永續會計準則理事會（SASB）準則

正　體　中　文　版　草　案

軟體與資訊科技服務
永續會計準則

徵　求　意　見　函

（有意見者請於 114 年 10 月 3 日前，將意見以電子郵件方式寄至 tifrs@ardf.org.tw）

財團法人 中華民國會計研究發展基金會

永續準則委員會

關於永續會計準則理事會（SASB）準則

國際財務報導準則基金會之國際永續準則理事會（ISSB）於 2022 年 8 月承接對永續會計準則理事會（SASB）準則之責任。國際永續準則理事會（ISSB）承諾維護、強化及發展永續會計準則理事會（SASB）準則，並鼓勵編製者及投資者繼續使用永續會計準則理事會（SASB）準則。

國際財務報導準則第 S1 號「永續相關財務資訊揭露之一般規定」（以下簡稱國際財務報導準則第 S1 號）規定個體於辨認可合理預期將影響個體展望之永續相關風險與機會時，參考永續會計準則理事會（SASB）準則中之揭露主題並考量其適用性。同樣地，國際財務報導準則第 S1 號規定個體於決定揭露哪些與永續相關風險與機會有關之資訊時，參考永續會計準則理事會（SASB）準則中之指標並考量其適用性。

國際永續準則理事會（ISSB）於 2023 年 6 月修正永續會計準則理事會（SASB）準則中之氣候相關主題及指標，使其與隨附於國際財務報導準則第 S2 號「氣候相關揭露」之行業基礎指引一致。國際永續準則理事會（ISSB）於 2023 年 12 月修正與「永續會計準則理事會（SASB）準則之國際適用性」計畫有關之非氣候相關之主題及指標。

生效日

此 2023-12 版本之準則對所有個體於 2025 年 1 月 1 日以後開始之年度期間生效，並得提前適用。

目錄

簡介

永續會計準則理事會（SASB）準則之概述

永續會計準則理事會（SASB）準則係一組 77 項行業特定之永續會計準則（「永續會計準則理事會（SASB）準則」或「行業準則」），根據永續行業分類系統®（SICS®）分類。

永續會計準則理事會（SASB）準則包括：

1.**行業描述**：意圖透過描述參與該行業所特有之經營模式、相關活動及其他共同特性，以協助個體辨認適用之行業指引。

2.**揭露主題**：描述與特定行業中之個體所進行之活動相關之特定永續相關風險或機會。

3.**指標**：搭配揭露主題，旨在單獨（或作為一組指標之一部分）提供與特定揭露主題之個體績效有關之有用資訊。

4.**技術協定**：提供對相關指標之定義、範圍、施行及表達之指引。

5.**活動指標**：量化個體特定活動或營運之規模，且旨在與第 3 點提及之指標結合使用以將資料標準化並便於比較。

使用永續會計準則理事會（SASB）準則作為其國際永續準則理事會（ISSB）準則之施行之一部分之個體應考量攸關之國際永續準則理事會（ISSB）應用指引。

對未適用國際永續準則理事會（ISSB）準則而單獨使用永續會計準則理事會（SASB）準則之個體而言，「永續會計準則理事會（SASB）準則之應用指引」對所有行業準則之使用建立適用之指引，且被視為準則之一部分。除行業準則所包含之技術協定另有規定外，永續會計準則理事會（SASB）準則之應用指引中之指引適用於行業準則中之指標之定義、範圍、施行、編製及表達。

歷來，「永續會計準則理事會（SASB）之觀念架構」訂定指引永續會計準則理事會（SASB）制定永續會計準則之作法之基本觀念、原則、定義及目的。

準則之使用

永續會計準則理事會（SASB）準則意圖協助個體揭露可合理預期將於短期、中期或長期影響個體之現金流量、其對籌資之可得性或資金成本之永續相關風險與機會之資訊。個體決定哪一（哪些）行業準則及揭露主題與其業務攸關，以及報導哪些相關指標。一般而言，個體應使用特定於其主要行業（如永續行業分類系統®所辨認）之永續會計準則理事會（SASB）準則。惟重大業務分屬數個永續行業分類系統®行業之公司應參考額外永續會計準則理事會（SASB）準則中之揭露主題及相關指標並考量其適用性。

本準則中所包含之揭露主題及相關指標，已被辨認為對投資者可能有用者。惟作出重大性判斷及決定之責任在於報導個體。

行業描述

軟體與資訊科技（IT）服務行業全球性地提供產品及服務予零售、企業及政府客戶，包括開發及銷售應用軟體、基礎架構軟體及中介軟體之個體。該行業通常競爭激烈，惟在某些產品領域仍有一些具主導優勢之業者。雖然相對不成熟，但該行業之特性為高度成長之個體，特別重視創新且仰賴人力及智慧資本。該行業亦包括提供專門資訊科技職能（諸如諮詢及外包服務）之資訊科技服務個體。新行業經營模式包括雲端計算、軟體即服務、虛擬化、機器對機器通訊、大數據分析及機器學習。此外，品牌價值對該行業之個體擴大規模及達成網絡效應係屬重要，由此廣泛採用某特定軟體產品可能促使銷售之自我持續成長。

