逕送董事會討論）	獨立董事迴避參與討論及表決，經董事會其餘出席董事一致討論通過本議案
	民國112年度員工酬勞案	薪資報酬委員會全體成員同意通過	董事會全體出席董事一致同意通過薪資報酬委員會提交董事會之議案與意見
	經理人異動案	薪資報酬委員會全體成員同意通過	董事會全體出席董事一致同意通過薪資報酬委員會提交董事會之議案與意見
	經理人伙食津貼調整討論案	薪資報酬委員會全體成員同意通過	董事會全體出席董事一致同意通過薪資報酬委員會提交董事會之議案與意見
	民國112年經理人目標獎金討論案	薪資報酬委員會全體成員同意通過	董事會全體出席董事一致同意通過薪資報酬委員會提交董事會之議案與意見
	民國113年經理人調薪討論案	薪資報酬委員會全體成員同意通過	董事會全體出席董事一致同意通過薪資報酬委員會提交董事會之議案與意見

薪資報酬委員會 日期及期別	議案內容	薪資報酬委員會決議結果	公司對薪資報酬委員會 意見之處理
113.07.30 113年 第二次薪資報酬 委員會	民國112年經理人員工酬勞分配建議案	薪資報酬委員會全體成員同意通過	董事會全體出席董事一致同意通過薪資報酬委員會提交董事會之議案與意見
113.10.24 113年 第三次薪資報酬 委員會	民國113年現金增資內部經理人認購股數建議案	薪資報酬委員會全體成員同意通過	董事會全體出席董事一致同意通過薪資報酬委員會提交董事會之議案與意見
113.10.29 113年 第四次薪資報酬 委員會	民國114年經理人目標獎金預算暨指標建議案	薪資報酬委員會全體成員同意通過	董事會全體出席董事一致同意通過薪資報酬委員會提交董事會之議案與意見
	民國114年調薪規劃及預算案	薪資報酬委員會全體成員同意通過	董事會全體出席董事一致同意通過薪資報酬委員會提交董事會之議案與意見

D. 薪資報酬委員會職責

薪酬委員會的職責包括訂定並定期檢討董事及經理人績效評估與薪資報酬之政策、制度、標準與結構，並定期評估訂定前述人員之薪資報酬。

薪酬委員會履行前項職權時，應依下列原則為之：

- 董事及經理人之績效評估及薪資報酬應參考同業通常水準支給情形，並考量與個人表現、公司經營績效及未來風險之關聯合理性。
- 不應引導董事及經理人為追求薪資報酬而從事逾越公司風險胃納之行為。
- 針對董事及高階經理人短期績效發放紅利之比例及部分變動薪資報酬支付時間應考量行業特性及公司業務性質予以決定。
- 符合相關法令之規定。

3. 提名委員會成員資料及運作情形資訊：本公司未設立提名委員會，故不適用。

（六）推動永續發展執行情形與上市上櫃公司永續發展實務守則差異情形及原因

評估項目	運作情形			與上市上櫃公司永續發展實務守則差異情形及原因
	是	否	摘要說明	
一、公司是否建立推動永續發展之治理架構，且設置推動永續發展專(兼)職單位，並由董事會授權高階管理階層處理，及董事會督導情形？	V		本公司已成立ESG工作小組，由總經理擔任召集人，公司治理主管擔任負責人，負責主導推行ESG推行ESG各項工作；預計於114年第二季董事會向董事報告「113年溫室氣體盤查與查證執行狀況」。	無重大差異
二、公司是否依重大性原則，進行與公司營運相關之環境、社會及公司治理議題之風險評估，並訂定相關風險管理政策或策略？	V		本公司定期由總經理召集經理人召開「經營策略會議」，進行與公司營運相關之環境、社會及公司治理議題之風險評估，若判斷有風險事項發生時，則會成立「專案小組」擬定相關因應措施。 本公司就環境、社會、公司治理三大面向進行公司潛在風險及新興風險的辨識、評估及討論。詳細的評估方法及相關風險管理策略,請參閱今年度永續報告書。	無重大差異
三、環境議題 (一)公司是否依其產業特性建立合適之環境管理制度？	V		(一)本公司已取得ISO14001環境管理系統標章認證(有效期限至115年10月)，以確保符合環境管理法規要求。 本公司係屬資訊服務業，溫室氣體排放源均屬間接排放，主要來自於辦公室空調與照明所需之電力、員工通勤及垃圾委外處理等。為落實環境保護之承諾，本公司遵守環保法規，同時致力於節約能源、資源回收利用、綠色採購等，對環境有益之政策及措施並承諾污染預防與持續改善。	無重大差異
(二)公司是否致力於提升能源使用效率及使用對環境負荷衝擊低之再生物料？	V		(二)本公司鼓勵員工落實資源分類，加強資源回收，並針對辦公室空調及照明使用節能設計，以達到節能的目的。	無重大差異
(三)公司是否評估氣候變遷對企業現在及未來的潛在風險與機會，並採取氣候相關議題之因應措施？	V		(三)本公司依據氣候相關財務揭露指引辨識關鍵氣候風險，從治理、策略、風險管理、指標與目標四大面向全面進行氣候風險管理，鑑別出氣候變遷對企業經營之風險與機會、分析財務面與非財務面影響，制定永續策略及環境目標並規畫因應措施。	無重大差異
(四)公司是否統計過去兩年溫室氣體排放量、用水量及廢棄物總重量，並制定節能減碳、溫室氣體減量、減少用水或其他廢棄物管理之政策？	V		(四)本公司致力於節約能源、回收廢棄物、遵守環保法規，並承諾污染預防與持續改善，相關政策如上題。 近兩年度溫室氣體年排放量、用水量及廢棄物總重量之情形： 本公司溫室氣體排放量2023年已完成範疇一&二盤查作業，並經台灣檢驗科技公司（SGS）查核驗證。	無重大差異

評估項目	運作情形			與上市上櫃公司永續發展實務守則差異情形及原因
	是	否	摘要說明	

項目	2022	2023
用水量（公噸）	6,866	5,587
廢棄物總重量(公噸）	14.33	28.66
溫室氣體排放量 範疇一（公噸）	235.61	218.24
溫室氣體排放量 範疇二（公噸）	1,649.83	710.39

*2022年初合併子公司宏碁雲架構股份有限公司所致

**本公司無有害廢棄物

***盤查範圍包含安碁資訊及其合併財務報表子公司

本公司持續統計溫室氣體排放量、用水量及廢棄物總重量，2024年之資訊截至年報刊印日止仍在進行查證中，最新資訊預計於8月底於本公司官網站永續報告書之ESG資訊摘要。

目標：

溫室氣體管理：本公司為宏碁集團的一分子，響應集團政策，並呼應1.5℃減碳路徑情境下的科學基礎減量目標（Science Based Targets, SBT），承諾於2030年組織營運（範疇1+2）達成相較於2022年減碳35%。

宏碁集團推動減碳關鍵策略，推出3大面向9項策略，致力從企業永續營運、產品與服務及價值鏈，並透過減少能源消耗、使用再生能源、負碳抵消、低碳產品與服務、投入智慧、循環與綠能應用、減碳目標與承諾、全面性地減少碳足跡。

水資源管理：以2022年，總用水量降低1%。

廢棄物管理：以2022年為基準年，設定2025年較基準年減少1%之短期目標、2030年較基準年減少10%之中長期目標。

達成情形：

因各項指標以2022年度為基準年，檢視2023年度其達成狀況。

2023年度範疇一及範疇二溫室氣體排放量以市場基礎計算年減50.75%，已超越原設定的目標。

本公司節能減碳及其他減少環境影響之措施說明如下：

1. 2023年再生電力用電量達到182.2萬度（REC），佔總用電量55.94%。
2. 2024年已自建太陽能發電系統約390kW裝置容量。

評估項目	運作情形			與上市上櫃公司永續發展實務守則差異情形及原因
	是	否	摘要說明	
			3. 空調：主機依季節設定適當冰水出水溫度，並設定室內機溫度，使得室內溫度維持26-28度之間，同時搭配自動控制方式定時開關主機及室內機，以達到降低空調用電之目的。 4. 照明：採用節能燈具（耗電量為為一般日光燈的二分之一）降低照明用電，搭配電燈開關分區域設置，使用時開啟該區域燈具，辦公室節電量共計15,967度。 5. 公司選址時鄰近捷運站，便於同仁上、下班及洽公時搭乘捷運，減少使用非公眾交通工具之頻率，同時達到減少溫室氣體排放之目的。 6. 提供視訊會議之軟體，鼓勵同仁以視訊方式與客戶或廠商招開會議，提升效率並減少洽公及差旅之發生，進而降低交通工具使用，達到減少溫室氣體排放之目的。 7. 選用環保認證紙張，減少對原始森林砍伐之危害，間接減緩溫室效應發生。 8. 採用環保認證洗潔精，減少對環境及水資源之危害。 9. 採購設備時優先選擇具有節能標章之設備（產品），使用設備時同時達到節能目的。 10. 使用烘手機取代擦手紙，減少一次性紙張使用。 11. 資源回收利用 (1) 可回收廢棄物：分類置於回收桶，由清潔人員細項分類委由回收廠商清運，達到再利用之目的，同時減少垃圾量降低對環境危害。 (2) 廢棄紙張：統一集中存放後，定期委由廢紙回收商回收後，再混入造紙紙漿中，再生成紙箱重複利用，減少原生紙漿使用。	
四、社會議題 (一)公司是否依照相關法規及國際人權公約，制定相關之管理政策與程序？	V		(一)本公司已訂定人權政策，人權保障範圍包括員工、供應商、客戶與合作夥伴等，此政策認同並依循聯合國世界人權宣言，聯合國全球盟約、國際勞動組織工作基本原則與權利宣言，與當地法令規範，透過保護、尊重和補救等原則，落實人權保障。	無重大差異
(二)公司是否訂定及實施合理員工福利措施（包括薪酬、休假及其他福利等），並將經營績效或成果適當反映於員工薪酬？	V		(二)本公司已訂定及實施薪酬、績效考核、績效獎金、調薪政策、休假制度及員工福利等;並將經營績效或成果均反映於員工績效獎金及調薪。	無重大差異

評估項目	運作情形			與上市上櫃公司永續發展實務守則差異情形及原因
	是	否	摘要說明	
(三)公司是否提供員工安全與健康之工作環境，並對員工定期實施安全與健康教育？	V		(三)本公司已取得ISO45001職業安全管理系統認證（有效期限至115年10月）；針對同仁工作環境與人身安全部份，透過管理制度的推行，加強公司環境維護與同仁作業之安全管理，每年定期辦理作業環境檢測、年度員工健康檢查、定期每年舉辦安全衛生教育課程及測驗及其他相關安全衛生教育訓練，提升同仁危害意識，降低危害發生。每年至少一次進行消防測試及演練,且配備有滅火器、自動灑水系統與緊急出口指示等。 ● 113年度無火災相關事故發生 ● 113年12月5日舉辦大樓避難逃生演練 ● 113年6月26日舉型一般勞工安全衛生教育訓練並進行測驗,共計602人次。	無重大差異
(四)公司是否為員工建立有效之職涯能力發展培訓計畫？	V		(四)本公司安排員工參加內外之職能訓練課程，透過職能設計及培訓發展，兼顧通才與專才之發展，使每位同仁得依其發展意向，規劃個人職涯路徑。	無重大差異
(五)針對產品與服務之顧客健康與安全、客戶隱私、行銷及標示等議題，公司是否遵循相關法規及國際準則，並制定相關保護消費者或客戶權益政策及申訴程序？	V		(五)本公司已通過ISO27701「個資管理認證」(有效期限至114年5月)對客戶資料保護，有完善管理制度，並與客戶間合作關係長久及穩定，且保有良好的溝通管道，針對客戶的問題/疑問/客訴皆有專責部門及人員，能提供有效與迅速的回覆處理。	無重大差異
(六)公司是否訂定供應商管理政策，要求供應商在環保、職業安全衛生或勞動人權等議題遵循相關規範，及其實施情形？	V		(六)本公司訂有供應商評鑑制度，並依據該制度執行相關作業。在採購或簽約前，評估合作供應商於合作期間的企業社會責任（CSR）紀錄，以確保其符合本公司之永續經營理念。針對主要供應商，亦要求填寫「供應商ESG自評調查表」，評估面向涵蓋環境（E）、社會（S）與公司治理（G）三大構面。於113年度，共有11家主要供應商完成該自評作業，均符合本公司所訂定之評估標準。	無重大差異
五、公司是否參考國際通用之報告書編製準則或指引，編製永續報告書等揭露公司非財務資訊之報告書？前揭報告書是否取得第三方驗證單位之確信或保證意見？	V		本公司預計於114年8月公佈永續報告書，並將揭露於本公司網站。	無重大差異

六、公司如依據「上市上櫃公司永續發展實務守則」定有本身之永續發展守則者，請敘明其運作與所定守則之差異情形：

本公司已依據「上市上櫃公司永續發展實務守則」及考量公司實務運作情形，制定「企業社會責任實務守則」，且依循相關法規確實「履行企業社會責任」。

七、其他有助於瞭解推動永續發展執行情形之重要資訊：

安碁資訊一直致力於資安技術領域之深耕，累積豐富的資安事件處理經驗，為善盡企業社會責任，特別推出『資安講堂』，將資安技術轉化為資安防護知識推廣至國內企業；113年針對上市櫃公司，舉辦四場線上資安教育課程，廣受參與者好評。

(七) 符合一定條件之公司應揭露氣候相關資訊

1. 氣候相關資訊執行情形

項目	執行情形
1.敘明董事會與管理階層對於氣候相關風險與機會之監督及治理。	本公司已成立 ESG 工作小組，由總經理擔任召集人，公司治理主管擔任負責人，負責主導推行 ESG 各項工作；113 年度每季董事會均向董事報告「溫室氣體盤查與查證時程規劃」。
2.敘明所辨識之氣候風險與機會如何影響企業之業務、策略及財務 (短期、中期、長期)。	短期影響： • 業務影響 : 突發性氣候事件 (如颶風、洪水、乾旱) 可能導致交通中斷，無法至客戶端執行專案，進而影響專案進度。 • 策略影響 : 技術單位可能需要立即調整專案執行模式，包括遠端執行、視訊會議等應急準備和風險管理策略，以應對突發氣候事件。 • 財務影響 : 突發性氣候事件可能導致額外成本，包括建立遠端執行系統、相關網路安全機制等設備購置。 中期影響： • 業務影響 : 氣候模式變化，可能導致硬體設備供應鏈穩定性受到影響，服務的需求也可能發生變化。 • 策略影響 : 公司需要重新評估氣候風險，可能會調整硬體供應鏈策略、產品組合和市場定位，以應對未來的氣候變化。 • 財務影響：中期內的氣候變化可能導致專案無法如期執行，從而對公司的營收認列及現金流產生影響。 長期影響： • 業務影響：氣候變化可能對產業結構和市場需求產生深遠影響，公司可能需要調整服務和業務模式以適應長期氣候趨勢。 • 策略影響 : 公司需要發展長期的氣候變化適應策略，包括投資遠端執行技術、減少碳排放量，參與氣候風險管理和減緩計劃。 • 財務影響 : 長期氣候變化可能導致公司需重大資本支出，例如投資太陽能、機電設備效能提升所需的投資。
3.敘明極端氣候事件及轉型行動對財務之影響。	• 直接損失：極端氣候事件 (如颶風、洪水、乾旱) 可能導致設施損壞、甚至對員工和顧客造成傷害，進而產生直接的損失。 • 保險成本增加：頻繁的極端氣候事件可能導致保險成本增加，包括財產保險和商業中斷保險，進一步增加企業的開支。
4.敘明氣候風險之辨識、評估及管理流程如何整合於整體風險管理制度。	將氣候風險辨識、評估和管理流程整合到整體風險管理制度中是公司維持長期穩健經營所必需的。以下是整合流程的一般步驟： • 辨識氣候風險： 透過政府相關單位，所發佈相關訊息，辨識可能影響公司的氣候相關風險，如極端氣候事件、氣候變化趨勢等。 • 評估風險的影響和可能性： 1.使用資料分析方法評估氣候風險的潛在影響，包括財務、運營等方面的影響。 2.考慮氣候風險的發生機率、影響程度和時間軸，以便制定相應的應對策略。 • 整合到風險管理框架中： 將氣候風險納入企業的風險管理框架，確確認相關的風險所有者和負責人，明確負責風險管理的流程和程序。

項目	執行情形
	• 制定應對策略： 1.基於風險評估結果，制定應對氣候風險的策略和計劃，包括風險減緩、轉移、接受或避免等策略。 2.考慮長期氣候趨勢，制定適應性措施，以應對氣候變化對業務的長期影響。 • 實施和監控： 1.將制定的策略和計劃實施到實際業務運營中，確保相應的風險管理措施得以執行。 2.定期監控氣候風險的變化和發展，並調整應對策略以應對新的情況和挑戰。 • 持續改進。
5.若使用情境分析評估面對氣候變遷風險之韌性，應說明所使用之情境、參數、假設、分析因子及主要財務影響。	情境分析的步驟： • 情境描述：首先，需要清楚描述所處的情境，例如一個城市、一個農村地區或一家企業。這包括地理位置、氣候特徵、經濟結構、社會人口結構等。 • 參數設定：確定評估的參數，這可能包括氣候變遷的預期影響，如極端氣候事件的頻率和強度、平均氣溫上升、海平面上升等。 • 假設設定：制定對未來可能發生的氣候變遷影響的假設，這些假設可能基於科學模型、歷史數據、專家意見等。 • 分析因子：確定影響韌性的主要因子，這些因子可能包括資源可用性、政府政策、科技水平等。將這些因子納入分析可以幫助確定強化韌性的關鍵措施。
6.若有因應管理氣候相關風險之轉型計畫，說明該計畫內容，及用於辨識及管理實體風險及轉型風險之指標與目標。	主要財務影響：評估氣候變遷風險對財務的主要影響，這可能包括直接損失，如基礎設施損壞，以及間接影響，如市場變動、保險成本增加等。
7.若使用內部碳定價作為規劃工具，應說明價格制定基礎。	尚未使用內部碳定價。
8.若有設定氣候相關目標，應說明所涵蓋之活動、溫室氣體排放範疇、規劃期程，每年達成進度等資訊；若使用碳抵換或再生能源憑證（RECs）以達成相關目標，應說明所抵換之減碳額度來源及數量或再生能源憑證（RECs）數量。	目標涵蓋的活動： • 減少溫室氣體排放：包括直接排放（如工廠排放、車輛排放）和間接排放（如供應鏈排放）。 • 能源效率提升：通過節能措施、技術更新等方式減少能源消耗。 • 可再生能源使用增加：增加可再生能源在能源結構中的比例，例如太陽能、風能等。 • 資源循環利用：推動資源的有效循環利用，減少廢棄物產生和排放。 • 氣候風險管理：加強對氣候變化和極端氣候事件的風險管理能力。 溫室氣體排放範疇： • 範疇 1：直接排放，如公司內部生產活動所產生的二氧化碳、甲烷等排放。 • 範疇 2：間接能源排放，如從電力和熱能的使用中產生的二氧化碳排放。 • 範疇 3：其他間接排放，包括供應鏈和產品使用後的排放，如原料生產、運輸、製造過程等。 規劃期程： • 短期目標：通常設定為 1 至 5 年，用於確定快速可行的措施，以實現即時效益和進展。 • 中期目標：設定為 5 至 10 年，用於實施較大範圍的改變，如能源結構調整、技術更新等。

項目	執行情形
	• 長期目標：通常設定為 10 年以上，用於達成更具挑戰性的目標。 建立監測和報告機制，以確定每年的進度和達成情況。定期進行測量和評估，並根據實際進展調整行動計劃。這些資訊將有助於公司確定氣候相關目標，並制定相應的行動計劃，以實現氣候目標並達成可持續發展的目標。
9.溫室氣體盤查及確信情形與減量目標、策略及具體行動(另填於 1-1 及 1-2)。	詳 1-1 及 1-2

2. 最近二年度公司溫室氣體盤查及確信情形

本公司基本資料
□資本額 100 億元以上公司、鋼鐵業、水泥業
□資本額 50 億元以上未達 100 億元之公司
■資本額未達 50 億元之公司

依上市櫃公司永續發展路徑圖規定至少應揭露
□母公司個體盤查 □合併財務報告子公司盤查
□母公司個體確信 □合併財務報告子公司確信

年度	範圍	排放量（公噸 CO2e）		密集度（公噸 CO2e/百萬元）		確信機構	確信準則	確信意見
		範疇一	範疇二 (註 2)	範疇一	範疇二 (註 2)			
2023	母公司	0.79	419.59	0.12	0.39	台灣檢驗科技股份(限)公司	ISO14064-3	合理保證
	子公司(註 1)	217.45	290.80					
2022	母公司	1.07	383.68	0.13	0.89	台灣檢驗科技股份(限)公司		合理保證
	子公司(註 1)	234.54	1266.15					

註 1：包含宏碁雲架構服務（股）公司及安碁學苑（股）公司。
註 2：市場基礎

3. 溫室氣體減量目標、策略及具體行動計畫

(1) 溫室氣體減排目標

- 本公司為宏碁集團的一分子，響應集團政策，從 3 大面向 9 項策略，致力從企業永續營運、產品與服務及價值鏈 3 大面向，並透過減少能源消耗、使用再生能源、負碳抵消、低碳產品與服務、使用再生物料、投入智慧、循環與綠能應用、減碳目標與承諾、綠色製造與物流及實踐低碳循環經濟等九大方針著手，全面性地減少碳足跡。
- 承諾於 2030 年組織營運（範疇 1+2）達成相較於 2022 年減碳 35%。

(2) 策略

- 轉型能源結構：促進可再生能源（如風能、太陽能）和其他低碳能源的發展，減少對化石燃料的依賴。
- 能源效率提升：通過技術創新和政策支持，提高能源利用效率，降低溫室氣體排放。

