BỘ TÀI CHÍNH
TỔNG CỤC HẢI QUAN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do – Hạnh phúc

Số: 1806 /TCHQ-TXNK
V/v hoàn thuế GTGT cho người nước ngoài

Hà Nội, ngày 20 tháng 5 năm 2022

Kính gửi: Công ty Bellazio.
(Tầng 3 Tòa nhà Opera View, 161 Đồng Khởi, P. Bến Nghé, Q.1, TP.Hồ Chí Minh)

Trả lời công văn số 04-22/CV-Bellazio ngày 24/3/2022 của Công ty Bellazio đề nghị triển khai hệ thống hoàn thuế GTGT chuyên nghiệp tại Việt Nam, Tổng cục Hải quan có ý kiến như sau :

Tổng cục Hải quan trân trọng cảm ơn đề nghị của Quý Công ty về việc hỗ trợ đưa hệ thống công nghệ áp dụng vào việc hoàn thuế GTGT cho người nước ngoài tại Việt Nam.

Trong thời gian tới, đề nghị Công ty cung cấp phần mềm chạy thử mô phỏng việc hoàn thuế GTGT cho người nước ngoài có sự kết nối giữa các bên có liên quan như: cơ quan hải quan, doanh nghiệp bán hàng hoàn thuế, ngân hàng thương mại, cơ quan thuế, đơn vị cung cấp dịch vụ hoàn thuế....

Về yêu cầu kỹ thuật hệ thống hoàn thuế giá trị gia tăng cho người nước ngoài triển khai cho Tổng cục Hải quan, đề nghị Công ty nghiên cứu các phụ lục đính kèm công văn này. Cụ thể:

- Phụ lục 1: Yêu cầu kỹ thuật về phần mềm;
- Phụ lục 2: Yêu cầu về phần cứng đáp ứng Hải quan số;
- Phụ lục 3: Yêu cầu về an ninh an toàn đối với hệ thống.

Tổng cục Hải quan thông báo để Công ty Bellazio biết./.

Nơi nhận:
- Như trên;
- Tổng cục trưởng (để b/c);
- Lưu: VT, TXNK (3b).

KT. TỔNG CỤC TRƯỞNG
PHÓ TỔNG CỤC TRƯỞNG

BỘ TÀI CHÍNH
TỔNG CỤC HẢI QUAN

Lưu Mạnh Tưởng

Phụ lục I

YÊU CẦU KỸ THUẬT VỀ PHẦN MỀM

(ban hành kèm theo công văn số 1806/TCHQ-TXNK ngày 20/5/2022 của Tổng cục Hải quan)

1. Yêu cầu về phần mềm nội bộ

1.1. Yêu cầu chung:

Các ứng dụng, dịch vụ khi được xây dựng phải đáp ứng các yêu cầu sau:

- Thủ tục Hải quan với hoàn thuế GTGT cho người nước ngoài có thể thực hiện 24/7;

- Thủ tục hải quan với hoàn thuế GTGT cho người nước ngoài có thể thực hiện bằng nhiều thiết bị, hướng tới các thiết bị di động;

- Toàn bộ hồ sơ được số hóa 100%, trong trường hợp chứng từ gốc là chứng từ giấy phải thực hiện chuyển đổi sang chứng từ số;

- Việc thực hiện thủ tục hải quan với với hoàn thuế GTGT cho người nước ngoài thông qua một cổng dịch vụ duy nhất. Cổng dịch vụ này có thể tích hợp cùng cổng dịch vụ của hệ thống hải quan số;

- Dữ liệu được tích hợp và chia sẻ trong toàn bộ cơ quan hải quan và các bộ ngành liên quan.

1.2. Yêu cầu về quản lý người sử dụng và phân quyền

Nhóm 1: Người sử dụng bên ngoài

- Nhóm 1: Người sử dụng bên ngoài (người khai hải quan, doanh nghiệp, người dân, cơ quan, tổ chức...) có nhu cầu sử dụng, khai thác trên ứng dụng, dịch vụ của hệ thống hoàn thuế GTGT cho người nước ngoài;

Nhóm 2: Người sử dụng nội bộ

- Nhóm 2: Người sử dụng nội bộ (cán bộ, công chức, viên chức, người lao động của cơ quan hải quan).

Nhóm 3: Người sử dụng là hệ thống

- Nhóm 3: Người sử dụng là hệ thống (gồm các kết nối từ các hệ thống bên ngoài vào các dịch vụ/hệ thống hoàn thuế GTGT cho người nước ngoài).

- Với mỗi hệ thống khi kết nối đến hệ thống hoàn thuế GTGT cho người nước ngoài cũng cần phải được định danh và xác thực nhằm đảm bảo kết nối, trao đổi thông tin đúng đối tượng.

Mỗi người sử dụng, nhóm người sử dụng được phân quyền phù hợp với chức năng nhiệm vụ của người sử dụng trên hệ thống.

1.3. Yêu cầu về theo dõi nhật ký hệ thống

Ghi và lưu trữ nhật ký về hoạt động của hệ thống thông tin và thao tác của người sử dụng, các lỗi phát sinh và các sự cố an toàn thông tin.