永續揭露主題及指標

表 1　永續揭露主題及指標

主題	指標	種類	衡量單位	代碼
硬體基礎設施之環境足跡	(1)總能源消耗量、(2)電網電力百分比及(3)再生百分比	量化	十億焦耳(GJ)，百分比(%)	TC-SI-130a.1
	(1)總取水量，於基線水壓力高或極高區域之百分比；(2)總耗水量，於基線水壓力高或極高區域之百分比	量化	千立方公尺 (1,000 m^3)，百分比(%)	TC-SI-130a.2
	將環境考量整合至資料中心需求之策略規劃之討論	討論及分析	不適用	TC-SI-130a.3
資料隱私與言論自由	與精準廣告及使用者隱私有關之政策及實務之描述	討論及分析	不適用	TC-SI-220a.1
	其資訊被用於次要目的之使用者人數	量化	數量	TC-SI-220a.2
	與使用者隱私相關之法律程序所造成之貨幣性損失總額[1]	量化	表達貨幣	TC-SI-220a.3
	(1)執法要求使用者資訊之次數、(2)其資訊被要求之使用者人數、(3)導致揭露之百分比	量化	數量，百分比(%)	TC-SI-220a.4
	核心產品或服務受到政府要求之監督、封鎖、內容過濾或審查之國家清單[2]	討論及分析	不適用	TC-SI-220a.5
資料安全	(1)資料被侵害數量、(2)係屬個人資料被侵害之百分比、(3)受影響之使用者人數[3]	量化	數量，百分比(%)	TC-SI-230a.1
	辨認及因應資料安全風險之作法(包括第三方網路安全標準之使用）之描述	討論及分析	不適用	TC-SI-230a.2

[1] **TC-SI-220a.3** 之註—個體應簡要描述貨幣性損失之性質、背景以及因而採取之任何改正行動。

[2] **TC-SI-220a.5** 之註—揭露應包括每一情況下影響程度之描述，以及對與言論自由有關之個體政策及實務之討論（若攸關時）。

[3] **TC-SI-230a.1** 之註—揭露應包括因應資料被侵害所實施之改正行動之描述。

主題	指標	種類	衡量單位	代碼
招募及管理全球性、多元與具技術之勞工	需要工作簽證之員工百分比[4]	量化	百分比(%)	TC-SI-330a.1
	員工投入百分比[5]	量化	百分比(%)	TC-SI-330a.2
	(a)高階管理階層、(b)非高階管理階層、(c)技術員工及(d)所有其他員工之(1)性別及(2)多元群體之代表性之百分比[6]	量化	百分比(%)	TC-SI-330a.3
智慧財產權保護與競爭行為	與反競爭行為法規相關之法律程序所造成之貨幣性損失總額[7]	量化	表達貨幣	TC-SI-520a.1
管理來自技術中斷之系統性風險	(1)性能問題及(2)服務中斷之次數；客戶總停機天數[8]	量化	數量，天數	TC-SI-550a.1
	與營運中斷有關之營業持續風險之描述	討論及分析	不適用	TC-SI-550a.2

表 2　活動指標

活動指標	種類	衡量單位	代碼
(1)授權或訂閱之數量、(2)雲端基礎之百分比	量化	數量，百分比(%)	TC-SI-000.A
(1)資料處理能力、(2)外包百分比[9]	量化	見註	TC-SI -000.B
(1)資料儲存量、(2)外包百分比[10]	量化	千兆位元組，百分比(%)	TC-SI -000.C

[4] **TC-SI-330a.1** 之註—揭露應包括招募需要工作簽證之員工之任何潛在風險，以及個體如何管理此等風險之描述。

[5] **TC-SI-330a.2** 之註—揭露應包括所使用方法之描述。

[6] **TC-SI-330a.3** 之註—個體應描述其於全球營運中促進公平之員工代表性之政策及計畫。

[7] **TC-SI-520a.1** 之註—個體應簡要描述貨幣性損失之性質、背景以及因而採取之任何改正行動。

[8] **TC-SI-550a.1** 之註—揭露應包括對每一重大之性能問題或服務中斷之描述，以及為防止未來中斷所採取之任何改正行動。

[9] **TC-SI-000.B** 之註—資料處理能力應以個體通常追蹤或用以簽訂軟體與資訊科技服務合約之衡量單位報導，諸如百萬服務單位(MSUs)、每秒百萬指令(MIPS)、每秒百萬次浮點運算(MFLOPS)、運算週期，或其他。另外，個體亦可以其他衡量單位揭露自有及外包之資料處理需求，諸如機櫃空間或資料中心平方英呎。外包百分比應包括駐地雲端服務、託管於公有雲端者，以及儲存於託管資料中心者。

[10] **TC-SI-000.C** 之註—外包百分比應包括駐地雲端服務、託管於公有雲端者，以及儲存於託管資料中心者。

硬體基礎設施之環境足跡

主題彙總

隨著提供雲端基礎服務之成長，此行業之個體不斷增加擁有、營運或租用更多之資料中心及其他硬體。因此，管理與資訊科技硬體基礎設施相關之能源及用水係與價值創造攸關。資料中心須持續供電，且能源供應之中斷可能對營運具重大影響，此取決於中斷之程度及時間。基於資料中心之冷卻需求，個體面臨能源與耗水間之權衡。利用水而非冰水機冷卻資料中心可改善能源效率，但此方法可能造成對大量當地水資源之依賴。資料中心規格之決策對管理成本、取得能源及水之可靠供應，以及降低聲譽風險係屬重要，特別是隨著全球主管機關對氣候變遷之日益關注及能源效率與再生能源創新產生之機會。

指標

TC-SI-130a.1. (1)總能源消耗量、(2)電網電力百分比及(3)再生百分比

1 個體應揭露(1)總能源消耗量之彙總數（以十億焦耳（GJ）為單位）。

1.1 能源消耗之範圍包括來自所有來源之能源，包括個體自外部來源購入之能源及個體本身製造（自行生產）之能源。例如，直接使用燃料、外購電力，以及加熱、冷卻與蒸汽之能源，均屬能源消耗之範圍。

