



Business Continuity  
Institute

# 地平線 掃描報告 2019

HORIZON SCAN REPORT



Correct as of January 2019

**bsi.**

## 序言

# 英國營運持續協會

## Business Continuity Institute (BCI)

歡迎參閱此 2019 年 BCI 地平線掃描報告。過去 12 個月是我有記憶以來地平線掃描最刺激的一段時期。2018 年似乎充滿著變化無常的事件，政治和經濟不穩定，新聞標題盡是災難。概括而言，這可能創造出無止盡的混亂印象。現實情況倒沒有這麼戲劇化，而且在這種時刻，執行地平線掃描有利於聚焦，並為這樣的不確定性提供說明。



2018 年 BCI 良好實務指南指出：「地平線掃描用於控管和辨識組織可能的威脅，並考量更長期的變化和潛在的趨勢。」2019 年 BCI 地平線掃描報告訪談了全球 569 位專業人士，瞭解他們預期營運中斷在 2019 年會帶來的影響，並揭示他們如何為組織做好迎接挑戰的準備。

今年是 BCI 第八年和 BSI 這位長期夥伴共同發表地平線掃描報告，地平線掃描已成為 BCI 最受歡迎且最受期待的報告之一，我們也感謝 BSI 的持續支持。

每份地平線掃描報告都有顯著的成果，可為我們消除對未來趨勢和非預期事故的疑慮。每年的報告分析反映了全球瞬息萬變的環境以及促進經濟活動的新技術，在 2019 年，區塊鏈和人工智慧被視為營運中斷的潛在來源。一度很難預料的「黑天鵝 (Black Swan)」災難事件已成了較可預見的「白天鵝 (White Swans)」。

組織也能藉此計算出財務損失，報告結果顯示出聲譽事件是代價第二昂貴的營運中斷形式，而且遠遠超過其他大多數的損失，甚至是自然災害。如同我們經常見到的，組織投入在營運持續的預算多寡仍然與經濟盛衰相互關聯，2019 年顯示有 30% 的組織在預算上有穩健成長的跡象。

令我欣慰的是，看到 5 間組織中有將近 4 間目前在進行更長期的趨勢分析，以及受訪者中有四分之三會利用其組織的趨勢分析資訊。懂得取得並利用這樣的情報，正是界定組織具有韌性的特徵。

2019 地平線掃描報告為從事營運持續和韌性的專業人員提供寶貴的資訊資源，可用以界定並確認先前的規劃設想並注入新的想法，惠及您營運持續的情境演練和計畫。

Tim Janes  
BCI 榮譽研究員  
BCI 主席

## 序言

### 英國標準協會

### British Standards Institute ( BSI )

很高興 BSI 再度合作 2019 年的 BCI 地平線掃描報告，第八版的報告呈現出長短期營運威脅的研究成果，已經成為專業人員寶貴的資源，讓他們能夠致力於建立營運持續計畫和組織韌性。經證實，有 70% 的受訪者確定會使用如地平線掃描報告等外部資源作為風險和威脅評估工具。



經過一年對許多著名營運衝擊事件的追蹤——尤其是關於惡劣氣候、政局不穩定和資料外洩——能將結果反映在這份報告和營運中斷對財政造成的影響上，是很有意思的。

資訊與通訊中斷、安全衛生事件以及缺乏人才和關鍵技術被評為 2018 年最顯著的營運衝擊事件，強調人對營運成功的重要性。

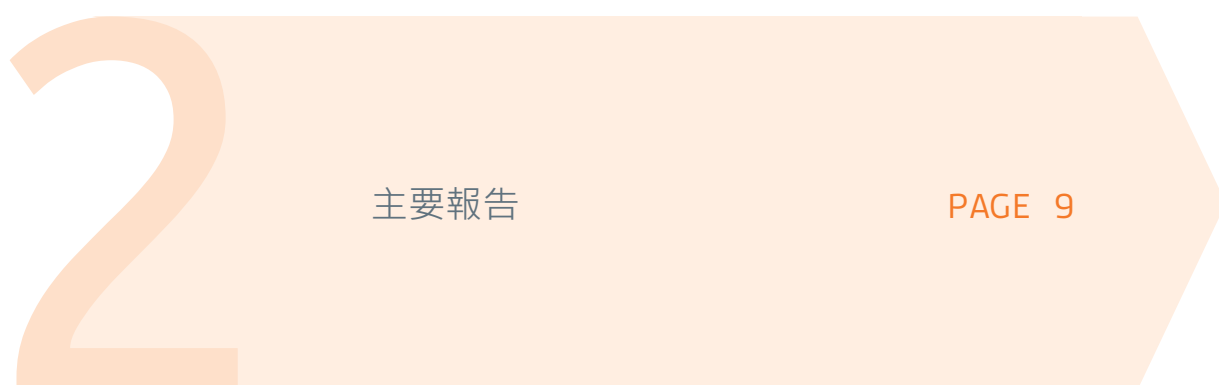
安全衛生事件不只是最普遍，也是最昂貴的風險，但其影響卻被視為相對較低。然而，組織應留心的是，如其頻率增加，也會對您的盈利造成負面的影響。組織若不認真看待其面臨的所有威脅並制定管理計畫，不僅是讓自己暴露在聲譽損害的風險中，也會成為影響盈利的財務成本。

很重要的是，組織應全面性地檢視其營運健康與成功，而非只是聚焦於風險管理。要實現組織韌性，每個人都有責任去辨識出不只是巨大的風險，也要找出看似只是「企業日常」且可能容易被忽略的次級議題。

今年的研究成果提供出色的洞見，有助於組織打造營運持續的根基，讓組織有能力進行預測、做好準備、回應變革和衝擊，並在瞬息萬變的商業環境中蓬勃發展。

Howard Kerr  
BSI 集團執行長

# 內容



# 1

## 報告摘要



## 報告摘要

- 以技術問題最為顯著：無預警的技術事件在過去的營運衝擊和未來的威脅排行榜中都居於首位：無預警的資訊與通訊中斷引起近 12 個月來大部份的營運中斷，而網路攻擊及資料外洩則是未來最受關注的議題。
- 惡劣氣候被視為較大威脅：2018 年一系列的天氣事件（例如歐洲的暴風雪、美國的野火和全球嚴重的風暴）意味著受訪者將天氣視為關鍵的未來威脅，在未來營運中斷的名單中排行第三。
- 政局變化回歸未來威脅的前十名：政局變化自 2015 年以來首度進入未來威脅名單的前十名。英國脫離歐盟增加了歐洲的不確定性，以及這為全球整體政局帶來的未知數，受訪者以此為證，認為這是未來 12 個月的重大挑戰。

### 前 10 大營運衝擊 ( disruptions ) - 過去 12 個月



2

安全衛生事件  
Health and safety incident



3

缺乏人才 / 關鍵技術  
Lack of talent/Key skills



4

網路攻擊與資料外洩  
Cyber attack & data breach



5

產品品質事件 / 產品回收下架  
Product quality incident/  
product recall



6

異常氣候 / 自然災害  
( 如：颶風 / 地震 )  
Adverse weather/natural disaster



7

匯率波動  
Exchange rate volatility



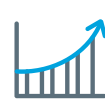
8

自然資源短缺  
Natural resources shortage



9

法規變更  
Regulatory changes



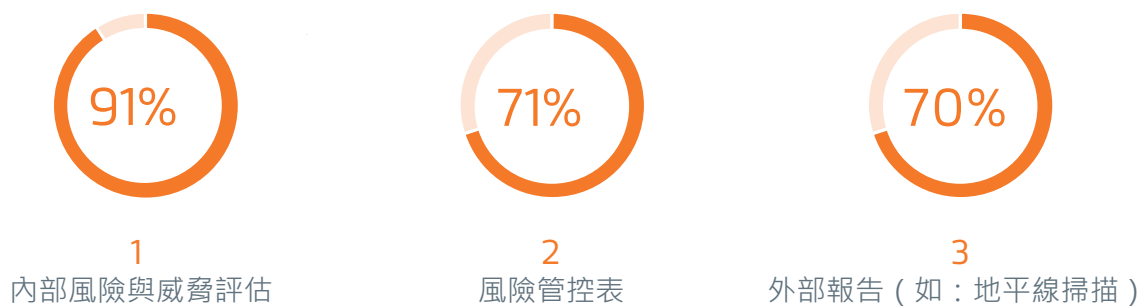
10

借貸成本提高  
Higher cost of borrowing

## 前 10 大營運威脅 ( threats ) - 未來 12 個月

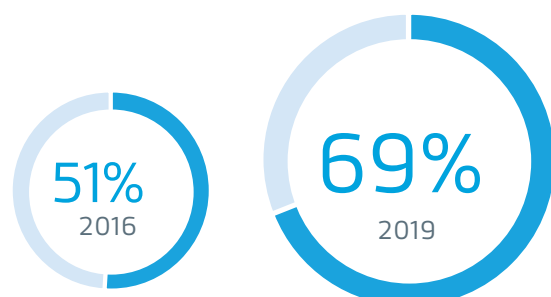


## 風險與威脅評估方法



## ISO 22301

有 69% 的人使用 ISO 22301 作為預防營運中斷的管理架構或進行驗證，證實這些年來的採用率有所成長。

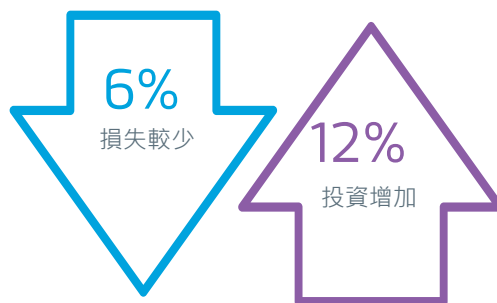


### 最昂貴的營運衝擊 (以美元計算的累積金額)



採用營運持續計畫超過一年的組織，他們的報告顯示在過去的 12 個月因營運中斷所遭受的損失 (6%) 低於平均值 (7%)。

規劃在未來 12 個月增加營運持續投資預算的組織在過去 5 年增加了 12%。



### 組織韌性意味著什麼



### 組織韌性從何落實





# 2

## 主要報告



## 營運持續的基準化分析

ISO 22301 的採用率較去年略為下降 ( 從 70% 降至 69% )，儘管決定驗證該標準的組織也有所減少 ( 從 16% 降至 14% )，然而，這些年來承諾符合該標準的組織比例則是增加的 ( 圖 2 )，顯示對組織的營運持續而言，ISO 22301 仍是關鍵的標準。

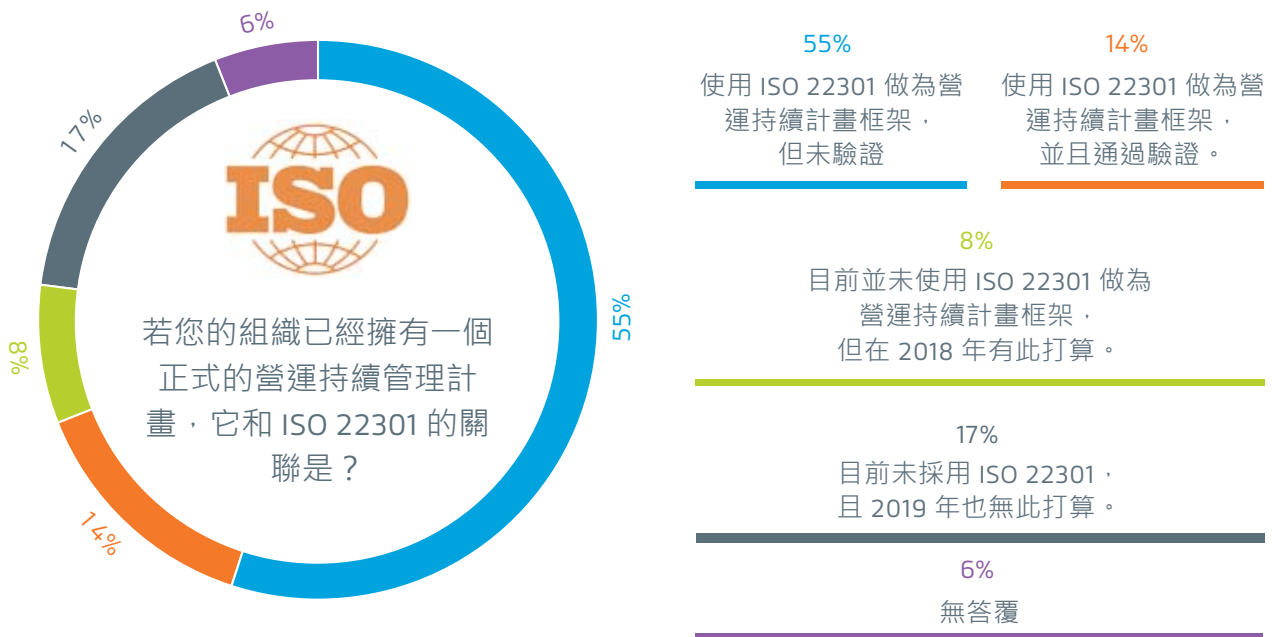


圖1. 若您的組織已經擁有一個正式的營運持續管理計畫，它和 ISO 22301 的關聯是？

年份	ISO 22301 採用率
2016	51%
2017	63%
2018	70%
2019	69%

圖2. 組織採用 ISO 22301 的近期統計

## 風險與威脅評估—過去12個月

關於組織過去營運遭受衝擊的部分今年新增一項分析層面，我們要求受訪者對營運衝擊的頻率和影響進行相關評分。這項作法的改變讓我們能夠將風險評分繪製在表 3 中，更能夠掌握營運衝擊對組織的影響程度。

	頻率*	影響**	風險 評分
資訊與通訊中斷	6.39	2.07	13.22
安全衛生事件	7.16	1.8	12.88
缺乏人才 / 關鍵技術	5.94	2.10	12.47
網路攻擊與資料外洩	6.45	1.92	12.38
產品品質事件 / 產品回收下架	5.62	2.01	11.29
惡劣氣候 / 自然災害 (如颶風 / 地震)	5.03	2.20	11.06
匯率波動	5.25	2.05	10.76
自然資源短缺	5.13	1.99	10.20
法規變更	4.58	2.06	9.43
借貸成本提高	4.63	2.02	9.35
公共服務中斷	4.85	1.92	9.31
政治暴力 / 內亂	4.78	1.93	9.22
關鍵基礎設施失效	3.95	2.32	9.16
聲譽事件	3.86	2.12	8.18
供應鏈中斷	4.22	1.9	8.01
孤狼式攻擊者/濫射槍手事件	3.55	2.25	7.98
新科技的引進 (區塊鏈、人工智慧、物聯網)	4.24	1.78	7.54
政局變化	3.59	2.10	7.53
疾病爆發	3.34	2.06	6.88