- 節能減排政策：制定和實施節能減排政策，鼓勵節能減排技術的應用和推廣。

(3) 具體行動計劃

- 推行能源監控系統建置、電力分電盤 PDU 汰換、電動車充電區設置等多項能源管理措施，並搭配自建太陽能發電系統，簽訂再生能源購電協議與購買再生能源憑證的方式，逐步提高再生電力使用佔比。
- 2023 年宏碁雲架構（股）(安碁資訊 100%持有子公司）與風力發電廠商-能源超商股份有限公司（台泥集團）簽訂再生能源購電合約，共購入綠電 182.2 萬度，減少排碳量 901.89 公噸。
- 2024 年宏碁雲架構（股）(安碁資訊 100%持有子公司)，已自建 390kw 太陽能發電系統。
- 2024 年宏碁雲架構(股)(安碁資訊 100%持有子公司)，已汰換部分冰水主機，以提高效能使用。

（八）履行誠信經營情形及與上市上櫃公司誠信經營守則差異情形及原因

評估項目	運作情形			與上市上櫃公司誠信經營守則差異情形及原因
	是	否	摘要說明	
一、訂定誠信經營政策及方案 (一)公司是否制定經董事會通過之誠信經營政策，並於規章及對外文件中明示誠信經營之政策、作法，以及董事會與高階管理階層積極落實經營政策之承諾？	V		(一)本公司已於民國 108 年 3 月 19 日經董事會訂定「誠信經營作業程序及行為指南」，並依守則確實執行。	無重大差異
(二)公司是否建立不誠信行為風險之評估機制，定期分析及評估營業範圍內具較高不誠信行為風險之營業活動，並據以訂定防範不誠信行為方案，且至少涵蓋「上市上櫃公司誠信經營守則」第七條第二項各款行為之防範措施？	V		(二)本公司訂有誠信經營作業程序及行為指南，公司於員工到職時亦進行宣導公司誠信經營之政策；並由人資、法務、稽核等跨部門單位定期分析及評估營業範圍內具較高不誠信行為風險之營業活動。	無重大差異
(三)公司是否於防範不誠信行為方案內明定作業程序、行為指南、違規之懲戒及申訴制度，且落實執行，並定期檢討修正前揭方案？	V		(三)本公司已訂有誠信相關政策，針對防範不誠信原則之方案，包括內部控制制度下各項辦法及循環，均納入相關作業程序，此外於人事管理規則就員工違規之懲戒及申訴制度定有相關規範，且公司於員工到職時及在職期間均不斷宣導公司誠信經營之政策，並由稽核單位定期稽核，以提高整體認知、偵測潛在的不當行為以監督遵行情形，並隨時據以檢討修正前揭方案。	無重大差異

評估項目	運作情形			與上市上櫃公司誠信經營守則差異情形及原因
	是	否	摘要說明	
二、落實誠信經營 (一)公司是否評估往來對象之誠信紀錄，並於其與往來交易對象簽訂之契約中明定誠信行為條款？	V		(一)公司商業活動，由財務部門進行往來客戶審查評等，並由法務顧問審查簽立之合約條款，以避免與有不誠信行為紀錄者進行交易。本公司與商業合作夥伴從事各類交易時，將要求商業合作夥伴簽訂「供應商廉潔暨企業社會責任承諾書」並將廉潔承諾訂於相關合約中。	無重大差異
(二)公司是否設置隸屬董事會之推動企業誠信經營專責單位，並定期(至少一年一次) 向董事會報告其誠信經營政策與防範不誠信行為方案及監督執行情形？	V		(二)本公司一直致力於以符合法律與道德之高標準來推展業務，要求公司經營階層必須建立一個重視道德誠信從業行為的良好典範。公司治理人為專責單位，在董事會的監督下，由人資、法務、稽核等跨部門單位共同推動企業誠信經營與敦促所有員工及各關係人確實遵行，且列入每年年度稽核計畫之稽核項目；並由稽核主管於審計委員會及董事會會議中報告執行情形，以具體落實企業誠信；預計於114年第二季向董事會報告113年度執行情形，執行重點如下： 1.將誠信與道德價值融入公司經營策略，併配合法令制度訂定確保誠信經營之相關措施。 2.規劃內部組織、職掌及職責，對營業範圍內較高不誠信行為風險之營業活動，建立相互監督制衡機制。 3.持續對員工宣導「公司誠信政策」，以提高員工對公司誠信政策的重視及警覺性。 4.訂定「供應商廉潔暨企業社會責任承諾書」並敦促本公司合作廠商簽署。	無重大差異
(三)公司是否制定防止利益衝突政策、提供適當陳述管道，並落實執行？	V		(三)本公司訂有誠信經營作業程序及行為指南，對於規範員工利益衝突之規定設有專章，並提於公司網站上提供申訴檢舉信箱。	無重大差異
(四)公司是否為落實誠信經營已建立有效的會計制度、內部控制制度，並由內部稽核單位依不誠信行為風險之評估結果，擬訂相關稽核計畫，並據以查核防範不誠信行為方案之遵循情形，或委託會計師執 行查核。	V		(四)公司建立之會計制度、內部控制制度之執行情形，由內部稽核人員依不誠信行為風險之評估結果，擬訂相關稽核計畫，計畫進行查核作業。經稽核單位查核本公司113年1月至12月，並未發現有違反誠信經營之相關事項。	無重大差異
(五)公司是否定期舉辦誠信經營之內、外部之教育訓練？	V		(五)本公司訂定員工業務行為準則，本規範為所有員工進行業務活動之最高行為準則，於每位新進人員加入時，均施以教育訓練	無重大差異

評估項目	運作情形			與上市上櫃公司誠信經營守則差異情形及原因
	是	否	摘要說明	
			要求員工務必遵守。此外，直屬主管必須負責督導所屬同仁，確實遵守員工業務行為準則。 114年2月11日針對部級以上主管及內部人等分別進行「誠信經營及內線交易證券法規與實例研討」及「內部人持股變動申報違反證券交易法規定之常見態樣」相關宣導，以提高相關單位及人員對於公司誠信政策及證交法令規定的重視及警覺性。	
三、公司檢舉制度之運作情形 (一)公司是否訂定具體檢舉及獎勵制度，並建立便利檢舉管道，及針對被檢舉對象指派適當之受理專責人員？	V		(一)本公司於員工業務行為準則中訂有檢舉制度，此外，員工於發現任何不法行為或違反公司治理活動時，得透過電子信箱由稽核室專責處理。	無重大差異
(二)公司是否訂定受理檢舉事項之調查標準作業程序、調查完成後應採取之後續措施及相關保密機制？	V		(二)本公司有受理檢舉事項之調查標準作業程序及相關保密機制。	無重大差異
(三)公司是否採取保護檢舉人不因檢舉而遭受不當處置之措施？	V		(三)本公司採取保護檢舉人不因檢舉而遭受不當處置之措施。	無重大差異
四、加強資訊揭露 (一)公司是否於其網站及公開資訊觀測站，揭露其所定誠信經營守則內容及推動成效？	V		(一)本公司已建立網站並揭露「誠信經營作業程序及行為指南」，並依法於公開資訊觀測站即時公告及更新相關資訊。	無重大差異
五、公司如依據「上市上櫃公司誠信經營守則」訂有本身之誠信經營守則者，請敘明其運作與所訂守則之差異情形：本公司已參酌「上市上櫃公司誠信經營守則」及考量公司實務運作情形，制定「誠信經營守則」、「誠信經營作業程序及行為指南」，且依循相關法規確實落實誠信經營，以規範本公司人員於執行業務時應注意之事項。				
六、其他有助於瞭解公司誠信經營運作情形之重要資訊：本公司遵循相關法規及內部控制制度，嚴禁不誠信或違反法令之行為。				

（九）其他足以增進對公司治理運作情形之瞭解的重要資訊，得一併揭露：無

（十）內部控制制度執行狀況應揭露下列事項

1. 內部控制聲明書，請參閱公開資訊觀測站【索引路徑：公開資訊觀測站>單一公司>公司治理>公司規章 / 內部控制>內控聲明書公告；網址：https://mops.twse.com.tw/mops/#/web/t06sg20】，輸入年度及公司代號，查詢內控聲明書公告。
2. 委託會計師專案審查內部控制制度者，應揭露會計師審查報告：無。

(十一)最近年度及截至年報刊印日止，股東會及董事會之重要決議

1. 董事會之重要決議

日期	會議名稱	重要決議
113.1.23	113年 第一次 董事會	(1) 通過購買南港利百代大樓建物及土地案 (2) 通過向銀行辦理購買南港利百代大樓建物及土地之不動產貸款案
113.2.27	113年 第二次 董事會	(1) 通過民國112年度董事酬勞預算案 (2) 通過民國112年度員工酬勞預算案 (3) 通過本公司民國112年度財務報表及營業報告書案 (4) 通過本公司民國112年度盈餘分派案 (5) 通過本公司民國112年度內部控制聲明書案 (6) 通過委任本公司民國113年度財務報表查核簽證會計師及評估會計師獨立性案 (7) 通過訂定註銷本公司收回民國110年第一次限制員工權利新股股份之減資基準日 (8) 通過本公司章程修訂案 (9) 通過召開本公司民國113股東常會相關事宜 (10)通過經理人異動案 (11)通過經理人伙食津貼調整討論案 (12)通過經理人薪酬討論案
113.4.30	113年 第三次 董事會	(1) 同意民國113年第一季經會計師核閱之財務季報告 (2) 同意向金融機構辦理續約授信案 (3) 通過訂定註銷本公司收回民國110年第一次限制員工權利新股股份之減資基準日案
113.7.30	113年 第四次 董事會	(1) 同意民國113年第二季經會計師核閱之財務季報告 (2) 通過辦理民國113年度第一次現金增資發行新股案 (3) 通過本公司內部規章修訂案 (4) 通過變更公司登記地址案 (5) 通過民國112年經理人員工酬勞分配案
113.9.4	113年 第五次 董事會	通過增資子公司宏碁雲架構服務股份有限公司
113.10.24	113年 第六次 董事會	(1) 通過民國113年度第一次現金增資新股發行價格案 (2) 通過民國113年度第一次現金增資新股員工認購分配計畫案
113.10.29	113年 第七次 董事會	(1) 同意民國113年第三季經會計師核閱之財務季報告 (2) 同意本公司民國114年度營運計畫暨預算案 (3) 同意本公司民國114年度稽核計畫 (4) 通過修訂本公司預先核准非確信服務政策及服務清單案 (5) 通過本公司內部規章增修訂案 (6) 同意本公司民國114度經理人目標獎金預算暨 (7) 同意本公司民國114年度調薪規劃及預算案

日期	會議名稱	重要決議
114.2.24	114年第一次董事會	(1) 通過民國113年董事酬勞案 (2) 通過民國113年員工酬勞案 (3) 同意民國113年度財務報表及營業報告書案 (4) 通過本公司民國113年度盈餘分派案 (5) 通過本公司民國113年度內部控制制度聲明書案 (6) 通過委任本公司民國114年度財務報表查核簽證會計師及評估會計師獨立性案 (7) 通過訂定註銷本公司收回民國110年第一次限制員工權利新股股份之減資基準日 (8) 通過本公司基層員工範圍案 (9) 通過本公司章程修訂案 (10)通過本公司薪工循環修訂案 (11)通過全面改選本公司董事七席（含獨立董事四席）暨提名董事（含獨立董事）候選人案 (12)通過提請股東會解除本公司新任董事及其法人代表人競業禁止之限制 (13)通過召集本公司民國114年股東常會相關事宜 (14)通過民國113年經理人目標獎金討論案 (15)通過民國114年經理人調薪討論案

2. 股東會之決議事項及執行情形

113 年股東常會（113 年 5 月 28 日）決議事項執行情形：

決議事項	執行情形
民國112年度財務報表、營業報告書及盈餘分配表承認案	股東會決議照案通過。
修訂公司章程討論案	股東會決議照案通過。

（十二）最近年度及截至年報刊印日止董事或監察人對董事會通過重要決議有不同意見且有紀錄或書面聲明者，其主要內容：無。

四、簽證會計師公費資訊

（一）給付簽證會計師與其所屬事務所及關係企業之審計公費與非審計公費之金額及非審計服務內容：

金額單位：新台幣千元

會計師事務所名稱	會計師姓名	會計師查核期間	審計公費	非審計公費	合計	備註
安侯建業聯合會計師事務所	趙敏如 張惠貞	113年度	2,370	830（註）	3,200	無

註：非審計公費係英文年度財報及稅務簽證、全時員工薪資檢查表（非主管職）查核費用。

（二）更換會計師事務所且更換年度所支付之審計公費較更換前一年度之審計公費減少者，應揭露更換前後審計公費金額及原因：無此情形。

（三）審計公費較前一年度減少達百分之十以上者，應揭露審計公費減少金額、比例及原因：無。

五、更換會計師資訊

無此情形。

六、公司董事長、總經理、負責財務或會計事務之經理人，最近一年內曾任職於簽證會計師所屬事務所或其關係企業之情形

無此情形。

七、最近年度及截至年報刊印日止，董事、監察人、經理人及持股比例超過百分之十之股東股權移轉及股權質押變動情形

請參閱公開資訊觀測站，【索引路徑：公開資訊觀測站>單一公司>公司治理>公司規章 / 內部控制>內部控制專案審查報告；網址：https://mops.twse.com.tw/mops/#/web/t06hsg20】。

八、持股比例占前十名股東，其相互間為關係人或為配偶、二親等以內之親屬關係之資訊

日期：114 年 3 月 29 日；單位：股

姓名	本人持有股份		配偶、未成年子女持有股份		利用他人名義合計持有股份		前十大股東相互間具有關係人或為配偶、二親等以內之親屬關係者，其名稱或姓名及關係		備註
	股數	持股比率	股數	持股比率	股數	持股比率	名稱(或姓名)	關係	
宏碁股份有限公司	15,561,992	51.87%	0	0.00%	0	0.00%	宏榮投資股份有限公司	宏榮公司為宏碁公司之法人董事	-
							群碁投資股份有限公司	群碁公司為宏碁公司子公司	
代表人：陳俊聖	0	0.00%	0	0.00%	0	0.00%	群碁股份有限公司	陳俊聖為群碁公司董事長	-
群碁投資股份有限公司	1,295,001	4.32%	0	0.00%	0	0.00%	宏碁股份有限公司	群碁公司為宏碁公司子公司	-
代表人：陳俊聖	0	0%	0	0.00%	0	0.00%	宏碁股份有限公司	陳俊聖為宏碁公司董事長	-

姓名	本人持有股份		配偶、未成年子女持有股份		利用他人名義合計持有股份		前十大股東相互間具有關係人或為配偶、二親等以內之親屬關係者，其名稱或姓名及關係		備註
	股數	持股比率	股數	持股比率	股數	持股比率	名稱(或姓名)	關係	
宏碁智聯網投資控股股份有限公司	1,200,000	4.00%	0	0.00%	0	0.00%	宏碁股份有限公司	宏碁智聯網公司為宏碁公司之子公司	-
代表人：陳俊聖	0	0%	0	0.00%	0	0.00%	宏碁股份有限公司	陳俊聖為宏碁公司董事長	-
渣打國際商業銀行營業部受託保管瑞穗證券股份有限公司投資專戶	344,000	1.15%	0	0.00%	0	0.00%	無	無	-
鄭威宏	260,000	0.87%	0	0.00%	0	0.00%	無	無	-
吳乙南	243,003	0.81%	0	0.00%	0	0.00%	無	無	-
宏榮投資股份有限公司	178,939	0.60%	0	0.00%	0	0.00%	無	無	-
代表人：葉紫華	0	0.00%	0	0.00%	0	0.00%	無	無	-
花旗(台灣)商業銀行受託保管星展銀行有限公司 - 外部帳戶管理者摩根大通投資專戶	159,000	0.53%	0	0.00%	0	0.00%	無	無	-
花旗(台灣)商業銀行受託保管ＢＮＰ金融市場投資專戶	156,000	0.52%	0	0.00%	0	0.00%	無	無	-
呂佳興	145,199	0.48%	0	0.00%	0	0.00%	無	無	-

九、公司、公司之董事、經理人及公司直接或間接控制之事業對同一轉投資事業之持股數，並合併計算綜合持股比例

轉投資事業	本公司投資		董事、監察人、經理人及直接或間接控制事業之投資		綜合投資	
	股數	持股比例(%)	股數	持股比例(%)	股數	持股比例(%)
安碁學苑(股)公司	1,000,000	100%	0	0	1,000,000	100%
宏碁雲架構服務(股)公司	114,462,350	100%	0	0	114,462,350	100%

參

、募資情況

參、 募資情形

一、公司資本及股份

(一) 股本來源

單位：股；新台幣元

年月	發行價格	核定股本		實收股本		備註		
		股數	金額	股數	金額	股本來源	以現金以外之財產抵充股款者	其他
89.05	10元	50,000	500,000	50,000	500,000	創立股本	無	註1
89.08	10元	30,050,000	300,500,000	30,050,000	300,500,000	現金增資300,000,000元	無	註2
90.04	10元	210,050,000	2,100,500,000	150,050,000	1,500,500,000	現金增資200,000,000元	無	註3
90.07	10元	210,050,000	2,100,500,000	200,050,000	2,000,500,000	現金增資500,000,000元	無	註4
91.11	10元	250,050,000	2,500,500,000	250,050,000	2,500,500,000	現金增資500,000,000元	無	註5
92.04	10元	300,050,000	3,000,500,000	300,050,000	3,000,500,000	現金增資500,000,000元	無	註6
95.04	10元	300,050,000	3,000,500,000	181,884,402	1,818,844,020	減資彌補虧損計1,181,655,980元	無	註7
97.11	10元	300,050,000	3,000,500,000	187,092,616	1,870,926,160	合併第三波增資52,082,140元	第三波股份(註8)	註8
106.10	10元	300,050,000	3,000,500,000	190,592,616	1,905,926,160	盈餘轉增資35,000,000元	無	註9
106.12	10元	300,050,000	3,000,500,000	4,000,000	40,000,000	分割減資1,865,926,160元	無	註10
107.02	10元	300,050,000	3,000,500,000	11,500,000	115,000,000	法定盈餘公積轉增資75,000,000元	無	註11
107.03	10元	300,050,000	3,000,500,000	11,886,000	118,860,000	員工認股權憑證執行	無	註12
107.05	10元	300,050,000	3,000,500,000	12,629,600	126,296,000	員工認股權憑證執行	無	註13
108.10	10元	300,050,000	3,000,500,000	16,339,600	16,339,600	現金增資37,100,000元	無	註14
109.09	10元	300,050,000	3,000,500,000	16,666,392	16,666,392	盈餘轉增資3,267,920元	無	註15

單位：股；新台幣元

年月	發行價格	核定股本		實收股本		備註		
		股數	金額	股數	金額	股本來源	以現金以外之財產抵充股款者	其他
110.09	10元	300,050,000	3,000,500,000	16,999,720	169,997,200	盈餘轉增資 3,333,280元	無	註16
111.03	10元	300,050,000	3,000,500,000	17,240,720	172,407,200	發行限制員工權利新股 2,410,000元	無	註17
111.07	10元	300,050,000	3,000,500,000	22,240,720	222,407,200	現金增資 50,000,000元	無	註18
112.03	10元	300,050,000	3,000,500,000	22,204,570	222,045,700	收回限制員工權利新股 361,500元	無	註19
113.03	10元	300,050,000	3,000,500,000	22,120,220	221,202,200	收回限制員工權利新股 843,500元	無	註20
113.05	10元	300,050,000	300,050,000	22,115,220	221,152,200	收回限制員工權利新股 50,000元	無	註21
114.01	10元	300,050,000	3,000,500,000	30,115,220	301,152,200	現金增資 80,000,000元	無	註22
114.03	10元	300,050,000	3,000,500,000	29,999,720	299,997,200	收回限制員工權利新股 1,155,000元	無	註23

註1：89.05.29北市建商二字第89294676號函。

註2：89.08.15經（089）商字第089129675號函。

註3：90.04.09經（90）商字第09001102810號函。

註4：90.07.16經（90）商字第09001271860號函。

註5：91.12.12經授商字第09101496310號函。

註6：92.04.24經授商字第09201124120號函。

註7：95.05.05經授商字第09501081490號函。

註8：98.01.12經授商字第09701329350號函；本公司發行股票計52,082仟元，以吸收合併方式與第三波資訊股份有限公司合併。本公司與第三波公司皆為宏碁股份有限公司百分之百持有之子公司，本公司為存續公司，第三波公司為消滅公司。

註9：106.11.08經授商字第10601152380號函。

註10：107.01.16經授商字第10701003560號函。

註11：107.03.09府產業商字第10746911710號函。

註12：107.04.24府產業商字第10747839710號函。

註13：107.05.10府產業商字第10749035400號函。

註14：108.11.08府產業商字第10856007700號函。

註15：109.08.31府產業商字第10953563710號函。

註16：110.09.02府產業商字第11053034500號函。

註17：111.03.31府產業商字第11147883200號函。

註18：111.07.08府產業商字第11150917800號函。

註19：112.03.16府產業商字第11247007300號函。

註20：113.03.26府產業商字第11347408000號函。

註21：113.05.21府產業商字第11349462000號函。

註22：114.01.15府產業商字第11445004210號函。

註23：114.03.17府產業商字第11447141600號函。

單位：股；新台幣元

股份種類	核定股本			備註
	流通在外股份	未發行股份	合計	
普通股	29,999,720股	270,050,280股	300,050,000股	上櫃公司股票

總括申報制度相關資訊：無

（二）主要股東名單

114 年 3 月 29 日；單位：股；%

主要股東名稱 \ 股份	持有股數	持股比例
宏碁股份有限公司	15,561,992	51.87%
群碁投資股份有限公司	1,295,001	4.32%
宏碁智聯網投資控股股份有限公司	1,200,000	4.00%
渣打國際商業銀行營業部受託保管瑞穗證券股份有限公司投資專戶	344,000	1.15%
鄭威宏	260,000	0.87%
吳乙南	243,003	0.81%
宏榮投資股份有限公司	178,939	0.60%
花旗（台灣）商業銀行受託保管星展銀行有限公司 - 外部帳戶管理者摩根大通投資專戶	159,000	0.53%
花旗（台灣）商業銀行受託保管ＢＮＰ金融市場投資專戶	156,000	0.52%
呂佳興	145,199	0.48%

