AWS 白皮書

AWS 雲端採用架構概觀

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 雲端採用架構概觀: AWS 白皮書

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標或商業外觀不得用於 Amazon 產品或服務之外的任何產品或服務，不得以可能在客戶中造成混淆的任何方式使用，不得以可能貶低或損毀 Amazon 名譽的任何方式使用。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能隸屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

摘要 1
摘要 1
簡介 2
加快實現業務成果 3
基礎能力 4
您的雲端轉型之旅 6
商業面向 8
人員面向 10
治理面向 13
平台面向 16
安全面向 19
營運面向 22
結論 25
附錄：AWS CAF 能力海報 26
作者群 27
深入閱讀 28
文件修訂 29
聲明 30

AWS 雲端採用架構概觀

發佈日期：2021 年 11 月 22 日 (文件修訂)

摘要

隨著激增的數位技術不斷重組客群及打破產業區隔，採用 Amazon Web Services (AWS) 可幫助您的組織轉型，以因應不斷變化的商業環境和不斷發展的客戶需求。AWS 是世界上最全面、最多人採用的雲端平台，可幫助您降低成本、降低業務風險、提高營運效率、變得更靈活、加速創新、創造新的營收來源，以及重塑客戶和員工體驗。

AWS 雲端採用架構 (AWS CAF) 利用 AWS 的經驗和最佳實務，幫助您以新穎的方式使用 AWS，完成數位轉型並加快實現業務成果。使用 AWS CAF 找出轉型機會並列為優先事項，接著評估和改進雲端整備度，然後迭代發展轉型藍圖。

簡介

快速激增的數位技術加速了變革，並在多種客群和產業加劇了競爭。因為要維持任何特定的競爭優勢日益困難，所以企業被迫得在越來越短的時間內脫胎換骨。例如，預計未來十年內，標準普爾 500 指數中有 50% 的公司會被替換。

同樣地，民眾不斷變化的期望和行為也對公部門組織施壓，要求改善提供數位服務。全球各地的組織都在進行數位轉型，利用數位技術推動組織變革，使其能適應不斷變化的市場環境，讓客戶滿意，並加快實現其業務成果。

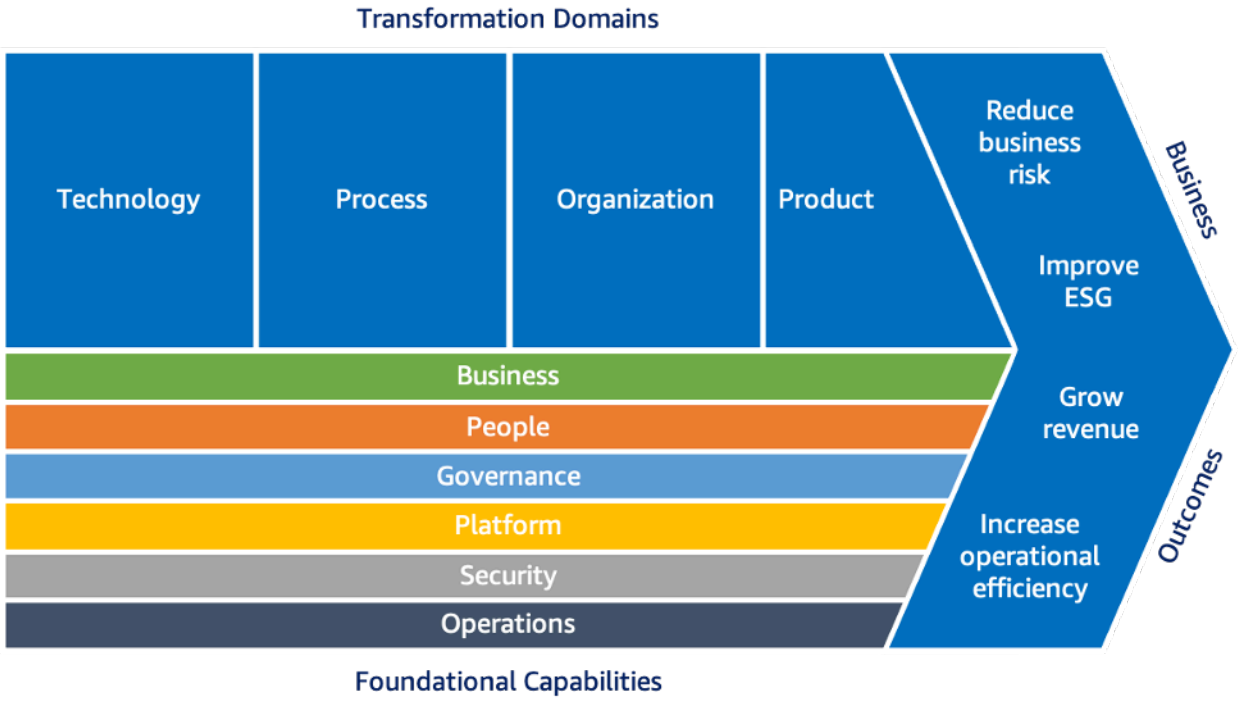
數百萬計的 AWS 客戶 (包括成長最快的新創公司、最大的企業和最先進的政府組織)，都利用 AWS 遷移及現代化舊式的工作負載，變成資料驅動的數位化和最佳化商業流程，並重塑營運和商業模式。這些客戶透過雲端驅動的數位轉型 (雲端轉型) 改善業務成果，包括降低成本、降低業務風險、提高營運效率、變得更靈活、加速創新、創造新的營收來源，以及改善客戶和員工體驗。

一組基礎的組織能力可以支援您有效利用雲端進行數位轉型 (雲端整備度) 的能力。AWS CAF 找出這些能力並提供規範性的指導，全球有數千組織已成功使用這些能力和指導，加快其雲端轉型之旅。

AWS 和 AWS 合作夥伴網路提供的工具和服務會在各個階段助您一臂之力。AWS 專業服務是全球性的專家團隊，透過一系列與 AWS CAF 一致的產品提供協助，幫助您實現與雲端轉型相關的特定成果。

藉助雲端驅動的數位轉型加快實現業務成果

下圖中的雲端轉型價值鏈顯示，透過多項基礎能力實現的雲端驅動組織變革 (轉型)，可加快實現業務成果。轉型領域代表如下的價值鏈：技術轉型實現流程轉型，從而促進可實現產品轉型的組織轉型。主要業務成果包括降低業務風險，改善環境、社會和治理 (ESG) 績效，以及提高收入和營運效率。