表3. 風險評分表(母體數=411)

\* 根據群體平均值，事件在過去一年發生的頻率。滿分=20

\*\* 根據群體平均值，事件在過去一年發生所造成的影響，其中1=不嚴重，而4=極嚴重



## 非實體營運中斷

資訊中斷是企業第三常見的中斷事件，平均影響程度介於中等和重大之間。另一方面，網路攻擊的稍為頻繁，但影響程度較低，介於不嚴重和中等之間。儘管調查樣本中的網路攻擊事件影響程度並非最大，但其發生頻率仍使網路威脅成為組織最大的挑戰之一。其他類似的產業報告也有一致的發現，即網路攻擊為最常反覆發生的威脅之一，儘管並不總是導致重大或極嚴重的損害<sup>1</sup>。

## 品質保證

涉及產品品質而且可能導致產品回收下架的事件頻率是營運衝擊事件的前幾名（第五名），據受訪者表示具中等影響。這對組織可能是真正的挑戰，尤其是職業健康和 safety 事件——可能和產品品質有關——在過去 12 個月是最常見的事件類型。這符合業界關於安全衛生事件的報告，例如在英國，這類的危害仍持續增加<sup>2</sup>。此外，英國幾個大零售商由於在聖誕節期間對健康造成危害，必須召回從衣物到寵物食品等不同的產品<sup>3</sup>。

## 自然災害

惡劣的氣候事件，例如颶風、暴風雪和極度的高溫，仍是組織主要的挑戰之一，在影響最大（第 3 名）和頻率最高（第 8 名）的評分中佔有一定重要性。此外，自然資源短缺的相關議題亦被評為今年最主要的挑戰之一，在風險評分表中排名第八。值得強調的是，儘管這些事件可能被歸類為黑天鵝，但根據這份報告進行的統計分析，它們光是過去 12 個月，對組織造成的影響便已超過 5 次。

## 政局變化與新法規

政局變化事件在過去對組織的影響頻率較低，但在影響最大的評分卻是前幾名（第 5 名），介於中等和重大影響之間。此外，一系列的相關營運中斷事件，例如缺乏人才和關鍵技術以及匯率波動在頻率和影響方面都是前十名。一項 BCI 著重於英國脫歐的政局變化研究報告也進一步證實這點，顯示組織對於英國脫離歐盟一事並未做好準備，尤其是在就業和金融等領域的動盪<sup>4</sup>。



1. WEF Global Risk report 2018; UK National Risk Register 2017

2. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/741286/Enclosure\\_1\\_MOD\\_Health\\_and\\_Safety\\_Statistics\\_Annual\\_Report\\_2017-18.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741286/Enclosure_1_MOD_Health_and_Safety_Statistics_Annual_Report_2017-18.pdf)

3. <https://www.gloucestershirelive.co.uk/news/cheltenham-news/products-being-recalled-lidl-aldi-2308641>

4. Brexit preparedness report

## 黑天鵝

今年的報告顯示頻率低且影響大的事件，即所謂的黑天鵝，實際上會在不同的場合對組織造成影響。例如根據報告，關鍵的基礎設施失效是最具破壞性的事件，即使它們並非頻率最高的營運衝擊事件，但它們在過去 12 個月仍對組織造成平均將近 4 次的影響。同樣地，孤狼式攻擊者是過去 12 個月影響第二大的事件，發生次數為三至四次。極端氣候事件已證實觀察到前述的類似情況。

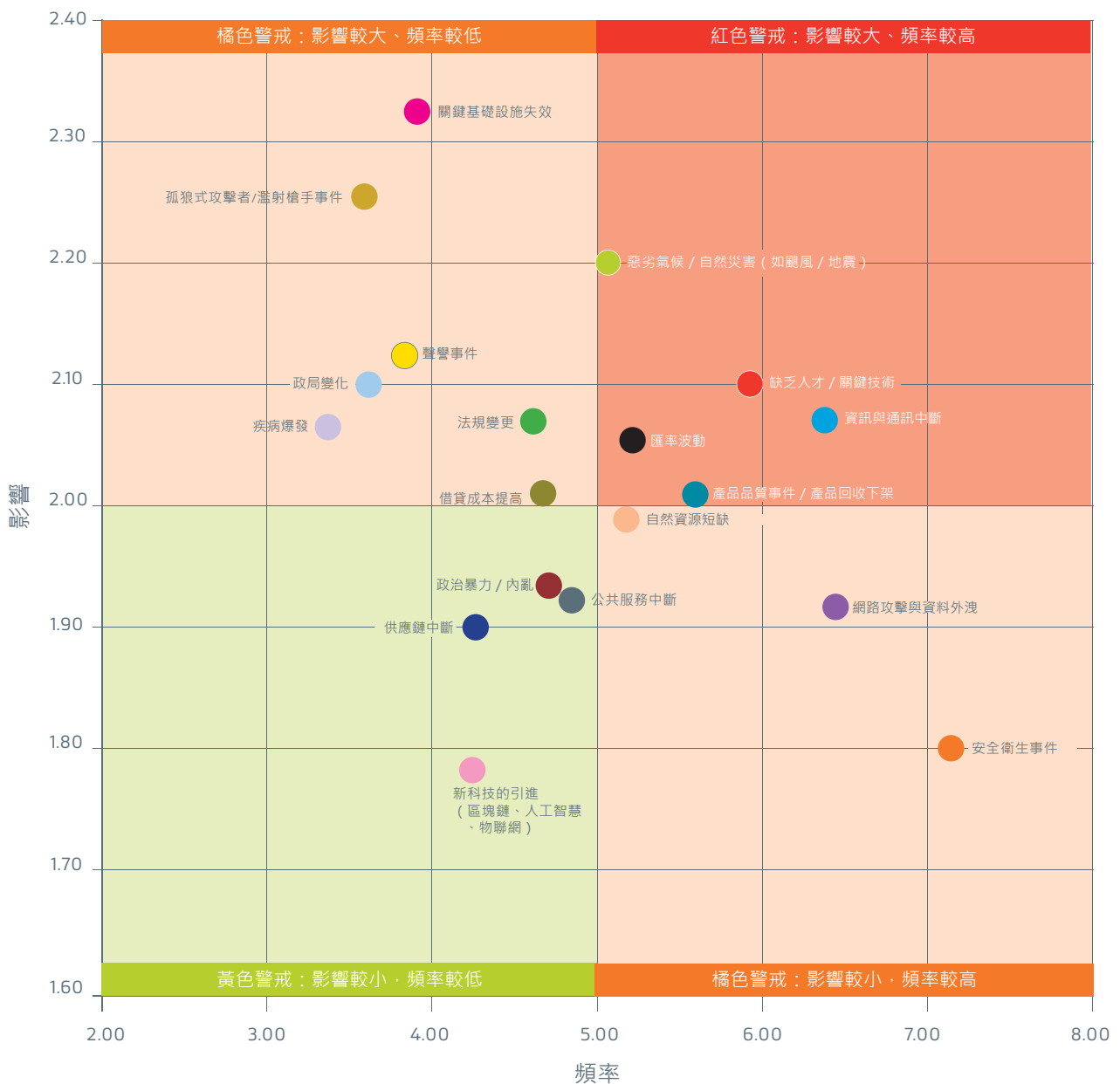


圖4.以下營運中斷事件的發生頻率和影響程度為何？(母體數=411)

## 風險與威脅評估：未來12個月

在第二部分的風險與威脅評估中，受訪者報告了未來的營運中斷因素。他們特別為未來威脅發生的可能性和影響進行風險評分。結果顯示，受訪者覺察未來可能發生的風險與實際發生的事件之間存有差異。分析顯示，專業人員更加擔憂那些影響力大的威脅和黑天鵝，即使較常反覆發生的事件（例如：健康和 safety 事件）可能會造成同樣的損害。

	頻率*	影響**	風險評分
網路攻擊與資料外洩	3.25	2.17	7.05
資訊與通訊中斷	3.12	1.91	5.95
惡劣氣候 / 自然災害 (如颶風 / 地震)	3.01	1.82	5.47
關鍵基礎設施失效	2.48	2.19	5.43
聲譽事件	2.53	2.02	5.11
法規變更	2.95	1.63	4.80
缺乏人才 / 關鍵技術	2.73	1.68	4.58
供應鏈中斷	2.5	1.78	4.45
公共服務中斷	2.67	1.65	4.40
政局變化	2.66	1.58	4.20
新科技的引進 (區塊鏈、人工智慧、物聯網)	2.63	1.57	4.12
安全衛生事件	2.69	1.53	4.11
孤狼式攻擊者/濫射槍手事件	1.71	2.32	3.96
匯率波動	2.31	1.57	3.62
疾病爆發	2.01	1.7	3.41
借貸成本提高	2.1	1.48	3.10
政治暴力 / 內亂	1.96	1.55	3.03
產品品質事件 / 產品回收下架	1.83	1.6	2.92
自然資源短缺	1.75	1.54	2.69

表5.風險評分-未來12個月(母體數=345)

\* 根據群體平均值，事件在未來一年發生的可能性，其中1=遙遠，而5=即將發生

\*\* 根據群體平均值，事件在未來一年發生所產生的影響，其中1=不嚴重，而4=極嚴重

### 非實體的營運中斷

網路攻擊和資訊中斷在去年登上營運議題的首要考量，如今也仍持續被評為未來關注的前兩名。然而，很有趣的是，我們注意到網路攻擊的影響分數成長了 13% (從 1.92 至 2.17)，被視為是未來較容易影響組織的事件。在可能性方面，兩種風險都被認為是介於有可能和很有可能之間 (可能性評分 3.25)。

### 政局變化

根據風險評分，政局變化 (4.2) 似乎是未來 12 個月的十大營運中斷因素之一，其他相關威脅包括如法規變更 (4.8)、缺乏人才和關鍵技術 (4.58) 和供應鏈中斷 (4.45)。儘管這有點符合過去營運中斷的分析，但政局變化的財務層面似乎受到忽略，因為和匯率波動相關的損失 (3.62) 和借貸成本提高 (3.1) 被排在十名之外。

### 關鍵基礎設施失效與供應鏈

關鍵基礎設施失效被視為是未來 12 個月內的第四大風險，整體影響評分為 2.19，是僅次於孤狼式攻擊者 ( 2.32 ) 的第二大影響因子。同樣值得注意的是，供應鏈中斷 ( 4.45 ) 進入未來十大威脅的名單，排名第八，發生的可能性被認為介於有可能和很有可能之間 ( 可能性評分 2.5 )。這樣的恐懼可能是隨著英國即將脫歐<sup>5</sup>，多佛海峽 ( Strait of Dover ) 間的貨物流通可能併發其他問題所導致，但也可能是因為如港口等關鍵基礎設施面臨到網路攻擊的威脅所致<sup>6,7</sup>。

### 被低估的挑戰

值得強調的是，部分營運中斷事件在未來 12 個月的狀況似乎備組織所低估。最明顯的例子就是安全衛生事件，儘管它是過去 12 個月最常見的營運中斷原因，但在預測未來風險時只被排在第十二名。同樣地，產品品質和產品回收下架從去年最具破壞性事件的第五名，降至來年的第十四名。如上所述，這代表了組織在展望未來時，一些不是那麼顯而易見的威脅往往被低估了。這可能是因為它們不像網路攻擊那樣惡意，也不像惡劣天氣事件那樣極端，即使它們也會造成高昂的成本支出且具有破壞性。

### 黑天鵝

黑天鵝是未來 12 個月裡組織首要關注的事項。如關鍵基礎設施失效和自然災害等風險是預期最有可能發生並具有高風險評分 ( 分別為 5.47 和 5.43 ) 的營運中斷事件。這類事件可能發生的假設或許反映了過去一年實際發生的頻率，例如：2018 年義大利的莫蘭迪橋 ( Morandi bridge ) 倒塌和加州的營溪路 ( Camp Creek Road ) 大火。



5. <https://www.bbc.co.uk/news/uk-politics-46480374>

6. <https://www.nextgov.com/cybersecurity/2018/12/russia-launched-cyber-attacks-against-ukraine-ship-seizures-firm-says/153387/>

7. <https://timesofsandiego.com/crime/2018/11/28/2-iranian-men-face-federal-charges-in-cyber-attack-on-port-of-san-diego/>

