TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 13810:2023
ISO/IEC TR 22678:2019

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – TÍNH TOÁN MÂY – HƯỚNG DẪN XÂY DỰNG CHÍNH SÁCH

Information technology — Cloud computing — Guidance for policy development

HÀ NỘI - 2023

Mục lục

Lời nói đầu

TCVN 13810:2023 hoàn toàn tương đương với ISO/IEC TR 22678:2019.

TCVN 13810:2023 do Ban kỹ thuật tiêu chuẩn quốc gia TCVN/JTC 1 "*Công nghệ thông tin*" biên soạn, Viện Tiêu chuẩn Chất lượng Việt Nam đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Công nghệ thông tin – Tính toán mây – Hướng dẫn xây dựng chính sách

Information technology — Cloud computing — Guidance for policy development

1. Phạm vi áp dụng

Tiêu chuẩn này cung cấp hướng dẫn về việc sử dụng các tiêu chuẩn như một công cụ trong việc phát triển các chính sách quản lý hoặc điều chỉnh các nhà cung cấp dịch vụ mây (CSP) và dịch vụ mây, cũng như quản trị các chính sách và việc thực thi sử dụng các dịch vụ mây trong các tổ chức.

Tiêu chuẩn này bao gồm tài liệu giải thích các khái niệm tính toán mây và vai trò của các tiêu chuẩn về tính toán mây trong việc định hình các chính sách và việc thực thi.

Tiêu chuẩn này tham khảo các tiêu chuẩn khác nhau. Nếu có thể, các tiêu chuẩn này là tiêu chuẩn ISO/IEC. Trong trường hợp không có tiêu chuẩn ISO/IEC phù hợp, các tài liệu tham khảo được xuất bản bởi các cơ quan tiêu chuẩn khác đã đăng ký với WTO.

Như đã giải thích trong Hiệp định về Hàng rào Kỹ thuật trong Thương mại (TBT) của WTO, các tiêu chuẩn đóng một vai trò quan trọng trong việc hỗ trợ các quy định kỹ thuật và đánh giá sự phù hợp, tuy nhiên, tiêu chuẩn này không đề cập đến các vấn đề thương mại.

2. Tài liệu viện dẫn

Các tài liệu viện dẫn dưới đây là cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

TCVN 12480:2019 (ISO/IEC 17788:2014), Công nghệ thông tin – Tính toán đám mây[1] – Tổng quan và từ vựng.

3. Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa trong TCVN 12480 (ISO/IEC 17788) và các thuật ngữ và định nghĩa dưới đây.

3.1

Tính toán mây (cloud computing)

Mô thức cho phép truy nhập mạng vào một bể chứa linh hoạt và có khả năng thay đổi các tài nguyên vật lý và tài nguyên ảo dùng chung có cung cấp sự tự phục vụ và quản trị theo nhu cầu.

CHÚ THÍCH Ví dụ về các tài nguyên bao gồm máy chủ, hệ điều hành, mạng, phần mềm, ứng dụng và thiết bị lưu trữ.

[NGUỒN: 3.25, TCVN 12480:2019 (ISO/IEC 17788:2014)]

[1] 'Đám mây' trong tiêu chuẩn này sử dụng là 'mây'

3.2

Phạm vi thẩm quyền (jurisdiction)

Phạm vi về địa lý hoặc công ty mà chính sách tính toán mây mở rộng.

CHÚ THÍCH 1 Trong bối cảnh chính sách của chính phủ, đây thường sẽ là khu vực địa lý mà cơ quan ban hành chính sách có thẩm quyền pháp lý với tư cách là chính phủ hoặc cơ quan quản lý có thẩm quyền. Tuy nhiên, trong môi trường doanh nghiệp hoặc cơ quan chính phủ, phạm vi thẩm quyền của một chính sách có thể bao gồm chức năng kinh doanh, bộ phận, cơ quan hoặc lĩnh vực tổ chức khác chịu trách nhiệm không ràng buộc về địa lý.

4. Thuật ngữ viết tắt

CSC	*Cloud Service Customer*	Khách hàng dịch vụ mây
CSN	*Cloud Service Partner*	Đối tác dịch vụ mây
CSP	*Cloud Service Provider*	Nhà cung cấp dịch vụ mây
CSU	*Cloud Service User*	Người dùng dịch vụ mây
DDoS	*Distributed Denial of Service (attack)*	Từ chối dịch vụ phân tán (tấn công)
DPA	*Data Protection Authority*	Cơ quan bảo vệ dữ liệu
EN	*European Norm*	Định mức châu Âu
EU	*European Union*	Liên minh châu Âu
IaaS	*Infrastructure as a Service*	Hạ tầng như một dịch vụ
ICT	*Information and Communications Technology*	Công nghệ thông tin và truyền thông
IEC	*International Electro-technical Commission*	Ủy ban kỹ thuật điện quốc tế
ISO	*International Organisation for Standardisation*	Tổ chức tiêu chuẩn hóa quốc tế
IT	*Information Technology*	Công nghệ thông tin
ITU	*International Telecommunication Union*	Liên minh Viễn thông quốc tế
ITU-T	*ITU Telecom sector (responsible for standardisation)*	Tổ chức thuộc ITU có trách nhiệm đối với tiêu chuẩn hóa.
JTC1	*Joint Technical Committee 1 (a joint project between the ISO and IEC on standards for ICT)*	Ban kỹ thuật chung giữa ISO và IEC về các tiêu chuẩn ICT

MLAT	*Mutual Legal Assistance Treaty*	Hiệp ước tương trợ tư pháp
PaaS	*Platform as a Service*	Nền tảng như một dịch vụ
PII	*Personally Identifiable Information*	Thông tin định danh cá nhân
SaaS	*Software as a Service*	Phần mềm như là một dịch vụ
SC 27	*Sub-committee 27 of JTC1, responsible for information security standards*	Tiểu ban 27 của JTC1, chịu trách nhiệm về các tiêu chuẩn an toàn thông tin
SC 38	*Sub-committee 38 of JTC1, responsible for cloud computing standards*	Tiểu ban 38 của JTC1, chịu trách nhiệm về các tiêu chuẩn tính toán mây
SLA	*Service Level Agreement*	Thỏa thuận mức dịch vụ
SLO	*Service Level Objective*	Mục tiêu mức dịch vụ
SME	*Small or Medium sized Enterprise*	Doanh nghiệp vừa hoặc nhỏ
SQO	*Service Qualitative Objective*	Mục tiêu định tính dịch vụ
WTO	*World Trade Organisation*	Tổ chức Thương mại Thế giới

5. Tóm lược tiêu chuẩn này

5.1 Mục đích của tiêu chuẩn này

Mục đích của tiêu chuẩn này là tạo thuật tiện cho việc định hình các chính sách của chính phủ và doanh nghiệp nhằm giúp cho việc áp dụng và sử dụng các dịch vụ tính toán mây dựa trên tiêu chuẩn.

Bằng cách làm theo hướng dẫn trong tiêu chuẩn này, các nhà phát triển chính sách có thể:

- tận dụng thích hợp các tiêu chuẩn khi xây dựng chính sách;
- đạt được sự nhất quán toàn cầu hơn trong các luật, quy định và chính sách hiện hành;
- giảm chi phí cho các CSP và CSC;
- tăng sự lựa chọn và cạnh tranh;
- đơn giản hóa các thách thức của việc triển khai và áp dụng các dịch vụ mây cục bộ, đa quốc gia hoặc toàn cầu với chi phí hiệu quả.

5.2 Đối tượng dự định

- Các nhà làm luật (ở cả các nước phát triển và đang phát triển) ở mọi cấp độ;
- Cơ quan quản lý, bao gồm Cơ quan bảo vệ dữ liệu (DPA);
- Những chính sách doanh nghiệp phát triển bao gồm:

- Khách hàng dịch vụ mây (lớn và nhỏ) và khách hàng tiềm năng,
- Các nhà cung cấp dịch vụ mây,
- Các đối tác dịch vụ mây;

- Những tổ chức đang phát triển các quy tắc và chính sách phi chính phủ về sự tin cậy và minh bạch cho tính toán mây, chẳng hạn như các cơ quan thương mại và tổ chức kỹ thuật;
- Các tổ chức cung cấp lời khuyên cho các chính phủ và doanh nghiệp về các tác động kinh tế và chính trị của các chính sách công nghệ, ví dụ: Tổ chức Hợp tác và Phát triển Kinh tế (OECD).

Đặc biệt, tiêu chuẩn này nhằm hỗ trợ những người trong các cơ quan hành chính nhỏ hơn như chính quyền địa phương, các nước đang phát triển và những người thiếu kiến thức chuyên môn về các vấn đề này.

5.3 Cách sử dụng tiêu chuẩn này

Tiêu chuẩn này đưa ra hướng dẫn về các tiêu chuẩn cụ thể có thể áp dụng cho các chính sách về tính toán mây và cung cấp hướng dẫn cách sử dụng tốt nhất.

6. Hiểu các khía cạnh tính toán mây để xây dựng chính sách

6.1 Giới thiệu

Điều này đưa ra giải thích về một số đặc điểm và ý nghĩa chính của tính toán mây khi các nhà xây dựng chính sách công hoặc công ty mong muốn hiểu các dịch vụ mây. Mục đích là trình bày tiêu chuẩn này theo cách dễ đọc và dễ tiếp cận cho những người không phải là kỹ sư tính toán mây toàn thời gian; đồng thời cung cấp tài liệu tham khảo đến tài liệu kỹ thuật khác có thể được xem xét khi thích hợp.

6.2 Các đặc điểm cơ bản của tính toán mây

6.2.1 Định nghĩa tiêu chuẩn về tính toán mây

Định nghĩa về tính toán mây (3.1) nắm bắt một số đặc điểm thiết yếu khác với tính toán truyền thống, cục bộ hoặc được lưu trữ. Các đặc điểm này được giải thích thêm trong TCVN 12480 (ISO/IEC 17788) và sẽ được mô tả chi tiết hơn trong ISO/IEC 221231 sắp tới [2].

Một cách hiệu quả, định nghĩa này nói rằng tính toán mây liên quan đến việc cung cấp hầu hết mọi tài nguyên ICT dưới dạng dịch vụ (dịch vụ mây) qua mạng và rằng việc cung cấp này có thể được thực hiện nhu cầu động theo yêu cầu của CSC, giống như cách các tiện ích, chẳng hạn như viễn thông, được cung cấp. Khách hàng sử dụng những gì cần thiết khi họ cần và mức tiêu thụ được lập hóa đơn tương ứng. Các tài nguyên Công nghệ thông tin và truyền thông có thể được truy cập gần như đơn giản bằng cách nhấn công tắc để bật đèn, và có thể được giải phóng gần như đơn giản bằng cách nhấn lại công tắc để tắt đèn. Sự cần thiết của CSC để thực hiện các quy trình dài để có được, cài đặt, cấu hình, bảo mật và vận hành phần cứng, phần mềm và ứng dụng đã giảm đáng kể, nếu không muốn nói là bị loại bỏ hoàn toàn.

[2] Đang xây dựng. Giai đoạn hiện tại: 30,60.

6.2.2 Các đặc điểm cơ bản của tính toán mây (theo TCVN 12480 (ISO/IEC 17788))

Tính toán mây có một loạt các đặc điểm thiết yếu, được tóm tắt trong Bảng 1 (trang sau).

Bảng 1 - Các đặc điểm thiết yếu tính toán mây

Đặc điểm	Trong tính toán mây
Truy cập mạng băng rộng	Dịch vụ mây có thể được truy cập từ một vị trí tùy ý bằng nhiều loại thiết bị bao gồm PC và thiết bị di động các loại, được kết nối theo nhiều cách, thường là bằng Internet nhưng đôi khi bằng mạng riêng, chẳng hạn như mạng nội bộ của công ty.
Dịch vụ được đo lường	Việc sử dụng dịch vụ mây của khách hàng được đo lường và họ có thể bị tính phí dựa trên những gì họ sử dụng thực, giống như việc cung cấp điện thường được lập hóa đơn dựa trên tiêu thụ năng lượng đo được. Do đó, việc sử dụng giảm có thể đồng nghĩa với việc giảm chi phí.
Nhiều bên thuê	Nhiều bên thuê có nghĩa là các tài nguyên được cung cấp bởi một dịch vụ mây được chia sẻ bởi nhiều CSC. Việc sử dụng tài nguyên của mỗi người thuê được cách ly và không thể tiếp cận được với tất cả những người thuê khác - để các CSC được đảm bảo rằng dữ liệu và việc sử dụng các ứng dụng không thể bị bất kỳ CSC nào khác nhìn thấy. Điều này có thể so sánh với kỳ vọng rằng các chi tiết trong tài khoản ngân hàng không hiển thị cho các khách hàng khác của ngân hàng. Lưu ý rằng một khách hàng đôi khi có thể có nhiều cách thuê khác nhau với một dịch vụ mây nhất định, ví dụ: nơi mà các hoạt động của các bộ phận khác nhau trong một tổ chức cần được giữ cô lập với nhau. Cũng lưu ý rằng trong khi một mây riêng theo định nghĩa chỉ có một CSC duy nhất, thì khách hàng đó vẫn có thể chọn thuê nhiều bên thuê của riêng họ cho các mục đích tách biệt.
Dịch vụ tự phục vụ theo nhu cầu	Nói chung, các dịch vụ mây cho phép khách hàng đăng ký, thanh toán và sử dụng dịch vụ mà không cần tương tác với đại diện dịch vụ khách hàng của con người. Khách hàng nói chung cũng có thể quản lý hoặc hủy dịch vụ của mình một lần nữa mà không cần sự can thiệp của con người. Có thể có những trường hợp ngoại lệ khi cần phải có sự tương tác với nhân viên vận hành, nhưng đây sẽ là những trường hợp bất thường, không phải là hoạt động kinh doanh thông thường.
Tính linh hoạt và khả năng mở rộng nhanh chóng	Các dịch vụ mây có thể phân bổ tài nguyên động cho một khối lượng công việc cụ thể khi cần thiết. Điều này đôi khi được mô tả là mở rộng chiều dọc - nâng cấp (tăng kích thước của một tài nguyên) hoặc mở rộng chiều ngang - tăng lượng (phân bổ thêm các tài nguyên tương tự). Mục đích là khách hàng có thể mở rộng và ký hợp đồng sử dụng dịch vụ mây một cách linh hoạt nhất có thể, thường là để đối phó với sự gia tăng hoặc giảm khối lượng công việc theo kế hoạch hoặc bất ngờ. Ví dụ: nếu một trang web được lưu trữ trên dịch vụ mây đột nhiên thu hút một lượng lớn sự quan tâm, chủ sở hữu trang web có thể đặt hàng (và trả tiền) để có thêm băng thông và sức mạnh tính toán để trang web không bị quá tải. Khi đã qua đỉnh, tài nguyên có thể được giải phóng và giảm chi phí. Một khía cạnh quan trọng khác của khả năng mở rộng dịch vụ mây là các tài nguyên có sẵn sàng thể mang lại hiệu quả không giới hạn cho khách hàng. Điều này trái ngược với các trung tâm dữ liệu truyền thống, nơi số lượng máy chủ, dung lượng lưu trữ dữ liệu, băng thông mạng thường có những giới hạn chỉ có thể thay đổi bằng cách lắp đặt thêm thiết bị.
Bể chứa tài nguyên	Tính toán mây đạt được hiệu quả bằng cách chia sẻ các tài nguyên khác nhau giữa nhiều bên thuê và khối lượng công việc. Ví dụ: trong máy tính truyền thống, mười khách hàng có thể được lưu trữ trên mười máy chủ riêng biệt, ngay cả khi mỗi người trong số họ chỉ sử dụng một nửa công suất của mỗi máy chủ. Trong môi trường tính toán mây, mười khách hàng đó có thể được cấp phép tự động chỉ trên năm máy chủ.

Để khám phá mối quan hệ qua lại giữa sáu đặc điểm cơ bản này và các hàm ý khác nhau của tính toán mây được xác định trong tiêu chuẩn này (xem Phụ lục A).

6.3 Những lợi ích chính của tính toán mây

6.3.1 Các lợi ích cho khách hàng sử dụng dịch vụ mây (Các CSC)

Các lợi ích mà các CSC được hưởng được tóm tắt trong Bảng 2 (trang sau).