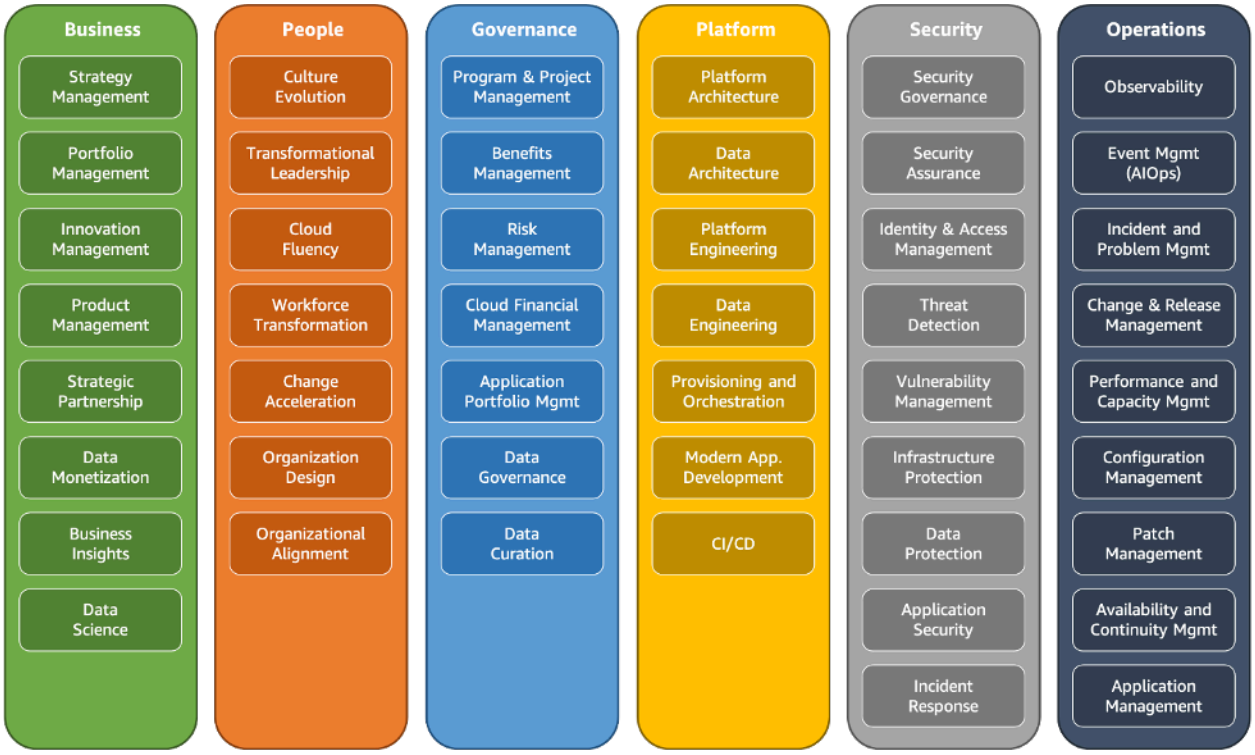


雲端轉型價值鏈

- 技術轉型側重於使用雲端遷移並現代化舊有的基礎設施、應用程式以及資料和分析平台。雲端價值基準研究報告指出，從內部部署遷移到 AWS，每位使用者成本可降低 27%、每位管理員管理的 VM 可增加 58%、停機時間減少 57%，安全事件則減少 34%。
- 流程轉型側重數位化、自動化和最佳化企業營運。這包括利用新的資料和分析平台建立切實可行的洞見，或使用機器學習 (ML) 改善您的客戶服務體驗、員工生產力和決策、業務預測、詐騙偵測和預防、產業營運等。這樣做有助於您提高營運效率，又能降低營運成本，並改善員工和客戶體驗。
- 組織轉型側重於重構營運模式；業務和技術團隊如何彼此協調，以創造客戶價值並達成您的戰略目標。圍繞產品和價值流組織您的團隊，同時利用敏捷的方法快速迭代和演進，有助於提升反應速度，並更以客戶為中心。
- 產品轉型側重透過建立新的價值主張 (產品、服務) 和營收模式，重構您的商業模式。這樣做可以幫助您接觸新客戶，打進新的客群。雲端價值基準研究報告指出，採用 AWS 可縮短 37% 的新功能和應用程式上市時間、程式碼部署頻率提高 342%，部署新程式碼的時間則縮短 38%。

基礎能力

上一節中介紹的每個轉型領域都是由下圖所示的一組基礎能力所實現。能力是利用流程部署資源 (人員、技術和任何其他有形或無形資產)，以實現特定結果的組織能力。AWS CAF 能力提供最佳實務指導，可幫助您提高雲端整備度 (您有效利用雲端從事數位轉型的能力)。AWS CAF 的能力分為六個面向：商業、人員、治理、平台、安全性和營運。每個面向都包含一組能力，與利害關係人在雲端轉型之旅中所擁有或管理的職務相關。



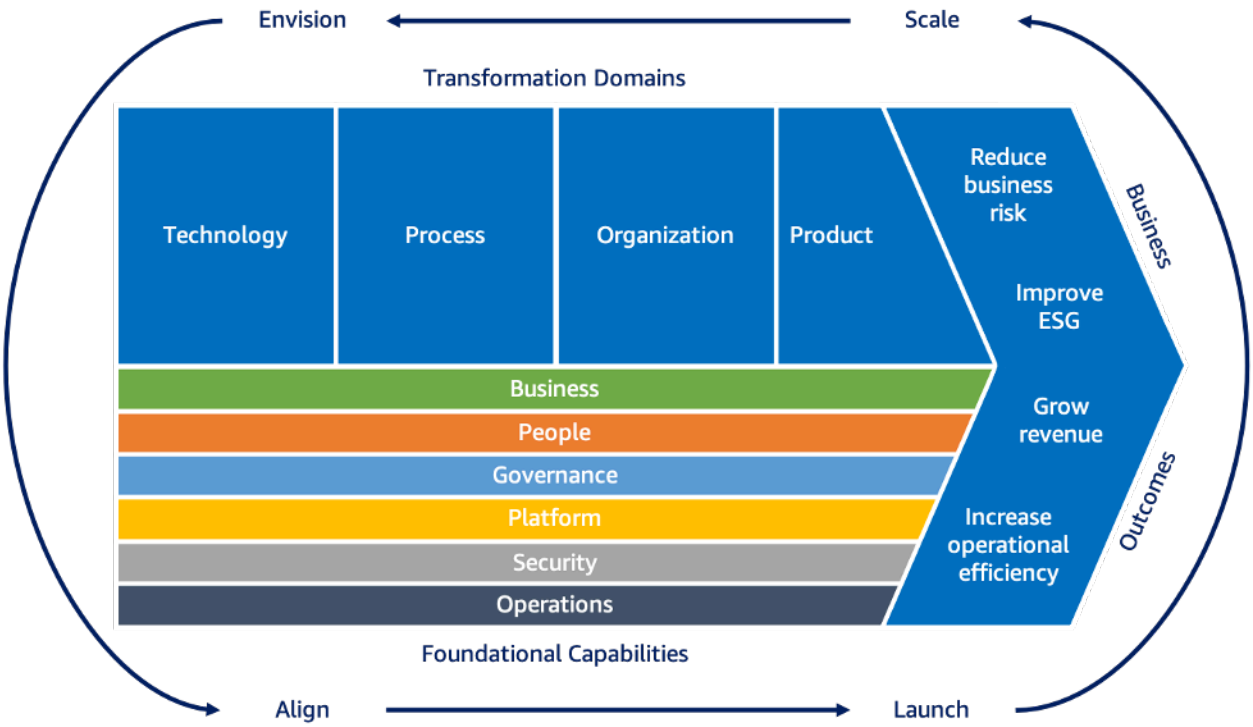
AWS CAF 面向和基礎功能

- 商業面向有助於確保您的雲端投資能加快實現您的數位轉型目標和業務成果。共同利害關係人包括執行長 (CEO)、財務長 (CFO)、營運長 (COO)、資訊長 (CIO) 和技術長 (CTO)。
- 人員面向是技術與業務之間的橋樑，能加快雲端之旅，幫助組織更快發展出持續成長、學習的文化，即使面臨變化也穩步向前，並以文化、組織結構、領導力和勞動力為重心。共同利害關係人包括資訊長、營運長、技術長、雲端經理及跨職能和企業各部門主管。
- 治理面向可幫助您協調雲端計劃，同時將組織效益提到最高、與轉型相關的風險降至最低。共同利害關係人包括轉型長、資訊長、技術長、財務長、資料長 (CDO) 和風險長 (CRO)。
- 平台面向可幫助您建置企業級的可擴展混合式雲端平台，將現有的工作負載現代化，並實作新的雲端原生解決方案。共同利害關係人包括技術長、技術主管、架構師和工程師。

- 安全性面向可幫助您達成資料和雲端工作負載的機密性、完整性和可用性。共同利害關係人包括資訊安全長 (CISO)、法遵長 (CCO)、內部稽核主管及安全架構師和工程師。
- 營運面向有助於確保您的雲端服務在提供時能滿足業務需求。共同利害關係人包括基礎設施和營運部門主管、網站可靠性工程師和資訊科技服務經理。

