TCVN

TIÊU CHUẨN QUỐC GIA

TCVN XXXXX:2026

Xuất bản lần 1

AN NINH MẠNG - NỀN TẢNG TÍNH TOÁN ĐÁM MÂY PHỤC VỤ HẠ TẦNG SỐ TRỌNG YẾU - YÊU CẦU CHUNG

Cyber security - Cloud computing platform for critical digital infrastructure - General requirements

HÀ NỘI – 2026

Mục lục

Lời nói đầu

TCVN XXXXX:2026 An ninh mạng - Nền tảng tính toán đám mây phục vụ hạ tầng số trọng yếu - Yêu cầu chung do Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao biên soạn, Cục Khoa học, Chiến lược và Lịch sử Công an trình duyệt, Bộ Khoa học và Công nghệ thẩm định, Bộ trưởng Bộ Công an ban hành theo Thông tư số XXXX/2026/TT-BCA ngày tháng năm 2026.

An ninh mạng - Nền tảng tính toán đám mây phục vụ hạ tầng số trọng yếu - Yêu cầu chung

Cyber security - Cloud computing platform for critical digital infrastructure - General requirements

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu kỹ thuật chung đối với nền tảng tính toán đám mây phục vụ hạ tầng số trọng yếu.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau 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.

- TCVN 14423:2026, An ninh mạng - Hệ thống thông tin - Yêu cầu cơ bản.

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

- TCVN 12481:2019 (ISO/IEC 17789:2014), Công nghệ thông tin - Tính toán đám mây - Kiến trúc tham chiếu.

- TCVN 13055 (ISO/IEC 19941), Công nghệ thông tin - Tính toán đám mây - Tính liên tác và tính khả chuyển.

- TCVN 13054-1:2020 (ISO/IEC 19086-1:2016), Công nghệ thông tin - Tính toán mây - Khung cam kết mức dịch vụ - Phần 1: Tổng quan và các khái niệm.

- TCVN 9250:2021, Trung tâm dữ liệu - Yêu cầu hạ tầng kỹ thuật viễn thông.

- TCVN 8695-1:2023 (ISO/IEC 20000-1:2018), Công nghệ thông tin - Quản lý dịch vụ - Phần 1: Yêu cầu hệ thống quản lý dịch vụ.

Văn bản quy phạm pháp luật liên quan trực tiếp:

- Luật An ninh mạng số 116/2025/QH15.

- Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15.

- Nghị định của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin.

- Thông tư của Bộ trưởng Bộ Công an ban hành Khung quản lý rủi ro an ninh mạng.

- Pháp luật về cơ yếu và về quản lý, sử dụng sản phẩm mật mã cơ yếu, mật mã an ninh và mật mã dân sự.

3 Thuật ngữ, định nghĩa và chữ viết tắt

Tiêu chuẩn này sử dụng các thuật ngữ, định nghĩa và chữ viết tắt dưới đây.

3.1 Thuật ngữ và định nghĩa

3.1.1

Khách hàng dịch vụ tính toán đám mây (cloud service customer)

Cơ quan, tổ chức nhà nước có thỏa thuận thuê/ sử dụng các dịch vụ từ nhà cung cấp dịch vụ điện toán đám mây.

3.1.2

Nhà cung cấp dịch vụ tính toán đám mây (cloud service provider)

Tổ chức chịu trách nhiệm cung cấp dịch vụ tính toán đám mây cho khách hàng dịch vụ tính toán đám mây.

3.1.3

Infrastructure as Code (IaC)

Phương pháp quản lý và cung cấp hạ tầng công nghệ thông tin thông qua mã nguồn thay vì các quy trình thủ công.

3.1.4

Vendor lock-in

Là một hoạt động thuộc an ninh chuỗi cung ứng, thể hiện sự phụ thuộc vào một nhà cung cấp (dịch vụ, sản phẩm hay nền tảng công nghệ), khiến việc chuyển sang nhà cung cấp khác trở nên khó khăn, do các rào cản như chi phí chuyển đổi cao, kỹ thuật phức tạp hoặc ảnh hưởng nghiêm trọng tới hoạt động.

3.1.5

Hypervisor

Thành phần ảo hóa chịu trách nhiệm quản lý các hệ điều hành khách trên một máy chủ và kiểm soát luồng thực thi lệnh giữa các hệ điều hành khách và phần cứng vật lý.

3.1.6

An ninh mạng (cyber security)

Sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

3.1.7

Tính toán đám mây (cloud computing)

Tính toán đám mây là mô hình dịch vụ cho phép sử dụng tài nguyên điện toán dùng chung (mạng, máy chủ, lưu trữ, ứng dụng, dịch vụ...) thông qua kết nối mạng. Tài nguyên tính toán đám mây có thể được thiết lập hoặc hủy bỏ bởi người dùng mà không cần sự can thiệp của Nhà cung cấp dịch vụ.

3.1.8

Container (vùng chứa)

Môi trường thực thi cô lập để chạy phần mềm sử dụng nhân hệ điều hành ảo hóa.

3.1.9

Mô hình chia sẻ trách nhiệm (shared responsibility model)

Khung phân định trách nhiệm về quản lý, vận hành và đảm bảo an ninh mạng giữa nhà cung cấp và khách hàng trong việc đảm bảo an toàn, tuân thủ và quản trị hệ thống.

3.1.10

Kiến trúc vi dịch vụ (microservices)

Phương pháp phát triển phần mềm trong đó một ứng dụng lớn được chia nhỏ thành nhiều dịch vụ độc lập, giao tiếp với nhau qua các giao diện lập trình ứng dụng (API) được định nghĩa rõ ràng.

3.1.11

Mô hình Active-Standby

Cấu hình hệ thống đảm bảo tính sẵn sàng cao, trong đó máy chủ/hệ thống chính (Active) xử lý toàn bộ khối lượng công việc, trong khi máy chủ/hệ thống dự phòng (Standby) luôn ở trạng thái chờ và tự động tiếp quản khi hệ thống chính gặp sự cố.

3.1.12

Mục tiêu điểm phục hồi (RPO - recovery point objective)

Lượng dữ liệu tối đa mà một tổ chức có thể chấp nhận bị mất mát khi xảy ra sự cố, được tính bằng khoảng thời gian từ lần sao lưu gần nhất đến thời điểm xảy ra sự cố.

3.1.13

Mục tiêu thời gian phục hồi (RTO - recovery time objective)

Khoảng thời gian tối đa cho phép để khôi phục lại các hệ thống và ứng dụng sau khi xảy ra sự cố nhằm tránh những hậu quả không thể chấp nhận được đối với hoạt động.

3.1.14

Tác nhân (Agent) / Tiện ích mở rộng (Extension)

Là các đoạn mã, trình cắm (plugin) hoặc ứng dụng phần mềm nhỏ được cài đặt thêm vào môi trường hệ điều hành hoặc nền tảng ảo hóa nhằm thực hiện các chức năng giám sát, thu thập log, hoặc bảo mật bổ sung.

3.2 Chữ viết tắt

CSC	Khách hàng dịch vụ tính toán đám mây	Cloud Service Customer
CSP	Nhà cung cấp dịch vụ tính toán đám mây	Cloud Service Provider
IaaS	Hạ tầng dưới dạng dịch vụ	Infrastructure as a Service
IaC	Hạ tầng dưới dạng mã	Infrastructure as Code
PaaS	Nền tảng dưới dạng dịch vụ	Platform as a Service
SaaS	Phần mềm dưới dạng dịch vụ	Software as a Service
SLA	Thoả thuận cung cấp dịch vụ	Service Level Agreement
SOC	Trung tâm điều hành an ninh	Security Operations Center
TTDL	Trung tâm dữ liệu	
VM	Máy ảo	Virtual Machine

4 Nguyên tắc áp dụng và mô hình chia sẻ trách nhiệm

4.1 Nguyên tắc áp dụng

a) Trong tiêu chuẩn này, cách diễn đạt các loại điều khoản thực hiện theo TCVN 1-2:2025: “phải” và “không được” chỉ yêu cầu; “nên” và “không nên” chỉ khuyến nghị; “được phép” và “cho phép” chỉ sự cho phép; “có khả năng để”, “có khả năng làm” và “không thể” chỉ khả năng và năng lực.

b) Tiêu chuẩn này chỉ đặt yêu cầu kỹ thuật đối với nền tảng đám mây, nhà cung cấp phần mềm nền tảng và tổ chức vận hành nền tảng; không đặt yêu cầu trực tiếp đối với các thành phần thuộc phạm vi kiểm soát riêng của chủ thuê (như cấu hình bên trong máy ảo, hệ điều hành khách, hoặc ứng dụng của chủ thuê).

c) Các năng lực an toàn liên quan đến chủ thuê trong tiêu chuẩn này được diễn đạt dưới dạng: nền tảng phải cung cấp sẵn các giao diện, tính năng hoặc công cụ quản trị tương ứng để chủ thuê có khả năng thực hiện được trách nhiệm bảo mật của mình.

d) Tiêu chuẩn này không thay thế hoặc loại trừ trách nhiệm của chủ thuê đối với HTTT do mình quản lý. Chủ thuê phải tự thực hiện các biện pháp bảo đảm an toàn theo TCVN 14423:2026 và các quy định pháp luật tương ứng với cấp độ của hệ thống.

đ) Tiêu chuẩn này quy định năng lực kỹ thuật mà nền tảng đám mây phải có, không quy định các nghĩa vụ dân sự trong thoả thuận dịch vụ (như thời hạn thông báo, phạm vi bồi thường). Trường hợp một nghĩa vụ chỉ thực hiện được khi nền tảng có năng lực kỹ thuật tương ứng, tiêu chuẩn này quy định năng lực đó làm cơ sở.

e) Mọi yêu cầu bắt buộc phải được chứng minh bằng thử nghiệm thực tế theo Phụ lục B, trừ các yêu cầu được ghi rõ là chứng minh bằng hồ sơ tài liệu. Tổ chức đánh giá xây dựng phép thử theo cùng cấu

trúc: điều kiện ban đầu - hành động - kết quả kỳ vọng. Cam kết bằng văn bản không được coi là bằng chứng đủ đối với bất kỳ yêu cầu bắt buộc nào có khả năng kiểm chứng bằng thử nghiệm.

g) Yêu cầu được ghi kèm cụm từ "yêu cầu bắt buộc về kiến trúc" là yêu cầu không có biện pháp bù đắp tương đương. Việc không đáp ứng một yêu cầu như vậy dẫn đến kết luận nền tảng không phù hợp với mức tương ứng và không làm phát sinh quyền áp dụng cơ chế tuân thủ hoặc giải trình quy định tại Khung quản lý rủi ro an ninh mạng.

h) Khi tiêu chuẩn này quy định nền tảng thực hiện một hành động tự động, hành động đó phải dựa trên điều kiện kiểm chứng được từ dữ liệu mà nền tảng quan sát được. Việc đánh giá tình huống và quyết định nghiệp vụ thuộc thẩm quyền của tổ chức vận hành nền tảng; nền tảng cung cấp cơ chế thực thi và ghi nhận quyết định đó.

i) Khi tiêu chuẩn này quy định một chức năng gắn với quy trình nghiệp vụ bao gồm: phát thông báo, phê duyệt, quản lý sự vụ, trình bày thông tin cho chủ thuê và lập báo cáo định kỳ, yêu cầu đối với nền tảng gồm ba nội dung: sinh dữ liệu và sự kiện với các trường tối thiểu đã quy định; cung cấp giao diện lập trình để hệ thống bên ngoài truy xuất dữ liệu đó và ghi nhận kết quả xử lý; và ghi bản ghi kiểm toán đối với dữ liệu, sự kiện cùng kết quả được ghi nhận. Việc vận hành quy trình được phép thực hiện bằng chính nền tảng hoặc bằng hệ thống độc lập do tổ chức vận hành nền tảng lựa chọn. Tổ chức vận hành nền tảng phải có quy trình quản lý đối với các chức năng này và phải lưu hồ sơ thực hiện, gồm nội dung, thời điểm, chủ thể thực hiện và kết quả.

k) Quy định tại điểm i) không áp dụng đối với điểm cưỡng chế. Điểm cưỡng chế là cơ chế mà nếu không được thỏa mãn thì nền tảng không thi hành thao tác tương ứng; điểm cưỡng chế phải nằm trong nền tảng, không phụ thuộc hệ thống bên ngoài, kể cả khi quyết định đầu vào của cơ chế đó đến từ hệ thống bên ngoài. Việc thực hiện các chức năng quy định tại điểm i) không được đòi hỏi thiết lập kết nối từ hệ thống bên ngoài vào nền tảng; dữ liệu trao đổi theo chiều từ nền tảng ra. Đối với thao tác yêu cầu phê duyệt trước khi thi hành, chủ thể phê duyệt phải xác thực và thao tác trực tiếp trên nền tảng.