Bảng 2 — Lợi ích cho khách hàng của tính toán mây

Lợi ích đối với khách hàng	Trong tính toán mây
Đầu tư vốn thấp	Khách hàng muốn xây dựng hoặc chạy một ứng dụng mới không cần phải cung cấp thiết bị công nghệ thông tin riêng, cũng như các công trình và hạ tầng cần thiết để chứa và hỗ trợ, và có khả năng không cần phải mua, cài đặt và vận hành nhiều hoặc tất cả ngăn xếp phần mềm cho ứng dụng. Khách hàng chỉ trả số tiền tương đối nhỏ (tức là không cần mua thiết bị máy chủ) trong khi xây dựng và/hoặc triển khai ứng dụng mới, sau đó dần xây dựng lượng tài nguyên máy chủ mây mà họ sử dụng như việc sử dụng ứng dụng.
Hiệu quả chi phí của quy mô mây	CSP có thể mua ở quy mô lớn, có nghĩa là máy chủ và các tài nguyên khác rẻ hơn nhiều khi mua với số lượng lớn. Các khoản tiết kiệm chi phí này có thể được chuyển cho các khách hàng cá nhân. Ngoài ra, chi phí cho mỗi máy chủ để chạy các trung tâm dữ liệu rất lớn, về nhân lực, năng lượng và các chi phí khác, thấp hơn nhiều so với hàng trăm cài đặt nhỏ.
Sử dụng khi cần	Các dịch vụ mây cho phép khách hàng bắt đầu với quy mô nhỏ, sau đó tăng và giảm nhanh khi cần thiết. Khách hàng có thể giảm hóa đơn trong thời gian hoạt động kinh doanh lắng xuống và tăng khả năng sẵn sàng (hoặc đáp ứng) khối lượng đỉnh, chẳng hạn như mua sắm theo mùa hoặc mức độ phổ biến bất ngờ.
Cạch tranh	Giá dịch vụ mây rất cạnh tranh do sự năng động của thị trường. Mỗi dự án mới có sự lựa chọn CSP sẽ sử dụng và các công ty khởi nghiệp mới tiếp tục thách thức các nhà khai thác lớn bằng các tính năng và đổi mới đặc biệt.
An ninh	An ninh được coi là mối quan tâm khi chuyển sang sử dụng các dịch vụ mây, nhưng ngày nay an ninh được coi là một thế mạnh đáng kể. An ninh không còn được coi là một trở ngại trong việc áp dụng tính toán mây. Điều này có một vài nguyên nhân. Thứ nhất, các CSP uy tín thường có các đội an ninh làm việc suốt ngày đêm trên toàn thế giới để giữ cho hệ thống an toàn, cập nhật các bản vá an ninh và trước bất kỳ mối đe dọa mới nổi nào có thể được xác định. Đội an ninh phản ứng rất nhanh khi có sự cố. Ngay cả các doanh nghiệp thương mại lớn và các chính phủ nhỏ hơn cũng khó khăn trong việc tuyển dụng và trả lương cho đội ngũ nhân viên của mình có trình độ chuyên môn an ninh 24 × 7 tương đương. Thứ hai, một trong những mối đe dọa lớn nhất đối với an ninh máy tính là cuộc tấn công "nội gián", trong đó ai đó có quyền truy cập quản trị hoặc vật lý có liên quan đến vi phạm, có thể là một nhân viên hư hỏng hoặc bất mãn, nhưng người sẽ không có cùng loại quyền truy cập một dịch vụ mây bên ngoài. (Xem ITU-T X.1601).
Tính sẵn sàng và độ tin cậy	Nhiều CSP vận hành nhiều trung tâm dữ liệu ở các vị trí riêng biệt và điều này mang lại cho các khách hàng cơ hội cải thiện tính sẵn sàng của các ứng dụng và dữ liệu. Các ứng dụng có thể được chạy trong nhiều trung tâm dữ liệu và dữ liệu có thể được sao chép giữa các trung tâm dữ liệu đó, tránh bất kỳ điểm lỗi nào. Nếu một trung tâm dữ liệu được đưa vào ngoại tuyến do một số thảm họa tự nhiên hoặc sự cố lớn, quyền truy cập CSC vào các ứng dụng và dữ liệu có thể được chuyển ngay lập tức sang một trung tâm dữ liệu khác.
Các khả năng nâng cao	Ngày càng có nhiều trường hợp CSP đang cung cấp các khả năng nâng cao dưới dạng các dịch vụ mây có sẵn. Ví dụ bao gồm các hệ thống AI, Phân tích nâng cao và các dịch vụ Dữ liệu lớn. Một số dịch vụ này được đào tạo trước trên bộ dữ liệu rộng lớn. Các CSC có thể gặp khó khăn trong việc triển khai nội bộ các khả năng nâng cao này hạn chế tiếp cận nhân lực có kỹ năng và các tài nguyên. Thường sẽ tiết kiệm chi phí hơn nhiều nếu tích hợp các dịch vụ mây nâng cao này vào các ứng dụng mới do CSC xây dựng.

Lợi ích đối với khách hàng	Trong tính toán mây
Lựa chọn mô hình triển khai dịch vụ mây	Tính toán mây cho phép CSC chọn mô hình triển khai phù hợp nhất để đáp ứng các yêu cầu của chúng, bao gồm các mô hình triển khai dịch vụ mây công cộng, riêng tư, cộng đồng và hỗn hợp (xem TCVN 12480 (ISO/IEC 17788)). Đối với mô hình triển khai mây riêng, CSP sẽ là một phần của tổ chức riêng của CSC.
Tuân thủ dễ dàng hơn	Hầu hết các CSP mây công cộng đều đạt được nhiều chứng nhận cho các dịch vụ mây. Bằng cách tận dụng các dịch vụ mây này, các CSC có thể dỡ bỏ một phần lớn gánh nặng về việc đạt được chứng chỉ và đảm bảo tuân thủ. Ngoài ra, các CSP thường cung cấp lời khuyên, hướng dẫn và hỗ trợ cho các CSC của chúng, những người đang tìm cách để việc sử dụng dịch vụ mây tuân thủ những điều như quy định về sự riêng tư và bảo vệ dữ liệu trong phạm vi thẩm quyền.

6.3.2 Các lợi ích đối với xã hội

Những lợi ích mang lại cho xã hội rộng hơn có thể mang lại từ tính toán mây được tóm tắt trong Bảng 3.

Bảng 3 — Lợi ích cho xã hội từ tính toán mây

Lợi ích đối với xã hội	Trong tính toán mây
Hiệu suất năng lượng	Các trung tâm dữ liệu được xây dựng cho mục đích lớn có thể tiết kiệm năng lượng hơn nhiều so với nhiều trung tâm dữ liệu nhỏ hơn. Chúng cũng có thể ở những nơi mà nguồn điện sẵn sàng hơn với chi phí thấp hơn, hoặc nơi nguồn điện được sử dụng dựa trên năng lượng tái tạo. Một số trung tâm dữ liệu thậm chí còn được ký hợp đồng để hoạt động trên cơ chế làm mát bằng không khí tự do, giúp giảm đáng kể nhu cầu năng lượng. Ngoài ra, CSP có thể tối ưu hóa khối lượng công việc và dữ liệu của khách hàng trên số lượng máy chủ cần thiết tối thiểu. [a]
Mạnh mẽ và khả năng phục hồi	Các kết nối với các dịch vụ mây được bảo vệ mạnh mẽ và ít bị tấn công bởi vi-rút hoặc phần mềm độc hại. Chúng cũng thường đủ mạnh để chống lại các cuộc tấn công từ chối dịch vụ phân tán (DDoS) được xác định từ tin tặc và các botnet. Các nhà cung cấp dịch vụ mây thường cung cấp sự đa dạng về địa lý, để các dịch vụ mây có thể tiếp tục ngay cả trong trường hợp thiên tai lớn làm vô hiệu một trong các trung tâm dữ liệu. Hơn nữa, bởi vì các hệ thống này thường sử dụng phần mềm để cung cấp khả năng phục hồi trên nhiều máy vật lý, chúng không yêu cầu mọi máy tính phải chạy một cách đáng tin cậy. Đối với một trung tâm dữ liệu dịch vụ mây lớn, không cần thiết phải quan tâm đến mọi máy chủ. Thay vào đó, khối lượng công việc có thể được di chuyển mà không ảnh hưởng đến khách hàng. Dịch vụ vẫn có khả năng phục hồi ngay cả khi các máy chủ riêng lẻ thì không. Các thiết bị hỏng hóc sau đó có thể được sửa chữa và sử dụng lại hoặc tái chế nếu thích hợp. Khả năng phục hồi của các dịch vụ mây mang lợi ích cho xã hội, vì các CSC không còn phụ thuộc vào nguồn lực và kỹ năng của chính họ để giữ cho các quy trình kinh doanh hoạt động.
Quyền truy cập hợp pháp	Sự riêng tư của khách hàng là quan trọng, xã hội cũng cần tự bảo vệ khỏi những tác nhân xấu. Khi dữ liệu được lưu trữ trong các dịch vụ mây, thay vì trên máy tính cục bộ, sẽ có các biện pháp bổ sung để có được quyền truy cập hợp pháp được cấp phép phù hợp vào dữ liệu đó cho các cuộc điều tra tội phạm, chống khủng bố và các mục đích khác của chính phủ. Tuy nhiên, đây không phải là một giải pháp cho tất cả và vẫn còn những thách thức về mặt pháp lý và kỹ thuật. Ví dụ: một tình huống mà dữ liệu được lưu trữ trong (và/hoặc được quản lý từ) một phạm vi thẩm quyền khác có thể liên quan đến sự phức tạp pháp lý đối với các nhà điều tra, chẳng hạn như yêu cầu sử dụng Hiệp ước Tương trợ Tư pháp (MLAT) để có được sự hợp tác của các cơ quan thích hợp trong các cơ quan tài phán khác. Một lĩnh vực liên quan là khám phá điện tử trong quá trình tố tụng pháp lý, trong

Lợi ích đối với xã hội	Trong tính toán mây
	đó các tiêu chuẩn như loạt tiêu chuẩn ISO/IEC 27050 có thể hữu ích.

[a] Một doanh nghiệp nhỏ chuyển sang mây có thể giảm hơn 90% mức tiêu thụ năng lượng và lượng khí thải carbon bằng cách chạy các ứng dụng kinh doanh trên mây thay vì chạy các ứng dụng tương tự trên hạ tầng của chính họ.
Nguồn: Tài liệu tham khảo [39]

6.4 Hàm ý đối với các nhà hoạch định chính sách

6.4.1 Trách nhiệm chung

Do bản chất của tính toán mây, trong đó CSC và CSU có quyền kiểm soát đáng kể việc sử dụng dịch vụ mây, nên có những *trách nhiệm chung* để duy trì sự an ninh, sự riêng tư, tính bảo mật và tính toàn vẹn của dịch vụ. Ví dụ, các CSC vẫn chịu trách nhiệm đối với các thực hành tốt nhất trong việc sử dụng dịch vụ mây của chúng, chẳng hạn như trong việc xử lý mật khẩu hoặc thông tin đăng nhập khác, trong việc cấp quyền phù hợp cho người dùng cụ thể, về loại dữ liệu họ đưa vào dịch vụ mây và trong việc ghi nhãn để dịch vụ mây có thể xử lý nội dung đó một cách chính xác. Các thực hành như vậy xác định tính bảo mật tổng thể, sự riêng tư, tính bảo mật và tính toàn vẹn của dịch vụ, nhưng nằm ngoài tầm kiểm soát của riêng CSP.

Việc sử dụng các quy tắc thực hành do ngành xác định để hướng dẫn cả CSP và CSC trong việc vận hành và sử dụng các dịch vụ mây được coi là một cách tiếp cận có giá trị.

6.4.2 Các dịch vụ mây được triển khai và quản lý trên nhiều phạm vi thẩm quyền

Theo truyền thống, các hệ thống CNTT được triển khai trong một tổ chức hoặc trong một môi trường được lưu trữ dành riêng cho một quốc gia hoặc khu vực tài phán khác. Ngay cả các hạ tầng viễn thông quốc tế cũng được xây dựng theo từng quốc gia, với các điểm kết nối rõ ràng được xác định ở ranh giới quốc tế, do đó, các nguồn lực và quản lý thường được thực hiện bởi nhân viên và sử dụng các cơ sở trong cùng thẩm quyền với khách hàng của dịch vụ. Điều này không còn đúng với nhiều hệ thống và dịch vụ tính toán mây.

Các dịch vụ mây toàn cầu và đa quốc gia đạt được quy mô và hiệu quả bằng cách tập trung hóa các hoạt động, quản lý và nhân viên nhiều nhất có thể. Điều này có nghĩa là khách hàng ở một quốc gia có thể đang sử dụng tài nguyên dịch vụ mây (ví dụ: máy chủ, kho dữ liệu và thiết bị mạng) được đặt ở quốc gia khác, với những máy chủ đó được quản lý từ quốc gia thứ ba.

Cách tiếp cận này mang lại nhiều lợi ích cho cả CSP và CSC.

1) Việc có một phiên bản toàn cầu duy nhất của bộ phần mềm cho dịch vụ mây có nghĩa là một đội an ninh, xây dựng và thử nghiệm có thể hỗ trợ toàn bộ mạng trung tâm dữ liệu của CSP, bất kể có bao nhiêu hay bao nhiêu quốc gia.
2) Các CSP và CSC được hưởng lợi từ các cải tiến liên tục, kịp thời cho dịch vụ, thay vì mỗi quốc gia hoặc trung tâm dữ liệu phải triển khai các bản cập nhật riêng lẻ.
3) Các bản vá và sửa lỗi an ninh có thể được triển khai dễ dàng hơn. Các lỗ hổng hoặc vi phạm được xác định ở bất kỳ đâu có thể được giải quyết đồng thời ở mọi nơi.

4) Nó cho phép sự đa dạng địa lý trong việc triển khai các dịch vụ và dữ liệu. Điều này có thể cung cấp khả năng dự phòng và bảo vệ khỏi các sự cố lớn như lũ lụt, động đất hoặc sự cố mạng, có thể khiến toàn bộ trung tâm dữ liệu ngừng hoạt động. Việc cung cấp nhiều trung tâm dữ liệu ở các quốc gia nhỏ hơn hiếm khi hiệu quả về chi phí hoặc hiệu quả, vì vậy dự phòng bên ngoài quốc gia có thể là lựa chọn duy nhất để đáp ứng các yêu cầu liên tục của doanh nghiệp.

5) Đối với dữ liệu không bị ràng buộc về mặt địa lý, dịch vụ mây có thể tự động di chuyển hoặc sao chép dữ liệu giữa các trung tâm dữ liệu để tối ưu hóa hiệu suất và việc sử dụng bộ nhớ. Ví dụ: một số dữ liệu có thể phù hợp để đọc trên toàn thế giới, có thể trên thiết bị di động (ví dụ: bản đồ, tin tức, video), vì vậy việc nhân rộng toàn cầu sẽ cải thiện đáng kể trải nghiệm của khách hàng bằng cách giảm độ trễ truy cập dữ liệu. Việc di chuyển và sao chép dữ liệu như vậy thường hoàn toàn tự động dựa trên các phép đo khách quan về các hành vi sử dụng dữ liệu.

6.4.3 Kinh tế quản lý dịch vụ mây toàn cầu

Các CSP, đặc biệt là các tổ chức lớn, có khả năng phục hồi và linh hoạt để giảm thiểu chi phí đầu tư vốn và chi phí hoạt động, đồng thời có thể cho phép định giá thấp hơn các dịch vụ mây. Các CSP thường sử dụng các cấu hình thiết bị tiêu chuẩn trên các trung tâm dữ liệu của họ, cho phép họ mua thiết bị với số lượng lớn. Các máy chủ được sử dụng trong trung tâm dữ liệu mây thông thường không có nhiều "chuông và còi" được tìm thấy trong các máy chủ bán sẵn giúp tiết kiệm chi phí và năng lượng. Các CSP chủ yếu sử dụng khả năng phục hồi dựa trên phần mềm thay vì dự phòng thiết bị để cung cấp cho hoạt động kinh doanh liên tục, giảm thêm vốn và chi phí hoạt động. Do đó, đối với một trung tâm dữ liệu dịch vụ mây lớn, vấn đề không phải là "giữ cho tất cả thiết bị hoạt động", mà là chuyển vị trí khối lượng công việc sao cho CSC không nhận thấy bất kỳ lỗi phần cứng hoặc thay đổi nào đối với dịch vụ. Khả năng phục hồi như vậy có thể yêu cầu các ứng dụng sử dụng các kiểu kiến trúc phần mềm cụ thể hoặc các mẫu thiết kế liên quan đến ví dụ như các ứng dụng "mây bẩm sinh" để minh bạch các lỗi cho người dùng dịch vụ mây.

Do quy mô của các trung tâm dữ liệu mây lớn, các CSP thiết kế để sử dụng năng lượng tối thiểu nhằm tiết kiệm chi phí và tối đa hóa mật độ tính toán theo cách mà các trung tâm dữ liệu nhỏ hơn không làm được. Máy chủ mây không cần giao diện (chẳng hạn như màn hình, chuột và bàn phím) vốn không bao giờ được sử dụng trong thiết kế máy chủ gắn trên giá đỡ số lượng lớn. Ngoài ra, các CSP được khuyến khích thiết kế hệ thống làm mát và phân phối điện hiệu quả cao để giảm tác động đến môi trường. Các CSP bắt đầu các dự án năng lượng tái tạo theo yêu cầu để cung cấp năng lượng cho các trung tâm dữ liệu và họ có thể sử dụng các nguồn năng lượng tiên tiến, thân thiện với môi trường như pin nhiên liệu sinh học khối lượng lớn. Bên cạnh năng lượng tái tạo, tùy thuộc vào vị trí, tái chế nhiệt có thể được sử dụng để thu thập và tận dụng nhiệt được tạo ra, ví dụ như nhà ở ấm áp của địa phương. Các kỹ thuật này và các kỹ thuật khác có sẵn và có thể đo lường được trong tất cả các trung tâm dữ liệu tiết kiệm năng lượng như được đề cập trong các tiêu chuẩn như ISO/IEC 19395 và ISO/IEC 30134-4, được xây dựng trong ISO/IEC JTC 1, Tiểu ban 39, Tính bền vững cho và bởi Công nghệ thông tin.

Sử dụng một phiên bản phần mềm duy nhất trên các trung tâm dữ liệu là một cách khác để các CSP

chứa chi phí. Do đó, một CSP sẽ cố gắng sử dụng cùng một phần mềm chính xác cho từng dịch vụ trong toàn bộ mạng trung tâm dữ liệu. Phần mềm này sau đó có thể được giám sát, quản lý và duy trì bởi một đội duy nhất (bao gồm cả các nhà phân tích an ninh). Các phiên bản phần mềm mới sẽ được thử nghiệm và triển khai dần dần, để giảm nguy cơ gây ra lỗi nghiêm trọng cho toàn mạng, nhưng mục tiêu vẫn là giữ cho một phiên bản phần mềm được triển khai duy nhất trong toàn bộ CSP càng nhiều càng tốt.

Khi có nhiều phiên bản phần mềm, mọi thay đổi sẽ cần được kiểm tra đối với tất cả các phiên bản đang hoạt động và mọi lỗ hổng bảo mật phải được kiểm tra và vá trong mọi phiên bản. Ngoài ra, cần phải kiểm tra toàn diện khi phần mềm của một phiên bản tương tác với phần mềm của phiên bản khác. Do đó, chi phí bảo trì tăng lên xấp xỉ bình phương số lượng phiên bản đang sử dụng.

Tính nhất quán của phần cứng và phần mềm tiếp tục cho phép quản lý tự động các dịch vụ mây. Các CSP có thể sử dụng nhiều cách (ví dụ: trí thông minh nhân tạo) để giám sát hàng triệu máy chủ và quy trình nhằm phát hiện các lỗi và bất thường sắp xảy ra. Điều này làm tăng tính liên tục của hoạt động kinh doanh và giảm chi phí cho các CSP và CSC.