您的雲端轉型之旅

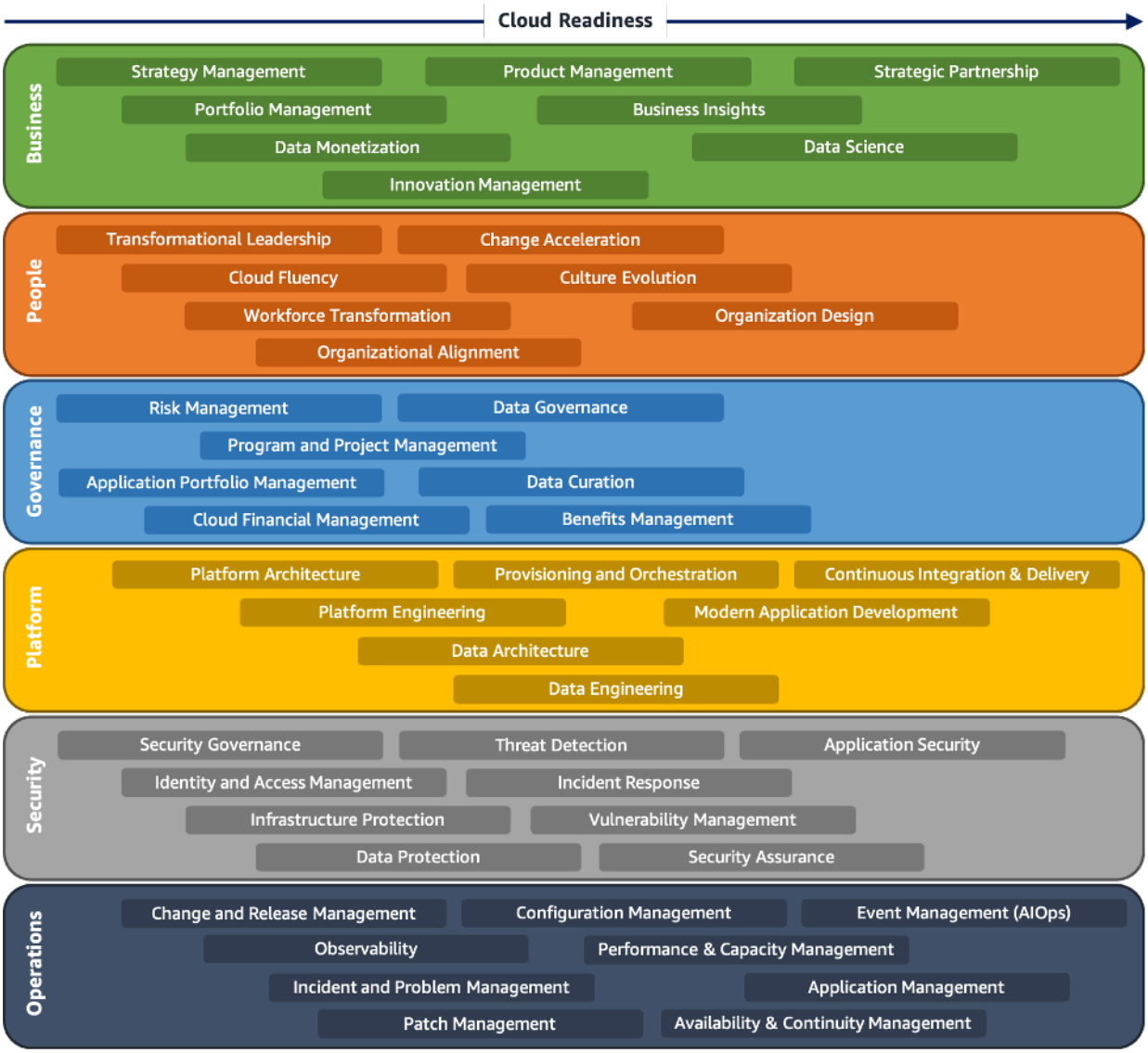
每個組織的雲端之旅都是獨一無二的。要成功轉型，您需要設想預期的目標狀態、了解您的雲端整備度，並採用敏捷的方法彌合差距。逐步轉型可讓您快速展示價值，同時將長遠預測的需求降至最低。採用迭代方法有助於保持勢頭，並隨著經驗愈加豐富而發展藍圖。AWS CAF 建議下圖所示的四個迭代和累進雲端轉型階段。



雲端轉型之旅

- 設想階段著重於展示雲端將如何幫助您加快實現業務成果。其會根據您的戰略商業目標確定四個轉型領域中每個領域的轉型機會，並排定其優先順序，助您實現目標。建立轉型計劃與主要利害關係人 (能夠影響和推動變革的高階主管) 及可衡量業務成果的關聯性，將有助於您在轉型過程中展現價值。
- 協調階段側重於確定六種 AWS CAF 面向中的能力差距，確定跨組織的相依性，並顯露出利害關係人的考量和挑戰。這樣做將可幫助您制定提高雲端整備度的策略，確保與利害關係人保持一致，並促進相關的組織變革管理活動。
- 啟動階段側重在傳遞生產試點計劃及展示累積的商業價值。這些領導人應該具有高度的影響力，並能在成功後，協助影響未來的方向。向這些領導人學習將可幫助您在擴大全面生產之前調整方法。
- 擴展階段側重於將生產試點和商業價值擴展到想要的規模，並確保實現與雲端投資相關的商業收益且加以保持。

您不需要一次駕馭所有基礎能力。隨著雲端轉型之旅的開展，發展基礎能力並提高雲端整備度。考慮根據您的特定需求，依下圖建議順序量身打造。



AWS CAF 面向和基礎能力的演變

以下各節會詳加說明 AWS CAF 的六個面向及基礎能力。

商業面向：策略和成果

商業面向側重於確保雲端投資能加快實現數位轉型目標和業務成果。此面向包含下圖所示的八項能力。共同利害關係人包括執行長、財務長、營運長、資訊長和技術長。

AWS CAF 商業面向能力

- 策略管理 – 利用雲端加快實現業務成果。思考雲端如何支援及塑造長期的業務目標。發現消除技術負債及利用雲端優化技術和商業營運的機會。探索新的雲端價值主張和營收模式。思考新推出或改良的雲端產品和服務可如何幫助您觸及新客戶或打進新客群。根據商業環境的技術發展和變化，確定策略目標的優先順序，並隨著時間的推移發展策略。
- 管理產品組合 – 根據策略目標、營運效率和生產能力決定雲端產品和計劃的優先順序。在正確的時間交付正確的雲端產品和計劃，將有助於您實施策略並加快實現業務成果。利用自動化探索工具以及將應用程式遷移到雲端的七種常用遷移策略 (稱為 7 個 R)，以合理化現有的應用程式組合，並建置資料驅動型商業案例。

  考慮短期和長期成果以及低風險 (經實證) 和高風險 (實驗性) 機會，藉以平衡您的雲端產品組合。納入遷移、現代化和創新計劃，並考慮財務 (降低成本及/或增加營收) 和非財務 (例如改善客戶和員工體驗) 的益處。根據您的資源、財務和排程限制，獲得產品組合最大的商業價值。為了加速實現價值的時間，請考慮提高規劃週期的頻率，或採用連續的規劃策略。
- 創新管理 – 利用雲端開發新的流程、產品和體驗，並改進現有的流程、產品和體驗。雲端讓您能夠即時佈建及關閉資源，藉以幫助您加速實現價值的時間，並降低與創新有關的成本和風險。為充分利用隨著採用雲端而有望提高的業務敏捷性，請研擬創新策略，並納入著重於優化現有產品、流程和體驗的累進式創新計劃，以及著重於實踐新商業模式的破壞式創新計劃。根據您的策略性優先事項建立集思廣益的機制，並開發端對端流程以擴展成功的創新試驗。

- 產品管理 – 管理資料和雲端產品，以在整個產品生命週期中為內部和外部客戶提供可以重複產生的價值。 圍繞資料和雲端產品組織您的團隊有助於提升敏捷度，並更以客戶為中心：
  - 開發可支持商業策略的平衡產品組合。
  - 建立小型、長久又有能力的跨職能團隊，以支持內部和外部客戶的需求。
  - 確定產品負責人、了解客戶旅程、定義及建立產品藍圖，並管理全程的產品生命週期和相關的價值流。
  - 利用雲端平台和敏捷方法快速迭代和發展。
  - 減少產品團隊之間的相依性，並透過定義明確的界面，將團隊有效地整合到更廣泛的營運模式中。
- 戰略合作夥伴關係 – 透過您與雲端供應商的戰略合作夥伴關係，建立或發展您的業務。如果您提供雲端託管軟體解決方案、雲端整合產品或與雲端相關的專業服務、諮詢服務或受管服務，則與您的雲端供應商建立戰略合作夥伴關係，可幫助您建立雲端專業知識、向客戶推銷解決方案及推動成功的客戶互動。

  隨著合作夥伴關係的開展，利用促銷抵用金、資助權益和共同銷售機會，幫助您建立或發展業務。利用雲端供應商的市集通路擴大觸及範圍，利用技術資源幫助您完善雲端產品和服務。發佈聯合案例研究，強調在解決特定商業挑戰時取得的成功。
- 資料變現 – 利用資料獲得可衡量的商業收益。雲端方便您收集、儲存及分析大量的資料。要獲得可衡量的商業收益，請制定與策略目標一致，且全面、長期的資料變現策略。發現利用資料和分析改善營運、客戶和員工體驗、決策以及實踐新商業模式的機會。

