CMC Open MSP

Technical Kits

Nov 2020

MỤC LỤC

Tự đánh giá	Hoàn thành **Checklist Tự đánh giá** Các Đối tác MSP được khuyến cáo rà soát và điền checklist với Kiến trúc sư Giải pháp hoặc chuyên gia cụ thể có năng lực chuyên môn Kĩ thuật cao trước khi gửi cho CMC để đảm bảo các thông tin hướng dẫn được hiểu chính xác
Đánh giá toàn diện	Sau khi hoàn thành **Checklist Tự đánh giá**, Đội ngũ CMC Open MSP sẽ xem xét, rà soát lại các thông tin đã nhận được và sẽ liên hệ với bạn để lên lịch thảo luận và thực hiện xác nhận đánh giá.

1 Quy trình & Thời gian Đánh giá

- Sau khi **Đánh giá toàn diện** diễn ra, Đối tác sẽ nhận được bản tóm tắt các câu hỏi làm rõ (trong vòng 5 ngày làm việc) từ CMC nêu chi tiết về thắc mắc hoặc yêu cầu các thông tin cung cấp cụ thể. Các tóm tắt đánh giá từ CMC sẽ được cung cấp đi kèm.
- Đối tác có 7 ngày làm việc kể từ khi nhận được tóm tắt đánh giá để phản hồi và cung cấp lại những thông tin theo yêu cầu
- CMC Và Đối tác sẽ thiết lập những buổi họp chính thức để thảo luận (nếu cần) với các hạng mục trong checklist này
- Đối tác sẽ gửi kết quả **Tự đánh giá** cuối cùng cho CMC sau 7 ngày làm việc sau buổi thảo luận/trao đổi cuối cùng
- Quyết định cuối cùng về kết quả hợp tác sẽ được CMC thông báo trong vòng 15 ngày sau khi CMC Cloud nhận được báo cáo tự đánh giá cuối cùng

2 Phản hồi của Đối tác

Phản hồi các tiêu chí từ Đối tác là phần thiết yếu trong quá trình tự đánh giá của Đối tác và Đánh giá toàn diện của CMC. Độ phủ đáp ứng là phương thức khách quan và định lượng được để đánh giá năng lực của Đối tác và định hướng rõ ràng được các cơ hội hợp tác cho hai bên.

Với những tiêu chí được tự đánh giá là đáp ứng CMC sẽ yêu cầu Đối tác thêm thông tin chi tiết, bằng chứng và thực hiện xác nhận.

Gồm có hai loại tiêu chí:

Tiêu chí bắt buộc	Các tiêu chí tiên quyết và bắt buộc cần chuẩn bị để tham gia chương trình Open MSP của CMC
Tiêu chí khuyến nghị	Các tiêu chí mong muốn, khuyến nghị thêm để CMC hiểu rõ về tiềm lực của Đối tác và thực hiện đánh giá chính xác hơn