4.2 Mức áp dụng, mô hình tin cậy và điều kiện tiên quyết

4.2.1 Mức áp dụng

a) Tiêu chuẩn này quy định ba mức yêu cầu, ký hiệu Mức 3, Mức 4 và Mức 5, áp dụng tương ứng với cấp độ an ninh mạng của HTTT theo quy định của pháp luật về an ninh mạng.

Mức	Áp dụng cho	Mô hình tin cậy đối với tổ chức vận hành nền tảng
Mức 3	Nền tảng phục vụ HTTT cấp độ 3	Được coi là đáng tin cậy. Kiểm soát tập trung vào cách ly logic giữa các chủ thuê và ghi nhận đầy đủ hành vi quản trị.

Mức 4	Nền tảng phục vụ HTTT cấp độ 4	Được coi là đáng tin cậy có điều kiện. Đặc quyền phải được phân tách, ràng buộc theo thời gian và chịu phê duyệt độc lập đối với thao tác nhạy cảm.
Mức 5	Nền tảng phục vụ HTTT cấp độ 5, bao gồm HTTT quan trọng về an ninh quốc gia	Không được tin cậy mặc định. Nền tảng phải được thiết kế sao cho không tồn tại đường tiếp cận kỹ thuật của tổ chức vận hành tới dữ liệu chủ thuê ở dạng rõ, và không tồn tại khả năng xóa hoặc sửa dấu vết hành vi quản trị.

b) Nền tảng phục vụ đồng thời nhiều HTTT có mức độ khác nhau phải áp dụng mức kiểm soát tương ứng với mức độ cao nhất. Yêu cầu của mức cao bao hàm toàn bộ yêu cầu của mức thấp.

c) Tổ chức vận hành nền tảng đám mây dùng chung phải áp dụng các yêu cầu cơ bản tại TCVN 14423:2026 đối với hạ tầng của chính mình, độc lập với cấp độ hệ thống của các chủ thuê chạy trên đó.

4.2.2 Mô hình tin cậy và kiến trúc tiên quyết

a) Tổ chức vận hành nền tảng phải công bố mô hình tin cậy, xác định rõ: chủ thể được tin cậy, chủ thể không được tin cậy, giả định an ninh và hệ quả khi vi phạm giả định. Đối với Mức 4 và Mức 5, mô hình tin cậy phải đưa chính người vận hành nền tảng vào danh sách chủ thể tấn công tiềm năng.

b) Không được sử dụng quy trình thủ công, biện pháp hành chính hay cam kết hợp đồng để thay thế (làm biện pháp kiểm soát duy nhất) đối với các rủi ro đã có biện pháp kỹ thuật khả thi để ngăn chặn.

c) Điều kiện kiến trúc Mức 5 (Zero-Trust): Không một chủ thể đơn lẻ nào (kể cả tài khoản có đặc quyền cao nhất) hội đủ đồng thời ba năng lực sau: Thay đổi cấu hình hạ tầng; Tiếp cận hoặc điều khiển khóa mật mã bảo vệ dữ liệu chủ thuê; Thay đổi cấu hình hoặc nội dung nhật ký kiểm toán.

d) Các yêu cầu tại điểm c) là điều kiện tiên quyết về kiến trúc. Việc không đáp ứng bằng thiết kế kỹ thuật sẽ dẫn đến kết luận nền tảng không đạt Mức 5 và không có bất kỳ biện pháp quản lý nào được phép dùng để bù đắp.

4.3 Phân định và chia sẻ trách nhiệm

4.3.1 Nguyên tắc chung

a) Trách nhiệm bảo đảm an toàn thông tin được phân định dựa trên phạm vi kiểm soát thực tế của từng bên đối với tài nguyên, cấu hình và dữ liệu.

b) Việc phân định trách nhiệm phải bảo đảm nguyên tắc không tồn tại khoảng trống trách nhiệm trên toàn bộ vòng đời và phạm vi dịch vụ đám mây.

c) Việc chủ thuê hoặc tổ chức vận hành thuê bên thứ ba thực hiện một phần công việc không làm loại trừ trách nhiệm cốt lõi của chủ thuê đối với phạm vi của mình.

4.3.2 Minh bạch trách nhiệm

a) Tổ chức vận hành nền tảng phải công bố bảng phân định trách nhiệm chi tiết đối với từng nhóm yêu cầu của TCVN 14423:2026 và tiêu chuẩn này.

b) Bảng phân định phải làm rõ ba yếu tố đối với mỗi điểm kiểm soát: (1) Chủ thể thực hiện; (2) Chủ thể giám sát; và (3) Cơ chế để chủ thuê kiểm chứng nền tảng đã thực hiện đúng.

4.4 Trách nhiệm đối với chuỗi cung ứng dịch vụ

a) Khi sử dụng hạ tầng, dịch vụ hoặc phần mềm của bên thứ ba, tổ chức vận hành nền tảng phải đánh giá rủi ro chuỗi cung ứng có thể ảnh hưởng đến chủ thuê.

b) Tổ chức vận hành nền tảng phải kiểm soát chặt chẽ quyền truy cập của bên thứ ba vào tài nguyên thuộc phạm vi dịch vụ của chủ thuê.

c) Tổ chức vận hành nền tảng phải ràng buộc cam kết mức chất lượng (SLA) và yêu cầu bảo mật với bên thứ ba sao cho không được thấp hơn cam kết đã ký với chủ thuê.

5. Quản trị an ninh mạng và quản lý rủi ro

5.1 Khái quát

Thiết lập khung quản trị an ninh mạng và quản lý rủi ro đối với nền tảng đám mây, dựa trên:

a) Tuân thủ các yêu cầu quản trị cơ bản theo TCVN 14423:2026.

b) Kiểm soát bổ sung các rủi ro đặc thù của hạ tầng dùng chung và an ninh chuỗi cung ứng.

5.2 Yêu cầu cụ thể

5.2.1 Quản trị an ninh mạng

a) Tổ chức vận hành nền tảng (đối với hạ tầng đám mây) và chủ thuê (đối với HTTT được triển khai trên đám mây) phải thiết lập cơ chế quản trị an ninh mạng và thực hiện quản lý rủi ro tuân thủ các yêu cầu tại TCVN 14423:2026 tương ứng với cấp độ HTTT .

b) Các quy trình chi tiết về xác định vai trò, thiết lập chính sách, đánh giá rủi ro, lựa chọn biện pháp xử lý rủi ro và rà soát định kỳ được thực hiện theo quy định tại TCVN 14423:2026; tiêu chuẩn này không lặp lại các yêu cầu quản trị cơ bản đó.

c) Việc áp dụng các yêu cầu kỹ thuật tại Mục 6 và Mục 7 của tiêu chuẩn này được sử dụng làm cơ sở bổ trợ đặc thù cho môi trường đám mây, không làm phát sinh yêu cầu đánh giá trùng lặp đối với các kiểm soát đã được nghiệm thu theo TCVN 14423:2026.

5.2.2 Quản lý rủi ro trong môi trường đám mây

Ngoài việc tuân thủ các biện pháp cơ bản theo 5.1, quản lý rủi ro trong môi trường đám mây phải bảo đảm các yêu cầu sau:

a) Tổ chức vận hành nền tảng phải cung cấp các tài liệu kiến trúc, chứng nhận tuân thủ hoặc báo cáo kiểm toán độc lập cần thiết để chủ thuê có đủ cơ sở dữ liệu thực hiện đánh giá rủi ro đối với HTTT của mình.

b) Quá trình quản lý rủi ro của tổ chức vận hành nền tảng phải phân tích và xử lý triệt để các rủi ro rò rỉ dữ liệu, leo thang đặc quyền hoặc cạn kiệt tài nguyên phát sinh từ việc chia sẻ chung tài nguyên vật lý giữa nhiều chủ thuê.

c) Tổ chức vận hành nền tảng phải định kỳ rà soát các rủi ro phát sinh từ việc tích hợp hoặc phụ thuộc vào hạ tầng của nhà cung cấp phụ, dịch vụ bên ngoài và các thành phần mã nguồn mở dùng chung. Cụ thể, tối thiểu 01 lần/năm đối với các hệ thống cấp độ 3; tối thiểu 01 lần/06 tháng đối với các hệ thống cấp độ 4 và cấp độ 5.

d) Tổ chức vận hành nền tảng và chủ thuê phải duy trì các hồ sơ, thông tin hoặc bằng chứng cần thiết để chứng minh việc thực hiện các hoạt động quản trị an ninh mạng và quản lý rủi ro trong phạm vi trách nhiệm của mình.

6. Yêu cầu an toàn chung đối với nền tảng

6.1 Khái quát

Thiết lập các yêu cầu kỹ thuật cốt lõi và các biện pháp kiểm soát an ninh mạng bắt buộc mà kiến trúc nền tảng tính toán đám mây phải đáp ứng. Các yêu cầu được thiết kế nhằm bảo vệ hệ thống trước các rủi ro đặc thù của môi trường đa tiền thuê, bảo đảm tính độc lập, khả năng cách ly, sự toàn vẹn của dữ liệu và tính sẵn sàng cao của các dịch vụ đám mây phục vụ hạ tầng số trọng yếu.

6.2 Yêu cầu cụ thể

6.2.1 Kiến trúc an toàn, phân tách thuê bao và bảo vệ mặt phẳng điều khiển

6.2.1.1 Độc lập giữa các phân hệ và giới hạn ảnh hưởng

a) Kiến trúc nền tảng phải phân lớp và tách biệt rõ ràng các phân hệ: điều khiển, dữ liệu và quản lý định danh/mật mã.

b) Nền tảng phải phân đoạn mạng logic hoặc vật lý đối với tối thiểu 05 vùng kiến trúc: vùng mặt phẳng điều khiển, mặt phẳng dữ liệu, mạng quản trị nội bộ, mạng chủ thuê và vùng kết nối Internet công cộng.

c) Sự cố tại phân hệ điều khiển không được làm mất khả năng kiểm soát truy cập và không làm lộ khóa.

d) Sự cố tại phân hệ điều khiển không được làm gián đoạn máy ảo, mạng và tường lửa tại phân hệ dữ liệu.

đ) Sau khi hệ thống khôi phục, phân hệ điều khiển và phân hệ dữ liệu phải tự đồng bộ mà không sinh tài nguyên vô chủ.

e) Phân hệ điều khiển không được thiết kế có điểm lỗi đơn.

g) Thời gian chuyển đổi dự phòng của phân hệ điều khiển không vượt quá 30 giây (Mức 3, Mức 4) và không quá 15 giây (Mức 5).

h) Nền tảng phải được phân hoạch thành các đơn vị cách ly sự cố độc lập; lỗi ở một đơn vị không được lan sang đơn vị khác.

i) Thay đổi cấu hình toàn cục đối với Mức 4 và Mức 5 phải được triển khai cuốn chiếu theo từng vòng.

k) Hệ thống phải có cơ chế tự động dừng và quay lui khi phát hiện suy giảm chỉ số trong quá trình thay đổi cấu hình.

l) Nền tảng phải có cơ chế giới hạn tần suất yêu cầu và xếp hàng công bằng tại mặt phẳng điều khiển.

m) Nền tảng phải bảo đảm một chủ thuê bị tấn công hoặc lỗi cấu hình không thể làm cạn kiệt năng lực điều phối API chung.

n) Các giao diện quản trị phải được bảo vệ bởi cơ chế chống tấn công từ chối dịch vụ.

o) Cấm phơi bày trực tiếp các giao diện quản trị cấp cao (giao diện đồ họa, API, SSH) ra mạng Internet công cộng.

p) Phải giới hạn nguồn truy cập đến giao diện quản trị thông qua IP Whitelist, mạng riêng ảo (VPN) hoặc nền tảng quản trị ngoài băng tần.

q) Nền tảng phải bảo đảm không một thành phần nào từ vùng mạng tin cậy thấp có thể truy cập trái phép vào vùng tin cậy cao hơn.

r) Nghiêm cấm cài đặt và sử dụng trình duyệt web hoặc phần mềm thư điện tử trên máy chủ ảo hóa lõi, máy chủ mặt phẳng điều khiển và máy chủ trạm nhảy.

6.2.1.2 Phân tách và cách ly giữa các chủ thuê ở lớp ảo hóa

a) Nền tảng phải áp dụng kiểm soát truy cập bắt buộc tại hệ điều hành chủ.

b) Một máy ảo bị chiếm quyền không được có khả năng tác động tới máy ảo của chủ thuê khác hoặc tới hệ điều hành chủ.

c) Tác nhân quản trị cài đặt trên máy chủ vật lý phải chạy với đặc quyền tối thiểu.

d) Nền tảng phải giới hạn hạn mức tài nguyên ở cấp độ phần cứng ảo hóa.