  例如，考慮利用客戶行為洞察來推動極高的個性化和本地化、細分客群、訂閱者留存、忠誠度和獎勵計劃等等。專注有助於了解和完成商業交易的交易價值、有助於描述過去績效和推斷結論的資訊價值，以及有助於自動化活動、指導決策和預測結果的分析價值。先在組織內部為資料賦予價值，再考慮外部變現的機會 (例如透過市場銷售資料)。
- 業務洞察 – 獲取即時洞察並回答有關業務的問題。近乎即時的描述性洞察有助於您追蹤商業績效、改進決策並優化營運，進而完成資料變現策略。建立清楚商業環境的跨職能分析團隊。注重技術性技能 (例如統計數字) 和非技術性技能 (如視覺化和溝通)。從分析工作得到相應的業務目標和關鍵績效指標 (KPI)。利用資料目錄找出相關的資料產品，並利用視覺化工具和技術探索資料中的趨勢、模式和關係。首先關注「大局」，再視需要深入鑽研細節。
- 資料科學 – 利用實驗、進階分析和機器學習解決複雜的商業問題。預測性和規範性分析可以讓您提高營運效率和決策以及客戶和員工體驗，助您完成資料變現策略。

  確定商業流程轉型的機會後，確保資料目錄包含支援構置、訓練和測試機器學習模型所需的資料產品。利用持續整合與持續交付 (CI/CD) 做法，提高機器學習工作流程的營運韌性和重現能力。了解模型如何預測並識別任何潛在偏見。為生產階段部署合適的模型並監控其效能。為降低風險，請將低信賴度預測委由人工審查。

人員面向：文化與變革

人員面向是技術與業務之間的橋樑，能加快雲端之旅，幫助組織更快發展出持續成長、學習的文化，即使面臨變化也穩步向前，並以文化、組織結構、領導力和勞動力為重心。此面向包含下圖所示的七項能力。共同利害關係人包括資訊長、營運長、技術長、雲端經理及跨職能和企業各部門主管。

AWS CAF 人員面向功能

- 文化演變 – 利用數位轉型的目標以及敏捷性、自主性、清晰性和可擴展性的最佳實務，評估、漸進發展及編纂組織文化。為在數位轉型中取得成功，您需要充分利用自己的傳統和核心價值，同時融入新的行為和思維模式，以吸引及留住代客戶持續進步和創新的人力，並增強其能力。維持客戶的長期關注與青睞，並大膽創新，以滿足客戶的需求。制定全組織適用的方法，以識別所有角色的行為和目標，從而幫助塑造您想要的文化。考慮快速實驗、敏捷方法和跨職能團隊，以推動所有權和自主權，實現快速決策，並盡可能避免過度審批或官僚主義。
- 轉型領導力 – 加強您的領導能力，並動員各部門主管推動轉型變革，實現以成果為中心的跨職能決策。為成功實現雲端轉型，您的各級主管必須像重視技術一樣，對變革的人員也投注相當的心力，因為若不能有效融合技術和業務領導力，轉型可能會減慢或停滯不前。爭取技術和業務部門高階主管積極、明確的支持，因為這些人會在策略、願景、範圍和資源方面制定重大決策，並在溝通、建立聯盟和讓團隊對成果負責方面採取行動。

  在管理層和計劃層面，確保您的業務和技術主管共同制定、共同領導和共同傳遞文化變革策略。確認每一個管理層面都能提供明確一致的溝通，使組織在雲端價值、輕重緩急和新行為方面保持一致。考慮透過轉型辦公室及/或 Cloud Center of Excellence (CCoE) 發展您的雲端領導職能，利用編纂好的模式推動轉型工作，實現一致性和可擴展性。逐步發展此職能，以滿足轉型之旅的當下需求。

- 雲端流暢性 – 打造數位敏銳度，堅定有效地利用雲端加快實現業務成果。對卓越人力的要求不是能適應數位環境就好，因為最大的挑戰不是技術本身，而是雇用、培養、留任和激勵有才華、知識淵博、熟練且表現優良員工的能力。

  鑑於技術創新的快速發展，請先傳達關於時間、工具和技術培訓的整體培訓策略，再評估您現有的雲端技能，以制定目標明確的培訓策略。發布技能指南，幫助您激發熱情，加速轉型之旅。樹立資料素養，提升資料分析的技能和知識。結合虛擬、課堂、體驗式和即時的培訓，充分利用 Immersion Days，並透過正式的認證驗證技能。實作指導、輔導、影子實習和工作輪換計劃。建立擁有特定目標領域的實踐社群。獎勵分享知識的個人，並制定正式的知識淬取、同儕評鑑和持續策管流程。
- 人力轉型 – 支持人才並實現角色現代化，以吸引、培養和留任熟練數位工具、表現良好且適應力強，能夠自主推動關鍵能力的員工。為成功實現雲端轉型，請採取超越傳統 HR 的主動方法規劃人才支持方案，納入高階主管領導力，並將領導力、學習、獎勵、包容性、績效管理、職業變動性和招聘方法現代化。

  您將需要具備合適的技術性和非技術性技能，兼具多元化和包容性的人力。找出整個組織中角色和技能的差距，並制定可提高組織雲端能力的人力策略。讓具備數位技能的人才以及渴望學習的人才發揮所長，並使其成為眾人學習的榜樣。從戰略角度考慮合作夥伴和受管服務供應商的運用，以暫時或永久增強人力。

  為吸引新進人才，透過公開宣傳數位願景和組織文化，打造優良僱主名聲，並用於招聘策略、社交網路媒體和外部營銷。
- 加速變革 – 從目前狀態邁向未來狀態時，運用程式設計變更加速框架，找出對人員、文化、角色和組織結構的影響，並將這些影響降至最低，從而加快採用新的工作方式。雲端轉型為業務和技術職能方面帶來了大量變化，而組織若套用了結構化、整合且透明的程式設計全端變更流程，則可在價值實現和採用新工作方式這兩方面，達到更高的成功率。

  從專案開始就自訂並運用變更加速框架，以實現組織協調、建立共同經歷的企業現實，並減少流程中的浪費。動員跨職能雲端領導力，並使其達成一致。在旅程初期即定義成功的模樣。透過影響力評鑑來評估組織的雲端整備度，以預想未來。確定主要利害關係人、跨組織相依性、關鍵風險和轉型障礙。制定變更加速策略和藍圖，以應對風險並利用由領導力行動計劃、人才互動、溝通、培訓和風險緩解策略所構成的優勢。

  參與組織活動，使其具備新能力，以提高對新工作方式的接受度、學習新技能並加快採用速度。追蹤明確定義的指標並慶祝早期階段的成功。建立變革聯盟，善加利用有助於產生動力的現有文化手段。在變革的同時，實行持續回饋的機制及獎勵和認可計劃。
- 組織設計 – 評估組織設計，以與新的雲端工作方式保持一致，並隨著轉型之旅的發展而演進。當您利用雲端實現數位轉型時，請確定您的組織設計能夠支援業務、人員和營運環境的核心策略。請建立變革案例，並評估您的組織設計能否反映您判定為業務成功關鍵因素所需要的行為、角色和文化。

就團隊組成方式、輪班模式、報告對象、決策程序和溝通管道等方面，判斷組織的結構和運行方式是否仍能支援您所期望的業務成果。設計新模型，並運用變更加速框架以實作該模型。考慮建立一個會隨著時間而演變的中央團隊，這個團隊最初的目標旨在促進及實現根據您的願景所量身定製的雲端營運模式。權衡集中式、分散式和分佈式結構的優劣，調整您的組織設計，以支援雲端工作負載的策略價值。釐清內部和外部團隊之間的關係 (使用受管服務供應商)。

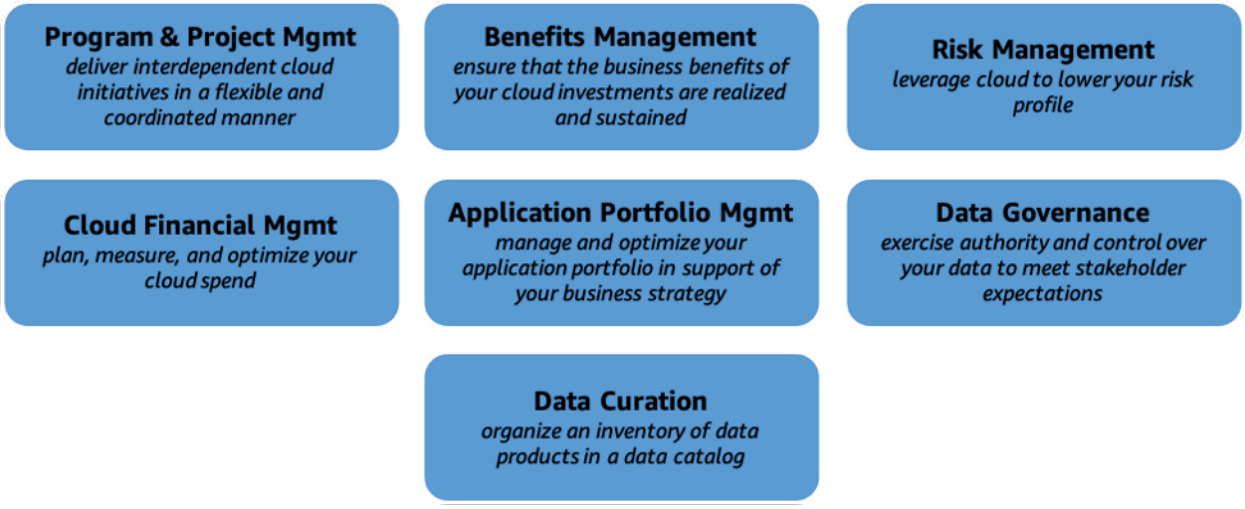
- 組織協調 – 在組織結構、業務營運、流程、人才和文化之間建立持續的合作夥伴關係，讓企業能快速適應市場條件，有能力利用新機遇營利。為擴大實現雲端價值，組織協調要肩負起技術和業務策略之間的溝通，以便產生業務成果的業務部門能接受技術變革。