1.2 能源消耗之範圍僅包括個體於報導期間內直接消耗之能源。

1.3 個體於計算來自燃料及生質燃料之能源消耗量時，應使用高熱值（HHV），亦稱為總熱值（GCV），其係直接衡量或取自政府間氣候變化專門委員會（IPCC）。

2 個體應揭露(2)其所消耗之能源中來自電網電力供應之百分比。

2.1 該百分比應以所購買電網電力之消耗量除以總能源消耗量計算。

3 個體應揭露(3)其所消耗之能源中屬再生能源之百分比。

3.1 再生能源係定義為來自補充率大於或等於消耗率之來源之能源，諸如地熱能、風力、太陽能、水力及生質能。

3.2 該百分比應以再生能源消耗量除以總能源消耗量計算。

3.3 再生能源之範圍包括個體消耗之再生燃料、個體直接製造之再生能源，以及個體透過下列方式購買之再生能源：明確包含再生能源憑證（RECs）或能源來源證明（GOs）之再生能源購電協議（PPA）、Green-e Energy 認證之公用事業或供應商計畫，或明確包含再生能源憑證或能源來源證明之其他綠色電力產品，或與電網電力配對之 Green-e Energy 認證之再生能源憑證。

3.3.1 對於現場產生之任何再生電力，任何再生能源憑證及能源來源證明應以個

體名義被保留（不出售）且註銷或取消，使個體可主張其為再生能源。

3.3.2 對於再生能源購電協議及綠色電力產品，該協議應明確包含並傳達再生能源憑證及能源來源證明以個體名義被保留或取代且註銷或取消，使個體可主張其為再生能源。

3.3.3 電力電網組合中非屬個體控制或影響之再生能源部分，係排除於再生能源之範圍。

3.4 就此揭露之目的，來自生質來源之再生能源範圍限於經第三方標準（例如，森林管理委員會、永續森林倡議、森林驗證認可計畫或美國林場系統）認證之材料、依「Green-e 再生能源認證框架第 1.0 版（2017 年版）」或 Green-e 區域標準作為合格供應來源之材料，或符合適用之司法管轄區之再生能源配額制度之材料。

4 個體對於此揭露下所報導之所有資料應適用一致之轉換係數，諸如將高熱值用於燃料（包括生質燃料）之使用及將千瓦時（kWh）轉換為十億焦耳（用於能源資料，包括來自太陽能或風力之電力）。

5 個體可揭露其資料中心最近 12 個月（TTM）加權平均能源使用效率（PUE）。

5.1 能源使用效率係定義為電腦資料中心設施使用之總電量與傳輸至資訊設備電量之比率。

5.2 若揭露能源使用效率，個體應遵循由美國冷凍空調工程師協會（ASHRAE）與綠色電網聯盟發布之「PUE™：指標之綜合檢查（2014 年版）」中描述之指引及計算方法論。

TC-SI-130a.2. (1)總取水量，於基線水壓力高或極高區域之百分比；(2)總耗水量，於基線水壓力高或極高區域之百分比

1 個體應揭露所有來源之取水量（以千立方公尺為單位）。

1.1 水源包括個體直接收集及儲存之地表水(包括來自濕地、河流、湖泊及海洋之水)、地下水、雨水，以及從城市供水、自來水公司或其他個體取得之水及廢水。

2 個體可按來源揭露供應之部分，例如，若取用之重大部分係來自非淡水來源。

2.1 淡水可依個體營運之當地法令規範定義。若法規定義不存在，淡水應被視為溶解固體含量低於百萬分之一千（即 1,000 ppm）之水。

2.2 自遵循司法管轄區飲用水法規之自來水公司取得之水，可被假設為符合淡水之定義。

3 個體應揭露營運中之耗水量（以千立方公尺為單位）。

3.1 耗水係定義為：

3.1.1 取用、使用及排放過程中蒸發之水

3.1.2 直接或間接包含於個體產品或服務中之水

3.1.3 不會回流至其被抽取之同一集水區之水，諸如回流至其他集水區或大海之水

4 個體應分析其所有營運之水資源風險，並辨認於世界資源研究所（WRI）之輸水道水源風險地圖分類為基線水壓力高(40-80%)或極高(>80%)之區域取水與耗水之活動。

5 個體應揭露於基線水壓力高或極高區域之取水量占總取水量之百分比。

6 個體應揭露於基線水壓力高或極高區域之耗水量占總耗水量之百分比。

TC-SI-130a.3. 將環境考量整合至資料中心需求之策略規劃之討論

1 個體應描述其如何將環境考量（包括能源及用水）整合至資料中心之策略規劃。

2 討論應包括（但不限於）環境因素如何影響個體有關資料中心選址、設計、建造、翻新及營運之決策。

2.1 環境因素及標準可能包括：

2.1.1 位置基礎之環境因素，諸如地區溼度、平均溫度及水資源可得性；

2.1.2 環境法規，諸如能源效率標準及國家或州層級之碳定價及電網電力之碳密集度之立法。

3 揭露之範圍包括對現存自有之資料中心、新資料中心之發展，以及資料中心服務之外包之考量（若攸關時）。

資料隱私與言論自由

主題彙總

軟體與資訊科技服務之個體愈來愈常透過網路與行動裝置提供產品及服務，因此其須謹慎管理兩個獨立且往往互相衝突之優先考量事項。首先，個體使用客戶資料來創新並提供客戶新產品及服務以產生收入。其次，個體存取廣泛客戶資料（諸如個人、人口統計、內容及行為資料），造成隱私相關疑慮。此情勢可能導致許多國家增加監管審查。雲端基礎之軟體與資訊科技服務之提供亦產生政府可能會存取使用者資料，使用該資料以限制公民自由之疑慮。對此領域之有效管理可降低可能導致收入減少、市場份額下降及增加涉及潛在罰款與其他法律成本之監管行動之監管及聲譽風險。