đ) Nền tảng phải ngăn chặn một chủ thuê chiếm dụng cạn kiệt tài nguyên toàn nền tảng hoặc gây ảnh hưởng chéo.

e) Đối với mức 5 nền tảng phải hỗ trợ cấu hình cách ly lõi xử lý vật lý theo từng chủ thuê.

g) Đối với mức 5 máy ảo của các chủ thuê khác nhau không được xếp lịch hoạt động trên cùng một lõi vật lý chia sẻ luồng.

h) Hệ thống phải vô hiệu hóa các tính năng chia sẻ hoặc tối ưu hóa bộ nhớ dùng chung giữa các máy ảo khác nhau để triệt tiêu rủi ro rò rỉ dữ liệu qua kênh bên.

i) Nền tảng phải hạn chế việc sử dụng cơ chế mô phỏng thiết bị bằng thuần phần mềm.

k) Nền tảng phải kích hoạt tính năng ánh xạ lại quyền truy cập bộ nhớ trực tiếp (IOMMU) nhằm chặn truy xuất bộ nhớ trái phép từ thiết bị ngoại vi.

6.2.1.3 Toàn vẹn khởi động và bảo vệ siêu dữ liệu

a) Máy chủ vật lý phải cấu hình khởi động an toàn, xác thực chữ ký số của nhân hệ điều hành và mô-đun ảo hóa.

b) Máy chủ không vượt qua xác minh tính toàn vẹn khởi động phải bị tự động cách ly khỏi cụm máy chủ.

c) Đối với mức 5, máy chủ vật lý phải đo lường trạng thái khởi động, lưu vào mô-đun phần cứng (TPM) và cho phép xác minh từ xa.

d) Nền tảng phải thiết lập và duy trì một kho lưu trữ bản mẫu chuẩn duy nhất cho các hình ảnh hệ điều hành và vùng chứa.

đ) Nền tảng phải tích hợp công cụ kiểm soát luồng triển khai nhằm tự động từ chối cấp phép khởi tạo đối với các tài nguyên sử dụng ảnh hệ thống không nằm trong danh mục bản mẫu chuẩn.

e) Tất cả ảnh máy ảo phải được ký số và rà quét lỗ hổng trước khi thực hiện cấp phát.

g) Dịch vụ cung cấp siêu dữ liệu của máy ảo phải có cơ chế chống truy cập trái phép và yêu cầu xác thực.

h) Nội dung siêu dữ liệu không được chứa khóa mật mã, thông tin quản trị nền tảng hoặc cấu trúc vật lý của hệ thống.

i) Nền tảng phải cho phép chủ thuê tự vô hiệu hóa dịch vụ siêu dữ liệu đối với từng máy ảo thuộc phạm vi của mình.

6.2.1.4 Chứng thư số nội bộ và nguồn thời gian tin cậy

a) Nền tảng phải phát cảnh báo tự động trước thời điểm chứng thư số nội bộ hết hạn.

b) Nền tảng phải hỗ trợ thao tác gia hạn chứng thư số không làm dừng dịch vụ và không phụ thuộc tổ chức cung cấp dịch vụ chứng thực bên ngoài.

c) Nền tảng phải đồng bộ thời gian từ nguồn tin cậy nội bộ có dự phòng.

6.2.1.5 Bảo mật môi trường vùng chứa và vi dịch vụ

a) Hệ thống phải triển khai giải pháp giám sát bảo mật ở cấp độ nhân hệ điều hành của máy chủ vật lý nền.

b) Giải pháp giám sát bảo mật không được làm thay đổi mã nguồn của hình ảnh ứng dụng gốc và phải có năng lực phát hiện nỗ lực thoát khỏi vùng chứa.

c) Hệ thống tệp gốc của vùng chứa bắt buộc phải được thiết lập cấu hình ở trạng thái chỉ đọc.

d) Nghiêm cấm cấu hình cho phép vùng chứa đính kèm các thư mục nhạy cảm từ hệ điều hành máy chủ vật lý hoặc máy ảo nền.

đ) Nghiêm cấm các vùng chứa tự ý khởi tạo thêm các vùng chứa con bên trong nó.

e) Lưu lượng mạng trao đổi giữa các vùng chứa xuyên suốt các nút vật lý khác nhau bắt buộc phải được đóng gói hoặc định tuyến qua kiến trúc mạng dịch vụ lưới để thực thi mã hóa an toàn.

6.2.1.6 Khả năng chịu lỗi và suy giảm có kiểm soát (Thực hiện theo quy định tại nhóm Quản lý kiểm tra an ninh mạng của TCVN 14423:2026)

a) Nền tảng phải bảo đảm hoạt động liên tục khi mất một máy chủ vật lý bất kỳ, một thiết bị chuyển mạch bất kỳ, một nút lưu trữ bất kỳ và một thành phần phân hệ điều khiển bất kỳ.

b) Khi tài nguyên suy giảm, nền tảng phải suy giảm có kiểm soát theo thứ tự ưu tiên là tham số cấu hình được, do tổ chức vận hành nền tảng xác định và công bố trước, trong đó ưu tiên cao nhất dành cho duy trì hoạt động của máy ảo đang chạy và tính toàn vẹn dữ liệu.

c) Nền tảng phải có cơ chế giới hạn tần suất yêu cầu và xếp hàng công bằng ở phân hệ điều khiển, bảo đảm một bên sử dụng không thể làm cạn kiệt năng lực điều phối của toàn nền tảng.

d) Đối với Mức 5, tổ chức vận hành nền tảng nên thực hiện thử nghiệm gây lỗi có chủ đích định kỳ tối thiểu 01 lần trên 12 tháng, trên môi trường do tổ chức vận hành lựa chọn, với phạm vi giới hạn ở các loại lỗi nêu tại điểm a) khoản này, có kế hoạch quay lui, kịch bản và kết quả được lập hồ sơ.

6.2.2 Bảo vệ mạng và kết nối an toàn

6.2.2.1 Phân lập mạng và kiểm soát luồng

a) Mạng riêng ảo (VPC) của các chủ thuê phải phân lập hoàn toàn ở cả lớp liên kết dữ liệu và lớp mạng. Việc liên thông kết nối giữa hai mạng VPC phải là hành động tường minh, trải qua phê duyệt và được ghi nhật ký.

b) Mọi chức năng mạng ảo phải thực hiện được và hỗ trợ tương đương với cả giao thức IPv4 và IPv6.

c) Nền tảng phải áp dụng cơ chế tường lửa phân tán tại giao diện mạng của từng máy ảo, hoạt động độc lập với hệ điều hành khách. Chính sách tường lửa mặc định trên toàn hệ thống phải là "Từ chối toàn bộ".

d) Nền tảng phải có tính năng chống giả mạo địa chỉ mạng (MAC/IP spoofing, Rogue DHCP/Router) phát sinh từ bên trong máy ảo. Các gói tin vi phạm quy tắc giả mạo phải bị loại bỏ tại lớp ảo hóa, sinh cảnh báo nhưng không được ngắt toàn bộ giao diện mạng hợp lệ của máy ảo.

đ) Đối với mức 4, mức 5 nền tảng phải hỗ trợ tính năng chuỗi dịch vụ mạng, ép luồng dữ liệu đi qua chuỗi các thiết bị bảo mật ảo (vFW, vWAF) trước khi ra hoặc vào mạng ngoài.

6.2.2.2 Bảo vệ đường truyền và giám sát mạng

a) Mọi giao tiếp giữa các thành phần nền tảng và giao tiếp với hệ thống ngoài phải được mã hóa.

b) Đối với mức 4, mức 5 nền tảng phải áp dụng cơ chế xác thực hai chiều đối với API quản trị.

c) Nền tảng phải cho phép chủ thuê thu thập và truy vấn nhật ký luồng mạng giữa các máy ảo nằm trong cùng một mạng con.

d) Dữ liệu nhật ký luồng mạng phải được hệ thống phân tách theo định danh của chủ thuê.

đ) Bộ định tuyến ảo phải có khả năng giao tiếp định tuyến động (BGP/OSPF) với thiết bị vật lý.

e) Các phiên định tuyến động giữa bộ định tuyến ảo và thiết bị vật lý phải được xác thực.

g) Nền tảng phải có cơ chế giới hạn dải địa chỉ IP được phép quảng bá trên bộ định tuyến ảo.

6.2.3 Quản lý danh tính, quyền truy cập và đặc quyền

6.2.3.1 Định danh và phân quyền chủ thuê

a) Nền tảng phải hỗ trợ chủ thuê tích hợp hệ thống định danh riêng (IdP).

b) Việc vô hiệu hóa tài khoản tại hệ thống định danh của chủ thuê phải sinh ra hiệu lực tức thời trên nền tảng đám mây.

c) Cơ chế kiểm soát truy cập theo vai trò (RBAC) phải có hiệu lực đồng nhất trên Console, CLI và API.

d) Nền tảng phải hỗ trợ tính năng cho phép chủ thuê tự định nghĩa các vai trò mới ngoài hệ thống mẫu.

đ) Nền tảng phải áp dụng nguyên tắc quyền hiệu lực là phần giao của các phạm vi được phép khi người dùng được gán nhiều vai trò.

e) Đối với mức 5, nền tảng phải áp dụng cơ chế xác thực liên tục theo ngữ cảnh, không mặc định tin tưởng kết nối dù xuất phát từ mạng nội bộ.

g) Đối với mức 5, quyền truy cập phải được đánh giá lại liên tục dựa trên định danh, trạng thái bảo mật của thiết bị đầu cuối, vị trí địa lý và thời điểm truy cập.

h) Yếu tố xác thực đa yếu tố (MFA) đối với tài khoản quản trị nền tảng phải dựa trên phần cứng chống sao chép.

6.2.3.2 Phân tách quyền quản trị

a) Nền tảng phải phân tách đặc quyền quản trị thành tối thiểu 03 vai trò độc lập: Quản trị hạ tầng (không tiếp cận dữ liệu rõ, không sửa kiểm toán); Quản trị khóa (không can thiệp hạ tầng); và Kiểm toán viên (chỉ đọc).

b) Nền tảng phải có cơ chế từ chối kỹ thuật đối với việc gán đồng thời nhiều vai trò quản trị độc lập cho cùng một chủ thể.

c) Đối với mức 5, không được phép tồn tại bất kỳ tài khoản kỹ thuật đơn lẻ nào (kể cả Root/Admin) có khả năng vượt qua sự phân tách quyền quản trị này.

d) Việc tuân thủ phân tách quyền quản trị phải được rà soát định kỳ tối thiểu 01 lần/06 tháng.

6.2.3.3 Giới hạn tiếp cận và mở quyền khẩn cấp

a) Quản trị viên điều hành nền tảng không được mặc định cấp các quyền: truy cập bảng điều khiển máy ảo, tải bản chụp, gắn ổ đĩa của chủ thuê.

b) Mọi can thiệp phá vỡ ranh giới quản trị thông thường phải áp dụng cơ chế mở quyền khẩn cấp với các yêu cầu: gắn mã sự vụ, có phê duyệt độc lập, tự động thu hồi quyền.

c) Thời hạn hiệu lực của một phiên mở quyền khẩn cấp không được vượt quá 08 giờ với mức 3, mức 4 và không quá 04 giờ đối với Mức 5.

d) Toàn bộ phiên thao tác dưới quyền khẩn cấp phải được ghi lại toàn bộ nội dung lệnh, gửi thông báo tức thời cho chủ thuê và tự động sinh báo cáo hậu kiểm trong không quá 24 giờ.

đ) Các thao tác nguy hiểm (xóa chủ thuê, xóa hàng loạt tài nguyên, đổi chính sách kiểm toán/thuật toán mật mã, hủy khóa) phải chịu cơ chế phê duyệt của tối thiểu hai chủ thể độc lập trực tiếp trên nền tảng.

e) Đối với mức 5, nền tảng phải áp dụng thời gian chờ hiệu lực mặc định không dưới 24 giờ đối với các thao tác có tác động không thể đảo ngược, trong đó bất kỳ chủ thể phê duyệt nào cũng có quyền hủy bỏ.

6.2.4 Bảo vệ dữ liệu, mật mã và quản lý khóa

6.2.4.1 Ranh giới trách nhiệm và quyền mã hóa của chủ thuê

a) Tổ chức vận hành nền tảng phải công bố rõ ràng về phạm vi dữ liệu hệ thống có khả năng giải mã và phạm vi không thể giải mã.

b) Nền tảng không được thiết lập cơ chế cản trở việc chủ thuê tự áp dụng mã hóa hoặc đưa ra yêu cầu chủ thuê phải giao khóa mã hóa.

c) Mọi chức năng duy trì hoạt động của nền tảng (sao lưu, tạo bản chụp, di chuyển máy ảo) phải hoạt động bình thường trên các ổ đĩa đã được chủ thuê mã hóa mà không cần bản rõ.

d) Nền tảng phải cho phép chủ thuê chỉ định vùng lưu trữ địa lý cho dữ liệu của mình.

đ) Hệ thống phải chặn kỹ thuật mọi thao tác di chuyển dữ liệu ra khỏi phạm vi vùng lưu trữ đã được chủ thuê chỉ định.