（三）公司股利政策及執行狀況

1. 公司章程所訂之股利政策

(1) 本公司年度總決算如有盈餘，應先提繳稅款，彌補以往虧損，次提百分之十為法定盈餘公積，但法定盈餘公積已達資本總額時不在此限。次依法令或主管機關規定提列或迴轉特別盈餘公積，其餘保留連同以前年度為未分配盈餘外，得派付股東股利，由董事會擬定股東股利分派案，提請股東會決議後分派之；除依法令以公積分派外，公司無盈餘時，不得分派股息及紅利。

本公司分派股息及紅利之全部或一部如以發放現金為之，授權董事會以三分之二以上董事之出席，及出席董事過半數之決議為之，並報告股東會。

(2) 本公司股利政策，係配合目前及未來之發展計畫、考量投資環境、資金需求及國內外競爭狀況，並兼顧股東利益等因素，每年就可供分配盈餘提撥不低於百分之十分配股東股息紅利，得以股票或現金之方式分派之。為達平衡穩定之股利政策，本公司股利分派時，其中現金股利不得低於股利總數之百分之十，惟經董事會決議不分配，並經股東會通過，不在此限。公司無盈餘時，不得分派股息及紅

利，惟依本公司財務、業務及經營面等因素之考量，得將法定盈餘及資本公積全部或一部分依法令或主管機關規定分派之。

2. 本公司依照當年度獲利情形、業務發展及評估資金規劃後配發股息，近三年均配發55%以上的獲利予股東。

3. 本年度擬（已）議股利分派之情形：

現金股利部分，按公司章程第二十四條之授權，由董事會於民國 114 年 2 月 24 日決議通過，每股配發新台幣 6 元，總計配發新台幣 179,998,320 元。

前揭盈餘分配之除息基準日擬訂為民國 114 年 7 月 10 日，發放日擬訂為民國 114 年 7 月 29 日，如遇有法令變更、主管機關職權行使或要求修正等情事而需變更前述時程，全權授權董事長調整之。

（四）本年度擬議之無償配股對公司營業績效及每股盈餘之影響：本公司 113 年僅配發現金股利及 114 年未公布財務預測，故不適用。

（五）員工、董事及監察人酬勞

1. 公司章程所載員工、董事及監察人酬勞之成數或範圍

本公司年度如有獲利，於預先保留彌補累積虧損之數額後，就其餘額應提撥不低於百分之二為員工酬勞及得另提撥不高於千分之八為董事酬勞。

前項員工酬勞得以現金或股票為之，其分派對象得包括符合一定條件之從屬公司員工，該一定條件由董事會訂定之。

2. 本期估列員工、董事及監察人酬勞金額之估列基礎、以股票分派之員工酬勞之股數計算基礎及實際分派金額若與估列數有差異時之會計處理財務報告通過發布日前經董事會決議之員工、董監事酬勞之估列金額與發放金額有重大差異時，該差異調整原提列年度費用，財務報告通過發布日後若金額仍有變動，則依會計估計變動處理，於次一年度調整入帳。

3. 董事會通過分派酬勞情形

(1) 以現金或股票分派之員工酬勞及董事、監察人酬勞金額。若與認列費用年度估列金額有差異，應揭露差異數、原因及處理情形：

A. 本公司民國 113 年度員工酬勞總金額為新台幣 27,429,000 元，董事酬勞為新台幣 2,170,000 元，業經民國 114 年 2 月 24 日董事會決議通過，皆以現金方式發放。

B. 員工酬勞及董事酬勞與認列費用年度估列金額無差異。

(2) 以股票分派之員工酬勞金額占本期稅後純益及員工酬勞總額合計數之比例：不適用。

4. 前一年度員工、董事及監察人酬勞之實際分派情形（包括分派股數、金額及股價）、其與認列員工、董事及監察人酬勞有差異者並應敘明差異數、原因及處理情形

	112年度		
	董事會決議金額	實際發放數	
		金額	折算股數
員工酬勞（以現金發放）	23,200,000元	23,200,000元	–
員工酬勞（以股票依市值發放）	0元	0元	0股
董事酬勞	1,800,000元	1,800,000元	–
合計	25,000,000元	25,000,000元	0股

（六）公司買回本公司股份情形：無。

二、公司債（含海外公司債）辦理情形

無。

三、特別股辦理情形

無。

四、海外存託憑證之辦理情形

無。

五、員工認股權憑證辦理情形

無。

六、限制員工權利新股辦理情形

（一）尚未全數達既得條件之限制員工權利新股辦理情形

114年3月29日

限制員工權利新股種類	110年第一次限制員工權利新股
申報生效日期及總股數	111年1月7日 300,000股
發行日期	111年3月9日
已發行限制員工權利新股股數	241,000股
尚可發行限制員工權利新股股數	59,000股

發行價格	新台幣0元
已發行限制員工權利新股股數占已發行股份總數比率	1.08%
員工限制權利新股之既得條件	員工自獲配限制員工權利新股後需於各既得日當日仍在職，且期間未曾有違反本公司勞動契約、工作規則、誠信經營作業程序及行為指南、道德行為準則、競業禁止、保密協議或與公司間合約約定等情事，並達成公司所設定之員工個人績效指標與公司營運績效指標；於各年度既得日可既得之最高股份比例分別為：2022年可既得股數比例上限為15%、2023年可既得股數比例上限為35%、2024年可既得股數比例上限為50%，2022至2024年三年合計可既得股數比例上限為100%。 員工個人績效指標：當年度績效考核達三顆星（精通/Proficient）（含）以上，如未達成，則獲配股數為0。 公司營運績效指標：公司營運績效指標以本公司（不含預計於2022年收購之宏碁雲架構服務股份有限公司）之營收及稅後淨利（PAT）為指標。各指標分別設定權重及低（LOW-Bar）、中（MID-Bar）、高（HIGH-Bar）三個目標區間，達LOW-Bar之既得股數獲配比率比例為50%，達MID-Bar之既得股數獲配比率比例為70%，達HIGH-Bar之既得股數獲配比率比例為100%，如任一指標未達LOW-Bar，則獲配股數為0。達成績效指標與水準之判定依各績效期間所對應經會計師查核簽證之財務報表為基礎。
員工限制權利新股之受限制權利	員工獲配新股後未達成既得條件前，除繼承外，不得將該限制員工權利新股出售質押、轉讓、贈與他人、設定負擔，或作其他方式之處分。 員工獲配新股後未達成既得條件前，股東會之出席、提案、發言、表決及選舉權等權利，與本公司已發行之普通股相同，且依本公司或本公司指定信託機構之保管契約執行之。 員工依本辦法獲配之限制員工權利新股，於未達成既得條件前，其他權利包括但不限於股息、股利、法定公積及資本公積受配權、現金增資之認股權等，與本公司已發行之普通股股份相同，相關作業方式依本公司或本公司指定信託機構之保管契約執行之。 本公司無償配股停止過戶日、現金股息停止過戶日、現金增資認股停止過戶日、公司法第165條第3項所訂股東會停止過戶期間、或其他依事實發生之法定停止過戶期間至權利分派基準日止，此期間達成既得條件之員工，其既得股票解除限制時間及程序依本公司或本公司指定信託機構之保管契約或相關法規規定執行之。
限制員工權利新股之保管情形	於既得條件成就前，交付信託保管。
員工獲配或認購新股後未達既得條件之處理方式	員工自獲配限制員工權利新股後，遇有既得日不在職，或未達成公司所設定個人績效指標與公司營運績效指標，或違反本公司勞動契約、工作規則、誠信經營作業程序及行為指南、道德行為準則、競業禁止、保密協議或與公司間合約約定等情事，本公司有權於前述任一事項發生時，即就其未達成既得條件之限制員工權利新股予以無償收回並辦理註銷。

	於既得期間內，員工如有自願離職、解雇、資遣，其之前獲配尚未既得之股份，本公司將無償收回並辦理註銷。
已收回或收買限制員工權利新股股數	241,000股
已解除限制權利之股數	0股
未解除限制權利之股數	0股
未解除限制權利之股數占已發行股份總數比率（%）	0%
對股東權益影響	本次發行股數占公司目前已發行股份總數比率約為1.08%，對原股東權益之影響係逐年稀釋，故其稀釋效果尚屬有限。

（二）取得限制員工權利新股之經理人及取得前十大之員工姓名、取得情形

114 年 3 月 29 日

	職稱	姓名	限制員工權利新股數量	取得限制員工權利新股之股數占已發行股份總數比率	已解除限制權利				未解除限制權利			
					已解除限制之股數	發行價格	發行金額	已解除限制之股數占已發行股份總數比率	未解除限制之股數	發行價格	發行金額	未解除限制之股數占已發行股份總數比率
經理人	總經理	吳乙南	60,000	0.27%	60,000	0	0	0.27%	0	0	0	0%
	技術副總	黃瓊瑩										
員工	處長	薛承文	181,000	0.82%	181,000	0	0	0.82%	0	0	0	0%
	經理	盧柏霖										
	副理	李冠億										
	副理	施姵含										
	資深經理	蔡東霖										
	資深經理	楊家豪										
	經理	吳榮昌										
	副理	黃文治										
	副理	楊景昇										

註：係依 114.03.17.台北市核准變更登記之已發行股份總數計算。

七、併購或受讓他公司股份發行新股辦理情形

無。

八、資金運用計畫執行情形

（一）計畫內容：截至年報刊印日之前一季止，前各次發行或私募有價證券尚未完成或最近三年內已完成且計畫效益尚未顯現者，應詳細說明前開各次發行或私募有價證券計畫內容：請參閱公開資訊觀測站【索引路徑：公開資訊觀測站>單一公司>股權變動 / 證券發行>募資>募資計畫執行；網址：https://mopsov.twse.com.tw/mops/web/bfhtm_q2】。

（二）執行情形：就前款之各次計畫之用途，逐項分析截至年報刊印日之前一季止，其執行情形及與原預計效益之比較：請參閱公開資訊觀測站【索引路徑：公開資訊觀測站>單一公司>股權變動 / 證券發行>募資>募資計畫執行；網址：https://mopsov.twse.com.tw/mops/web/bfhtm_q2】。

肆

、營運概況

肆、 營運概況

一、業務內容

（一）業務範圍

1. 所營業務之主要內容

事業部別	商品（服務）
資訊安全服務	資訊安全整合性監控及防護服務 資訊安全專業顧問服務 營運不中斷服務
資訊部門營運委外服務	資訊部門營運委外服務

2. 營業比重

單位：新台幣仟元；%

年度 產品名稱	112年度		113年度	
	金額	比例（%）	金額	比例（%）
資訊安全服務	1,558,961	84.52	1,911,686	89.06
資訊部門營運委外服務	285,597	15.48	234,748	10.94
合計	1,844,558	100.00	2,146,434	100.00

3. 公司目前之商品（服務）項目

本公司及子公司 (以下簡稱「合併公司」) 以自有之研發專業技術能力為核心，專注於發展資訊安全相關服務，服務可分為事前預防、事中偵測、事後應變及災變復原。在事前預防時，提供資安管理制度顧問服務，弱點掃瞄、滲透測試、健檢服務及資料與系統備份備原服務；在事中偵測時，透過 SOC 進行全天候 24 小時的監控，並增加備援演練頻率及種類；在事後應變時，則以專業數位鑑識的技術保留證據，以還原攻擊全貌，並啟動緊急備援，執行災變復原程序，以降低災損。

4. 計畫開發之新商品（服務）

為因應日益多樣化的資安威脅態樣，進一步優化自身資安服務品質、切合市場需求，本公司持續投入資源於新興資安服務與解決方案之開發上。

(1) 發展主動式資安監控中心（Intelligent SOC, iSOC）

主動式資安監控中心（Intelligent SOC, iSOC）成為企業資安的新標準，結合 AI 分析、自動化回應、威脅情報整合，提供更快、更準確的威脅偵測與應變能力。運用多種 AI 模型進行日誌分析，涵蓋 IT、OT、雲端等三大環境，針對不同客戶和各種不同設備進行多面向分析，從監控服務客戶端的日誌來源，找出異常的行為，挖掘潛藏資安威脅，實現自動化的偵測、判斷與回應，到整合外部威脅情資來源，提升事前日誌監控分析的精準度。

在事中、事後階段方面，與 SOC 整合的事件調查、鑑識服務、SOAR，以及惡意威脅狩獵分析服務也是重點。

(2) 發展威脅情資 AI 分析平台（ATHENA）

透過每月蒐集的高達 4,000 億筆資料，結合已知資安事件的處理經驗進行監督式學習。這種訓練模型的成果將協助企業有效地預測資安事件的發生，只需新接收到的特定日誌紀錄，即可透過監督學習的結果判定是否為資安事件。這樣的判定過程不僅省卻了事先設計大量規則的需求，更有效地降低了人力投入。

透過引入 AI 技術，將巨量資料與機器學習結合，產生異常偵測（Anomaly Detection）、預測分析（Predictive Analytics）以及歸類（Clustering）等模型，以提高資安事件檢測的效率並彌補現有監控邏輯的不足。同時，我們融入 Green AI 的理念，以節省能源並減少碳足跡。

(3) Cloud SOC 雲端及地端資安監控整合服務

本公司是國內唯一完整整合雲原生資安監控平台與 7x24 資安監控維運服務的資安服務廠商。面對現今企業多採混合雲布局的主流趨勢，安碁資訊更可協助客戶導入雲地整合監控與聯防服務機制，整合多雲與地端的資安監控機制於單一監控服務平台，確保企業資安治理與資安維運的完整性與一致性。透過宏碁雲架構，將微軟 Azure 雲端設備日誌與資料整合平台 API 串接，結合既有 ACSI SOC 核心技術能量，並由安碁資訊專家進行關聯規則建立，監控雲端各種資安設備被刺探的行為，將監控的日誌資料所觸發的「事件」進行彙整，再將「事件」遞送轉

交給地端的安全監控中心（SOC）進行關聯分析，進而比對雲、地所發生的資安事件關聯，雲端日誌不落地，節省大量日誌下載的網路傳輸費用，建立雲地監控中心混合互相回饋循環機制。安碁資訊能夠協助企業由單一環境無痛整合至混合雲，提供更安全可靠的雲端服務，使得企業在雲端服務上的共享資源，擁有更大的彈性與靈活性，捍衛雲地 IT / OT 安全，實現企業永續營運的韌性。

(4) 發展雲端資安監控中心服務（Cloud SOC）

是專門為雲端環境設計的資安事件監控與應變平台，負責監測、分析、應對雲端環境中的各種安全威脅與攻擊。Cloud SOC 的核心目標是透過自動化、安全分析、AI 與零信任技術，確保企業的雲端基礎設施、應用、數據免受網路攻擊的威脅。雲端資安監控的核心技術如下：

- 監控層次與技術
- 資安事件監控
- 威脅偵測與異常行為識別

(5) 發展雲端資安健檢服務

主要目的是幫助企業評估其雲端環境的安全性，識別潛在的漏洞與風險，並提供改進建議。這樣的服務應結合自動化掃描工具、合規要求及威脅情報，確保雲端架構的完整性和安全性。雲端資安健檢核心服務項目如下：

- 雲端基礎設施配置評估
- 雲端數據保護與隱私評估
- 雲端身份與存取管理（IAM）
- 監控與偵測能力
- 應急應變計劃與災難復原

(6) 紅隊演練服務

紅隊演練（Red Teaming）是一種模擬真實攻擊者的資安測試技術，目標是評估組織的資安防禦能力。核心技術涵蓋情報蒐集、滲透測試、橫向移動、數據竊取、持久化存取，目的是找出組織的資安弱點，提升資安應變能力。

(7) 入侵與攻擊模擬服務（Breach and Attack Simulation, BAS）

BAS（Breach and Attack Simulation，入侵及攻擊模擬）是一種自動化攻擊模擬技術，可以持續測試組織的資安防禦能力，並識別安全弱點。BAS 主要模擬真實

攻擊者的行為，但不會影響業務運作，BAS 更具自動化、持續性、可量化分析的優勢。可以自動模擬駭客進行多面向攻擊的一種服務。建構資安監控基準，提升監控中心有效性。

(8) 雲端資安治理解決方案

雲端組態、雲端監控、雲端健診、雲端鑑識與雲端備份（資料加密分持）等五項雲端資安治理解決方案，協助企業在數位轉型提升營運績效之際，共同打造雲端安全的防護力。隨著企業上雲的應用趨勢，整合多雲安全防護也更加重要，安碁資訊在政府、金融、高科技製造業已具備雲地監控整合經驗，從雲端部署、維運監控至雲地兩端關聯分析與情資分享，為客戶在搬遷上雲兼顧雲端安全，提供最佳化的解決方案。

(9) 零信任架構導入服務

零信任架構（Zero Trust Architecture, ZTA）是一種「永不信任，持續驗證」的安全策略，旨在防止內部與外部威脅。與傳統安全模式不同，零信任不假設內部網路是可信的，而是對每個存取請求進行驗證，確保只有合法用戶與設備能夠存取資源。

(10) 整合營運不中斷解決方案

因應駭客勒索黑色產業日益茁壯，復原與備援服務已成為優化與完善本公司提供客戶資安服務所必需，故將整合營運不中斷服務納入資訊安全服務架構，即事前預防-資料與系統備份備援服務、事中偵測-備援演練、事後應變-啟動緊急備援，執行災變復原程序，使整體資安服務架構更為完整，進而強化公司競爭力。

（二）產業概況

1. 產業之現況與發展趨勢

(1) 全球資訊安全產業發展趨勢

全球資訊安全產業的發展趨勢受到數位轉型、人工智慧（AI）、雲端運算、網路犯罪等多重因素影響。以下是幾個關鍵趨勢：

● AI 驅動的資安防禦與攻擊

AI 增強資安能力：企業廣泛採用 AI 和機器學習來自動化威脅檢測、異常行為分析和即時回應，提高資安效率。

AI 驅動的攻擊增加：駭客開始利用 AI 生成更難偵測的網路釣魚（Phishing）攻

擊、Deepfake 社交工程詐騙，以及更精密的惡意軟體變體。

- 雲地端資安整合（Hybrid Cloud Security Integration）

  隨著企業數位轉型的加速，越來越多組織採用混合雲（Hybrid Cloud）架構，結合公有雲（Public Cloud）、私有雲（Private Cloud）和地端（On-Premises）基礎設施。然而，這種混合環境也帶來了新的資安挑戰，包括跨環境的存取控制、數據保護、合規要求、威脅偵測與應變能力等。因此，雲地端資安整合成為企業 IT 安全策略的核心。

- 雲端環境威脅增長

  隨著企業大規模採用公有雲（Public Cloud）、私有雲（Private Cloud）和混合雲（Hybrid Cloud），雲端環境的安全威脅也在急速增長。駭客利用配置錯誤（Misconfiguration）、憑證洩露（Credential Leakage）、API 漏洞、勒索軟體（Ransomware）、供應鏈攻擊等方式，針對雲端基礎設施、應用和數據發動攻擊。

- 零信任架構（Zero Trust）成為標準

  各國政府與企業加速推動「永不信任，持續驗證」的零信任安全模型，確保內外部流量都需經過強身份驗證（MFA）、存取控制與行為監控。零信任網路存取（ZTNA）取代傳統 VPN，提供更精細的存取控管。

- 供應鏈攻擊與 API 安全

  隨著企業 IT 供應鏈複雜化，攻擊者開始針對供應商和第三方 API 進行滲透，造成更大規模的資料外洩與業務中斷。

  API 安全變成資安重點，企業需強化 API 存取控制與流量監控，並導入 API 安全閘道（API Security Gateway）。

- 法規遵循與資安治理強化

  各國政府強化資安法規，如歐盟 NIS2 指令、美國 CISA 指南、新版 ISO27001，企業需加強法規遵循（Compliance）與資安治理。

  資料保護與隱私法規（如 GDPR、CCPA）驅動企業投資於隱私增強技術（PETs），如同態加密、聯邦學習等。

- 勒索軟體（Ransomware）與 MDR（Managed Detection and Response）

  勒索軟體攻擊升級，駭客不只加密資料，還會威脅公開洩漏以施壓支付贖金（Double Extortion）。

  MDR（Managed Detection and Response，受管式偵測與回應是一種托管資安服務，透過 24/7 持續監控、威脅偵測、事件調查及快速回應，協助企業即時發

現並阻止網路攻擊。MDR 結合資安專家（SOC 分析師）、AI 威脅偵測技術和自動化應變機制，即時應對勒索軟體、APT 攻擊、內部威脅等資安事件。

在勒索軟體攻擊頻繁、APT 駭客活動增加、資安人力短缺的環境下，MDR 已成為企業與政府機構的重要資安解決方案，未來更將與 AI、MDR 及雲端資安技術深度融合，提升企業的資安韌性與應變能力。

- 關鍵基礎設施資安防護（Critical Infrastructure Security）

  隨著全球網路攻擊日益頻繁，關鍵基礎設施（Critical Infrastructure，CI）已成為國家級駭客與網路犯罪組織的主要攻擊目標。關鍵基礎設施包含電力、通訊、金融、交通、醫療、供水、政府機構、半導體與製造業等領域，若遭受攻擊，將影響社會運作，甚至威脅國家安全。

- 全球資安市場產值概況

  主要受網路攻擊日益複雜化、地緣政治與供應鏈風險、法規合規要求提升、資安人才短缺等因素驅動，全球資訊安全市場正經歷快速增長，預計 2025 年市場規模將達到 2000 千億美元，2027 年市場規模將達到 2,885 億美元，年複合成長率（CAGR）為 11.9%。

