AWS 白皮书

AWS Cloud Adoption Framework 概览

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

AWS Cloud Adoption Framework 概览: AWS 白皮书

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

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆或者贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

摘要 1
摘要 1
介绍 2
加速实现业务成果 3
基础功能 5
您的云转型历程 7
业务观点 9
人员视角 11
治理视角 14
平台视角 17
安全视角 19
运营视角 22
总结 25
附录：AWS CAF 功能海报 26
贡献者 27
延伸阅读 28
文档修订 29
声明 30

AWS Cloud Adoption Framework 概览

发布日期：2021 年 11 月 22 日（文档修订）

摘要

随着数字技术的普及，细分市场和行业不断被打乱，采用 Amazon Web Services (AWS) 可以帮助您实现企业转型，以应对不断变化的商业环境和不断演变的客户需求。作为全球最全面、应用最广泛的云平台，AWS 可以帮助您降低成本和业务风险、提高运营效率和敏捷性、加快创新速度、创造新的收入流以及重塑客户和员工体验。

AWS Cloud Adoption Framework (AWS CAF) 采用了 AWS 的经验和最佳实践，帮助您通过以创新方式使用 AWS 来实现数字化转型并加快获得业务成果。使用 AWS CAF 识别转型机会并确定其优先级，评估和改善云就绪情况，并以迭代方式逐步演变转型路线图。

引言

数字技术的迅速普及加速了变革，并加剧了一系列细分市场和行业的竞争。由于保持任何特定的竞争优势变得越来越难，企业被迫在越来越短的时间间隔内进行自我改造。例如，预计标准普尔 500 指数中有 50% 的公司将在未来十年内被取代。

同样，公民不断变化的期望和行为也在给公共部门施加压力，要求它们改进数字服务交付。全球范围内的各家企业都在进行数字化转型；他们正在利用数字技术来推动组织变革，从而适应不断变化的市场环境，取悦客户，并加快实现业务成果。

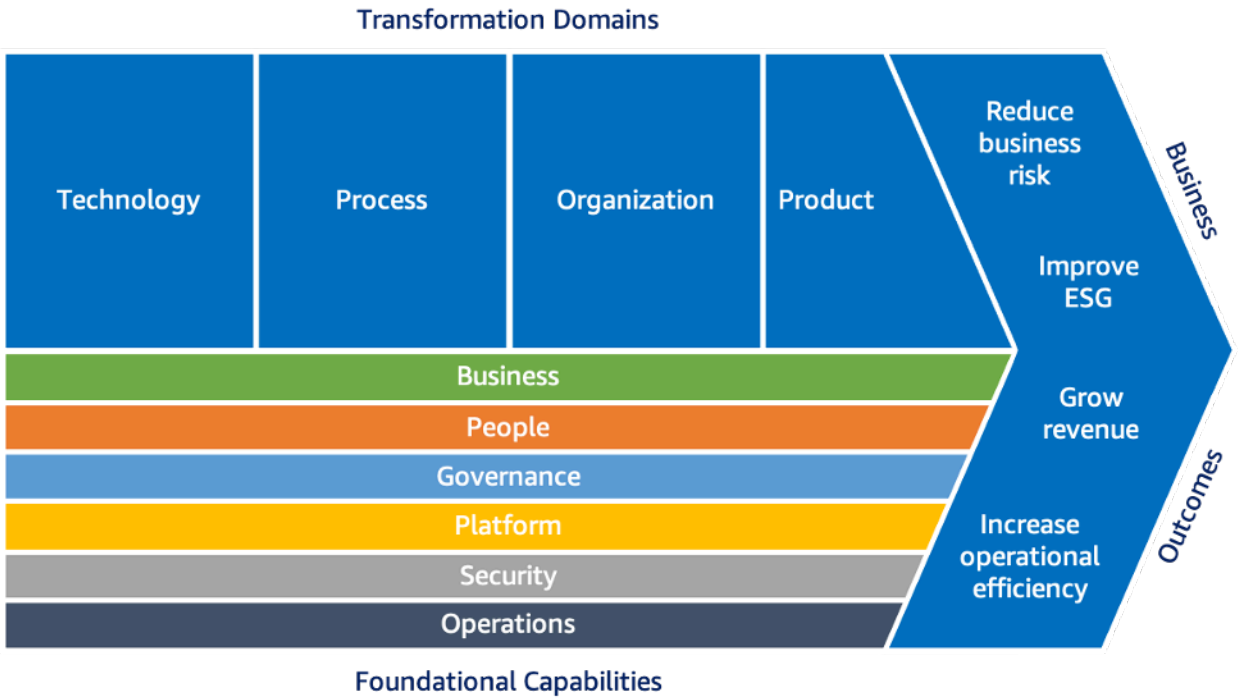
数百万个 AWS 客户（包括增长最快的初创公司、大型企业和领先的政府组织）都在利用 AWS 迁移并现代化旧式工作负载，从而成为数据驱动型组织，实现业务流程的数字化和优化，以及重塑运营和业务模式。通过云驱动的数字化转型（云转型），他们能够改善业务成果，包括降低成本和业务风险、提高运营效率和敏捷性、加快创新、开辟新的收入来源以及改善客户和员工体验。

您有效利用云进行数字化转型（云就绪性）的能力是以一系列基本组织功能为基础的。AWS CAF 可以识别这些功能，并提供了规范性准则，全球数千家企业已成功利用这些准则来加快云转型历程。

AWS 和 AWS 合作伙伴网络提供的工具和服务可帮助您完成这个历程中的每一个步骤。AWS 专业服务是一个由专家组成的全球团队，该团队通过一系列与 AWS CAF 一致的产品/服务来帮助您实现与云转型相关的特定成果。

利用云驱动的数字化转型加速实现业务成果

下图中的云转型价值链表明，一系列由基础能力支持的云驱动的组织变革（转型）加速了业务成果的实现。转型领域表示一个价值链，其中技术转型推动流程转型，流程转型推动组织转型，而组织转型又推动产品转型。关键业务成果包括降低了业务风险、改善了环境、社会和治理 (ESG) 绩效，以及提高了收入和运营效率。