3 Open MSP Technical Checklist

		Tiêu chí	Đáp ứng	Không đáp ứng
3.1 Khả năng thiết kế giải pháp				
Khả năng giải pháp	Đối tác chứng minh rằng trong quá trình cung cấp dịch vụ cho khách hàng, Các tài liệu thiết kế chi tiết hoàn chỉnh sẽ được cung cấp để khách hàng yên tâm về năng lực hỗ trợ, kiến trúc kỹ thuật tốt và tối ưu quy trình hoạt động được lâu dài. Chứng minh với 3 tài liệu thiết kế chi tiết về hệ thống khách hàng đã từng thực hiện bao gồm:			
	1.1 Tài liệu về các yêu cầu của khách hàng.	✅		
	1.2 Chi tiết kiến trúc của thiết kế đề xuất.	✅		
	1.3 Chi tiết về hiệu suất hệ thống, quản lý năng lực và hệ thống đo lường tính sẵn sàng được cung cấp để đo lường mức độ thành công của thiết kế đề xuất.	✅		
	1.4 Đánh giá các yêu cầu và quy trình bảo mật của khách hàng để xác định lỗ hổng.	❌		
	1.5 Thiết kế chi tiết thể hiện cơ sở hạ tầng của khách hàng được kiến trúc tốt theo Khung kiến trúc tốt của CMC	✅		
3.2 DevOps				
Hỗ trợ DevOps	DevOps đại diện cho sự thay đổi văn hóa nhằm khuyến khích cộng tác để cung cấp phần mềm nhanh hơn với mức độ tin cậy cao. Đối tác tương tác với khách hàng để hỗ trợ việc chuyển đổi công nghệ và kinh doanh DevOps và / hoặc hỗ trợ nhu cầu DevOps hiện tại của khách hàng. Đối tác nên xem xét các điểm tích hợp Cloud sau để hỗ trợ DevOps trên CMC Cloud:			
	• Khách hàng sẽ tận dụng quy trình hoặc phương pháp luận phát hành (release) và triển khai phần mềm nào? • Làm cách nào để khách hàng giữ an toàn cho mã (code) và các ứng dụng bao gồm cả quản lý thông tin xác thực truy cập? • Bằng chứng phải ở dạng minh họa về cách Đối tác khảo sát và hỗ trợ quản lý triển khai và phát	✅		

	hành ứng dụng của khách hàng và 1 ví dụ về khách hàng.			
3.3 Khả năng di chuyển ứng dụng và cơ sở hạ tầng				
3.3.1 Khả năng di chuyển cơ sở hạ tầng Cloud	Khách hàng khi lựa chọn nhà cung cấp luôn quan tâm về hạng mục dịch vụ di chuyển hạ tầng Cloud, với các lĩnh vực chuyên môn cụ thể (ví dụ: Dữ liệu lớn). Đối tác cần cung cấp cho khách hàng kiến trúc cơ sở hạ tầng phù hợp với các phương án của CMC Cloud. Bằng chứng phải ở định dạng thiết kế và sơ đồ kiến trúc Cloud cho khách hàng đã triển khai, bao gồm lý do cho bất kỳ phần nào của thiết kế không được kiến trúc tốt. Thông tin kiến trúc này phải bao gồm tất cả các thành phần và dịch vụ Cloud được triển khai, cũng như các yêu cầu thiết kế, giả định và các thành phần chức năng và cơ chế tương tác của chúng.	✅		
3.3.2 Khả năng di chuyển ứng dụng	Đối tác chứng minh khả năng di chuyển ứng dụng bằng cung cấp công cụ hoặc kiến trúc triển khai tóm tắt việc triển khai ứng dụng từ triển khai cơ sở hạ tầng. Điều này cho phép khách hàng độc lập hoặc kết hợp với dịch vụ được quản lý - triển khai và cấu hình các ứng dụng của họ. Bằng chứng phải ở dạng một kiến trúc khách hàng đã thực hiện và các khuyến nghị tương ứng, kèm theo giải thích cụ thể về kịch bản khách hàng đã được phát triển.	✅		
3.4 Bảo mật				
Đối với các mục trong phần này, Đối tác phải sử dụng môi trường thử nghiệm hoặc “Sandbox” ở mức tối đa có thể.				
3.4.1 Quản lý bảo mật	3.4.1.1 Đối tác thiết lập các chính sách và quy trình bảo mật để bảo vệ hệ thống của mình khỏi các cuộc tấn công và các chính sách này đã được ban quản lý nội bộ của Đối tác xem xét và phê duyệt. Bằng chứng về các chính sách và thủ tục bảo mật cũng có thể ở dạng chứng nhận hiện hành liên quan đến an toàn thông tin (ví dụ: ISO 27001, SOC2) hoặc bằng chứng về bảo mật cơ sở hạ tầng và các quy trình quản lý thông tin và các phê duyệt liên quan.	✅		
	3.4.1.2 Đối tác có một hệ thống cung cấp quyền truy cập vào tài nguyên khách hàng cho các kỹ sư của mình dựa trên nguyên tắc đặc quyền tối thiểu. Đã có quy trình để xác định và duy trì mức độ truy cập thích hợp. Quyền truy cập vào dữ liệu quan trọng hoặc	✅		