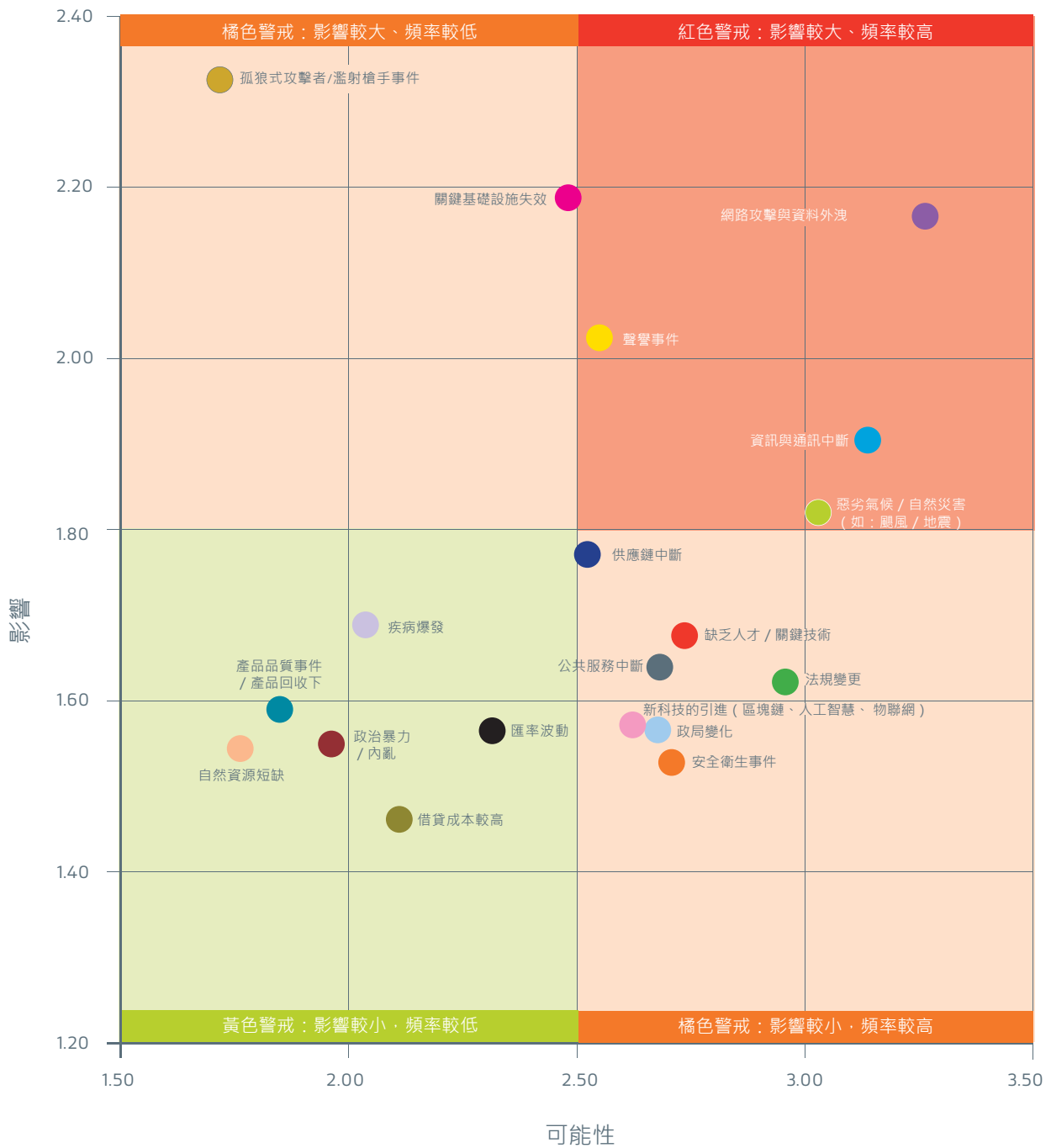


圖6. 風險與威脅評估 – 未來12個月

大多數組織 ( 78% ) 會依據前一年的努力成果進行趨勢分析 ( +6% )。此外，表示完全未進行趨勢分析的專業人員數量在今年減少 7%，整體總計為 16%，顯示地平線掃描的影響正在成長。



## 過去對比未來

惡劣氣候越來越令人擔憂：

惡劣氣候被評為過去 12 個月營運中斷事件的第五名，但在受訪者意識到的未來威脅表中，上升至第三名。今年與氣候相關的事件增加，例如：影響歐洲的暴風雪和澳洲的熱浪更是加強了這樣的擔憂。

全球政局的不穩定不再事不關己：

政局變化過去 12 個月在風險排行榜的倒數第二名停滯不前，但美國一年來的政局不明朗再加上歐洲面臨英國脫歐的挑戰，將政局不穩定推進未來 12 個月的前十大威脅。

網路攻擊位居未來挑戰名單之首：

網路攻擊為過去 12 個月第四大營運中斷事件，但如今在未來威脅的名單上已躍升至首位。過去 12 個月，有許多令人矚目的攻擊事件發生在那些人們以為能夠防止這些攻擊事件的公司（例如：Google 和 Apple），這表示網路攻擊為如今已成為董事會會討論的重要議題：確實，埃森哲（Accenture）顧問公司指出，2016 年至 2017 年間在因應網路攻擊方面的成本花費已增加 23%，顯示這是成長中的挑戰。



## 朝韌性邁進

一半以上的受訪者 ( 51% ) 將「組織韌性」( Organizational Resilience ) 視為企業長期生存的基本要素，但超過四分之一 ( 28% ) 的受訪者只從中聯想到企業的持續營運。而在「其他」選項中提供不同答案的受訪者中，有 70% 的人相信組織韌性必須是全面性的，而且涵蓋所有單位，例如：企業的持續營運、危機管理、事件應變和災難復原。根據這樣的概念，幾乎三分之二 ( 61% ) 的受訪者確信組織中的每個人都應該為組織韌性負責。此外，在受訪的專業人士中有超過四分之一的人 ( 26% ) 認為組織韌性應是高階管理者的策略重心之一。

組織韌性意味著什麼	組織韌性從何落實
企業長期生存	組織中的每個人
營運持續	高階管理者
全面性的方法	營運持續

表7. 與組織韌性的意義與責任相關的前三大用詞

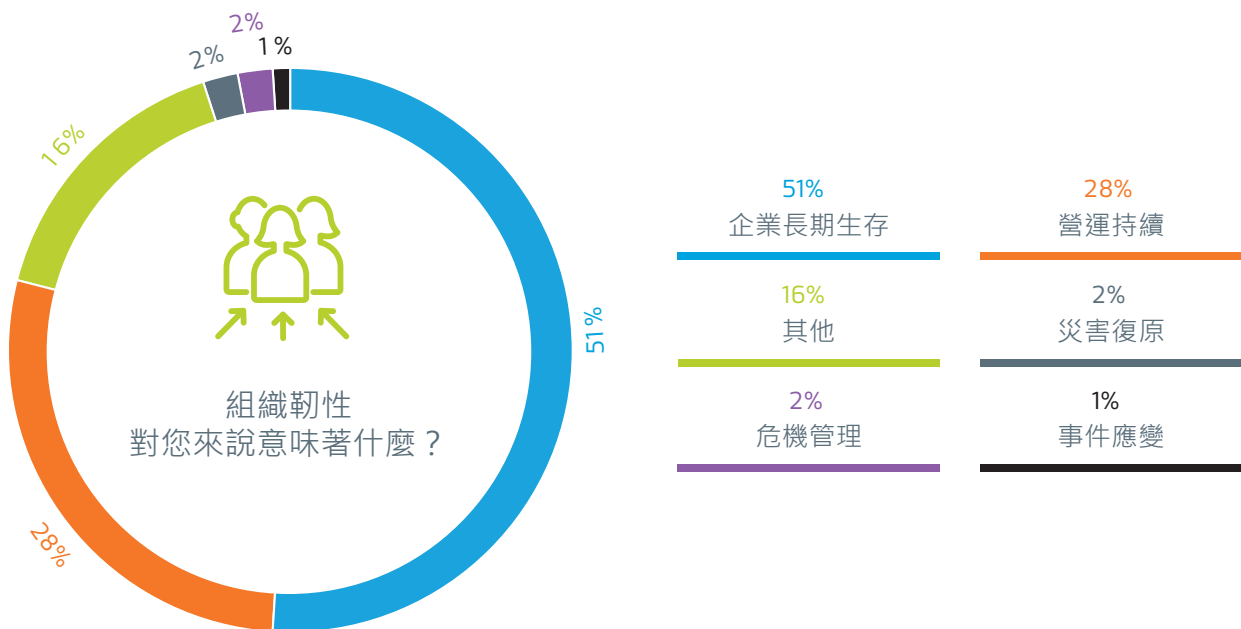


圖8. 組織韌性對您來說意味著什麼？(母體數=342)

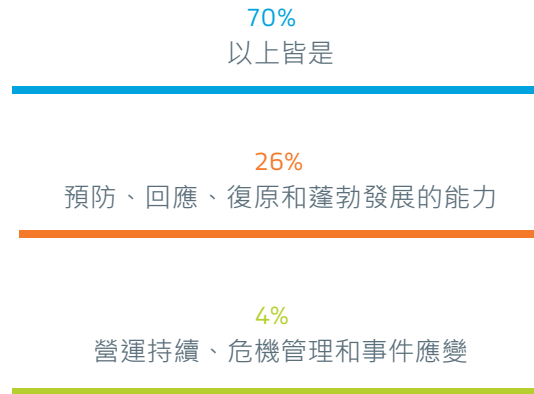
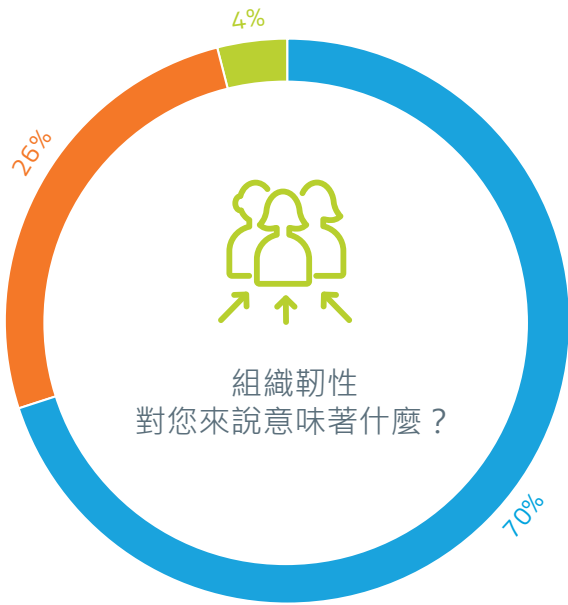


圖9. 組織韌性對您來說意味著什麼? (選擇「其他」; 母體數=53)

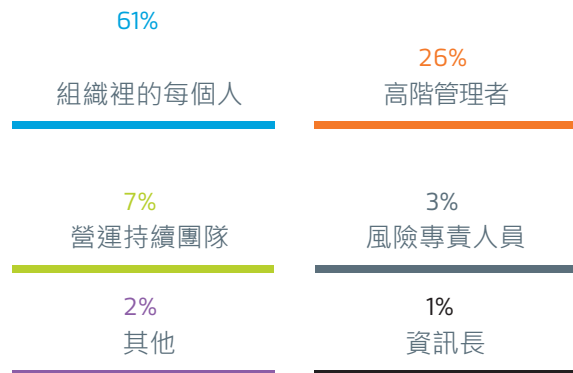
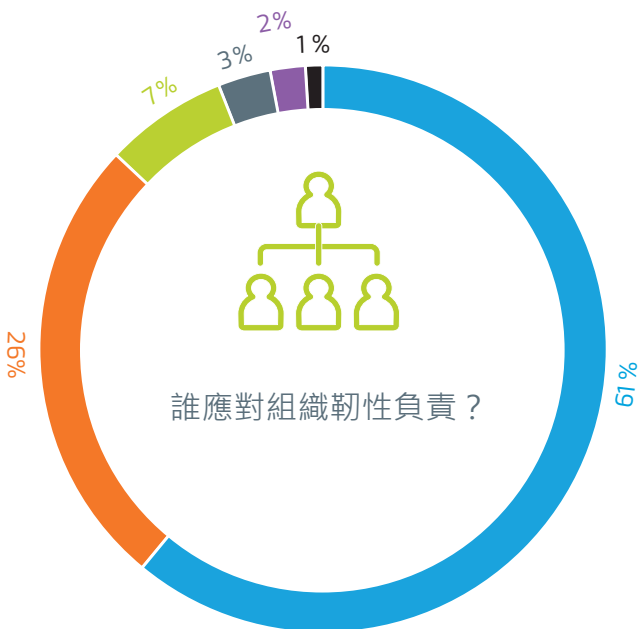


圖10. 誰應對組織韌性負責? (母體數=339)

# 個案討論

## 產品品質事件：被低估的風險



美國食品與藥物管理局 ( United States Food and Drug Administration ) 在 2018 年報告了將近 400 件因影響安全衛生而回收下架商品的案例。例如某家全球食品零售商因危及消費者生命安全的消毒疑慮，被迫回收超過 60,000 件商品。所幸該組織迅速採取行動，因而沒有造成實質的傷害。但由於事件發生在冬季的假期，商品遍及包括美國的 26 個國家，讓回收行動變得相當複雜。同樣的，某家極受歡迎的速食連鎖店因為擔心他們的莎莎醬疑似含有有害細菌<sup>1</sup>，因而必須回收他們的其中一項產品。不幸的是，安全衛生的危害也可能由具惡意的行為者所導致。2018 年便有數件罪犯損害產品的案例，例如藏針的澳洲草莓和德國麵包，以及巴基斯坦導致超過 30 人死亡<sup>2</sup> 的受污染甜食。隨著產品離開組織的供應鏈，要辨識並反擊這類的事件就會變得很困難，因為在不同的地區會涉及多項的因素。然而，技術可能會提供部分迫切需要的協助。例如，世界自然基金會( WWF )提出可追蹤鮭魚供應鏈的區塊鏈工具，因為在先前的事件中，有其他魚種被標示為鮭魚並以罐裝出售。可想而知，推出這類創新的過程並不總是那麼順利，因為在區塊鏈的每個環節都必須嵌入新技術而且要懂得如何使用，這可能才是真正的挑戰<sup>3</sup>。此外，唯有先承認問題才能夠進步。今年的地平線掃描顯示，儘管安全衛生事件非常頻繁且代價高昂，但專業人員以長期的眼光來看，往往不會將這類的事件視為主要的威脅之一。對風險的覺察及其實際發生的狀況之間的差異，對組織是一種威脅，在危機發生時，可能會讓人措手不及。



1 <https://www.fda.gov/Safety/Recalls/ArchiveRecalls/2018/default.htm?Page=1>

2 <https://www.dw.com/en/food-tampering-scandals-that-shocked-the-world/g-45516037>

3 <https://newfoodeconomy.org/blockchain-seafood-supply-chain-traseable-sea-quest-viant-wwf/>