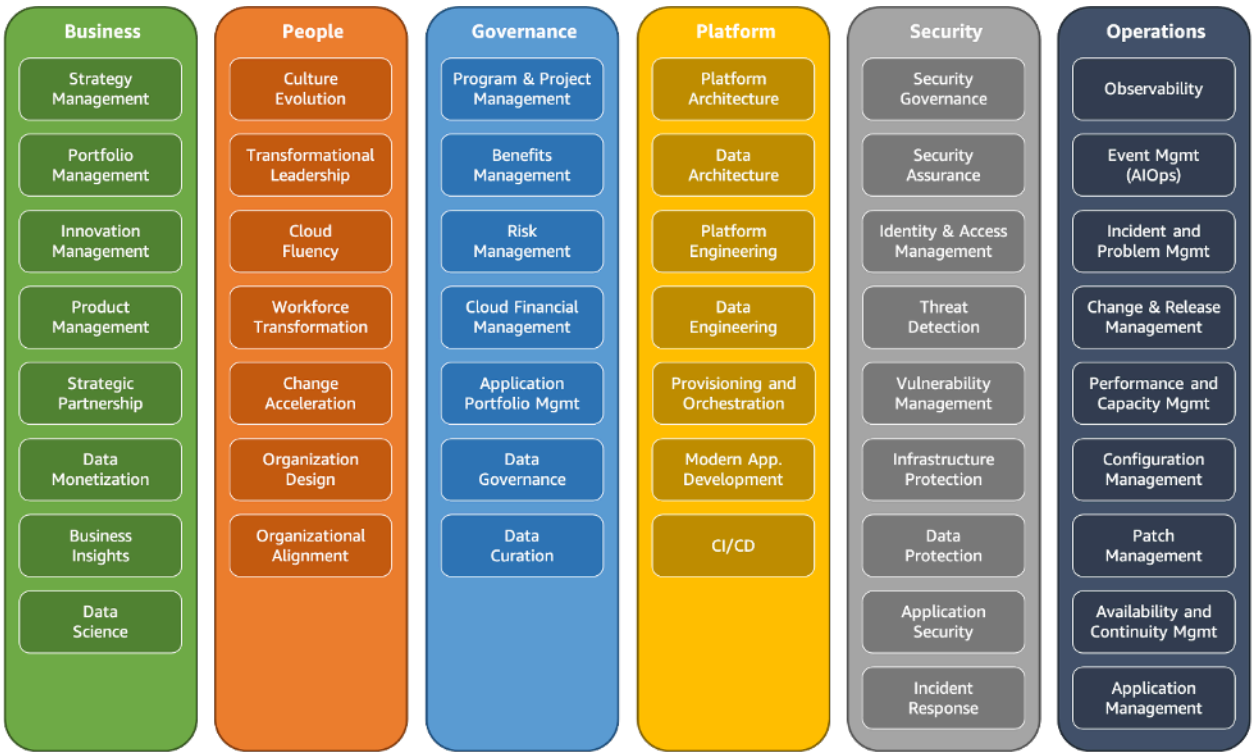
云转型价值链

- 技术转型专注于使用云来迁移和现代化旧式基础设施、应用程序以及数据平台和分析平台。云价值基准测试表明，通过从本地部署迁移到 AWS，每个用户的成本降低了 27%，每个管理员管理的虚拟机数量增加了 58%，停机时间减少了 57%，安全事件减少了 34%。
- 流程转型专注于实现业务运营的数字化、自动化和优化。这可能包括利用新的数据和分析平台来挖掘切实可行的洞察，或使用机器学习 (ML) 来改善客户服务体验、员工生产力和决策、业务预测、欺诈侦测和预防、工业运营等。这样做可以帮助您提高运营效率，降低运营成本并改善员工和客户体验。
- 组织转型专注于重新构想您的运营模式；您的业务和技术团队如何编排工作以创造客户价值并满足您的战略意图。通过围绕产品和价值流组建团队，并利用敏捷方法进行快速迭代和发展，可帮助您提高响应能力并践行客户至上的理念。

- 产品转型专注于通过确立新的价值主张（产品、服务）和收入模式来重新塑造您的业务模式。这样做可以帮助您接触新客户并进入新的细分市场。云价值基准测试表明，借助 AWS，新功能和应用程序的上市时间缩短了 37%，代码部署频率提高了 342%，部署新代码所需的时间减少了 38%。

基础功能

上一个部分中描述的每个转换领域都由下图所示的一组基础功能提供支持。功能是指利用流程部署资源（人员、技术以及任何其他有形或无形资产）来实现特定成果的组织能力。AWS CAF 功能可提供最佳实践指导，帮助您改善云就绪情况（有效利用云进行数字化转型的能力）。AWS CAF 从六个视角对其功能进行分组：业务、人员、治理、平台、安全和运营。每个视角均包含一组功能，职能上相关的利益攸关方在云转型之旅中将拥有或管理这些功能。



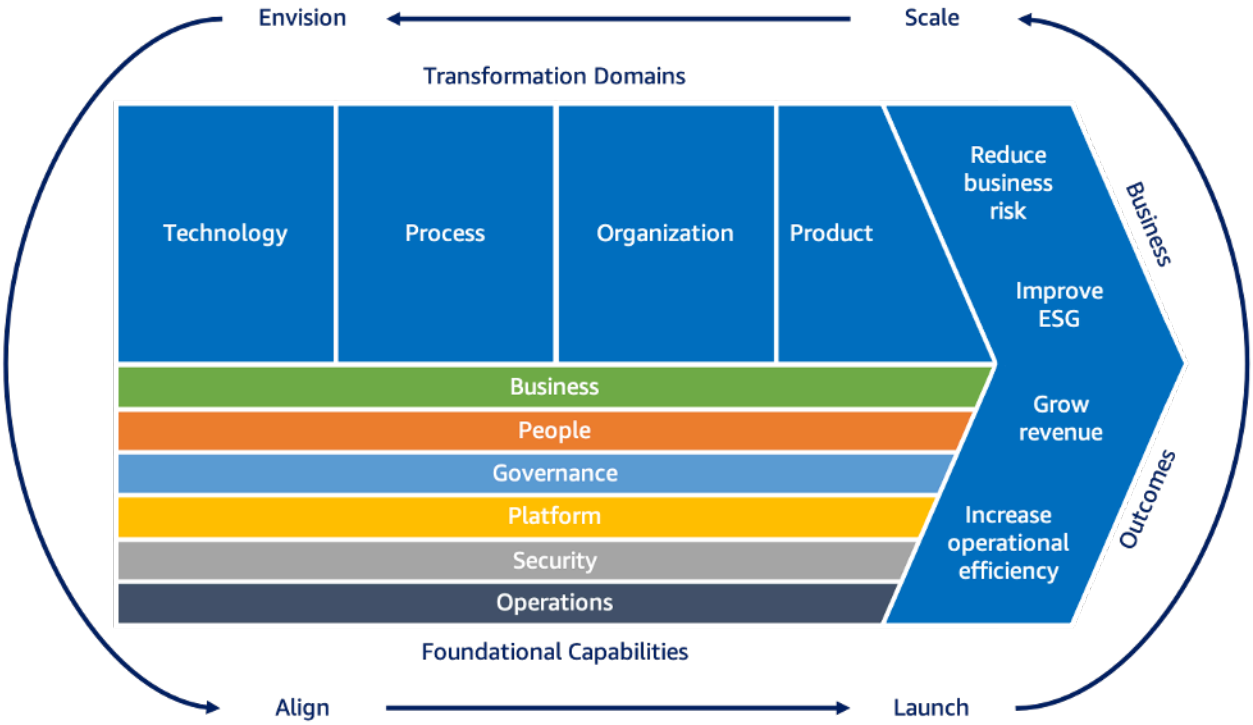
AWS CAF 视角和基础功能

- 业务视角有助于确保您的云投资能够加快实现数字化转型雄心和业务成果。常见的利益攸关方包括首席执行官 (CEO)、首席财务官 (CFO)、首席运营官 (COO)、首席信息官 (CIO) 和首席技术官 (CTO)。
- 人员视角充当了技术与业务之间的桥梁，可加速云之旅以帮助企业更快地打造持续增长和学习的文化，使变革成为业务常态，并将重点放在文化、组织结构、领导力和劳动力上。常见的利益攸关方包括 CIO、COO、CTO、云主管以及跨职能部门和企业内的领导者。
- 治理视角可帮助您协调云计划，最大限度地提高组织收益并最大限度地降低与转型相关的风险。常见的利益攸关方包括首席转型官、CIO、CTO、CFO、首席数据官 (CDO) 和首席风险官 (CRO)。
- 平台视角可帮助您构建企业级、可扩展的混合云平台，实现现有工作负载的现代化，并实施新的云原生解决方案。常见的利益攸关方包括 CTO、技术负责人、架构师和工程师。

- 安全视角可帮助您实现数据和云工作负载的机密性、完整性和可用性。常见的利益攸关方包括首席信息安全干事 (CISO)、首席合规官 (CCO)、内部审计主管以及安全架构师和工程师。
- 运营视角有助于确保云服务的交付水平能够满足您的业务需求。常见的利益攸关方包括基础设施和运营负责人、站点可靠性工程师和信息技术服务经理。

您的云转型历程

每个企业的云之旅都是独一无二的。要成功实现转型，您需要设想所需的目标状态，了解云就绪情况，并采用敏捷方法来缩小差距。递增式转型可让您快速展示价值，并最大限度地减少做出深远预测的需要。采用迭代方法将帮助您保持势头，并在您从经验中学习的过程中演进您的路线图。AWS CAF 推荐了四个迭代和递增式云转型阶段，如下图所示。