(2) 我國資訊安全產業發展趨勢

根據 Check Point 的數據，臺灣在 2024 年第三季的資安狀況相當嚴峻，每週遭受的攻擊次數高達 4,129 次，這一數字遠超過全球平均的 1,876 次，並且使臺灣成為亞太地區的主要網路攻擊目標。以下是具體情況分析：

A. 產業受攻擊情況

- 硬體供應商：每週平均遭受 7,046 次攻擊，這顯示出對關鍵技術供應鏈的威脅。
- 政府與軍事機構：每週遭受 5,357 次攻擊，這突顯了國家安全領域的重大風險。
- 製造業：儘管相對較少，但仍然面臨顯著的攻擊頻率，強調了工業領域的資安防護需求。

根據臺灣證券交易所與櫃買中心的規範，所有上市櫃公司在發生資安事件時，無論是否涉及核心機密，都必須公開重大訊息。截至 2024 年 11 月底，已有超過 55 家上市櫃公司發布了資安重大訊息，這一數字顯示出資安事件的頻發與其揭露要求的增加。隨著資安事件的揭露，主管機關與資安產業可以更有效地

掌握企業的資安態勢，並加強防護能力。

企業能夠透過同業間的資安事件揭露，進一步強化自身的防禦措施，並加強與同行業的聯防機制，減少資安事件的風險。

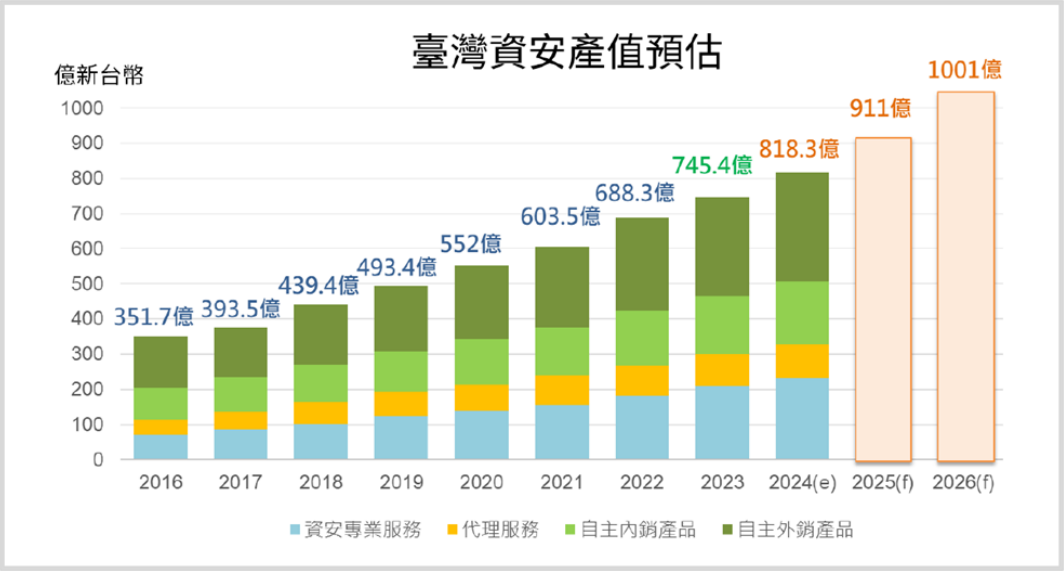
在企業面對的主要資安事件類型中，勒索軟體攻擊依然是最常見且危害最大的。這類攻擊已變得更加普及，主要原因在於網路犯罪的「服務化」盛行，讓有心人士能輕易獲得各種攻擊工具和洗錢管道，進而提高了勒索軟體攻擊的頻率與成功率。這些攻擊不再局限於大型企業或特定行業，無論規模大小的企業、個人或組織都有可能成為攻擊目標，且由於贖金的誘因，使得越來越多網路犯罪者選擇這種攻擊方式。

除了勒索軟體攻擊外，零時差漏洞也是企業面臨的重要資安威脅。對於台灣這樣的 ICT 製造大國來說，網路設備和聯網產品的安全漏洞已經成為重大問題。例如，奇偶科技的視訊監控設備、兆勤科技的無線基地台和資安路由器設備，以及中華電信提供的 D-Link 數據機，都曾經發現存在零時差漏洞。這些設備即便已經停止支援，但許多舊型設備仍在使用中，成為駭客攻擊的目標。這類漏洞的存在提醒企業要加強對安全漏洞的監控和修補，同時設備供應商也有責任提醒和教育客戶及時更新或更換有資安風險的設備。

至於政府機構，今年最重大的資安事件之一就是大規模的 DDoS 攻擊。2024 年 9 月，至少 45 個政府單位與企業遭受到 DDoS 攻擊，這些攻擊是由親俄駭客組織 NoName057 發動的，這次攻擊波及台灣的政府機構及企業，甚至包括金融業、半導體大廠及電子廠商，但幸好並未造成過多影響。

B. 台灣資安市場概況

臺灣資安廠商家數大約 368 家左右，以資安系統整合或代理服務 138 家、資安專業服務（顧問服務、數位鑑識服務）約 66 家、網路安全約 51 家佔較多數。自 2017 年開始，臺灣資安產業每年平均成長率 11.82%，高於全球平均 9%。2024 年臺灣資安產業因駭客攻擊事件使資安服務、上雲需求大幅成長，但同時，資安服務化趨勢，使純代理或硬體系統成長減緩，綜合使 2024 年資安產業成長 9.8%，產值達新臺幣 818.3 億元，預期 2026 年資安產業產值將上看新臺幣 1,000 億元以上。（資料來源：工研院）



資料來源：工研院產科國際所(2024/12)

目前台灣資安產業以硬體出口為主，包括防火牆、高速網路安全平台、指紋辨識 IC、可信任平台模組（TPM）、IoT 安全閘道器等。

網路安全次產業（242.5 億）與終端與行動裝置防護（165 億）產值均超過百億元，主要受雲端與高速網路設備需求推動。硬體產值佔比下降，從 2016 年 57% 下降至 2024 年 50.4%。資安服務產值由 2023 年 299 億成長至 2024 年 327 億，成長 9.4%。

企業因應勒索軟體攻擊，增加資安系統建置或採取資安外包服務，帶動資安代理服務與資安營運管理服務(SOC)需求成長。資安服務佔整體產值比重從 2016 年 31.9%上升至 2024 年 40%，逐步接近國際標準。

企業開始採用滲透測試、弱點掃描、攻防演練、程式碼檢測、威脅情資分析與分享等服務。資安營運監控（SOC）、攻擊聯防通報、緊急應變處理、資安事件災害復原、自動化防護（SOAR）等需求成長。

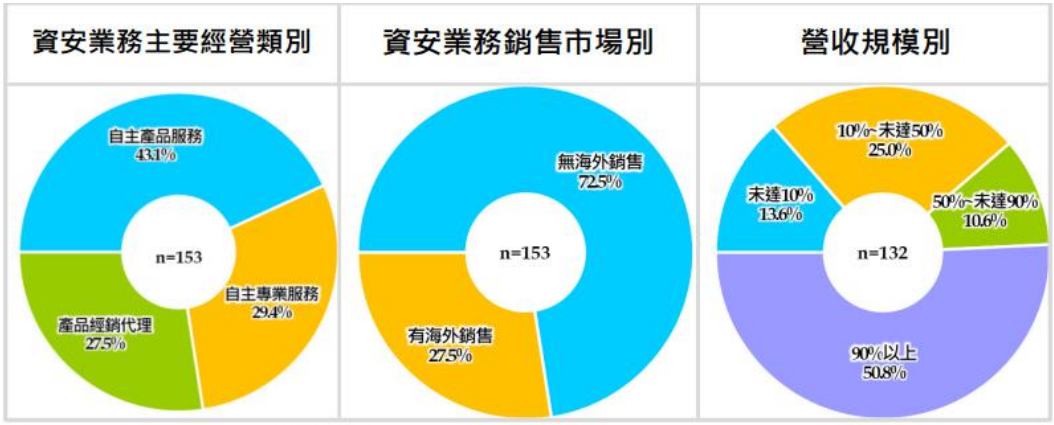
政府推動資安檢測標準，協助法人與企業建立資安檢測實驗室，提升 ICT 產品資安檢測能量。針對資通防禦、網路接取、智慧行動裝置、智慧連網設備等類別進行資安檢測，並要求政府採購案符合資安標準。

台灣資安產業正由硬體導向逐步轉向資安服務與聯防機制，企業對資安專業服務、SOC 監控、資安事件應變的需求日益增加，政府亦強化 ICT 產品的資安檢測規範，帶動資安服務市場的持續成長。

依據工研院臺灣資安產業調查報告，以資安產業鏈上、中、下游與產品服務型

態進行分類。資安產業鏈上中下游方面，上游為提供資安產品，包括終端、網路、雲端等應用場景的防護產品與服務外，加上物聯網安全；而中游資安營運服務類，則包括日常營運服務的資安營運管理服務及資安專業顧問類，如資安檢測服務、資安顧問服務、資安鑑識服務等；最後再到下游與用戶直接面對面的資安支援服務體系，包括國內外資安產品服務代理銷售、系統整合服務、資安教育以及資安保險服務等。其中，超過 3 成的自主業者經營範疇提供「網路安全防護產品」及「資安檢測分析服務」是為最多。超過 6 成的代理業者經營範疇提供「網路安全防護產品」，其次亦有近 5 成的業者提供「終端防護產品或服務」與「網路安全檢測防護產品」。

臺灣資安產業基礎樣貌



資料來源：工研院產科國際所(2024/12)

2024 臺灣資安各子產業發展現況（資料來源：工研院）

- 終端與行動裝置防護產值 165 億元 (+8.6%)，受遠距辦公需求驅動，身分與存取管理 (IAM)、零信任解決方案成長多因子驗證 (MFA)、生物辨識模組、安全晶片需求增加，端點偵測與回應（EDR）。
- 網路安全產值 242.5 億元 (+5.9%)，UTM、IDS/IPS 需求仍在，但受企業上雲影響，設備投資成長趨緩。
- 資料與雲端應用安全產值 45 億元 (+16.3%)，隨著企業數位轉型，雲端安全防護成為關鍵。
- 物聯網安全產值 50.6 億元 (+24.7%)，針對 ICS（工業控制系統）的資安需求成長，因 IT/OT 融合增加攻擊風險。
- 資安營運管理服務（SOC）產值 93.5 億元 (+14.9%)，企業委外 SOC 監控需求增加，包括早期預警、事件通報、緊急應變。
- 資安專業服務產值 98.5 億元 (+13.5%)，企業導入 AI 偵測、數位鑑識、異

地備援，確保資安事件證據保全。

- 資安系統整合與代理服務產值 117.9 億元 (+5.2%)，企業資安採購依賴系統整合商與代理商，市場持續擴展。
- 資安教育與保險產值 5.3 億元 (+2.5%)，資安教育訓練需求增長，但資安保險發展仍受限。

2024 年台灣資安市場穩健成長，雲端安全、物聯網安全、資安營運管理、EDR 成為主要增長領域。

2. 產業上、中、下游之關聯性

資訊安全服務產業之上、中、下游關聯圖：

上游-資安產品	中游-資安營運服務	下游-用戶直接面對面的資安支援服務體系
包括終端、網路、雲端物聯網等應用場景的防護產品	包括日常營運服務的資安營運管理服務及資安專業顧問類，如資安檢測服務、資安顧問服務、資安鑑識服務等	包括國內外資安產品服務代理銷售、系統整合服務、資安教育以及資安保險服務等。

3. 產品之各種發展趨勢及競爭情形

(1) 產品未來發展趨勢

2025 年的資安技術發展趨勢將圍繞著更強的自動化、AI 驅動的防禦機制，以及

應對雲端與供應鏈威脅的新策略。以下是幾個主要趨勢：

A. 主動式資安監控中心（Intelligent SOC）

主動式監控智能中心（Intelligent SOC, iSOC）成為企業資安的新標準，結合 AI 分析、自動化回應、威脅情報整合，提供更快、更準確的威脅偵測與應變能力。

運用多種 AI 模型進行日誌分析，涵蓋 IT、OT、雲端等三大環境，針對不同客戶和各種不同設備進行多面向分析，從監控服務客戶端的日誌來源，找出異常的行為，挖掘潛藏資安威脅，實現自動化的偵測、判斷與回應，到整合外部威脅情資來源，提升事前日誌監控分析的精準度。在事中、事後階段方面，與 SOC 整合的事件調查、鑑識服務、SOAR，以及惡意威脅狩獵分析服務也是重點。

B. AI 驅動的資安防禦

- AI 與機器學習威脅偵測：更強的 AI 模型將被用來偵測異常行為，快速識別進階持續性威脅（APT）。
- 自動化事件回應（SOAR）：透過安全協調、自動化和回應（SOAR）技術，提升資安團隊處理威脅的速度與準確度。
- AI 生成攻擊（AIGC 攻擊）防禦：針對 AI 生成的社交工程攻擊（如 Deepfake 釣魚郵件）的新防禦機制。

C. Cloud SOC 雲端及地端資安監控整合

隨著企業數位轉型加速，雲端環境與地端 IT 環境的整合資安監控成為關鍵挑戰。傳統 SOC 主要監控內部網路與端點，但現在需要擴展到 AWS、Azure、GCP、SaaS、Kubernetes、無伺服器架構（Serverless）等多雲環境。

Cloud SOC 透過 SIEM（安全資訊與事件管理）、MDR（擴展偵測與回應）、SOAR（安全協同自動化）、雲端原生安全監控，整合雲端與地端資安事件，提供統一的可視性與自動化回應能力。

D. 端點與零信任安全（Zero Trust）深化

- 雲端原生資安技術：企業將更依賴「雲端存取安全代理（CASB）」與「雲端工作負載防護平台（CWPP）」來確保多雲環境的安全。
- 零信任架構普及：企業將採用「持續驗證」與「最小權限」機制，確保即使內部用戶也無法無限制存取敏感數據。
- 身份與存取管理（IAM）升級：隨著無密碼身份驗證技術（如 FIDO2、行為

生物識別）的進步，企業將逐步淘汰傳統密碼登入。

E. 建構雲端資安監控基準（Cloud Security Monitoring Baseline）

隨著企業向雲端遷移，確保雲端環境的安全變得至關重要。傳統資安監控方法已無法滿足動態、分散的雲端架構，因此需要建立雲端資安監控基準（Cloud Security Monitoring Baseline），確保從基礎架構到應用層的全面防護。

雲端資安監控基準框架可參考國際標準與最佳實踐來建立監控基準，如 CIS Benchmarks、NIST 800-53、ISO27001、MITRE ATT&CK Cloud Matrix。

- 身分與存取監控基準
- 網路安全監控基準
- 應用程式與 API 監控基準
- 雲端工作負載與端點監控基準
- 資料安全監控基準
- SIEM 與 MDR 監控基準

F. 供應鏈與物聯網（IoT）安全挑戰加劇

- 軟體供應鏈安全：隨著開源軟體與第三方程式庫的廣泛使用，企業需要採用「SBOM（軟體物料清單）」來強化軟體供應鏈管理。
- 5G 與 IoT 裝置安全：隨著 IoT 裝置普及，攻擊者可能透過 5G 網路入侵工業控制系統（ICS），需要更強的網路分段與設備認證機制。
- OT（營運技術）與 IT 融合安全：工業控制系統（ICS）與 IT 網路融合，使工業物聯網（IIoT）更容易成為攻擊目標，企業需加強關鍵基礎設施的防禦機制。

G. 發展主動式防禦系統（Active Defense）：交戰、阻斷、欺敵技術

隨著攻擊者手法不斷進化，企業的防禦策略也需從被動監控（Passive Defense）轉向主動防禦（Active Defense）。主動式防禦不僅關注威脅偵測，更強調攻擊交戰、即時阻斷、欺敵技術，有效降低攻擊成功率，並反制駭客行動。

MITRE Engage 定義的交戰、阻斷、欺敵領域，主要是把 APT 攻擊狙殺鏈應對技術，從「被動偵測防禦」進化至「與攻擊者接觸交戰」，並且主動欺騙、防禦、反制，讓企業資安體系從單純的威脅偵測與防禦，發展到干擾攻擊者活動、獲取攻擊情資、控制攻擊者，徹底扭轉被動態勢。

運用既有邊界防禦再搭配內部部署的欺敵（Deception）系統實作，讓攻擊者只要失誤一次就會被發現，如此才有能力把被動防禦轉換為主動。欺敵系統具備學習與融入既有 IT 環境的能力，例如依據內部網路配置邏輯，增設不存在的網段，用以製造陷阱誘敵深入，誘使攻擊者竊取偽裝的機敏資料，同時惡意行徑也隨之曝光。

當思惟從被動偵測防禦改成與攻擊者接觸交戰，戰術上便會有干擾入侵活動，抑或是運用誘餌中夾帶可發出訊號的機制，攻擊者開啟當下訊號主動回傳到 SOC 監控中心，即可追蹤攻擊者的所在位置。誘敵深入後掌握情資再對應到 MITRE ATT&CK 知識庫，則可釐清攻擊活動手法、影響範圍，即時調整防禦措施來應對，讓過去的反應式防護體系與主動式技術相互融合。

H. 使用人工智慧和機器學習來分析和預測網路安全威脅是近年來的重要趨勢

網路攻守雙方運用 AI 技術愈加普遍，這些技術用於改善威脅檢測和回應時間，以及自動執行重複和耗時的任務，使安全團隊能夠專注於更具戰略性的計畫。應用技術包括：

- 威脅情資預測：AI 和 ML 將用於分析來自各種來源的大量數據，以便在網路攻擊發生之前預測和預防網路攻擊。這將涉及使用來自各種來源的數據，包括使用者行為、網路活動和安全事件，以構建可以識別新出現的威脅和漏洞的模型。
- 自動威脅回應：AI 和 ML 將用於自動回應安全威脅，減少組織回應事件所需的時間，並將攻擊的影響降至最低。這可能包括自動隔離受感染的系統、隔離受感染的帳戶或刪除惡意代碼。
- 詐騙檢測與預防：AI 和 ML 將用於檢測和防止欺詐活動，例如網路釣魚攻擊、帳戶接管嘗試和其他類型的金融犯罪。這將涉及使用來自多個來源的數據，包括用戶行為、交易歷史和網路活動，以構建可以即時識別和防止欺詐活動的模型。
- 安全行為分析：AI 和 ML 將用於分析大量安全數據，以識別使用模式和相關性，從而幫助組織做出更明智的安全決策。這將涉及使用來自多個來源的數據，包括安全日誌、網路活動和用戶行為，以識別可能表明安全威脅的趨勢和異常。

I. 勒索軟體與社交工程攻擊進化

- 雙重/多重勒索攻擊：攻擊者不僅加密數據，還會威脅公開企業機密，增加勒索談判籌碼。
- AI 生成的社交工程詐騙：生成式 AI 將讓詐騙郵件、Deepfake 影片更難以識別，企業需加強員工資安意識培訓與反詐騙技術。
- 區塊鏈技術應用於勒索防禦：企業可能會利用區塊鏈記錄數據完整性，防止勒索軟體篡改數據。

(2) 競爭情形

資訊安全服務業是技術密集及專業度高的產業，就目前國內而言，資安服務廠商包含系統整合商、資安顧問公司、資安服務專業公司及電信業者眾多經營型態業者，大部份只能提供部份資安服務。惟隨資安威脅面向多元，資安防護整合需求日趨殷切，安碁資訊是目前可同時提供 SOC 營運、資安資訊分享分析建置與監控服務（ISAC）、資安檢測、鑑識與顧問服務予客戶之高度整合資安服務專業公司，取得多項國際級專業認證，尤其 SOC 下設之數位鑑識實驗室係目前國內唯一通過 ISO17025 實驗室認證者，所出具之鑑識報告可為國際所承認，故具備相當之競爭優勢。未來除加強維持與既有客戶之緊密關係，本公司亦將積極提升專業技術及其競爭力，建立差異化的服務特色。

安碁資訊亦憑藉長期服務累積之客戶端實務作業資料，積極通過迴歸分析、分類分群、圖形辨識、近似度分析等技術之應用及本公司技術專家之專業知識投入、案例與趨勢研究、平台與系統之優化及回饋以發展高度切合實務應用需求並具備即時性之關聯性分析規則，俾使現有資訊安全服務得以進一步智慧化，以因應日益增加的資安威脅態樣，使偵防機制趨於主動。

此外，在基礎建設運營及生產流程自動化、智慧化趨勢下，資訊科技（Information Technology, IT）及維運科技（Operation Technology, OT）領域的重合度增加、過去主要見於 IT 領域之資安威脅亦擴及 OT 領域，惟因 OT 與廠商的生產活動密切相關，其系統之穩定性要求較 IT 更高，在運作中不容中斷、且囿於生產效率性考量，傳統 IT 資安防護體系下之停機檢修、系統更新作業模式難以適用於 OT 領域。

從而，較諸傳統資安服務廠商所聚、主要涵蓋電腦等端點設施、網路及伺服器資安偵防之 IT 領域，涉及關鍵基礎建設、生產設備與機械運作之 OT 領域資安防護過去所受重視程度較低，但其資安漏洞造成的潛在經濟損失與社會成本鉅大。因

此，安碁資訊在 OT 領域資安解決方案上，亦發展 TestBed 平台，利用客戶端提供之實際 OT 系統配置資訊，建構高度近似之作業環境，從而得以在不干擾實際營運及生產活動下進行資安防護機制評估、弱點分析，並發展切合實務需要之解決方案。

本公司依「行動應用 App 基本資安自主檢測推動制度」規範，將行動應用 App 基本資安檢測納入實驗室服務項目，檢測基準採用工業局制定之「行動應用 App 基本資安檢測基準」辦理，並通過全國認證基金會（TAF）國際 ISO17025 測試實驗室認證（實驗室編號：3334），提供客戶國際水準之檢測專業服務。

（三）技術及研發概況

1. 所營業務之技術層次及研究發展

(1) 所營業務之技術層次

資安營運服務商（Managed Security Service Providers, MSSP）的技術層次通常可以分為以下幾個層面，涵蓋從基礎監控到高階威脅獵捕與應變：