6.4.4 Tính toán mây công cộng có khả năng mở rộng và hoạt động toàn cầu

Được triển khai trên toàn cầu, các dịch vụ mây công cộng có khả năng mở rộng cao đưa ra các dịch vụ hiệu quả về chi phí và có thể mở rộng trên các biên giới địa chính trị. Các dịch vụ như vậy đưa ra các khả năng không có sẵn trong triển khai tại chỗ truyền thống hoặc các mây riêng. Ví dụ như các dịch vụ toàn cầu như vậy cho phép thu thập và chuyển dữ liệu người dùng cũng như dữ liệu tổ chức qua các ranh giới địa chính trị. Khối lượng và tốc độ thu thập và truyền dữ liệu là chưa từng có.

Với sự ra đời của phân tích dữ liệu và kỹ thuật học máy sử dụng sức mạnh của các dịch vụ mây công cộng và số lượng lớn dữ liệu được thu thập, cần phải hiểu rõ nguồn gốc và thể loại dữ liệu. Ngoài ra, khi dữ liệu được tổng hợp và không được xác định (xem TCVN 13056 (ISO/IEC 19944)), các nhà xây dựng chính sách công và doanh nghiệp cần hiểu các khái niệm, thuật ngữ và công cụ cần thiết để truyền đạt các hành vi và kết quả mong muốn nhằm bảo vệ cá nhân cũng như bảo vệ bí mật của tổ chức dữ liệu.

6.4.5 Quy mô và tốc độ dịch vụ

Đặc điểm chính của tính toán mây là dịch vụ này là "Tự phục vụ theo yêu cầu" (xem 6.2, TCVN 12480:2019 (ISO/IEC 17788:2014)). Điều này có nghĩa là khách hàng có thể tạo tài khoản, thanh toán cho (các) dịch vụ đã chọn, bắt đầu sử dụng, đăng nội dung, thực hiện thay đổi hoặc bất kỳ điều gì khác mà dịch vụ mây cung cấp cho họ, trong một quy trình tự động hóa cao. Tốc độ sử dụng dịch vụ này được các CSC đánh giá cao và là động lực chính trong việc áp dụng dịch vụ mây. Tuy nhiên, cũng là một thách thức đối với các CSP trong việc lọc ra các hành vi "tác nhân xấu" của các CSC. Ví dụ về hành vi xấu đó bao gồm sử dụng dịch vụ mây cho các mục đích xấu (ví dụ: phát tán phần mềm độc hại, chia sẻ nội dung bất hợp pháp hoặc cực đoan, vi phạm bản quyền, v.v...), sử dụng bất cẩn (ví dụ: đưa thông tin bí mật vào những nơi không an ninh) hoặc sử dụng thiếu hiểu biết (ví dụ: đăng nội dung được chấp nhận ở quốc gia của họ, nhưng không phù hợp hoặc bất hợp pháp ở nơi khác).

Mặc dù các CSP liên tục làm việc để giảm thiểu các tác nhân xấu này, nhưng nó vẫn là một "cuộc chạy đua vũ trang" giữa các CSP và các CSU độc hại (được ủy quyền hoặc không). Các CSP đã và đang triển khai cả các chuyên gia về con người và các công cụ trí tuệ nhân tạo để giảm thiểu việc sử dụng không đúng các dịch vụ.

Các CSC, nếu có, đảm nhận trách nhiệm và quản lý việc kiểm soát truy cập và việc sử dụng môi trường của chúng. Ví dụ như CSC cần kiểm soát việc ủy quyền và xác thực cho các dịch vụ mây để đảm bảo rằng các CSU không lạm dụng các dịch vụ mây. Hơn nữa, CSC cần giám sát nội dung và việc sử dụng các dịch vụ mây để đảm bảo rằng tất cả các luật hiện hành của địa phương, quốc gia và quốc tế đều được tôn trọng (xem thêm 6.4.1).

6.4.6 Phát triển liên tục

Trước tính toán mây, phần mềm được xây dựng dưới dạng các "bản phát hành" lớn, thường cách nhau hai năm hoặc hơn. Cách tiếp cận này cho phép thực hiện một lượng lớn thử nghiệm và chứng nhận trước khi mỗi bản phát hành được phát hành trực tuyến. Trên thực tế, việc cập nhật từ bản phát hành này sang bản tiếp theo thường yêu cầu hệ thống phải gỡ xuống, cập nhật mã mới và sao lưu lại, cùng một lúc hoặc theo lô máy, do đó gây ra gián đoạn dịch vụ theo kế hoạch. Nếu cập nhật không thành công, toàn bộ quá trình có thể cần phải được đảo ngược. Điều này cũng có nghĩa là các bản cập nhật bảo mật có thể phải đợi vài tuần hoặc vài tháng để "gói dịch vụ" hoặc cơ hội cập nhật phần mềm khác được triển khai.

Tính toán mây, do tính chất hoạt động 24×7 và môi trường đe dọa an ninh hiện đại, đã chuyển sang mô hình phát triển liên tục trong đó các thay đổi gia tăng nhỏ được đưa ra rất thường xuyên, thường là hàng tuần hoặc thậm chí hàng ngày. Các bản sửa lỗi an ninh có thể được triển khai nhanh chóng hơn nữa khi cần thiết.

Hiệu quả của việc này là không còn một lịch trình "phát hành" rõ ràng với thời gian dài dành cho các quy trình kiểm tra hoặc chứng nhận được lên kế hoạch nghiêm ngặt. Chu kỳ phê duyệt truyền thống cho hệ thống kế thừa sẽ không được hoàn thành trên hệ thống mây trước khi nó được chuyển sang phiên bản mới và với những thay đổi tiếp theo đang được thực hiện. Do đó, kiểm tra và chứng nhận cần phải thích ứng với môi trường phần mềm thay đổi liên tục. TCVN TCVN ISO/IEC 27001:2019 (ISO/IEC 27001:2013) cung cấp cấu trúc để kiểm tra và chứng nhận công nghệ đổi mới nhanh chóng. Một tác dụng là việc kiểm tra có thể tập trung hơn. Chắc chắn có thể xảy ra một số lỗi do chính nhà cung cấp dịch vụ kiểm tra để ảnh hưởng đến khách hàng. Tuy nhiên, cũng đúng là bản sửa lỗi cho một vấn đề như vậy có thể được triển khai nhanh hơn nhiều.

6.4.7 Dịch vụ mây nhiều bên thuê

Vì tài nguyên mây như máy tính, bộ nhớ và mạng là tài nguyên tổng hợp được chia sẻ bởi nhiều CSC và/hoặc người thuê (xem 6.2.2), nên không thể cấp cho kiểm toán viên thương mại hoặc kiểm tra viên chính phủ quyền truy cập vật lý vào thiết bị cụ thể cho một CSC mà không có có khả năng vi phạm tính bảo mật của các CSC khác sử dụng cùng một tài nguyên được gộp chung. Một số dữ liệu có thể được trải rộng trên nhiều tài nguyên lưu trữ được chia sẻ bằng cách sử dụng "phân mảnh".

Trong mọi trường hợp, CSC kiểm soát dữ liệu của chính họ và CSP có thể không thể xem hoặc kiểm soát dữ liệu cụ thể trong kho dữ liệu mây của khách hàng, chẳng hạn như nếu dữ liệu đó được mã hóa.

Điều này cũng có nghĩa là việc xóa dữ liệu hoàn toàn an ninh, theo một số chính sách cũ hơn có thể yêu cầu phá hủy phương tiện lưu trữ, không thể thực hiện thường xuyên hoặc nhanh chóng như trong các hệ thống dành cho một khách hàng. Trong trường hợp dữ liệu của một khách hàng chỉ chiếm 10% dung lượng trên ổ đĩa, thì việc mất quyền sử dụng nó cho những khách hàng khác cho đến khi ổ đĩa đó không còn hoạt động sẽ không hiệu quả và kinh tế.

Xem 9.2.8.2, TCVN 13056:2020 (ISO/IEC 19944:2017),[3] để biết mô tả về cách tiếp cận phân lớp để xóa an ninh mà không yêu cầu phá hủy phương tiện.

Khi đề cập đến các vấn đề về điều tra hợp pháp, một lần nữa truy cập vật lý vào các tài nguyên được chia sẻ bởi một nhóm lớn người dùng không phải là cách tiếp cận thích hợp. Thay vào đó, cần phải có một cách tiếp cận theo hướng mây dựa vào khả năng của các dịch vụ mây để hỗ trợ điều tra và phá hủy. Trong nhiều trường hợp, dữ liệu nhật ký dựa trên mây cấp ứng dụng có thể cung cấp quyền truy cập phiên và chi tiết hoạt động để hỗ trợ kiểm tra, ghi nhật ký và pháp y.

6.4.8 Hàm ý về các hạn chế về địa lý

Các CSP với các hoạt động lớn hơn và toàn cầu, sẽ có nhiều cách tiếp cận khác nhau để lưu trữ dữ liệu tĩnh. Khi khách hàng chọn lưu trữ (hoặc tạo) dữ liệu, CSP cần đưa ra quyết định thông minh về nơi dữ liệu sẽ được lưu trữ thực tế. Những cân nhắc đi đến quyết định này bao gồm:

- Khách hàng hoặc các yêu cầu pháp lý hoặc chính sách.
- Dung lượng lưu trữ hiện có sẵn (ví dụ: với số lượng rất lớn).
- Hiệu suất lưu trữ (trung tâm dữ liệu gần nhất có thể rất bận do khách hàng khác, dẫn đến truy cập dữ liệu và băng thông chậm hơn so với khả năng có thể có từ một trung tâm dữ liệu ít tải hơn nhưng ở xa hơn).
- Chi phí bảo quản (bảo quản ở một số nơi có thể khiến CSP tốn kém hơn những nơi khác, ví dụ như do sự khác biệt về chi phí năng lượng hoặc chi phí vận hành khác).
- Khả năng và tính sẵn sàng của mạng (đôi khi có kết nối tốt hơn đến một địa điểm xa hơn là một địa phương) [4]
- Các CSC có thể phải tuân theo các chính sách và quy định về tính liên tục của doanh nghiệp (khôi phục sau thảm họa) yêu cầu họ duy trì các bản sao dự phòng về địa lý của dữ liệu. Ở các phạm vi thẩm quyền nhỏ hơn, có thể không cung cấp bộ nhớ địa lý dự phòng trong phạm vi phạm vi thẩm quyền. Thông thường người ta cũng yêu cầu rằng các nguồn lực địa dư thừa phải được đặt ở một khoảng cách thích hợp để ngăn chặn sự thất bại của cả nguồn tài nguyên chính và nguồn lực địa

[3] Tài liệu tham khảo hữu ích từ TCVN 13056 (ISO/IEC 19944) là Joel Reardon, David Basin, Srdjan Capkun, SOK: Xóa dữ liệu an toàn, Hội nghị chuyên đề IEEE về an ninh và quyền riêng tư, 2013, có sẵn http://www.ieee-security.org/TC/SP2013/papers/4977a301.pdf>.

[4] Ví dụ điển hình là một công ty trò chơi điện tử lớn đã tung ra dịch vụ nhạy cảm với độ trễ ở bờ biển phía đông Hoa Kỳ từ một trung tâm dữ liệu ở London, Anh chứ không phải dịch vụ hiện có của họ ở bờ biển phía tây Hoa Kỳ. Điều này là do kết nối xuyên Đại Tây Dương có độ trễ tốt hơn nhiều so với xuyên lục địa Hoa Kỳ.

dư thừa do các thảm họa tự nhiên và nhân tạo quy mô lớn.

- Nhiều CSC có nhân viên hiện trường, khách hàng, nhà cung cấp và/hoặc đối tác ở các nơi khác trên thế giới. Đối với những người dùng này, dữ liệu họ cần được lưu trữ cục bộ nhiều hơn có thể cải thiện hiệu suất của dịch vụ.
- Các CSC có thể chọn thu thập và xử lý dữ liệu ở cấp địa phương và hợp nhất dữ liệu từ các địa phương trong một cơ sở quy mô lớn hơn ở một phạm vi thẩm quyền khác. Điều này đôi khi được thực hiện để giảm lo ngại về độ trễ của mạng và đôi khi để giảm khối lượng dữ liệu cần được chuyển đến trung tâm dữ liệu trung tâm (ví dụ từ hàng nghìn ứng dụng di động, thiết bị IoT hoặc các nguồn thu thập dữ liệu khác).
- Giới hạn địa lý của dữ liệu không phải lúc nào cũng ngăn dữ liệu rời khỏi vị trí bị giới hạn vì hầu hết các lỗ hổng bảo mật đều được khai thác từ xa. Tài nguyên nội bộ và cấu hình sai dữ liệu theo cách thủ công cũng có thể gây ra mất dữ liệu; hai điều cuối cùng có thể được giảm thiểu trong một môi trường mây toàn cầu hiệu quả hơn.

Một số chính sách, cả chính phủ và doanh nghiệp, có thể yêu cầu một số hoặc tất cả dữ liệu được lưu trữ trong dịch vụ mây được lưu giữ thực tế trong một phạm vi thẩm quyền cụ thể.

Vì những lý do được đưa ra ở trên, dữ liệu bị hạn chế về mặt địa lý theo cách này có thể hơi tốn kém hơn khi lưu trữ do chi phí quản lý, hiệu quả lưu trữ kém hơn và cũng có thể bị giảm hiệu suất ứng dụng do độ trễ mạng hoặc tắc nghẽn băng thông.

Đối với các phạm vi thẩm quyền nhỏ hơn, có thể có rất ít CSP có trung tâm dữ liệu cục bộ. Ngay cả khi có một, có thể không có khả năng cung cấp dự phòng địa lý chỉ với một trung tâm dữ liệu duy nhất trong phạm vi thẩm quyền liên quan. Điều này có thể làm tăng tính dễ bị tổn thương đối với bất kỳ thảm họa cục bộ nào. Xem 6.3.10.

6.4.9 Sự cần thiết để phân hạng và phân loại dữ liệu dịch vụ mây

Các dịch vụ mây chứa một lượng lớn dữ liệu, thuộc về CSP và của khách hàng. Sẽ rất hữu ích khi phân loại dữ liệu để cải thiện việc sử dụng và quản lý. TCVN 12480 (ISO/IEC 17788) cung cấp ba danh mục cơ bản của dữ liệu mây, trong khi TCVN 13056 (ISO/IEC 19944) mở rộng các danh mục đó thành bốn danh mục cấp cao nhất và cũng cung cấp phân loại chi tiết cho nhiều danh mục con khác nhau.

Bốn danh mục cấp cao nhất như sau:

- Dữ liệu khách hàng Dịch vụ mây (được cung cấp hoặc tạo bởi chính CSC, chẳng hạn như tài liệu, cơ sở dữ liệu, thiết kế, danh sách khách hàng, hồ sơ nhân sự, v.v...)
- Dữ liệu nhà cung cấp dịch vụ mây (liên quan đến hoạt động của dịch vụ mây và không liên quan đến CSC, chẳng hạn như cấu hình thiết bị, tuyến mạng, hồ sơ bảo trì, danh sách nhân viên CSP, v.v...)
- Dữ liệu gốc từ dịch vụ mây (phát sinh từ việc khách hàng sử dụng dịch vụ mây, chẳng hạn như hồ sơ hoạt động của họ, nhật ký cuộc gọi, nhật ký kiểm tra, v.v...)
- Dữ liệu Tài khoản (chẳng hạn như thông tin liên hệ và thanh toán CSC)

Trên bất kỳ dịch vụ mây đã có, tất cả các danh mục này sẽ có mặt và tất cả đều có khả năng bao gồm một số PII cho mục đích của luật Bảo vệ dữ liệu và Sự riêng tư.

Cách tiếp cận chính sách áp dụng các quy tắc thích hợp cho các thể loại dữ liệu cụ thể, hạn chế và được xác định rõ ràng (chẳng hạn như các danh mục được liệt kê trong TCVN 13056 (ISO/IEC 19944)) cho phép quản lý dữ liệu hiệu quả hơn nhiều và do đó hiệu quả về chi phí của dịch vụ mây. Nó cũng làm cho nhiệm vụ kiểm toán tuân thủ rõ ràng hơn nhiều.

Đối với Bộ kiểm soát dữ liệu, việc tập trung các hạn chế thích hợp đối với dữ liệu có chứa PII sẽ tiết kiệm chi phí và hiệu quả hơn nhiều so với việc áp dụng kiểm soát rộng rãi cho các thể loại dữ liệu có khả năng chứa PII, vì như đã lưu ý ở trên, nhóm thứ hai lớn hơn rất nhiều.

(Ngược lại, Bộ xử lý dữ liệu thường không biết liệu bất kỳ dữ liệu nhất định nào có chứa bất kỳ PII nào hay không.)

Một ví dụ khác, đối với dữ liệu không phải PII, có sự khác biệt rất lớn trong việc xử lý phù hợp thông tin hiện tại, bí mật hoặc có giá trị và dữ liệu lỗi thời, công khai hoặc vô giá trị.

Xem thêm 6.4.1 về trách nhiệm của CSC và CSU trong việc đạt được sự đảm bảo về tính bảo mật của các dịch vụ mây để bảo vệ khu vực công và khối lượng công việc được quy định.

6.4.10 Tính liên tác và tính khả chuyển

Thứ nhất, điều quan trọng là phải hiểu rằng hai thuật ngữ này có ý nghĩa rất khác nhau và riêng biệt. Nói một cách dễ hiểu:

Tính liên tác là khả năng của hai hệ thống được kết nối để trao đổi thông tin và sử dụng lẫn nhau thông tin đã được trao đổi. Ví dụ PC và máy in có thể tương tác với nhau nếu PC có thể gửi tài liệu đến máy in để in và máy in có thể hiểu định dạng và nội dung của tài liệu.

Tính khả chuyển có hai dạng:

- Tính khả chuyển dữ liệu là nơi các đối tượng dữ liệu (như tài liệu, hình ảnh, tệp hoặc cơ sở dữ liệu) có thể được sao chép hoặc di chuyển từ hệ thống này sang hệ thống khác và vẫn có thể được sử dụng trên hệ thống thứ hai.
- Tính khả chuyển ứng dụng là nơi phần mềm thực thi có thể được sao chép hoặc di chuyển từ hệ thống này sang hệ thống khác, và vẫn có thể được sử dụng (chạy) trên hệ thống thứ hai.