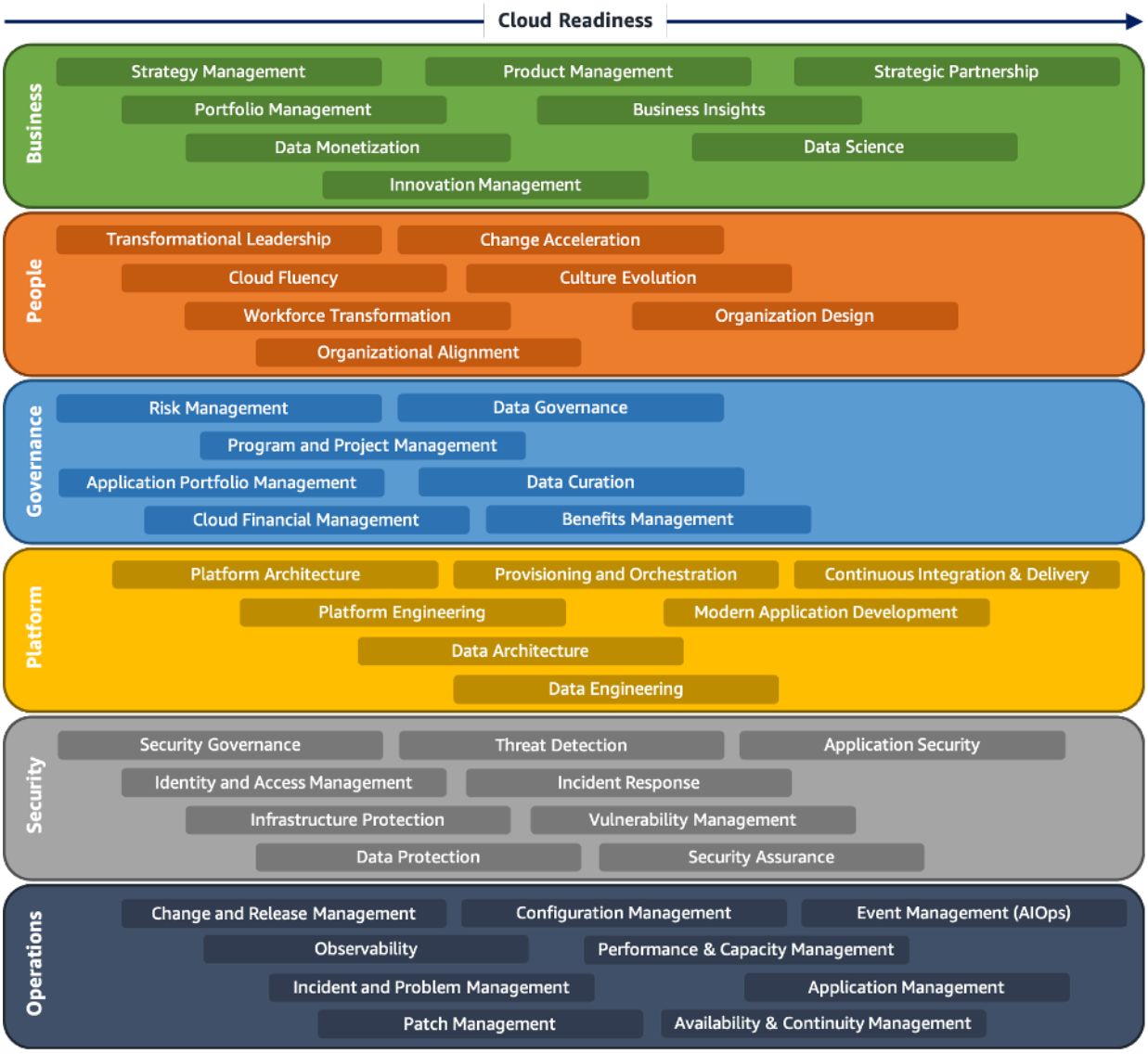


云转型历程

- 设想阶段专注于演示云将如何帮助您加快获得业务成果。它通过根据您的战略业务目标确定四个转型领域中每个领域的转型机会并确定这些机会的优先次序来做到这一点。将转型计划与关键利益攸关方（能够影响和推动变革的资深人士）和可衡量的业务成果联系起来，这将有助于您在转型历程中展示价值。
- 调整阶段专注于标识 AWS CAF 的六个视角之间的能力差距，识别跨组织的依赖关系，并揭示利益攸关方的担忧和挑战。这样做将有助于您制定策略来改善云就绪情况，确保利益攸关方协调一致，并促进相关的组织变革管理活动。
- 启动阶段专注于在生产环境中交付试点计划，并展示递增商业价值。试点计划应具有很大的影响力，如果获得成功/当获得成功时，它们将帮助影响未来的方向。从试点计划中学习将有助于您在全面生产之前调整方法。

- 扩展阶段专注于将生产试点和商业价值扩展到所需的规模，并确保实现和维持与云投资相关的商业利益。

您可能不需要一次性地处理所有基本功能。在您的云转型历程中，逐步发展基本功能并改善云就绪情况。考虑根据您的特定需求定制建议的顺序，如下图所示。



AWS CAF 视角和基础功能的演进

后续部分将更详细地介绍所有六个 AWS CAF 视角和基础功能。

业务观点：策略和成果

业务观点专注于确保您的云投资能够加快实现您的数字化转型雄心和业务成果。它包含八项功能，如下图所示。常见的利益攸关方包括 CEO、CFO、COO、CIO 和 CTO。

AWS CAF 业务观点功能

- 策略管理 – 利用云加速实现业务成果。考虑云如何支持和塑造您的长期业务目标。找出偿还技术债务、利用云优化技术和业务运营的机会。探索借助云功能实现的新的价值主张和收入模式。考虑新的或改进的支持云的产品和服务如何帮助您接触新客户或进入新的细分市场。优先考虑您的战略目标，并随着时间的推移不断改进您的策略，以响应业务环境中的技术发展和变化。
- 产品组合管理 – 根据战略意图、运营效率和您的交付能力，确定云产品和计划的优先次序。通过在正确的时间交付正确的云产品和计划，有助于实施您的策略并加快实现业务成果。利用自动发现工具以及将应用程序迁移到云的七种常见迁移策略（称为 7 R）来合理化现有的应用程序组合，并构建数据驱动型业务案例。

  考虑短期和长期成果以及低风险（经验证）和高风险（实验性）机会，使您的云产品组合保持平衡。包含迁移、现代化和创新计划，并考虑财务收益（降低成本和/或增加收入）和非财务益处（例如，改善客户和员工体验）。根据您的资源、财务和计划限制，优化产品组合的商业价值。要缩短价值转化时间，请考虑提升规划周期的频率或采用持续规划策略。
- 创新管理 – 利用云开发新的流程、产品和体验，并改进现有的流程、产品和体验。云让您能够即时预置和关闭资源，因此可以帮助您缩短价值转化时间，并降低与创新相关的成本和风险。云采用提高了业务敏捷性，要充分利用这一优势，可以制定一个创新策略，其中混合专注于优化现有产品、流程和体验的增量式创新计划和专注于实现新商业模式的颠覆性创新计划。根据您的战略重点，建立征求和选择创意的机制，并开发端到端流程来推广成功的创新试点。

- 产品管理 – 管理支持数据和云的产品/服务，在产品的生命周期内为内部和外部客户提供可重复创造的价值。 通过围绕支持数据和云的产品组建您的团队，您能够变得更敏捷，更专注于客户：
  - 开发均衡的产品组合来支持您的商业策略。
  - 组建强大的、持久性的小型跨职能团队，满足内部和外部客户的需求。
  - 确定产品负责人，了解客户历程，定义和创建产品路线图，并管理端到端产品生命周期和相关的价值流。
  - 利用您的云平台和敏捷方法实现快速迭代和发展。
  - 减少各个产品团队之间的依赖，并通过明确定义的接口有效地将其融入更广泛的运营模式中。
- 战略伙伴关系 – 通过与云提供商建立战略伙伴关系，构建或拓展您的业务。如果您提供云托管的软件解决方案、云集成产品或与云相关的专业服务、咨询服务或托管式服务，则与云提供商进行战略合作可以帮助您建立云专业知识，向客户推介您的解决方案，并加快实施成功的客户参与。

  随着合作的进一步加强，您可以利用服务抵扣金、资助计划权益和联合销售机会来构建或拓展业务。利用云提供商的市场渠道扩大覆盖面，并利用技术资源来帮助您使基于云的产品和服务变得更加成熟。发布联合案例研究，重点说明在解决特定业务挑战方面取得的成功。
- 数据货币化 – 利用数据获得可衡量的商业利益。云有助于收集、存储和分析大量数据。要获得可衡量的商业利益，请制定符合您的战略意图的全面、长期的数据货币化策略。发现机会，利用数据和分析来改善运营、客户和员工体验与决策以及实施新的商业模式。