	nhạy cảm (do khách hàng xác định) được kiểm soát thêm bằng xác thực đa yếu tố hoặc số lượng với các cảnh báo dựa trên quyền truy cập. Bằng chứng phải ở dạng minh chứng trực tiếp về các khả năng và quy trình nội bộ để duy trì các chính sách truy cập đặc quyền ít nhất trong phạm vi thực hành dịch vụ được quản lý trên Cloud			
	3.4.1.3 Đối tác có các chính sách và quy trình bảo mật để bảo vệ hệ thống của khách hàng khỏi sự truy cập trái phép từ những người dùng đã xác thực. Bằng chứng có thể ở dạng chứng nhận ngành liên quan đến quản lý an toàn thông tin (ví dụ: ISO 27001) dành riêng cho môi trường khách hàng hoặc tài liệu về các chính sách và thủ tục của Đối tác	✅		
	3.4.1.4 Đối tác không truy cập tài khoản Cloud bằng cách sử dụng thông tin đăng nhập tài khoản gốc (root account). Bằng chứng phải ở dạng trình diễn công nghệ và tài liệu về các chính sách áp dụng.	✅		
	3.4.1.5 Đối tác có Chiến lược Quản lý Truy cập được lập thành văn bản, bao gồm nhưng không giới hạn: Quản lý danh tính và truy cập người dùng (Identity and Access Management - IAM), các vai trò liên kết/chia sẻ. Bằng chứng phải ở dạng biểu diễn công nghệ và tài liệu quy trình giải quyết vấn đề ở trên và một ví dụ về khách hàng thuộc phạm vi thực hành dịch vụ được quản lý trên CMC Cloud của Đối tác.	✅		
	3.4.1.6 Đối tác truy cập tài khoản Cloud thông qua việc sử dụng các vai trò được liên kết để truy cập Cloud Console hoặc cấp thông tin xác thực tạm thời, trái ngược với việc cấp phép cho từng nhóm và người dùng IAM. Bằng chứng phải ở dạng biểu diễn công nghệ.	❌		
	3.4.1.7 Đối tác sử dụng xác thực đa yếu tố (MFA) để bảo vệ tài khoản khách hàng cho tất cả các phương pháp truy cập tài khoản khách hàng đó của người dùng tương tác, theo mặc định.	✅		
	3.4.1.8 Đối tác cung cấp mã hóa ở các dịch vụ cho cơ sở hạ tầng CMC Cloud Bằng chứng phải ở dạng tài liệu thiết kế chỉ rõ việc sử dụng mã hóa tại các dịch vụ.	✅		