Khả năng tương tác và tính khả chuyển là những chủ đề nhiều mặt rất phức tạp và các chi tiết được đề cập rộng rãi trong TCVN 13055 (ISO/IEC 19941).

6.4.10.1 Cân nhắc về tính liên tác trong môi trường tính toán mây

Điều 3.1.5, TCVN 12480:2019 (ISO/IEC 17788:2014), định nghĩa tính liên tác là khả năng hai hoặc nhiều hệ thống hoặc ứng dụng trao đổi thông tin và sử dụng thông tin đã được trao đổi lân nhau. Trong bối cảnh tính toán mây, tính liên tác được mô tả thêm như một khía cạnh xuyên suốt cung cấp khả năng cho hệ thống khách hàng sử dụng dịch vụ mây tương tác với dịch vụ mây và trao đổi thông tin theo một phương pháp quy định và thu được kết quả có thể dự đoán được (xem TCVN 12480:2019

(ISO/IEC 17788:2014), 6.6). Tính liên tác cũng bao gồm khả năng một dịch vụ mây tương tác với các dịch vụ mây khác (xem 8.5.5, TCVN 12481:2019 (ISO/IEC 17789:2014) và TCVN 13055 (ISO/IEC 19941)).

Tính liên tác và tính khả chuyển trong tính toán mây hiếm khi bị giới hạn trong một quyết định nhị phân là có thể hoặc không thể. Khả năng tương tác có khả năng chịu chi phí triển khai. Cần phải phân tích chi phí/lợi ích để xác định xem liệu các nguồn lực cần thiết để đảm bảo trao đổi thông tin theo phương pháp quy định trong khi thu được kết quả dự đoán có đáng giá hay không. Khả năng tương tác của các hệ thống của một CSC và các dịch vụ mây cũng như nhiều dịch vụ mây không chỉ là vấn đề đầu tư các nguồn lực để đảm bảo trao đổi thông tin giữa các giao diện ở hai đầu. Ngoài ra, bất kỳ thay đổi nào gây ra bởi các yêu cầu tương tác có thể đòi hỏi phải đào tạo thêm cho người dùng cuối, nhân viên quản lý và vận hành.

Các cân nhắc khi giải quyết tính liên tác mây gồm:

- khả năng của CSC tương tác với dịch vụ mây bằng cách trao đổi thông tin theo một phương pháp quy định để thu được kết quả có thể dự đoán được;
- khả năng dịch vụ mây hoạt động với các dịch vụ mây khác;
- các thuộc tính cần thiết để tạo điều kiện cho các tương tác thành công giữa các cơ sở Công nghệ thông tin và truyền thông của một tổ chức và dịch vụ mây;
- các vai trò và hoạt động như được định nghĩa trong TCVN 12481 (ISO/IEC 17789);
- các kiểu khả năng mây như được định nghĩa trong TCVN 12480 (ISO/IEC 17788);
- giao diện giữa các thành tố chức năng khác nhau được định nghĩa trong 9.2, TCVN 12481:2019 (ISO/IEC 17789:2014).

6.4.10.2 Cân nhắc về tính khả chuyển trong môi trường tính toán mây

Trong bối cảnh tính toán mây, tính khả chuyển đề cập đến khả năng của một CSC di chuyển và điều chỉnh phù hợp các ứng dụng và dữ liệu giữa các hệ thống của CSC và dịch vụ mây, giữa các mô hình triển khai mây khác nhau và giữa các dịch vụ mây của các CSP khác nhau. TCVN 13055 (ISO/IEC 19941) đưa ra những cân nhắc về tính khả chuyển ứng dụng mây và tính khả chuyển dữ liệu mây một cách riêng biệt.

Tính khả chuyển là "có thể chịu chi phí chuyển đổi". Cần phải phân tích chi phí/lợi ích để xác định xem việc chuyển các ứng dụng và/hoặc dữ liệu có đáng giá hay không. Do đó, điểm giống nhau của hệ thống CSC và CSP là vấn đề giảm chi phí chuyển đổi hơn là "cho phép" tính khả chuyển diễn ra, vì hầu hết mọi tính khả chuyển đều có thể thực hiện được nếu khách hàng sẵn sàng và có khả năng trả tiền cho nó. Mối quan tâm chuyển đổi không giới hạn ở chi phí; nó cũng thường liên quan đến một số rủi ro và thường kéo theo nỗ lực và thời gian của CSC và có thể là một khoảng thời gian gián đoạn dịch vụ.

Có nhiều cân nhắc khi giải quyết tính khả chuyển trong tính toán mây. Bao gồm:

- cho phép các CSC di chuyển các ứng dụng và dữ liệu để đáp ứng các nhu cầu kinh doanh như dịch vụ nhanh hơn, chi phí thấp hơn, độ tin cậy cao hơn hoặc nhu cầu khôi phục sau thảm họa;

- tính có sẵn rộng hơn của ứng dụng và dữ liệu cho phép tiếp cận thị trường rộng hơn;
- thời gian và nỗ lực cần thiết để chuyển cả ứng dụng và dữ liệu, tuy nhiên, chi phí đó có thể được giảm bớt bằng cách sử dụng các ngôn ngữ lập trình phổ biến, tiêu chuẩn, công cụ, khuôn khổ, mô hình, thời gian chạy và API;
- giới hạn các tình huống khóa trong đó CSC được liên kết với các dịch vụ mây của một CSP.

Nói chung, các CSP cố gắng cung cấp một số mức độ khả năng tương tác và tính khả chuyển giữa sản phẩm và sản phẩm của đối thủ cạnh tranh. Đây là lợi ích thương mại của riêng họ như một phương tiện để thuyết phục khách hàng tiềm năng. Tuy nhiên, không được đánh giá thấp những thách thức về kỹ thuật.

6.4.11 Tin cậy và minh bạch

Các CSP đã nhận ra rằng sự tin tưởng của khách hàng và cơ quan quản lý vào các dịch vụ mây là điều cần thiết cho sự thành công về mặt thương mại. Một định nghĩa về "dịch vụ mây đáng tin cậy" (có những dịch vụ khác) như sau:

dịch vụ mây đáng tin cậy: Dịch vụ mây đáp ứng một loạt các yêu cầu như tính minh bạch trong quản trị, quản lý và bảo mật để khách hàng sử dụng dịch vụ mây (CSC) có thể tin tưởng sử dụng dịch vụ mây. (Nguồn: ITU-T Y.3501, 2016).

CHÚ THÍCH 1 Tập các yêu cầu sẽ khác nhau tùy thuộc vào khách hàng sử dụng dịch vụ mây có liên quan, bản chất của dịch vụ mây và quyền hạn quản lý.

CHÚ THÍCH 2 Tập các yêu cầu cũng có thể liên quan đến các khía cạnh xuyên suốt bổ sung như hiệu suất, khả năng phục hồi, khả năng đảo ngược, SLA, v.v...

CHÚ THÍCH 3 Tính minh bạch có nghĩa là nhà cung cấp dịch vụ mây (CSP) phải cam kết với CSC rằng họ có các cơ chế kiểm soát và báo cáo phù hợp và rõ ràng để quản trị, quản lý và bảo mật, chẳng hạn như cam kết SLA, thông báo trực tuyến, chính sách xử lý dữ liệu, v.v...

Định nghĩa này cho thấy rõ ràng rằng sự tin tưởng bao gồm nhiều khía cạnh.

Tính minh bạch: Để được tin cậy, một CSP cần phải làm đúng, nhưng cũng cần được nhìn nhận để làm đúng. Điều này bao gồm những điều như tuân thủ các tiêu chuẩn, quy định và chính sách liên quan, thường được xác minh bằng chứng nhận và đánh giá (xem 6.4.13). Nó cũng có thể bao gồm việc cung cấp các tuyên bố và báo cáo ở các định dạng tiêu chuẩn ngành sử dụng các thuật ngữ tiêu chuẩn hóa (ví dụ: TCVN 12480 (ISO/IEC 17788), bộ ISO/IEC 19086[5], TCVN 13056 (ISO/IEC 19944), ISO/IEC 27017, ISO/IEC 27018) để khách hàng và cơ quan quản lý một cơ sở rõ ràng để so sánh và hiểu biết.

An ninh: Các CSP nên triển khai mức độ an ninh thích hợp cho dịch vụ đang được cung cấp. Đối với trò chơi trực tuyến dựa trên mây miễn phí để chơi, điều này có thể không nhiều, nhưng đối với bất kỳ dịch vụ nào xử lý thông tin nhận dạng cá nhân, đặc biệt là thông tin nhạy cảm như thông tin tài chính hoặc y tế, các yêu cầu an ninh sẽ cao hơn rất nhiều.

[5] Hiện nay, đã công bố TCVN 13054-1: 2020 (ISO/IEC 19086-1:2016) và TCVN 13054-3: 2020 (ISO/IEC 19086-3:2017).

Quản lý: Hệ thống quản lý dịch vụ mây phải có khả năng xử lý các yêu cầu của CSC và các nghĩa vụ tuân thủ khác nhau của CSP. Ví dụ không thể tin cậy một dịch vụ mây rất an ninh nhưng không thể ràng buộc dữ liệu khách hàng một cách chính xác ở (các) khu vực tài phán.

Quản trị: Một dịch vụ mây có khả năng an ninh tuyệt vời và quản lý hiệu quả vẫn chỉ đáng tin cậy như sự quản lý của tổ chức. Ví dụ một CSP mà Giám đốc điều hành có thể thực hiện các thay đổi đối với chính sách xử lý dữ liệu theo ý thích để đáp ứng cơ hội kinh doanh mới (ví dụ: bằng cách bán dữ liệu), không thể thực sự được gọi là đáng tin cậy. Tính minh bạch của quản trị có thể được giải quyết bằng chứng nhận tuân thủ các tiêu chuẩn trong lĩnh vực này, chẳng hạn như ISO/IEC 38500.

Như đã nêu trong Ghi chú ở trên, những khía cạnh này mang tính ngữ cảnh cao và sẽ rất khó nếu không muốn nói là không thể tạo ra một bộ tiêu chí hoặc quy định chung cho tất cả mọi người.

6.4.12 Các trường hợp ngoại lệ

Một số CSP có năng lực và nguồn lực lớn hơn trong việc duy trì và tồn tại các thảm họa quy mô lớn như động đất hoặc lũ lụt có thể làm hỏng một hoặc nhiều trung tâm dữ liệu hoặc cô lập chúng khỏi mạng. Tuy nhiên, khi chỉ có một cơ sở như vậy trong phạm vi thẩm quyền thì có thể thích hợp để xem xét tác động có thể xảy ra nếu nó bị ngừng hoạt động nghiêm trọng, cho dù nguyên nhân tự nhiên hay con người.

Nếu một chính sách yêu cầu dịch vụ mây hạn chế một số dữ liệu hoặc ứng dụng đối với phạm vi thẩm quyền địa phương (xem 6.4.8), thì có thể thích hợp để xem xét một khoản hỗ trợ cho các trường hợp ngoại lệ.

Trong mỗi trường hợp, tổ chức thiết lập chính sách cần đánh giá xem liệu có nên duy trì giới hạn địa lý tốt hơn, do đó gây rủi ro cho hoạt động kinh doanh liên tục hay không, hoặc liệu CSP có thể tiếp tục cung cấp dịch vụ từ một trung tâm dữ liệu ở phạm vi thẩm quyền khác cho đến khi dịch vụ bình thường có thể được tiếp tục hay không. Đây không phải là quyết định có thể được đưa ra sau khi thảm họa xảy ra, vì CSP sẽ cần phải thu xếp trước cho việc bàn giao trước khi trung tâm dữ liệu ban đầu bị mất hoặc bị cô lập. Ví dụ một CSP có thể cung cấp một cơ chế để lưu giữ các bản sao lưu dữ liệu được mã hóa ở một nơi khác trên thế giới, sao cho chúng chỉ có thể được giải mã và đưa vào sử dụng trong những trường hợp đặc biệt như vậy.

SLA mây nhằm mục đích hữu ích cho CSC và CSP để làm rõ các tiêu chí của các trường hợp ngoại lệ.

6.4.13 Tuân thủ, chứng nhận, đánh giá

Một số (mặc dù không phải tất cả) tiêu chuẩn về tính toán mây được thiết kế để sử dụng chứng nhận độc lập về CSP, hoặc thực sự là CSC [6]. Các chuẩn mực này cung cấp các tiêu chí rõ ràng để đánh giá viên có thể đo lường.

Có giá trị trong việc tận dụng các chứng nhận được quốc tế công nhận để tránh phải thực hiện lại công việc đánh giá theo các chế độ chứng nhận mới. Việc sử dụng lại công việc đã được thực hiện bởi một chuyên gia đánh giá được công nhận sẽ thúc đẩy một cách tiếp cận hài hòa trên toàn cầu.

[6] Lưu ý rằng không phải tất cả các tiêu chuẩn quốc tế đều phù hợp để chứng nhận. Ví dụ, một số mô tả thuật ngữ hoặc khái niệm tiêu chuẩn nhưng không bao gồm bất kỳ yêu cầu nào có thể được kiểm toán viên xác nhận.

Các ví dụ bao gồm TCVN TCVN ISO/IEC 27001:2019 (ISO/IEC 27001:2013) cùng với ISO/IEC 27017 và ISO/IEC 27018 bao gồm bảo mật dựa trên rủi ro của thông tin cá nhân được lưu trữ trên mây.

Một CSP tìm kiếm và đạt được chứng nhận theo các tiêu chuẩn này có thể chứng minh rằng họ đã được đánh giá và kiểm toán bởi các chuyên gia độc lập và có thể được tin cậy để tuân theo thực tiễn tốt nhất được tiêu chuẩn hóa (quốc tế) một cách chính xác.

Một khi chứng chỉ tuân thủ một tiêu chuẩn phù hợp được cấp, việc tuân thủ các yêu cầu liên tục được đảm bảo bằng các quy trình nội bộ và đánh giá định kỳ bên ngoài.

6.4.14 Những thách thức đối với việc áp dụng cho doanh nghiệp vừa và nhỏ (SME)

Việc các doanh nghiệp vừa và nhỏ (SME) áp dụng dịch vụ tính toán mây có cả lợi thế và thách thức.

Nhìn chung, các SME sử dụng dịch vụ mây được chia thành hai loại:

- Doanh nghiệp vừa và nhỏ không sử dụng CNTT;
- Doanh nghiệp vừa và nhỏ theo định hướng CNTT.

6.4.14.1 Các doanh nghiệp vừa và nhỏ phi CNTT

Thứ nhất, có những SME nơi dịch vụ CNTT phụ thuộc vào hoạt động kinh doanh thực tế của họ, ví dụ: nhà bán lẻ, nhà sản xuất nhỏ, trang trại, quan hệ đối tác, chuyên gia. Loại SME này có nhiều khả năng chọn các ứng dụng dựa trên mây được điều chỉnh (hoặc có thể tùy chỉnh) theo nhu cầu kinh doanh của riêng họ, chẳng hạn như các ứng dụng năng suất văn phòng chung (bộ xử lý công việc, bảng tính, lưu trữ tài liệu, kế toán, theo dõi chứng khoán, điện thoại). Ngoài ra, họ có thể sử dụng các ứng dụng chuyên biệt được thiết kế cho ngành cụ thể của họ, có thể được xây dựng bởi một đối tác dịch vụ mây (CSN - xem TCVN 12480 (ISO/IEC 17788)).

Đối với các SME này, tính toán mây làm giảm đáng kể nhu cầu sở hữu, quản lý và bảo mật phần mềm khác với phần mềm nằm trên máy tính để bàn của chính họ hoặc các thiết bị khác. Họ không bao giờ cần phải xem hoặc lo lắng về việc chạy hoặc bảo mật một máy chủ.

Thách thức chính thường là đạt được kết nối mạng đáng tin cậy và hiệu quả về chi phí (bao gồm đủ băng thông) với CSP. Điều này có thể đặc biệt khó khăn ở các vùng nông thôn (ngay cả ở các nước xây dựng cao) vì có thể chỉ có một nhà cung cấp dịch vụ mạng duy nhất với ít động lực đầu tư, hoặc có thể không có. Các doanh nghiệp vừa và nhỏ ở các nước đang xây dựng có thể bị thách thức đặc biệt trong vấn đề này. Các bản đồ đã xuất bản cho thấy tính sẵn sàng của băng thông rộng trên diện rộng đôi khi gây hiểu lầm vì chúng có thể bao gồm vùng phủ sóng di động như 3G và 4G thường không phù hợp hoặc quá đắt để sử dụng liên tục hàng ngày các dịch vụ mây cho doanh nghiệp SMB. Đối với nhân viên SME khi ra đường, việc sử dụng các điểm phát WiFi có thể hữu ích, nhưng ngay cả những điểm này cũng có thể gây khó chịu nếu không được thiết kế và bảo trì tốt.

Ngoài ra còn có những thách thức đối với các SME đang cố gắng tuân thủ các quy tắc bảo vệ dữ liệu và sự riêng tư, những người không đủ khả năng chi trả cho các chuyên gia tư vấn hoặc nhân viên chuyên môn đắt tiền để giải quyết vấn đề này. Thay vào đó, họ chủ yếu phải dựa vào lời khuyên và các tính năng do CSP cung cấp, điều này có thể dễ hiểu hoặc không dễ hiểu khi đáp ứng theo luật và quy

định địa phương. Tuy nhiên, các dịch vụ mây có thể cung cấp một lựa chọn tốt hơn so với phần mềm tại chỗ tương đương, vì nhiều khả năng CSP sẽ có quyền truy cập vào các kỹ năng phù hợp để đảm bảo tuân thủ hơn so với một tổ chức SME.

6.4.14.2 Doanh nghiệp vừa và nhỏ định hướng CNTT

Thứ hai, có các SME như các công ty khởi nghiệp theo định hướng CNTT chọn tính toán mây làm nền tảng để xây dựng hoạt động kinh doanh mới. Họ có thể tận dụng lợi thế của việc bắt đầu đầu tư vốn tối thiểu và sau đó xây dựng nhẹ nhàng hoặc nhanh chóng nếu cơ hội thị trường cho phép.