  例如，考虑利用客户行为洞察来推动超个性化和本地化、微观市场细分、订户保留、忠诚度和奖励计划等。重点关注可帮助您理解和达成商业交易的交易价值、可帮助您描述过去业绩和推断结论的信息价值，以及可帮助您自动执行活动、指导决策和预测结果的分析价值。在考虑外部货币化的机会（例如，通过市场销售数据）之前，首先在企业内部将数据货币化。
- 业务洞察 – 获取实时洞察并回答有关业务的问题。近乎实时的描述性洞察可让您跟踪业务绩效、改进决策并优化运营，从而帮助您成功实施数据货币化策略。组建跨职能分析团队，充分了解业务环境。专注于技术性技能（例如统计数据）和非技术性技能（例如可视化和沟通）。使您的分析工作与业务目标和关键绩效指标 (KPI) 保持一致。利用数据目录找到相关的数据产品，并利用可视化工具和技术来发现数据的趋势、模式和关系。首先以“大局”为主，然后根据需要深入到细节。
- 数据科学 – 使用实验、高级分析和机器学习来解决复杂的业务问题。利用预测性分析和规范性分析，您可以改进运营效率和决策并提升客户和员工体验，从而成功实施数据货币化策略。

  在确定业务流程转型机会后，请确保您的数据目录包含所需的数据产品，以支持机器学习模型的构建、训练和测试。利用持续集成和持续交付 (CI/CD) 实践来提高机器学习工作流的运营弹性和可再现性。了解您的模型如何进行预测并识别任何潜在的偏差。将合适的模型部署到生产环境并监控其性能。要降低风险，可将低置信度的预测委托给人工审查。

人员视角：文化与变革

人员 视角充当技术与业务之间的桥梁，可加速云之旅以帮助企业更快地打造持续增长和学习的文化，使变革成为业务常态，并关注文化、组织结构、领导力和人力等方面。此视角包含七项功能，如下图所示。常见的利益攸关方包括 CIO、COO、CTO、云主管以及跨职能部门和企业内的领导者。

AWS CAF 人员视角功能

- 文化演变 – 依据数字化转型愿望以及敏捷性、自主性、清晰度和可扩展性的最佳实践，评估、逐步发展组织文化和编集成典。要成功实施数字化转型，您需要利用自己的传统和核心价值观，同时融入新的行为和思维方式来吸引和留住人力并为其提供支持，他们代表客户不断改进和创新。保持长期关注，专注于客户，大胆创新以满足他们的需求。制定一种企业范围的方法来识别所有角色的行为和目标，帮助塑造所需的文化。考虑快速实验、敏捷方法和跨职能团队，以推动所有权和自主权，实现快速决策，并最大限度地减少过度审批或消除官僚主义行为。
- 变革型领导力 – 增强领导能力，动员领导者推动变革，实施注重结果的跨职能决策。要成功实现云转型，领导者必须像关注技术一样关注变革中的人员，因为如果没有技术和业务领导力的有效结合，转型过程可能会放缓或停滞。获得来自技术和业务职能部门的积极明确的高管支持，他们将在战略、愿景、范围和资源方面做出关键决策，并在沟通、联盟建设以及让团队对结果负责方面采取行动。

  在执行和计划层面，确保您的业务和技术领导者共同制定、共同领导和共同实施文化变革策略。确认在每个层次的管理人员中，都传达了清晰、一致的沟通信息，使企业在云价值、优先级和新行为方面保持一致。考虑通过转型团队和/或卓越云中心 (CCoE) 提升您的云领导职能，以使用编集成典的模式宣传和推动您的转型工作，从而实现一致性和可扩展性。在转型过程中，逐步提升此职能以满足您当前的需求。

- 云的流畅性 – 建立数字敏感度，自信和有效地利用云加速业务成果。对优秀员工的要求不仅仅是适应数字环境，最大的挑战并不是技术本身，而是聘用、培养、保留和激励有才华、知识渊博、熟练和高效的人力的能力。

  鉴于技术创新的快速发展，应考虑与时间、工具和技术培训相关的整体培训策略，然后评估现有的云技能，以制定有针对性的培训策略。实施 Skills Guild 来帮助您激发兴奋感，为您的转型之旅创造动力。倡导数据素养，增强数据分析方面的人才技能和知识。将虚拟、课堂、体验式和即时培训相结合，利用沉浸日，并通过正式认证验证技能。实施指导、辅导、跟踪和轮岗计划。建立拥有特定兴趣领域的实践社群。奖励分享知识的人员，并且确立知识启发、同行评审和持续管理的正式过程。

- 人力转型 – 为人才提供支持并实现角色现代化，以吸引、培养和留住能够自主推动关键能力、熟练掌握数字技能、高绩效且适应能力强的员工。要成功实现云转型，在传统人力资源之外，应采取积极主动的人才支持规划方法，包括高管层领导，并实现领导、学习、奖励、包容、绩效管理、职业流动性和招聘方法的现代化。

  您将需要多元化和包容性的员工，而且他们应拥有适当的技术和非技术技能组合。确定整个企业范围内的角色和技能差距，并制定人力策略以提高组织云能力。充分利用拥有数字技能的人才，以及那些渴望学习的人才，并将他们作为榜样。在战略上考虑使用合作伙伴和托管式服务提供商来临时或永久性扩充人力。

  为了吸引新的人才，可以公开宣传您的数字愿景和组织文化来打造强大的雇主品牌，并将其应用到您的招聘策略、社交网络渠道和外部营销中。

- 变革加速 – 通过应用程序化的变更加速框架，在从当前状态转移到未来状态时，确定并最大限度地减小对人员、文化、角色和组织结构产生的影响，从而加速新工作方式的采用。云转型为业务和技术职能部门带来了大范围的变化，而当企业应用结构化、集成和透明的端到端程序化变更流程后，可以通过价值实现并采用新的工作方式，提高成功率。

  从项目一开始就定制和应用变革加速框架，以实现组织协调，打造共享的企业氛围，并减少流程中的浪费。协调和调动跨职能的云领导力。在该历程的早期明确成功的定义。通过影响评估来评估企业的云就绪性，展望未来。确定关键利益攸关方、跨组织的依赖关系、关键风险和转型障碍。制定应对风险和发挥优势的变革加速策略和路线图，包括领导力行动计划、人才参与、沟通、培训和风险缓解策略。

  让企业参与进来，并赋予其新的能力，以便提高对新工作方式的接受度，学习新的技能，并加速采用。跟踪明确定义的指标，奖励初步成功。建立一个变革联盟，利用现有的文化杠杆来帮助您创造动力。通过持续的反馈机制、奖励和认可程序来坚持变革。

- 企业设计 – 评估企业设计，以便与新的云工作方式保持一致，并随着转型历程的不断深入而演进。在利用云进行数字化转型时，请确保您的企业设计支持针对业务、人员和运营环境制定的核心策略。

建立一个变革案例，并评估您的企业设计是否反映了您视为业务成功关键因素的所需行为、角色和文化。

根据团队构成、轮班模式、报告路线、决策过程和沟通渠道，确定企业的结构和运营方式是否仍能帮助您实现所需的业务成果。设计新模式，并通过应用变革加速框架来实施该模式。考虑组建一个集中式团队，该团队随着时间的推移而发展，最初将促进并实现向可根据您的愿景定制的云运营模式进行过渡。考虑在集中式、去中心化和分布式结构之间进行权衡，调整企业设计以帮助实现云工作负载的战略价值。阐明内部团队和外部团队之间的关系（使用托管式服务提供商）。

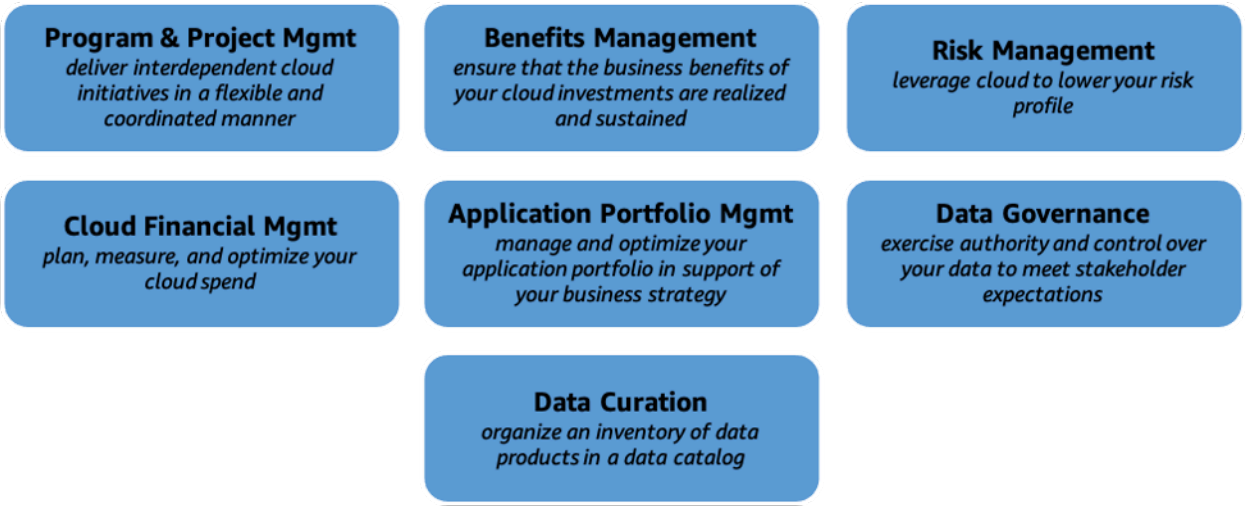
- 组织协调 – 在组织结构、业务运营、流程、人才和文化之间建立持续的合作关系，使企业能够快速适应市场条件，并有能力利用新的机会。为了加强云价值实现，可以将组织协调作为技术与业务策略之间的桥梁，以便创造业务成果的业务部门能够接受技术变革。