6.2.4.2 Mã hóa nền tảng và linh hoạt thuật toán

a) Nền tảng phải có chức năng mã hóa dữ liệu tĩnh đối với toàn bộ ổ đĩa, bản chụp và hệ thống sao lưu.

b) Khi chức năng mã hóa được kích hoạt, mỗi đối tượng dữ liệu riêng biệt phải sử dụng một khóa riêng độc lập.

c) Kiến trúc mật mã của nền tảng phải tách biệt tính năng ứng dụng khỏi thư viện mã nguồn gốc.

d) Nền tảng phải cho phép người dùng thay đổi thuật toán và tích hợp sản phẩm mật mã an ninh mà không cần khởi động hay dừng dịch vụ.

đ) Đối với mức 5, nền tảng phải hỗ trợ khả năng chuyển đổi sang việc sử dụng thuật toán kháng lượng tử (PQC) khi có chính sách yêu cầu.

6.2.4.3 Quản lý khóa, bí mật và xóa dữ liệu an toàn

a) Nền tảng phải có cơ chế quản lý vòng đời độc lập cho các thông tin bí mật như khóa API token, chứng thư, mật khẩu cơ sở dữ liệu.

b) Hệ thống phải hỗ trợ luân chuyển khóa bí mật tự động và cung cấp thông tin an toàn vào máy ảo mà không lộ bản rõ ra ngoài.

c) Khóa mật mã phải được lưu trữ trong mô-đun bảo mật phần cứng (HSM).

d) Đối với mức 4, mức 5 thiết bị HSM phải đạt chuẩn an toàn vật lý được công nhận (tối thiểu tương đương chuẩn FIPS 140-2/3 Mức 3 hoặc tiêu chuẩn quốc gia tương ứng).

đ) Thiết bị HSM phải có tính năng chống giả mạo vật lý, tự động xóa khóa khi phát hiện cạy phá và không cung cấp thao tác trích xuất khóa ở dạng rõ.

e) Thao tác hủy khóa hoặc xuất khóa phải trải qua phê duyệt nhiều bên và phải sinh nhật ký kiểm toán hệ thống.

g) Khi ổ đĩa hoặc máy ảo bị xóa/thu hồi, vùng vật lý (RAM, Storage, GPU) phải được hệ thống tự động xóa an toàn trước khi cấp phát cho người dùng mới thông qua phương pháp hủy khóa mã hóa hoặc ghi đè.

h) Phương pháp ghi đè đối với vùng lưu trữ không sử dụng mã hóa phải tuân thủ tiêu chuẩn an toàn (ví dụ: NIST SP 800-88), bảo đảm dữ liệu không thể khôi phục bằng công cụ pháp y số.

i) Việc xóa an toàn phải hoàn tất trong thời hạn không quá 24 giờ kể từ thời điểm tài nguyên được giải phóng đối với Mức 5, và không quá 07 ngày đối với Mức 3 và Mức 4.

6.2.5 Quản lý cấu hình, điểm yếu, thay đổi và sự cố

6.2.5.1 Quản lý vòng đời, điều phối tài nguyên và cấu hình an toàn

a) Nền tảng phải cho phép tăng giảm mức cấp phát tài nguyên tính toán (CPU, RAM, Disk) khi máy ảo vẫn đang ở trạng thái chạy.

b) Nền tảng phải hỗ trợ di chuyển máy ảo đang chạy giữa các máy chủ vật lý với nhau.

c) Hệ thống phải thực hiện xác thực điểm đầu và điểm cuối trước khi thực hiện luồng di chuyển máy ảo.

d) Toàn bộ dữ liệu truyền tải trong quá trình di chuyển máy ảo phải được mã hóa.

đ) Đối với mức 4, mức 5 mạng và luồng lưu lượng phục vụ việc di chuyển máy ảo phải được tách biệt logic hoàn toàn khỏi mạng chứa dữ liệu của chủ thuê.

e) Hệ điều hành chủ và các thành phần ảo hóa của nền tảng phải được thiết lập cấu hình an toàn theo các tiêu chuẩn quốc tế/quốc gia được công nhận.

g) Nền tảng phải triển khai công cụ tự động quét và cảnh báo sự sai lệch cấu hình của các thành phần lõi.

h) Khi phát hiện sự sai lệch cấu hình ngoài cửa sổ bảo trì, hệ thống phải có cơ chế tự động hoàn tác để đưa tài nguyên về lại trạng thái cấu hình an toàn tiêu chuẩn.

i) Hệ thống phải triển khai giải pháp phát hiện và phản hồi điểm cuối (EDR) ở cấp độ nhân hệ điều hành trên các máy chủ vật lý chạy lớp ảo hóa lõi nhằm phát hiện tấn công thoát lớp ảo hóa.

k) Tác nhân (Agent) giám sát và bảo mật phải đăng ký trực tiếp với mô-đun an ninh nhân hệ điều hành để tạo cảnh báo thời gian thực khi bị vô hiệu hóa.

l) Tác nhân và tiện ích mở rộng không được phép tải trực tiếp từ mạng Internet; phải được tải qua kho lưu trữ tập trung và tự động kiểm tra chữ ký số, mã băm trước khi cài đặt.

m) Nền tảng phải tự động phát hiện, cảnh báo hoặc cô lập các máy ảo không có tương tác cấu hình hoặc hiệu năng sử dụng ở mức tối thiểu liên tục trong vòng 14 ngày (hệ thống có hỗ trợ danh sách ngoại lệ đối với máy ảo dự phòng).

n) Đối với môi trường vùng chứa ở trạng thái lỗi liên tục hoặc không hoạt động, hệ thống điều phối phải tự động gỡ bỏ trong thời gian không quá 48 đến 72 giờ.

o) Trước khi tự động xóa bỏ vùng chứa, nền tảng bắt buộc phải thực hiện kết xuất và bảo lưu an toàn hệ thống siêu dữ liệu cùng nhật ký trạng thái cục bộ để phục vụ mục đích điều tra sự cố.

p) Hoạt động rà quét điểm yếu, lỗ hổng bảo mật phải được thiết kế và cấu hình theo phương thức không gây gián đoạn.

q) Công cụ rà quét phải có cơ chế kiểm soát băng thông và tài nguyên nhằm đảm bảo không làm ảnh hưởng đến hiệu năng của các máy ảo/vùng chứa đang vận hành.

r) Kết quả báo cáo rà quét lỗ hổng bảo mật phải được phân tách nghiêm ngặt theo ranh giới của từng khách thuê.

6.2.5.2 Nâng cấp, bảo trì và vá khẩn cấp

a) Nền tảng phải hỗ trợ quy trình nâng cấp theo hình thức cuốn chiếu và duy trì khả năng vận hành hỗn hợp giữa các phiên bản.

b) Nền tảng phải hỗ trợ khả năng quay lại (rollback) phiên bản mà không gây mất dữ liệu.

c) Tổ chức vận hành nền tảng phải thiết lập quy trình vá khẩn cấp đối với các lỗ hổng bảo mật đang bị khai thác thực tế, đáp ứng thời hạn quy định pháp luật.

d) Quy trình vá khẩn cấp được phép cấu hình bỏ qua thời gian chờ nhưng không được miễn trừ bước xác minh chữ ký gói cập nhật và ghi nhật ký kiểm toán.

đ) Nền tảng phải hỗ trợ chế độ bảo trì máy chủ chuyên dụng, cho phép tự động sơ tán toàn bộ máy ảo sang máy chủ khác trước khi thực hiện bảo trì.

6.2.5.3 Xác định ảnh hưởng và thông báo sự cố

a) Khi phát sinh sự cố tại tầng hạ tầng, nền tảng phải tự động xác định được danh sách các chủ thuê bị ảnh hưởng.

b) Nền tảng phải có khả năng tự động gửi thông báo qua tối thiểu hai kênh liên lạc độc lập tới các chủ thuê bị ảnh hưởng.

c) Thông báo sự cố chỉ được chứa thông tin liên quan đến tài nguyên của chủ thuê nhận thông báo, tuyệt đối không bao gồm thông tin của chủ thuê khác.

d) Hệ thống phải cho phép cấu hình thời gian giới hạn tự động phát thông báo sự cố để chủ quản HTTT kịp báo cáo theo quy định pháp luật.

6.2.5.4 Bảo mật Hạ tầng dưới dạng mã (Infrastructure as Code - IaC)

a) Nền tảng phải hỗ trợ tính năng quản lý cấu hình và triển khai hạ tầng thông qua tệp mã nguồn (IaC).

b) Phân hệ quản lý IaC phải được cấu hình kiểm soát phiên bản, kiểm soát truy cập và phân quyền chi tiết cho từng tác vụ chỉnh sửa hoặc triển khai hạ tầng.

c) Nền tảng phải triển khai cơ chế kiểm tra tự động trước mỗi lần triển khai tệp IaC vào môi trường vận hành.

d) Hệ thống kiểm tra phải phát hiện được các cấu hình sai lệch mất an toàn và rà quét để ngăn chặn thông tin xác thực, khóa mật mã bị lưu trữ dưới dạng bản rõ trong mã nguồn.

đ) Nền tảng phải cung cấp môi trường độc lập (Staging/Sandbox) phục vụ việc kiểm thử cấu hình tệp IaC trước khi chính thức áp dụng vào mặt phẳng điều khiển hoặc phân hệ dữ liệu.

e) Kho quản lý mã nguồn của nền tảng và các tệp IaC phải được thiết lập cấu hình bảo vệ nhằm khóa chặt các nhánh mã nguồn chính.

g) Nền tảng quản lý mã nguồn phải vô hiệu hóa tính năng tự động phê duyệt gộp mã.

h) Mọi sự thay đổi và đẩy mã (push/merge) vào nhánh chính phải bị hệ thống từ chối nếu chưa trải qua kiểm tra độc lập và phê duyệt bởi nhân sự có thẩm quyền.

6.2.6 Nhật ký, giám sát, tích hợp và cung cấp bằng chứng

6.2.6.1 Nhật ký kiểm toán nội bộ và neo toàn vẹn

a) Nền tảng phải ghi nhận đầy đủ vào nhật ký kiểm toán đối với mọi thao tác nhạy cảm: đọc dữ liệu nhạy cảm (truy cập bảng điều khiển máy ảo, tải/xuất ảnh máy ảo, bản chụp, ổ đĩa), mọi thao tác thất bại hoặc bị từ chối quyền, hoạt động của cơ chế mở quyền khẩn cấp/phê duyệt nhiều bên, thao tác trên khóa mật mã và chính sách thuật toán.

b) Mỗi bản ghi kiểm toán phải chứa bổ sung các trường: vai trò đang sử dụng; định danh bên sử dụng liên quan; mã truy vết liên kết các bản ghi thuộc cùng một giao dịch.

c) Nhật ký kiểm toán phải được ghi ở chế độ chỉ thêm. Nền tảng không được có chức năng cho phép sửa đổi hoặc xóa từng bản ghi riêng lẻ, kể cả đối với tài khoản có đặc quyền cao nhất. Việc xóa theo chính sách lưu giữ chỉ được thực hiện theo đơn vị là toàn bộ khoảng thời gian hoặc toàn bộ tệp nhật ký đã hết thời hạn lưu giữ và đã được chuyển thành công ra hệ thống lưu trữ độc lập; thao tác xóa theo chính sách phải sinh bản ghi kiểm toán. Đây là yêu cầu bắt buộc về kiến trúc theo quy định.

d) Bản ghi kiểm toán phải mang số thứ tự liên tục theo nguồn sinh nhật ký, cho phép phát hiện khoảng trống. Đối với Mức 4 và Mức 5, dữ liệu nhật ký kiểm toán phải được bảo vệ bằng cơ chế neo toàn vẹn mật mã để phát hiện hành vi sửa đổi, xóa hoặc chèn bản ghi.

đ) Đối với Mức 5, nền tảng phải tự động gửi định kỳ (chu kỳ không quá 01 giờ) giá trị neo toàn vẹn tới một hệ thống lưu giữ độc lập nằm ngoài phạm vi kiểm soát của tổ chức vận hành nền tảng hoặc hệ thống giám sát của cơ quan có thẩm quyền. Nền tảng không được có chức năng cho phép sửa đổi hoặc chặn luồng gửi này, kể cả đối với tài khoản có đặc quyền cao nhất.

e) Nền tảng phải sinh bản ghi kiểm toán và cảnh báo đối với các sự kiện điều khiển hoạt động ghi nhật ký (bật, tắt, tạm dừng tiến trình sinh nhật ký, thay đổi chính sách lưu giữ, thay đổi đích chuyển nhật ký). Bản ghi đối với các sự kiện này phải được sinh trên đường độc lập với tiến trình sinh nhật ký bị tác động.