# 個案討論

## 關鍵基礎設施失效：黑天鵝變成白天鵝



黑天鵝指的是突如其來的打擊事件，會對受影響的事物造成重大衝擊。黑天鵝理論在 2007 年由 Nassim Nicholas Taleb 發明，徹底改革了組織對風險的管理和預測的方式。作者試圖傳達的主要訊息之一就是目前的風險模式不夠有效率，而且可能會因為缺乏遠見而發生難以預測的災難<sup>4</sup>。回顧過去 12 個月，我們可以觀察到關鍵基礎設施失效是如何被視為黑天鵝。例如在 2018 年 12 月，一台無人機進入倫敦的蓋威克 ( Gatwick ) 機場上方領空，導致所有的飛機停飛並延誤數日。這樣的情況被英國的運輸大臣形容為「史無前例」，是過去從未見過的情況<sup>5</sup>。在這個案例中，我們很難不認同 Taleb 所說的，是否為黑天鵝取決於遠見，尤其是先前在機場附近的無人機活動實際上已經發生並且被報導過，但卻受到忽略。在過去兩年的不同時間裡，無人機在倫敦的希斯洛 ( Heathrow ) 機場<sup>6</sup>和魁北克市 ( Quebec City )<sup>7</sup> 撞擊商務機，導致倫敦蓋威克機場的延誤 ( 和 12 月的事件類似，但規模較小<sup>8</sup> )，而葉門的恐怖分子實際上成功地使用無人機襲擊杜拜機場的事件<sup>9</sup>。更重要的是，美國聯邦航空總署 ( Federal Aviation Administration ) 多年來已對危險的無人機活動提出警告，甚至發佈了可能的撞擊情況報告<sup>10</sup>。這些先前的警告證明了無人機風險和媒體及政府敘述的狀況不同，因為這黑天鵝既非未知，也非史無前例的威脅。這和 2017 年英國發生的另一起關鍵基礎設施事件類似，勒索軟體的活動重創了英國國家醫療服務系統 ( UK National Health Service )。這樣的攻擊導致了重大的混亂並使許多人措手不及，即使前一年在其他國家已發生過類似的醫院攻擊事件<sup>11</sup>。這些例子強調了地平線掃描和做好準備的重要性。我們不可能掌握一切風險，永遠都會有我們不知道且未知的情況發生，但保持心胸開放並盡可能地扭轉局面是很重要的。



4 [https://web.archive.org/web/20120907061933/http://www.wrap20.com/files/The\\_Black\\_Swan.pdf](https://web.archive.org/web/20120907061933/http://www.wrap20.com/files/The_Black_Swan.pdf)

5 <https://www.bbc.co.uk/news/uk-england-sussex-46643173>

6 <https://www.bbc.co.uk/news/uk-36067591>

7 <https://money.cnn.com/2017/10/16/technology/drone-passenger-plane-canada/index.html>

8 <https://www.bbc.co.uk/news/uk-40476264>

9 <https://www.aljazeera.com/news/2018/07/yemen-rebels-attack-abu-dhabi-airport-drone-180726155103669.html>

10 <https://www.businessinsider.com/faa-report-of-drone-incidents-2016-3?r=US&IR=T>

11 BCI Cyber Resilience Report 2017

# 3

財務損失



本報告接下來分析的部分是財務損失超過年營業額 7% 的組織，透過統計分析可推知各種威脅累積的財務損失金額。

從過去的營運中斷找出趨勢並加以確認時，我們發現安全衛生事件具有重大影響，是導致組織最多支出的事件，損失高達 11.86 億美元，緊接著是聲譽損害，損失達 10.36 億美元。組織對安全衛生事件在未來 12 個月可能發生的相關風險缺乏關注也更加令人擔憂。可能也會有人主張，在這張圖表中代價最高昂的兩項營運中斷事件是相關的，因為安全衛生事件可能導致聲譽受損，進而遭到負面報導和外部利害關係人的密切關注<sup>8</sup>。

非實體的營運中斷事件也在前十名內佔據主要位置，總計損失超過 4 億 5000 萬美元，介於網路攻擊（1 億 4500 萬美元）及資訊與通訊中斷（3 億 800 萬美元）之間。另一個值得注意的是，像是區塊鏈或人工智慧的新技術引進，共導致 9700 萬美元的財務虧損。新技術可能導致財務損失的原因很多，例如：組織會因為競爭者研發了新的解決方案而失去機會，或是組織嵌入新技術的實際支出。

如極端氣候事件（5 億 100 萬美元）、關鍵基礎設施失效（2600 萬美元）和政局變化（6600 萬美元）等黑天鵝在圖表中的呈現，再度顯示儘管不太可能，但破壞性高的事件確實會發生，而且會造成支出。值得強調的是，因考量資料分析品質，此部分的損失金額統計實際上源自較小的樣本數。



8. <http://www.hse.gov.uk/business/costs-damage.htm>

## 財物損失

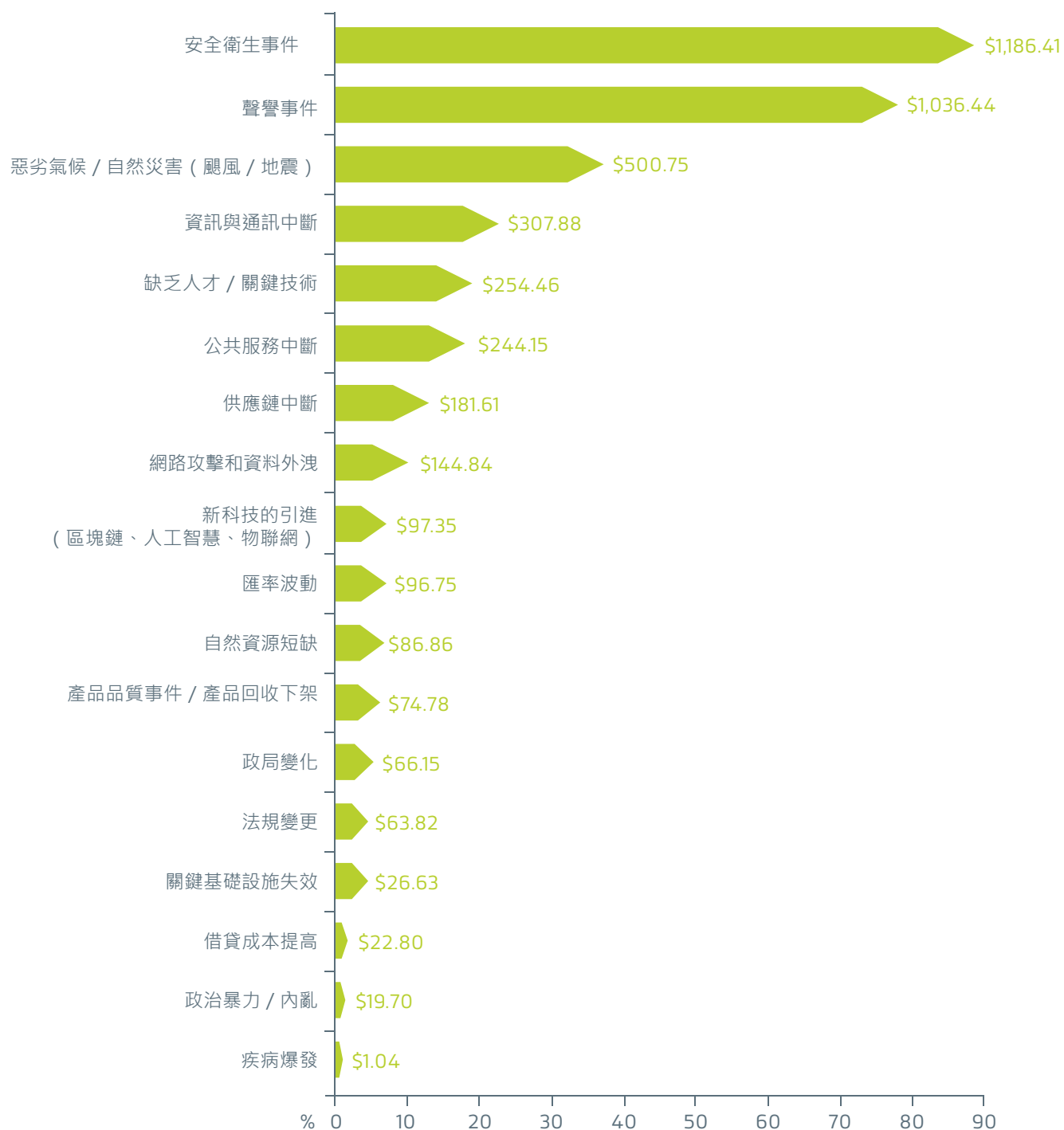


圖11. 造成最大財務損失的營運中斷事件 (年營業額超過7% ; 母體數=28)



## 長期趨勢分析之執行評效

大多數受訪者 (75%) 知曉並且會利用趨勢分析的資料，較前年增加 7%。此外，未取得趨勢分析結果或不會利用其研究成果的受訪者也減少了 7% (從 32% 降至 25%)。這是令人欣慰的消息，這或許意味著組織內的穀倉正在瓦解，越來越多的從業人員能夠取得趨勢分析及其他類似的資料。BCI 先前的研究顯示，建立整合中心有助減少穀倉現象，並可帶動如資訊分享和聯合演習等活動<sup>9</sup>。

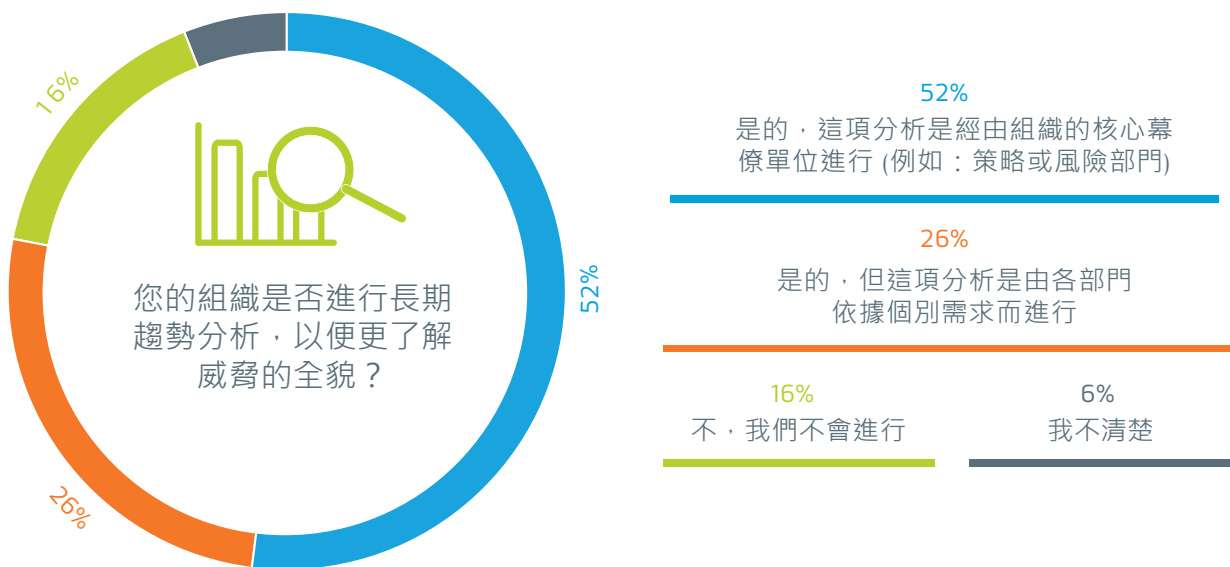


圖12. 您的組織是否進行長期趨勢分析，以便更了解威脅的全貌？ (母體數=332)

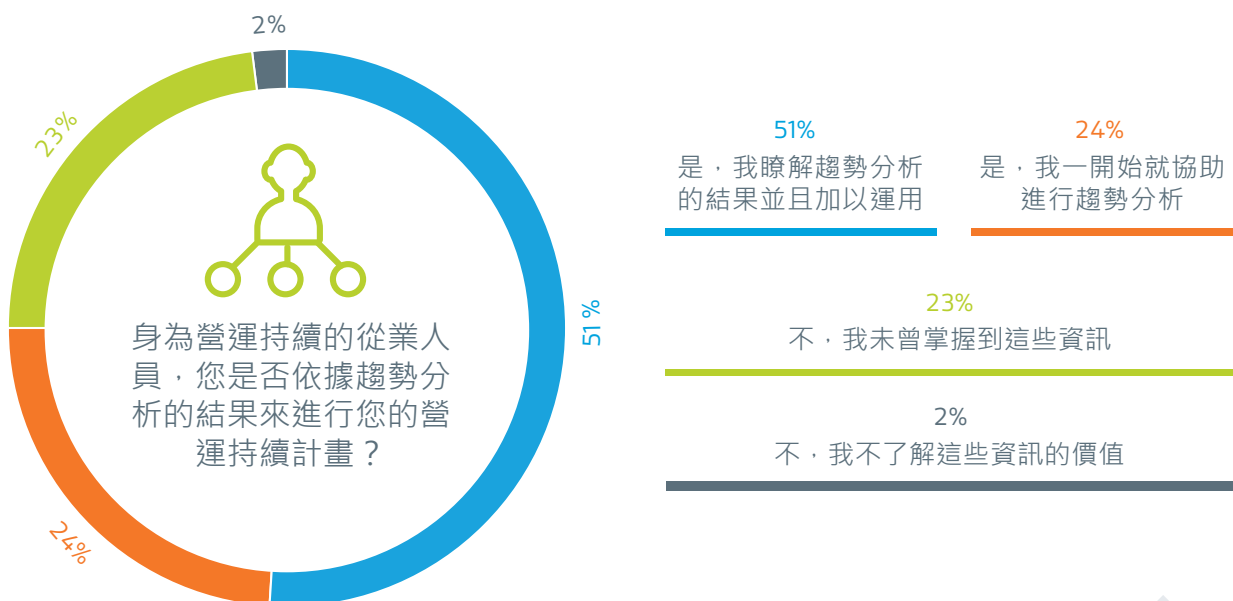


圖13. 身為營運持續的從業人員，您是否依據趨勢分析的結果來進行您的營運持續計畫？ (母體數=332)

組織偏好用來審視未來營運中斷的方式，首要是進行內部風險與威脅評估 ( 91% )，其次是風險管控表 ( 71% ) 和如地平線掃描 ( Horizon Scan ) ( 70% ) 等外部報告。在具體詢問他們如何使用這份報告時，受訪者表示地平線掃描可讓他們的趨勢分析更加完善，而且有助建立準確的復原計畫。此外，這也包括提高風險意識的溝通行動，以獲得最高管理層的支持。很有趣的是，我們觀察到科技的解決方案，例如社交媒體監控 ( 42% ) 和網路安全自動化系統 ( 32% ) 是最不受組織青睞的方式。