A. 基礎監控與管理層

- 防火牆與入侵偵測系統（IDS/IPS）管理：設定、維護與監控網路安全設備。
- 安全日誌管理（Log Management）：集中收集來自不同設備的安全日誌，如防火牆、端點防護、應用程式等。
- 弱點掃描與補丁管理：定期執行系統與應用程式的弱點掃描，並提供修補建議。
- 身分與存取管理（IAM）：確保權限分配正確，避免未授權存取。

B. 進階安全監控層（SOC）

- 安全事件監控與分析（SIEM）：透過安全資訊與事件管理（SIEM）平台，即時分析日誌，偵測異常行為。
- 行為分析（UEBA）：透過使用者和實體行為分析（UEBA）技術，偵測異常行為模式，如帳號濫用或內部威脅。
- 端點偵測與回應（EDR）：監控端點活動，及時攔截惡意攻擊。
- 網路偵測與回應（NDR）：監控網路流量，發現異常模式，如 C2（Command & Control）活動。

C. 威脅情報與應變層

- 威脅情報（Threat Intelligence, TI）: 收集外部與內部威脅情報，提高預測與防禦能力。
- 主動威脅獵捕（Threat Hunting）: 透過行為分析與威脅情報，主動尋找潛在攻擊者。
- 數位鑑識與應變（DFIR）: 發生資安事件時，提供數位鑑識調查與應變服務。
- 勒索軟體與惡意軟體分析：針對惡意檔案進行靜態與動態分析，以制定應對策略。

D. 雲端與零信任安全層

- 雲端安全監控（CSPM、CWPP）: 針對雲端環境提供安全組態管理與工作負載保護。
- 零信任架構（Zero Trust Security）: 透過微分段（Microsegmentation）、存取控制等技術，降低內部橫向移動風險。
- API 安全防護：監控 API 存取行為，防範 API 攻擊與資料外洩。
- SASE（Secure Access Service Edge）: 結合 SD-WAN 與雲端安全服務，確保遠端與分散式存取安全。

E. 合規與風險管理層

- 合規管理（Compliance Management）: 協助企業符合 ISO27001、NIST、GDPR、PCI-DSS 等資安標準。
- 風險評估與管理（Risk Assessment & Management）: 透過風險分析，提供策略建議以降低潛在威脅。
- 紅隊演練與滲透測試（Red Teaming & Penetration Testing）: 模擬攻擊情境，檢測企業防禦能力。

(2) 研究發展

A. 發展主動式資安監控中心（Intelligent SOC）

研發主動式 SOC 的核心能力

a. 威脅情報整合與分析

- 整合全球威脅情報（Threat Intelligence, TI）識別最新攻擊趨勢
- 跨雲與地端環境的資安情資共享（如 MISP、STIX/TAXII）
- 攻擊特徵比對與關聯分析（如 MITREATT&CK 框架）

b. AI 驅動的威脅偵測

- 使用 AI/ML 進行行為分析（UEBA），檢測異常存取與攻擊模式
- 利用大數據 SIEM/XDR 分析內部異常流量與跨層級攻擊行為
- 自主學習異常模式，降低誤報與漏報

c. 威脅獵捕（Threat Hunting）

- 基於 MITRE ATT & CK 進行主動式威脅搜尋，不依賴已知攻擊特徵
- 紅隊與藍隊演練，模擬駭客攻擊路徑
- 使用記憶體分析、網路封包分析、端點遙測（EDR）等方式發掘隱藏威脅

d. 自動化應變與修復（SOAR）

- 資安協同自動化（SOAR），根據攻擊情境自動執行應變措施
- 即時阻斷惡意 IP、帳戶停權、封鎖惡意程序
- 自動回應機制：不同攻擊情境對應不同應變流程

e. 雲端與地端安全整合

- 雲端 SOC（Cloud SOC）整合多雲環境（AWS、Azure、GCP）
- 邊緣端點偵測（EDR/XDR）與 OT/IoT 資安監控
- 零信任架構（Zero Trust）確保設備、使用者與應用程式安全

B. 發展 AI 在資安領域的應用與技術發展

- 威脅檢測與回應：AI 能即時監控網路和系統，分析大量數據以快速偵測和回應威脅。這包括識別異常行為模式，預測潛在攻擊，並自動化威脅回應。
- 惡意程式偵測：AI 演算法可以分析檔案特性和行為模式，偵測惡意程式。這些演算法能夠比傳統方法更快、更準確地識別新型惡意軟體。
- 行為分析：AI 能分析使用者和系統的行為，發現可能意味著資安威脅的異常情況，從而提前預防攻擊。
- 自動化資安工作：AI 可以自動化例行性資安工作，如威脅偵測和事件回應，讓資安人員專注於更複雜的任務。
- 漏洞挖掘：AI 技術被用來發現和修補軟體漏洞，提升軟體開發的安全性。例如，AI 可以幫助縮小漏洞範圍，並加速漏洞修補過程。
- 深度偽造防護：AI 技術也被用來識別和防止利用假視頻和音頻進行的詐騙和身份冒充。

C. 發展 Cloud SOC 雲端及地端資安監控整合機制

需要結合 SIEM、EDR、NDR、SOAR、威脅情報（TI）等技術，打造具備即時監控、主動威脅偵測、自動應變的雲地聯防資安監控運營中心。

a. 多雲資安監控（AWS, Azure, GCP, Private Cloud）:

- 整合 CSPM（Cloud Security Posture Management）與 CWPP（Cloud Workload Protection）。
- 混合環境監控(Hybrid SOC): 透過 SIEM 監控企業內部與雲端資安日誌，確保可視性。
- 端點與網路整合（EDR+NDR）: 同步偵測端點與網路異常行為，提升攻擊識別能力。

b. 分層防禦架構

- L1：自動監控（SOC 基礎層）→即時告警，統一管理 SIEM 日誌。
- L2：事件分析（進階資安分析）→AI 驅動異常行為分析，進行深度威脅調查。
- L3：應變處理（資安應變與獵捕）→威脅獵捕、攻擊溯源、事件回應。

D. 發展雲端資安監控技術

是確保雲端環境中資料、應用和基礎設施的安全性，對於企業保護其雲端基礎設施免受各類攻擊與威脅至關重要。隨著企業將更多業務遷移到雲端，這些監控技術需要有針對性地涵蓋不同層級的資安防禦，並具備強大的即時偵測與反應能力。雲端資安監控的核心技術如下：

a. 監控層次與技術

- 基礎設施監控：針對雲端基礎設施（如虛擬機、容器、存儲、網絡等）進行監控，及時發現異常情況。
- 虛擬化層監控：如 VMware vSphere、Kubernetes 集群，及時偵測容器與虛擬機的異常行為。
- 網絡監控：監控雲端環境中的流量，識別異常流量模式，使用工具如 AWS VPC Flow Logs、Azure Network Watcher，實現網絡層的安全監控。
- 應用監控：針對雲端部署的應用進行實時監控，確保其運行正常並未受到攻擊。
- 應用層監控：使用 APM（應用程式性能管理）工具（如 Dynatrace、New

Relic）來監測雲端應用的運行狀態，檢測安全漏洞或性能問題。

- 身份和存取管理（IAM）監控：監控和分析雲端環境中用戶身份與存取權限的變更，預防未授權訪問。
- 權限管理與審計：如 AWS IAM、Azure AD，進行用戶、群組和角色的存取控制，並記錄所有的權限變更與異常活動。

b. 資安事件監控

- 安全軌跡與事件管理（SIEM）：將多個數據源（如防火牆、入侵檢測系統、系統日誌等）集中到一個平台，進行實時分析，偵測安全事件。
- AWS GuardDuty：用於監控 AWS 環境中的潛在威脅，識別不尋常的 API 活動、未授權訪問等。
- Azure Sentinel：Azure 的 SIEM 解決方案，用於實時分析與偵測雲端環境中的安全事件。
- AWS CloudTrail、Azure Activity Logs：這些工具記錄雲端操作的詳細日誌，並支持異常行為檢測。
- CloudWatch Logs（AWS）或 Log Analytics（Azure）可以對日誌數據進行收集、篩選與分析，提供安全事件的詳細背景。

c. 威脅偵測與異常行為識別

- 機器學習與 AI 偵測：利用 AI 與機器學習技術對資安數據進行分析，發現潛在威脅與異常行為。
- AWS Macie：基於機器學習的數據安全服務，可以識別敏感數據並警告可能的泄露事件。
- Azure Defender：利用 AI 偵測雲端基礎設施中潛在的異常行為，如未經授權的數據存取或配置錯誤。
- 行為分析與用戶端偵測（UEBA）：UEBA 工具（如 Sumo Logic、Exabeam）能基於用戶行為模式識別可疑行為或潛在的內部威脅。
- CloudTrail 和 GuardDuty 可以幫助識別不尋常的 AWS API 調用模式或身份竄改。

E. 研發雲端資安監控基準

隨著企業向雲端遷移，確保雲端環境的安全變得至關重要。傳統資安監控方法已無法滿足動態、分散的雲端架構，因此需要建立雲端資安監控基準（Cloud

Security Monitoring Baseline），確保從基礎架構到應用層的全面防護。

雲端資安監控基準涵蓋身分與存取、網路安全、應用程式與工作負載、資料保護、安全日誌與事件管理（SIEM）、威脅偵測與回應（MDR）等領域。雲端資安監控基準框架，可參考國際標準與最佳實踐來建立監控基準，如 CIS Benchmarks、NIST 800-53、ISO27001、MITRE ATT&CK Cloud Matrix。

a. 身分與存取監控基準

- 最小權限原則（Least Privilege）: 監控高權限帳戶（如 AWS Root、Azure Global Admin）是否有異常行為。
- 多重驗證（MFA）強制執行：監控所有管理帳戶是否開啟 MFA，防止憑證竊取。
- 異常存取行為分析（UEBA）: 檢測帳戶是否從異常 IP、國家、設備登入，並觸發警報。

b. 網路安全監控基準

- 雲端防火牆與網路分段：確保 VPC/VNET 的網路規則符合零信任原則。
- 異常流量偵測：分析 VPC Flow Logs、CloudArmor、WAF 日誌，識別潛在攻擊。
- DDoS 防禦機制：啟用 AWS Shield、Azure DDoS Protection，確保雲端應用可用性。

c. 應用程式與 API 監控基準

- API 存取異常監控：檢測 API 過度請求、未授權存取行為。
- 自動化憑證輪換：確保 API Key、OAuth Token 具備自動輪換機制，降低外洩風險。
- 應用日誌分析：使用 WAF、應用日誌（如 CloudTrail、Azure Monitor）識別異常行為。

d. 雲端工作負載與端點監控基準

- 雲端主機端點防護（EDR）: 確保 EC2、VM、Kubernetes 節點均部署 EDR/CWPP。
- 檔案完整性監控（FIM）: 監控雲端 VM、Serverless 是否有異常變更，防篡改攻擊。

- 零信任存取控制（ZTNA）。

e. 資料安全監控基準

- 數據存取日誌：監控的存取紀錄，避免資料洩露。
- 自動化數據分類與加密：透過 AWS Macie、Azure Purview、Google DLP 自動識別機敏數據並加密。
- 異常資料傳輸監測：監控大規模資料下載行為，防止內部資料外洩。

f. SIEM 與 MDR 監控基準

- 統一日誌管理：確保雲端與地端日誌整合至 SIEM。
- 跨平台關聯分析：將 IAM、網路、API、端點、資料存取等資訊串聯，偵測 APT 攻擊。
- 自動化回應（SOAR）：根據攻擊行為自動執行隔離、帳戶停用、流量封鎖等應變措施。

F. 發展雲端資安健檢技術

主要目的是幫助企業評估其雲端環境的安全性，識別潛在的漏洞與風險，並提供改進建議。這樣的服務應結合自動化掃描工具、合規要求及威脅情報，確保雲端架構的完整性和安全性。雲端資安健檢核心服務項目如下：

a. 雲端基礎設施配置評估

- CSPM（Cloud Security Posture Management）：檢查雲端服務提供商（AWS、Azure、GCP）的資安設置，確保資源符合最佳實踐。
- 虛擬機、容器、存儲資源的配置：檢查不當設定，如開放的端口、不正確的 IAM 政策等。
- 自動化掃描：自動化評估虛擬機、容器、API、網路等的安全配置，確保沒有不必要的風險。

b. 雲端數據保護與隱私評估

- 數據加密：檢查靜態數據與傳輸中的數據是否使用強加密方法。
- 數據存取控制：確認只有授權人員能夠存取敏感資料，並進行審計。
- 隱私合規性：檢查是否符合 GDPR、CCPA 等隱私保護法規。

c. 雲端身份與存取管理（IAM）

- 權限最小化原則：檢查 IAM 設定，確保使用者與應用程序的權限最小化，

並實施多重身份驗證（MFA）。

- IAM 審計：評估存取控制是否存在過度授權或錯誤的權限設置。

d. 監控與偵測能力

- 事件監控：評估雲端監控系統的設定，確保能夠及時捕捉安全事件。
- 異常行為分析：透過 AI 驅動的工具檢測異常流量和活動，及早發現威脅。
- 整合 SIEM 和 MDR：檢查是否將所有雲端日誌集成到 SIEM 系統中，並提供實時警報。

e. 應急應變計劃與災難復原

- 災難復原測試：檢查雲端環境的恢復策略，確保在遭遇攻擊或故障時，業務可以迅速恢復。
- 自動化應急回應：評估是否已部署 SOAR 自動化應變流程。

G. 發展紅隊演練技術

紅隊演練（Red Teaming）是一種模擬真實攻擊者的資安測試技術，目標是評估組織的資安防禦能力。核心技術涵蓋情報蒐集、滲透測試、橫向移動、數據竊取、持久化存取，目的是找出組織的資安弱點，提升資安應變能力。

a. 情報蒐集（Reconnaissance）

紅隊透過開源情報（OSINT）與主動掃描來收集目標資訊，以利規劃攻擊路徑。

(a) 開源情報蒐集（OSINT）

- Google Hacking/Dorking（搜尋敏感資料）
- Shodan/Censys（掃描目標設備資訊）
- theHarvester（收集電子郵件、子域名、IP 等）
- Maltego（關聯式情報分析工具）

(b) 網路掃描與分析

- Nmap/Masscan（端口與服務掃描）
- Amass/Sublist3r（子域名發現）
- WhatWeb/Wappalyzer（Web 應用指紋分析）

b. 初始滲透（Initial Access）

攻擊者透過社交工程或技術漏洞獲取初步存取權限。

(a) 社交工程攻擊（Social Engineering）

- 釣魚攻擊（Phishing）：Gophish、Evilginx（代理攻擊 MFA）
- USB 攻擊：Rubber Ducky、BadUSB
- 語音詐騙（Vishing）：冒充 IT 支援獲取憑證

(b) 漏洞利用（Exploitation）

- Web 應用漏洞（SQLi、XSS、RCE）：SQLmap、Burp Suite
- 外部服務漏洞（VPN、RDP）：Metasploit、Cobalt Strike
- Zero-Day/N-Day 漏洞：利用 Exploit DB 或 CVE

c. C2 指揮與控制（Command & Control, C2）

紅隊確保入侵成功後可以持續控制受害者機器。

d. 權限提升（Privilege Escalation）

紅隊利用系統漏洞或錯誤設定提升權限，以獲取更高級存取權限（如 Administrator 或 root）。

e. 橫向移動（Lateral Movement）

紅隊在內部網路中擴展影響範圍，從一台機器移動到更多內部系統。

(a) Active Directory（AD）攻擊

- BloodHound（分析 AD 權限關係）
- Pass-the-Hash（PTH）（使用 NTLM Hash 進行身份驗證）
- Kerberoasting（攻擊 AD 服務帳號）
- DCsync/DCshadow（Active Directory 主控權劫持）

(b) 內網滲透技術

- SMB 傳播→CrackMapExec、PsExec
- RDP 劫持→Mimikatz、Rubeus
- SSH 橫向移動→SSH Key 竊取
- VPN 滲透→OpenVPN 憑證盜取

f. 數據竊取（Data Exfiltration）

紅隊在攻擊最後階段會將敏感數據透過隱蔽管道傳輸到外部。

(a) 數據壓縮與加密

- 7zip/WinRAR（壓縮並加密文件）
- PowerShell/Python（加密傳輸）

(b) 隱蔽數據傳輸

- FTP/SFTP 上傳
- DNS 隧道（IODINE、DNSCat2）
- 雲端同步（Rclone：Google Drive/Dropbox 傳輸）

g. 持久化存取（Persistence）

紅隊確保即使系統重啟或憑證變更後仍能存取內部網路。

h. 攻擊痕跡清除（Covering Tracks）

為避免被資安團隊偵測，紅隊會刪除相關記錄。

H. 發展入侵及攻擊模擬 BAS（Breach and Attack Simulation）技術

BAS（Breach and Attack Simulation，入侵及攻擊模擬）是一種自動化攻擊模擬技術，可以持續測試組織的資安防禦能力，並識別安全弱點。BAS 主要模擬真實攻擊者的行為，但不會影響業務運作，BAS 更具自動化、持續性、可量化分析的優勢。BAS 平台透過模擬攻擊技術來測試組織的資安狀態，涵蓋以下幾個核心功能：

- 持續性測試（Continuous Testing） 透過自動化攻擊模擬，定期檢測資安系統的防禦能力
- 攻擊路徑分析（Attack Path Mapping） 識別可能的攻擊途徑，如橫向移動、特權提升、數據外洩
- 資安控制驗證（Security Control Validation） 測試防火牆、EDR、XDR、SIEM、DLP 是否能成功阻擋攻擊
- MITREATT&CK 對照（MITRE ATT&CK Alignment） 基於 MITRE ATT&CK 框架，模擬 APT（Advanced Persistent Threat）攻擊技術
- 風險評分與報告（Risk Scoring & Reporting） 透過數據分析，提供可操作的風險報告與修復建議

I. 發展威脅情資 AI 分析平台（ATHENA）

透過每月蒐集的高達 4,000 億筆資料，可結合機器學習（ML）、自然語言處理（NLP）與威脅情報（Threat Intelligence, TI）技術，打造自動化、精準的資安威脅分析系統。以下是關鍵技術架構與發展方向：

a. 威脅情資收集與解析

(a) 多來源情報整合

- 開源情報（OSINT）: 監控暗網（Dark Web）、論壇、社群媒體、資安部落格等。
- 企業內部情報（Internal TI）: 整合 SIEM、EDR、NDR、端點日誌等內部數據。
- 商業情報(Commercial TI): 串接威脅情報供應商(如 Recorded Future、VirusTotal、IBM X-Force)。

(b) NLP 驅動情報解析

- 自動化關鍵字提取（Keyword Extraction）: 辨識攻擊者名稱、攻擊手法（TTPs）、CVE 編號等。
- 實體關係圖譜（Knowledge Graph）: 分析攻擊組織與其基礎架構（IP、域名、惡意程式）。
- 情境分析（Sentiment Analysis）: 透過 NLP 判斷攻擊意圖與影響範圍。

b. AI 驅動威脅分析

(a) 機器學習偵測

- 異常行為分析(UEBA): 偵測使用者與系統的異常行為，例如異常登入、橫向移動攻擊。
- 惡意流量分類（Malware Traffic Classification）: 透過深度學習識別 C2（Command & Control）流量。
- 攻擊預測模型（Attack Prediction Models）: 基於 MITRE ATT&CK 框架建立攻擊預測模型。

(b) 自動化關聯分析

- 威脅鏈(Kill Chain) 自動對應 : 將威脅事件與攻擊鏈(Kill Chain) 比對，提高預警能力。
- 指標交叉驗證（Indicator Correlation）: 透過多來源情報確認 IP、域名、惡意軟體樣本的可信度。

2. 最近二年度每年投入之研發費用

單位：新台幣仟元

項目/年度	112年度	113年度
研發費用	257,718	309,537
營收淨額	1,844,558	2,146,434
研發費用占營收淨額比率	13.97%	14.42%

3. 最近年度開發成功之技術或產品

(1) 主動式資安監控中心（Intelligent SOC）

因應新世代 SOC 架構，發展具自動化的主動式監控智能中心 Intelligent SOC，已導入 AI 創新技術，持續佈署以人工智慧為核心的安全監控中心 AI-Driven SOC，達到優化流程與減少人力投入的目標。運用多種 AI 模型進行日誌分析，涵蓋 IT、OT、雲端等三大環境，針對不同客戶和各種不同設備進行多面向分析，從監控服務客戶端的日誌來源，找出異常的行為，挖掘潛藏資安威脅，實現自動化的偵測、判斷與回應，到整合外部威脅情資來源，提升事前日誌監控分析的精準度。在事中、事後階段方面，與 SOC 整合的事件調查、鑑識服務、SOAR，以及惡意威脅狩獵分析服務也是重點。

(2) 雲地端資安 SOC 整合平台

建構雲端安全監控中心（Cloud SOC），監控雲端各種資安設備被刺探的行為，將監控的日誌資料所觸發的「事件」進行彙整，再將「事件」遞送轉交給地端的安全監控中心（SOC）進行關聯分析，進而比對雲、地所發生的資安事件關聯，雲端日誌不落地，節省大量日誌下載的網路傳輸費用，建立雲地監控中心混合互相回饋循環機制。

(3) 雲端資安監控基準

隨著企業向雲端遷移，確保雲端環境的安全變得至關重要。傳統資安監控方法已無法滿足動態、分散的雲端架構，因此需要建立雲端資安監控基準(Cloud Security Monitoring Baseline)，確保從基礎架構到應用層的全面防護。

雲端資安監控基準涵蓋身分與存取、網路安全、應用程式與工作負載、資料保護、安全日誌與事件管理（SIEM）、威脅偵測與回應（MDR）等領域。

(4) 雲端資安監控技術

是確保雲端環境中資料、應用和基礎設施的安全性，對於企業保護其雲端基礎設施免受各類攻擊與威脅至關重要。隨著企業將更多業務遷移到雲端，這些監控技術需要有針對性地涵蓋不同層級的資安防禦，並具備強大的即時偵測與反應能力。