  優先考慮營運韌性、業務敏捷性和產品/服務創新等業務成果。使人才能夠自發工作、專注於關鍵目標、制定更好的決策，並提高生產力。在應用變更加速框架初期即獲得領導層承諾，以便從一開始就整合人員在領導力敏捷性、人力轉型、人才培養、文化和組織結構等各方面的能力。

  設定雲端採用的可衡量目標、共同目標和機制，並在角色層級建立對技能發展的期望，從而掌握對可持續變革的主動權。採取由上而下的方法來開發共同價值觀、流程、系統、工作方式和技能，共同推動業務成果，並打破職能障壁。讓創新成果傳達到客戶體驗。認可並獎勵持續吸收新知和創新的人。

治理面向：控制和監督

治理面向側重協調雲端計劃，同時將組織效益提到最高、與轉型相關的風險降至最低。此面向包含下圖所示的七項能力。共同利害關係人包括轉型執行長、資訊長、技術長、財務長、資料長和風險長。



AWS CAF 治理面向功能

- 計劃和專案管理 – 以靈活、協調的方式交付相互依賴的雲端計劃。複雜的跨職能雲端轉型計劃需要仔細協調，尤其是在結構較為傳統的組織。因為許多交互相依性只會在交付過程中變得明顯，所以計劃管理尤為重要。管理交互相依性的方式是協調多個計劃，以實現最佳化或整合的成本、排程、工作量和收益。

  定期向公司贊助者驗證您的藍圖，並及時將任何問題上報給高階主管，以推動問責制和透明度。採用敏捷的方法將長遠預測的需求降至最低，改從經驗中學習，並將習得的經驗用於轉型之旅。為協助您因應變化，請將待處理工作按優先順序分好，並依大方向和案例的形式設定工作結構。
- 優勢管理 – 確保能實現與雲端投資相關的業務優勢，並長久維持。轉型成功與否，取決於由此產生的商業優勢。預先辨明想要的優勢，將可讓您確定雲端投資的優先順序，並追蹤一段時間後的轉型進度。選定指標，量化想要的優勢，並傳達給相關利害關係人。根據策略目標調整優勢的時間和生命週期。在優勢實現藍圖中納入優勢傳遞。定期衡量已實現的優勢，再根據優勢實現藍圖評估進度，視需要調整預期優勢。
- 風險管理 – 利用雲端降低風險概況。識別並量化與基礎設施可用性、可靠性、效能和安全性相關的營運風險，以及與聲譽、業務持續性以及快速因應多變市場環境能力相關的業務風險。了解雲端如何幫助您降低風險程度，並持續在您的敏捷步調當中，以迭代方式識別和管控風險。考慮利用雲端降低與基礎設施營運和故障相關的風險。減少對大量前端基礎設施開銷的需求，並降低購買了資產卻再也用不到的風險。根據使用者需求，利用雲端立即佈建和解除佈建資源，以降低採購排程風險。

- 雲端財務管理 – 規劃、衡量及優化您的雲端支出。為團隊的雲端支出，結合雲端提供的輕鬆資源佈建和敏捷優勢與財務問責制。這有助於確保團隊持續優化雲端工作負載，並使用最佳的定價模型。釐清與雲端相關的財務角色和職責，並確保您的財務、業務和技術部門主要利害關係人對雲端成本有一致的理解。發展成更動態的預測和預算規劃流程，並更快找出成本差異和異常。

  將您的帳戶結構和標記策略與組織和產品對應到雲端的方式保持一致。將帳戶和成本分配標籤結構化，以將雲端資源對應到特定的團隊、專案和業務計劃，獲得精細的取用模式檢視。定義成本類別，使用自訂規則整理成本和使用情況資訊，以簡化用量制 (showback) 或退款。使用合併帳單以利簡化雲端計費，並實現大量折扣。建立防護機制，以可擴展且對敏捷性影響最小的方式來管理雲端使用。

  為避免產生技術負債，請確保您的工作負載有良好的架構，並以最符合成本效益的方式運行。利用需求型和計時型的動態佈建，僅支付所需資源的費用。找出並消除有關閒置或使用率過低之雲端資源的開支，以降低雲端成本。

  集中管理內部部署和雲端軟體授權，以減少授權超額費用、減少不合規情況及避免誤報。區分雲端資源包含的授權和您擁有的授權。利用授權使用方式的規則型控制措施，為新的和現有的雲端部署設定硬性或軟性限制。使用儀表板建立授權使用情況的可見性，並加快供應商稽核速度。啟用不合規問題的即時提醒。

- 應用程式組合管理 – 管理及優化您的應用程式組合，以支援您的商業策略。應用程式會為您的商業能力提供支撐，並將能力連結到相關資源。準確而完整的應用程式清單將幫助您發現合理化、遷移和現代化的機會。有效的應用程式組合管理能力可助您將應用程式耗用過多資源的狀況降至最低，輔助應用程式生命週期規劃，並確保能持續與雲端轉型策略保持一致。

  從最重要的應用程式開始，依總體商業能力定義這些應用程式，再對應到提供動能的軟體產品和相關資源。從企業架構、IT 服務管理 (ITSM) 及專案和組合項目管理等相關企業系統中獲取資料，以塑造每個應用程式的全貌。認明主要技術和業務利害關係人 (包括應用程式負責人)，要求這些人定期擴充及驗證應用程式中繼資料。定期評估應用程式組合的運作狀態，以將組織從應用程式投資中獲得的價值最大化。

- 資料治理 – 行使資料的使用權和控制權，以滿足利害關係人的期望。業務流程和分析能力有賴於準確、完整、及時且相關的資料。定義與指派關鍵角色，包括資料擁有者、管理員和保管人。考慮採用聯合 (資料網格) 方法治理。指定標準，包括資料字典、分類和商業詞彙表。確定需要參考的資料集，並建立參考資料實體間的關聯模型。

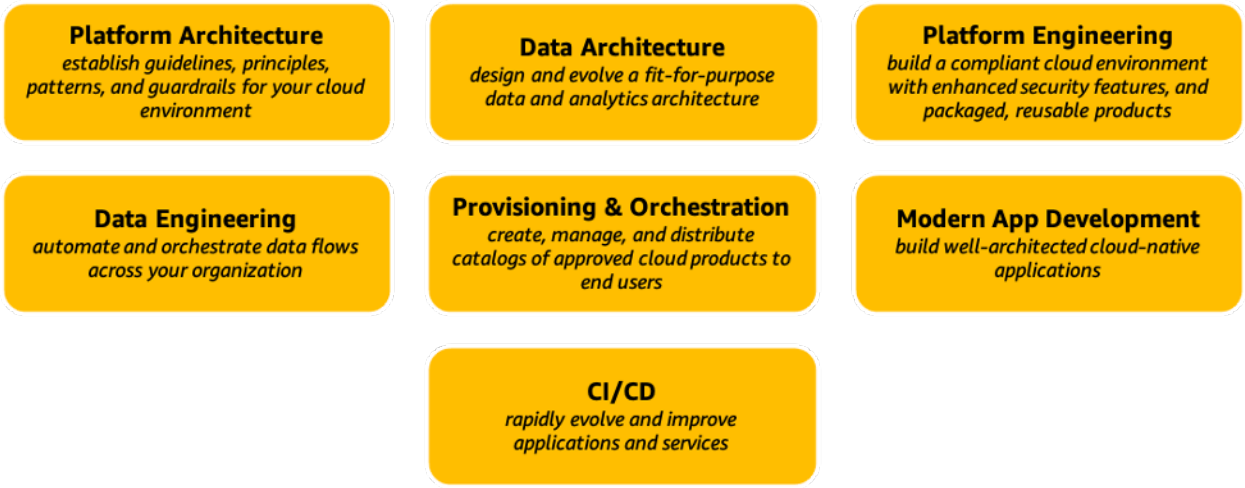
  制定資料生命週期政策，並持續監控合規性。根據您的策略和營運資料需求，將資料品質工作列為優先。建立資料品質標準：確定關鍵品質屬性、商業規則、指標和目標。監控資料價值鏈每一步的資料品質。確定資料品質問題的根本原因，從源頭改善相關流程。為重要資料產品使用資料品質儀表板。