指標

TC-SI-220a.1. 與精準廣告及使用者隱私有關之政策及實務之描述

1 個體應描述其與使用者隱私有關之政策及實務之性質、範圍及施行，包括其精準廣告實務，並特別聚焦於其如何管理使用者資訊之蒐集、使用及保存。

1.1 使用者資訊係定義為涉及使用者之屬性或行為之資料，其可能包括對帳單、交易紀錄、溝通紀錄、溝通內容、人口統計資料、行為資料、位置資料及個人資料。

1.1.1 人口統計資料係定義為辨認及區分特定人口之資訊。人口統計資料之例包括性別、年齡、種族/族裔、語言、身心障礙、遷徙、房屋所有權及就業狀況。

1.1.2 行為資料係定義為追蹤、衡量及記錄個人行為之資訊，諸如上網瀏覽模式、購物習慣、品牌偏好及產品使用模式。

1.1.3 位置資料係定義為描述個人之實體位置或移動模式之資訊，諸如全球定位系統（GPS）座標或能辨認及追蹤個人實體位置之其他相關資料。

1.1.4 個人資料係定義為與已辨認或可辨認在世之人有關之任何資訊。當各種資訊片段一起蒐集後可辨認出特定人士時，該等資訊片段亦構成個人資料。

1.1.5 個體可基於適用之司法管轄區法令規範定義個人資料。於此等情況下，個體應揭露所使用之適用之司法管轄區標準或定義。

1.2 精準廣告係定義為以個別使用者資訊為基礎選擇廣告並向其投放之實務。

2 個體應描述資訊之「生命週期」（即資訊之蒐集、使用、保存、處理、揭露及銷毀）以及每一階段之資訊處理實務可能如何影響個人隱私。

2.1 關於資料蒐集，個體可討論其所蒐集無須經個人同意之資料或資料類型、須個人

選擇同意之資料及須個人選擇退出之資料。

2.2 關於資料使用，個體可討論其供內部使用之資料或資料類型，以及於何種情況下個體共享、銷售、出租或以其他方式傳遞資料或資訊予第三方。

2.3 關於資料保存，個體可討論其保存哪些資料或資料類型、保存之持續時間及用以確保資料安全儲存之實務。

3 個體應討論其對隱私影響評估（PIAs）、資料保護影響評估（DPIAs）或類似評估之使用。

3.1 隱私影響評估或資料保護影響評估係分析如何處理資訊以確保該處理符合適用之司法管轄區之法令規範及政策對隱私相關之規定；決定在電子資訊系統中以可辨認之形式蒐集、維護及傳播資訊之風險與影響；以及檢查並評估為降低潛在隱私風險對處理資訊所作之保護措施及替代流程。

4 個體應討論其與使用者資訊之隱私有關之政策及實務如何處理兒童隱私，包括適用之司法管轄區之兒童隱私法令規範之規定。

5 揭露範圍包括第一方與第三方兩者之廣告。

TC-SI-220a.2. 其資訊被用於次要目的之使用者人數

1 個體應揭露使用者資訊被用於次要目的之獨立使用者總人數。

1.1 使用者資訊係定義為涉及使用者之屬性或行為之資料，其可能包括對帳單、交易紀錄、溝通紀錄、溝通內容、人口統計資料、行為資料、位置資料及個人資料。

1.1.1 人口統計資料係定義為辨認及區分特定人口之資訊。人口統計資料之例包括性別、年齡、種族/族裔、語言、身心障礙、遷徙、房屋所有權及就業狀況。

1.1.2 行為資料係定義為追蹤、衡量及記錄個人行為之資訊，諸如上網瀏覽模式、購物習慣、品牌偏好及產品使用模式。

1.1.3 位置資料係定義為描述個人之實體位置或移動模式之資訊，諸如全球定位系統（GPS）座標或辨認及追蹤個人實體位置之其他相關資料。

1.1.4 個人資料係定義為與已辨認或可辨認在世之人有關之資訊。當各種資訊片段一起蒐集後可辨認出特定人士時，該等資訊片段亦構成個人資料。

1.1.5 個體可基於適用之司法管轄區法令規範定義個人資料。於此等情況下，個體應揭露所使用之適用之司法管轄區標準或定義。

1.2 次要目的係定義為個體有意地將所蒐集之資料用於主要目的以外。次要目的之例

可能包括銷售精準廣告，以及透過出售、出租或共享而將資料或資訊移轉予第三方。

1.3 對於個體無法驗證屬於同一個人之使用者帳戶，應分別揭露。

2 揭露範圍應包括其資訊被個體本身用於次要目的之使用者，以及其資訊就次要目的被提供予第三方（包括個體直接或間接控制者，控制個體者，或與個體處於共同控制下者）使用之使用者。

TC-SI-220a.3. 與使用者隱私相關之法律程序所造成之貨幣性損失總額

1 個體應揭露報導期間內所發生與使用者隱私相關之法律程序所導致之貨幣性損失總額。

2 法律程序應包括個體涉及之任何裁決程序，無論是經由法院、主管機關、仲裁人或其他程序。

3 損失應包括對相對人或其他人之所有貨幣性負債（無論係因和解、審理後之判決或其他方式之結果），包括報導期間內因任何個體（例如，政府、企業或個人）提起之民事訴訟（例如，民事判決或和解）、監理程序（例如，處罰、追繳或返還）及刑事訴訟（例如，刑事判決、處罰或返還）所發生之罰款及其他貨幣性負債。

4 貨幣性損失之範圍應排除個體於其辯護過程中所發生之法律與其他費用及支出。

5 揭露範圍應包括與適用之司法管轄區法令規範之執行相關之法律程序。

TC-SI-220a.3 之註

1 個體應簡要描述法律程序所導致之所有貨幣性損失之性質（例如，審理後發布之判決或命令、和解、認罪答辯、緩起訴協議或不起訴協議）及背景（例如，未經授權之監控，資料之共享或兒童隱私）。

