Microsoft 365

透過 Microsoft 合規性分數簡化合規性並降低風險

目錄

執行摘要

目標讀者：

尋求指導以管理雲端風險和合規性的公司。

快速導讀：

隨著資料呈指數型成長以及資料保護法規的數量越來越多，公司需要更好的工具和更豐富的知識來評估和管理與 IT 相關的風險。移轉到雲端可以將許多規定轉移成供應商的責任，因而減輕一些負擔。

Microsoft 致力於透過授信任的平台和工具 (如 Microsoft 合規性分數) 來協助簡化合規性。這種風險型分數有助於衡量您的控制措施有多符合特定的合規性標準，並建議改善措施。

合規性挑戰

合規性所涉及的技術、營運和法規方面的複雜度，為企業帶來獨特的挑戰。

因為合規性的種類甚多，對於在多個產業服務且必須考慮部分合規性領域間的重疊性、法規遵循和相容性的公司，這是一項艱鉅的任務。」

資訊安全主管 [1]

IT 合規性是相對少見的技能組合。專注於此領域的人才不可多得。很難找到適合的人選。」

企業資安長 [2]

[1、2]《Microsoft 客戶研究》

要趕上不斷推陳出新的法規一直都是件困難的事

平均而言，1,000 個監管機構每天會進行 220 次和規要求更新。快速的變化是組織面臨的最大合規性挑戰之一，這使得他們必須時時做好應對準備。

時間點評估無法識別兩次稽核間隔期的風險

手動機和很快就會過時，因而在兩次評估間隔期造成風險。企業正在尋找更完善地跨系統整合和即時更新評估的方法，以因應數位化變革的腳步。

風險和合規性管理方面的協作效率低下，且相互孤立

遺憾的是，IT 和合規性團隊並非總是相互理解。IT 部門了解技術，但缺乏解讀法規所需的專業知識。另一方面，合規性和隱私團隊熟悉規則，卻不是能夠協助遵循法規的解決方案專家。

缺乏有關設計和實施有效控制的協助指導

IT 決策者對工具和技術感到不知所措。他們需要簡單的逐步指導，以了解如何在所在產業中正確使用工具並遵循法規要求。

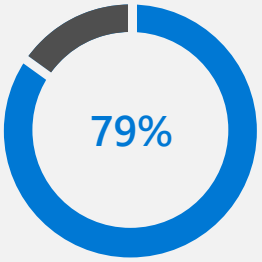
運用這些指南、見解和資源簡化您的合規性之旅。

[3]《合規性的成本》，路透社，2019 年。

Microsoft 與您的共同責任

建立和維護資料保護控制可能既耗時又費力。如果您將所有資料保留在內部，您將獨自負責合規性控制和管理隨之而來的複雜性。您使用雲端服務時，合規性成為共同的責任。擁有值得信任的合作夥伴可大幅減輕您團隊的負擔。

我們以 NIST 800-53 為例：在標準的最新版本中，有 1,021 個控制項目。這些控制項目中有 79% 是 Microsoft 的責任，但只有 21% 是客戶的責任。



其中 79% 的控制項目的 Microsoft 的責任

Microsoft 承擔並管理軟體及服務 (SaaS) 應用程式 (例如 Microsoft 365) 的大部分控制項目。這使您無須在控制項目上投入過多精力，可以將更多時間用於策略計劃。在這種模式下，Microsoft 會與您密切合作，協助您保護資料並簡化合規性。以 NIST 800-53 為例，其中包括 1,021 個控制項目。您使用 Office 365 時，我們將負責其中將近 80%。

我們還為您提供管理合規責任的解決方案。例如，對於 Office 365，我們不僅使用加密箱系統來限制和控制對生產環境及客戶資料的存取，也為您提供像是 Azure Active Directory 條件式存取等解決方案，以幫助您在己端建立有效的存取控制。

我們可以簡化的另一個領域是加密。透過 Microsoft 雲端服務，我們預設會對傳輸中的資料加密，並為您提供 Microsoft 資訊保護和客戶金鑰，以提供額外的加密控制。