	3.4.1.9 Đối tác đảm bảo rằng xác thực đa yếu tố được kích hoạt trên tất cả các tài khoản gốc của Đối tác và CMC Cloud của khách hàng. Đối tác phải hiển thị công nghệ làm bằng chứng rằng nó thường xuyên kiểm tra các tài khoản kích hoạt MFA và kích hoạt MFA trên các tài khoản gốc CMC Cloud	✅		
	3.4.1.10 Thông tin nhận dạng cá nhân của khách hàng được mã hóa hoàn toàn trên tất cả các hệ thống Đối tác bao gồm các portal cho đối tác, thanh toán và yêu cầu hỗ trợ. Bằng chứng phải ở dạng tài liệu của hệ thống lưu trữ thông tin khách hàng với bằng chứng mã hóa.	❌		
3.4.2 Ghi lại và lưu trữ sự kiện bảo mật	Các sự kiện bảo mật được lưu trữ trong nhật ký cho các mục đích quản lý và phân tích. Bằng chứng phải ở dạng ví dụ về Nhật ký sự kiện bảo mật (Security Event Log) của khách hàng theo kinh nghiệm	✅		
3.4.3 Tính liên tục của Dịch vụ	Đối tác có khả năng giám sát các hệ thống dịch vụ của mình để đảm bảo rằng các dịch vụ triển khai với CMC của khách hàng không bị ảnh hưởng bởi, gặp lỗi và có các quy trình hợp lý và được kiểm tra để ứng phó với sự cố. Điều này sẽ bao gồm độ phức tạp của lỗi và bao gồm quản lý thảm họa đối với dữ liệu, sự toàn vẹn của dữ liệu và mất mát hoặc thỏa hiệp cơ sở hạ tầng. Bằng chứng phải ở dạng tài liệu quy trình giải quyết các vấn đề trên, cũng như kết quả kiểm tra tính liên tục của hoạt động kinh doanh được thực hiện trong vòng 12 tháng qua. Bằng chứng bổ sung có thể ở dạng chứng nhận ngành liên quan đến quản lý tính liên tục của hoạt động kinh doanh (ví dụ: ISO 22301).	❌		
3.5 Quản lý dịch vụ				
3.5.1 Customer Service Availability	Đối tác cung cấp dịch vụ khách hàng 24x7 trên nhiều kênh giao tiếp; có thể là tổng đài thoại 24x7 hoặc dịch vụ trực tuyến 8x5 có nhân viên hỗ trợ sau giờ làm việc (ví dụ: hỗ trợ nhắn tin / cảnh báo sau giờ làm việc trên cơ sở luân phiên theo ca). Đối tác phải giải thích hoặc chỉ ra cách thức dịch vụ khách hàng được cung cấp; nếu Đối tác không duy trì một tổng đài thoại có nhân viên hoạt động 24 giờ, thì phải có các thủ tục dạng văn bản để hỗ trợ sau giờ làm việc, cuối tuần và ngày lễ.	✅		

	Bằng chứng có thể ở dạng chứng nhận ngành hiện tại liên quan đến ITSM (ITSM) (ví dụ: ISO 20000)			
3.5.2 Hệ thống yêu cầu hỗ trợ (Ticket)	Đối tác có hệ thống yêu cầu hỗ trợ ITSM có khả năng thực hiện như sau:			
	3.5.3.1 Tạo sự cố yêu cầu xử lý và báo cáo vượt cấp. Đối tác phải đưa ra bằng chứng và ví dụ các sự cố đã được tạo và báo cáo	✅		
	3.5.3.2 Ghi nhật ký ngay lập tức và thời gian của vé. Đối tác phải cung cấp bằng chứng	✅		
3.5.4 Các chỉ tiêu hỗ trợ dành riêng cho CMC	Đối tác theo dõi các trường hợp được chuyển đến bộ phận hỗ trợ CM và cung cấp các đánh giá thường xuyên với để tương tác và chia sẻ bài học kinh nghiệm, tận dụng thông tin thu được từ sự kiện đó để cải thiện kiến thức cho hai bên.	❌		
3.5.5 Giám sát và chủ động cảnh báo	Đối tác có các hệ thống, công cụ hoặc ứng dụng có khả năng giám sát hiệu suất của tất cả các dịch vụ hợp tác Giám sát chủ động tìm kiếm các mẫu cố để dự đoán các lỗi có thể xảy ra trong tương lai. (Vận hành Dịch vụ ITIL) Chức năng giám sát và cảnh báo cũng phải đi kèm với chức năng tại hệ thống hỗ trợ tương ứng để thực hiện xử lý các sự cố / cảnh báo theo SLA Các đối tác chứng minh năng lực của mình bằng: 1. **Giám sát cơ sở hạ tầng**; một số ví dụ bao gồm: • Các chỉ số đặc biệt về giám sát, cảnh báo và cấu hình tự động cho CMC Cloud • Các chỉ số tùy chỉnh để giám sát ứng dụng, cảnh báo và cấu hình tự động • Các công cụ giám sát cơ sở hạ tầng CMC Cloud của các bên thứ 3 khác 2. **Giám sát dịch vụ**; một số ví dụ bao gồm: • Các công cụ giám sát vận hành hệ thống để giám sát ở mức độ hệ điều hành (OS) • Các công cụ giám sát ứng dụng để giám sát ở mức độ ứng dụng • Các công cụ giám sát giao dịch được mô phỏng để giám sát hệ thống đầu cuối (end-to-end) Bằng chứng phải ở dạng biểu diễn công nghệ về công cụ được sử dụng để thực hiện giám sát và cảnh báo	✅		