(5) 紅隊演練技術

紅隊演練（Red Teaming）是一種模擬真實攻擊者的資安測試技術，目標是評估組織的資安防禦能力。核心技術涵蓋情報蒐集、滲透測試、橫向移動、數據竊取、持久化存取，目的是找出組織的資安弱點，提升資安應變能力。

(6) 入侵及攻擊模擬 BAS（Breachand Attack Simulation）技術

BAS（Breachand Attack Simulation，入侵及攻擊模擬）是一種自動化攻擊模擬技術，可以持續測試組織的資安防禦能力，並識別安全弱點。BAS 主要模擬真實攻擊者的行為，但不會影響業務運作，BAS 更具自動化、持續性、可量化分析的優勢。

(7) 威脅情資 AI 分析平台（ATHENA）

透過每月蒐集的高達 4,000 億筆資料，結合已知資安事件的處理經驗進行監督式學習。這種訓練模型的成果將協助企業有效地預測資安事件的發生，只需新接收到的特定日誌紀錄，即可透過監督學習的結果判定是否為資安事件。這樣的判定過程不僅省卻了事先設計大量規則的需求，更有效地降低了人力投入。

透過引入 AI 技術，將巨量資料與機器學習結合，產生異常偵測（Anomaly Detection）、預測分析（Predictive Analytics）以及歸類（Clustering）等模型，以提高資安事件檢測的效率並彌補現有監控邏輯的不足。同時，我們融入 Green AI 的理念，以節省能源並減少碳足跡。

(8) 零信任架構導入

零信任架構的核心組件主要包含 5 大部分：

- 備份與存取管理（IAM, Identity & Access Management）
- 裝置與端點安全（Endpoint & Device Security）
- 網路與微分段（Network Security & Microsegmentation）
- 持續監控與威脅偵測（Security Analytics & Continuous Monitoring）
- 存取決策引擎（Policy Engine & Enforcement）

（四）長、短期業務發展計劃

1. 長期業務發展計劃

(1) 導入 AI 技術，發展主動式資安監控中心（Intelligent SOC）

強調即時偵測與預防攻擊，結合威脅情資、AI 分析、自動化回應，確保系統安全。以下是主要技術架構與核心組件：

- 威脅情資與行為分析
- AI/ML 驅動的威脅分析
- SOAR（安全編排與自動化）
- SIEM（安全事件與資訊管理）
- EDR/MDR（端點與擴展式偵測與回應）
- 網路流量分析與零信任架構
- 自適應 AI 安全防禦（Adaptive AI Security）
- 自動化紅隊/藍隊攻防測試（Automated Red Teaming）
- 入侵及攻擊模擬 BAS（Breach and Attack Simulation）

(2) 發展 AI 在資安領域的應用與技術發展

- 威脅檢測與回應：AI 能即時監控網路和系統，分析大量數據以快速偵測和回應威脅。這包括識別異常行為模式，預測潛在攻擊，並自動化威脅回應。
- 惡意程式偵測：AI 演算法可以分析檔案特性和行為模式，偵測惡意程式。這些演算法能夠比傳統方法更快、更準確地識別新型惡意軟體。
- 行為分析：AI 能分析使用者和系統的行為，發現可能意味著資安威脅的異常情況，從而提前預防攻擊。
- 自動化資安工作：AI 可以自動化例行性資安工作，如威脅偵測和事件回應，讓

資安人員專注於更複雜的任務。

- 漏洞挖掘 : AI 技術被用來發現和修補軟體漏洞，提升軟體開發的安全性。例如，AI 可以幫助縮小漏洞範圍，並加速漏洞修補過程。
- 深度偽造防護 : AI 技術也被用來識別和防止利用假視頻和音頻進行的詐騙和身份冒充。

(3) 發展威脅情資 AI 分析平台（ATHENA）

透過每月蒐集的高達 4,000 億筆資料，結合已知資安事件的處理經驗進行監督式學習。這種訓練模型的成果將協助企業有效地預測資安事件的發生，只需新接收到的特定日誌紀錄，即可透過監督學習的結果判定是否為資安事件。這樣的判定過程不僅省卻了事先設計大量規則的需求，更有效地降低了人力投入。透過引入 AI 技術，將巨量資料與機器學習結合，產生異常偵測（Anomaly Detection）、預測分析（Predictive Analytics）以及歸類（Clustering）等模型，以提高資安事件檢測的效率並彌補現有監控邏輯的不足。同時，我們融入 Green AI 的理念，以節省能源並減少碳足跡。

(4) 發展雲端資安技術架構

雲端資安技術可以依照零信任（Zero Trust）、自動化監控、攻防演練、數據保護進行分類，涵蓋 6 大核心技術領域：

- 雲端身份與存取管理（Cloud IAM）
- 雲端威脅監控與安全資訊管理（SIEM, SOAR, CSPM）
- 雲端工作負載防護（CWPP, Container Security）
- 數據安全與加密技術（DLP, KMS, Homomorphic Encryption）
- 雲端攻防演練與 BAS 技術（Breach & Attack Simulation）
- API 與 DevSecOps 安全（API Security, Shift Left Security）

2. 短期業務發展計劃

(1) 發展主動式資安監控中心（Intelligent SOC）服務

主動式監控智能中心（Intelligent SOC, iSOC）成為企業資安的新標準，結合 AI 分析、自動化回應、威脅情報整合，提供更快、更準確的威脅偵測與應變能力。

運用多種 AI 模型進行日誌分析，涵蓋 IT、OT、雲端等三大環境，針對不同客戶和各種不同設備進行多面向分析，從監控服務客戶端的日誌來源，找出異常的行

為，挖掘潛藏資安威脅，實現自動化的偵測、判斷與回應，到整合外部威脅情資來源，提升事前日誌監控分析的精準度。在事中、事後階段方面，與 SOC 整合的事件調查、鑑識服務、SOAR，以及惡意威脅狩獵分析服務也是重點。

(2) 發展雲端資安監控中心服務（Cloud SOC）

是專門為雲端環境設計的資安事件監控與應變平台，負責監測、分析、應對雲端環境中的各種安全威脅與攻擊。

Cloud SOC 的核心目標是透過自動化、安全分析、AI 與零信任技術，確保企業的雲端基礎設施、應用、數據免受網路攻擊的威脅。

(3) 發展 Cloud SOC 雲端及地端資安監控整合服務

提供雲端與地端資安監控整合，確保企業在混合雲與地端環境中的資安事件可視化、威脅偵測、應變處理與合規管理。

需要結合 SIEM、EDR、NDR、SOAR、威脅情報（TI）等技術，打造具備即時監控、主動威脅偵測、自動應變的資安監控運營中心。

(4) 發展雲端健診服務

主要目的是幫助企業評估其雲端環境的安全性，識別潛在的漏洞與風險，並提供改進建議。這樣的服務應結合自動化掃描工具、最佳實踐標準、合規要求及威脅情報，確保雲端架構的完整性和安全性。

(5) 發展紅隊演練服務

紅隊演練（Red Teaming）是一種模擬真實攻擊者的資安測試技術，目標是評估組織的資安防禦能力。核心技術涵蓋情報蒐集、滲透測試、橫向移動、數據竊取、持久化存取，目的是找出組織的資安弱點，提升資安應變能力。

(6) 發展入侵及攻擊模擬 BAS（Breach and Attack Simulation）服務

BAS（Breach and Attack Simulation，入侵及攻擊模擬）是一種自動化攻擊模擬技術，可以持續測試組織的資安防禦能力，並識別安全弱點。BAS 主要模擬真實攻擊者的行為，但不會影響業務運作，BAS 更具自動化、持續性、可量化分析的優勢。

(7) 發展零信任架構導入服務

零信任架構（Zero TrustArchitecture, ZTA）是一種「永不信任，持續驗證」的安

全策略，旨在防止內部與外部威脅。與傳統安全模式不同，零信任不假設內部網路是可信的，而是對每個存取請求進行驗證，確保只有合法用戶與設備能夠存取資源。零信任架構的核心組件主要包含 5 大部分：

- 備份與存取管理（IAM, Identity & Access Management）
- 裝置與端點安全（Endpoint & Device Security）
- 網路與微分段（Network Security & Microsegmentation）
- 持續監控與威脅偵測（Security Analytics & Continuous Monitoring）
- 存取決策引擎（Policy Engine & Enforcement）

(8) 整合營運不中斷解決方案

因應駭客勒索黑色產業日益茁壯，復原與備援服務已成為優化與完善本公司提供客戶資安服務所必需，故，將整合營運不中斷服務納入資訊安全服務架構，即事前預防-資料與系統備份備原服務、事中偵測-備援演練、事後應變-啟動緊急備援，執行災變復原程序，使整體資安服務架構更為完整，進而強化公司競爭力。

(9) 配合證交所及櫃買中心所公佈的上市上櫃公司資通安全管控指引，要求落實依期程導入國際資安標準並通過驗證及辦理系統滲透測試、資安健診等強化資安防護措施，擴大對上市上櫃公司業務範圍。

(10) 安碁學苑已通過勞動部 TTQS 人才發展品質系統認證，將持續加速職訓機構的設立，以利推動相關資安職能教育訓練，在現有通過的職訓課程中，資安教育訓練成為亮點，也將擴大線上課程以外的實體上課以及企業包班。

(11) 海外業務的開發，提供 MDR 及各項資安檢測服務，並持續深化與當地夥伴合作，朝向資安區域聯防的目標前進。

二、市場及產銷概況

（一）市場分析

1. 主要商品（服務）之銷售（提供）地區

單位：新台幣仟元

年度 項目	112年度		113年度	
	金額	比例（%）	金額	比例（%）
內銷	1,842,868	99.91	2,140,177	99.7
外銷	1,690	0.09	6,257	0.3
合計	1,844,558	100.00	2,146,434	100.00

2. 市場占有率

本公司係資訊安全服務廠商，為因應整體資安市場之快速變動及客戶對整體性資安解決方案之需求，提供包含資安管理服務、資安監控整合性服務等客製化服務，除利用其具豐富經驗與技術基礎之資安監控防護中心（SOC）提供持續性資安威脅監控管理外，也提供多樣的資安防護教育訓練課程，以提升客戶端人員之資安意識，從而減少資安事件之發生可能性與潛在危害。

按照本公司 112~113 年度資訊安全服務事業單位營業收入金額 1,558,961 仟元及 1,911,686 仟元占工研院產業研究估計的各該年度台灣資訊安全服務市場規模 7,464,800 仟元及 9,350,000 元比例來計算，安碁資訊在各該年度的市場占有率分別為 20.9%及 20.4%。

單位：新台幣仟元

年度 項目	112年度	113年度	
	金額	金額	變動率
資訊安全服務事業單位營收淨額(A)	1,558,961	1,911,686	20.3%
工研院估計台灣資訊安全服務市場規模(B)	7,464,800	9,350,000	25.2%
推算市場佔有率(A)/(B)	20.9%	20.4%	

資料來源：(A)經會計師查核簽證之財務報告。

(B)工研院產科國際所；工研院IEK（2024）。

3. 市場未來之供需狀況與成長性

(1) 供給面

資訊安全服務業是技術密集及專業度高的產業，就目前國內而言，資安服務廠商

包含系統整合商、顧問公司、資安服務專業公司及電信業者眾多經營型態業者，大部份只能提供部份資安服務，且廠商多數屬中小型企業。

(2) 市場未來之成長性

資安市場正處於高速增長階段，隨著雲端化、AI 技術、量子運算、5G、物聯網(IoT)等科技的發展，資安需求持續攀升，未來市場前景極為廣闊。

雲端資安-在數位轉型下，企業使用外部雲端進行管理服務，將資料上雲比率大幅提高，導致雲端成為駭客的首要目標，有越來越頻繁的雲端跳躍網攻 (Operation Cloud Hopper)，進階持續性滲透攻擊(APT)更是防不勝防，影響層面涵蓋金融、教育、醫療等產業，顯示企業無論大小，資安事件偵測能力都有必要持續提升強化。

物聯網 (IoT) 資安-萬物聯網的時代，資安議題不只影響個人隱私，舉凡企業、政府乃至於公共安全層面都陷入潛在威脅，像是智慧城市包含的交通、醫療、電力基礎設施，未來經由 5G 連結之後，倘若遭受攻擊造成系統癱瘓，城市將瞬間陷入停擺。近年來，互聯網成功驅動各行各業快速發展與轉型，後繼的大數據與人工智慧技術，也藉由數以萬計的連網裝置，將全球緊緊牽繫在一起，於是提供駭客絕佳機會，利用這些特性在網路上發動惡意攻擊，使得數位轉型替社會與企業帶來便利及商機，卻同時引入不容小覷的破壞風險。

4. 競爭利基

(1) 為因應全球 5G、物聯網 (IoT)、人工智慧 (AI) 數位技術的發展應用，將持續帶動國內外資安服務的需求，安碁資訊仍將強化資安技術營運智慧和能量來強化競爭服務優勢，提供國內外企業最佳化的資安防禦服務。

(2) 多年 SOC 專業實務維運經驗與龐大的客戶服務範圍。

(3) 本公司深耕台灣資安服務市場多年，自 2005 年開始提供 SOC 建置與偕同維運服務，就 SOC 的相關組織與執掌之設計與規劃、SOC 人員的培訓 (包含平台操作與資安事件處理) 與及日後維運的作業規範 SOP 等已具備豐富經驗，並為台灣少數可同時提供 SOC 建置與維運服務之資安廠商。

安碁資訊 SOC 累績十餘年之經驗，已建立相當穩定之維運管理能量與經驗豐富之資安團隊，服務客戶範圍與數量相當龐大，為國內領先之資安業者，以政府部門案件而言，涵蓋能源、水資源、交通及金融等領域，故自 2005 年起即累積大量

資安事件資料，目前並以每月約 4000 億筆的速度累積自客戶端蒐集的實務作業資料（operationdata），憑藉本公司專業技術人力研析，持續增加並不斷更新的資安偵防規則，使本公司提供的資安服務具備高度即時性與實務切合性，而本公司因具備實際維運經驗，並高度整合 SOC 前置規畫與建置作業，因此相較於其他資安廠商而言，本公司得以協助客戶達到資安投資項目的高度整合與集中管理而不僅是分散採購資安系統或設備，並得以充分有效發揮功能，此外尚可透過資安偵防規則及豐富的專業經驗等，協助有效縮短安全事件之應變時間，徹底找出事件的問題來源。而龐大實務作業資料庫亦為人工智慧與機器學習等技術之應用提供良好的發展基礎。

(4) 導入 AI 技術並開發智慧 SOC（Intelligent SOC）

傳統 SOC 分析平台，需即時完成原始事件比對與分析後，確認是否有安全威脅，依據結果，發布資安警訊通報通知客戶、追蹤處理結果，如果有需要進一步執行事件調查，再依照雙方合約規範執行，因此係偏向反應式（reactive）之資安防護措施，較受限於難以實現跨設備、跨客戶大範圍與長週期分析。本公司累積長期資安事件分析與調查之心得，發現尚有很多潛伏之資安威脅，需要透過大數據分析平台，執行跨設備（如：防火牆、入侵偵測設備）、大範圍（跨客戶）、長週期（數週或數月）的分析，才能夠發掘出來 - 這些潛伏期之資安威脅，是目前資安設備、防毒軟體尚未能夠辨識出來的潛藏危害。且為因應日益加快的資安攻擊樣態演化速度、及多元化的資安威脅樣態，導入人工智慧科技、使資安偵防機制智慧化、自動化，主動就各類潛在攻擊事件進行偵防，已是當前市場的重要趨勢。

本公司同時具備(1)龐大的實務作業資料庫而得以實現大數據平台；(2)資安專業人才與豐富經驗，並為國內少數擁有通過 ISO17025 認證數位鑑識實驗室之 SOC 業者，因此得以辨識哪些徵兆或特徵是潛伏的資安威脅；(3)導入機器學習演算法，以**海**量原始日誌為學習對象，並由資安專家驗證與調整學習演算法，反覆進行確認與改良，最終得出可靠的學習結果。此演算法於 Intelligent SOC 中自動運算，將資安專家的智慧自動化，讓安碁資訊 SOC 具備智慧運算的能力。故而本公司在發展人工智慧之資安應用上業已具備堅實之基礎，憑藉自客戶端蒐集之實務作業資料發展的關連性分析規則，可直接投入真實場景應用，並藉由客戶與專家提供之回饋不斷調整。結合本公司在 SOC 建置營運領域的豐富經驗、及龐大的客戶基數，人工智慧技術的導入使本公司資安偵防平台得以在傳統資安防護設施資訊整合的基礎上，就客戶端回傳之資訊進行統合分析，偵知共通惡意攻擊之來源，

從而與以先制封鎖並為其他客戶提供預警。較諸傳統 SOC，導入人工智慧技術的智慧 SOC（Intelligent SOC）更具前瞻性與整合性，使資安防護化由傳統反應式（reactive）提升至主動式（proactive）服務，將資安威脅提早排除與解決，對潛在資安威脅得以制敵先機。

(5) 情資來源多元、建構國內首屈一指之資安情資平台

除經多年累積之龐大客戶基數外，本公司亦與亦與國際資安情資組織、暗網之調研機構頻繁進行交流，從而得以及時掌握資安領域之國際動態，及時並持續回饋至偵防平台中。由於資料來源皆係客戶端實務作業所產生，基於該等資料發展的偵防與因應規則能高度切合實務需要，並能及時反應當前資安環境趨勢。相對同業而言，本公司因具備龐大客戶基數、長久資安服務歷史、多樣的資料來源，得以發展實務應用性佳、具備高度即時性之資安防護方案，鞏固自身競爭優勢，並具備發展整合性、主動性資安防護與因應措施之良好基礎。

(6) 技術能力與服務品質取具國際認證，擔綱國家級資安防護計畫重任

本公司具備 ISO27001 資訊安全管理系統認證、ISO27701 個人資訊管理認證、數位鑑識中心 ISO17025 實驗室認證等國際級認證，出具之資安鑑識與調查報告為國際所公認。除取具國際級認證作為自身技術實力與服務品質之表彰，以鞏固客戶信任及市場地位外，本公司亦於全球最大之資安弱點情資資料庫（CVE）發布研究成果，並獲得美國國家資安弱點資料庫（NVD）之承認，顯示本公司就資安威脅事件之自主研究與評估能力亦獲得相當肯定。在營運實績方面，本公司就國內資安市場的長期耕耘、已建立良好商譽，往來客戶涵蓋臺灣證券交易所、財政部、科技部等重要公部門機關，亦擔綱國家級資安防護規劃之八大關鍵基礎設施中之能源、水資源、交通等領域之防護機制建構維運工作，並參與資訊安全暨區域聯防委託服務案等重點資安計畫，善用自身在資安服務領域的豐富經驗，協助建構構成國家安全重要部分之資安防護體制。

(7) 領域橫跨 IT 與 OT，切合資安防護發展趨勢

較諸傳統資安服務廠商所聚焦、主要涵蓋電腦等端點設施、網路及伺服器資安偵防之資訊科技（Information Technology, IT）領域，涉及關鍵基礎建設、生產設備與機械運作之操作科技(Operation Technology, OT)領域過去所受重視程度較低，但其資安漏洞造成的潛在經濟損失與社會成本鉅大，由去年台積電機台遭惡意程式入侵、導致部分生產線停擺之事件可見一斑。有鑑於基礎建設運營及生產流程

自動化、智慧化趨勢下，IT 及 OT 領域的重合度增加、過去主要見於 IT 領域之資安威脅亦擴及 OT 領域，本公司已積極投入 OT 資安領域，係國內少數同時跨足 IT 及 OT 領域之資安服務廠商，不僅在傳統資訊系統、網路、伺服器、資料庫等 IT 領域監控防護具有豐富實務經驗，亦跨足重要工業設施作業平台、基礎建設核心系統等 OT 領域資安防護業務，通過 TestBed 平台進行逼近實務作業情況之模擬測試，在不影響正常作業活動的情況下，辨認系統弱點所在與潛在威脅樣態。

(8) Cloud SOC 雲端及地端資安監控整合服務

本公司是國內唯一完整整合雲原生資安監控平台與 7x24 資安監控維運服務的資安服務廠商。面對現今企業多採混合雲布局的主流趨勢，安碁資訊更可協助客戶導入雲地整合監控與聯防服務機制，整合多雲與地端的資安監控機制於單一監控服務平台，確保企業資安治理與資安維運的完整性與一致性。透過宏碁雲架構，將微軟 Azure 雲端設備日誌與資料整合平台 API 串接，結合既有 ACSI SOC 核心技術能量，並由安碁資訊專家進行關聯規則建立，監控雲端各種資安設備被刺探的行為，將監控的日誌資料所觸發的「事件」進行彙整，再將「事件」遞送轉交給地端的安全監控中心（SOC）進行關聯分析，進而比對雲、地所發生的資安事件關聯，雲端日誌不落地，節省大量日誌下載的網路傳輸費用，建立雲地監控中心混合互相回饋循環機制。安碁資訊能夠協助企業由單一環境無痛整合至混合雲，提供更安全可靠的雲端服務，使得企業在雲端服務上的共享資源，擁有更大的彈性與靈活性，捍衛雲地 IT / OT 安全，實現企業永續營運的韌性。

5. 發展遠景之有利、不利因素與因應對策

(1) 有利因素

A. 台灣企業資安市場穩定成長、金融業資安支出成長尤快

為因應日益增加的潛在資安威脅，國內企業在資安防護領域的開支持續成長。基於其掌握大量具高度敏感性與價值之資訊、組織所管理之資產及收益較具規模，國內的政府部門與金融業常成為包含 DDoS、勒索型惡意軟體、APT 等資安攻擊之主要目標。鑒於資安事件可能對正常營業乃至具急迫性之重大活動構成顯著之妨害、重創品牌商譽或構成民眾對組織的不信任、乃至損及我國國際形象，國內民間各產業部門及政府機關幾皆致力於資安領域之投入，除防範潛在的資安威脅外，亦是各該組織對於維繫自身產品或服務品質、重視客戶及人民權益之表彰。