只有在您可以信任雲端服務提供者，而且可以輕鬆評估其控制措施時，共同責任才有價值。Microsoft 推出了 Microsoft 合規性分數；這是一種風險型分數，可讓您輕鬆評估 Microsoft 管理的控制項目，因此您可以全面了解 Microsoft 如何保護您的資料。此外，該分數還為您提供實施和改善資料保護控制的建議措施。

閱讀《雲端計算共同責任》白皮書，了解更多有關共同責任模式的資訊。

合規性分數概觀

Microsoft 合規性分數可幫助您了解組織的合規狀況。它可以衡量您在降低資料保護和法規合規性相關風險方面的工作進度。您可以輕鬆查看目前分數、需要改進的領域以及要採取的措施。

即使不是 GDPR 等複雜法規方面的專家，您也仍然可以快速學習建議的措施，以協助您逐步實現合規。透過持續控制評估，您現在可以主動維持合規性，而不是在稽核之後才修正設定。

持續評估風險

88% 的組織正在尋找自動風險偵測工具，因為時間點評估很容易使組織在兩次定期評估 (例如年度稽核) 的間隔期間暴露在未知的風險中。[4]

Microsoft 合規性分數可協助您持續識別風險。它會自動掃描 Microsoft 365 環境，以偵測和監控系統中資料保護控制的有效性，並提醒您潛在的風險。

例如，如果您的組織尚未為 Windows 設定合規性原則，合規性分數就會將此控制突顯為含有高風險的失敗，並建議您在 Intune 中心新增裝置合規性原則。新增原則後，您的分數將在 24 小時後更新。

取得可行的建議

由於有太多的法規和技術需要追蹤，因此要知道下一步該做什麼才能提高合規性並不容易。合規性分數會建議資料保護法規和標準的改善措施，並提供詳細的實施指引，以協助合規性和 IT 團隊保持同步。

「合規性分數」儀表板會顯示您的改善措施；這些措施可以解決最關鍵的問題，大幅提高分數。您可以輕鬆地將這些措施指派給組織中的利害關係人，以實施和測試控制。在每個操作頁面上，您還可以上傳和儲存證明，並記錄實施和測試詳細資料，為稽核做好準備。

[4] 風險管理市場狀況網路調查 (n=500，IRM 解決方案購買者和影響人士，超過 1,000 名員工)，Gartner，2019 年。

簡化合規性

Gartner 預測，到 2022 年，根據《一般資料保護規定》(GDPR)，全球一半人口的個人資料將受到當地隱私法規的保護，而今天此比例只有十分之一。IT 決策者將越來越多的法規描述為在鄉村市集玩「打地鼠」遊戲：他們不斷對變化做出反應，而不是主動應對。

在 Microsoft，我們已經為自己的服務構建了具有 1,900 項控制的通用控制架構。它使我們能夠擴展保證工作，以滿足 90 多項法規和標準的合規性要求。我們使用相同的方法，在 Microsoft 合規性分數中運用了相關知識並建立了通用控制架構，因此您可以運用內建的控制對應來擴展合規工作。透過採取一項行動，您可以協助組織同時滿足多項要求。透過消除重複工作有助於減少在管理合規性方面所花的時間，並簡化稽核。