2 個體應描述其為回應法律程序所實施之任何改正行動。此可能包括營運、管理、流程、產品、商業夥伴、訓練或技術上之具體改變。

TC-SI-220a.4. (1)執法要求使用者資訊之次數、(2)其資訊被要求之使用者人數、(3)導致揭露之百分比

1 個體應揭露(1)政府或執法機關對使用者資訊（包括使用者之內容及非內容資料）之獨立要求之總次數。

1.1 內容資料包括使用者產生之資訊，諸如電子郵件、簡訊及電話交談錄音。

1.2 非內容資料包括諸如電子郵件地址、姓名、居住國家、性別，以及系統產生之資料（諸如 IP 位址及流量資料）等資訊。

1.3 內容及非內容資料兩者均可能包含個人資料。

1.3.1 個人資料係定義為與已辨認或可辨認在世之人有關之任何資訊。當各種資訊片段一起蒐集後可辨認出特定人士時，該等資訊片段亦構成個人資料。

1.3.2 個體可基於適用之司法管轄區法令規範定義個人資料。於此等情況下，個體應揭露所使用之適用之司法管轄區標準或定義。

2 個體應揭露(2)其資訊被政府機關或執法機關要求之獨立使用者之總人數。

2.1 被要求紀錄之人數應以報導期間內所收到政府或執法機關之所有資訊要求中被要求資訊之獨立使用者之總和計算。

2.1.1 若個體無法驗證兩筆紀錄（使用者資訊）屬於同一使用者，個體應將此視為兩位使用者。

3 個體應揭露(3)政府機關及執法要求中導致向要求方揭露之百分比。

3.1 該百分比應以導致向要求方揭露之獨立要求次數除以所收到之獨立要求總次數計算。

3.2 導致揭露之要求之範圍，應包括於報導期間內導致完全或部分遵循揭露要求者。

3.3 導致揭露之要求之範圍，應包括彙總、去識別化及匿名之資料（其係意圖防止接收者重組資料以識別個人之行動或身分）之揭露。

3.3.1 個體可討論此等特性是否適用於其資料釋出之某一部分，若該討論可對解釋個體之揭露提供必要之背景。

4 個體可額外按地區或國家細分其揭露。

5 個體可描述其決定是否遵循使用者資料要求之政策，包括在哪些條件下將釋出使用者資料、此等要求必須符合哪些規定，以及所需管理階層核准之層級。

6 個體可描述其通知使用者有關此等要求之政策，包括通知之時間。

TC-SI-220a.5.核心產品或服務受到政府要求之監督、封鎖、內容過濾或審查之國家清單

1 個體應揭露其產品及服務因政府、司法或執法要求或規定而受到監督或封鎖，或內容過濾或審查之國家清單。

1.1 監督係於政府機關或執法機關例行性取用特定產品或服務之某些或所有使用者之內容或非內容資料時發生。

1.2 封鎖係於法律或政府機關禁止個體在某一國家或地區提供個體之部分或全部產品或服務時發生。

1.3 內容過濾或審查係於政府機關透過直接凌駕於服務條款或間接要求一個體刪除特定內容而改變對產品或服務內容之取用或呈現時發生。其例之一係被認為具有政治或文化敏感性之內容。

2 揭露範圍包括因與監督、封鎖、內容過濾或審查有關之政府活動而在某一地區停止或從未提供之個體營運。

TC-SI-220a.5 之註

1 個體應描述對其產品或服務線之監督、封鎖、內容過濾或審查之程度，包括受影響之特定產品、過濾或審查之性質及持續時間，以及受影響之客戶百分比。

2 個體可討論封鎖或審查之影響，諸如對擴大市場份額之能力之不利影響，或為遵循該等限制所增加之成本。

3 對於重大修改功能之產品及服務，個體應辨認受影響之產品或服務，並討論修改之性質，指明進行修改究係為了避免被監督或封鎖，抑或使其能被監督或封鎖。個體應描述修改後之產品或服務與其於註冊地國或其他重大市場提供之產品或服務有何不同。

4 若攸關時，個體應討論其與言論自由有關之政策及實務，包括該等政策及實務將如何影響其對在可能要求或規定對個體之內容進行某種形式之監督、封鎖、內容過濾或審查之國家營運之決策。

資料安全

主題彙總

軟體與資訊科技服務行業之個體成為來自網路攻擊日益增加之資料安全威脅之目標，此將其自身資料及其客戶資料置於風險中。對資料安全威脅之預防、偵測及補救之不足，可能影響對客戶之取得及留存，並導致市場份額下降，以及對個體產品之需求降低。除聲譽受損及客戶流失增加外，資料被侵害亦可能導致費用增加，通常與補救努力有關，諸如身分保護之提供及資料保護之員工訓練。同時，新增及新興之資料安全標準及法規可能會透過增加遵循成本而影響營業費用。此外，透過提供安全軟體及服務以符合確保資料安全之需求，此行業之個體可能處於掌握收入機會之有利地位。

指標

TC-SI-230a.1. (1)資料被侵害數量、(2)係屬個人資料被侵害之百分比、(3)受影響之使用者人數

1 個體應揭露(1)報導期間內所辨認之資料被侵害總數量。

1.1 資料被侵害係定義為在個體之資訊系統上，或透過個體之資訊系統進行之未獲授權之事件，該事件危及個體之資訊系統或其中所包含之任何資訊之機密性、完整性或可得性。

1.1.1 資訊系統係定義為個體所擁有或使用之資訊資源，包括由此等資訊資源所控制之實體或虛擬基礎設施，或其組成部分，該等系統係用於蒐集、處理、維護、使用、共享、傳播或處置個體之資訊，以維持或支持營運。

1.2 揭露範圍排除個體具有合理且可佐證之信念認為該事件(i)不致帶來對個體之經營績效或展望造成損害之風險，且(ii)不致帶來對個人造成經濟或社會之不利影響之風險。