6.2.6.2 Cung cấp nhật ký và giám sát cho chủ thuê

a) Nền tảng phải cung cấp chức năng cho phép chủ thuê trích xuất toàn bộ nhật ký thao tác trên tài nguyên của họ, bao gồm cả các thao tác được thực hiện bởi người vận hành nền tảng.

b) Tổ chức vận hành nền tảng bị cấm hoàn toàn khả năng chỉnh sửa hoặc lọc bỏ các bản ghi trong tệp nhật ký gửi cho chủ thuê.

c) Nhật ký đẩy về hệ thống giám sát an ninh mạng (SOC/SIEM) tập trung theo quy định của pháp luật và phải được phân tách định danh rõ ràng theo từng chủ thuê.

d) Luồng dữ liệu đẩy nhật ký phải đi qua bộ đệm cục bộ chống mất dữ liệu và phải tích hợp tính năng tự động che giấu đối với các trường dữ liệu xác thực nhạy cảm.

đ) Hệ thống tường lửa phân tán, tường lửa ứng dụng web (WAF) hoặc API Gateway của nền tảng phải được tích hợp cơ sở dữ liệu định tuyến địa lý (Geo-IP) và được cập nhật liên tục.

e) Hệ thống phải có cơ chế nhận diện, chặn hoặc ghi nhật ký kiểm toán mang tính bất biến đối với các tác vụ trích xuất dữ liệu hàng loạt hướng đến địa chỉ IP đích nằm ngoài lãnh thổ Việt Nam.

6.2.6.3 Báo cáo tuân thủ và chứng cứ số

a) Nền tảng phải cung cấp tính năng tự động đánh giá và xuất báo cáo trạng thái tuân thủ cấu hình an toàn của hệ thống dựa trên các tiêu chuẩn bảo mật hiện hành.

b) Bất kỳ thay đổi trái phép nào đối với cấu hình lõi của hệ thống phải tự động sinh ra cảnh báo mức cao.

c) Nền tảng phải cung cấp tính năng cho phép chủ thuê tự thực hiện thao tác cách ly khẩn cấp (cắt mạng lưới, không tắt máy ảo).

d) Nền tảng phải cho phép chủ thuê thực hiện tạo bản chụp bộ nhớ máy ảo để thu thập chứng cứ số, xuất kèm giá trị băm nhằm bảo toàn chuỗi hành trình chứng cứ pháp y.

6.2.6.4 Giám sát tình trạng hoạt động và mục tiêu khả dụng

a) Nền tảng phải theo dõi và hiển thị tình trạng hoạt động của từng thành phần thuộc: phân hệ điều khiển, phân hệ dữ liệu, phân hệ mạng ảo, phân hệ lưu trữ, phân hệ quản lý định danh và phân hệ quản lý khóa. Phân biệt tối thiểu ba trạng thái: hoạt động bình thường, hoạt động suy giảm và ngừng hoạt động.

b) Nền tảng phải sinh cảnh báo khi một thành phần chuyển sang trạng thái suy giảm hoặc ngừng hoạt động, kể cả khi cơ chế chịu lỗi đã che lấp tác động đối với bên sử dụng. Cảnh báo phải nêu thành phần, thời điểm và mức độ.

c) Nền tảng phải xuất được chỉ số vận hành theo định dạng chuẩn máy đọc được, cho phép tổ chức vận hành nền tảng đưa vào hệ thống giám sát của mình. Nhà cung cấp phải công bố danh mục chỉ số và ý nghĩa của từng chỉ số.

d) Tổ chức vận hành phải công bố mục tiêu khả dụng của từng dịch vụ đám mây, phương pháp đo và cách xử lý thời gian bảo trì có kế hoạch. Việc xác định, mô tả và đo lường chỉ tiêu mức dịch vụ thực hiện theo TCVN 13054-1:2020.

đ) Mục tiêu khả dụng phải được đo bằng chỉ số quan sát được từ phía bên sử dụng. Nền tảng phải cung cấp được số liệu mức độ đạt mục tiêu khả dụng đối với dịch vụ và tài nguyên thuộc phạm vi của từng bên sử dụng, theo khoảng thời gian do bên yêu cầu lựa chọn, truy xuất được qua giao diện lập trình dành cho bên sử dụng mà không cần thao tác của tổ chức vận hành nền tảng.

e) Phương pháp đo mục tiêu khả dụng phải tuân thủ các nguyên tắc sau: đo riêng cho từng dịch vụ, tối thiểu tách phân hệ điều khiển và phân hệ dữ liệu; phân hệ điều khiển đo bằng tỷ lệ yêu cầu giao diện lập

trình được xử lý thành công trong ngưỡng thời gian đáp ứng đã công bố; phân hệ dữ liệu đo bằng khả năng truy cập và thực hiện chức năng chính của từng tài nguyên.

g) Đơn vị tính khả dụng là thời lượng theo từng tài nguyên của từng bên sử dụng, không tính gộp trên toàn nền tảng; một tài nguyên chỉ được tính là không khả dụng khi mất khả năng liên tục quá khoảng thời gian tối thiểu cấu hình được; chu kỳ tính là tháng; thời gian bảo trì có kế hoạch chỉ được loại trừ khi đã thông báo trước đúng thời hạn công bố; suy giảm một phần được tính theo tỷ lệ tài nguyên bị ảnh hưởng.

6.2.7 Sao lưu, phục hồi, tính liên tục và triển khai đa vùng

6.2.7.1 Sao lưu bất biến

a) Bản sao lưu hệ thống phải được lưu ở chế độ ghi bất biến.

b) Nền tảng phải bảo đảm không một tài khoản nào (kể cả tài khoản đặc quyền cao nhất) được phép xóa, sửa đổi hoặc ghi đè bản sao lưu trong thời gian chu kỳ lưu giữ đã được cấu hình.

c) Nền tảng phải hỗ trợ khả năng tạo các bản sao lưu nhất quán với trạng thái ứng dụng.

d) Chủ thuê phải được cấp quyền tự kích hoạt kiểm tra tính toàn vẹn và khả năng khôi phục bản sao lưu của mình mà không cần chờ tổ chức vận hành nền tảng thực hiện.

đ) Nền tảng phải cung cấp cơ chế và công cụ tự động thực hiện rà quét mã độc/phần mềm độc hại đối với toàn bộ các bản sao lưu trước khi tiến hành trích xuất hoặc khôi phục dữ liệu vào môi trường thực tế.

e) Toàn bộ cơ sở dữ liệu trạng thái và cấu hình của phân hệ điều khiển phải được sao lưu định kỳ và khôi phục được về trạng thái nhất quán. Sau khi khôi phục, nền tảng phải nhận diện lại đầy đủ và chính xác toàn bộ tài nguyên đang tồn tại, không làm mất tài nguyên và không phát sinh tài nguyên vô chủ.

6.2.7.2 Liên tục hoạt động và diễn tập dự phòng (DR)

a) Nền tảng phải cung cấp tính năng đồng bộ hóa dữ liệu giữa cụm trung tâm dữ liệu chính và trung tâm dữ liệu dự phòng.

b) Tổ chức vận hành phải cung cấp các chỉ tiêu công bố rõ ràng về thời gian mất dữ liệu tối đa (RPO) và thời gian phục hồi tối đa (RTO).

c) Đối với mức 4, mức 5 khả năng chuyển đổi dự phòng của hệ thống phải được thử nghiệm và lập biên bản định kỳ tối thiểu 01 lần/12 tháng.

d) Nền tảng phải hỗ trợ tính năng diễn tập khôi phục thảm họa tự động, tạo môi trường cô lập tại vùng dự phòng nhằm không làm gián đoạn luồng dịch vụ sản xuất đang hoạt động tại vùng chính.

đ) Hệ thống phải duy trì khả năng tự vận hành theo kịch bản liên tục hoạt động (BCP) ngay cả trong tình huống mất khả năng tiếp cận nhà cung cấp phần mềm nền tảng.

6.2.7.3 Quản trị đa vùng

a) Đối với mức 4, mức 5 nền tảng phải hỗ trợ cổng quản trị khả năng quản lý liên vùng.

b) Cổng quản trị liên vùng không được phép làm mở rộng quyền hạn của người quản trị vượt quá phạm vi đặc quyền đã được xét duyệt tại từng vùng.

c) Nền tảng phải hỗ trợ khả năng liên kết mạng riêng ảo (VPC) giữa các vùng thông qua dải địa chỉ IP dùng riêng.

d) Hệ thống phải hỗ trợ tính năng luân chuyển tải tự động giữa các vùng nếu một vùng gặp sự cố mất khả năng phục vụ.

6.2.8 Quản lý chuỗi cung ứng, khả chuyển và chủ quyền công nghệ

6.2.8.1 Chủ quyền công nghệ và kiểm chứng mã nguồn

a) Quyền sử dụng phần mềm cấu thành nền tảng phải là quyền vĩnh viễn, nền tảng tuyệt đối không bị khóa tính năng khi hết thời hạn bảo hành hoặc hỗ trợ kỹ thuật.

b) Đối với các thành phần thuộc đường thực thi lõi (bộ ảo hóa, phân hệ điều khiển, mạng ảo, lưu trữ, định danh, quản lý khóa), nhà cung cấp dịch vụ phải làm chủ toàn diện kiến trúc mã nguồn từ lớp ảo hóa và sở hữu đội ngũ phát triển tại Việt Nam. Nhà cung cấp phải đáp ứng đồng thời ba điều kiện sau: có quyền hợp pháp sửa đổi và phân phối lại mã nguồn; dựng lại được toàn bộ bản triển khai từ mã nguồn trong môi trường không kết nối ra ngoài; và thực hiện được việc sửa đổi mã nguồn, biên dịch, kiểm thử hồi quy, ký số và phát hành bản vá mà không cần hành động của tổ chức nước ngoài.

c) Hệ thống nền tảng không được tồn tại các tài khoản mặc định hoặc ẩn, không có khóa mật mã và chứng thư gắn cứng trong mã nguồn, không có kênh quản trị không được tài liệu hóa và không chứa mã lệnh kết nối ra ngoài không được khai báo.

d) Nhà cung cấp phải đáp ứng năng lực và sẵn sàng dựng môi trường độc lập theo yêu cầu của cơ quan có thẩm quyền để rà soát mã nguồn. Mã nguồn sau khi rà soát phải chứng minh được sự khớp nối hoàn toàn với bản cài đặt thực thi đang vận hành thông qua quy trình đối chiếu mã băm.

đ) Nhà cung cấp phải công bố thời hạn phát hành bản vá đối với lỗ hổng của phần mềm nền tảng theo mức độ nghiêm trọng. Nhà cung cấp phải công bố số liệu thời gian phát hành bản vá thực tế của các phiên bản đã phát hành, phục vụ đối chiếu với thời hạn đã công bố.

6.2.8.2 Vận hành ngoại tuyến và an ninh chuỗi cung ứng

a) Nền tảng phải hoạt động 100% chức năng trong môi trường mạng đóng kín và không yêu cầu kết nối Internet để xác thực bản quyền với nhà cung cấp.

b) Nền tảng phải hỗ trợ đầy đủ quy trình cập nhật ngoại tuyến và bảo đảm mọi bản vá phát hành phải được ký số.

c) Nền tảng phải có khả năng tự động sinh Bản kê thành phần phần mềm (SBOM) ở định dạng dữ liệu có cấu trúc chuẩn quốc tế (như CycloneDX JSON, SPDX hoặc định dạng tương đương).

d) Nền tảng không được sử dụng SBOM xuất ở định dạng văn bản phi cấu trúc (ví dụ: PDF, TXT thông thường).

đ) Danh mục SBOM phải được tích hợp vào hệ thống đường ống CI/CD nhằm thực thi rà quét tự động đối chiếu với cơ sở dữ liệu lỗ hổng bảo mật (CVE).

e) Nền tảng phải cung cấp giao diện API lập trình mở, có tài liệu hỗ trợ xuất/nhập toàn bộ máy ảo và dữ liệu của chủ thuê theo định dạng tiêu chuẩn.

g) Nền tảng phải bảo đảm tính khả chuyển dữ liệu để ngăn chặn hoàn toàn rủi ro khóa chặt vào hệ sinh thái của một nhà cung cấp.

7. Yêu cầu chức năng nghiệp vụ riêng đối với sản phẩm theo mô hình dịch vụ

7.1 Khái quát

Thiết lập các tính năng, giao diện và công cụ quản trị mà nền tảng điện toán đám mây bắt buộc phải cung cấp cho bên sử dụng (chủ thuê) tương ứng với từng mô hình dịch vụ: Hạ tầng dưới dạng dịch vụ (IaaS), Nền tảng dưới dạng dịch vụ (PaaS) và Phần mềm dưới dạng dịch vụ (SaaS). Việc đáp ứng các yêu cầu này là điều kiện kỹ thuật cốt lõi để chủ thuê có đủ năng lực tự quản lý, tự kiểm soát tài nguyên và bảo vệ dữ liệu thuộc phạm vi trách nhiệm của mình trên hạ tầng dùng chung.