	chủ động đối với tài nguyên của khách hàng trong CMC Cloud.			
3.5.6 Báo cáo Thông minh và Dashboard cho Khách hàng	Đối tác cung cấp cho khách hàng Dashboard và khả năng báo cáo nâng cao để giám sát thông minh. Dashboard phải cung cấp khả năng hiển thị toàn diện trong thời gian thực, đồng thời cung cấp phân tích lịch sử và xu hướng. Bằng chứng phải là ví dụ dashboard và báo cáo cho khách hàng của Đối tác hiện tại	✓		
3.5.7 Quản lý sự cố	3.5.7.1 Đối tác có tài liệu hóa các quy trình quản lý sự cố, bao gồm: • Cách xác định sự cố • Các sự cố được ghi lại như thế nào • Cách phân loại sự cố • Các sự cố được ưu tiên như thế nào • Cách các sự cố được điều tra và xác định • Các sự cố được giải quyết như thế nào • Làm thế nào các sự cố được đóng lại Sự cố là sự gián đoạn không có kế hoạch đối với một dịch vụ CNTT hoặc giảm chất lượng của một dịch vụ CNTT. Việc hỏng một mục cấu hình chưa ảnh hưởng đến dịch vụ cũng là một sự cố. Quản lý sự cố là quy trình chịu trách nhiệm quản lý vòng đời của tất cả các sự cố. Quản lý sự cố đảm bảo rằng hoạt động dịch vụ bình thường được khôi phục càng nhanh càng tốt và tác động kinh doanh được giảm thiểu. Đối tác phải cung cấp bằng chứng về quy trình quản lý sự cố bằng văn bản đáp ứng các yêu cầu trên đi kèm Ví dụ. Ngoài ra, bằng chứng có thể ở dạng chứng nhận ngành hiện tại liên quan đến ITSM (ví dụ: ISO 20000)	✓		
	3.5.7.2 Đối tác có quy trình cập nhật thông tin về sự cố. Các phương pháp, tần suất và kênh giao tiếp dựa trên SLA được xác định trước, bao hàm tác động đến hoạt động kinh doanh và / hoặc mức độ quan trọng của sự cố. Đối tác có quy trình để khách hàng được cập nhật thông tin về sự cố. Bằng chứng ở dạng quy trình tài liệu và có ví dụ cụ thể hoặc các chứng chỉ liên quan đến ITSM (ví dụ: ISO 20000)	✓		