- 策管資料 – 收集、整理、存取及擴充中繼資料，再用以整理資料目錄的資料產品清單。資料目錄幫助資料取用者快速找到相關資料產品及了解其背景 (例如來源和品質)，有利於促進資料變現和自助式分析。

  確定負責審核資料目錄的主要策管人。根據您的資料變現策略，建立關鍵資料產品的目錄，包括結構化和非結構化資料。識別及擷取相關的技術和商業中繼資料，包括資料歷程。利用標準本體、商業詞彙表和自動化 (包括機器學習) 來標記、索引和自動分類資料。視需要輔以手動標記，並適當處理任何個人身分識別資訊 (PII)。考慮透過社交策管，進行群眾外包以擴充資料，也就是考慮讓資料取用者對資料產品進行評級、審查和註釋。

平台面向：基礎設施和應用程式

平台面向側重於透過企業級的可擴展混合式雲端環境，加快傳輸雲端工作負載的速度。此面向包含下圖所示的七項能力。共同利害關係人包括技術長、技術主管、架構師和工程師。



AWS CAF 平台面向功能

- 平台架構 – 建立並維護雲端環境的指導方針、原則、模式和防護機制。架構良好的雲端環境將可協助您加快實作、降低風險及推動雲端採用。在組織內部就推動雲端採用的企業標準達成共識。定義最佳實務藍圖和防護機制，以利進行身分驗證、安全性、聯網和記錄與監控。考慮因延遲、資料處理或資料駐留時間要求，可能需要保留在內部部署的工作負載。評估混合式雲端使用案例，例如雲端服務爆量、備份及災難復原到雲端、分佈式資料處理和邊緣計算。
- 資料架構 – 設計與發展符合用途的資料和分析架構。精心設計的資料和分析架構有助於降低複雜性、成本和技術負債，同時能讓您從以指數級成長的資料量中獲得可行的洞見。採用分層和模組化架構，讓您使用正確的工具處理正確的工作，並以迭代和累進方式發展架構，以滿足層出不窮的需求和使用案例。

  根據您的要求，選擇每個架構層適用的關鍵技術，包括擷取、儲存、編目、處理和使用。為簡化永不停歇的管理工作，請考慮採用無伺服器技術。專注支援即時資料處理，並考慮採用資料湖倉儲架構以促進資料湖和專用資料存放區之間的資料移動。
- 平台工程 – 使用增強的安全功能和封裝的可重複使用雲端產品建立合規的多帳戶雲端環境。有效的雲端環境可讓您的團隊輕鬆佈建新帳戶，同時又能確保這些帳戶符合組織政策。一套經策管的雲端產品將可讓您編纂最佳實務，幫助您實現管理的同時，又能提高雲端部署的速度和一致性。部署您的最佳實務藍圖，以及兼具偵測性和預防性的防護機制。將您的雲端環境與現有生態系統整合在一起，以實現所需的混合式雲端使用案例。

自動化帳戶佈建工作流程，並利用多個帳戶支援安全性和治理目標。設定內部部署和雲端環境間，以及不同雲端帳戶間的連線。在現有的身分供應商 (IdP) 和雲端環境間實作聯合，以便使用者可以使用現有的登入資料驗證身分。集中記錄、建立跨帳戶安全稽核、建立入站和出站網域名稱系統 (DNS) 解析程式，以在儀表板中檢視帳戶和防護機制。

根據公司標準和組態管理評估及認證要取用的雲端服務。將這些企業標準封裝成自助式的可部署產品與可取用服務，同時持續改良。利用 infrastructure as code (IaC) 以宣告方式定義組態。

- 資料工程 – 自動化並協調全組織的資料流程。自動化的資料和分析平台和管道可以幫助您提高生產力並加快產品上市速度。組建包含基礎設施和營運、軟體工程及資料管理的跨職能資料工程團隊。利用中繼資料將取用原始資料並產生最佳化資料的管道自動化。實作相關的架構防護機制和安全控制措施，以及監控、記錄和提醒，以協助解決管道故障問題。識別常見的資料整合模式，並建立可重複使用的藍圖，以抽離管道開發的複雜性。提供藍圖給業務分析師和資料科學家，使其能夠使用自助方法操作。
- 佈建與協同運作 – 建立、管理已核准的雲端產品目錄，並分發給最終使用者。隨著組織的發展，以可擴展和可重複的方式維護一致的基礎設施佈建變得更加複雜。簡化的佈建與協同運作可幫助您實現一致的治理並滿足合規性要求，同時讓使用者只能快速部署經過核准的雲端產品。設計與實作集中管理的自助式入口網站，以發佈、分發、瀏覽及取用已核准的雲端產品。讓大眾透過 API 以及個人化的入口網站存取您的雲端產品。與 IT 服務管理 (ITSM) 工具整合，並將組態管理資料庫 (CMDB) 的所有更新自動化。
- 現代化應用程式開發 – 建立架構良好的雲端原生應用程式。現代化應用程式開發實務可以幫助您實現創新帶來的速度和敏捷性。使用容器和無伺服器技術可幫助您最佳化資源利用率，並自動擴展從零到高峰的需求。考慮將應用程式建立為利用事件驅動架構的獨立微服務，以解耦應用程式。在應用程式開發生命週期的每一層、每一階段都賦予安全性。

  自動化水平擴展和縮減的流程或使用無伺服器技術。現代化您現有的應用程式，以降低成本，提升效率，並充分利用現有的投資。考慮重建平台 (將自己的容器、資料庫或訊息代理程式移動到受管雲端服務) 以及重構 (將舊版應用程式重寫成雲端原生架構)。確保您的架構有考慮到服務配額和實體資源，以免對您的工作負載效能或可靠性產生負面影響。
- 持續整合與持續交付 – 發展與改進應用程式和服務的速度，會比使用傳統軟體開發和基礎設施管理流程的組織更快。採用包含持續整合、測試和部署的 DevOps 實務，將可讓您變得更加靈活，從而使您能夠更快創新、更容易適應不斷變化的市場，並且更有效地推動業務成果。實作持續整合和持續交付 (CI/CD) 管道。

  從持續整合的最低可行管道開始，然後過渡到具有更多元件和階段的持續交付管道。鼓勵開發人員儘早建立單元測試，並先運行程式碼，再將這些程式碼推送到中央儲存庫。在持續交付管道中納入預

備和生產步驟，並考慮手動核准生產部署。考慮多種部署策略，包括就地、滾動、不可變和藍/綠部署。

安全面向：合規與保證

安全面向可幫助您實現資料和雲端工作負載的機密性、完整性和可用性。此面向包含下圖所示的九項能力。共同利害關係人包括資訊安全長、法遵長、內部稽核主管及安全架構師和工程師。

AWS CAF 安全面向功能

- 安全治理 – 開發、維護並有效溝通安全角色、應負的責任、完成工作的責任、政策、流程和程序。確保明確的問責制對安全計劃的有效性至關重要。了解適用於您所在行業及/或組織的資產、安全風險和合規要求，將有助於您安排安全工作的優先順序。提供持續的指導和建議將有助於加快團隊的轉型速度。

  了解您對雲端安全應負的責任。對相關利害關係人、資產和資訊交流進行清點、分類和排列優先順序。找出適用於您所在行業及/或組織的法律、法規、條例和標準/框架。執行組織的年度風險評估。風險評估可協助判斷會影響組織之已知風險及/或漏洞的可能性和影響。為已確定的安全角色和職責配置足夠的資源。依您的合規性要求和組織風險承受能力，制定安全政策、流程、程序和控制措施，並根據不斷變化的風險和要求不斷更新。

- 安全保障 – 持續監控、評估、管理及提高安全和隱私計劃的有效性。您的組織和您服務的客戶都需要信賴您實作的控制措施，相信其可讓您滿足法規要求，並根據您的業務目標和風險承受能力高效地管理安全和隱私風險。

  將控制措施記錄在全面的控制架構中，並建立可證明的安全和隱私控制，以滿足這些目標。檢查雲端供應商曾取得的稽核報告、合規認證或證明，有助您了解其實施措施的控制、這些控制措施的驗證方式，以及這些控制措施能否在您擴展的 IT 環境中有效運作。