2 個體應揭露(2)資料被侵害係屬個人資料被侵害之百分比。

2.1 個人資料被侵害係定義為已傳輸、儲存或以其他方式處理之個人資料因意外或未經授權之毀損、遺失、修改、揭露或存取所導致之資料被侵害。

2.2 個人資料係定義為與已辨認或可辨認在世之人有關之任何資訊。當各種資訊片段一起蒐集後可辨認出特定人士時，該等資訊片段亦構成個人資料。

2.2.1 個體可基於適用之司法管轄區法令規範定義個人資料。於此等情況下，個體應揭露所使用之適用之司法管轄區標準或定義。

2.3 揭露範圍應包括加密資料被取得且加密金鑰亦被取得之事件，以及是否合理認為

加密資料可被輕易轉換為明文。

2.3.1 加密係定義為將明文轉換為密文之過程。

3 個體應揭露(3)受個人資料被侵害影響之獨立使用者總人數。

3.1 對於個體無法驗證屬於同一使用者之帳戶，應分別揭露。

4 若執法機關判定通知會妨礙刑事調查，個體可延遲揭露，直至執法機關判定此通知不會危及調查。

TC-SI-230a.1 之註

1 個體應描述為因應資料被侵害所採取之任何改正行動，例如於營運、管理、流程、產品、商業夥伴、訓練或技術方面之變動。

2 所有揭露應充分，俾能具體針對個體所面臨之風險，但揭露本身不會損及個體維護資料隱私及安全之能力。

3 個體可揭露其以及時之方式向受影響之使用者揭露資料被侵害之政策。

TC-SI-230a.2. 辨認及因應資料安全風險之作法（包括第三方網路安全標準之使用）之描述

1 個體應描述其辨認可能帶來資料安全風險之資訊系統漏洞之作法。

1.1 漏洞係定義為資訊系統、施行、系統安全程序或內部控制中之弱點，該弱點可能被利用。

1.2 資料安全風險係定義為透過資訊系統發生未經授權之存取、毀損、揭露、資訊修改或阻斷服務而可能影響組織營運（包括使命、功能、形象或聲譽）、資產、個人，或其他組織或政府之任何情況或事件之風險。

2 個體應描述其管理已辨認資料安全風險及漏洞之作法，其可能包括操作程序、管理流程、產品結構、商業夥伴選擇、員工訓練及技術使用。

3 個體應描述其對第三方網路安全風險管理標準之使用。

3.1 第三方網路安全風險管理標準係定義為由第三方所制定之標準、架構或指引，其明確之目的係協助個體辨認網路安全威脅，或預防、補救或回應網路安全事件。

3.2 第三方網路安全風險管理標準之例包括：

3.2.1 美國會計師協會（AICPA）之網路安全之服務組織控制（SOC）；

3.2.2 國際電腦稽核協會（ISACA）之 COBIT 5；

3.2.3 ISO/IEC 27000 系列；及

3.2.4 美國國家標準暨技術研究院（NIST）之「改善關鍵基礎設施網路安全架構（2018 年版）」。

3.3 揭露應包括：

3.3.1 辨認已施行或以其他方式使用之特定網路安全風險管理標準；

3.3.2 其使用網路安全風險管理標準之程度之描述，諸如按適用之營運、業務單位、地理區域、產品或資訊系統；

3.3.3 網路安全風險管理標準在個體辨認其資訊系統漏洞及因應資料安全風險與漏洞之整體作法中之角色；

3.3.4 是否對網路安全風險管理標準之使用進行第三方驗證，包括獨立檢查或查核；及

3.3.5 與增加網路安全風險管理標準之使用有關之活動及倡議，即使此等標準目前尚未被使用。

4 個體可就其資料安全及資訊系統受攻擊之類型、頻率及來源討論所觀察到之趨勢。

5 所有揭露應充分，俾能具體針對個體所面臨之風險，但揭露本身不會損及個體維護資料隱私及安全之能力。

招募及管理全球性、多元與具技術之勞工

主題彙總

員工係軟體與資訊科技服務行業價值創造之重要貢獻者。個體通常發現招募適任員工填補此等職缺係屬困難。具技術員工之短缺可能造成為取得高技術員工之全球激烈競爭，從而導致員工高流動率。某些個體致力於攸關教育及訓練計畫以擴展本地具技術之員工之可得性。個體提供重大之貨幣及非貨幣性福利以改善員工投入，且因而提高留任及生產力。改善員工投入及工作與生活平衡之舉措，可能會影響多元勞工之招募及留任。由於該行業之特性為女性及少數族群之代表性相對較低，招募及發展全球多元人才庫之努力可能因應人才短缺，並能提升個體提供之價值。較多元之勞工對創新係屬重要，且其協助個體了解多元及全球客戶群之需求。

指標

TC-SI-330a.1 需要工作簽證之員工百分比

1 個體應揭露報導期間結束日員工在其受僱用之國家需要工作簽證之百分比。

1.1 工作簽證係定義為適用之司法管轄區法律或主管移民機關核發之任何非移民簽證、許可或其他相關文件，以允許外籍員工在其受僱用之國家暫時工作。工作簽證排除授予外國公民永久工作及居留之授權（例如，永久居留許可或永久居民身分）。