7.2 Yêu cầu cụ thể

7.2.1 Yêu cầu riêng đối với mô hình dịch vụ hạ tầng (IaaS)

Trong mô hình IaaS, tổ chức vận hành nền tảng quản lý hạ tầng vật lý và lớp ảo hóa; chủ thuê quản lý hệ điều hành khách, nền tảng ứng dụng và dữ liệu.

a) Nền tảng phải cung cấp cổng thông tin và giao diện lập trình ứng dụng (API) an toàn, cho phép chủ thuê tự thực hiện các thao tác quản lý vòng đời tài nguyên (khởi tạo, cấu hình, tạm dừng, khởi động lại, thu hồi) đối với máy ảo, mạng ảo và không gian lưu trữ mà không cần sự can thiệp thủ công từ tổ chức vận hành nền tảng.

b) Nền tảng phải cung cấp giao diện cho phép chủ thuê tự thiết lập cấu hình mạng riêng ảo (VPC), tự phân chia mạng con (subnet), tự cấu hình bảng định tuyến và tự quản lý các quy tắc kiểm soát truy cập/tường lửa (Security Groups/NACL) cho từng máy ảo.

c) Nền tảng phải cho phép chủ thuê tự tải lên và khởi tạo máy ảo từ các tệp tin ảnh hệ điều hành do chủ thuê tự chuẩn bị. Quá trình tải lên phải đi kèm tính năng rà quét mã độc tự động trước khi lưu vào kho ảnh của chủ thuê.

d) Nền tảng phải cung cấp cơ chế truy cập bảng điều khiển ngoài băng tần (Out-of-Band Console qua VNC, SPICE hoặc Serial) trực tiếp trên giao diện web để chủ thuê có thể can thiệp vào máy ảo khi máy ảo bị mất kết nối mạng. Kênh truy cập này phải được mã hóa và xác thực.

đ) Nền tảng phải cung cấp bảng điều khiển cho phép chủ thuê theo dõi thời gian thực mức độ tiêu thụ tài nguyên (vCPU, RAM, IOPS, Băng thông) và thiết lập cảnh báo khi chi phí hoặc mức tiêu thụ vượt ngưỡng (Quota/Billing Alerts).

e) Nền tảng phải hỗ trợ tính năng truyền các tập lệnh cấu hình khởi tạo vào máy ảo ngay trong quá trình khởi tạo để chủ thuê tự động hóa việc thiết lập hệ điều hành khách.

7.2.2 Yêu cầu riêng đối với mô hình dịch vụ nền tảng (PaaS)

a) Sản phẩm PaaS phải tự động hóa toàn bộ việc cài đặt, cấu hình và cập nhật bản vá bảo mật cho hệ điều hành nền và các phần mềm môi trường thực thi (ví dụ: nền tảng Java, Node.js, PHP) mà không làm thay đổi hay gián đoạn mã nguồn ứng dụng của chủ thuê.

b) Nền tảng phải cung cấp tính năng tự động mở rộng hoặc thu hẹp số lượng phiên bản ứng dụng (instances/pods) dựa trên các chỉ số hiệu năng (CPU, Memory, Request rate) do chủ thuê thiết lập trước.

c) Đối với các dịch vụ cơ sở dữ liệu, nền tảng phải cung cấp tính năng tự động sao lưu định kỳ, hỗ trợ khôi phục dữ liệu theo mốc thời gian cụ thể và hỗ trợ tính năng mã hóa dữ liệu minh bạch (Transparent Data Encryption - TDE) ở cấp độ cơ sở dữ liệu.

d) Nền tảng phải cung cấp các điểm kết nối tự động (Webhooks) và giao diện API chuẩn để chủ thuê dễ dàng tích hợp quy trình đẩy mã nguồn tự động từ kho lưu trữ lên môi trường thực thi.

đ) Trích xuất nhật ký ứng dụng tập trung: Nền tảng phải tự động thu thập nhật ký hoạt động của ứng dụng, nhật ký truy cập web và cung cấp công cụ để chủ thuê xem trực tiếp, phân tích hoặc cấu hình đẩy các nhật ký này về hệ thống giám sát SIEM của chủ thuê.

7.2.3 Yêu cầu riêng đối với mô hình dịch vụ phần mềm (SaaS)

a) Cách ly logic dữ liệu đa tiền thuê sản phẩm SaaS phải được thiết kế kiến trúc phân tách rạch ròi dữ liệu giữa các chủ thuê ở mức ứng dụng và cơ sở dữ liệu (thông qua Tenant ID, Schema riêng hoặc Database riêng). Nền tảng phải có cơ chế kiểm soát mã nguồn nghiêm ngặt bảo đảm người dùng của chủ thuê này tuyệt đối không thể truy vấn trái phép dữ liệu của chủ thuê khác thông qua việc thao túng URL hoặc tham số API.

b) Ứng dụng SaaS phải hỗ trợ tính năng đăng nhập một lần (SSO) thông qua các giao thức định danh liên thông tiêu chuẩn (SAML 2.0, OpenID Connect), cho phép chủ thuê quản lý xác thực người dùng hoàn toàn trên hệ thống định danh nội bộ (IdP) của riêng chủ thuê.

c) Sản phẩm phải cung cấp giao diện quản trị cho phép quản trị viên của chủ thuê tự do tạo nhóm, định nghĩa vai trò và phân quyền truy cập chức năng chi tiết cho từng người dùng thuộc tổ chức của mình.

d) Ứng dụng SaaS phải tự động ghi nhận nhật ký kiểm toán đối với các hành vi truy cập và thao tác trên dữ liệu nghiệp vụ nhạy cảm (như: ai đã xem, ai đã tải xuống, ai đã sửa đổi dữ liệu gì, vào thời điểm nào). Nhật ký này phải được cung cấp cho quản trị viên của chủ thuê.

đ) Sản phẩm phải cung cấp các công cụ trực quan hoặc giao diện API cho phép chủ thuê chủ động xuất toàn bộ dữ liệu nghiệp vụ, tệp đính kèm và nhật ký hoạt động của họ ra các định dạng tệp chuẩn mở (như CSV, JSON, XML) mà không cần sự trợ giúp thủ công từ nhà cung cấp.

e) Khi chủ thuê chấm dứt sử dụng dịch vụ SaaS, sản phẩm phải có quy trình kỹ thuật để xóa bỏ vĩnh viễn toàn bộ dữ liệu nghiệp vụ của chủ thuê đó khỏi cơ sở dữ liệu dùng chung và các bản sao lưu, đồng thời cung cấp xác nhận kỹ thuật về việc hoàn tất tiêu hủy dữ liệu.

Phụ lục A
(quy định)
Bảng áp dụng yêu cầu theo mức

Mục	Nội dung tóm tắt	Mức 3	Mức 4	Mức 5
6.2.1.1 (a-g)	Độc lập giữa phân hệ điều khiển và phân hệ dữ liệu; không điểm lỗi đơn	B	B	B
6.2.1.1 (i-k)	Quay lui thay đổi cấu hình	K	B	B
6.2.1.6 (d)	Thử nghiệm gây lỗi có chủ đích định kỳ 12 tháng	—	K	K
6.2.5.2 (đ-e)	Quy trình vá khẩn cấp có kiểm soát	B	B	B
6.2.5.2 (g)	Thông báo bảo trì có kế hoạch tới bên sử dụng	B	B	B
6.2.1.4	Quản lý chứng thư số nội bộ; nguồn thời gian tin cậy khi vận hành ngoại tuyến	B	B	B
6.2.6.4 (a-c)	Giám sát tình trạng hoạt động thành phần nền tảng; xuất chỉ số vận hành	B	B	B
6.2.6.4 (d-g)	Xác định và đo lường mục tiêu khả dụng theo từng bên sử dụng	B	B	B
6.2.5.1 (a-c)	Điều phối tải, phòng ngừa quá tải cục bộ	B	B	B
6.2.1.2 (đ)	Kiểm soát cấp phát vượt tài nguyên; không cấp phát vượt bộ nhớ ở Mức 5	K	B	B
6.2.5.1 (d)	Theo dõi và cảnh báo khi chỉ số quy mô đạt ngưỡng	K	B	B
6.2.1.2 (a-d)	Cách ly tiến trình máy ảo; giảm bề mặt tấn công lớp ảo hóa	B	B	B
6.2.1.2 (e-g)	Cách ly lõi xử lý vật lý theo bên sử dụng	—	K	B
6.2.1.3 (a-c)	Khởi động an toàn của máy chủ vật lý; đo lường trạng thái và xác minh từ xa	B	B	B

Mục	Nội dung tóm tắt	Mức 3	Mức 4	Mức 5
6.2.1.3 (d)	Rà quét và ký số ảnh máy ảo do nền tảng phát hành	B	B	B
6.2.1.3 (đ)	Năng lực rà quét ảnh máy ảo do bên sử dụng đưa vào	K	B	B
6.2.5.1 (đ)	Cấp phát tài nguyên khi máy ảo đang chạy	B	B	B
6.2.5.1 (e-i)	Di chuyển máy ảo đang chạy; cửa sổ gián đoạn và bảo đảm hội tụ	B	B	B
6.2.1.3 (e-h)	Bảo vệ dịch vụ siêu dữ liệu của máy ảo	B	B	B
6.2.2.1 (a-b)	Phân lập mạng giữa các bên sử dụng; hỗ trợ đồng thời IPv4 và IPv6	B	B	B
6.2.2.1 (h)	Chuỗi dịch vụ mạng	K	B	B
6.2.2.2 (d-đ)	Giám sát nhật ký luồng mạng giữa các máy ảo	K	B	B
6.2.2.2 (e-g)	Định tuyến động; xác thực phiên định tuyến; giới hạn dải quảng bá	K	B	B
6.2.2.2 (b-c)	Xác thực hai chiều giao diện quản trị; Hỗ trợ lớp mã hóa riêng trên đường truyền	K	B	B
6.2.4.2 (b)	Mã hóa theo từng đối tượng dữ liệu	B	B	B
6.2.7.1 (a-b)	Sao lưu bất biến	B	B	B
6.2.7.1 (c-d)	Bản sao lưu nhất quán với ứng dụng; tự kiểm tra khôi phục	K	B	B
6.2.7.1 (đ)	Sao lưu và khôi phục phân hệ điều khiển	B	B	B
6.2.4.3 (đ-h)	Xóa an toàn dữ liệu tồn dư ở lớp tài nguyên ảo	B	B	B
6.2.4.1 (d-đ)	Ràng buộc vị trí dữ liệu	K	B	B
6.2.3.1 (e)	Xác thực đa yếu tố dựa trên phần cứng chống sao chép	-	K	B

Mục	Nội dung tóm tắt	Mức 3	Mức 4	Mức 5
6.2.4.2 (c-e)	Kiến trúc mật mã tách rời cài đặt; tích hợp mật mã an ninh; chính sách thuật toán	B	B	B
6.2.4.2 (a)	Chức năng mã hóa dữ liệu bên sử dụng	B	B	B
6.2.4.3 (a-d)	Quản lý khóa tập trung; khóa trong HSM không trích xuất	B	B	B
6.2.4.1 (a-c)	Công bố phạm vi giải mã; không cản trở mật mã của bên sử dụng	B	B	B
6.2.3.2	Phân tách các vai trò quản trị được hệ thống cưỡng chế	K	B	B
6.2.3.3 (a-c)	Giới hạn tiếp cận tài nguyên bên sử dụng; cơ chế mở quyền khẩn cấp	K	B	B
6.2.3.3 (đ-g)	Phê duyệt nhiều bên đối với thao tác nguy hiểm; thời gian chờ hiệu lực	K	B	B
6.2.3.2 (d)	Thử nghiệm mô phỏng tấn công nội bộ (Red Teaming) định kỳ	-	K	B
6.2.6.1 (a-c)	Phạm vi ghi nhật ký bổ sung; nhật ký chỉ thêm	B	B	B
6.2.6.1 (d-đ)	Neo toàn vẹn mật mã cho nhật ký; gửi neo tới hệ thống lưu giữ độc lập bên ngoài	K	B	B
6.2.6.2 (c-e)	Đẩy nhật ký ra hệ thống lưu trữ độc lập; chặn trích xuất dữ liệu xuyên biên giới	B	B	B
6.2.6.2 (a-b)	Nhật ký dành cho bên sử dụng	B	B	B
6.2.6.3 (a-b)	Giám sát toàn vẹn thành phần nền tảng	K	B	B
6.2.6.3 (c-đ)	Cách ly khẩn cấp; thu thập chứng cứ số có kiểm soát	B	B	B
6.2.5.3	Xác định phạm vi ảnh hưởng sự cố và năng lực phát thông báo	B	B	B

Mục	Nội dung tóm tắt	Mức 3	Mức 4	Mức 5
6.2.7.2 (b-c)	Công bố chỉ tiêu dự phòng định lượng; thử nghiệm định kỳ	K	B	B
6.2.7.3 (a-c)	Quản trị liên vùng có kiểm soát; liên kết mạng và ảnh máy ảo giữa các vùng	-	B	B
6.2.7.3 (d)	Phân phối lưu lượng đa vùng và chuyển hướng khi mất vùng	K	K	B
6.2.8.1 (a-d)	Quyền và năng lực sửa đổi mã nguồn lõi; rà soát an ninh mã nguồn	B	B	B
6.2.8.1 (đ)	Cam kết thời hạn vá lỗ hổng; dựng lại bản triển khai đối chiếu băm	K	B	B
6.2.8.2 (a-b)	Vận hành ngoại tuyến; ký số gói cập nhật; chống hạ cấp	B	B	B
6.2.8.2 (c-đ)	Bản kê thành phần phần mềm (SBOM) định dạng chuẩn quốc tế sinh tự động	K	B	B
6.2.8.2 (e-g)	Quyền bên sử dụng chủ động rút dữ liệu (Khả chuyển)	B	B	B
7.2.1	Yêu cầu chức năng nghiệp vụ riêng đối với mô hình IaaS (cổng tự phục vụ, mạng ảo, BYOI, giám sát)	B	B	B
7.2.2	Yêu cầu chức năng nghiệp vụ riêng đối với mô hình PaaS (môi trường thực thi, DBaaS, CI/CD, trích xuất nhật ký)	B	B	B
7.2.3	Yêu cầu chức năng nghiệp vụ riêng đối với mô hình SaaS (cách ly dữ liệu, SSO, RBAC mức ứng dụng, khả chuyển)	B	B	B
Trong đó, B - bắt buộc; K - khuyến nghị; dấu gạch ngang - không áp dụng.				