了解更多有關合規性分數的資訊。

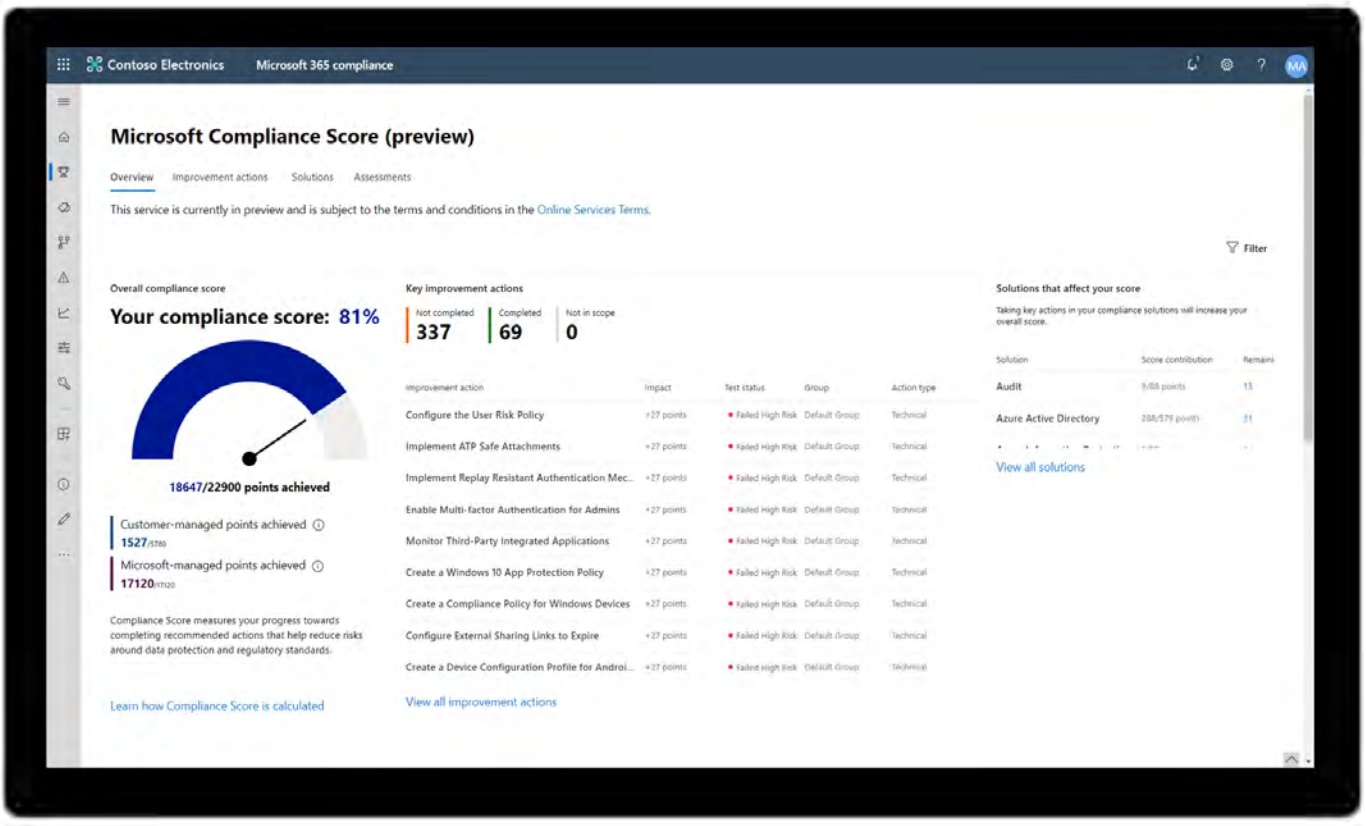
[5]《隱私與個人資料法規現狀》，Nader Henein 和 Bart Willemsen，2019 年 4 月。

了解您的分數

合規性分數會依照資料保護基準 (由關鍵的全球法規和標準等要求所組成) 提供初始評分。之後，您可以新增與您組織相關的特定評估。例如，銀行可以新增 FFIEC 評估。或者，如果您在醫院工作，則可以新增 HIPAA/HITECH 評估。

由於採用本白皮書前述的共同責任模式，大多數得分是來自 Microsoft 管理的控制項目。您可以改進的方面列為客戶管理的得分點。您採取措施並實施控制時，就會看到合規性分數相應地提高。

您可以依照類別查看詳細的得分情況，例如資料保護和存取控制的得分明細。分數類別可協助您專注於最需要關注的領域，並將其指派給適合的管理員來幫助您進行操作。



您也可以依照選定的法規和標準來查看分數明細，這對於合規性和風險評估團隊特別實用。IT 管理員還可以輕鬆地了解哪些操作有助於提高分數，以及它們如何為整體合規性目標做出貢獻。