  优先考虑诸如运营弹性、业务敏捷性和产品/服务创新这样的业务成果。使人才能够自主工作，专注于关键目标，制定更佳的决策，并提高生产力。获得领导层对早期应用变革加速框架的承诺，以便从一开始就整合人员在领导力敏捷性、人力转型、人才赋能、文化和企业结构方面的能力。

  为云采用设定可衡量的目标、共同目标和机制，并在职位层面设定技能培养期望，以实现可持续的变革主人翁精神。采用自上而下的方法来开发共同的价值观、流程、体系、工作方式和技能，共同加快实现业务成果，打破职能孤岛。将创新工作与客户体验紧密联系起来。认可并奖励那些不断采用云和做出创新的人员。

治理视角：控制和监督

治理视角专注于协调云计划，最大限度地提高组织收益并最大限度地降低与转型相关的风险。它包含七项功能，如下图所示。常见的利益攸关方包括首席转型官、CIO、CTO、CFO、CDO 和 CRO。



AWS CAF 治理视角功能

- 计划和项目管理 – 以灵活、协调的方式交付相互依赖的云计划。复杂的跨职能云转型计划需要谨慎地协调，尤其是在组织结构更为传统的企业中。项目管理尤为重要，因为其中的许多相互依赖关系只有在交付过程中才会凸显出来。针对优化或整合的成本、时间安排、工作量和收益来协调多个计划，从而管理相互依赖关系。

  定期与业务赞助商一起验证您的路线图，并及时将任何问题上报给高级领导层，以推动问责制和提高透明度。相反，采用敏捷方法来最大限度地减少做出深远预测的需求，这样您可以从经验中学习并随着转型历程的不断深入做出调整。您可以合理地安排积压工作的优先次序，并以蓝图和案例的形式整理您的工作，从容应对变革。
- 收益管理 – 确保实现和维持与云投资相关的商业利益。转型的成功与否取决于最终获得的商业利益。提前明确预期收益可让您确定云投资的优先次序，并跟踪一段时间内的转型进度。确定指标，量化预期收益，并与相关的利益攸关方进行沟通。使收益的时间和生命周期与您的战略目标保持一致。将收益交付纳入到收益实现路线图中。定期衡量已实现的收益，根据收益实现路线图评估进度，并根据需要调整预期收益。
- 风险管理 – 利用云降低风险状况。识别和量化与基础设施可用性、可靠性、性能和安全性相关的运营风险，以及与声誉、业务连续性和快速响应不断变化的市场状况的能力相关的业务风险。了解云如何帮助您降低风险状况，并继续按照您的敏捷节奏以迭代方式识别和管理风险。考虑利用云来降低与基础设施运营和故障相关的风险。减少对大量前期基础设施支出的需求，同时降低购买可能不再需要的资产的风险。根据用户的需求，利用云即时预置和取消预置资源，降低采购计划风险。

- 云财务管理 – 规划、衡量和优化云支出。将云提供的资源预置简便性和敏捷性益处与团队的云支出财务责任结合起来。这有助于确保您的团队持续优化云工作负载，并使用最佳定价模式。明确与云相关的财务角色和责任，并确保金融、商业和技术型企业中的主要利益攸关方就云成本达成共识。发展到更加动态的预测和预算编制流程，更快地识别成本差异和异常情况。

  调整您的账户结构和标记策略，让它们适应您的企业和产品与云相对应的方式。构建账户和成本分配标签，将云资源与特定的团队、项目和商业计划相对应，并获得消费模式的精细视图。定义成本类别以使用自定义规则来整理成本和使用情况信息，从而简化计量制或收费制。使用整合账单可帮助简化云账单并获取批量折扣。构建防护机制，以可扩展的方式管理云使用情况，并将对敏捷性的影响降至最低。

  为避免产生技术负担，请确保您的工作负载符合架构完善原则，并以最具成本效益的方式运行。利用基于需求和基于时间的动态预置，只需为所需的资源付费。通过识别和消除与闲置或未充分利用的云资源相关的支出，降低云成本。

  集中管理本地部署和云软件许可证，以削减与许可证相关的成本超支，减少不合规情况并避免误报。区分云资源附带的许可证和您拥有的许可证。利用对许可证使用的基于规则的控制，为新的和现有的云部署设置硬性或软性限制。使用控制面板显示许可证使用情况，并加快供应商审计速度。提供有关不合规情况的实时提示。

- 应用程序组合管理 – 管理和优化应用程序组合以支持您的业务策略。应用程序为业务功能提供支持，并将它们关联到相关资源。准确而完整的应用程序清单可以帮助您发现合理化、迁移和现代化的机会。有效的应用程序组合管理功能将帮助您最大限度地减少应用程序蔓延，促进应用程序生命周期规划，并确保持续与云转型策略保持一致。

  从最关键的应用程序开始，根据总体业务功能来定义它们，然后将它们与基础软件产品和相关资源相对应。通过从相关企业系统（例如企业架构、IT 服务管理 (ITSM) 以及项目和项目组合管理）中获取数据，全面了解每种应用程序。确定关键技术和业务利益攸关方（包括应用程序负责人），并要求他们定期扩充和验证应用程序元数据。定期评估应用程序组合的运行状况，以最大限度地增加企业从其应用程序投资中获得的价值。

- 数据治理 – 对数据行使权力和控制，以满足利益攸关方的期望。您的业务流程和分析功能取决于准确、完整、及时和相关的数据。定义和分配关键角色，包括数据拥有者、管理员和保管人。考虑采用联合（数据网格）方法来进行治理。指定各种标准，包括数据字典、分类法和业务词汇表。确定需要参考的数据集，并对各个参考数据实体之间的关系进行建模。

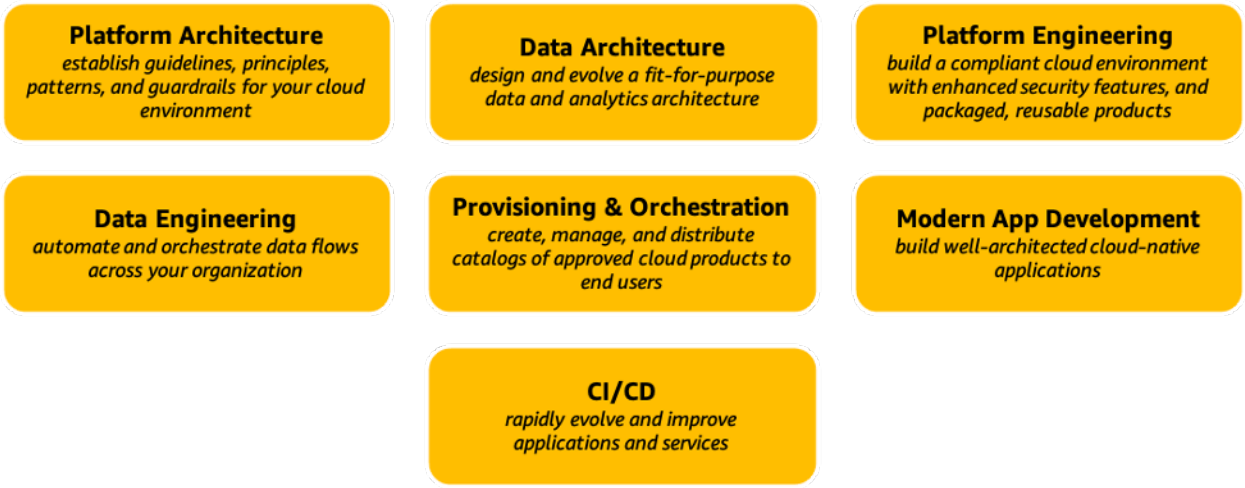
  制定数据生命周期策略，并持续实施合规性监控。根据您的战略和运营数据需求，确定数据质量工作的优先次序。制定数据质量标准：确定关键质量属性、业务规则、指标和目标。监控数据价值链中每一步的数据质量。确定数据质量问题的根本原因，从源头改进相关流程。为关键数据产品实施数据质量控制面板。