Phụ lục B
(quy định)
Phương pháp thử nghiệm

Mỗi phép thử được mô tả theo cấu trúc: điều kiện ban đầu — hành động — kết quả kỳ vọng. Kết quả đạt yêu cầu chỉ khi toàn bộ kết quả kỳ vọng được thỏa mãn. Kết quả thử nghiệm theo Phụ lục này là bằng chứng về hiệu quả của biện pháp theo quy định của Khung quản lý rủi ro an ninh mạng.

B.1 Thử nghiệm độc lập giữa phân hệ điều khiển và phân hệ dữ liệu (Điều 6.2.1.1)

- Điều kiện: cụm đang vận hành với tối thiểu 20 máy ảo có tải, phân bố trên tối thiểu 3 máy chủ vật lý, có luồng lưu lượng đông–tây và bắc–nam liên tục.

- Hành động: Cô lập hoàn toàn mạng quản trị của toàn bộ phân hệ điều khiển trong 30 phút, sau đó khôi phục.

- Kết quả kỳ vọng: Không máy ảo nào dừng; không đứt phiên kết nối lớp giao vận; luật tường lửa phân tán giữ nguyên hiệu lực khi thử luồng vi phạm; sau khôi phục, trạng thái tự đồng bộ trong không quá 10 phút, không phát sinh tài nguyên vô chủ khi đối chiếu số lượng trước và sau.

B.2 Thử nghiệm xóa an toàn dữ liệu tồn dư (Điều 6.2.4.3)

Điều kiện: Cụm lưu trữ có dung lượng trống giới hạn để bảo đảm khả năng tái cấp phát cùng vùng vật lý.

Hành động: Tạo ổ đĩa cho bên sử dụng A, ghi mẫu dữ liệu nhận dạng được có độ dài tối thiểu 1 GB, xóa máy ảo và ổ đĩa. Tạo ổ đĩa mới cho bên sử dụng B, đọc thô toàn bộ khối dữ liệu bằng công cụ đọc mức khối. Lặp lại với bản chụp và với vùng nhớ của máy ảo bị hủy.

Kết quả kỳ vọng: Không tìm thấy bất kỳ đoạn dữ liệu nào của bên sử dụng A. Nhật ký kiểm toán ghi nhận việc hoàn tất xóa an toàn cho từng đối tượng. Thời điểm hoàn tất xóa an toàn ghi trong nhật ký nằm trong thời hạn quy định tại Điều 6.2.4.3.

B.3 Thử nghiệm ranh giới khả năng giải mã (Điều 6.2.4.1 và 6.2.4.2)

Điều kiện: Bên sử dụng thử nghiệm ghi hai tập dữ liệu. Tập thứ nhất chỉ được bảo vệ bằng chức năng mã hóa của nền tảng. Tập thứ hai được bên sử dụng mã hóa thêm ở lớp của mình, khóa không cung cấp cho tổ chức vận hành.

Hành động: Sử dụng tài khoản có đặc quyền cao nhất và có sự tham gia đồng thời của cả vai trò quản trị hạ tầng lẫn vai trò quản trị khóa, thử đọc nội dung của cả hai tập dữ liệu qua giao diện nền tảng, qua truy cập trực tiếp vùng lưu trữ và qua khôi phục từ bản sao lưu.

Kết quả kỳ vọng: Tập thứ nhất giải mã được, phù hợp với bản công bố; tập thứ hai không giải mã được bằng mọi đường. Mọi thao tác đều sinh bản ghi kiểm toán. Kết quả thử nghiệm phải trùng khớp với bản công bố phạm vi dữ liệu mà nền tảng có khả năng giải mã; sai lệch giữa bản công bố và kết quả thử nghiệm là không đạt.

B.4 Thử nghiệm khả năng thay thế thư viện mật mã (Điều 6.2.4.2)

Hành động: Nhà cung cấp cung cấp tài liệu giao diện tích hợp. Tổ chức đánh giá thực hiện thay thế thư viện mật mã đang dùng bằng một thư viện thay thế do tổ chức đánh giá chỉ định, trong khi hệ thống đang vận hành có tải.

Kết quả kỳ vọng: Việc thay thế hoàn tất mà không sửa đổi mã nguồn thành phần ứng dụng, không biên dịch lại thành phần ứng dụng và không dừng dịch vụ. Sau khi thay thế, bản kiểm kê mật mã sinh tự động phản ánh đúng thư viện mới.

B.5 Thử nghiệm toàn vẹn nhật ký (Điều 6.2.6.1)

Hành động: Sử dụng tài khoản có đặc quyền cao nhất, lần lượt thử: sửa nội dung một bản ghi kiểm toán; xóa một bản ghi; xóa một khoảng bản ghi; vô hiệu hóa chức năng ghi kiểm toán; thay đổi dấu thời gian hệ thống rồi ghi bản ghi mới; chặn luồng gửi giá trị neo ra ngoài.

Kết quả kỳ vọng: Tất cả các thao tác đều bị từ chối hoặc bị phát hiện bởi cơ chế neo toàn vẹn. Đối với Mức 5, việc đối chiếu với giá trị neo lưu tại hệ thống lưu giữ độc lập bên ngoài phát hiện được mọi can thiệp.

B.6 Thử nghiệm mô phỏng tấn công nội bộ - Red Teaming (Điều 6.2.3.2 và 6.2.3.3)

Điều kiện: Tổ chức đánh giá được cấp đặc quyền quản trị cao nhất mà nền tảng cho phép, kể cả quyền truy cập vật lý tới máy chủ và quyền quản trị hệ điều hành chủ. Bên sử dụng thử nghiệm đã ghi dữ liệu mẫu và đã cấu hình đầy đủ các biện pháp bảo vệ theo mức áp dụng. Danh mục kịch bản bắt buộc thực hiện: Đọc dữ liệu ổ đĩa của bên sử dụng ở dạng rõ qua mọi kênh khả dụng.

- Truy cập bảng điều khiển máy ảo của bên sử dụng không qua cơ chế chấp thuận.

- Tạo và tải về bản chụp có kèm bộ nhớ của máy ảo bên sử dụng.

- Trích xuất khóa dữ liệu của bên sử dụng ở dạng rõ khỏi phân hệ quản lý khóa.

- Xóa hoặc sửa bản ghi kiểm toán liên quan tới các hành vi trên.

- Vô hiệu hóa cơ chế thông báo tới bên sử dụng. Xóa hoặc ghi đè bản sao lưu của bên sử dụng trong chu kỳ lưu giữ.

- Di chuyển hoặc sao chép dữ liệu bên sử dụng ra ngoài phạm vi ràng buộc vị trí.

Kết quả kỳ vọng: toàn bộ kịch bản thất bại; mọi nỗ lực đều sinh bản ghi kiểm toán không tẩy xóa được và sinh cảnh báo tới bên sử dụng và bộ phận giám sát an ninh.

B.7 Thử nghiệm không cản trở mật mã do bên sử dụng áp dụng (Điều 6.2.4.1)

Điều kiện: Bên sử dụng thử nghiệm mã hóa toàn bộ ổ đĩa bên trong hệ điều hành khách bằng một sản phẩm mật mã do bên sử dụng tự lựa chọn và thiết lập một kênh mã hóa đầu cuối từ máy ảo ra bên ngoài. Khóa không được cung cấp cho tổ chức vận hành nền tảng.

Hành động: Thực hiện lần lượt các chức năng của nền tảng trên máy ảo đó, gồm sao lưu và khôi phục, tạo bản chụp, di chuyển giữa máy chủ vật lý, di chuyển giữa không gian lưu trữ, nhân bản và khởi động lại tự động khi máy chủ gặp sự cố.

Kết quả kỳ vọng: Toàn bộ chức năng hoàn tất thành công mà không yêu cầu khóa hoặc dữ liệu ở dạng rõ; sau mỗi thao tác, dữ liệu bên trong máy ảo vẫn giải mã được bằng khóa của bên sử dụng và không bị hỏng; kênh mã hóa đầu cuối không bị chấm dứt hoặc thay đổi chứng thư.

B.8 Thử nghiệm tách vai trò quản trị khóa (Điều 6.2.4.3)

Điều kiện: nền tảng đã bật chức năng mã hóa đối với ổ đĩa máy ảo và bản sao lưu của một bên sử dụng thử nghiệm.

Hành động: sử dụng tài khoản có quyền quản trị hạ tầng cao nhất, lần lượt thử: đọc nội dung ổ đĩa ở dạng rõ; trích xuất khóa khỏi phân hệ quản lý khóa; tự gán thêm quyền quản trị khóa cho chính mình; sử dụng khóa để giải mã bản sao lưu; hủy khóa. Sau đó, sử dụng tài khoản có quyền quản trị khóa, thử: truy cập bảng điều khiển máy ảo; gắn ổ đĩa sang máy ảo khác; đọc dữ liệu đối tượng.

Kết quả kỳ vọng: Toàn bộ thao tác đều bị từ chối. Mỗi nỗ lực sinh cảnh báo và bản ghi kiểm toán. Việc gán chồng hai vai trò bị hệ thống từ chối.

B.9 Thử nghiệm ký số gói cập nhật (Điều 6.2.8.2)

Hành động: Sửa một byte trong gói cập nhật hợp lệ, thực hiện cài đặt ngoại tuyến. Lặp lại với gói được ký bằng khóa không thuộc chuỗi tin cậy. Lặp lại với gói hợp lệ nhưng phiên bản thấp hơn phiên bản đang cài.

Kết quả kỳ vọng: Cả ba trường hợp bị từ chối, sinh cảnh báo, không làm thay đổi trạng thái hệ thống.

B.10 Thử nghiệm di chuyển máy ảo đang chạy (Điều 6.2.5.1)

Điều kiện: Máy ảo có tải trọng ghi bộ nhớ đang phục vụ phiên kết nối lớp giao vận hoạt động liên tục.
Hành động: Di chuyển máy ảo sang máy chủ vật lý khác và đo cửa sổ gián đoạn từ phía bên sử dụng. Lặp lại với tải trọng ghi bộ nhớ vượt quá năng lực hội tụ của băng thông mạng di chuyển.

Kết quả kỳ vọng: Ở lần thứ nhất, phiên kết nối không đứt và cửa sổ gián đoạn đo được không vượt ngưỡng quy định. Ở lần thứ hai, quá trình hoặc hội tụ bằng cơ chế bảo đảm hội tụ, hoặc bị hủy bỏ với máy ảo tiếp tục chạy trên máy chủ nguồn; không phát sinh tài nguyên vô chủ và có cảnh báo tương ứng.

B.11 Thử nghiệm năng lực sửa đổi mã nguồn lõi (Điều 6.2.8.1)

Điều kiện: Môi trường dựng không kết nối ra ngoài, do nhà cung cấp chuẩn bị trọn bộ mã nguồn, công cụ dựng và kho phụ thuộc.

Hành động: Tổ chức đánh giá giao một yêu cầu sửa đổi nhỏ bắt buộc phải chạm mã nguồn của thành phần lõi. Nhà cung cấp định vị mã nguồn, sửa đổi, dựng lại, chạy kiểm thử hồi quy, ký số gói phát hành và triển khai lên môi trường thử nghiệm.

Kết quả kỳ vọng: Gói phát hành đã ký được dựng và triển khai thành công, vượt qua phép thử tại B.9; không phát sinh liên hệ với tổ chức nước ngoài; giá trị băm của bản dựng lại từ mã nguồn gốc trùng khớp với bản đang chạy; thời gian hoàn thành không vượt quá mức cam kết.