持續監控與評估您的環境，以驗證這些控制措施運作的有效性，並證明符合法規和業界標準。查看安全政策、流程、程序、控制和記錄，並視需要與關鍵人員進行面談。

- 身分和權限管理 – 大規模管理身分和權限。您可以使用 AWS 建立身分或連線到您的身分來源，然後授予使用者必要的權限，以便其登入、存取、佈建或協調 AWS 資源和整合的應用程式。有效的身分和存取管理有助於驗證在正確的條件下，正確的人員和機器可以存取正確的資源。

  AWS 設定良好的架構描述了管理身分的相關概念、設計原則和架構最佳實務。其中包括：依賴集中式的身分供應商；利用使用者群組和屬性取得大規模的精細定義存取權和臨時登入資料；以及使用強式登入機制，例如多重要素驗證 (MFA)。若要按 AWS 的人類和機器身分及您的工作負載控制存取，請在特定條件下針對特定資源的特定服務動作設定權限；使用最低權限原則，設定權限邊界，並使用服務控制政策，以便正確的實體可以隨著環境和使用者基數的增長存取正確的資源；以屬性型存取控制 (ABAC) 為基礎，以便政策擴展；以及持續驗證政策是否提供了您所需要的保護。

- 威脅偵測 – 了解並識別可能的安全錯誤組態、威脅或意外行為。更清楚認識安全威脅將能使您優先考慮保護性控制措施。有效的威脅偵測可讓您更快回應威脅並獲得安全事件處理經驗。商定戰術、營運和戰略情報目標和總體方法。挖掘相關資料來源，處理及分析資料，然後傳播並應用見解。

  在環境中普遍部署監控以收集基本資訊，並在非例行位置部署監控以追蹤特定類型的交易。為來自多個事件來源的監控資料建立相互關聯，包括網路流量、作業系統、應用程式、資料庫和端點裝置，以提供穩健的安全狀態並增強可見性。考慮利用欺敵技術 (例如蜜罐)，以了解未經授權的使用者行為模式。

- 漏洞管理 – 持續識別、分類、修復及緩解安全漏洞。改變現有系統或增加新系統也可能會引入漏洞。定期掃描漏洞，有助於抵禦新威脅。使用漏洞掃描程式和端點代理程式建立系統與已知漏洞的關聯。根據漏洞風險排定修補動作的優先順序。應用補救措施並向相關利害關係人報告。利用紅隊演練和滲透測試找出系統架構中的漏洞，視需要向雲端供應商尋求事先授權。

- 保護基礎設施 – 驗證工作負載內的系統和服務皆受到保護，避免意外和未經授權的存取以及可能的漏洞。保護基礎設施遠離意外和未經授權的存取以及可能的漏洞，有助於提升雲端的安全狀態。利用深度防禦將一系列旨在保護資料和系統的防禦機制分層。

  建立網路層，並將不需要存取網際網路的工作負載放在私有子網路中。使用安全群組、網路存取控制清單和網路防火牆來控制流量。根據系統和資料的價值套用零信任。利用 virtual private cloud (VPC) 端點建立雲端資源的私有連線。透過 Web 應用程式防火牆及/或網路防火牆等檢查及篩選每個層的流量。使用強化的作業系統映像，並以物理方式保護內部部署和邊緣的任何混合式雲端基礎設施。

- 保護資料 – 保持對資料的查看和控制能力，並掌握組織存取和使用資料的方式。保護資料免於意外和未經授權的存取以及出現可能的漏洞，是安全計劃的主要目標之一。為幫助您確定適當的保護和保留控制措施，請根據重要性和敏感度分類資料 (例如個人身分識別資訊)。定義資料保護控制措施和生

命週期管理政策。加密所有靜態和傳輸中的資料，並將敏感資料儲存在單獨的帳戶中。利用機器學習自動探索、分類和保護敏感資料。

- 應用程式安全 – 在軟體開發過程中偵測並解決安全漏洞。當您在應用程式編碼階段發現並修復安全缺陷後，就可以省下時間、精力和成本，從啟動到生產都無須憂慮安全狀態。掃描及修補程式碼和相依性中的漏洞，有助於抵禦新威脅。將開發和營運的流程及工具中與安全相關的工作自動化，可將對人工干預的需求降至最低。使用靜態程式碼分析工具找出常見的安全問題。
- 事件回應 – 有效回應安全事件以減少可能的危害。對安全事件快速、有效且一致的回應，將有助於減少可能的危害。讓您的安全作業和事件回應團隊接受有關雲端技術的教育訓練，並說明您的組織將如何使用這些技術。開發 Runbook 並建立事件回應機制庫。邀集主要利害關係人，以更加了解您的選擇對組織其他部分造成的影響。

  模擬安全事件，透過桌上練習和演習訓練事件回應。反覆查看模擬結果，以改善回應態勢的規模、縮短創造價值的時間，並進一步降低風險。利用標準化機制識別及解決根本原因，執行事件後分析，獲得安全事件處理經驗。

營運面向：運作狀態和可用性

營運面向側重於確保依與業務利害關係人商定的等級提供雲端服務。自動化和最佳化作業將可讓您有效擴展，同時提高工作負載的可靠性。此面向包含下圖所示的九項能力。共同利害關係人包括基礎設施和營運部門主管、網站可靠性工程師和資訊科技服務經理。

AWS CAF 營運面向功能

- 可觀察性 – 從基礎設施及應用程式資料中取得可行的洞見。當您以雲端速度和規模作業時，您需要能夠在問題浮現時立即察覺，最好是在干擾客戶體驗之前發現這些問題。開發必要的遙測記錄 (日誌、指標和追蹤)，以了解工作負載的內部狀態和運作狀態。監控應用程式端點，評估對最終使用者的影響，並在測量值超過閾值時產生提醒。

  使用綜合監控建立 Canary (這是按排程執行的可設定指令碼)，以監控您的端點和 API。執行追蹤，以追蹤這些請求在整個應用程式中的傳輸路線，並找出瓶頸或效能問題。利用指標和記錄深入了解資源、伺服器、資料庫和網路。設定時間序列資料的即時分析，以了解影響效能的原因。將資料集中在單一儀表板中，為您提供有關工作負載及其效能重要資訊的整合檢視。
- 事件管理 (AIOps) – 偵測事件、評估其潛在影響並判斷適當的控制動作。能夠過濾雜訊、專注於優先事件、預測資源即將耗盡的情況、自動產生提醒和事件，以及識別可能的原因和補救措施，將有助於您改進事件偵測和回應時間。建立事件儲存模式，利用機器學習 (AIOps) 自動建立事件關聯、偵測異常及判定因果關係。與雲端服務和第三方工具整合，包括您的事件管理系統和流程。自動回應事件，減少因手動流程造成錯誤，並確保快速一致的回應。
- 事件和問題管理 – 快速還原服務營運，並將對業務的不利影響降至最低。經由雲端採用，服務問題和應用程式運作狀態問題的回應流程得以高度自動化，從而拉長服務正常運行時間。隨著您轉向更為

分散的營運模式，簡化相關團隊、工具和流程之間的互動，將有助於加快解決重大及/或複雜事件的速度。在 Runbook 中定義向上呈報路徑，包括觸發向上呈報的條件以及向上呈報的程序。

實行事件反應演習，並將學到的經驗納入 Runbook。識別事件模式以判斷問題和修正措施。利用 Chatbot 和協作工具連接營運團隊、工具和工作流程。利用不指責的事件後分析，確定導致事件的因素，並制定相應的行動計劃。