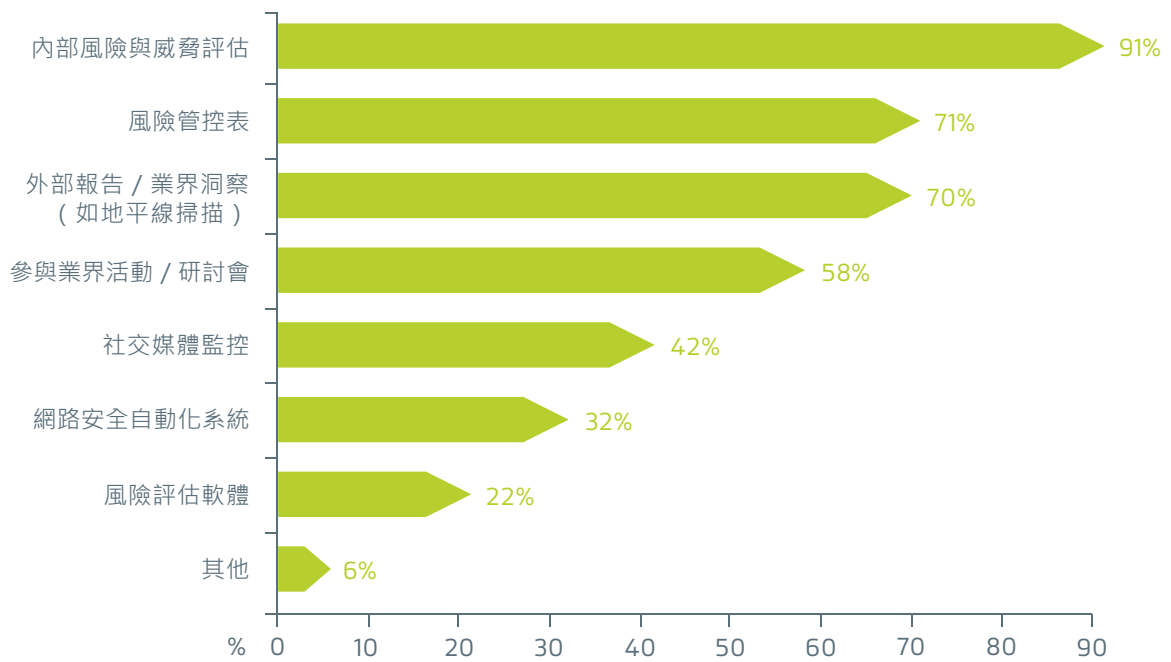


圖14. 您如何進行您組織的風險與威脅趨勢分析？ (母體數=334)

在目前從事營運持續管理規劃的組織中有將近一半具備成熟的方案 ( 五年或五年以上 )，而有將近五分之一 ( 19% ) 的組織已採取三至五年的相關規劃。從事三年或三年以下營運持續的組織數量 ( 33% ) 較符合去年的數字 ( 32% )。更進一步的數據分析顯示，較長期的營運持續規劃與減少營運中斷的損失 ( 6% )<sup>10</sup> 有關，確切地說是低於平均值 ( 7% )。

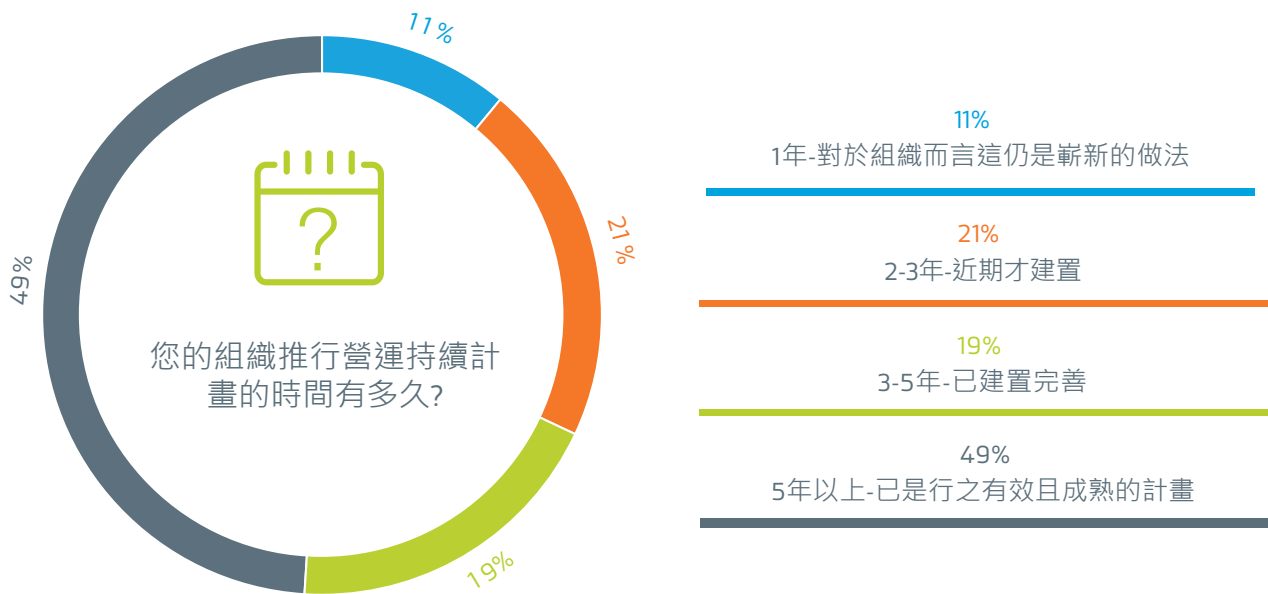


圖15. 您的組織推行營運持續計畫的時間有多久? (母體數=344)

## 未來對營運持續的投資

相較於前一年的結果，專業人士對營運持續效益的領略成長了 5% ( 從 25% 至 30% )。在分析營運持續的投資趨勢時，可看到這些年的穩定成長，顯示需求和資源的增加 ( 表 3 )。儘管需要更進一步的改善提升，但這是朝正確的方向邁進。確實，先前的 BCI 研究顯示，相較於其他如風險管理和資訊安全等組織職能，營運持續的預算仍然不足<sup>11</sup>。

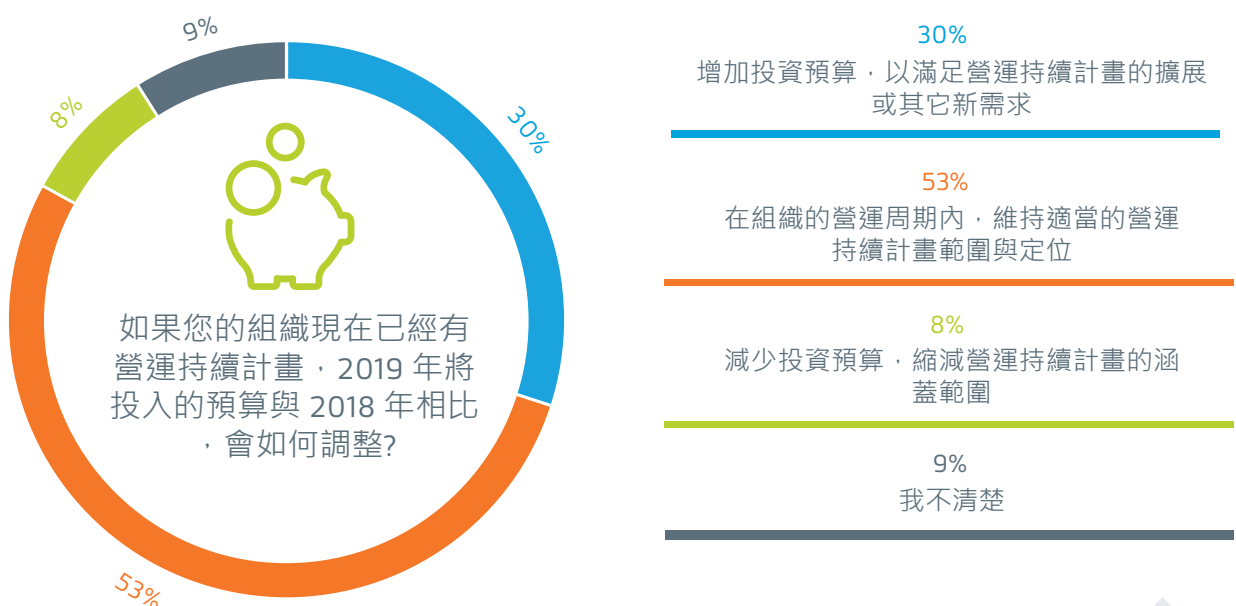


圖16. 如果您的組織現在已經有營運持續計畫，2019 年將投入的預算與 2018 年相比，會如何調整? (母體數=329)

% 與去年同期相比的變動

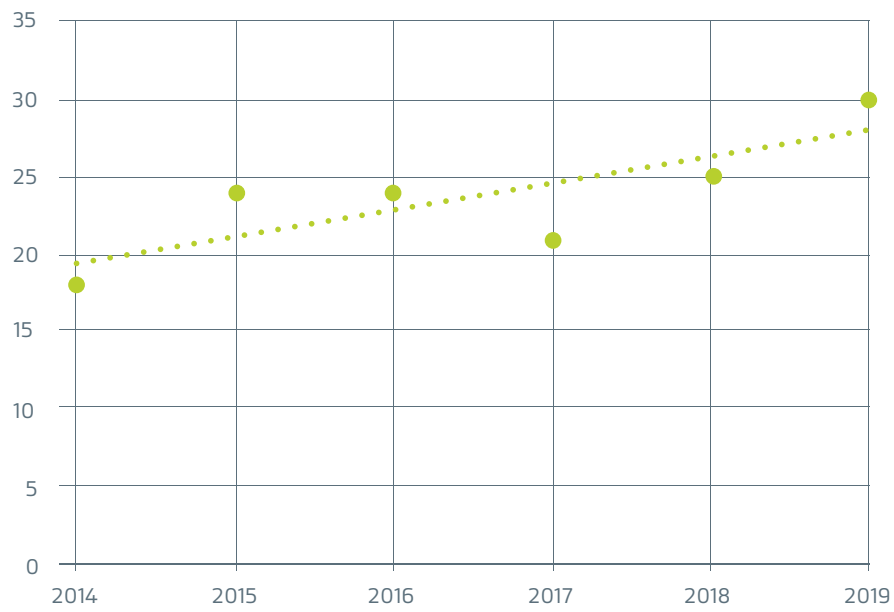
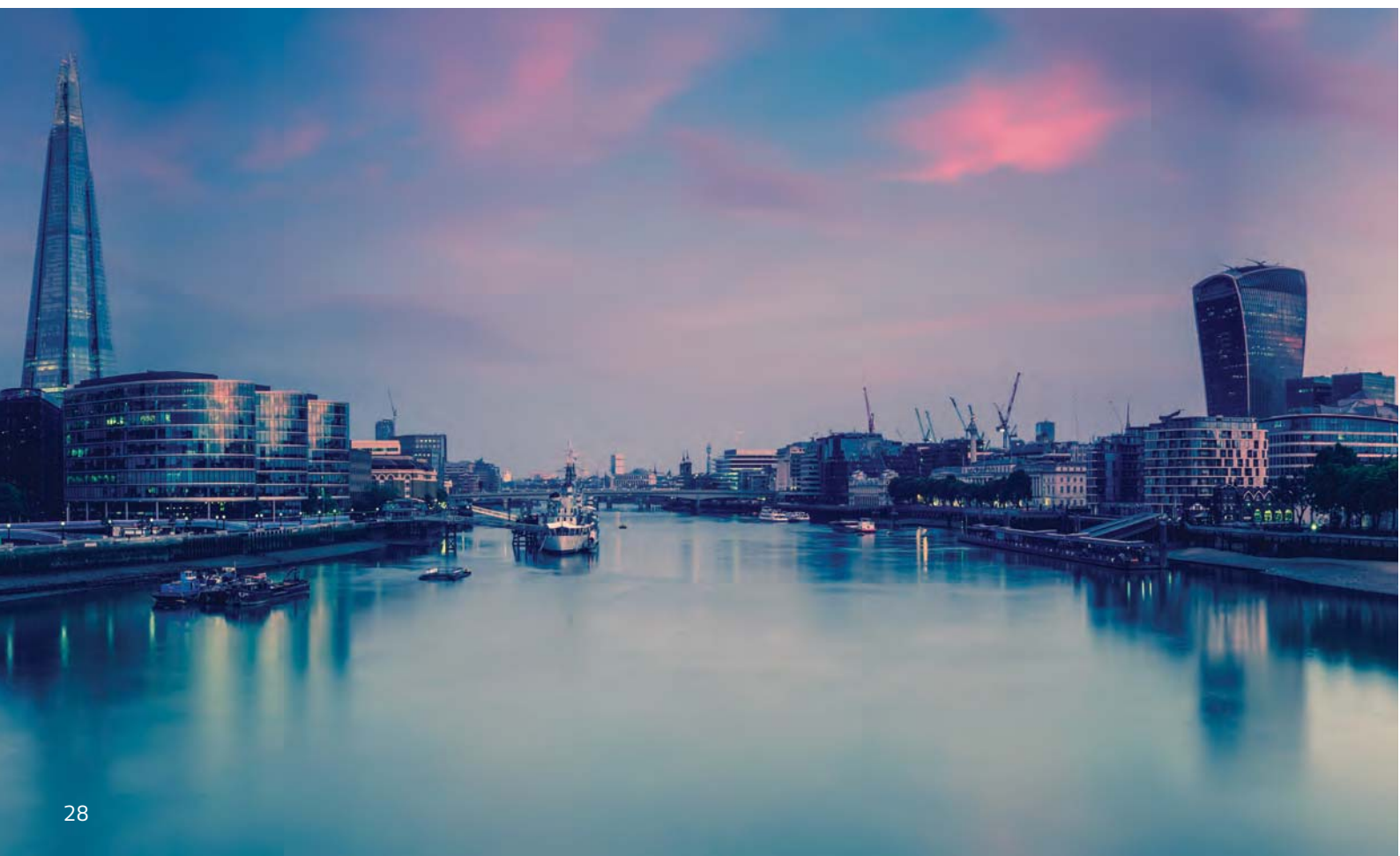