B. 政府資安監理規範趨嚴、推動公部門資安需求扮演積極角色

鑒於近年來台灣資安事件頻仍、資安威脅的可能型態與影響程度皆持續增加，除民間企業強化自身資安防護措施外，國內政府機關也對資安議題表達高度重視，行政院於民國 105 年 8 月 1 日成立資安專責單位資通安全處，將資安正式定調為國安層級事項外，資安專法《資通安全管理法》也於民國 106 年 5 月 11 日通過，自 108 年 1 月 1 日起正式施行，使資安防護建立體制化的要求與相關檢核機制層級由行政命令進一步提高為具強制力之法律，適用範圍亦由公務機關擴張至受有政府資源投入、涉及公眾利益、組織機能對國家安全與大眾影響重大之非公務機關。在 106 年 7 月核定版本的前瞻基礎建設－數位建設計畫中，亦正式將資訊安全基礎建設納入前瞻計畫的重點投入項目，彰顯當局對國家整體資訊安全之重視。是故，對於主要經營國內市場、積極參與公領域資安採購案件的整合性資安服務提供者而言，市場前景趨於正向。

C. 資安威脅模式日益增加、整合性資安服務需求增加

在資安威脅態樣多元化的趨勢下，從終端聯網裝置、通訊網路、伺服器、乃至雲端設施都可能成為攻擊的目標，且混合多種攻擊模式之進階持續性滲透攻擊（APT）事件亦越發頻繁，資安防護措施之布置必須兼具深度與廣度，能有效且及時地統合來自不同防護機制之威脅情資，並持續因應當前資訊科技領域動態與個體本身特性做出彈性之動態調整，方能有效偵知潛在之威脅活動，從而提早加以因應。

資安監控中心（SOC）以其具備整合端點防護、防火牆（Firewall）、網路型入侵偵測系統（NIDS/IPS）、主機型入侵偵測系統（HIDS）等多元防護措施、提供公司個體層級多面向防護的能力之特性，在資安威脅態樣演進快速、所需應對量能劇增的環境下，已成為越來越多企業的資安防護選擇。除此之外，為確保組織之資安防護布置可切合當前實務運作需求、因應資安環境變動而及時調整，在初始建置外，後續維運與相關顧問服務的重要性也顯著提升，以確保組織保有最適的因應量能，以最大程度發揮防護效能。

D. 資安防護措施智慧化趨勢下，作業資料及資安情資具高度價值

導入人工智慧與機器學習技術於現有之資安偵防平台上，可使資安公司就自客戶端蒐集的惡意軟體、垃圾郵件、勒索軟體等攻擊事件資訊進行更有效率的整合、分析與比較，並結合人類專家的經驗與即時市場資料，演繹出未來可能產

生的攻擊模式、發掘已存在系統中的潛在威脅，配合導入機器人流程自動化（Robotic Process Automation）等方式，使因應措施可被即時且一致地執行，廣泛應用於辨識惡意攻擊，偵測和分析攻擊形式上。為確保智慧化偵防機制得以充分切合客戶之實務運營需要，長期之資安服務經驗、自客戶端蒐集的實務作業資料（operation data）之累積、及即時之市場資安情資來源便至關重要，因為投入的資訊越即時、越貼近實務、內容越豐富、涵蓋面向越廣泛，可能演繹出的規則越富於價值，並能切合實務需求，具備豐富營運經驗、在業界累積有深厚情資網絡的資安業者，也因而將更受市場青睞。

(2) 不利因素

A. 國內資安市場規模有限，海外市場拓展不易

台灣資安市場雖在民間企業投資與政府政策規劃帶動下被預期將迎來顯著成長，惟整體市場規模相較國際資安市場而言，仍顯狹隘，而海外市場則因應當地環境及法令規範而有較高之在地化與客製化門檻，拓展不易。

因應對策：

本公司雖已在國內民間與政府部門皆已建立相當的商譽並維繫穩定的客戶關係，但亦有鑒於台灣市場的侷限性，憑藉自身在資安服務領域的豐富實務經驗與與能力，積極布局東南亞資安市場。

B. 系統整合商、電信業者等紛紛投入資安市場，造成競爭

資安市場除資安管理服務供應商（Managed Security Service Provider, MSSP）外，尚有系統整合商（System Integration, SI）、電信業者及資安顧問公司等之參與，市場日趨競爭。

因應對策：

資安服務業是技術密集及專業度高的產業，就目前國內而言，資安服務廠商包含系統整合商、資安顧問公司、資安服務專業公司及電信業者眾多經營型態業者，大部分只能提供部分資安服務。惟隨資安威脅面向多元，資安防護整合需求日趨殷切，本公司是目前可同時提供 SOC 營運、資安資訊分享分析建置與監控服務（ISAC）、資安檢測、鑑識與顧問服務予客戶之高度整合資安服務專業公司，故具備一定競爭優勢，且本公司除加強維持與既有客戶之緊密關係，亦積極提升專業技術及其競爭力，建立差異化的服務特色，並積極拓展新客戶，

以因應未來可能加入之競爭廠商。

C. 人才留才與培育日漸困難

資安監控領域相關人才流動率較高，SOC 營運管理經驗傳承及專業實力需仰賴有效的留才及培育。

因應對策：

本公司通過對國內市場的長期經營，已在資安檢測、監控、管理、及顧問服務領域累積豐富的經驗，並持續投注研究資源於包含大數據分析、機器學習在內的市場主流科技趨勢，致力於將該等科技與公司目前旗下的服務相結合，以期進一步強化資安防護服務的即時性、準確性與前瞻性，鞏固並強化自身的市場地位，並同時以龐大的資料庫與處理經驗，增加人才留任動因；此外，本公司認為具有功能完整的系統平台（Platform）搭配完善的作業規範（Process）與訓練有素之技術人力（People）等成功的關鍵因素，故相當重視人力素質之培養及技術專業認證質量，本公司因有資訊安全管理制度（Information Security Management System）導入服務，及 SOC 規劃建置，在人才養成不遺餘力，培訓員工在資安管理、資安監控、資安檢測、輔導國際認證等各類專業能力；本公司也設有通過 ISO17025 實驗室認證之數位鑑識中心與資安實驗室（Security LAB），提升資安監控人才的培育。

（二）主要產品之重要用途與生產過程

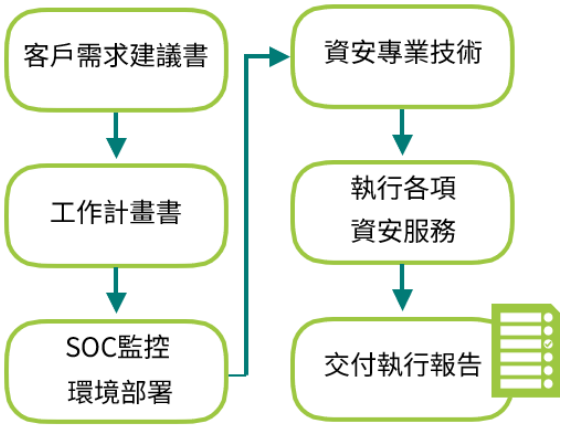
1. 主要產品重要用途

產品名稱	主要用途或功能
資訊安全服務	事前預防 1. 顧問服務-資訊安全管理制度（ISMS）建置輔導、個資風險評鑑、金融和規檢視。 2. 建立備援-資料備援、系統備援。 3. 檢測-資安健診服務、分散式阻斷服務攻擊演練、紅隊演練、入侵及及攻擊模擬、系統弱點掃描、網頁弱點掃描、滲透測試、電子郵件警覺性測試、Apps檢測、工業控制系統弱點與威脅評估等服務。 4. 導入零信任架構 事中偵測 1. 監控-含資安監控防護中心營運，提供7x24的資安防護維運服務，將蒐集的設備原始營運資訊進行深度的分析，研判潛在的安全問題，有效的處理的攻擊事件。防駭監控：將企業內部多種資安設備，所產生的資安事件記錄，以系統化的方式進行收集、關聯性分析、異常網路行為監控、警訊通報及協助事件處理。防毒監控：針對病毒活動進行監控，隨時注意防毒系統之異常訊息，發掘是否有變種病毒的存在。即時掌握病毒疫情資訊，建立快速回應及有效的通報機制。

產品名稱	主要用途或功能
	2. 備援演練-增加備援演練種類。 事後應變 1. 數位鑑識-資安事件調查分析、數位鑑識中心調查鑑識服務。 2. 啟動備援-啟用備援機制、預防災損擴大。
資訊部門 營運委外服務	委外資訊管理服務包括電腦硬體設備、網路設備和通訊系統等方面的管理和維護，以提高企業的效率和降低成本，並確保企業的資訊系統運作正常並得到保障。

2. 主要產品之生產過程

本公司資訊安全服務之主要提供過程如下：



（三）主要原料之供應狀況

產品名稱	主要原料供應情況說明
資訊安全服務	本公司主要係以資安專業技術為核心，向國內、外資安軟硬體原廠或經銷商，採購相關資安軟硬體工具，用以提供SOC營運、資安檢測、數位鑑識與顧問服務予終端客戶。本公司均與供應商建立穩定之合作關係，供應情形穩定，未有供貨來源中斷之情事。

（四）最近二年度任一年度中曾占進（銷）貨總額百分之十以上之客戶名稱及其進貨金額與比例，並說明其增減變動原因。

1. 最近二年度任一年度中曾占進貨總額百分之十以上供應商

單位：新台幣仟元

項次	112年度				113年度			
	名稱	金額	占全年度進貨淨額比率%	與發行人之關係	名稱	金額	占全年度進貨淨額比率%	與發行人之關係
1	台達電子工業	404,299	34.56	無	台達電子工業	222,025	22.12	無
2	零壹科技	68,163	5.83	無	零壹科技	87,954	8.76	無
	其他	697,465	59.61		其他	693,953	69.12	
	進貨淨額	1,169,927	100		進貨淨額	1,003,932	100	

2. 最近二年度任一年度中曾占銷貨總額百分之十以上客戶名單

本公司最近二年度無佔銷貨總額 10%的客戶。

三、最近二年度及截至年報刊印日從業員工資料

年度		112年度	113年度	114年 3月31日
員工人數	業務銷售	62	81	83
	技術服務	293	278	279
	研究開發	192	238	243
	客戶服務	20	19	17
	管理及財務	25	27	28
	合計	592	643	650
平均年歲		40.05	40.17	40.33
平均服務年資		5.91	6.07	6.15
學歷分布比率	博士	0.34%	0.31%	0.31%
	碩士	25.00%	25.51%	25.69%
	大專	72.97%	73.09%	73.08%
	高中	1.69%	1.09%	0.92%
	高中以下	0.00%	0.00%	0.00%

四、環保支出資訊

(一)依法令規定，應申領污染設施設置許可證或污染排放許可證或應繳納污染防治費用或應設立環保專責單位人員者，其申領、繳納或設立情形之說明：本公司提供資安監控及防護等專業服務，並無特殊污染產生，毋須申請污染設置許可證或污染設施排放許可證，亦毋須繳納污染防治費用或設立環保專責單位人員。

(二)列示公司有關對防治環境污染主要設備之投資及其用途與可能產生之效益：不適用。

(三)說明最近二年度及截至年報刊印日止，公司改善環境污染之經過，其有污染糾紛情事者，並應說明其處理經過：無。

(四)說明最近二年度及截至年報刊印日止，公司因污染環境所遭受之損失(包括賠償及環境保護稽查結果違反環保法規事項，應列明處分日期、處分字號、違反法規條文、違反法規內容、處分內容)，並揭露目前及未來可能發生之估計金額與因應措施，如無法合理估計者，應說明其無法合理估計之事實：無。

(五)說明目前污染狀況及其改善對公司盈餘、競爭地位及資本支出之影響及其未來二年度預計之重大環保資本支出：不適用。

五、勞資關係

（一）列示公司各項員工福利措施、進修、訓練、退休制度與其實施狀況，以及勞資間之協議與各項員工權益維護措施情形：

1. 員工福利措施

(1) 保險方面

本公司除依規定辦理勞健保外，並為所有同仁投保團體保險（含意外險、住院醫療險），並提供同仁眷屬可以團險優惠投保金額一同投保團險。

(2) 健康方面

每年辦理全體員工健康檢查，重視員工身心工作平衡，並於健檢時提供醫師諮詢健檢報告及分析健康狀況之服務。

(3) 福利方面

本公司職工福利委員會每年提供每人旅遊補助，藝文活動補助、部門聚餐、年節禮品獎金、子女獎學金補助等各項福利活動使用。

(4) 員工協助方面

本公司遴選合格之外部專業顧問公司，提供心情專線供同仁諮詢在工作、生活、親子、婚姻、人際、情緒、壓力、健康等任何心情狀況，照顧員工身心靈健康。

(5) 休假方面

本公司全面比照勞基法規定給予特別休假，並提供線上系統供同仁及主管隨時查詢休假狀況，以協助同仁達成工作與生活之均衡。

(6) 員工滿意度調查

本公司每年實施員工滿意度調查，以了解同仁對組織的認同度及工作的滿意程度，並將同仁之回饋納入次年度公司施策之重要參考指標。

(7) 婚喪喜慶

本公司每月發予當月壽星生日禮金，對於同仁婚喪喜慶及住院、重大災害給予各項定額互助金。

2. 員工進修、訓練狀況

本公司以人為本，重視人才培育，依各部門所需要的專業技術與訓練分別安排員工

內部上課及不定期外派訓練，並在兼顧個人成長與公司發展之宗旨下，規劃全方位之教育訓練，提供員工完整之教育訓練體系。

3. 退休制度與其實施狀況

本公司均依「勞工退休金條例」採確定提撥制，其退休金之給付由本公司按月於每月薪資提繳百分之六做為退休金，儲存於勞工退休金個人專戶。

4. 勞資間之協議情形與各項員工權益維護措施情形

本公司依據相關法令規定並致力於維持和諧勞資關係，依照服務契約書、工作規則及各項管理規章辦理，內容明訂員工權利義務及福利項目，以維護員工權益。本公司自成立以來即積極建立雙向及開放之溝通管道，截至目前尚無勞資糾紛及公司損失之情事發生。

本公司訂有完整書面管理辦法，內容明訂員工權利義務及福利項目，以維護員工權益。

（二）最近年度及截至年報刊印日止，公司因勞資糾紛所遭受之損失（包括勞工檢查結果違反勞動基準法事項，應列明處分日期、處分字號、違反法規條文、違反法規內容、處分內容），並揭露目前及未來可能發生之估計金額與因應措施，如無法合理估計者，應說明無法合理估計之事實：本公司自成立至今，勞資關係和諧，並無發生因勞資糾紛而導致損失之情事，估計未來因勞資糾紛而導致損失的可能性極低。

六、資通安全管理

（一）資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等。

1. 資通安全風險管理架構

本公司資訊安全管理與個資管理的最高層級組織是「資訊安全暨個資保護委員會」，由總經理擔任召集人，委員由一級主管擔任，下轄「資訊安全推動及業務永續運作小組」、「個資保護執行小組」、「緊急應變處理小組」、「稽核小組」等，並由資訊安全長監督、管理各小組之日常實務運作。

2. 資通安全政策

- 致力維護本公司與客戶相關資訊資產的機密性、完整性與可用性。
- 提昇人員的資訊安全技能與認知，建立本公司可信賴的形象。

- 建構完善的資訊安全管理制度，達成國際等級的資訊安全管理水準。
- 採用先進科學技術，提供全方位、高安全性的資訊安全監控中心（SOC）相關服務。

3. 資訊安全相關國際標準之驗證

本公司已通過下列三項資訊安全相關國際標準之驗證，並持續維持證書之有效性：

- ISO27001：2013 資訊安全管理驗證（有效日期 2025-05-02）
- ISO27701：2019 個人資訊安全管理驗證（有效日期 2025-05-12）
- ISO17025：2017 實驗室能力驗證

4. 具體管理方案

(1) 「資訊安全暨個資保護委員會」每年實施兩次管理審查，確保本公司資訊安全與個資保護相關作業的落實。

針對前述資訊安全管理、個資保護相關實務，每年延請公正第三方組織依據國際標準之要求實施兩次驗證稽核，並於每次驗證稽核之前擇期由本公司「稽核小組」實施內部稽核。前述稽核所發現之不符合事項與改善建議，均須依據本公司「矯正預防作業程序」完成改善及存證。

(2) 資訊安全管理，涵蓋下列程序：

- 實體安全管制程序
- 資訊系統維運安全程序
- 通訊安全程序
- 存取控制程序
- 電腦安全事件管理程序
- 風險評鑑與風險管理程序
- 應用系統取得、發展及維護程序
- 稽核管理程序
- 服務中斷回復程序
- 資訊委外管理程序
- 文件管理程序
- 安全組織程序
- 帳號管理作業程序
- 資訊安全教育作業程序

- 入侵防範與系統強化作業程序
- 矯正預防作業程序
- 客戶文件管制作業程序

(3) 個人資訊保護，涵蓋下列程序：

本公司之資訊安全管理與個資保護實務，依據國際標準「規劃(Plan)、實作(Do)、審查（ Check)、改善活動（ Act)」的管理循環，分為管理面與技術面予以落實。

- 個人資料保護組織程序
- 個人資料檔案風險評鑑與管理程序
- 個資保護生命週期管理程序
- 個人資料檔案安全維護計畫程序
- 個人資料當事人權利聲明程序
- 業務終止後個人資料處理程序
- 個人資料安全控管作業程序
- 個人資料保護緊急應變處理作業程序
- 個人資料委外監督控管作業程序

(4) 技術面實務

- 每季一次電腦主機弱點掃描
- 每半年一次網站弱點掃描
- 每半年一次全員電子郵件警覺性測試
- 每年一次滲透測試
- 至少每季一次全員端點電腦防駭檢測
- 建置及維運防火牆、網路入侵偵測系統、網站應用防火牆系統、防毒系統
- 7X24 全年無休 SOC 資安監控
- 每半年一次資安新知與資安規範宣導活動
- 每年一次全員線上資安測驗
- 建置網路隔離、SSL VPN 加密通道、跳板主機相關存取控制機制，跳板主機並實施作業錄影存證

(5) 風險的移轉

公司已於 113 年參與宏碁集團共同投保資安險。

5. 影響營運事件之監控與通報應變

- 針對 SOC 資安監控所發現或人工通報之資訊、網路系統異常事件，依循本公司之「電腦安全事件管理程序」，先經過人工研判後決定事件等級，之後依據事件等級啟動對應之程序，包含緊急聯絡、客戶通知、事件鑑識、證據保全、法務與公關處理等作業。
- 如果發生重大資安事件、重大疫病感染、天災等而導致本公司服務中斷或有中斷疑慮時，則依本公司之「服務中斷回復程序」啟動應變組織，包含電腦設備搶修小組、系統回復小組、網路回復人員、資安回復人員、客服與公關、分地上班群組等，依程序進行必要的系統回復、服務回復、溝通、公關等作業。
- 每個月定期召開「資訊安全策略會議」。

（二）最近二年度及截至年報刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施：無。

七、重要契約

契約性質	契約對象	契約起迄日期	主要內容	限制條款
銷售合約	臺北市政府資訊局	Mar-01-2021-Sep-30-2025	資通安全專業委託服務案	保密與限制轉包
銷售合約	財政部財政資訊中心	Apr-09-2021-Dec-31-2026	整合性資安監控中心建置案	保密與限制轉包
銷售合約	能源局	Jan-01-2025-Dec-31-2025	能源領域安全管理推動	保密與限制轉包
銷售合約	司法院	Jan-01-2024-Dec-31-2026	進階持續性滲透攻擊防護系統使用授權及事件監控鑑識服務採購案	保密與限制轉包
銷售合約	環境部	Aug-01-2024-Jul-31-2025	網路資訊安全防護監控服務專案	保密與限制轉包
銷售合約	經濟部	Jan-01-2025-Dec-31-2025	資安整合聯防機制服務案	保密與限制轉包
銷售合約	交通部	Jan-01-2025-Dec-31-2026	交通領域資安聯防平台維運案	保密與限制轉包

伍

、財務狀況及財務績效之檢討分析與風險事項之評估

伍、 財務狀況及財務績效之檢討分析與風險事項之評估

一、財務狀況（合併財報）

最近二年度資產、負債及股東權益發生重大變動之主要原因及其影響：

單位：新台幣仟元；%

年度 項目	112年	113年	差異	
			增(減)金額	變動比率
流動資產	1,086,861	2,262,174	1,175,313	108.14
不動產、廠房及設備	441,693	1,353,427	911,734	206.42
無形資產	94,965	86,703	(8,262)	(8.70)
其他資產	896,454	978,413	81,959	9.14
資產總額	2,519,973	4,680,717	2,160,744	85.74
流動負債	973,039	889,517	(83,522)	(8.58)
非流動負債	252,694	779,272	526,578	208.39
負債總額	1,225,733	1,668,789	443,056	36.15
股本	222,045	301,152	79,107	35.63
資本公積	769,344	2,288,650	1,519,306	197.48
保留盈餘	347,607	458,345	110,738	31.86
股東權益總額	1,294,240	3,011,928	1,717,688	132.72

差異說明（差異金額達 10,000 仟元且變動比例達 20%者）：

1. 流動資產：主係現金及約當現金增加所致。現金及約當現金增加的主要原因為本年度辦理現金增資取得現金 1,600,000 千元、因應購置不動產作為辦公室而向銀行進行房屋貸款現金流入 270,377 千元及不動產取得成本 855,305 千元。
2. 不動產、廠房及設備：主要係本年度購買位於台北市南港區之不動產以作為辦公室使用，取得成本為 855,305 千元所致。
3. 資產總額：主要原因為本年度辦理現金增資、因應購置不動產作為辦公室而向銀行進行房屋貸款及購買位於台北市南港區之不動產以作為辦公室使用所致。
4. 非流動負債：主要係認列一年期以上之合約負債及向銀行舉借長期借款所致。
5. 負債總額：主要係認列一年期以上之合約負債及向銀行舉借長期借款所致。
6. 股本：主要係今年度辦理現金增資所致。
7. 資本公積：主要係今年度辦理現金增資所致。
8. 保留盈餘：主要係今年度本期淨利所致。