3.5.8 Quản lý vấn đề	3.5.8.1 Đối tác có tài liệu hóa các quy trình quản lý vấn đề bao gồm các sự cố không có cách giải quyết đã biết hoặc có sẵn hoặc những sự cố được xác định chủ động dựa trên xu hướng hoạt động hoặc giám sát. Sự cố được định nghĩa là nguyên nhân của một hoặc nhiều sự cố. Nguyên nhân thường không được xác định tại thời điểm tạo hồ sơ sự cố và quy trình quản lý sự cố có trách nhiệm điều tra thêm. Quản lý vấn đề là quá trình chịu trách nhiệm quản lý vòng đời của tất cả các vấn đề. Quản lý sự cố chủ động ngăn ngừa sự cố xảy ra và giảm thiểu tác động của sự cố không thể ngăn chặn được. (Vận hành Dịch vụ ITIL) Bằng chứng phải ở dạng các ví dụ trong đó các sự cố được phát hiện hoặc được xác định chủ động dựa trên xu hướng hoạt năng/ giám sát / phân tích mẫu. Ngoài ra, bằng chứng có thể ở dạng chứng nhận ngành hiện tại liên quan đến ITSM (ví dụ: ISO 20000)	✗		
	5.7.2 Đối tác có khả năng xác định và ghi lại các nguyên nhân gốc rễ và lưu trữ trong Cơ sở dữ liệu lỗi đã biết (Known Error Database - KEDB) có thể tìm kiếm được. KEDB là một cơ sở dữ liệu chứa tất cả các bản ghi lỗi đã biết. Cơ sở dữ liệu này được tạo ra để quản lý sự cố. KEDB có thể là một phần của hệ thống quản lý cấu hình, hoặc có thể được lưu trữ ở nơi khác trong hệ thống quản lý dịch vụ. (Hoạt động Dịch vụ ITIL) Bằng chứng phải ở dạng các vấn đề đã được xác định, ghi lại, phân tích và sau đó được đưa vào KEDB. Đối tác phải chứng minh rằng cơ sở dữ liệu có thể tìm kiếm được. Ngoài ra, bằng chứng có thể ở dạng chứng nhận ngành hiện tại liên quan đến ITSM (ví dụ: ISO 20000)	✗		
3.5.9 Quản lý tài nguyên	Đối tác có chiến lược theo dõi và quản lý các tài nguyên được triển khai trên CMC Cloud. Tài nguyên được xác định như bất cứ ứng dụng nào triển khai hoặc dữ liệu lưu trữ phát sinh khi cung cấp dịch vụ. Cần một quy trình chung thực hiện theo dõi và báo cáo về các tài nguyên này (Chiến lược dịch vụ ITIL / Chuyển đổi dịch vụ) Chiến lược quản lý tài nguyên của Đối tác: • Doanh nghiệp của bạn có đang sử dụng metadata cụ thể của dịch vụ và instance trong chiến lược quản lý tài nguyên không?	✗		

	• Doanh nghiệp của bạn có đang tận dụng các thẻ tài nguyên tùy chỉnh để theo dõi và xác định các tài nguyên Cloud không? • Doanh nghiệp của bạn có chiến lược gắn thẻ tài nguyên không? • Tài nguyên Cloud sẽ được tích hợp với hệ thống quản lý tài nguyên của các Hệ thống quản lý dịch vụ của Doanh nghiệp của bạn như thế nào? Bằng chứng phải ở dạng biểu diễn công nghệ.			
3.5.10 Báo cáo cho Khách hàng	Đối tác cung cấp các báo cáo cho khách hàng Web-portal. Báo cáo nên cho phép khách hàng tự chọn các thông số để thiết lập dữ liệu. Ví dụ về các báo cáo được cung cấp là: • Quản lý sự cố • Dịch vụ không ảnh hưởng bởi sự cố • Phân tích hiệu năng • Tài nguyên Bằng chứng phải ở dạng minh họa về web-portal có thể truy cập của khách hàng hoặc những bằng chứng tương đương khác.	✗		
3.6 Thỏa thuận Mức độ Cung cấp Dịch vụ (SLA)				
3.6.1 SLAs cơ bảm	Đối tác có SLA cơ bản. Các SLA cơ bản là những SLA liên quan đến thời gian phản hồi, các hoạt động xử lý và thông báo của Đối tác cho khách hàng. SLA có thể bao gồm thời gian phản hồi khi khách hàng gửi yêu cầu, thời gian từ khi xảy ra sự cố hoặc tạo lập yêu cầu đến khi khắc phục, và thời gian quay vòng cho các thay đổi / yêu cầu do khách hàng khởi tạo. Bằng chứng phải ở dạng tài liệu SLA và các quy trình và chỉ số hỗ trợ các dịch vụ Cloud	✓		
3.6.2 Khối lượng công việc hoặc giải pháp-SLA cụ thể	Đối tác có các SLA dựa trên khối lượng công việc của khách hàng hoạt động trên Cloud như SLA dịch vụ Cloud, khối lượng công việc hỗ trợ lớn Bằng chứng phải ở dạng tài liệu SLA và các quy trình và chỉ số hỗ trợ các dịch vụ Cloud	✗		
3.7 Quản lý chi Hóa đơn và Chi phí				
3.7.1 Bảng điều khiển Quản lý	Đối tác sử dụng để thanh toán hóa đơn sử dụng dịch vụ Cloud của Khách hàng, theo dõi việc lưu sử dụng và chi phí ngân sách.	✓		