圖17. 組織對營運持續投資的成長幅度，與去年同期相比的百分比變化

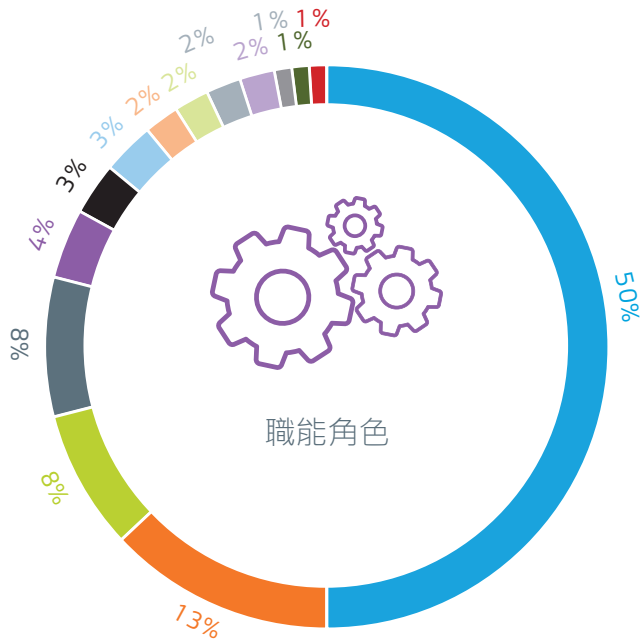


# 4

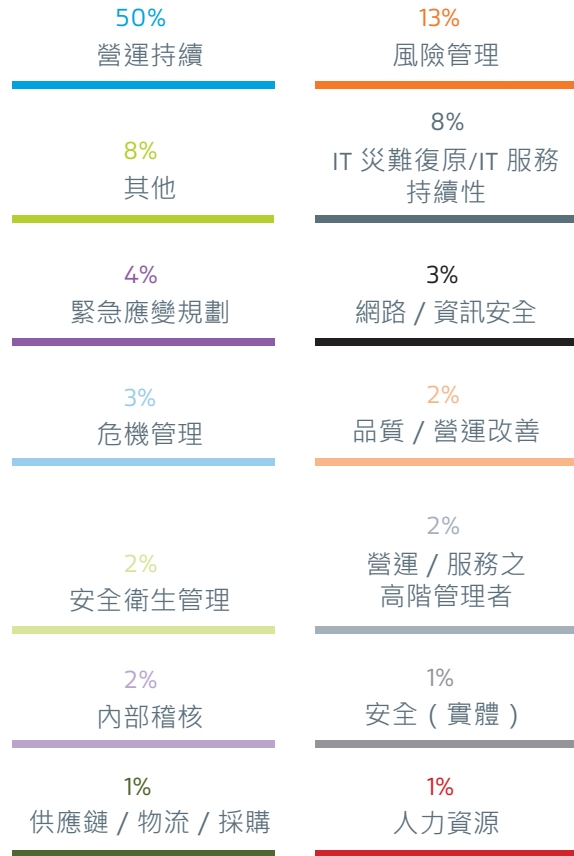
## 附錄



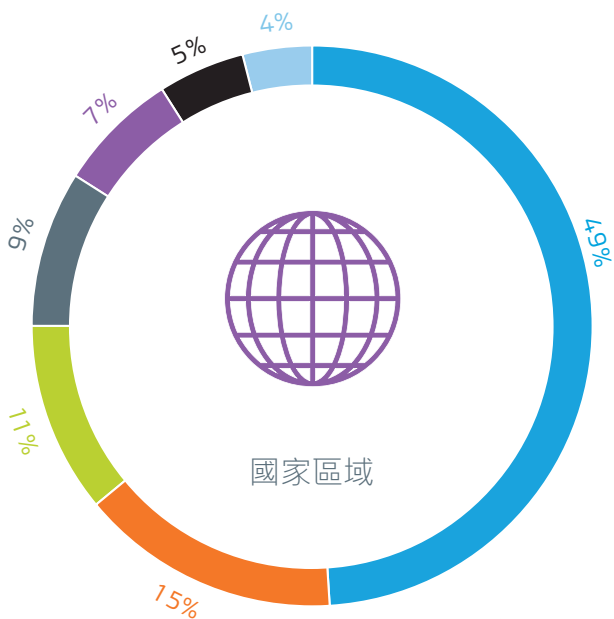
## 人口統計資訊



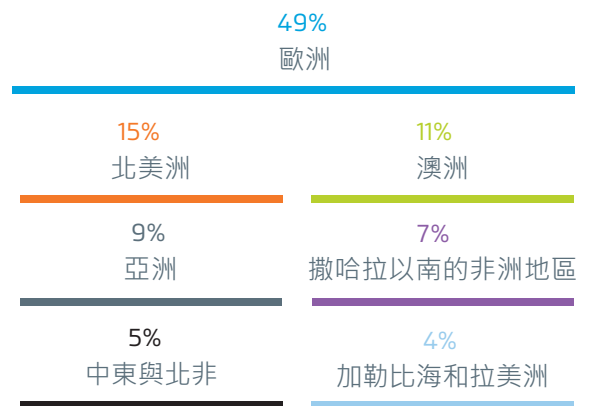
職能角色 (母體數=569)



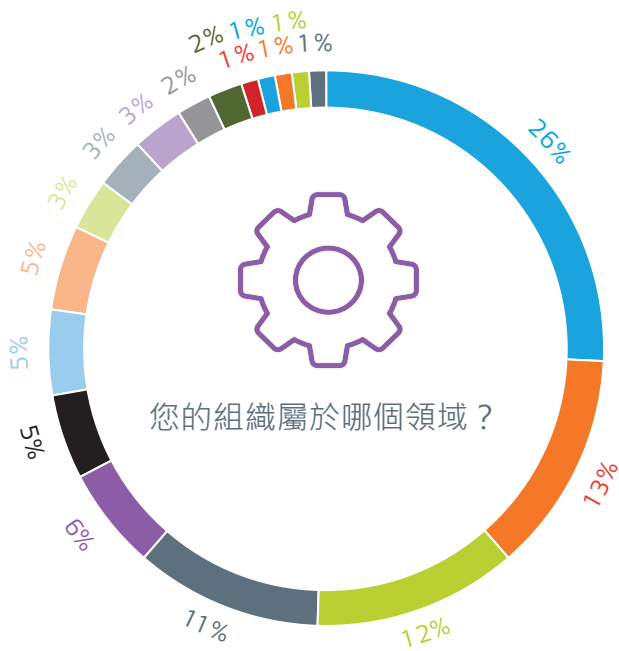
## 地理分佈



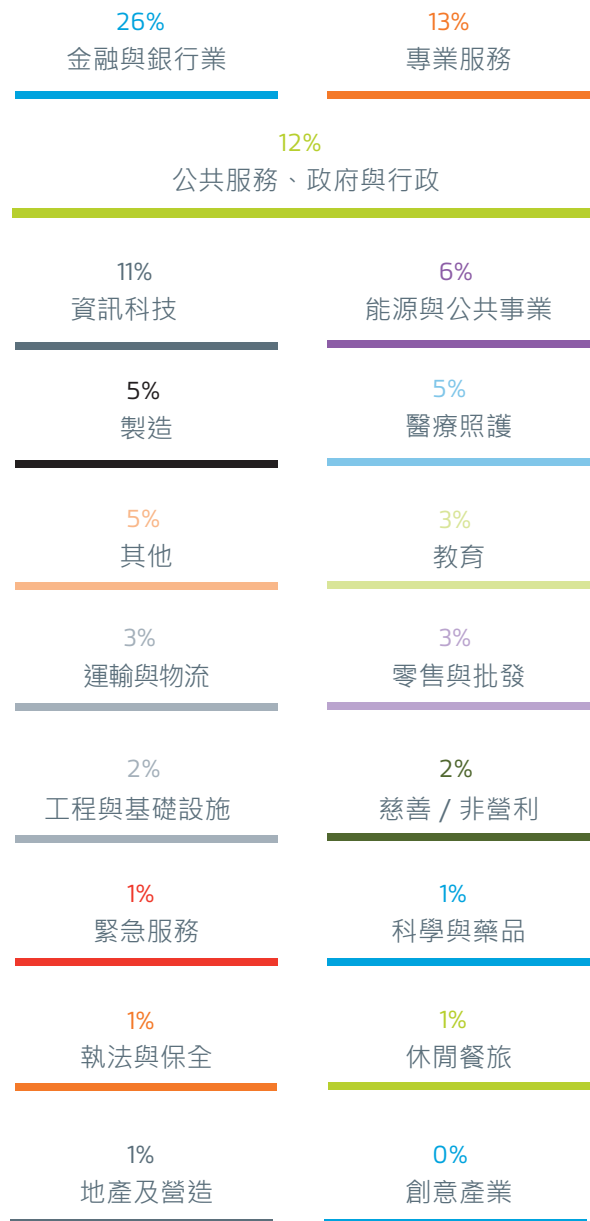
國家(母體數=569)



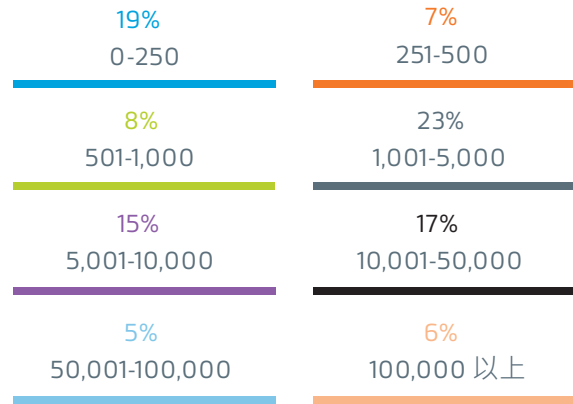
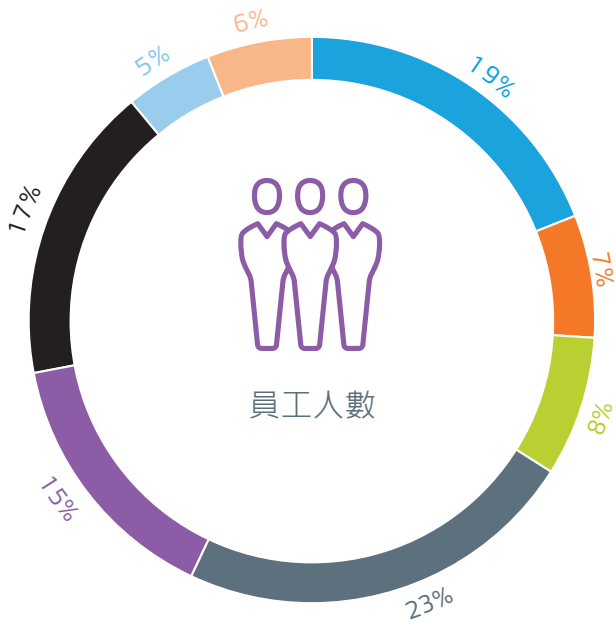
## 產業別



問題2. 您的公司屬於哪個領域？(母體數=569)



## 員工人數



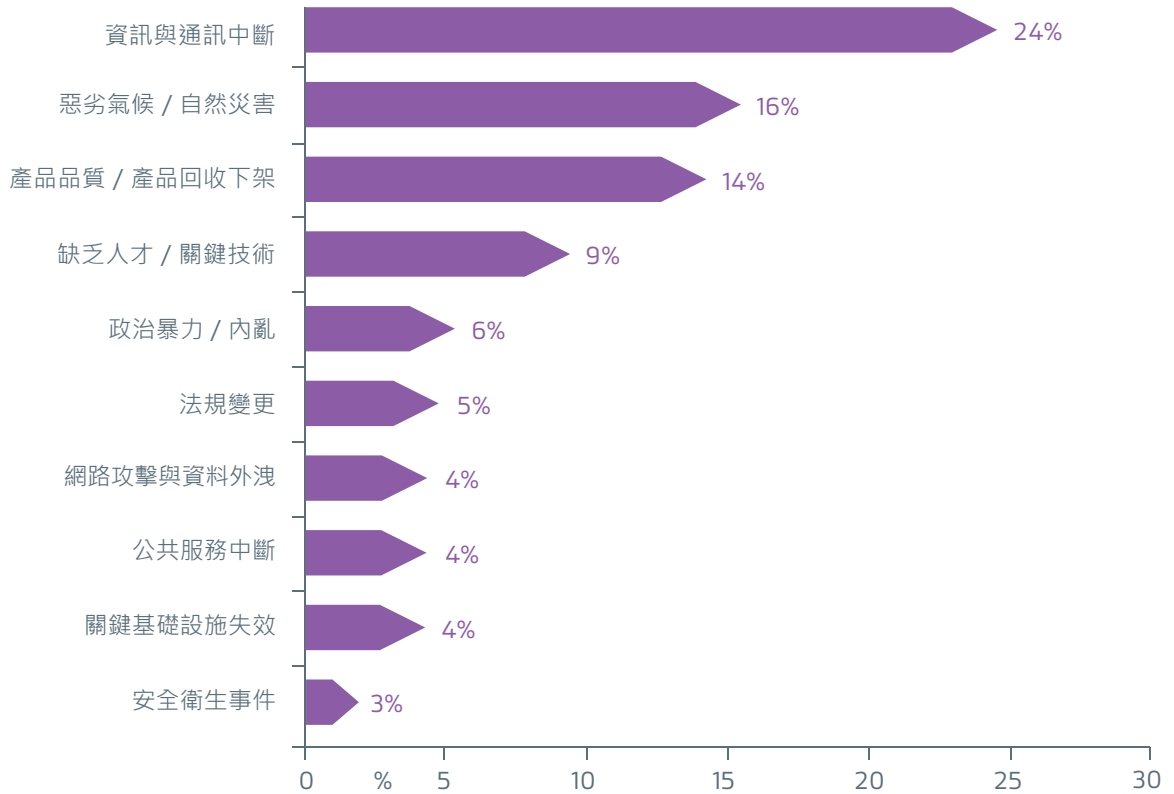
員工人數 (母體數=569)