1.2 該百分比應以報導期間結束日需要工作簽證之員工人數除以個體員工總人數計算。

2 員工之範圍包括受個體直接僱用之員工，並排除承包商及外包員工。

3 員工之範圍包括全職及兼職員工兩者。

TC-SC-330a.1 之註

1 個體應描述來自招募需要工作簽證之員工之潛在風險，其可能源自移民、歸化及簽證之法規。

2 個體應描述其如何管理與招募需要工作簽證之員工有關之已辨認風險。

TC-SI-330a.2. 員工投入百分比

1 個體應揭露員工投入之百分比。

1.1 員工投入程度之類型可能包括：

1.1.1 主動投入；

1.1.2 不投入；

1.1.3 被動；及

1.1.4 主動疏離。

1.2 若將員工投入作為一衡量指標（例如，員工同意調查陳述之程度），則個體應為此揭露將該指標轉換為百分比。

2 該百分比應以由個體、與個體簽約執行之外部方，或獨立第三方所執行對員工投入之調查或研究結果為基礎計算。

2.1 該百分比應以自我描述為主動投入之員工人數除以完成調查之員工總人數計算。

TC-SI-330a.2 之註

1 個體應簡要描述：

1.1 調查來源（例如，第三方調查或個體自行調查）；

1.2 用以計算百分比之方法；及

1.3 調查或研究中所包含問題或陳述（例如，與目標設定、達成目標之支持、訓練與發展、工作流程及對組織之承諾有關者）之摘要。

2 當調查方法相較於先前報導年度有變動時，個體應提供該變動發生年度在新舊兩方法下之結果。

3 當結果僅限於部分員工，個體應提供納入研究或調查中之員工百分比及樣本之代表性。

4 個體可揭露其他調查發現之結果，諸如對其工作/其所任職之公司引以為傲、受到其工作/同事啟發，以及與公司策略與目標一致之員工之百分比。

TC-SI-330a.3. (a)高階管理階層、(b)非高階管理階層、(c)技術員工及(d)所有其他員工之(1)性別及(2)多元群體之代表性之百分比

1 個體應揭露其員工中(a)高階管理階層、(b)非高階管理階層、(c)技術員工及(d)所有其他員工之(1)性別代表性之百分比。

1.1 個體應將其員工之性別分類為女性、男性或不揭露。

1.1.1 個體可揭露額外之性別認同或表現之類別。

1.2 個體應使用下列員工類別：(a)高階管理階層、(b)非高階管理階層、(c)技術員工及(d)所有其他員工。

1.3 高階管理階層係定義為制定及審查個體之政策，並在其他經理之支持下規劃、指

導、協調及評估個體整體活動之執行長及高階主管。

1.3.1 個體可參考國際職業標準分類（ISCO）之次主要群組11或適用之司法管轄區職業分類系統對高階管理階層之定義。於此等情況下，個體應揭露用以分類高階管理階層之職業分類標準。

1.4 非高階管理階層係定義為除高階管理階層外，規劃、指導、協調及評估個體或個體內部之組織單位之活動，並制定及審查其政策、規則與規定者。

1.4.1 個體可參考國際職業標準分類（ISCO）之主要群組1（排除次主要群組11）或適用之司法管轄區職業分類系統對非高階管理階層之定義。於此等情況下，個體應揭露用以分類非高階管理階層之職業分類標準。

1.5 技術員工係定義為從事高技術或高資格門檻工作之員工，通常分類為計算、數學、建築及工程職業。

1.5.1 個體可參考國際職業標準分類（ISCO）之次主要群組21及25或適用之司法管轄區職業分類系統對技術員工之定義。於此等情況下，個體應揭露用以分類技術員工之職業分類系統。