Thanh toán và Chi phí	Bằng chứng phải ở dạng minh họa bảng điều khiển Quản lý chi phí và lập hóa đơn Cloud, bao gồm cả việc chứng minh các khả năng sau: • Tải xuống Hóa đơn PDF từ Bảng điều khiển Quản lý Chi phí và Lập hóa đơn • Báo cáo thanh toán • Bật Cảnh báo Thanh toán • Quản lý Thẻ phân bổ chi phí • Giải thích các hạng mục chi phí chi tiết bên trong • Khả năng quản lý việc miễn thuế (Nếu có)			
3.7.2 Thiết lập tài khoản Cloud	Đối tác sử dụng trang Thiết lập để quản lý thông tin liên hệ và bảo mật để cập nhật cho Khách hàng, CMC và / hoặc (các) tài khoản được liên kết. • Bằng chứng phải ở dạng minh họa trang Thiết lập tài khoản, bao gồm cả việc chứng minh các khả năng sau: • Cập nhật thông tin địa chỉ cho Tài khoản • Mô tả và thêm địa chỉ liên hệ thay thế • Đặt câu hỏi thách thức bảo mật • Mô tả cách đóng Tài khoản • Quản lý việc hủy bỏ dịch vụ (ví dụ: Hỗ trợ)	✅		
3.7.3 Khả năng quản lý tài khoản của nhà cung cấp giải pháp	Đối tác có các khả năng quản lý tài khoản như sau: Tạo tài khoản mới và bật Thanh toán tổng hợp • Liên kết hoặc xóa tài khoản khỏi Tài khoản người thanh toán hóa đơn tổng hợp, Ví dụ: Doanh nghiệp sử dụng CMC Cloud • Đăng ký dịch vụ Hỗ trợ CMC Cloud • Khả năng bật CMC Cloud Identity and Access Management (IAM) để quản lý tài khoản dựa trên vai trò • Khả năng cấp quyền truy cập tài khoản • Khả năng mua dung lượng dự trữ Các dẫn chứng ở dạng phù hợp Đối tác chứng minh các khả năng trên.	✅		
3.7.4 Khả năng thanh toán của nhà cung cấp giải pháp	Đối tác có các khả năng thanh toán sau: • Giải thích sự khác biệt giữa tỷ lệ / chi phí • Mô tả chi tiết các cấu phần bên trong của Báo cáo Chi phí và Sử dụng	✅		