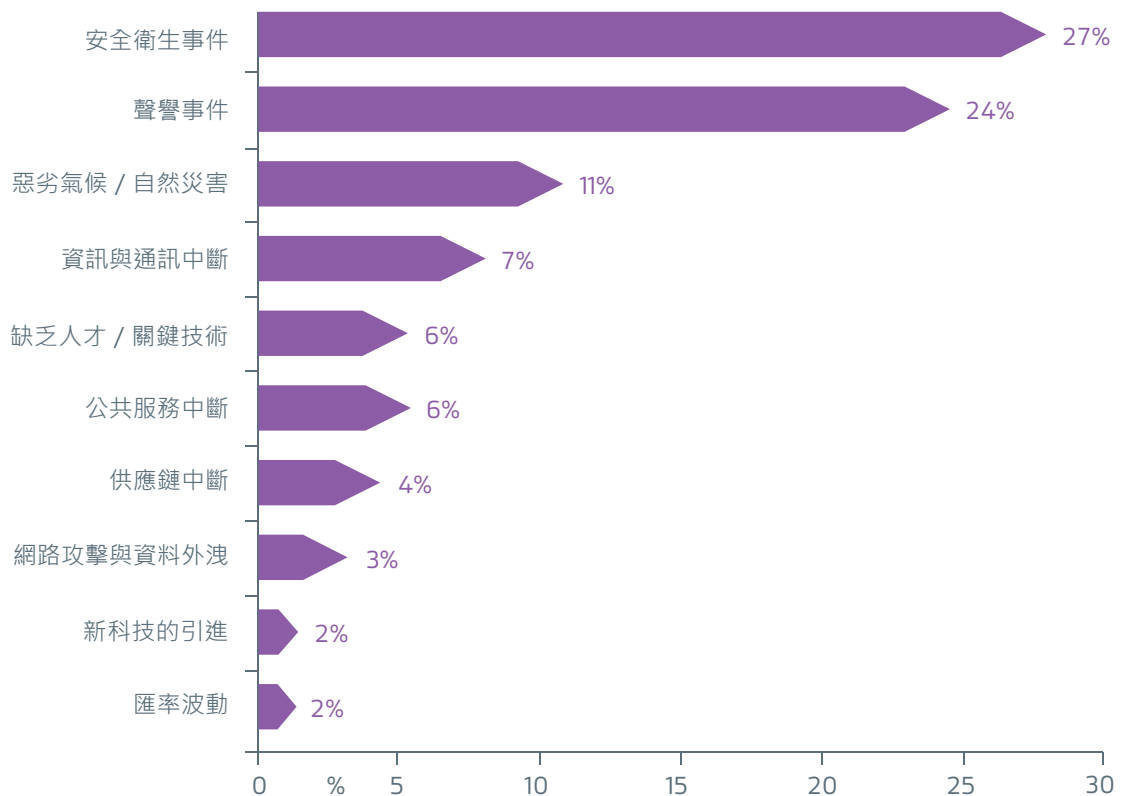


## 財務損失的主要驅動因子：中小企業與大企業

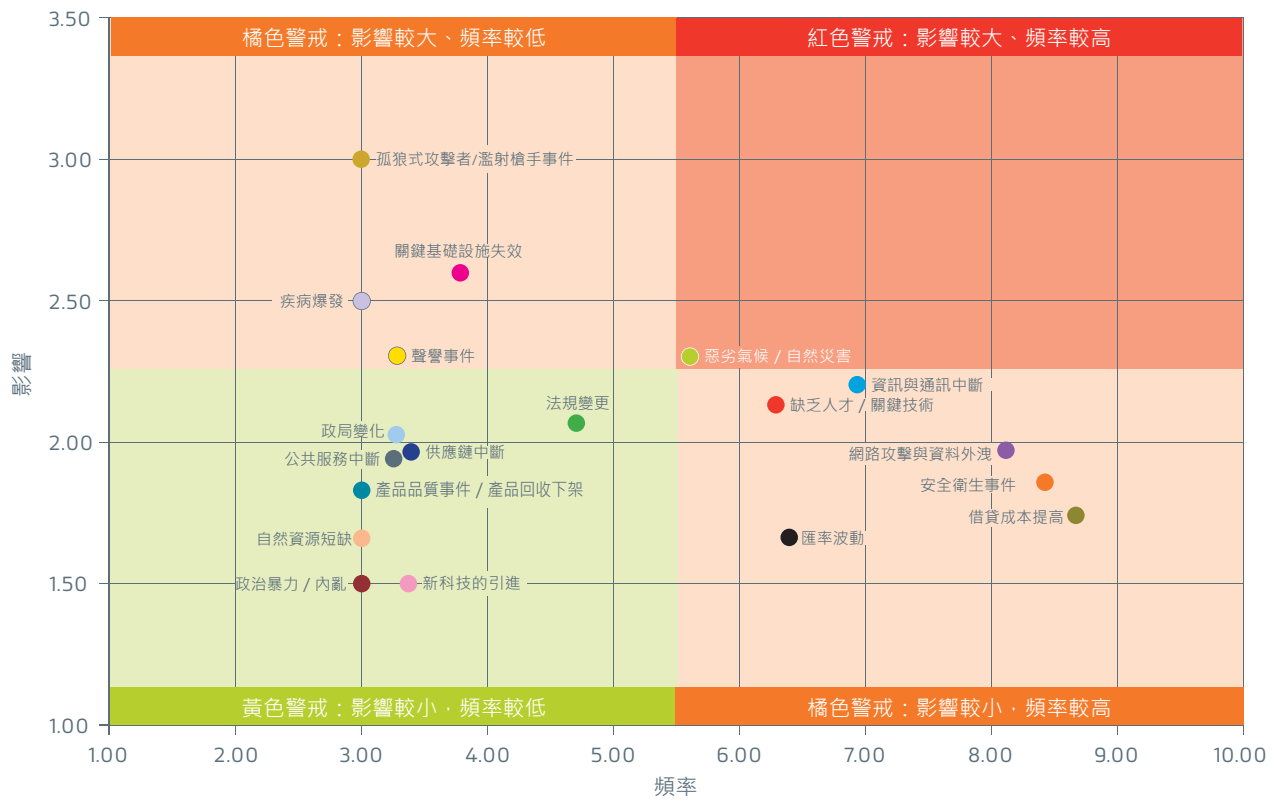
### 中小企業



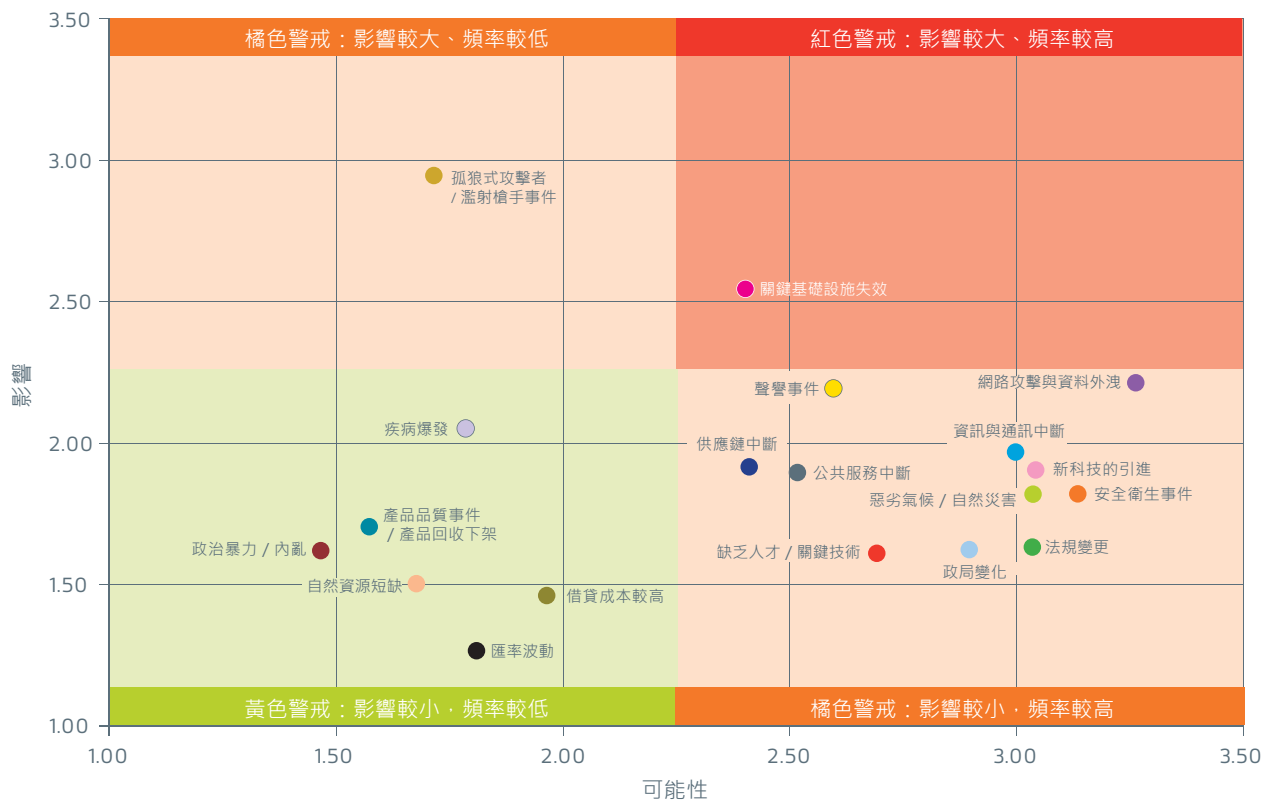
### 大型企業



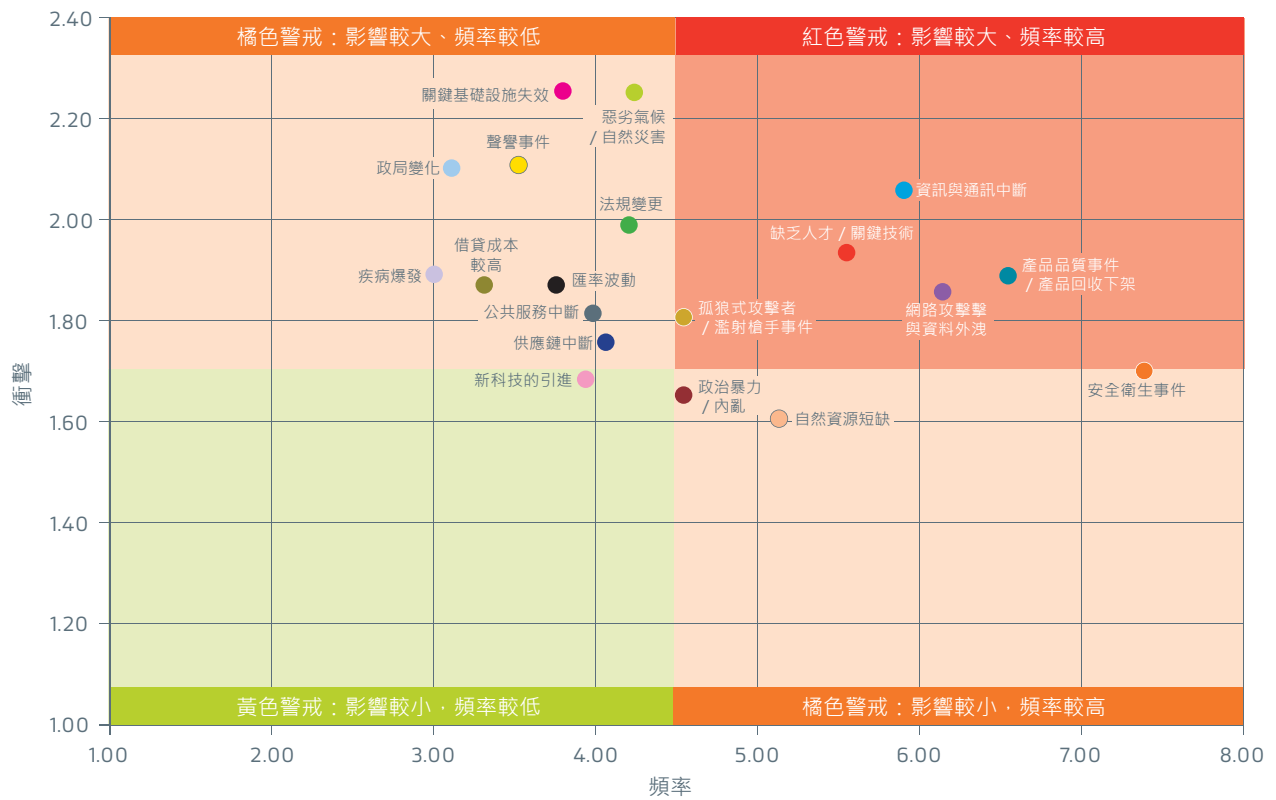
## 澳洲：過去12個月



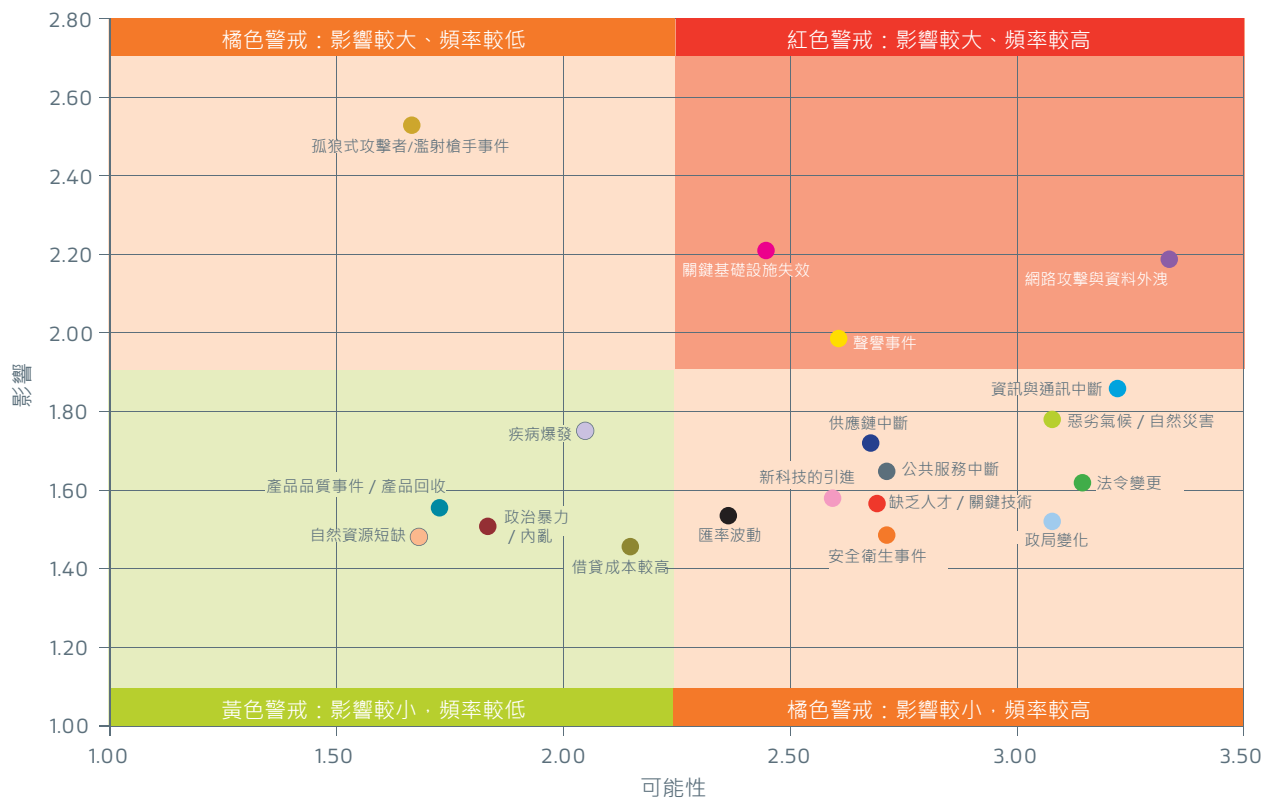
## 澳洲：未來12個月



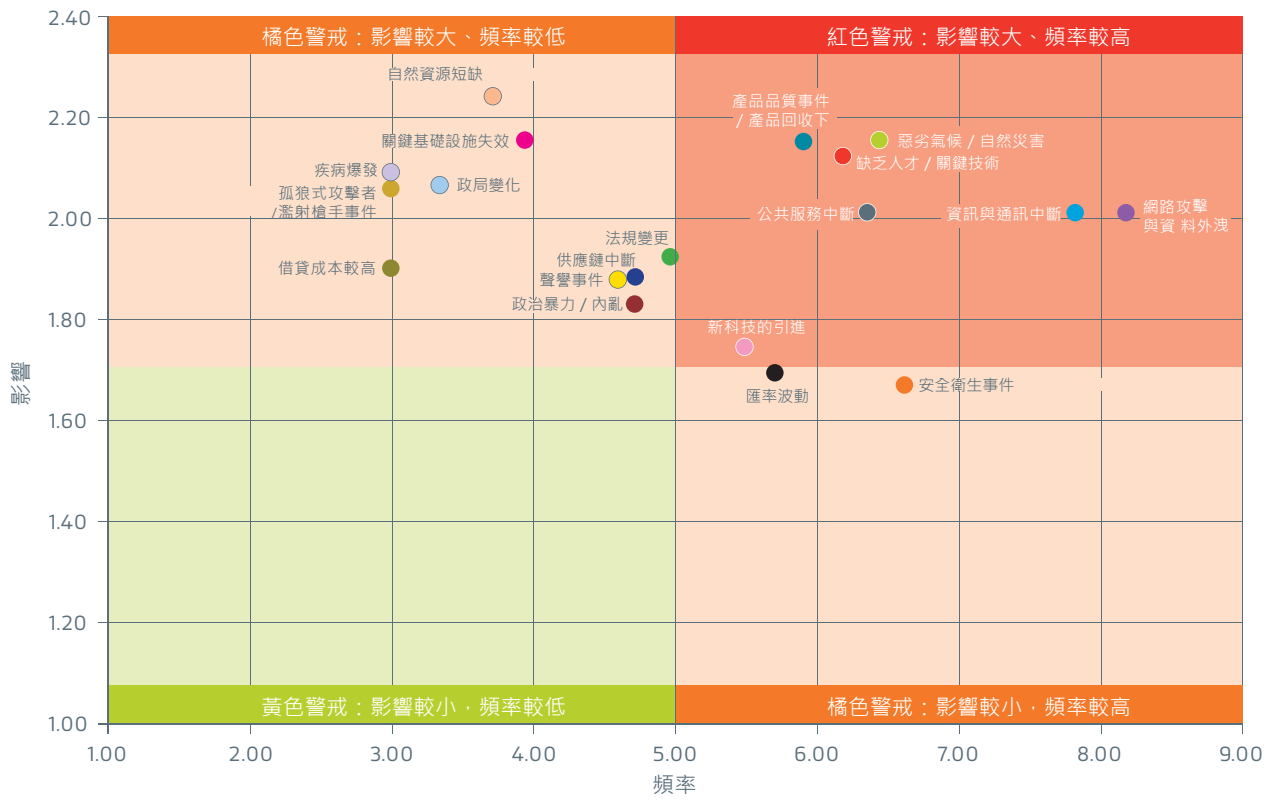
## 英國：過去12個月



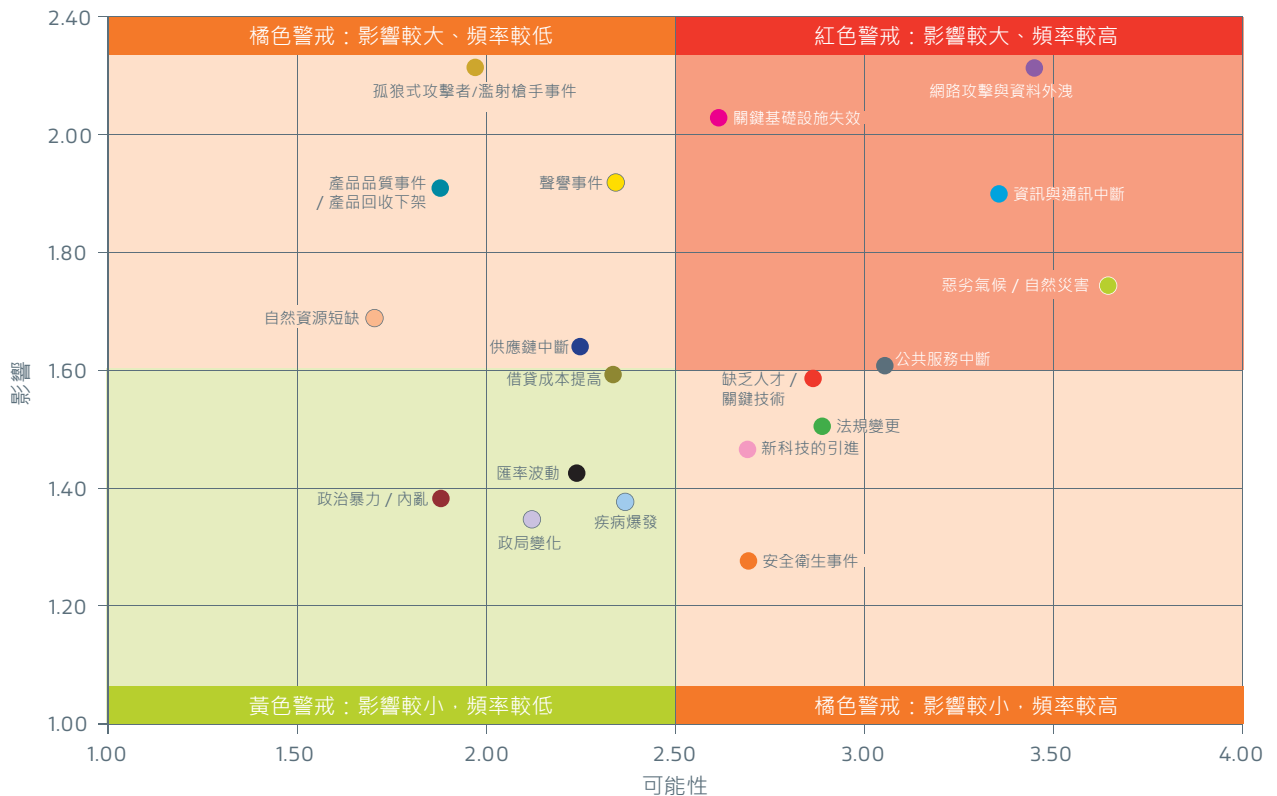
## 英國：未來12個月



## 美國：過去12個月



## 美國：未來12個月



## 作者介紹

### Rachael Elliott ( 思維領袖主任 )

Rachael 在如 HSBC、BdO IIP、marakon Associates、世邦魏理仕 ( CBRE ) 和營運持續管理系統 ( BCMS ) 等組織內具有二十年的頂尖商業研究經驗。她具備科技與通訊、零售、製造業和地產等領域的特殊專長。她的研究用於議會以協助發展政府的產業策略和 BDO 的高街零售銷售追蹤 ( High Street Sales Tracker )。Rachael 亦協助研發，而她的研究至今仍是英國用來追蹤零售業銷售績效的主要評量。她對競爭情報與調查研究技術有高度的興趣。

聯絡方式 [rachael.elliott@thebci.org](mailto:rachael.elliott@thebci.org)



### Gianluca Riglietti CBCI ( BCI 研究與洞察經理 )

Gianluca 畢業於倫敦國王學院，取得地緣政治、領土與安全的碩士學位，曾為擔任歐盟理事會主席的義大利總理工作。他具備撰寫學術與產業刊物的經驗，並且在國際論壇發表，亦替 BSI、Everbridge 與 Transputec 等企業進行專案工作。

聯絡方式 [gianluca.riglietti@thebci.org](mailto:gianluca.riglietti@thebci.org)



### Lucila Aguada ( BCI 研究與洞察分析員 )

Lucia 擁有計量心理學專家執照，專精於量化與質化研究，為菲律賓大學心理學準碩士。她協助非營利機構、製藥與健康照護客戶進行研究，同時也是一名合格教師，擁有 7 年以上的經驗，專精於兒童與特殊教育。

聯絡方式 [lucila.aguada@thebci.org](mailto:lucila.aguada@thebci.org)



### Kamal Muhammad ( BCI 研究與洞察分析員 )

Kamal muhammad 為英國營運持續協會的研究分析員，他具有五年以上的經濟學研究員經驗，致力於經濟成長與發展。他先前以研究員 / 經濟學家的身分在聯合國工作，隸屬於宏觀經濟政策部門，而且負責進行政策分析並為成員國提供技術協助。他持有赫爾大學 ( University of Hull ) 經濟學博士學位以及曼徹斯特大學 ( University of Manchester ) 經濟學與政策發展碩士學位。

聯絡方式 [rachael.elliott@thebci.org](mailto:rachael.elliott@thebci.org)



## 致謝

BCI 感謝 BSI 連續 8 年支持此項研究。

## 關於 英國營運持續協會 (BCI)

英國營運持續協會 (BCI) 成立於 1994 年，旨在打造適應力佳、復原力強的世界；創立至今，已成為協助各企業維持營運持續與打造組織韌性的國際性領導協會。BCI 也是營運持續與組織韌性運作專家心目中的首選會員認證組織，在全球超過 100 個國家 / 地區擁有 8,000 名以上的會員，估計來自 3,000 個私人、公家與第三方部門組織。