1.6 所有其他員工係定義為未分類為高階管理階層、非高階管理階層或技術員工之員工。

1.7 個體應以每一員工類別中每一性別類別之員工人數除以相應員工類別中之員工總人數計算每一員工類別之性別代表性百分比。

2 個體應揭露其員工中(a)高階管理階層、(b)非高階管理階層、(c)技術員工及(d)所有其他員工之(2)多元群體代表性之百分比。

2.1 個體應辨認其勞工中之多元群體。

2.1.1 多元係定義為在某一特定領域代表性不足或在某一特定社會歷史上被邊緣化之人群之存在。

2.1.2 多元群體可能依諸如種族、族裔、身心障礙狀態、原籍地、移民身分、原住民背景、年齡、社會經濟背景、宗教信仰、性取向或性別認同等方面定義。

2.1.3 多元群體可透過適用之司法管轄區之法令規範或第三方架構定義。

2.1.4 個體可省略多元群體，若蒐集該群體之資料被適用之司法管轄區之法令規範所禁止，或可能帶來傷害該群體成員之風險。

2.2 個體應以每一員工類別中每一多元群體之員工人數除以相應員工類別中之員工總人數計算每一員工類別之多元群體代表性百分比。

3 個體可提供按司法管轄區細分之性別或多元群體之揭露。

4 個體可提供對重大影響性別或多元群體之代表性之因素之補充性背景揭露，諸如員工所處之司法管轄區。

5 個體可按下表格式依員工類別揭露性別或多元群體之代表性：

表 3 全球員工之性別代表性（%）

	女性	男性	…	N/D*
高階管理階層				
非高階管理階層				
技術員工				
所有其他員工				

*N/D=不揭露

表 4 全球員工之多元群體代表性（%）

	群體 A	群體 B	群體 C	…	N/A*
高階管理階層					
非高階管理階層					
技術員工					
所有其他員工					

*N/A=不可得或不揭露

TC-SI-330a.3 之註

1 個體應描述其於全球營運中促進公平之員工代表性之政策及計畫。

1.1 攸關政策可能包括維持招聘、升遷及工資實務之透明度、確保就業機會平等、制定及傳播多元政策，以及確保對公平代表性之管理階層課責性。

1.2 攸關計畫可能包括多元培訓、指導及贊助計畫、與員工資源及諮詢小組之合作，以及提供彈性之工作時間表以配合員工不同需求。

智慧財產權保護與競爭行為

主題彙總

軟體與資訊科技服務行業之個體花費其收入之重大部分於智慧財產權之保護（包括取得專利權及著作權）。雖然智慧財產權保護係某些個體之經營模式所固有且為創新之一重要動因，但個體之智慧財產權實務有時可能係一項具爭議性之社會議題。個體有時取得專利權及其他智慧財產權保護以限制競爭與創新，特別是當該等個體係具主導優勢之業者時。因軟體之複雜性、其抽象性，以及與軟體有關之智慧財產權權利保護增加，該行業之個體須因應處理專利權重疊之主張以營運。因此，該行業之個體可能發現，因其從事違反倫理之商業實務（或被視為如此作）而被指控侵害專利權，又或因其從事智慧財產權侵權訴訟，致使其經常陷入訴訟或受到監管審查。與反托拉斯及智慧財產權有關之不利法律或監管裁決可能使該行業之個體面臨成本高昂且冗長之訴訟及潛在之貨幣性損失。此等裁決亦可能影響個體之市場份額及訂價能力（若其專利權或在重要市場中之主導地位在法律上受到挑戰），並對收入具潛在重大影響。因此，個體若能在其智慧財產權保護與促進創新之使用間取得平衡並同時確保個體智慧財產權管理與其他商業實務不會不公平地限制競爭，將可減少監管審查及法律行動，同時保護其市場價值。

指標

TC-SI-520a.1.與反競爭行為法規相關之法律程序所造成之貨幣性損失總額

1 個體應揭露報導期間內所發生與反競爭行為相關之法律程序（諸如與價格壟斷、反托拉斯行為（例如，獨家合約）、專利濫用或網絡效應，以及搭售之服務及產品以限制競爭有關者）所導致之貨幣性損失總額。

2 法律程序應包括個體涉及之任何裁決程序，無論是經由法院、主管機關、仲裁人或其他程序。

3 損失應包括對相對人或其他人之所有貨幣性負債（無論係因和解、審理後之判決或其他方式之結果），包括報導期間內因任何個體（例如，政府、企業或個人）提起之民事訴訟（例如，民事判決或和解）、監理程序（例如，處罰、追繳或返還）及刑事訴訟（例如，刑事判決、處罰或返還）所發生之罰款及其他貨幣性負債。

4 貨幣性損失之範圍應排除個體於其辯護過程中所發生之法律與其他費用及支出。

5 揭露範圍應包括與適用之司法管轄區法令規範之執行相關之法律程序。

TC-SI-520a.1 之註

1 個體應簡要描述法律程序所導致之所有貨幣性損失之性質（例如，審理後發布之判決或命令、和解、認罪答辯、緩起訴協議或不起訴協議）及背景（例如，價格壟斷、專利

濫用或反托拉斯）。

2 個體應描述其為回應法律程序所實施之任何改正行動。此可能包括營運、管理、流程、產品、商業夥伴、訓練或技術上之具體改變。

管理來自技術中斷之系統性風險

主題彙總

隨著雲端運算與軟體即服務（SaaS）之趨勢，軟體與資訊科技服務提供者須確保其具有穩固之基礎設施及政策，以最小化其服務之中斷。因運算及資料儲存功能自不同行業之各個體之伺服器移至雲端運算服務提供者之資料中心，諸如程式錯誤或伺服器停機之中斷可能產生系統性風險。特別是若受影響客戶係屬於被視為關鍵國家基礎設施之敏感產業（諸如金融機構或公用事業），該風險將增加。個體對改善其資訊科技基礎設施及服務之可靠性及品質之投資可能吸引並留住客戶，從而於新市場中創造收入及機會。

指標

TC-SI-550a.1. (1)性能問題及(2)服務中斷之次數；(3)客戶總停機天數

1 個體應揭露提供予客戶之軟體及資訊科技（IT）服務中之(1)性能問題之次數。

1.1 性能問題係定義為在提供雲端基礎服務予客戶時，任何已規劃或非預期之停機所造成超過 10 分鐘但少於或等於 30 分鐘之中斷。

1.2 性能問題可能包括由技術故障、程式錯誤、網路攻擊、天氣事件或託管設施面臨之自然災害導致之效能問題。

2 個體應揭露提供予客戶之軟體及資訊科技服務中之(2)服務中斷之次數。

2.1 服務中斷係定義為在提供雲端基礎服務予客戶時，任何已規劃或非預期之停機所造成超過 30 分鐘之服務中斷。

2.2 服務中斷可能包括由技術故障、程式錯誤、網路攻擊、天氣事件或託管設施面臨之自然災害導致之服務中斷。

3 個體應揭露提供予客戶之軟體及資訊科技服務中與性能問題及服務中斷有關之(3)客戶總停機天數。

3.1 總客戶停機天數係定義為每一服務中斷持續時間乘以受影響之軟體及資訊科技服務授權數量（以授權天數報告）。為提供背景，個體應說明授權之基礎（例如，座位數、CPU 核心數、雲端服務訂閱數）以及該等授權究係消費基礎或容量基礎。

TC-SI-550a.1 之註

1 就每一重大之服務中斷，個體應揭露該中斷之持續時間、中斷之程度及根本原因，以及為防止未來中斷所採取之任何改正行動。若重大，個體應揭露相關發生成本，諸如，改正技術或流程問題之補救成本，以及任何責任成本。

2 若某一服務中斷之改正成本係屬重大，或以影響產品上市時間、收入取得或其他重大參數之方式對大量客戶或基本業務營運造成干擾，則該服務中斷視為重大。

TC-SI-550a.2. 與營運中斷有關之營業持續風險之描述

1 個體應描述與影響營運之技術中斷相關之潛在營業持續風險。

1.1 中斷之例可能包括由技術故障、程式錯誤、網路攻擊、天氣事件或託管設施面臨之自然災害導致之中斷。

2 個體應討論為管理營業持續風險所實施之措施，諸如中斷之影響之技術或流程、強化系統韌性、為損失投保，或為關鍵業務營運提供備援。

3 個體應辨認哪些關鍵業務營運支持雲端基礎服務，且個體應進一步說明該等營運究係自有或外包。

4 個體可討論潛在損失之估計金額、該損失之機率及相關時程。此等估計可能係基於保險數據或其他第三方或內部對潛在損失之評估。