- 数据整理 – 收集、整理、访问和扩充元数据，并使用元数据来整理数据目录中的数据产品清单。数据目录可以帮助数据使用者快速找到相关数据产品并了解其上下文（例如来源和质量），从而推动数据货币化和自助式分析。

  确定负责审核数据目录的主要策划人。根据您的数据货币化策略，为关键数据产品（包括结构化和非结构化数据）编写目录。识别并捕获相关的技术和业务元数据，包括沿袭。利用标准本体论、业务词汇表和自动化（包括机器学习）为数据贴标签、编制索引和自动分类。必要时增加手动标记，并适当地处理任何个人身份信息 (PII)。考虑通过社交策划来实现数据众包。换句话说，考虑向数据使用者授予对数据产品进行评级和审查以及添加注释的权利。

平台视角：基础设施和应用程序

平台 视角专注于通过企业级、可扩展的混合云环境来加快云工作负载的交付。它包含七项功能，如下图所示。常见的利益攸关方包括 CTO、技术负责人、架构师和工程师。



AWS CAF 平台视角功能

- 平台架构 – 建立和维护云环境的指导方针、原则、模式和防护机制。架构完善的云环境将帮助您加快实施、降低风险并推动云采用。在企业内部就企业标准达成共识，推动云的采用。定义最佳实践蓝图和防护机制，以促进身份验证、安全、联网以及日志记录和监控。考虑因延迟、数据处理或数据驻留要求，可能需要在本地保留哪些工作负载。评估混合云使用案例，如云爆发、云备份和灾难恢复、分布式数据处理和边缘计算。
- 数据架构 – 设计并发展适用的数据和分析架构。精心设计的数据和分析架构可以帮助您降低复杂性、成本和技术负担，并让您能够从呈指数增长的数据量中获得切实可行的洞察。采用分层的模块化架构，使您能够使用正确的工具来完成正确的工作，并以迭代和增量方式改进您的架构以满足新出现的要求和使用场景。

  根据您的要求，为每个架构层（包括摄取、存储、编目、处理和使用）选择关键技术。要简化日常管理工作，可以考虑采用无服务器技术。专注于支持实时数据处理，并考虑采用智能湖仓架构来促进数据湖与专用数据存储之间的数据移动。
- 平台工程 – 构建一个合规的多账户云环境，该环境可提供增强的安全功能以及打包的可重用云产品。利用有效的云环境，您的团队将能够轻松地预置新账户，并确保这些账户符合组织策略。一组精选云产品将使您能够编写最佳实践，帮助您进行治理，同时提高云部署的速度和一致性。部署最佳实践蓝图以及检测性和预防性防护机制。将云环境与现有生态系统集成，以实现所需的混合云使用场景。

自动执行账户预置工作流，并利用多个账户来支持您的安全和治理目标。在本地部署环境与云环境之间以及不同的云账户之间建立连接。在现有身份提供商 (IdP) 与云环境之间实施联合身份验证，以便用户能使用现有登录凭证进行身份验证。集中化日志记录，建立跨账户的安全审计，创建入站和出站域名系统 (DNS) 解析器，并获得对账户和防护机制的控制面板可见性。

根据企业标准和配置管理，评估和认证可使用的云服务。对企业标准进行打包和不断改进，使其成为可自助部署的产品和可供消费的服务。利用基础设施即代码 (IaC) 以声明方式定义配置。

- 数据工程 – 自动执行和编排企业内的数据流。自动化的数据与分析平台和管道可帮助您提高生产力并加快产品上市。组建跨职能的数据工程团队，这些团队涵盖基础设施和运营、软件工程以及数据管理领域。利用元数据来自动实施使用原始数据并生成优化数据的管道。实施相关的架构防护机制和安全控制措施以及监控、记录和警报，从而帮助修复管道故障。确定常见的数据集成模式并构建可重用的蓝图，从而消除管道开发的复杂性。与业务分析师和数据科学家共享蓝图，以便他们能够使用自助服务方法进行操作。
- 预置和编排 – 创建和管理已批准的云产品目录，并分发给终端用户。随着企业的发展，以可扩展和可重复的方式保持一致的基础设施预置变得更加复杂。简化的预置和编排可帮助您实现一致性管理并满足合规性要求，同时仅允许用户快速部署已批准的云产品。设计和实施集中管理的自助服务门户，以便发布、分发、浏览和使用已批准的云产品。使您的云产品能够通过 API 和个性化门户网站进行访问。与您的 IT 服务管理 (ITSM) 工具集成，并自动执行对配置管理数据库 (CMDB) 的任何更新。
- 现代化应用程序开发 – 构建架构完善的云原生应用程序。现代化应用程序开发实践可帮助您实现创新带来的速度和敏捷性。使用容器和无服务器技术可帮助您提高资源利用率，并自动从零需求扩展到峰值需求。考虑利用事件驱动型架构将应用程序构建为独立的微服务，从而对应用程序进行解耦。在应用程序开发生命周期的所有层和每个阶段实施安全性。

  自动执行横向扩展和缩减的过程或使用无服务器技术。对现有应用程序进行现代化，以降低成本、提高效率并充分利用现有投资。考虑重新搭建平台（将自己的容器、数据库或消息代理迁移到托管式云服务）和重构（将旧式应用程序重写为云原生架构）。确保您的架构考虑了 Service Quotas 和物理资源，这样它们就不会对工作负载性能或可靠性产生负面影响。
- 持续集成和持续交付 – 与使用传统软件开发和基础设施管理流程的企业相比，以更快的速度发展和改进应用程序和服务。采用 DevOps 实践以及持续集成、测试和部署，将帮助您提高敏捷性，从而更快地进行创新，更好地适应不断变化的市场，并更高效地推动业务成果。实施持续集成和持续交付 (CI/CD) 管道。

  从持续集成的最小可行管道开始，然后过渡到包含更多组件和阶段的持续交付管道。鼓励开发人员尽早创建单元测试，并在将代码推送到中央存储库之前运行这些测试。在持续交付管道中包括暂存和生产步骤，并考虑生产部署的手动批准。考虑多种部署策略，包括就地部署、滚动部署、不可改变部署和蓝/绿部署。

安全视角：合规性和保证

安全 视角可帮助您实现数据和云工作负载的机密性、完整性和可用性。它包含九项功能，如下图所示。常见的利益攸关方包括 CISO、CCO、内部审计主管以及安全架构师和工程师。

AWS CAF 安全视角功能

- 安全治理 – 制定、维护并有效地传达安全角色、职责、问责制、策略、流程和程序。确保明确的问责范围对于安全计划的有效性至关重要。了解适用于您所在行业和/或企业的资产、安全风险和合规性要求，这能够帮助您确定安全工作的优先次序。提供持续的指导和建议，让您的团队更快地行动，从而加速转型。

  了解您在云中安全性方面承担的责任。对相关利益攸关方、资产和信息交换进行清理和分类，并设定优先次序。确定适用于您的行业和/或企业的法律、法规、条例和标准/框架。对您的企业进行年度风险评估。风险评估可帮助确定给企业带来影响的已识别风险和/或漏洞的可能性和影响。为确定的安全角色和职责分配足够的资源。根据您的合规性要求和组织风险承受能力制定安全策略、流程、程序和控制措施；根据不断变化的风险和要求不断地更新。

- 安全保障 – 持续监控、评估、管理和提高安全和隐私计划的有效性。您的企业和您所服务的客户需要相信您已实施控制措施，能够满足监管要求，并根据您的业务目标和风险承受能力有效地管理安全和隐私风险。

  将控制措施记载到一个全面的控制框架中，并制定满足这些目标的可证明的安全和隐私控制措施。查看云供应商获得的审计报告、合规性认证或证明，以帮助您了解他们已实施的控制措施、如何验证这些控制措施以及扩展 IT 环境中的控制措施是如何有效实施的。