Một SME thành công thuộc loại này có thể nhanh chóng có được khách hàng dựa trên mây trên khắp thế giới và mang lại nguồn doanh thu xuất khẩu mạnh mẽ cho khu vực tài phán nội địa. Một số trong số các SME này có thể xây dựng thành những cường quốc về đổi mới và doanh thu, và thậm chí trở nên có ảnh hưởng trên toàn thế giới kinh doanh.

Mặc dù họ có nhiều khả năng sống ở các thành phố và do đó có khả năng tiếp cận băng thông rộng tốt hơn so với nhóm đầu tiên, nhưng họ có thể phải vật lộn với việc giải thích và dự đoán (các) mô hình kinh doanh mới có thể được các cơ quan quản lý hiểu và xử lý như thế nào, đặc biệt nếu cách tiếp cận được coi là phá vỡ các hoạt động kinh doanh hoặc các chuẩn mực xã hội hiện có.

6.4.14.3 Tác động của các chính sách kinh doanh lớn đối với các doanh nghiệp vừa và nhỏ

Cả hai loại SME đều có thể bị ảnh hưởng không cân đối bởi các chính sách được xây dựng chủ yếu xoay quanh việc quản lý các doanh nghiệp lớn.

Ví dụ một quy định mới có thể yêu cầu sự hỗ trợ của luật sư và nhà thầu chuyên về khoa học dữ liệu cho một doanh nghiệp lớn có 10.000 nhân viên cũng có thể yêu cầu luật sư và nhà thầu cho một doanh nghiệp mới thành lập có 5 nhân viên, điều này có thể vượt quá tài chính của SME hoặc khiến việc áp dụng tính toán mây không thể thực hiện được.

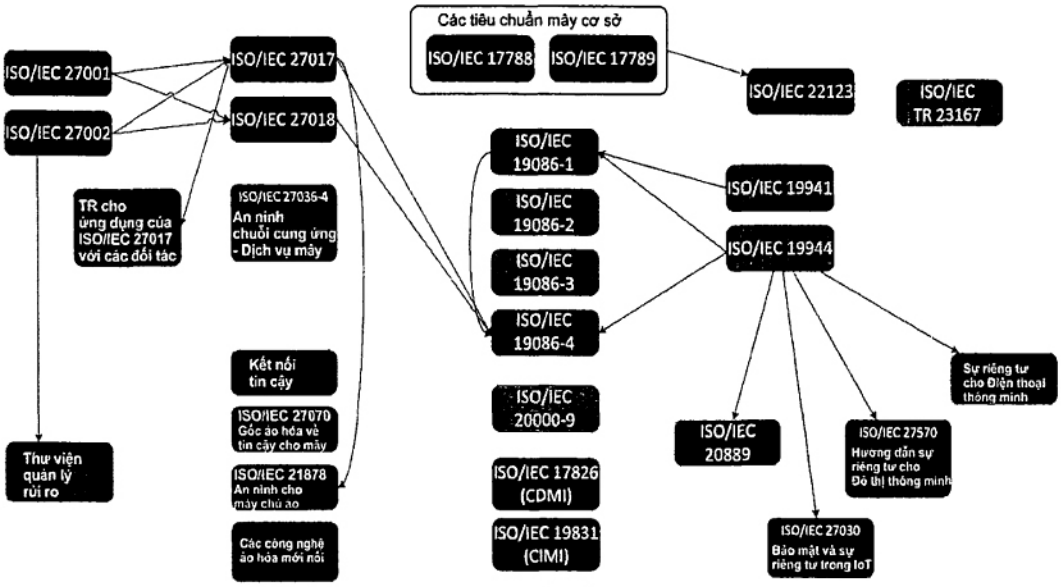
Bất kỳ tác động không cân xứng nào đối với các SME đều có thể gây ra hậu quả kinh tế nghiêm trọng ở bất kỳ nơi nào mà các SME chiếm một phần đáng kể trong cộng đồng doanh nghiệp địa phương. Mặc dù các CSP lớn ít bị ảnh hưởng trực tiếp hơn, nhưng sự mất mát của doanh nghiệp vừa và nhỏ tại địa phương cũng có thể ảnh hưởng tiêu cực đến các CSP lớn cung cấp (các) dịch vụ mây cho họ, do đó làm giảm giá trị của toàn bộ hệ sinh thái mây cục bộ và tước đi của một số người dân địa phương trong số các lợi ích được xác định ở trên.

7 Sử dụng các tiêu chuẩn để hỗ trợ xây dựng các chính sách bao gồm tính toán mây

7.1 Các tiêu chuẩn liên quan đến xây dựng chính sách tính toán mây

Các tiêu chuẩn được tạo ra bởi ISO/IEC JTC 1 thường được xây dựng dựa trên nhau, hoặc tối thiểu là tài liệu tham chiếu có trong các tiêu chuẩn khác. Điều quan trọng là phải hiểu mối quan hệ giữa các tiêu chuẩn như vậy, đặc biệt là khi nói đến những tiêu chuẩn liên quan đến tính toán mây. Bằng cách này, những người sử dụng các tiêu chuẩn như vậy có hiểu biết về cách họ có thể sử dụng chúng trong một bộ công cụ toàn diện. Ví dụ, Hình 1 dưới đây cho thấy cách các khuôn khổ quản lý rủi ro về sự riêng tư và an ninh nền tảng được xây dựng trong ISO/IEC JTC 1 SC 27 là cơ sở cho các tiêu chuẩn

dẫn xuất như ISO/IEC 27018 hoặc cách thức tiêu chuẩn ISO/IEC JTC 1 SC 38 của TCVN 13056 (ISO/IEC 19944) và TCVN 13055 (ISO/IEC 19941) bắt nguồn từ các tiêu chuẩn tính toán mây nền tảng TCVN 12480 (ISO/IEC 17788) và TCVN 12481 (ISO/IEC 17789), và lần lượt chúng được tham chiếu bởi các phần khác nhau của bộ ISO/IEC 19086, mô tả các thỏa thuận dịch vụ mây.



Hình 1 - Các tiêu chuẩn về tính toán mây

CHÚ THÍCH ISO/IEC 27070 đang được xây dựng (giai đoạn hiện tại: 10.99), ISO/IEC 27030 đang được xây dựng (giai đoạn hiện tại: 20.00), ISO/IEC 27570 đang được xây dựng (giai đoạn hiện tại: 20.00).

Bảng sau đây cung cấp mô tả ngắn gọn về từng tiêu chuẩn được thể hiện trong Hình 1.

Bảng 4 – Mô tả các tiêu chuẩn về tính toán mây

Tiêu chuẩn	Mô tả
TCVN 12480:2019 (ISO/IEC 17788:2014) *Information technology – Cloud computing – Overview and vocabulary* (Công nghệ thông tin – Tính toán mây – Tổng quan và từ vựng)	Cung cấp tổng quan về tính toán mây cùng với một tập các thuật ngữ và định nghĩa. Nó là một nền tảng thuật ngữ cho các tiêu chuẩn tính toán mây.
TCVN 12481:2019 (ISO/IEC 17789:2014) *Information technology – Cloud computing – Reference architecture* (Công nghệ thông tin – Tính toán mây – Kiến trúc tham chiếu)	Chỉ định kiến trúc tham chiếu tính toán mây (CCRA). Kiến trúc tham chiếu bao gồm các vai trò của tính toán mây, các hoạt động của tính toán mây và các thành tố chức năng của tính toán mây và các mối quan hệ của chúng.
ISO/IEC 19086-1:2016 *Information technology – Cloud computing – Service level agreement (SLA) framework – Part 1: Overview and concepts* (Công nghệ thông tin – Tính toán mây – Khung thỏa thuận mức dịch vụ (SLA) – Phần 1: Tổng quan và khái niệm)	Tìm cách thiết lập một tập các khối xây dựng SLA trên mây chung (khái niệm, thuật ngữ, định nghĩa, ngữ cảnh) có thể được sử dụng để tạo các Thỏa thuận mức dịch vụ (SLA) trên mây.
ISO/IEC 19086-2 *Cloud computing – Service level agreement (SLA) framework – Part 2: Metric model* (Tính toán mây – Khung thỏa thuận mức dịch vụ (SLA) – Phần 2: Mô hình số liệu)	Thiết lập thuật ngữ chung, xác định mô hình để xác định các chỉ số cho các Thỏa thuận mức dịch vụ mây (SLA) và bao gồm các ứng dụng của mô hình với các ví dụ. ISO/IEC 19086-2 thiết lập một thuật ngữ và cách tiếp cận chung để xác định các số liệu.
ISO/IEC 19086-3:2017	

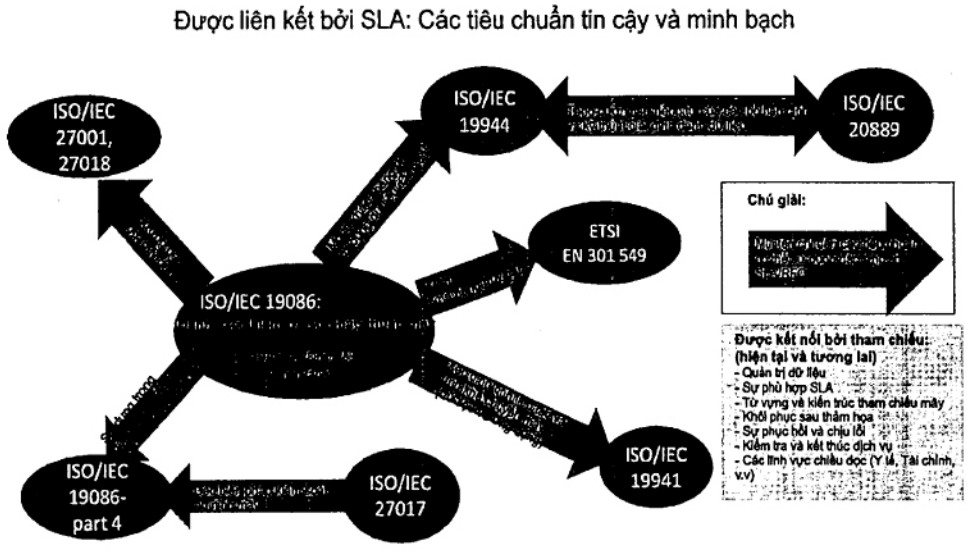
Tiêu chuẩn	Mô tả
Information technology – Cloud computing – Service level agreement (SLA) framework – Part 3: Core conformance requirements (Công nghệ thông tin – Tính toán mây - Khung thỏa thuận mức dịch vụ (SLA) – Phần 3: Các yêu cầu tuân thủ chủ yếu)	Chỉ định các yêu cầu tuân thủ chủ yếu đối với các thỏa thuận mức dịch vụ (SLA) cho các dịch vụ mây dựa trên ISO/IEC 19086-1 và hướng dẫn về các yêu cầu tuân thủ chủ yếu. Tiêu chuẩn này dành cho lợi ích của cả nhà cung cấp dịch vụ mây và khách hàng sử dụng dịch vụ mây.
ISO/IEC 19086-4 *Cloud computing – Service level agreement (SLA) framework – Part 4: Security and privacy* (Tính toán mây – Khung thỏa thuận mức dịch vụ (SLA) – Phần 4: An ninh và sự riêng tư)	Chỉ định an ninh và bảo vệ các thành tố thông tin nhận dạng cá nhân, các SLO và SQO cho các thỏa thuận mức dịch vụ mây (SLA mây) bao gồm các yêu cầu và hướng dẫn.
ISO/IEC 19941:2017 *Information technology – Cloud computing – Interoperability and portability* (Công nghệ thông tin – Tính toán mây – Khả năng tương tác và tính khả chuyển)	Chỉ định các loại tính liên tác và tính khả chuyển của tính toán mây, mối quan hệ và tương tác giữa hai khía cạnh xuyên suốt này của tính toán mây và các thuật ngữ và khái niệm phổ biến được sử dụng để thảo luận về khả năng tương tác và tính khả chuyển, đặc biệt liên quan đến các dịch vụ mây.
TCVN 13056 (ISO/IEC 19944):2017 *Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use* (Công nghệ thông tin – Tính toán mây – Dịch vụ và thiết bị mây: Luồng dữ liệu, thể loại dữ liệu và sử dụng dữ liệu)	Đặt tên và mô tả các thể loại dữ liệu, luồng dữ liệu giữa thiết bị và dịch vụ mây hỗ trợ cũng như cách mô tả việc sử dụng các thể loại dữ liệu khác nhau của CSP.
TCVN ISO/IEC 27001:2019 (ISO/IEC 27001:2013):2013 *Information technology – Security techniques – Information security management systems – Requirements* (Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin – Các yêu cầu)	Chỉ rõ các yêu cầu để thiết lập, thực hiện, duy trì và cải tiến liên tục hệ thống quản lý an toàn thông tin trong bối cảnh của tổ chức. Nó cũng bao gồm các yêu cầu về đánh giá và xử lý các rủi ro an toàn thông tin phù hợp với nhu cầu của tổ chức. Các yêu cầu đặt ra trong TCVN ISO/IEC 27001:2019 (ISO/IEC 27001:2013) là chung và nhằm áp dụng cho tất cả các tổ chức, bất kể loại hình, quy mô hay tính chất.
ISO/IEC 27002:2013 *Information technology – Security techniques – Code of practice for information security controls* (Công nghệ thông tin – Các kỹ thuật an toàn – Quy tắc thực hành về kiểm soát an toàn thông tin)	Đưa ra các hướng dẫn về các tiêu chuẩn an toàn thông tin của tổ chức và các thông lệ quản lý an toàn thông tin bao gồm việc lựa chọn, thực hiện và quản lý các biện pháp kiểm soát có tính đến (các) môi trường rủi ro về an toàn thông tin của tổ chức.
ISO/IEC 27017:2015 *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services* (Công nghệ thông tin – Các kỹ thuật an toàn – Quy tắc thực hành thông tin kiểm soát bảo mật dựa trên ISO/IEC 27002 cho các dịch vụ mây)	Cung cấp các hướng dẫn về kiểm soát an toàn thông tin áp dụng cho việc cung cấp và sử dụng các dịch vụ mây bằng cách cung cấp: - hướng dẫn thực hiện bổ sung đối với các biện pháp kiểm soát liên quan được quy định trong ISO/IEC 27002; - kiểm soát bổ sung với hướng dẫn triển khai liên quan cụ thể đến các dịch vụ mây.
ISO/IEC 27018 *Information technology – Security techniques – Code of practice for protection of per- sonally identifiable information (PII) in public clouds acting as PII processors* (Công nghệ thông tin – Bảo mật kỹ thuật – Quy tắc thực hành để bảo vệ thông tin nhận dạng đặc biệt (PII) trong các mây công cộng hoạt động như bộ xử lý PII)	Thiết lập các mục tiêu, quy trình và hướng dẫn kiểm soát được chấp nhận phổ biến để thực hiện các biện pháp bảo vệ Thông tin nhận dạng cá nhân (PII) phù hợp với các nguyên tắc bảo mật trong ISO/IEC 29100 cho môi trường tính toán mây công cộng.
ISO/IEC 20889 *Privacy enhancing data de-identification techniques* (Các kỹ thuật khử nhận dạng dữ	Cung cấp mô tả về các kỹ thuật khử định danh dữ liệu nâng cao sự riêng tư, được sử dụng để mô tả và thiết kế các biện pháp khử nhận dạng phù hợp với các

Tiêu chuẩn	Mô tả
liệu nâng cao sự riêng tư)	nguyên tắc về sự riêng tư trong ISO/IEC 29100. Đặc biệt, tiêu chuẩn này quy định thuật ngữ, phân loại các kỹ thuật khử nhận dạng theo đặc điểm của chúng và khả năng áp dụng của chúng để giảm rủi ro nhận dạng lại.
ISO/IEC 27036-4:2016 *Information technology – Security techniques – Information security for supplier rela-tionships – Part 4: Guidelines for security of cloud services* (Công nghệ thông tin – Bảo mật kỹ thuật – Bảo mật thông tin cho mối quan hệ với nhà cung cấp – Phần 4: Hướng dẫn bảo mật các dịch vụ mây)	Cung cấp cho khách hàng dịch vụ mây và nhà cung cấp dịch vụ mây với hướng dẫn về a) có được tầm nhìn về các rủi ro bảo mật thông tin liên quan đến việc sử dụng các dịch vụ mây và quản lý những rủi ro đó một cách hiệu quả, b) và ứng phó với các rủi ro cụ thể đối với việc mua lại hoặc cung cấp các dịch vụ mây có thể có tác động đến bảo mật thông tin đối với các tổ chức sử dụng các dịch vụ này.

7.1.1 Bộ tiêu chuẩn ISO/IEC 19086[7] áp dụng đối với sự tin cậy và minh bạch

Các tiêu chuẩn tính toán mây được tạo ra trong ISO/IEC JTC1 có thể được xem là liên quan đến nhau từ quan điểm của các Thỏa thuận mức dịch vụ mây (SLA). Bộ tiêu chuẩn ISO/IEC 19086 mô tả Mục tiêu mức dịch vụ mây (SLO) và Mục tiêu chất lượng dịch vụ mây (SQO) là các cấu phần của thỏa thuận dịch vụ mây. Các SLO hoặc SQO như vậy thường được mô tả bằng cách tham chiếu đến các tiêu chuẩn tính toán mây trước đây, chẳng hạn như ISO/IEC 27018 cho các chủ đề liên quan đến bộ xử lý mây công cộng hoặc TCVN 13056 (ISO/IEC 19944) cho SLO quản lý dữ liệu hoặc SQO cần xây dựng dựa trên phân loại dữ liệu và các tuyên bố sử dụng.