	• Khả năng giải thích cách phân bổ lợi ích tín dụng cho một hóa đơn tổng hợp • Khả năng giải thích cách phân bổ và mục đích dự trữ cho hóa đơn tổng hợp Các dẫn chứng ở dạng phù hợp Đối tác chứng minh các khả năng trên.			
3.7.5 Báo cáo người dùng cuối	Các đối tác được yêu cầu cung cấp Báo cáo người dùng cuối cho CMC. Đối tác phải chia sẻ cách thức thu thập, duy trì và báo cáo lại thông tin cho CMC.	✅		
3.8 Kiến thức về CMC Cloud và Công nghệ Điện toán đám mây				
3.8.1 Các dịch vụ và tính năng Cloud	Khách hàng chuyển sang sử dụng Cloud quan tâm đến khả năng tư vấn có cung cấp chuyên môn và hướng dẫn về Công nghệ Điện toán Đám mây như cách sử dụng, vận hành tốt nhất tất cả các dịch vụ và tính năng độc đáo mà CMC cùng Đối tác đang cung cấp.			
	3.8.1.1 Cơ sở dữ liệu	✅		
	3.8.1.2 Lưu trữ	✅		
	3.8.1.3 Bảo mật	✅		
	3.8.1.4 Công cụ quản lý Cloud	✅		
	3.8.1.5 DevOps	✅		
	3.8.1.6 Containers	❌		
	3.8.1.7 Dữ liệu lớn / Phân tích	❌		
	3.8.1.8 IoT (Internet vạn vật)	❌		
3.8.2 Chứng chỉ CMC Cloud	Chứng chỉ CMC Cloud Associate giúp Đối tác hiểu rõ hạ tầng, dịch vụ về các sản phẩm của CMC Cloud đang cung cấp. Trải nghiệm các tính năng của từng dịch vụ CMC Cloud và tối ưu chi chi & kết hợp ứng dụng dịch vụ mang lại hiệu quả cao nhất.			
	3.8.2.1 Elastic Compute Elastic Compute là dịch vụ cho phép khách hàng khởi tạo theo nhu cầu hàng loạt các tài nguyên máy chủ ảo bao gồm bộ vi xử lý trung tâm (CPU), bộ nhớ tạm thời (RAM), dung lượng lưu trữ (Storage) và hệ thống mạng (Networks) mà không cần phải đầu tư thiết bị phần cứng tại trung tâm dữ liệu (Data Center)	✅		
	3.8.2.2 KVM Private Cloud CMC Private Cloud là dịch vụ CMC Cloud cung cấp tới khách hàng 1 hệ thống máy chủ ảo dùng riêng theo nhu cầu với công nghệ điện toán đám mây KVM hiện đại, giúp doanh nghiệp đảm bảo vấn đề bảo mật, độc	✅		

	lập về tài nguyên, tiết kiệm chi phí hạ tầng và tối ưu trong việc quản trị hệ thống			
	3.8.2.3 VMWare Private Cloud CMC Private Cloud là dịch vụ CMC Cloud cung cấp tới khách hàng 1 hệ thống máy chủ ảo dùng riêng theo nhu cầu với công nghệ điện toán đám mây KVM hiện đại, giúp doanh nghiệp đảm bảo vấn đề bảo mật, độc lập về tài nguyên, tiết kiệm chi phí hạ tầng và tối ưu trong việc quản trị hệ thống	✅		
	3.8.2.4 CMC CDN CMC Content Delivery Network là dịch vụ Mạng phân phối nội dung (Content Delivery Network) giúp phân phối các tài nguyên như hình ảnh, video và ứng dụng đến người dùng một cách nhanh chóng, bảo mật và hiệu quả nhất.	✅		
	3.8.2.5 CMC S3 Storage CMC Storage S3 đang là một giải pháp tối ưu mà CMC đưa đến tay người dùng. Với dịch vụ này khách hàng có thể lưu trữ theo đối tượng được xây dựng và truy xuất với khối lượng lớn và ở bất kỳ đâu như: ứng dụng của công ty, các trang web và ứng dụng di động từ bộ cảm biến IOT hoặc các thiết bị khác	✅		
	3.8.2.6 Backup as a Service BaaS (Backup as a Service) là dịch vụ sao lưu và khôi phục dữ liệu theo mô hình điện toán đám mây, sử dụng các công nghệ hiện đại và phát triển dựa vào mạng Internet.	✅		