持续监控和评估您的环境，以验证控制措施的实施有效性，并证明符合法规和行业标准。审查安全策略、流程、程序、控制措施和记录，并根据需要采访关键人员。

- 身份和权限管理 – 大规模管理身份和权限。您可以在 AWS 中创建身份或连接身份源，然后向用户授予必要的权限，以便他们能够登录、访问、预置或编排 AWS 资源和集成式应用程序。有效的身份和访问管理可帮助验证适当的人员和计算机是否能够在适当的条件下访问正确的资源。

  AWS Well-Architected Framework 描述了相关概念、设计原则和架构最佳实践以管理身份。其中包括：依赖集中式身份提供商；利用用于进行大规模精细访问的用户组和属性以及临时凭证；以及使用强大的登录机制，例如多重身份验证 (MFA)。要控制人员和计算机身份对 AWS 及您的工作负载的访问，可在特定条件下对特定资源设置特定服务操作的权限；使用最低权限原则，设置权限边界，并使用服务控制策略，以便随着环境发展和用户群的扩大，正确的实体能够访问正确的资源；基于属性 (ABAC) 授予权限，以便您的策略可以扩展；并不断验证您的策略是否提供了所需的保护。

- 威胁检测 – 了解并识别潜在的安全配置错误、威胁或意外行为。更好地了解安全威胁将使您能够确定保护性控制措施的优先级。有效的威胁检测可让您更快地响应威胁并从安全事件中学习。在战术、运营和战略情报目标和总体方法上达成一致。挖掘相关数据源，处理和分析数据，传播和实施洞察。

  在环境中无死角地部署监控以收集基本信息，并在临时位置部署监控以跟踪特定类型的事务。使来自多个事件源（包括网络流量、操作系统、应用程序、数据库和端点设备）的监控数据相关联，以提供稳健的安保状况并增强可见性。考虑利用欺骗技术（例如 honeypots）来了解未经授权的用户行为模式。

- 漏洞管理 – 持续标识、分类、修复和缓解安全漏洞。更改现有系统或添加新系统也可能会引入漏洞。定期扫描漏洞，帮助防御新的威胁。使用漏洞扫描程序和端点代理将系统与已知漏洞关联起来。根据漏洞风险确定补救措施的优先级。采取补救措施并向相关发利益攸关方报告。利用红队测试和渗透测试来识别系统架构中的漏洞；根据需要向您的云提供商寻求事先授权。

- 基础设施保护 – 验证您的工作负载中的系统和服务是否受到保护，防止意外和未经授权的访问以及潜在的漏洞对其造成危害。保护您的基础设施，使其免受意外和未经授权的访问以及潜在漏洞的侵害，这将有助于您改善云中的安保状况。利用深度防御，分层放置一系列旨在保护数据和系统的防御机制。

  创建网络层，将不需要 Internet 访问权限的工作负载放置在私有子网中。使用安全组、网络访问控制列表和网络防火墙来控制流量。根据系统和数据的值对它们应用零信任。利用 Virtual Private Cloud (VPC) 端点建立与云资源的私有连接。检查和过滤每层的流量；例如，通过 Web 应用程序防火墙和/或网络防火墙。使用经过强化的操作系统映像，并在本地和边缘对任何混合云基础设施进行物理保护。

- 数据保护 – 了解和控制数据以及数据在企业中的访问和使用方式。保护您的数据，使数据不会受到意外和未经授权的访问，也不会出现潜在的漏洞，这是安全计划的主要目标之一。为了帮助您确定适

当的保护和保留控制措施，请根据重要性和敏感性对数据进行分类（例如，个人身份信息）。确立数据保护控制措施和生命周期管理策略。对所有静态数据和传输中的数据进行加密，并将敏感数据存储在单独的账户中。使用机器学习自动发现、分类和保护敏感数据。

- 应用程序安全 – 在软件开发过程中检测和修复安全漏洞。在应用程序的代码编写阶段发现并修复安全漏洞可以节省时间、工作量和成本，并且在投入生产时对自己的安保状况充满信心。扫描和修补您的代码和依赖项中的漏洞，以帮助防御新的威胁。通过在整个开发和运营流程和工具中自动执行与安全相关的任务，最大限度地减少人为干预的需求。使用静态代码分析工具来识别常见的安全问题。
- 事件响应 – 通过有效地响应安全事件来减少潜在危害。快速、有效且一致地响应安全事件将帮助您减少潜在危害。培训您的安全运营和事件响应团队，使他们了解云技术以及您的企业如何使用这些技术。制作运维手册并创建事件响应机制库。包括关键利益攸关方，让他们更好地了解您的选择对更广泛的企业产生的影响。

  通过桌面练习和实际演练，模拟安全事件并练习事件响应。迭代您的模拟结果，以提高您的响应能力、缩短价值实现时间并进一步降低风险。利用标准化的机制来识别和解决根本原因，进行事后分析，从安全事件中汲取经验教训。

运营视角：运行状况和可用性

运营 视角专注于确保在与业务利益攸关方议定的级别交付云服务。自动化和优化运营将使您能够有效地进行扩展，同时提高工作负载的可靠性。此视角包含九项功能，如下图所示。常见的利益攸关方包括基础设施和运营负责人、站点可靠性工程师和信息技术服务经理。

AWS CAF 运营视角功能

- 可观测性 – 从基础设施和应用程序数据获得切实可行的洞察。当您以云的速度和规模运营时，您需要能够在问题出现时指出问题（理想的情况是，在问题导致客户体验中断之前指出问题）。开发必要的遥测（日志、指标和跟踪），以了解工作负载的内部状态和运行状况。监控应用程序端点，评估对终端用户的影响，并在测量值超过阈值时生成提示。

  可使用合成监控创建 Canary（按计划运行的可配置脚本）来监控端点和 API。实施跟踪功能，以便在请求遍历整个应用程序时对其进行跟踪，并确定瓶颈或性能问题。使用指标和日志获得有关资源、服务器、数据库和网络的洞察。设置时间序列数据的实时分析，了解性能影响的原因。将数据集中到单一控制面板，为您提供有关工作负载及其性能的关键信息的统一视图。
- 事件管理 (AIOps) – 检测事件，评估事件的潜在影响，并确定适当的控制措施。能够过滤噪音、关注优先事件、预测即将发生的资源耗尽、自动生成提示和事件并确定可能的原因和补救措施，将有助于您改进事件检测和缩短响应时间。建立事件存储模式并利用机器学习 (AIOps) 来自动执行事件关联、异常检测和因果关系确定。与云服务和第三方工具（包括事件管理系统和流程）集成。自动响应事件以便减少由手动流程引起的错误，并确保响应及时且一致。
- 事件和问题管理 – 快速恢复服务运营并将不良业务影响降至最低。随着云的采用，可实现服务问题和应用程序运行状况问题的响应流程的高度自动化，从而增加服务正常运行时间。随着您转向更加分

散的运营模式，简化相关团队、工具和流程之间的交互将有助于您加快解决关键和/或复杂事件。在运维手册中定义上报路径，包括触发上报的事件和上报程序。

练习事件响应实际演练，并将汲取的经验教训纳入运维手册。标识事件模式以确定问题和纠正措施。利用 Chatbot 和协作工具将运营团队、工具和工作流联系起来。利用完善的事件后分析来确定造成事件的因素并制定相应的行动计划。