- 變更和版本管理 – 引入及修改工作負載，同時將生產環境風險降至最低。傳統的版本管理流程很複雜，部署速度緩慢又難以轉返。雲端採用讓您有機會利用 CI/CD 技術快速管理版本和轉返。建立允許自動核准工作流程的變更流程，使其與雲端敏捷性保持一致。使用部署管理系統來追蹤和實作變更。透過頻繁、細微和可逆的變更來縮小變更範圍。測試變更並在生命週期所有階段驗證結果，以將失敗部署的風險和影響降至最低。當無法實現結果時，自動還原到先前的良好狀態，以最大限度縮短還原時間，並減少由手動程序引起的錯誤。
- 效能和容量管理 – 監控工作負載效能，並確保容量滿足當下和未來的需求。雖然雲端容量幾乎無限制，但服務配額、容量預留和資源約束會限制實際的工作負載容量。您需要了解這種容量約束，才能有效加以管理。辨明主要利害關係人並議定中長期目標、範圍和指標。收集及處理效能資料，並定期針對目標檢閱及報告效能。定期評估新技術以提高效能，並酌情建議變更目標和指標。監控工作負載的利用率，建立未來的比較基準，並視需要確定擴展容量的閾值。分析一段時間的需求，以確保容量能符合季節性趨勢和波動的營運條件。
- 組態管理 – 維護準確且完整的一段時間內所有雲端工作負載、其關係及組態變化記錄。若不以有效方式管理，雲端資源佈建的動態和虛擬性質會造成組態偏移。定義並強制執行可將商業屬性覆蓋到雲端使用方式的標記結構描述，然後利用標籤按照技術、業務和安全層面安排資源。指定強制標籤並透過政策強制執行合規性。利用 Infrastructure as Code (IaC) 和組態管理工具進行資源佈建和生命週期管理。建立組態基準並透過版本控制加以維護。
- 修補程式管理 – 以系統化方式分配及套用軟體更新。軟體更新可解決新出現的安全漏洞、修復錯誤，並引入新功能。管理修補程式的系統化方法會確保您能從最新的更新獲益，同時將生產環境風險降至最低。在指定的維護時段內套用重要更新，並儘快套用重大安全性更新。提前通知使用者即將進行之更新的詳細資訊，並允許使用者在有其他緩解控制措施可用時延遲修補程式。先更新機器映像和測試修補程式，再發佈到生產環境。為確保修補過程中的持續可用性，請考慮為每個可用區域 (AZ) 和環境設定不同的維護時段。定期審查修補程式的合規性，並提醒不符合規範的團隊套用必要的更新。
- 可用性和持續性管理 – 確保商業重大資訊、應用程式和服務的可用性。建置雲端備份解決方案需要仔細考慮現有的技術投資、恢復目標和可用資源。災難和安全事件後的及時還原有助於保持系統可用性和業務持續性。根據定義的排程備份資料和文件。

  在業務持續性計劃之下，制定災難復原計劃。確定每個工作負載不同災難情境下的威脅、風險、影響和成本，並據以指定復原時間點目標 (RTO) 和復原點目標 (RPO)。利用多可用區域或多區域架構，

實作您選擇的災難復原策略。考慮利用混沌工程，透過對照實驗，改善復原力和效能。定期審查和測試您的計劃，根據習得的經驗調整方法。

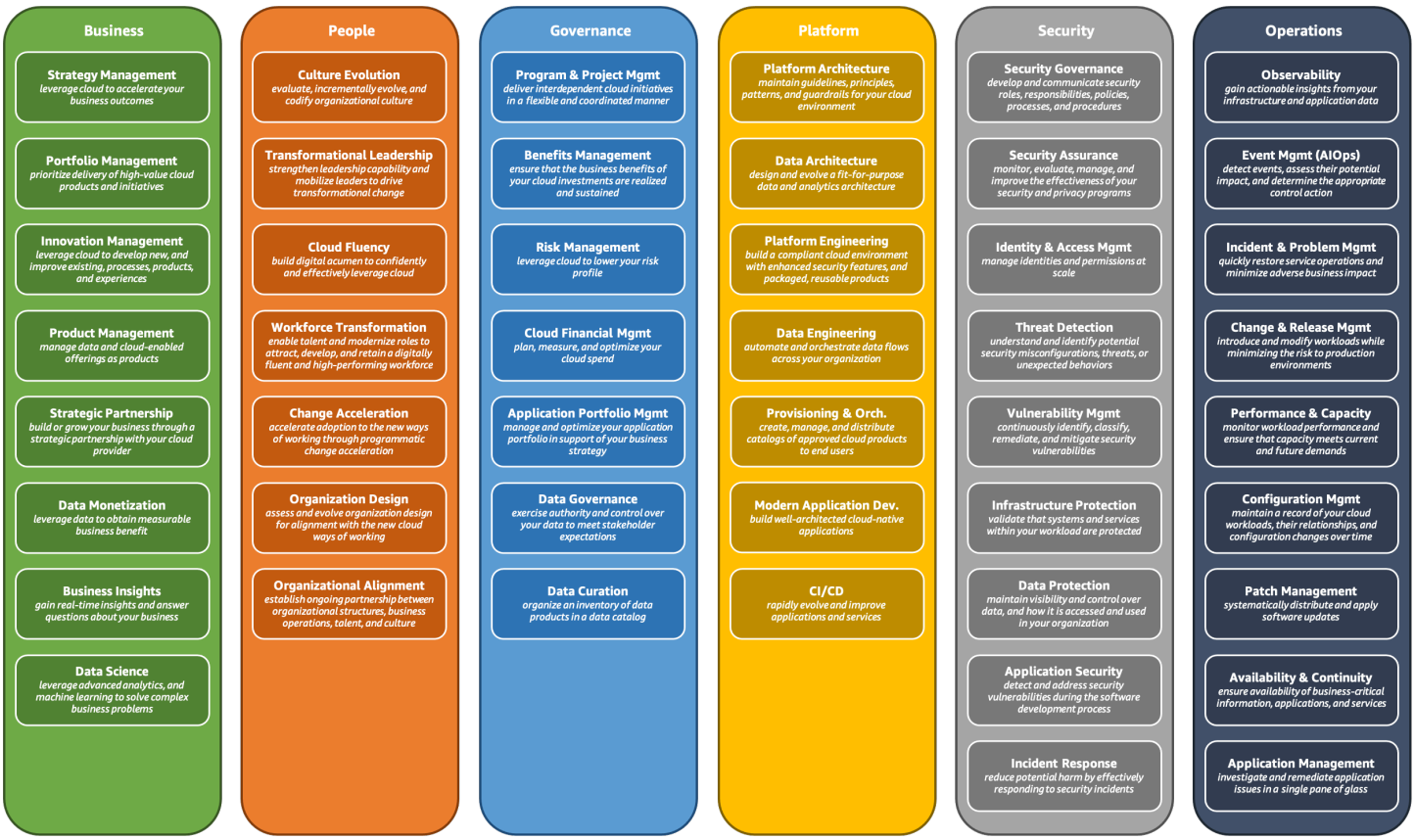
- 應用程式管理 – 使用單一虛擬管理平台調查及修復應用程式問題。將應用程式資料彙總到單一管理主控台，可以簡化營運監督，並透過降低切換不同管理工具環境的需求，加快修復應用程式問題。

  與其他營運和管理系統整合 (例如應用程式組合管理和 CMDB)，將發現應用程式元件和資源的流程自動化，並將應用程式資料合併到單一管理控制台中。納入軟體元件和基礎設施資源，並說明不同的環境，如開發、預備和生產。為更快、更一致地修復作業問題，請考慮將 Runbook 自動化。

結論

隨著技術創新不斷加快，持續進行數位轉型的需求將變得更加迫切。AWS CAF 利用 AWS 的經驗和最佳實務，幫助您以新穎的方式使用 AWS，加快實現業務成果。使用 AWS CAF 找出轉型機會並列為優先事項，接著評估和改進雲端整備度，然後迭代發展轉型藍圖。

附錄：AWS CAF 能力海報



AWS CAF 基礎功能

作者群

- 撰寫者：AWS CAF 全球領導人 Saša Baškarada 博士，滙集眾多 AWS 主題專家的意見。

深入閱讀

如需其他資訊，請參閱：

- AWS 架構中心
- AWS 案例研究
- AWS 一般參考資料
- AWS 詞彙表
- AWS 知識中心
- AWS 方案指引
- AWS 快速入門
- AWS 安全性文件
- AWS 解決方案資源庫
- AWS Training and Certification
- AWS Well-Architected
- AWS 白皮書和指南
- AWS 入門
- Amazon Web Services 概觀

文件修訂

請訂閱 RSS 摘要，以收到此白皮書的更新通知。

update-history-change	update-history-description	update-history-date
第三次發行	更新及擴展了能力。增加了轉型領域和旅程階段。	2021 年 11 月 22 日
第二次發行	面向和能力的結構性變化。	2017 年 2 月 1 日
初次發行	白皮書第一次發行。	2015 年 2 月 1 日

聲明

客戶應負責對本文件中的資訊自行進行獨立評估。本文件：(a) 僅供參考之用，(b) 代表目前的 AWS 產品供應與實務，如有變更恕不另行通知，以及 (c) 不構成 AWS 及其附屬公司、供應商或授權人的任何承諾或保證。AWS 產品或服務以「現況」提供，不提供任何明示或暗示的擔保、主張或條件。AWS 對其客戶之責任與義務，應受 AWS 協議之約束，且本文件並不屬於 AWS 與其客戶間之任何協議的一部分，亦非上述協議之修改。

© 2021 Amazon Web Services, Inc. 或其關係企業。保留所有權利。