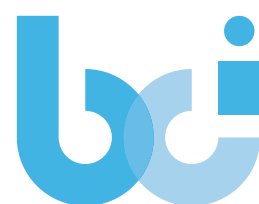
BCI 擁有廣大的會員與合作夥伴關係網路，提供各種不同的體驗服務，包括世界級的教育課程、持續性的專業進修以及交流活動。每年有超過 1,500 人選擇參加 BCI 訓練課程，課程內容從認知提升工具的應用，到完整學位資格的取得，皆提供線上與課堂進修管道。

BCI 擁有卓越的韌性建置專業能力與全球知名的認證標準，能夠提供技術與專業能力保證。BCI 為尋求提升組織韌性的專業人士提供各種不同資源；此外也透過見多識廣的領導團隊與研究計劃協助促進產業提升。BCI 在全球擁有約 120 名合作夥伴，各企業可與本協會攜手合作，一同努力推廣營運持續與組織韌性的最佳實務。

BCI 歡迎任何對組織韌性工作有興趣的人士，無論您是新手、經驗老道的專家或各行各業的企業組織，我們都竭誠歡迎您加入我們的行列。更多關於 BCI 的資訊請上 [www.thebci.org](http://www.thebci.org) 網站查詢。

### 聯絡 BCI

10-11 Southview Park,  
Marsack Street, Caversham,  
RG45AF, United Kingdom  
+44 118 947 8215 | [bci@thebci.org](mailto:bci@thebci.org)



## 關於 英國標準協會 (BSI)

英國標準協會 (BSI) 為全球性機構，專門提供企業必要的解決方案，將最佳標準實務轉換成卓越的日常表現。

BSI 成立於 1901 年，為全球第一個國家標準機構，也是國際標準組織 (ISO) 的創始會員。BSI 影響力跨足航太、汽車、營造、食品、金融、健康照護、IT、及零售等產業等。

BSI 與全球 193 個國家超過 86,000 位客戶合作，BSI 制定的各種標準帶動了全球卓越發展。

一世紀以來，BSI 所創始之標準被全球廣泛採用，BSI 持續透過制定標準與知識解決方案、驗證與專業服務等專業來改善組織績效，協助客戶持續成長、妥善管理並降低風險、並且更具韌性。

請造訪 [bsigroup.com/zh-tw/](https://bsigroup.com/zh-tw/) 瞭解更多資訊

## 關於 BSI 訓練學苑

BSI 訓練學苑講師團隊每位均累積了豐富的稽核及講師經驗，並取得國際認可。BSI 身為百年國家標準制定機構，經驗及知識的累積，是無與倫比的。

在營運持續方面，目前已規劃了 BS 10012 個人資訊管理系統、ISO/IEC 27001 資訊安全管理系統、ISO/IEC 20000 服務管理系統、ISO 22301 營運持續管理系統及營運衝擊分析等相關課程。

企業組織可依據員工執掌內容，安排課程做完整的訓練規劃，以培養並提升員工在風險管控與建構組織韌性的能力。

進一步開課日期，可連絡 BSI 訓練學苑 [training.taiwan@bsigroup.com](mailto:training.taiwan@bsigroup.com) 或來電洽詢。

### 聯絡 BSI

簡慧伶 (Julia Chien)

行銷部協理 BSI台灣分公司  
台北市內湖區基湖路39號5樓

+886 (0)2 2656 0333 | [julia.chien@bsigroup.com](mailto:julia.chien@bsigroup.com)





Business Continuity  
Institute

## BCI 營運持續協會

10-11 Southview Park, Marsack Street,  
Caversham, Berkshire, UK, RG4 5AF

[bci@thebci.org](mailto:bci@thebci.org)  
[www.thebci.org](http://www.thebci.org)



**bsi.**