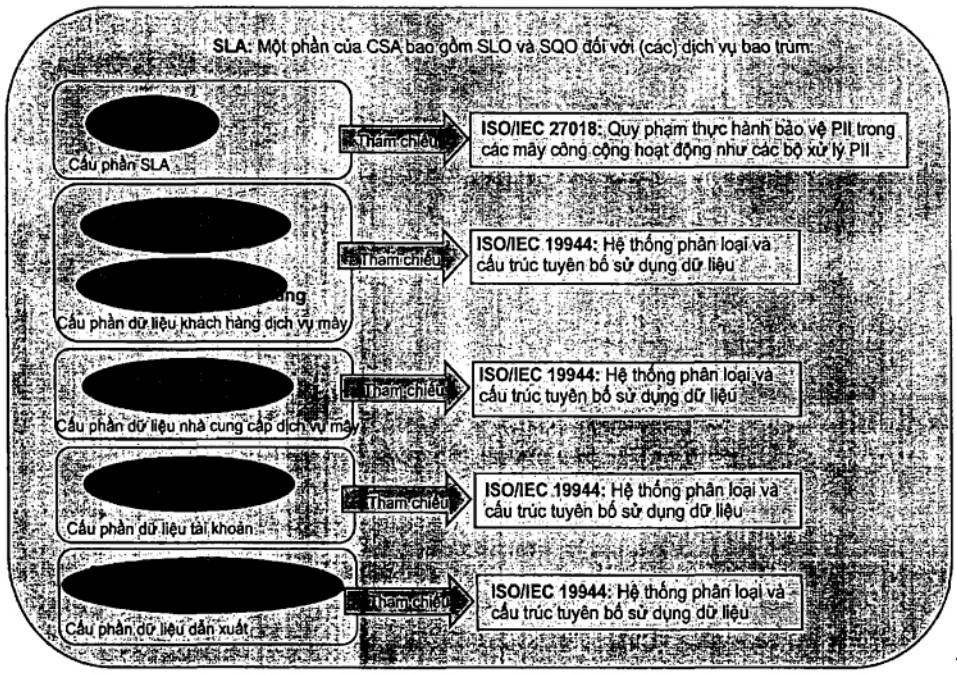
Hình 2 mô tả cách bộ tiêu chuẩn ISO/IEC 19086 tham chiếu các tiêu chuẩn khác. Sẽ rất hữu ích khi xem các tiêu chuẩn tính toán mây khác nhau được liên kết với nhau như thế nào từ quan điểm của các thỏa thuận dịch vụ mây.



Hình 2 - Các tiêu chuẩn liên quan đến Thỏa thuận mức dịch vụ (SLA)

[7] Hiện nay, đã công bố TCVN 13054-1: 2020 (ISO/IEC 19086-1:2016) và TCVN 13054-3: 2020 (ISO/IEC 19086-3:2017).

Hình 3 cho thấy một vài ví dụ về các SQO trích dẫn các tiêu chuẩn ISO/IEC JTC1 khác như TCVN 13056 (ISO/IEC 19944) trong các lĩnh vực phân loại dữ liệu và tuyên bố sử dụng, cũng như ISO/IEC 27018 để bảo vệ PII bởi nhà điều hành mây công cộng hoạt động như Bộ xử lý PII. Việc sử dụng các tiêu chuẩn có liên quan như vậy tạo điều kiện thuận lợi cho việc tạo ra các thỏa thuận dịch vụ mây dựa trên các khái niệm và thuật ngữ đồng thuận được quốc tế công nhận, cho phép các mối quan hệ có cấu trúc và hiệu quả hơn giữa các nhà cung cấp dịch vụ mây, khách hàng dịch vụ mây và các cơ quan quản lý.

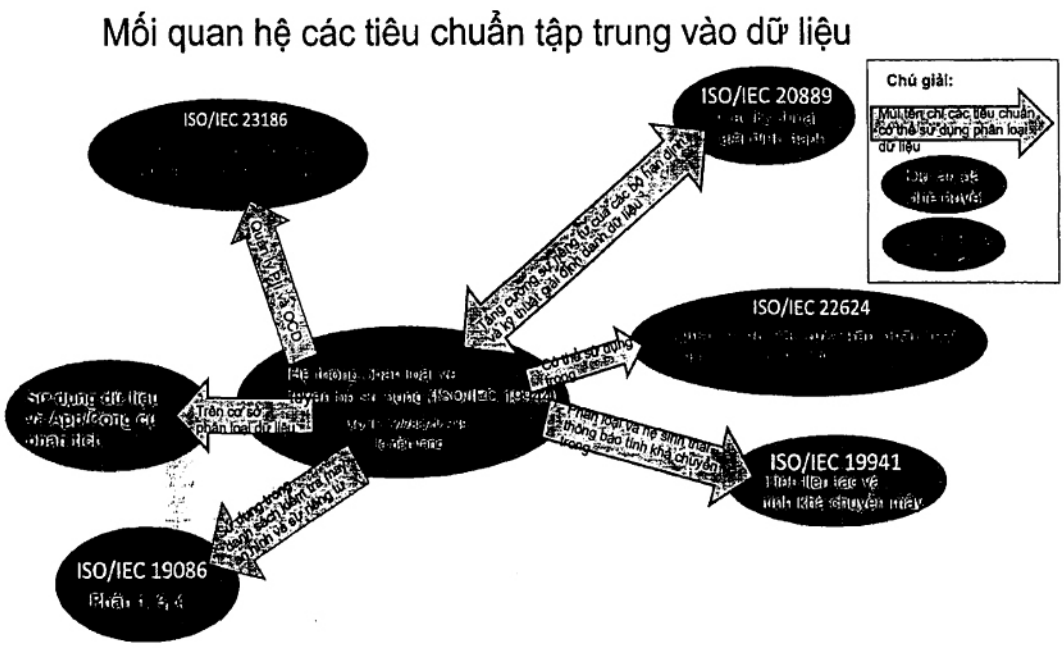


Hình 3 - Ví dụ về các SQO tham chiếu các tiêu chuẩn khác trong bộ tiêu chuẩn ISO/IEC 19086

7.1.2 TCVN 13056 (ISO/IEC 19944) có thể áp dụng để làm rõ các khái niệm dữ liệu

Một bản đồ quan hệ giữa các mối quan hệ và sự phụ thuộc tương tự có thể được thiết lập cho các tiêu chuẩn lấy dữ liệu làm trung tâm. Cốt lõi là TCVN 13056 (ISO/IEC 19944) dựa trên các tiêu chuẩn tính toán mây nền tảng TCVN 12480 (ISO/IEC 17788) và TCVN 12481 (ISO/IEC 17789). TCVN 13056 (ISO/IEC 19944) đã được sử dụng bởi các dự án khác trong JTC1, chẳng hạn như các thỏa thuận cấp độ dịch vụ (bộ ISO/IEC 19086), khử nhận dạng dữ liệu (ISO/IEC 20889, tính khả chuyển của dữ liệu (như được đề cập trong TCVN 13055 (ISO/IEC 19941)).

Hiểu được mối quan hệ giữa các bên này có thể hữu ích cho các nhà hoạch định chính sách công và doanh nghiệp, các bên cần đưa ra các chính sách và thực tiễn sử dụng các khái niệm được mô tả trong đó.



Hình 4 - Các tiêu chuẩn liên quan đến dữ liệu mây

7.1.3 ISO/IEC 27552 [8], Hệ thống quản lý thông tin riêng tư

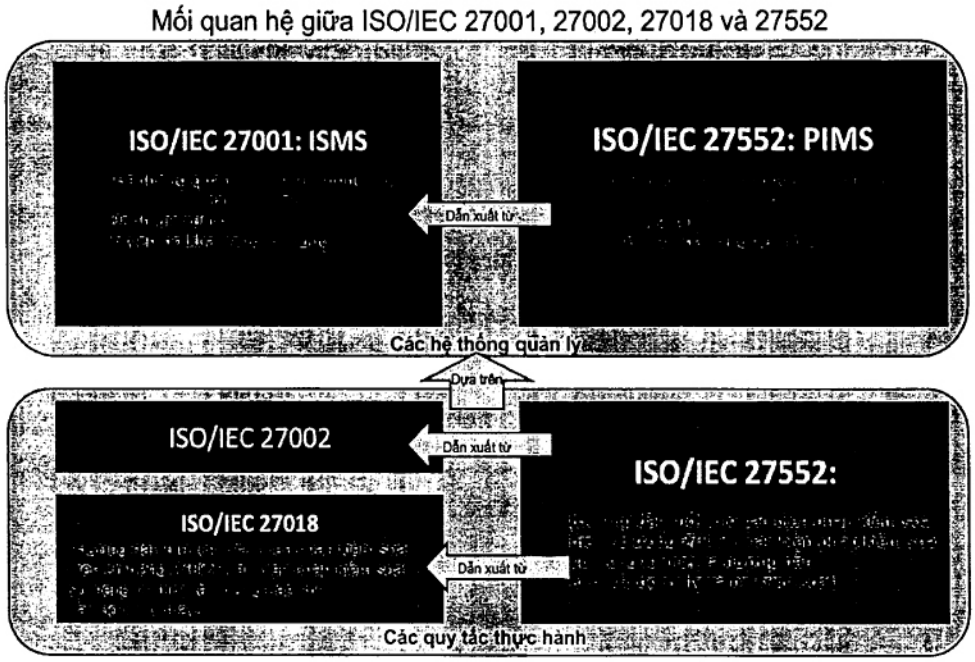
ISO/IEC 27552 là phần mở rộng của TCVN ISO/IEC 27001:2019 (ISO/IEC 27001:2013) (Hệ thống quản lý an toàn thông tin) cũng như TCVN ISO/IEC 27002 (Quy tắc thực hành). Đặc biệt, nó chứa các biện pháp kiểm soát phù hợp với bộ kiểm soát PII và bộ xử lý PII (bao gồm bộ kiểm soát và bộ xử lý tính toán mây). ISO/IEC 27552 mở rộng ISMS bằng cách yêu cầu rõ ràng rằng quá trình xử lý PII phải được xem xét trong phạm vi của ISMS và tính riêng tư phải được tính đến các bên quan tâm, rủi ro, nghĩa vụ, v.v...

ISO/IEC 27552 phù hợp để đáp ứng các nghĩa vụ của các quy định bảo vệ dữ liệu hiện đại. ISO/IEC 27552 nhằm phục vụ như một cơ chế đảm bảo trong mối quan hệ người kiểm soát/người xử lý, đồng thời là nguồn cung cấp bằng chứng có thể hữu ích cho các cơ quan giám sát.

Nó cũng có thể đóng vai trò là nền tảng cho chứng nhận thông tin về sự riêng tư, giống như cách mà TCVN ISO/IEC 27001:2019 (ISO/IEC 27001:2013) và ISO/IEC 27002 đóng vai trò là nền tảng cho chứng nhận bảo mật thông tin.

Hình 5 mô tả cách ISO/IEC 27552 đã được bắt nguồn từ tiêu chuẩn hiện có về hệ thống quản lý an toàn thông tin (TCVN ISO/IEC 27001:2019 (ISO/IEC 27001:2013)) và cách thức các biện pháp kiểm soát sự riêng tư đã được xây dựng trong mối quan hệ và cấu thành với các biện pháp kiểm soát bảo mật và sự riêng tư hiện có tiêu chuẩn về quy phạm nghề nghiệp.

[8] Đang xây dựng. Giai đoạn hiện tại: 40.00.



Hình 5 - Các tiêu chuẩn liên quan đến an toàn và sự riêng tư trong tính toán mây

Tương tự như các tiêu chuẩn ISO/IEC JTC1 khác, ISO/IEC 27552 xây dựng dựa trên các tiêu chuẩn hiện có như được mô tả trong Hình 5 và viện dẫn các tiêu chuẩn tính toán mây khác như TCVN 13056 (ISO/IEC 19944) và ISO/IEC 20889 vì chúng chứa phân loại dữ liệu và biểu thức sử dụng dữ liệu, cũng như các kỹ thuật loại bỏ nhận dạng có thể được sử dụng trong các diễn đạt, thực hành và chứng nhận chính sách liên quan đến sự riêng tư.

7.2 Các tiêu chuẩn, đặc tả và tài liệu quan trọng khác

Các tiêu chuẩn về tính toán mây được xác định trong 7.1 phù hợp với một bộ sưu tập các tiêu chuẩn và đặc tả rộng hơn, nhiều tiêu chuẩn trong số đó cũng có thể hữu ích khi xây dựng chính sách tính toán mây. Có thể tìm thấy danh sách không đầy đủ các tiêu chuẩn và đặc tả bổ sung như vậy trong Phụ lục B.

8 Các cân nhắc khi xây dựng chính sách

8.1 Các cân nhắc về chính sách điều tiết

Sau đây là những cân nhắc hợp lệ khi xây dựng chính sách sẽ được ủy quyền hợp pháp về việc triển khai, cung cấp hoặc sử dụng các dịch vụ mây trong một khu vực tài phán.

Việc đánh số không hàm ý bất kỳ hình thức ưu tiên hoặc ưu tiên nào.

8.1.1 Quy định chung

Các CSP thường cung cấp một lượng đáng kể tài liệu cho khách hàng, đối tác và cơ quan quản lý. Do đó, không thể là nguyên nhân khác biệt với sự đồng thuận quốc tế về cách mô tả các hệ thống tính toán mây.

1) Chính sách này có sử dụng hoặc định nghĩa các thuật ngữ tính toán mây theo cách mâu thuẫn với

các định nghĩa được cung cấp trong các tiêu chuẩn (xem 6.2 và TCVN 12480 (ISO/IEC 17788), TCVN 12481 (ISO/IEC 17789)) không?

2) Chính sách này có luôn tham chiếu đến các tiêu chuẩn về các định nghĩa nếu có thể hay không (xem 6.2)?

3) Chính sách này có tránh hoặc giảm thiểu các hậu quả kỹ thuật không mong muốn bằng cách cho phép tham vấn ngành hợp lý trước khi thay đổi chính sách không?

4) Chính sách này có bất kỳ ràng buộc nào về thời gian và giới hạn thời gian thực hiện không? Những điều này có phù hợp với những thách thức kỹ thuật để thực hiện các yêu cầu không?

8.1.2 Các vấn đề về nhiều bên thuê

Như được mô tả trong 6.4.7 ở trên, các dịch vụ mây đạt được tính kinh tế về quy mô và chi phí bằng cách chia sẻ tài nguyên giữa nhiều khách hàng/người thuê.

Những điều sau đây đối với nhiều bên thuê cần được xem xét:

1) Chính sách này có yêu cầu các CSP cấp quyền truy cập vật lý vào dữ liệu hoặc hệ thống của các quan chức chính phủ không?

   a) Nếu vậy, nó bảo vệ các quyền (ví dụ: tính bảo mật, tính toàn vẹn, tính sẵn sàng) của các bên thuê dịch vụ mây khác được lưu trữ trên cùng hệ thống vật lý hoặc kho dữ liệu như mục tiêu (xem 6.4.7) như thế nào?

2) Chính sách này có bao gồm việc xóa dữ liệu không?

   a) Nếu vậy, nó có tính đến nhu cầu của những người thuê khác có dữ liệu nằm trên cùng một phương tiện lưu trữ (xem 6.4.7) không?

3) Có tính đến chi phí tài chính khi tiêu hủy các phương tiện lưu trữ còn sống trước khi kết thúc vòng đời hoạt động của nó không (xem 6.4.3)?

4) Chính sách này có bao gồm quyền của các CSC trong việc truy xuất dữ liệu từ CSP không?

   a) Nếu vậy, chính sách này có tính đến việc xử lý PII về những người khác có thể được nhúng trong dữ liệu đó không?

8.1.3 Tránh các rào cản không cần thiết đối với việc sử dụng mây

Các chính sách ban đầu được xây dựng để điều chỉnh các hệ thống tính toán tại chỗ hoặc các hệ thống được lưu trữ cục bộ đôi khi có thể đóng vai trò là trở ngại cho việc triển khai các kiến trúc tính toán mây hiệu quả.

Những điều sau đây cần được xem xét:

1) Chính sách này có bao gồm các giả định ngầm định hoặc các yêu cầu rõ ràng về nhân viên CSP, chẳng hạn như quốc tịch hoặc vị trí (xem 6.4.2)?

2) Chính sách có yêu cầu (các) trình độ chuyên môn cụ thể của nhân viên địa phương hoặc (các) giải phóng mặt bằng có thể gây khó khăn hoặc không thể điều hành hoặc quản lý bởi nhân viên CSP ở

phạm vi thẩm quyền khác (xem 6.4.2)?

3) Chính sách này có hạn chế khả năng của CSP trong việc di chuyển dữ liệu của nhà cung cấp dịch vụ mây (xem TCVN 13056 (ISO/IEC 19944)) giữa các phạm vi thẩm quyền (xem 6.4.2, 6.4.3)?

4) Chính sách này có hạn chế vị trí lưu trữ của dữ liệu khách hàng sử dụng dịch vụ mây hoặc dữ liệu có nguồn gốc trong một phạm vi thẩm quyền cụ thể (xem 6.4.2)?

   a) Nếu vậy, ràng buộc này có áp dụng cho tất cả dữ liệu đó hay cho một tập hợp con các thể loại dữ liệu đã xác định không?

   b) Nếu sau này, các thể loại dữ liệu này có dựa trên phân loại dữ liệu được định nghĩa trong TCVN 13056 (ISO/IEC 19944) không?

5) Nếu chính sách bao gồm các ràng buộc về vị trí dữ liệu, thì chính sách có cho phép các ngoại lệ hoạt động trong các trường hợp đặc biệt, ví dụ: duy trì dịch vụ mây hoạt động trong trường hợp khẩn cấp lớn ảnh hưởng đến (các) trung tâm dữ liệu mây cục bộ không?

   Chính sách này có phù hợp với các tiêu chuẩn về quản trị CNTT (xem ISO/IEC 38500) không?

6) Chính sách này có cho phép phát triển liên tục các dịch vụ mây và các ứng dụng được kết nối không (xem 6.4.6)?

7) Chính sách có cho phép tạo mẫu, xây dựng, thử nghiệm và triển khai liên tục không?

8) Chính sách có khuyến khích hoặc ngăn cản các CSP và CSC luôn cập nhật hệ thống không?

9) Chính sách có yêu cầu chứng nhận lại hoặc phê duyệt lại khi phần mềm được thay đổi không?

   a) Nếu vậy, có bao nhiêu thay đổi được phép trước khi chứng nhận lại hoặc phê duyệt lại?

8.1.4 Tin cậy và minh bạch

Các CSC cần tin tưởng CSP và kinh nghiệm cho thấy rằng sự tin tưởng được thiết lập và duy trì tốt nhất bằng cách trung thực và minh bạch về (các) dịch vụ được cung cấp và hoạt động.