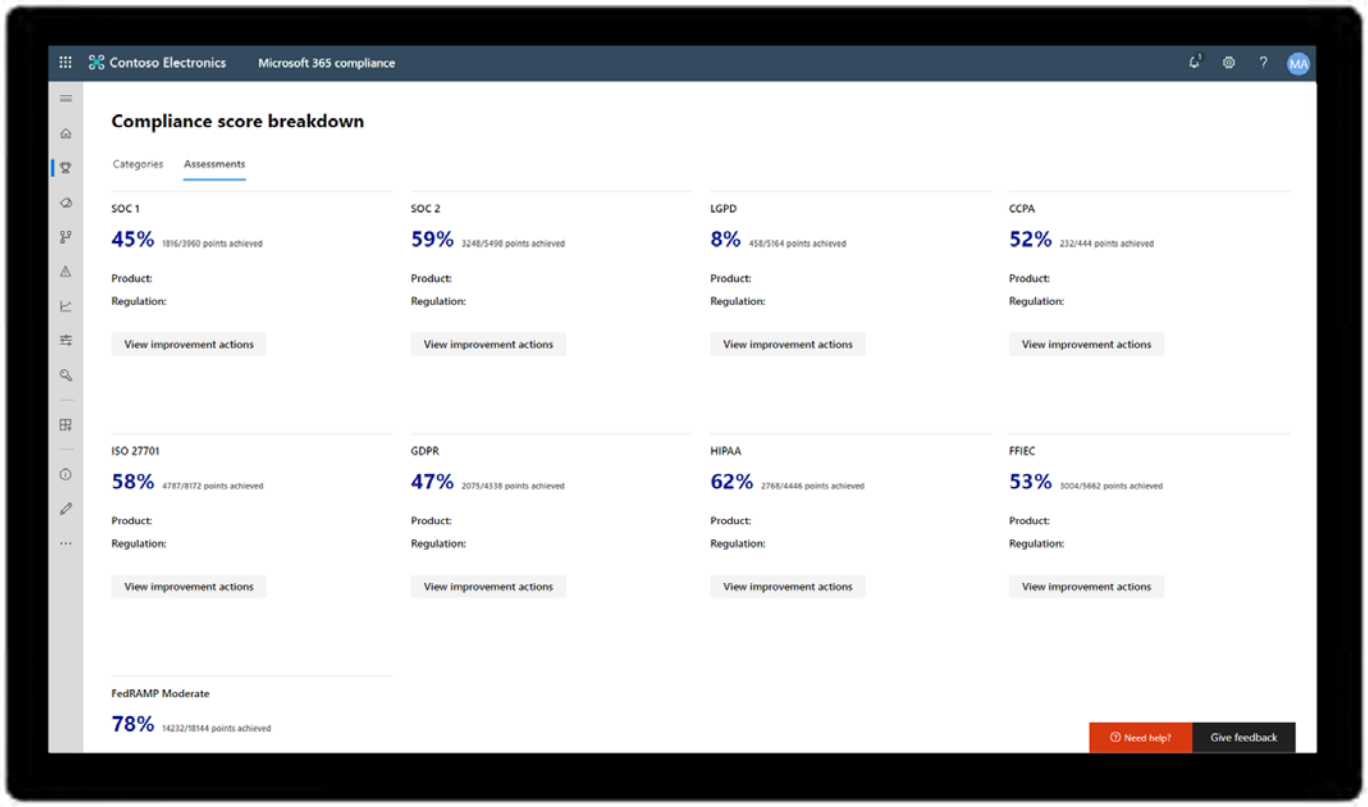


圖 1. 依照類別劃分的分數明細可協助您找出需要立即關注的類別。

開始使用

隨著數位化轉型步伐加快，風險管理已不再是一年一度的活動了。Microsoft 合規性分數使您能夠根據特定的法規環境來持續監控控制的有效性。它使組織中的各個團隊 (包括 IT、安全等) 能夠了解並提升合規性。通用控制架構可提高效率，而內建的工作流程工具可實現有效的協作。它是降低風險和管理合規性複雜度的必備工具。

Microsoft 合規性分數可用於所有 Microsoft 365 和 Office 365 企業授權。您可以註冊取得試用版或導覽志 Microsoft 365 合規中心立即開始使用。您可以閱讀此支援文件，了解更多有關 Microsoft 合規性分數的資訊。

與我們聯絡

注意：合規性分數是風險型分數，可協助您簡化風險評估以及將風險評估自動化，並提供有助於解決風險的建議。它不表示對組織對任何特定標準或法規遵循程度的絕對度量，而是表示您在何種程度上採取了控制措施，以減少個人資料和個人隱私的風險。合規性分數不應以任何方式解釋為保證。

Microsoft 365