- 变更和发布管理 – 引入和修改工作负载，并最大限度地降低生产环境面临的风险。传统的发布管理是一个复杂的过程，部署速度慢且难以回滚。通过采用云，可以利用 CI/CD 技术快速管理发布和回滚。建立变更流程，实现与云的敏捷性保持一致的自动化审批工作流。使用部署管理系统来跟踪并实施更改。频繁进行可逆的小规模更改可以缩小变更的范围。在所有生命周期阶段测试更改并验证结果，最大限度地减小部署失败的风险和影响。在没有达到预期时自动回滚到之前的已知良好状态，尽可能缩短恢复时间，并减少手动过程引起的错误。
- 性能和容量管理 – 监控工作负载性能并确保容量满足当前和未来的需求。尽管云的容量实际上是无限的，但可以借助 Service Quotas、容量预留和资源约束来限制工作负载的实际容量。需要理解并有效管理此类容量限制。确定主要利益攸关方，并就目标、范围和指标达成一致。收集和处理性能数据，并根据目标定期审查和报告性能。定期评估新技术以提高性能，并根据需要提出目标和指标更改建议。监控工作负载的利用率，制定基准以便将来比较，并根据需要确定阈值以扩展容量。分析一段时间内的需求，确保容量可满足季节性趋势和波动的运营条件。
- 配置管理 – 保留所有云工作负载、它们之间的关系以及一段时间内的配置更改的完整准确的记录。除非得到有效管理，否则云资源预置的动态和虚拟特性可能会导致出现配置偏差。定义并实施标记架构，将您的业务属性叠加到云使用情况，并利用标签按技术、业务和安全维度整理资源。指定强制性标签，并通过策略实施合规性。利用基础设施即代码 (IaC) 和配置管理工具进行资源预置和生命周期管理。制定配置基准并通过版本控制予以维护。
- 补丁管理 – 系统地分发和应用软件更新。软件更新可以修复新出现的安全漏洞、纠正错误并引入新功能。系统化的补丁管理方法将确保您受益于最新的更新，同时最大限度地减少生产环境面临的风险。在指定的维护时段内应用重要更新，并尽快应用关键安全更新。提前告知用户即将发布的更新的详细信息，并允许他们在有其他缓解控制措施可用时延迟修补。在投入生产环境之前，更新您的机器映像并测试补丁。为确保修补期间的持续可用性，请考虑为每个可用区 (AZ) 和环境设立单独的维护时段。定期审查补丁合规性，并提示不合规团队应用所需的更新。
- 可用性和连续性管理 – 确保业务关键型信息、应用程序和服务的可用性。在构建支持云的备份解决方案时，需要仔细考虑现有的技术投资、恢复目标和可用资源。在发生灾难和安全事件后，及时恢复将有助于保持系统可用性和业务连续性。根据确立的时间表备份您的数据和文档。

  制定灾难恢复计划，将它作为业务连续性计划的一部分。确定每个工作负载的不同灾难场景的威胁、风险、影响和成本，并相应地指定恢复时间目标 (RTO) 和恢复点目标 (RPO)。利用多可用区或多区

域架构实施所选灾难恢复策略。考虑利用混沌工程来提高受控实验的弹性和性能。定期审查和测试您的计划，并根据汲取的经验教训调整您的方法。

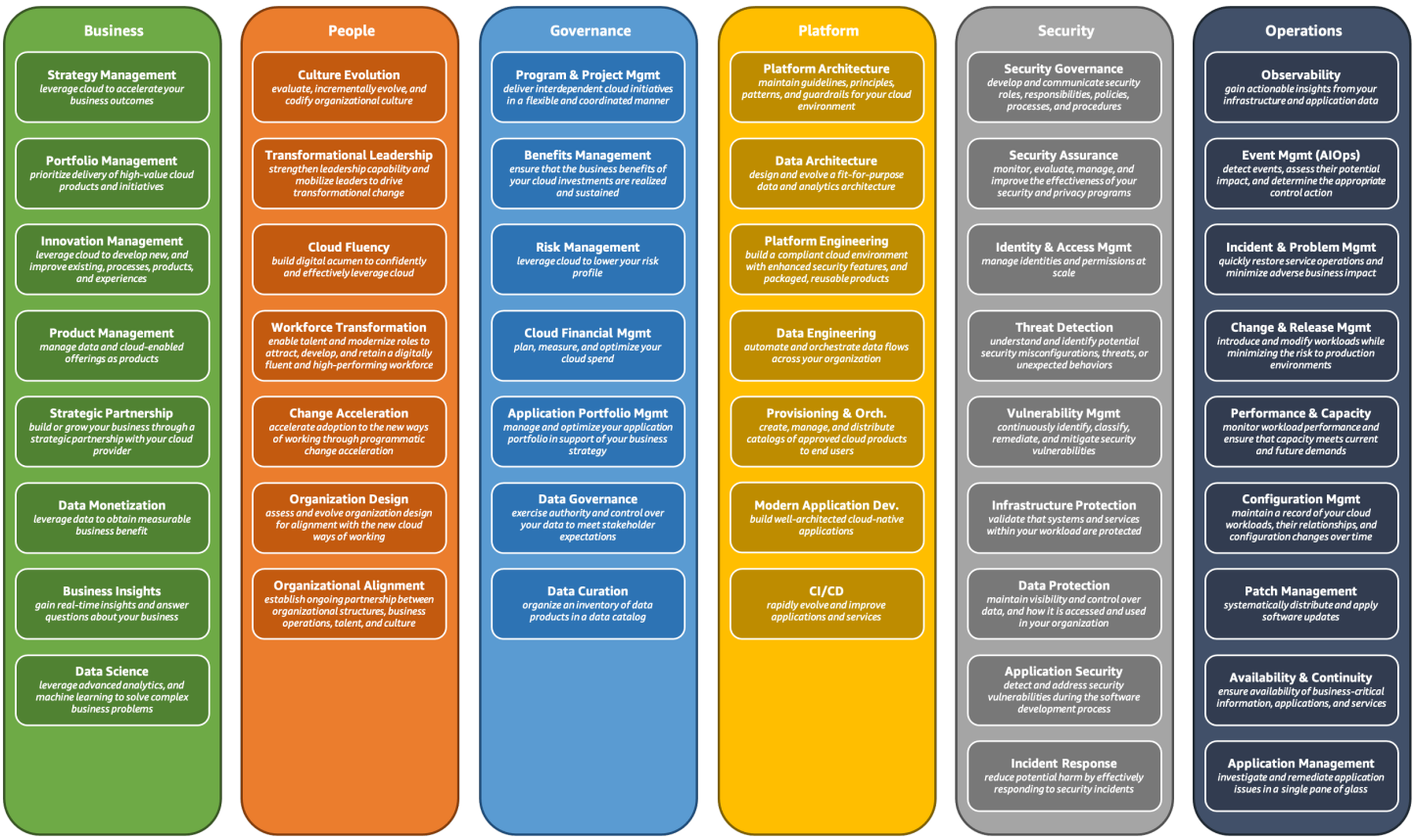
- 应用程序管理 – 在单个管理控制台中调查和修复应用程序问题。通过将应用程序数据聚合到单个管理控制台中，可以减少在不同的管理工具之间切换上下文的需求，从而简化运营监督并加快修复应用程序问题。

  与其他运营和管理系统（例如应用程序组合管理和 CMDB）集成，自动发现应用程序组件和资源，并将应用程序数据整合到单个管理控制台中。包括软件组件和基础设施资源，并描述不同的环境，例如开发、暂存和生产环境。要更快、更一致地修复运营问题，可以考虑自动执行运维手册工作流程。

总结

随着技术创新的不断加速，持续数字化转型的需求将变得更加迫切。AWS CAF 采用了 AWS 的经验和最佳实践，帮助您通过以创新方式使用 AWS 来加快获得业务成果。使用 AWS CAF 识别转型机会并确定其优先级，评估和改善云就绪情况，并以迭代方式逐步演变转型路线图。

附录：AWS CAF 功能海报



AWS CAF 基础功能

贡献者

- 由AWS CAF 全球主管 Saša Baškarada 博士撰写，并融合了众多 AWS 主题专家的意见。

延伸阅读

有关其他信息，请参阅：

- AWS 架构中心
- AWS 案例研究
- AWS 一般参考
- AWS 词汇表
- AWS 知识中心
- AWS 规范指引
- AWS 快速入门
- AWS 安全性文档
- AWS 解决方案库
- AWS 培训与认证
- AWS Well-Architected
- AWS 白皮书和指南
- AWS 入门
- Amazon Web Services 概览

文档修订

要获得有关此白皮书的更新通知，请订阅 RSS 源。

更新-历史记录-更改	更新-历史记录-描述	更新-历史记录-日期
第三次发布	更新并扩展了功能。增加了转型领域和历程阶段。	2021 年 11 月 22 日
第二次发布	对观点和能力进行了结构性更改。	2017 年 2 月 1 日
初次发布	白皮书首次发布。	2015 年 2 月 1 日

声明

客户负责对本文档中的信息进行独立评估判断。本文档：(a) 仅供参考；(b) 代表当前提供的 AWS 产品和实践，如有更改，恕不另行通知；并且 (c) AWS 及其附属机构、供应商或许可方不做任何承诺或保证。AWS 产品或服务“按原样”提供，不提供任何形式的保证、陈述或条件，无论是明示还是暗示。AWS 对其客户的责任和义务由 AWS 协议决定，本文档与 AWS 和客户之间签订的任何协议无关，亦不影响任何此类协议。

© 2021 Amazon Web Services, Inc. 或其联属公司。保留所有权利。