B.12 Thử nghiệm cách ly giữa các bên sử dụng ở lớp ảo hóa (Điều 6.2.1.2)

Điều kiện: Hai máy ảo thuộc hai bên sử dụng khác nhau đang chạy trên cùng một máy chủ vật lý; tổ chức đánh giá được truy cập hệ điều hành chủ với quyền quản trị.

Hành động: Từ ngữ cảnh tiến trình của máy ảo thứ nhất tại hệ điều hành chủ, lần lượt thử mở tệp ổ đĩa ảo của máy ảo thứ hai, mở khe cắm giao tiếp quản trị của máy ảo thứ hai, và mở một tệp cấu hình của hệ điều hành chủ nằm ngoài hồ sơ chính sách. Thử gắn một thiết bị mô phỏng cũ nằm ngoài danh mục cho phép. Đo lại hiệu năng của máy ảo thứ hai khi máy ảo thứ nhất phát sinh tải tối đa.

Kết quả kỳ vọng: Cơ chế kiểm soát truy cập bắt buộc ở chế độ cưỡng chế; cả ba thao tác truy cập chéo bị từ chối và sinh bản ghi; thiết bị mô phỏng ngoài danh mục không gắn được; mức suy giảm hiệu năng không vượt ngưỡng công bố.

B.13 Thử nghiệm khôi phục phân hệ điều khiển (Điều 6.2.7.1)

Điều kiện: nền tảng đang vận hành với tập tài nguyên đã biết; bản sao lưu phân hệ điều khiển được tạo tại thời điểm T. Sau thời điểm T, thực hiện thêm các thao tác tạo mới và xóa tài nguyên.

Hành động: mô phỏng mất toàn bộ cơ sở dữ liệu trạng thái của phân hệ điều khiển, khôi phục từ bản sao lưu tại thời điểm T, sau đó đối chiếu danh mục tài nguyên mà phân hệ điều khiển nhận diện được với tài nguyên thực tế đang tồn tại.

Kết quả kỳ vọng: Máy ảo đang chạy không bị dừng trong suốt quá trình; sau khi khôi phục, mọi tài nguyên thực tế đang tồn tại đều được nhận diện; không tồn tại bản ghi trỏ tới tài nguyên đã bị xóa.

B.14 Thử nghiệm tính bất biến của bản sao lưu (Điều 6.2.7.1)

Điều kiện: Một bản sao lưu đang trong chu kỳ lưu giữ đã cấu hình; tài khoản có đặc quyền cao nhất của nền tảng.

Hành động: Lần lượt thử xóa, ghi đè và sửa đổi bản sao lưu. Thử rút ngắn chu kỳ lưu giữ và thử vô hiệu hóa chế độ bất biến. Thử đặt lại đồng hồ hệ thống về sau thời điểm hết chu kỳ lưu giữ.

Kết quả kỳ vọng: Mọi thao tác xóa, ghi đè và sửa đổi bị từ chối và sinh cảnh báo; thao tác rút ngắn chu kỳ chỉ được tiếp nhận qua cơ chế phê duyệt nhiều bên và không có hiệu lực trước 24 giờ; việc thay đổi đồng hồ hệ thống không làm chấm dứt chu kỳ lưu giữ.

B.15 Thử nghiệm cách ly dữ liệu đa tiền thuê mô hình SaaS (Điều 7.2.3)

Điều kiện: Nền tảng cung cấp dịch vụ SaaS, hai bên sử dụng A và B đang có dữ liệu nghiệp vụ trên cùng một ứng dụng.

Hành động: sử dụng tài khoản người dùng của bên sử dụng A, thử truy vấn dữ liệu của bên sử dụng B thông qua việc thay đổi Tenant ID, thao túng tham số URL hoặc tham số API.

Kết quả kỳ vọng: Ứng dụng từ chối quyền truy cập, không trả về bất kỳ dữ liệu nào của bên sử dụng B.

B.16 Thử nghiệm giải pháp EDR cấp nhân hệ điều hành (Điều 6.2.5.1)

Điều kiện: Tổ chức đánh giá được cấp quyền truy cập vào máy chủ vật lý chạy lớp ảo hóa lõi (Hypervisor).

Hành động: Kiểm tra cấu hình và trạng thái hoạt động của Agent EDR. Chạy một đoạn mã mô phỏng hành vi tải động mã lệnh trái phép vào nhân hệ điều hành hoặc mô phỏng kỹ thuật tấn công thoát lớp ảo hóa.

Kết quả kỳ vọng: Giải pháp EDR phát hiện, chặn đứng tiến trình và sinh cảnh báo thời gian thực về hệ thống SOC. Nếu giải pháp EDR chỉ hoạt động ở cấp ứng dụng và không phát hiện được mã mô phỏng cấp kernel, kết quả là Không đạt.

B.17 Thử nghiệm kiểm soát bề mặt tấn công máy chủ quản trị (Điều 6.2.1.1)

Điều kiện: Truy cập bằng quyền quản trị vào máy chủ vật lý lõi, máy chủ mặt phẳng điều khiển và máy chủ trạm nhảy (Bastion Host).

Hành động: Sử dụng lệnh hệ thống để kiểm tra danh sách phần mềm đã cài đặt (ví dụ: dpkg -l, rpm -qa, Get-Package). Thử thực hiện lệnh cài đặt mới một trình duyệt web hoặc phần mềm thư điện tử (email client).

Kết quả kỳ vọng: Tuyệt đối không phát hiện trình duyệt web hoặc email client đang tồn tại trên hệ thống. Nỗ lực cài đặt mới bị hệ thống từ chối hoặc bị công cụ quản lý cấu hình cảnh báo và chặn lại ngay lập tức.

B.18 Kiểm chứng Bản kê thành phần phần mềm (SBOM) và rà quét chuỗi cung ứng (Điều 6.2.8.2)

Hành động: Yêu cầu nền tảng xuất SBOM của phiên bản phần mềm hiện hành. Đưa tệp SBOM vào công cụ phân tích chuẩn. Đẩy một đoạn mã hoặc cấu hình IaC chứa thư viện mã nguồn mở có lỗ hổng CVE mức độ cao đã biết (mô phỏng) vào đường ống CI/CD.

Kết quả kỳ vọng: Tệp SBOM xuất ra đúng định dạng cấu trúc chuẩn quốc tế (CycloneDX JSON, SPDX), không phải định dạng PDF hay TXT. Hệ thống CI/CD tự động đối chiếu với cơ sở dữ liệu CVE, phát hiện thư viện lỗi và chặn luồng triển khai trước khi đưa vào môi trường vận hành.

B.19 Thử nghiệm xác thực liên tục Zero Trust (Điều 6.2.3.1)

Điều kiện: Một phiên quản trị đang duy trì trạng thái đăng nhập hợp lệ vào mặt phẳng điều khiển.

Hành động: Giả lập sự thay đổi đột ngột về ngữ cảnh truy cập của người quản trị (ví dụ: thay đổi địa chỉ IP/vị trí địa lý nguồn, hoặc công cụ quản lý thiết bị báo cáo thiết bị đầu cuối vừa tắt phần mềm diệt virus). Thực hiện tiếp một lệnh gọi API quản trị bất kỳ.

Kết quả kỳ vọng: Nền tảng ngay lập tức đánh giá lại ngữ cảnh, từ chối lệnh gọi API, ngắt phiên làm việc và yêu cầu xác thực lại (hoặc chặn hoàn toàn truy cập).

B.20 Thử nghiệm chặn trích xuất dữ liệu xuyên biên giới (Geo-IP) (Điều 6.2.6.2)

Điều kiện: Thiết lập một kết nối từ dải địa chỉ IP được xác định là nằm ngoài lãnh thổ Việt Nam.

Hành động: Sử dụng tài khoản hợp lệ, gọi API hoặc dùng công cụ thực hiện tải xuống hàng loạt dữ liệu, ảnh máy ảo hoặc bản chụp từ vùng lưu trữ.

Kết quả kỳ vọng: Tường lửa ứng dụng web (WAF) hoặc API Gateway tự động nhận diện IP ngoại biên, từ chối tác vụ tải xuống hàng loạt và ghi nhận sự kiện vào nhật ký kiểm toán bất biến.

B.21 Kiểm chứng các chỉ tiêu thời gian (SLAs) và quy trình ứng phó (Điều 6.2.5 và 6.2.4)

Điều kiện: Rà soát hồ sơ vận hành, hệ thống giám sát và nhật ký kiểm toán trong 12 tháng gần nhất (hoặc thực hiện qua kịch bản giả lập nếu hệ thống mới).

Hành động: Đối chiếu dấu thời giangiữa thời điểm phát hiện lỗ hổng/sự cố và thời điểm đưa ra biện pháp giảm thiểu, phát thông báo; đối chiếu thời điểm xóa tài nguyên với thời điểm hoàn tất ghi đè/xóa khóa mã hóa.

Kết quả kỳ vọng: Có bằng chứng kỹ thuật xác nhận biện pháp giảm thiểu tạm thời đối với lỗ hổng nghiêm trọng được triển khai không quá 72 giờ. Thời gian phát thông báo sự cố cho chủ thuê qua 02 kênh độc lập tuân thủ đúng khung thời gian cấu hình. Việc xóa an toàn dữ liệu tồn dư hoàn tất không quá 24 giờ (Mức 5) và không quá 07 ngày (Mức 3, 4) kể từ khi giải phóng tài nguyên..

Phụ lục C
(tham khảo)
Hướng dẫn xây dựng lộ trình chuyển đổi mật mã kháng lượng tử

C.1 Nguyên tắc.

Việc chuyển đổi sang mật mã kháng lượng tử là quá trình nhiều năm, không phải một lần thay thế. Yếu tố quyết định thành công không phải là lựa chọn thuật toán mà là khả năng thay đổi lựa chọn đó về sau.

C.2 Thứ tự ưu tiên chuyển đổi.

Giai đoạn	Nội dung	Lý do ưu tiên
Giai đoạn 1	Xây dựng và duy trì bản kiểm kê mật mã đầy đủ theo 10.2.6	Không thể lập kế hoạch chuyển đổi khi chưa biết mật mã đang được dùng ở đâu, bằng thuật toán nào và bảo vệ dữ liệu nào.
Giai đoạn 2	Tách lời gọi mật mã khỏi cài đặt thuật toán theo 10.2	Đây là công việc tốn kém nhất và phải hoàn thành trước mọi bước sau. Nếu bỏ qua, mỗi lần đổi thuật toán sẽ là một lần sửa toàn bộ mã nguồn.
Giai đoạn 3	Áp dụng trao đổi khóa lai cho các kênh truyền tải	Bảo vệ trước nguy cơ thu thập dữ liệu hôm nay để giải mã về sau, đồng thời giữ được tương thích với hệ thống chưa chuyển đổi.
Giai đoạn 4	Chuyển đổi chữ ký số, gồm chữ ký gói cập nhật và chữ ký khởi động tin cậy	Chữ ký số có vòng đời dài và gắn với chuỗi tin cậy của nền tảng, cần thời gian dài để thay thế toàn bộ.
Giai đoạn 5	Mã hóa lại kho dữ liệu có thời hạn bảo mật dài	Khối lượng lớn, thực hiện dần theo mức độ nhạy cảm của dữ liệu.

C.3 Về lựa chọn thuật toán.

Việc lựa chọn thuật toán cụ thể thuộc thẩm quyền của cơ quan quản lý nhà nước về mật mã. Tiêu chuẩn này khuyến nghị nền tảng hỗ trợ đồng thời nhiều họ thuật toán để tránh phụ thuộc vào một giả thiết toán học duy nhất, và hỗ trợ tích hợp thư viện mật mã trong nước ngay từ Giai đoạn 2.

C.4 Về dữ liệu đã lưu trữ.

Dữ liệu đã được mã hóa và lưu trữ bằng thuật toán cổ điển trước thời điểm chuyển đổi vẫn chịu nguy cơ nếu bản mã đã bị sao chép ra ngoài. Đối với dữ liệu có thời hạn bảo mật vượt quá thời điểm dự kiến máy tính lượng tử đủ năng lực, việc mã hóa lại là bắt buộc theo 10.2.5 chứ không phải tùy chọn.

Thư mục tài liệu tham khảo

[1] TCVN 13810:2023 (ISO/IEC TR 22678:2019), Công nghệ thông tin - Tính toán mây - Hướng dẫn xây dựng chính sách.

[2] TCVN 14481-1:2025 (ISO/IEC 19944-1), Tính toán đám mây và các nền tảng phân tán - Luồng dữ liệu, loại dữ liệu và sử dụng dữ liệu.

[3] ISO/IEC 27017, Code of practice for information security controls for cloud services.

[4] ISO/IEC 27018, Code of practice for protection of PII in public clouds acting as PII processors.

[5] Bộ ISO/IEC 19086, Cloud computing - Service level agreement (SLA) framework.

[6] Các tiêu chuẩn về mật mã kháng lượng tử do các tổ chức tiêu chuẩn hóa quốc tế công bố, sử dụng làm tài liệu tham khảo khi xây dựng chính sách thuật toán.