二、財務績效（合併財報）

最近二年度營業收入、營業純益及稅前純益重大變動之主要原因及預期銷售數量與其依據，對公司未來財務業務之可能影響及因應計畫：

單位：新台幣仟元；%

年度 / 項目	112年	113年	差異	
			增(減)金額	變動比率
營業收入淨額	1,844,558	2,146,434	301,876	16.37
營業成本	1,111,226	1,256,105	144,879	13.04
營業毛利	733,332	890,329	156,997	21.41
營業費用	500,335	596,838	96,503	19.29
營業損益	232,997	293,491	60,494	25.96
營業外收入及支出	(803)	(10,636)	(9,833)	(1,224.53)
稅前淨利	232,194	282,855	50,661	21.82
本期所得稅費用	41,607	57,092	15,485	37.22
本期淨利（損）	190,587	225,763	35,176	18.46

差異說明（差異金額達 10,000 仟元且變動比例達 20%者）：

1. 營業毛利：主要係本年度取得部分專案毛利較高所致。
2. 營業損益：主要係本年度營業毛利成長幅度高於營業費用成長幅度所致。
3. 營業外收入及支出：主要係本年度銀行借款利息增加所致。
4. 本期所得稅費用：主要係本年度稅前淨利較 112 年度成長所致。

三、現金流量

（一）最近年度（113 年度）現金流量變動之分析說明

單位：新台幣仟元

年度 / 項目	112年	113年	增(減)變動金額
營業活動	859,380	1,487,082	627,702
投資活動	(979,467)	(1,983,547)	(1,004,080)
籌資活動	4,845	1,563,781	1,558,936

最近年度現金流量變動之主要原因如下：

1.營業活動：主要係本年度與營業活動相關之負債現金淨流入較去年度增加所致。

2.投資活動：主要係本年度購置不動產作為辦公室使用所致。

3.籌資活動：主要係本年度現金增資所致。

（二）流動性不足之改善計畫：本公司並無現金流動性不足之情形。

（三）未來一年現金流動性分析：不適用。

四、最近年度重大資本支出對財務業務之影響

無。

五、最近年度轉投資政策、其獲利或虧損之主要原因、改善計畫及未來一年投資計畫

本公司轉投資皆為長期策略性投資；本公司於 110 年度 100%轉投資安碁學苑股份有限公司，主要提供與資訊安全之相關教育訓練服務；本公司於 111 年度 100%購併宏碁雲架構公司股權，主要提供營運不中斷解決方案、雲端技術服務；未來本公司仍將以長期策略性投資資安產業上下游相關公司為原則，將持續審慎評估轉投資計劃，以強化公司競爭力。

六、最近年度及截至年報刊印日止風險事項之分析評估

（一）利率、匯率變動、通貨膨脹情形對公司損益之影響及未來因應措施：

1. 利率變動影響

單位：新台幣仟元

項目 / 年度	112年度	113年度
營業收入淨額	1,031,866	1,153,350
利息費用	345	8,743
利息費用占營業收入淨額比率	0.03%	0.76%

資料來源：各年度經會計師查核簽證之財務報告。

本公司 112 及 113 年度利息費用分別為 345 仟元及 8,743 仟元，占該年度營業收入淨額比率分別為 0.03%及 0.76%，顯示利率變動對本公司營運並無重大影響。本公司資金運用穩健保守，閒置資金大部分存放於銀行孳息為主，本公司除隨時觀察金融市場利率變化對本公司資金之影響，以期隨時採取變通措施，並與往來銀行維持良好關係及密切聯繫，掌握利率變動等相關資訊以研判未來利率走勢，適當調整借款利率，本公司未來亦視金融利率變動狀況適時調整資金運用情形。

2. 匯率變動影響

單位：新台幣仟元

項目 / 年度	112年度	113年度
營業收入淨額	1,031,866	1,153,350
兌換利益（損失）	(447)	286
兌換利益（損失）占營業收入淨額比率	(0.04)%	0.02%

資料來源：各年度經會計師查核簽證之財務報告。

本公司 112 及 113 年度兌換利益（損失）分別為(447)仟元及 286 仟元，占該年度營業收入淨額比率分別為(0.04)%及 0.02%，對本公司損益影響尚屬有限。本公司銷售予客戶之產品與服務主要以新台幣計價，外幣銷售比重相對微小，顯示匯率變動對本公司並無重大影響。惟本公司財務部門與金融機構仍保持密切關係，持續觀察匯率變動情形，充分掌握國際間匯率走勢及變化訊息，並進行風險評估，以規避匯率變動所產生之風險。

3. 通貨膨脹情形

本公司產品非直接售予一般消費者，故通貨膨脹對本公司並無直接立即之影響，且本公司會視通貨膨脹情形以彈性因應以避免損失，預計對公司營運沒有重大影響，故最近年度及截至年報刊印日止，尚無因通貨膨脹而對本公司損益有重大影響之情事。

（二）從事高風險、高槓桿投資、資金貸與他人、背書保證及衍生性商品交易之政策、獲利或虧損之主要原因及未來因應措施：

本公司一向秉持專注本業及務實原則經營事業，財務政策以穩健保守為原則，並無從事高風險、高槓桿之投資業務。本公司已訂定「資金貸與他人作業程序」、「背書保證作業程序」及「取得或處分資產處理程序」等作業辦法，作為本公司從事相關行為之遵循依據。

（三）未來研發計畫及預計投入之研發費用

1. 未來研發計畫

(1) 導入 AI 技術，發展主動式資安監控中心（Intelligent SOC）

強調即時偵測與預防攻擊，結合威脅情資、AI 分析、自動化回應，確保系統安全。以下是主要技術架構與核心組件：

- 威脅情資與行為分析
- AI/ML 驅動的威脅分析
- SOAR（安全編排與自動化）
- SIEM（安全事件與資訊管理）
- EDR/MDR（端點與擴展式偵測與回應）
- 網路流量分析與零信任架構
- 自適應 AI 安全防禦（Adaptive AI Security）
- 自動化紅隊/藍隊攻防測試（Automated Red Teaming）
- 入侵及攻擊模擬 BAS（Breachand Attack Simulation）

(2) 發展 AI 在資安領域的應用與技術發展

- 威脅檢測與回應：AI 能即時監控網路和系統，分析大量數據以快速偵測和回應威脅。這包括識別異常行為模式，預測潛在攻擊，並自動化威脅回應。
- 惡意程式偵測：AI 演算法可以分析檔案特性和行為模式，偵測惡意程式。這些演算法能夠比傳統方法更快、更準確地識別新型惡意軟體。
- 行為分析：AI 能分析使用者和系統的行為，發現可能意味著資安威脅的異常情況，從而提前預防攻擊。
- 自動化資安工作：AI 可以自動化例行性資安工作，如威脅偵測和事件回應，讓資安人員專注於更複雜的任務。
- 漏洞挖掘 : AI 技術被用來發現和修補軟體漏洞，提升軟體開發的安全性。例如，AI 可以幫助縮小漏洞範圍，並加速漏洞修補過程。
- 深度偽造防護：AI 技術也被用來識別和防止利用假視頻和音頻進行的詐騙和身份冒充由反應式（reactive）資安防護進入主動式（proactive）資安防護。

(3) 發展威脅情資 AI 分析平台（ATHENA）

透過每月蒐集的高達 4,000 億筆資料，結合已知資安事件的處理經驗進行監督式學習。這種訓練模型的成果將協助企業有效地預測資安事件的發生，只需新接收到的特定日誌紀錄，即可透過監督學習的結果判定是否為資安事件。這樣的判定過程不僅省卻了事先設計大量規則的需求，更有效地降低了人力投入。

透過引入 AI 技術，將巨量資料與機器學習結合，產生異常偵測（Anomaly Detection）、預測分析（Predictive Analytics）以及歸類（Clustering）等模型，以提高資安事件檢測的效率並彌補現有監控邏輯的不足。同時，我們融入 Green AI

的理念，以節省能源並減少碳足跡。

(4) 發展雲端資安技術架構

雲端資安技術可以依照零信任（Zero Trust）、自動化監控、攻防演練、數據保護進行分類，涵蓋 6 大核心技術領域：

- 雲端身份與存取管理（Cloud IAM）
- 雲端威脅監控與安全資訊管理（SIEM, SOAR, CSPM）
- 雲端工作負載防護（CWPP, Container Security）
- 數據安全與加密技術（DLP, KMS, Homomorphic Encryption）
- 雲端攻防演練與 BAS 技術（Breach & Attack Simulation）
- API 與 DevSecOps 安全（API Security, Shift Left Security）

(5) 發展雲端資安監控基準

建構雲端安全監控中心（Cloud SOC），監控雲端各種資安設備被刺探的行為，將監控的日誌資料所觸發的「事件」進行彙整，再將「事件」遞送轉交給地端的安全監控中心（SOC）進行關聯分析，進而比對雲、地所發生的資安事件關聯，雲端日誌不落地，節省大量日誌下載的網路傳輸費用，建立雲地監控中心混合互相回饋循環機制。

(6) 發展雲端資安治理解決方案

推動雲端資安治理解決方案：雲端組態、雲端監控、雲端健診、雲端鑑識與雲端備份（資料加密分持）等五項雲端資安治理解決方案，協助企業在數位轉型提升營運績效之際，共同打造雲端安全的防護力。隨著企業上雲的應用趨勢，整合多雲安全防護也更加重要，安碁資訊在政府、金融、高科技製造業已具備雲地監控整合經驗，從雲端部署、維運監控至雲地兩端關聯分析與情資分享，為客戶在搬遷上雲兼顧雲端安全，提供最佳化的解決方案。

(7) 發展實戰的防駭攻防演練

藉由駭客入侵模擬演練情境，進行全天候持續性入侵與攻擊模擬，不論是情境演練還是實境演練，企業可依預算和業務範圍之需要，選用最適化的攻防演練服務，讓企業組織了解可能遭受的攻擊環節，並在每次模擬演練後依據報告產出的防護等級建議與風險報告，即時調整資安部署，修正防護弱點漏洞，強化資安防護韌性。

為擴大增強攻防演練的服務能量，安碁資訊導入美國資安專業組織 MITRE 發布之攻擊與防禦方法論（MITRE ATT&CK & ENGAGE），創新推出適用於金融領域的主動式防禦方案，此方案以欺敵系統為基礎，採用由淺至深、由點到面五階段主動式防禦機制，協助金融機構從預防、檢測乃至回應的整個過程都採自動持續地進行。

2. 預計投入之研發費用

為了鞏固現有的資安技術優勢，預計以 114 年總營收的 12%~15%之總研發費用，繼續投入經費挖掘、培訓與資安技術相關研發人才，並編列預算擴充資安服務平台能量，希望能持續推出技術領先資安服務，以提升核心競爭力進而成為資安服務中的技術領導廠商。

（四）國內外重要政策及法律變動對公司財務業務之影響及因應措施

本公司日常營運均遵照國內外相關法令規定辦理，並隨時注意國內外政策發展趨勢及法規變動情形，蒐集相關資訊提供經營階層決策參考，以調整本公司相關營運策略。最近年度及截至年報刊印日止，經本公司評估，尚無受國內外重要政策及法律變動而足以重大影響本公司財務業務之情形。

（五）科技改變及產業變化對公司財務業務之影響及因應措施

本公司隨時注意所處產業之科技變化及技術發展演變，並掌握市場脈動及同業訊息，面對多樣化的資訊安全攻擊，發展資安鑑識機器學習平台，透過大量數據分析與機器學習建立模型，識別未知的手法攻擊模式，提升本公司競爭力；最近年度及截至年報刊印日止，本公司尚無發生科技改變及產業變化而對公司財務業務造成重大影響之情事。

（六）企業形象改變對企業危機管理之影響及因應措施

本公司係屬資訊服務業，成立至今皆致力於經營並維護良好之企業形象，並遵守各項法令之規定，最近年度及截至年報刊印日止，本公司並無企業形象改變造成對企業危機管理之情事。

（七）進行併購之預期效益、可能風險及因應措施

投資併購標的之選擇係以與本公司策略發展相符之標的為主，並與本公司之營運可緊密結合，故，本公司對事業整合、投資效益及財務等風險預期將可有效控制。

（八）擴充廠房之預期效益、可能風險及因應措施

本公司係屬資訊服務業，暫無擴充廠房之需求與計畫。

（九）進貨或銷貨集中所面臨之風險及因應措施

1. 進貨方面

本公司係屬資訊服務業，經營業務多屬專案性質，因此進貨主要為搭配專案所需求之軟硬體設備。每項專案搭配的軟硬體設備，隨專案需求不同而異，且本公司有多家供應商可以搭配，提供不同軟硬體的穩定貨源，故最近年度及截至年報刊印日止，並未有進貨集中的風險。

2. 銷貨方面

本公司最近年度對單一客戶銷售比率尚無超過 10%以上者。本公司主係提供資訊安全服務。就資訊安全服務業務而言，客戶數量眾多，且最近年度絕大多數銷售比率占比並未超過 10%以上，故尚無銷貨集中之情事。

（十）董事、監察人或持股超過百分之十之大股東，股權之大量移轉或更換對公司之影響、風險及因應措施：無。

（十一）經營權之改變對公司之影響、風險及因應措施：無。

（十二）訴訟或非訟事件

1. 公司最近二年度及截至年報刊印日止已判決確定或目前尚在繫屬中之訴訟、非訟或行政爭訟事件，其結果可能對股東權益或證券價格有重大影響者，應揭露其系爭事實、標的金額、訴訟開始日期、主要涉訟當事人及目前處理情形：無。

2. 公司董事、監察人、總經理、實質負責人、持股比例超過百分之十之大股東及從屬公司，最近二年度及截至年報刊印日止已判決確定或目前尚在繫屬中之訴訟、非訟或行政爭訟事件，其結果可能對公司股東權益或證券價格有重大影響者：

本公司除持股比例超過百分之十之大股東宏碁股份有限公司（以下簡稱宏碁公司）有下述訴訟案尚於進行中外，其餘董事、總經理並無其他尚在繫屬中之重大訴訟、非訟、行政爭訟事件或行政調查之情事，相關訴訟評估分析如下：

(1) 宏碁公司在日常業務過程中不時接獲第三人主張專利侵權或要求專利授權之通知，儘管宏碁公司並不預期其結果（個別或整體）對財務狀況或業務狀況造成重大不利影響，惟法律程序結果難以預料，因此爭議解決方案可能對宏碁公司特定

期間的經營成果或現金流量造成影響。

(2) 由於國際稅務環境變化快速，宏碁公司在全球多國面臨各式各樣的稅務挑戰與各地稅務機關有不同見解，宏碁公司對於符合認列負債準備條件之稅務案件（包括但不限於所得稅、扣繳稅及營業稅等）已依相關規定適當估算以為因應。然由於稅務問題通常較為複雜且耗時多年始能釐清，其結果難以預料，因此最終結果可能對宏碁公司特定期間之經營成果或現金流量造成影響。

綜上評估，上述訴訟事件皆屬宏碁公司企業經營所衍生之事件，經評估應無其他重大違反法令或誠實信用原則之行為，對其未來正常營運亦無重大影響，應不影響本公司財務業務，故並無對本公司股東權益或證券價格有重大影響之情事。

3. 公司董事、監察人、經理人及持股比例超過百分之十之大股東，最近二年度及截至年報刊印日止發生證券交易法第一百五十七條規定情事及公司目前辦理情形：無。

（十三）資安風險評估分析及其因應措施

本公司為資訊安全專業服務公司，深知資訊安全管理的重要性。為控制資安風險，避免發生資安事件而導致服務品質與企業信譽之危害，本公司於民國 95 年即通過國際資訊安全管理標準 ISO27001 之驗證稽核，並取得證書。之後迄今每一年均由公正第三方驗證機構實施驗證覆核，並於每三年依國際標準組織之要求實施重新驗證稽核，目前證書仍持續有效。本公司除已建立由總經理及一級主管所組成的資訊安全委員會，並已建立資訊安全政策和相關標準作業程序多年，且每年定期實施資安風險評鑑、資安風險處理、全員資訊安全教育訓練、資安內部稽核、資訊安全委員會審查等作業，除確認整體資訊安全之落實度與風險之可控度之外，也針對各種新興資安風險進行及時的檢討與因應。

另，為移轉相關風險，公司已於 113 年參與宏碁集團共同投保資安險。

此外，本公司也已建置各種資安技術控管方案，包括網路防火牆、入侵防禦系統、網頁應用程式防火牆、防毒系統等，搭配 SOC 全天候資安監控、系統弱點掃描、電子郵件警覺性測試等作業，可確保本公司將資安風險控制於可接受的範圍內，且能維持本公司所提供資安專業服務的高品質及穩定度，使服務水準與客戶權益得到保障。

（十四）其他重要風險及因應措施：無。

七、其他重要事項

無。

陸、特別記載事項

陸、 特別記載事項

一、關係企業相關資料

請參閱公開資訊觀測站，【索引路徑：公開資訊觀測站>單一公司>電子文件下載>關係企業三書表專區；網址：https://mopsov.twse.com.tw/mops/web/t57sb01_q10】，輸入公司代號，查詢關係企業相關資料。

二、最近年度及截至年報刊印日止，私募有價證券辦理情形

應揭露股東會或董事會通過日期與數額、價格訂定之依據及合理性、特定人選擇之方式、辦理私募之必要理由、私募對象、資格條件、認購數量、與公司關係、參與公司經營情形、實際認購（或轉換）價格、實際認購（或轉換）價格與參考價格差異、辦理私募對股東權益影響、自股款或價款收足後迄資金運用計畫完成，私募有價證券之資金運用情形、計畫執行進度及計畫效益顯現情形：無。

三、其他必要補充說明事項

無。

附錄

柒、 附錄一

一、公司董事兼任其他公司職務一覽表

企業名稱	職稱	姓名
Acer Cloud Technology（US）, Inc.	董事長	施宣輝
Acer Cloud Technology Inc.	董事長	施宣輝
安碁資訊股份有限公司	董事長	施宣輝
宏碁双智（重庆）有限公司	董事長	施宣輝
宏碁智雲服務股份有限公司	董事長	施宣輝
宏碁雲架構服務股份有限公司	董事長	施宣輝
宏碁雲端技術服務股份有限公司	董事長	施宣輝
拓輝控股股份有限公司	董事長	施宣輝
智探太空股份有限公司	董事長	施宣輝
智輝研發股份有限公司	董事長	施宣輝
智聯服務股份有限公司	董事長	施宣輝
Acer Synergy Tech America Corporation	董事	施宣輝
上海立開信息科技服務有限公司	董事	施宣輝
旭誼工程股份有限公司	董事	施宣輝
宏碁股份有限公司	董事	施宣輝
宏碁通信股份有限公司	董事	施宣輝
宏碁創達股份有限公司	董事	施宣輝
宏碁智通股份有限公司	董事	施宣輝
宏碁資訊服務股份有限公司	董事	施宣輝
奇邑科技股份有限公司	董事	施宣輝
建碁股份有限公司	董事	施宣輝
重慶仙桃前沿消費行為大數據有限公司	董事	施宣輝
奧暢雲服務股份有限公司	董事	施宣輝
宏碁訊息有限公司	董事長	陳怡如
上海立開信息科技服務有限公司	董事	陳怡如
上海飆騎信息科技有限公司	董事	陳怡如
北京安圖斯科技有限公司	董事	陳怡如
好漾生活股份有限公司	董事	陳怡如
安碁資訊股份有限公司	董事	陳怡如
安圖斯科技股份有限公司	董事	陳怡如
宏星技術股份有限公司	董事	陳怡如
宏碁双智（重庆）有限公司	董事	陳怡如
宏碁創達股份有限公司	董事	陳怡如

企業名稱	職稱	姓名
宏碁智通股份有限公司	董事	陳怡如
宏碁智雲服務股份有限公司	董事	陳怡如
宏碁智雲資訊股份有限公司	董事	陳怡如
宏碁智聯網投資控股股份有限公司	董事	陳怡如
宏碁雲架構服務股份有限公司	董事	陳怡如
宏碁雲端技術服務股份有限公司	董事	陳怡如
宏碁資訊服務股份有限公司	董事	陳怡如
宏碁跨世紀投資股份有限公司	董事	陳怡如
展碁國際股份有限公司	董事	陳怡如
海柏特股份有限公司	董事	陳怡如
智聯服務股份有限公司	董事	陳怡如
渴望園區服務開發股份有限公司	董事	陳怡如
愛普瑞股份有限公司	董事	陳怡如
群碁投資股份有限公司	董事	陳怡如
龍顯國際股份有限公司	董事	陳怡如
聯永基股份有限公司	董事	陳怡如
Acer America Corporation	Director	陳怡如
Acer American Holdings Corp.	Director	陳怡如
Acer Cloud Technology Inc.	Director	陳怡如
Acer Computer （Far East） Limited	Director	陳怡如
Acer European Holdings SA	Director	陳怡如
Acer Holdings International, Incorporated	Director	陳怡如
Acer Japan Corp.	Director	陳怡如
Acer Service Corporation	Director	陳怡如
Acer Technology and Business Development Pte. Ltd.	Director	陳怡如
AGP Insurance（Guernsey）Limited	Director	陳怡如
Boardwalk Capital Holdings Limited	Director	陳怡如
DropZone Holding Limited	Director	陳怡如
Gateway, Inc.	Director	陳怡如
PT. Acer Indonesia	Director	陳怡如
PT. Acer Manufacturing Indonesia	Director	陳怡如
安碁資訊股份有限公司	董事	蔡傑智

安碁資訊股份有限公司

董事長：施宣輝

Acer Cyber Security Inc.

企業永續經營 ∞ 實踐數位韌性