Những điều sau đây cần được xem xét:

1) Chính sách này có khuyến khích hoặc bắt buộc sử dụng thuật ngữ dựa trên tiêu chuẩn trong việc mô tả các dịch vụ tính toán trực tuyến (dựa trên mây hay cách khác) không?

2) Chính sách này có ngăn cản hoặc cấm sử dụng các thuật ngữ như "mây" hoặc "tính toán mây" để mô tả các dịch vụ không đáp ứng định nghĩa tiêu chuẩn về tính toán mây, được định nghĩa trong TCVN 12480 (ISO/IEC 17788) (thông lệ được gọi là "tẩy rửa mây")?

3) Chính sách này có bắt buộc phải thông báo cho CSC về cách CSP sẽ sử dụng dữ liệu khách hàng hoặc dữ liệu thu được không?

   a) Nếu vậy, chính sách có bắt buộc hoặc khuyến khích CSP thực hiện các tuyên bố sử dụng dữ liệu được xây dựng theo phương pháp tiêu chuẩn được xác định trong TCVN 13056 (ISO/IEC 19944) không?

4) Chính sách này có yêu cầu sử dụng thuật ngữ tiêu chuẩn trong các thỏa thuận dịch vụ tính toán

mây hoặc thỏa thuận mức dịch vụ (SLA) không?

a) Nếu vậy, chính sách có tuân theo thuật ngữ và khuôn khổ tiêu chuẩn được xác định trong loạt tiêu chuẩn ISO/IEC 19086 không?

8.1.5 Tính liên tác và tính khả chuyển

Tính liên tác và tính khả chuyển là những vấn đề quan trọng đối với CSC và đối với các cơ quan quản lý, đặc biệt là đối với những người liên quan đến sự cạnh tranh giữa các nhà cung cấp dịch vụ. Tuy nhiên, đây là một chủ đề rất phức tạp và cần được xử lý cẩn thận.

Những điều sau đây cần được xem xét:

1) Chính sách này có bao gồm các vấn đề về tính liên tác hoặc tính khả chuyển không?
2) Chính sách này có làm rõ sự khác biệt giữa (xem TCVN 13055 (ISO/IEC 19941)):
   a) Tính liên tác
   b) Tính khả chuyển dữ liệu
   c) Tính khả chuyển ứng dụng
3) Chính sách này có yêu cầu các khía cạnh cụ thể của tính liên tác hoặc tính khả chuyển không?
   a) Nếu vậy, các khía cạnh này có phù hợp với hoặc được xác định bằng cách sử dụng các khía cạnh được xác định trong TCVN 13055 (ISO/IEC 19941) không?
4) Chính sách này có yêu cầu khả năng tương tác trực tiếp (xem TCVN 13055 (ISO/IEC 19941)) hay nó cũng cho phép sử dụng:
   a) Bộ chuyển đổi giao thức
   b) Các định dạng trung gian
   c) Các công cụ chuyển đổi dữ liệu của bên thứ ba (ví dụ: nguồn mở)
   d) Các giải pháp khác
5) Chính sách này có yêu cầu khả năng di chuyển dữ liệu trực tiếp không hay nó cũng cho phép sử dụng:
   a) Các định dạng trung gian
   b) Bộ điều hợp của bên thứ ba (ví dụ: nguồn mở)
   c) Các giải pháp khác
6) Chính sách này có yêu cầu tính khả chuyển ứng dụng trực tiếp không, hay nó cũng cho phép sử dụng:
   a) Trình giả lập
   b) Chuyển đổi mã ứng dụng
   c) Các giải pháp khác

8.1.6 An ninh và riêng tư

Tin tưởng an toàn thông tin và bảo vệ thông tin cá nhân trong các dịch vụ mây là điều kiện tiên quyết cần thiết để áp dụng thành công các công nghệ tính toán mây.

Những điều sau đây cần được xem xét:

1) Chính sách này có áp đặt các yêu cầu về an ninh cụ thể đối với các nhà cung cấp dịch vụ mây và khách hàng sử dụng dịch vụ mây không?
2) Chính sách này có thừa nhận khái niệm về trách nhiệm chung giữa nhà cung cấp dịch vụ mây và khách hàng sử dụng dịch vụ mây trong việc giữ dữ liệu an ninh và riêng tư không?
3) Chính sách này có cho phép và khuyến khích những tiến bộ trong công nghệ và các kỹ thuật an toàn khi các mối đe dọa mới xuất hiện không?
4) Chính sách này có cho phép hoặc thúc đẩy việc sử dụng mã hóa dữ liệu mạnh mẽ khi ở trạng thái nghỉ và khi đang di chuyển không?
5) Chính sách này có cho phép sử dụng các phương pháp tiếp cận quản lý rủi ro được ngành công nghiệp tin cậy cho an ninh và riêng tư như các phương pháp được mô tả trong TCVN ISO/IEC 27001:2019 (ISO/IEC 27001:2013), ISO/IEC 27017, ISO/IEC 27018 và ISO/IEC 27552 không?

8.2 Cân nhắc về chính sách tư vấn

8.2.1 Quy định chung

Điều này bao gồm các cân nhắc có liên quan khi xây dựng chính sách tư vấn hoặc khuyến nghị việc sử dụng tính toán mây nhưng không đặt ra các yêu cầu bắt buộc.

Ví dụ về các chính sách như vậy sẽ là nơi chính phủ quốc gia cung cấp các hướng dẫn và khuyến nghị về việc sử dụng các dịch vụ mây cho chính quyền địa phương hoặc cho các cơ quan chính phủ, mặc dù các quyết định cuối cùng về việc (và cách thức) sử dụng dịch vụ mây được để cho các cơ quan đó, theo như https://www.gov.uk/go Government/news/go Government-adopts-cloud-first-policy-for-public-sector-it.

Những điều sau đây cần được xem xét khi xây dựng chính sách cung cấp lời khuyên và/hoặc hướng dẫn về việc triển khai, cung cấp hoặc sử dụng các dịch vụ mây trong phạm vi thẩm quyền.

Việc đánh số không hàm ý bất kỳ hình thức đặc quyền hoặc ưu tiên nào.

8.2.2 Thúc đẩy việc chấp thuận công nghệ mây

Nhiều chính phủ nhận thấy những lợi thế đối với doanh nghiệp, xã hội và môi trường từ việc chuyển sang các phương pháp tiếp cận tính toán mây phù hợp với CNTT, như được xác định trong 6.3 ở trên, và thường sẽ tư vấn cho chính quyền địa phương và các cơ quan tương ứng.

Những điều sau đây cần được xem xét:

1) Chính sách tư vấn này có đề xuất phương pháp tiếp cận "mây đầu tiên", ưu tiên sử dụng các dịch vụ mây công cộng cho những trường hợp có khả năng về mặt kỹ thuật để đáp ứng các yêu cầu về chính sách và tổ chức không?

2) Chính sách này có tư vấn cho chính quyền địa phương hoặc các cơ quan về các tiêu chí để xác định có áp dụng tính toán mây (hay không) cho nhu cầu CNTT không?

3) Chính sách này có tư vấn về lợi ích môi trường khi chuyển sang phương pháp tiếp cận dựa trên tính toán mây không?

8.2.3 Thuật ngữ và phân loại

Việc giải thích chính sách tư vấn một cách chính xác phụ thuộc vào sự hiểu biết chung về thuật ngữ được sử dụng và việc xác định đúng các loại dữ liệu mà nó sẽ áp dụng.

Những điều sau đây cần được xem xét:

1) Chính sách tư vấn này có sử dụng thuật ngữ tính toán mây tiêu chuẩn theo các thuật ngữ đã định nghĩa trong TCVN 12480 (ISO/IEC 17788) và ISO/IEC 22123 không?

2) Chính sách này chỉ đưa ra lời khuyên chung hay nó cung cấp hướng dẫn cụ thể cho các danh mục hoặc phân loại dữ liệu cụ thể (xem TCVN 13056 (ISO/IEC 19944)), loại ứng dụng hoặc mục đích?

8.2.4 Sự chấp thuận của các doanh nghiệp vừa và nhỏ

Các chính sách chủ yếu dành cho các doanh nghiệp quy mô lớn và các CSP lớn đôi khi có thể tạo ra gánh nặng không cân xứng cho các tổ chức nhỏ hơn.

Những điều sau đây cần được xem xét:

1) Chính sách tư vấn này có hỗ trợ hoặc làm phức tạp việc sử dụng tính toán mây cho các triển khai nhỏ hơn như chính quyền địa phương nhỏ, cơ sở giáo dục hoặc các cơ quan nhỏ hơn không?

2) Chính sách tư vấn này có khuyến khích hay ngăn cản việc áp dụng tính toán mây của các doanh nghiệp vừa và nhỏ (các SME) cung cấp hoặc đảm nhận công việc cho chính phủ và các cơ quan không?

8.2.5 Chứng nhận của nhà cung cấp

Việc tuân theo chính sách tư vấn sẽ dễ dàng hơn khi nó cung cấp hướng dẫn rõ ràng về loại chứng nhận có thể được sử dụng để xác thực việc tuân thủ toàn bộ hoặc một phần.

Những điều sau đây cần được xem xét:

1) Chính sách tư vấn này có đưa ra hướng dẫn về loại chứng nhận có thể mong đợi của các nhà cung cấp và nhà thầu cung cấp dịch vụ dựa trên mây cho chính phủ và các cơ quan không?

   a) Nếu có, hướng dẫn này có xác định các chứng nhận phù hợp so với các tiêu chuẩn ISO/IEC như các chứng chỉ được liệt kê trong Điều khoản 7 không?

8.2.6 Kết nối mạng

Việc sử dụng tính toán mây có nghĩa là có đủ tính sẵn sàng của mạng thích hợp, cho dù thông qua Internet công cộng hay mạng riêng.

Những điều sau đây cần được xem xét:

1) Chính sách này có tư vấn về các vấn đề mạng là thiết yếu đối với lợi ích của tính toán mây không?

   a) Nếu có, chính sách có khuyến khích việc cung cấp kết nối, tính sẵn sàng và độ tin cậy của mạng băng thông rộng đầy đủ và phù hợp không?

2) Chính sách này có cung cấp hướng dẫn về các vấn đề phân định ranh giới thích hợp, chẳng hạn như phạm vi trách nhiệm của các CSC, CSP (với tư cách là bộ kiểm soát dữ liệu và bộ xử lý dữ liệu) và nhà cung cấp kết nối mạng?

8.2.7 Tính liên tác và tính khả chuyển

Việc kích hoạt tính liên tác và tính khả chuyển thường được coi là điều cần thiết để cạnh tranh thị trường tự do giữa các nhà cung cấp dịch vụ CNTT bao gồm cả tính toán mây.

Những điều sau đây cần được xem xét:

1) Chính sách này có cung cấp hướng dẫn về các kiểu khả năng tương tác hoặc tính khả chuyển cần được tìm kiếm không?

   a) Nếu có, chính sách có thể hiện đầy đủ mức độ phức tạp của các chủ đề này và tuân theo khung tiêu chuẩn được cung cấp trong TCVN 13055 (ISO/IEC 19941) không?

8.3 Cân nhắc về chính sách đấu thầu

8.3.1 Quy định chung

Điều khoản con này đề cập đến những cân nhắc có liên quan khi xây dựng chính sách mua sắm cho người mua và người dùng dịch vụ mây, cho dù được mua bởi chính phủ, cơ quan chính phủ hay doanh nghiệp thương mại.

Ví dụ là khi chính phủ, doanh nghiệp, phòng ban hoặc CSC khác đặt ra các quy tắc sẽ xác định, giới hạn hoặc kiểm soát dịch vụ mây nào mà bộ phận và nhân viên có thể mua hoặc sử dụng.

Những điều sau đây cần được xem xét khi xây dựng chính sách sẽ kiểm soát việc mua, triển khai, cung cấp hoặc sử dụng dịch vụ mây trong một tổ chức.

Việc đánh số không bao hàm bất kỳ hình thức ưu tiên hoặc sự ưu tiên nào.

8.3.2 Thuật ngữ và phân loại

Một số nhà cung cấp tính toán mây và CNTT khác đôi khi sử dụng thuật ngữ trong các mô tả sản phẩm hoặc tiếp thị khác với (hoặc ít rõ ràng hơn) các thuật ngữ được tiêu chuẩn hóa quốc tế. Đối với chính sách mua sắm, điều quan trọng là phải đảm bảo rằng tất cả các nhà cung cấp đều hiểu và sử dụng các thuật ngữ được sử dụng theo cùng một cách trong các dịch vụ cung cấp.

Những điều sau đây cần được xem xét:

1) Chính sách mua sắm này có sử dụng thuật ngữ tính toán mây tiêu chuẩn theo các thuật ngữ được định nghĩa trong TCVN 12480 (ISO/IEC 17788), ISO/IEC 22123 và các tiêu chuẩn khác không?

2) Chính sách mua sắm này có tham chiếu đến bộ tiêu chuẩn ISO/IEC 19086 cho các điều khoản và khái niệm của thỏa thuận dịch vụ mây không?

3) Nếu chính sách mua sắm này đặt ra các hạn chế đối với việc sử dụng dữ liệu khách hàng hoặc dữ liệu dẫn xuất của CSP, thì chính sách này có xác định các loại dữ liệu bị ảnh hưởng theo nguyên tắc phân loại được mô tả trong TCVN 13056 (ISO/IEC 19944) không?

8.3.3 Các mô hình triển khai dịch vụ mây

Có nhiều cách khác nhau để có được các dịch vụ mây và chính sách mua sắm phải cho phép xem xét tất cả các mô hình triển khai dịch vụ phù hợp.

Những điều sau đây cần được xem xét:

1) Chính sách mua sắm này có ràng buộc các nhà cung cấp với bất kỳ (các) mô hình triển khai cụ thể nào không (ví dụ: mây riêng, mây công cộng, mây cộng đồng hoặc mây hỗn hợp - xem TCVN 12480 (ISO/IEC 17788))?

   a) Nếu vậy, hạn chế này có được chứng minh bằng các yêu cầu cụ thể khác không?

2) Nhà cung cấp có quyền tự do đưa ra (các) mô hình triển khai thay thế nếu họ có thể chứng minh rằng họ vẫn có thể đáp ứng các yêu cầu cụ thể đó không?

8.3.4 Chứng nhận của nhà cung cấp

Chính sách mua sắm tính toán mây phải nêu rõ bất kỳ chứng chỉ nào mà CSP phải có.

Những điều sau đây cần được xem xét:

1) Chính sách mua sắm này có xác định các chứng chỉ mà CSP và nhà thầu mong đợi không?

   a) Nếu vậy, chính sách này có đề cập đến các chứng nhận dựa trên các tiêu chuẩn ISO/IEC như những tiêu chuẩn được liệt kê trong Điều khoản 7 không?

8.3.5 Tính liên tác và tính khả chuyển

Kích hoạt khả năng tương tác và tính khả chuyển thường được coi là điều cần thiết để cạnh tranh thị trường tự do giữa các nhà cung cấp dịch vụ CNTT bao gồm cả tính toán mây.

Những điều sau đây cần được xem xét:

1) Chính sách này có yêu cầu các tính năng khả năng tương tác hoặc tính khả chuyển cụ thể không?

   a) Nếu vậy, các tính năng này có được xác định theo các khía cạnh và khuôn khổ được giải thích trong TCVN 13055 (ISO/IEC 19941) không?

2) Khi yêu cầu các tính năng về khả năng tương tác hoặc tính khả chuyển, chính sách có cho phép các cơ chế kỹ thuật thay thế để đạt được mục tiêu mong muốn (chẳng hạn như các cơ chế được đề xuất trong 8.1.5) không?

9 Kết luận

Tiêu chuẩn này

- giải thích các khía cạnh kỹ thuật của tính toán mây có ý nghĩa đối với việc xây dựng chính sách,
- xác định một số tiêu chuẩn có thể được sử dụng để đơn giản hóa và thúc đẩy sự xây dựng của

chính sách đó,

- xác định các cân nhắc khác nhau khi xây dựng chính sách như vậy.

Tiêu chuẩn này thúc đẩy niềm tin rằng việc sử dụng các tiêu chuẩn trong việc xây dựng chính sách tính toán mây sẽ giúp quá trình xây dựng chính sách đó trở nên dễ dàng và nhất quán hơn trên toàn thế giới, đồng thời sẽ tạo điều kiện thuận lợi cho việc triển khai chính sách đó của các nhà cung cấp dịch vụ mây. Do đó, cách tiếp cận dựa trên tiêu chuẩn sẽ tăng tính minh bạch và cạnh tranh, đồng thời khuyến khích việc áp dụng dịch vụ mây vì lợi ích của khách hàng, chính phủ và xã hội nói chung về dịch vụ mây.

Phụ lục A

(Tham khảo)

Mối quan hệ giữa các đặc điểm chính và ý nghĩa

Các đặc điểm chính của tính toán mây theo TCVN 12480 (ISO/IEC 17788)	Mô tả	Ý nghĩa
Truy cập mạng băng rộng	Một tính năng trong đó các tài nguyên vật lý và ảo có sẵn trên mạng và được truy cập thông qua các cơ chế tiêu chuẩn thúc đẩy việc sử dụng bởi các ứng dụng và thiết bị khách không đồng nhất.	6.2.2, 6.4.4, 6.4.8, 6.4.10, 6.4.12, 8.1.6, 8.2.5
Dịch vụ được đo lường	Việc phân phối các dịch vụ mây được đo lường sao cho việc sử dụng có thể được theo dõi, kiểm soát, báo cáo và lập hóa đơn.	6.2.2, 6.4.4, 6.4.6, 7
Đa khách hàng	Phân bổ tài nguyên vật lý và tài nguyên ảo sao cho nhiều đối tượng thuê cũng như tính toán và dữ liệu được tách biệt và không thể truy cập lẫn nhau.	6.2.2, 6.4.2, 6.4.7, 6.4.11, 7.1.1, 8.1.2, 8.1.4, 8.1.6
Dịch vụ tự phục vụ theo nhu cầu	Tính năng mà một CSC có thể cung cấp khả năng tính toán, khi cần, một cách tự động hoặc tương tác tối thiểu với CSP.	6.2.2, 6.3.1, 6.4.2, 6.4.3, 6.4.4, 6.4.5
Tính linh hoạt và khả năng mở rộng nhanh chóng	Một tính năng trong đó tài nguyên vật lý và tài nguyên ảo có thể được điều chỉnh nhanh chóng và linh hoạt, trong một số trường hợp là tự động, để tăng hoặc giảm tài nguyên một cách nhanh chóng.	6.2.2, 6.4.2, 6.4.3, 7
Nguồn tổng hợp	Tập hợp các tài nguyên vật lý và tài nguyên ảo của CSP để phục vụ một hoặc nhiều CSC.	6.2.2, 6.3.1, 6.4.2, 6.4.3, 6.4.7, 6.4.10, 7, 8.1.5, 8.2.6, 8.3.4

Phụ lục B

(Tham khảo)

Các tiêu chuẩn, đặc điểm kỹ thuật và tài liệu liên quan khác

Ngoài các tiêu chuẩn được xác định trong phần chính của tiêu chuẩn này, các tiêu chuẩn khác sau đây có thể hữu ích cho các nhà xây dựng chính sách cho tính toán mây.

Tiêu chuẩn	Nguồn	Mô tả
ETSI EN 301 549	ETSI	Đặt ra các yêu cầu về khả năng tiếp cận phù hợp với việc mua sắm công các sản phẩm và dịch vụ Công nghệ thông tin và truyền thông ở Châu Âu
ISO/IEC 19772	ISO/IEC JTC1	Mô tả mã hóa xác thực
Bộ tiêu chuẩn ISO/IEC 20000	ISO/IEC JTC1	Công nghệ thông tin – Quản lý dịch vụ
Bộ tiêu chuẩn ISO/IEC 27050	ISO/IEC JTC1	Công nghệ thông tin - Các kỹ thuật an toàn - Khám phá điện tử
ISO/IEC 27552	ISO/IEC JTC1	Cung cấp các yêu cầu để nâng cao tiêu chuẩn TCVN ISO/IEC 27001:2019 (ISO/IEC 27001:2013) về quản lý sự riêng tư
ISO/IEC 29100	ISO/IEC JTC1	Mô tả một khuôn khổ sự riêng tư
ISO/IEC 30134-2	ISO/IEC JTC1	Xác định thước đo tiêu chuẩn về Hiệu quả sử dụng năng lượng (PUE) của toàn bộ trung tâm dữ liệu tính toán mây
ISO/IEC 30134-5	ISO/IEC JTC1	Chỉ định việc Sử dụng Thiết bị công nghệ thông tin cho các máy chủ riêng lẻ (ITEUsv) làm Chỉ số Hiệu suất Chính (KPI) để cải thiện hiệu suất năng lượng tổng hợp của các máy chủ trong một trung tâm dữ liệu nhất định.
ISO/IEC 38500	ISO/IEC JTC1	Xác định khuôn khổ quản trị CNTT trong một tổ chức
ISO/IEC 38505-1	ISO/IEC JTC1	Mở rộng ISO/IEC 38500 với các chi tiết cụ thể về quản trị dữ liệu
ISO/IEC 40500:2012 *Các hướng dẫn truy cập nội dung Web W3C (WCAG) 2.0*	ISO/IEC JTC1/W3C	Các hướng dẫn truy cập nội dung Web (WCAG) 2.0 bao gồm một loạt các đề xuất để làm cho nội dung Web dễ truy cập hơn. Việc tuân theo các hướng dẫn này sẽ giúp nhiều người khuyết tật có thể tiếp cận nội dung hơn, bao gồm người mù và thị lực kém, điếc và giảm thính lực, khuyết tật học tập, hạn chế nhận thức, cử động hạn chế, khuyết tật nói, nhạy cảm với ánh sáng và sự kết hợp của những khuyết tật này. Việc tuân theo những hướng dẫn này cũng thường làm cho nội dung Web của bạn dễ sử dụng hơn đối với người dùng nói chung. Lưu ý rằng WCAG 2.1 đang trong giai đoạn xây dựng cuối trong W3C nhưng vẫn chưa được xuất bản.
ISO/IEC 29138-1	ISO/IEC JTC1	Mô tả nhu cầu trợ năng của người dùng đối với giao diện người dùng có thể truy cập
Hướng dẫn ISO/IEC 71:2014	ISO/IEC JTC1	Cung cấp một hướng dẫn để giải quyết khả năng truy cập trong các tiêu chuẩn
ISO/IEC TR 38505-2	ISO/IEC JTC1	Bao gồm ý nghĩa của ISO/IEC 38505-1 đối với quản lý dữ liệu
ITU-D ISBN 978-92-61-16551-2.	ITU-D	Báo cáo về xu hướng cải cách viễn thông từ năm 2016, bao gồm tài liệu về các khuyến khích theo quy định để đạt được các cơ hội kỹ thuật số như áp dụng tính toán mây.
ITU-D ISBN 978-92-61-22091-4.	ITU-D	Báo cáo về triển vọng quy định Công nghệ thông tin và truyền thông toàn cầu năm 2017.
ITU-T X.1601	ITU-T	Mô tả khung bảo mật tính toán mây cấp cao. Điều này bao gồm một danh sách khá đầy đủ các mối đe dọa và thách thức bảo mật đối với người dùng dịch vụ mây và nhà cung cấp dịch vụ.

Tiêu chuẩn	Nguồn	Mô tả
W3C 1999-05-05 Hướng dẫn truy cập nội dung web	W3C	Những hướng dẫn này giải thích cách tác giả và nhà xây dựng trang có thể làm cho nội dung Web có thể truy cập được đối với người khuyết tật.
W3C 2000-02-03 Hướng dẫn truy cập công cụ soạn thảo (ATAG)	W3C	ATAG 1.0. Đặc điểm kỹ thuật này cung cấp hướng dẫn cho các nhà xây dựng công cụ soạn thảo Web về cách làm cho công cụ có thể sử dụng được bởi người khuyết tật. Một phiên bản cập nhật đã được xuất bản vào năm 2015 (xem bên dưới).
W3C 2002-12-17 Hướng dẫn truy cập tác nhân người dùng (UAAG)	W3C	Tiêu chuẩn này cung cấp các hướng dẫn để thiết kế "tác nhân người dùng" giúp hạ thấp các rào cản đối với khả năng truy cập Web đối với người khuyết tật (thị giác, thính giác, thể chất, nhận thức và thần kinh). Tác nhân người dùng bao gồm các trình duyệt HTML và các loại phần mềm khác truy xuất và hiển thị nội dung Web.
W3C 2013-03-28 Thuộc tính vai trò 1.0	W3C	Đặc điểm kỹ thuật này xác định một "thuộc tính vai trò" cho phép tác giả web chú thích các tài liệu web với thông tin ngữ nghĩa có thể trích xuất bằng máy về mục đích của phần tử mà nó được liên kết. Điều này có thể được sử dụng cho khả năng truy cập, thích ứng thiết bị, xử lý phía máy chủ và mô tả dữ liệu phức tạp.
W3C 2014-03-20 Các ứng dụng Internet phong phú có thể truy cập (WAI-ARIA) 1.1	W3C	Còn được gọi là WAI-ARIA, đặc điểm kỹ thuật này cung cấp một bản thể luận về vai trò, trạng thái và thuộc tính có thể được sử dụng để xác định các phần tử giao diện người dùng có thể truy cập và có thể được sử dụng để cải thiện khả năng truy cập và khả năng tương tác của nội dung web và ứng dụng.
W3C 2015-09-24 Hướng dẫn truy cập công cụ soạn thảo (ATAG) 2.0	W3C	ATAG 2.0. Đặc điểm kỹ thuật này cập nhật tài liệu trong ATAG 1.0 cho các yêu cầu và công nghệ mới.

Thư mục tài liệu tham khảo

Khái niệm tính toán mây

[1] ISO/IEC 17789, Information technology - Cloud computing - Reference architecture (Công nghệ thôn tin – Tính toán mây – Kiến trúc tham chiếu)

[2] ISO/IEC 19941, Information technology - Cloud computing - Interoperability and portability (Công nghệ thôn tin – Tính toán mây – Tính liên tác và tính khả chuyển)

[3] TCVN 13056 (ISO/IEC 19944), Information technology - Cloud computing - Cloud services and devices: Data flow, data categories and data use Interoperability and portability (Công nghệ thôn tin – Tính toán mây – Các dịch vụ và thiết bị mây: Luồng dữ liệu, thể loại dữ liệu và sử dụng dữ liệu)

[4] ISO/IEC 22123, Information technology - Cloud computing - Concepts and terminology (Công nghệ thôn tin – Tính toán mây – Khái niệm và thuật ngữ)

[5] ITU-T Y.3501, 2016, Cloud computing — Framework and high-level requirements (Tính toán mây - Khung và các yêu cầu cấp cao)

Hợp đồng và thỏa thuận tính toán mây

[6] ISO/IEC 19086-1, Information technology - Cloud computing - Service level agreement (SLA) framework - Part 1: Overview and concepts (Công nghệ thôn tin – Tính toán mây – Khung thỏa thuận cấp độ dịch vụ (SLA) - Phần 1: Tổng quan và khái niệm)

[7] ISO/IEC 19086-2, Information technology - Cloud Computing - Service Level Agreement (SLA) Framework — Part 2: Metric Model (Công nghệ thôn tin – Tính toán mây – Khung thỏa thuận cấp độ dịch vụ (SLA) - Phần 2: Mô hình số liệu)

[8] ISO/IEC 19086-3, Information technology - Cloud computing - Service level agreement (SLA) framework - Part 3: Core conformance requirements (Công nghệ thôn tin – Tính toán mây – Khung thỏa thuận cấp độ dịch vụ (SLA) - Phần 3: Yêu cầu tuân thủ cốt lõi)

[9] ISO/IEC 19086-4, Information technology - Cloud Computing - Service Level Agreement (SLA) Framework - Part 4: Components of Security and Protection of PII (Công nghệ thôn tin – Tính toán mây – Khung thỏa thuận cấp độ dịch vụ (SLA) - Phần 4: Các cấu phần của An ninh và Bảo vệ PII)

An toàn

[10] ISO/IEC 19772, Information technology - Security techniques - Authenticated encryption (Công nghệ thông tin – Các kỹ thuật an toàn – Mã hóa chứng thực)

[11] TCVN ISO/IEC 27001:2019 (ISO/IEC 27001:2013), Information technology - Security techniques - Information security management systems - Requirements (Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin – Các yêu cầu)

[12] ISO/IEC 27002, Information technology - Security techniques - Code of practice for information

security controls (Công nghệ thông tin – Các kỹ thuật an toàn – Mã thực hành để kiểm soát an toàn thông tin)

[13] ISO/IEC 27017, Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services (Công nghệ thông tin – Các kỹ thuật an toàn – Mã thực hành để kiểm soát an toàn thông tin dựa trên ISO/IEC 27002 về các dịch vụ mây)

[14] ISO/IEC 27030, Information technology - Security techniques - Guidelines for security and privacy in Internet of Things (IoT) (Công nghệ thông tin – Các kỹ thuật an toàn – Hướng dẫn về về bảo mật và sự riêng tư trong Internet of Things (IoT))

[15] ISO/IEC 27050 (tất cả các phần), Information technology - Electronic discovery (Công nghệ thông tin – Khám phá điện tử)

[16] ISO/IEC 27036-4:2016, Information technology - Security techniques - Information security for supplier relationships - Part 4: Guidelines for security of cloud services (Công nghệ thông tin – Các kỹ thuật an toàn – Bảo mật thông tin cho quan hệ nhà cung cấp - Phần 4: Hướng dẫn an ninh của dịch vụ mây)

[17] ISO/IEC 27070, Information technology - Security techniques - Security requirements for establishing virtualized roots of trust (Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu an ninh để thiết lập nguồn tin cậy ảo hóa)

[18] ISO/IEC TS 27570, Information technology - Security techniques - Privacy guidelines for Smart Cities (Công nghệ thông tin – Các kỹ thuật an toàn – Hướng dẫn sự riêng tư cho các thành phố thông minh)

[19] ITU-T X.1601, Cloud Computing Security Framework (Khung an ninh tính toán mây)

Sự riêng tư

[20] ISO/IEC 20889, Information technology - Security techniques - Privacy enhancing data de-identification techniques (Công nghệ thông tin – Các kỹ thuật an toàn – Các kỹ thuật khử nhận dạng dữ liệu nâng cao sự riêng tư)

[21] ISO/IEC 27018, Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (Công nghệ thông tin – Các kỹ thuật an toàn – Mã thực hành để bảo vệ thông tin định dạng các nhân (PII) trong các mây công cộng đóng vai trò là bộ xử lý PII)

[22] ISO/IEC 27552, Information technology - Security techniques - Enhancement to TCVN ISO/IEC 27001:2019 (ISO/IEC 27001:2013) for privacy management - Requirements (Công nghệ thông tin – Các kỹ thuật an toàn – Nâng cao TCVN ISO/IEC 27001:2019 (ISO/IEC 27001:2013) để quản lý sự riêng tư - Yêu cầu)

[23] ISO/IEC 29100, Information technology - Security techniques - Privacy framework (Công nghệ thông tin – Các kỹ thuật an toàn – Khung riêng tư)

Quản lý dịch vụ

[24] ISO/IEC 20000 (tất cả các phần), *Information technology — Service management* (Công nghệ thông tin – Quản lý dịch vụ)

Truy cập

[25] ISO/IEC 29138-1, *Information technology - User interface accessibility - Part 1: User accessibility needs* (Công nghệ thông tin - Khả năng truy cập giao diện người dùng - Phần 1: Nhu cầu truy cập của người dùng)

[26] ISO/IEC 40500:2012, *Information technology - W3C Web Content Accessibility Guidelines (WCAG) 2.0* (Công nghệ thôn tin – W3C Hướng dẫn truy cập nội dung Web (WCAG) 2.0)

[27] ETSI EN 301-549, Các yêu cầu truy cập phù hợp với việc mua sắm công các sản phẩm và dịch vụ Công nghệ thông tin và truyền thông ở Châu Âu

[28] W3C 2015-09-24, Authoring Tool Accessibility Guidelines (ATAG) 2.0 (Hướng dẫn truy cập công cụ soạn thảo (ATAG) 2.0)

[29] W3C 2014-03-20, Accessible Rich Internet Applications (WAI-ARIA) 1.0 (Các ứng dụng internet đa dạng có thể truy cập (WAI-ARIA) 1.0)

[30] W3C 2014-03-20, WAI-ARIA 1.0 User Agent Implementation Guide (Hướng dẫn triển khai tác nhân người dùng)

[31] W3C 2013-03-28, Role Attribute 1.0 (Thuộc tính vai trò 1.0)

[32] W3C 2002-12-17, User Agent Accessibility Guidelines 1.0 (Hướng dẫn truy cập tác nhân người dùng)

[33] W3C 2000-02-03, Authoring Tool Accessibility Guidelines 1.0 (Hướng dẫn truy cập công cụ soạn thảo)

[34] W3C 1999-05-05, Web Content Accessibility Guidelines 1.0 (Hướng dẫn truy cập nội dung Web)

[35] ISO/IEC Guide 71:2014, *Guide for addressing accessibility in standards* (Hướng dẫn giải quyết khả năng tiếp cận trong các tiêu chuẩn)

Quản trị

[36] ISO/IEC 38500, Information technology - Governance of IT for the organization (Công nghệ thông tin - Quản trị CNTT cho tổ chức)

[37] ISO/IEC 38505-1, Information technology - Governance of IT - Governance of data - Part 1: Application of ISO/IEC 38500 to the governance of data (Công nghệ thông tin - Quản trị CNTT - Quản trị dữ liệu - Phần 1: Áp dụng ISO/IEC 38500 vào quản trị dữ liệu)

[38] ISO/IEC/TR 38505-2, Information technology - Governance of IT - Governance of data - Part 2: Implications of ISO/IEC 38505-1 for data management (Công nghệ thông tin - Quản trị CNTT -

Quản trị dữ liệu - Phần 2: Ý nghĩa của ISO/IEC 38505-1 đối với quản lý dữ liệu)

Hiệu suất năng lượng

[39] THÔNG TIN TỪ ỦY BAN ĐẾN NGHỊ VIỆN CHÂU ÂU. HỘI ĐỒNG, ỦY BAN KINH TẾ - XÃ HỘI CHÂU ÂU VÀ ỦY BAN CÁC KHU VỰC – "Xây dựng nền kinh tế dữ liệu châu Âu"

[40] ISO/IEC 19395, Information technology - Sustainability for and by information technology -Smart data centre resource monitoring and control (Công nghệ thông tin — Tính bền vững cho và bởi công nghệ thông tin – Giám sát và kiểm soát tài nguyên trung tâm dữ liệu thông minh)

[41] ISO/IEC 30134-2, Information technology - Data centres - Key performance indicators - Part 2: Power usage effectiveness (PUE) (Công nghệ thông tin - Trung tâm dữ liệu - Các chỉ số hiệu suất chính - Phần 2: Hiệu quả sử dụng điện năng (PUE))

[42] ISO/IEC 30134-4, Information technology - Data centres - Key performance indicators - Part 4: IT Equipment Energy Efficiency for servers (ITEEsv) 4: Tiết kiệm Năng lượng Thiết bị công nghệ thông tin cho máy chủ (ITEEsv))

[43] ISO/IEC 30134-5, Information technology - Data centres - Key performance indicators - Part 5: IT Equipment Utilization for servers (ITEUsv) (Công nghệ thông tin - Trung tâm dữ liệu - Các chỉ số hiệu suất chính - Phần 5: Sử dụng thiết bị công nghệ thông tin cho máy chủ (ITEUsv))

Sử dụng các tiêu chuẩn để xây dựng chính sách

[44] ISO/IEC. Sử dụng và tham khảo các tiêu chuẩn ISO và IEC để hỗ trợ chính sách công, https://www.iso.org/publication/PUB100358.pdf

[45] Xu hướng Cải cách Viễn thông 2016: Các biện pháp khuyến khích theo quy định để đạt được các cơ hội kỹ thuật số 2016 - ITU-D ISBN 978-92-61-16551-2

[46] Triển vọng về Quy định Công nghệ thông tin và truyền thông Toàn cầu 2017 - ITU-D ISBN 978-92-61-22091-4