Dữ liệu nhật ký của hệ thống thông tin phải được lưu trữ trực tuyến tối thiểu 3 tháng theo hình thức tập trung và sao lưu tối thiểu một năm.

Các chức năng ghi nhật ký và thông tin nhật ký được bảo đảm, chống giả mạo và truy cập trái phép;

Người quản trị hệ thống và người sử dụng không thể xóa hay sửa đổi nhật ký hệ thống

1.4. Yêu cầu về đo thời gian xử lý

Cho phép thiết lập đo thời gian phục vụ:

- Giám sát và tối ưu hệ thống

- Đánh giá hiệu quả công việc của cán bộ Hải quan

Thông tin đo thời gian xử lý được lưu trữ có cấu trúc để thuận tiện cho việc phân tích.

Việc thiết lập bật/tắt đo thời gian xử lý không được làm gián đoạn hoạt động của hệ thống.

1.5. Yêu cầu cần đáp ứng về thời gian xử lý, độ phức tạp xử lý

Hiệu năng của hệ thống được xác định dựa trên các thông số được ước tính như sau:

- Thời gian hệ thống phản hồi yêu cầu của người dùng.

+ Đối với người dùng nội bộ: thời gian phản hồi người dùng không quá 5 giây với số lượng dữ liệu nghiệp vụ lưu trữ trong 1 tháng

+ Đối với người dùng bên ngoài: thời gian phản hồi người dùng không quá 10 giây với số lượng dữ liệu nghiệp vụ lưu trữ trong 1 tháng

- Thời gian hệ thống tải giao diện của nó.

+ Đối với người dùng nội bộ: thời gian phản hồi người dùng không quá 3 giây với số lượng dữ liệu nghiệp vụ lưu trữ trong 1 tháng

+ Đối với người dùng bên ngoài: thời gian phản hồi người dùng không quá 5 giây với số lượng dữ liệu nghiệp vụ lưu trữ trong 1 tháng

- Thời gian hệ thống tra cứu thông tin.

+ Đối với người dùng nội bộ:

++ Đối với tra cứu chính xác theo mã hoặc khóa chính của ứng dụng thì thời gian phản hồi người dùng không quá 3 giây với số lượng dữ liệu nghiệp vụ lưu trữ trong 1 tháng

++ Đối với tra cứu gần đúng thì thời gian phản hồi không quá 10 giây với số lượng dữ liệu nghiệp vụ lưu trữ trong 1 tháng

++ Đối với tra cứu, báo cáo, tổng hợp dữ liệu phức tạp với số lượng dữ liệu báo cáo lưu trữ trong 1 năm thì thời gian phản hồi người dùng không quá 3 phút

+ Đối với người dùng bên ngoài:

++ Đối với tra cứu chính xác theo mã hoặc khóa chính của ứng dụng thì thời gian phản hồi người dùng không quá 5 giây với số lượng dữ liệu nghiệp vụ lưu trữ trong 1 tháng

++ Đối với tra cứu gần đúng thì thời gian phản hồi không quá 15 giây với số lượng dữ liệu nghiệp vụ lưu trữ trong 1 tháng

++ Đối với tra cứu, báo cáo, tổng hợp dữ liệu phức tạp với số lượng dữ liệu báo cáo lưu trữ trong 1 năm thì thời gian phản hồi người dùng không quá 5 phút.

1.6. Yêu cầu về bảo trì

Hệ thống hoặc thành phần của hệ thống có thể được sửa đổi để sửa lỗi, cải thiện hiệu năng hoặc các thuộc tính khác, hoặc thích ứng với một môi trường đã thay đổi. Các yêu cầu về bảo trì gồm:

- Hệ thống phải có khả năng bảo trì cao (dễ dàng điều chỉnh các lỗi mà

chưa được phát hiện trong giai đoạn xây dựng hoặc trong quá trình sử dụng phần mềm);

- Hệ thống phải được thiết kế để có thể bảo trì ngay từ đầu (là việc có khả năng điều chỉnh ngay từ giai đoan đầu triển khai các lỗi mà chưa được phát hiện trong giai đoạn xây dựng hoặc trong quá trình sử dụng phần mềm có nhiều thay đổi, nâng cấp tính năng sử dụng và an toàn vận hành của phần mềm);

- Vòng đời phát triển phần mềm hệ thống sẽ tuân theo một phương pháp luận tiêu chuẩn được xác định rõ bằng cách sử dụng các kinh nghiệm tốt nhất và kết hợp với quá trình lặp đi lặp lại phát triển và rà soát, hiệu chỉnh phần mềm

- Mã nguồn của phần mềm hệ thống phải được hệ thống hóa thành tài liệu và tài liệu sẽ được kết hợp trong quá trình quản lý thay đổi và quá trình quản lý phiên bản phần mềm

- Kiểm thử tự động sẽ được sử dụng để kiểm tra phần mềm hệ thống trong suốt vòng đời phát triển và bảo trì. Các cơ chế tích hợp liên tục sẽ được đồng thời áp dụng.

1.7. Yêu cầu về giao diện

Các yêu cầu chi tiết về giao diện được thể hiện trong tài liệu thiết kế chi tiết của hệ thống. Ngoài các yêu cầu này, giao diện của hệ thống cần đáp ứng các yêu cầu chung bao gồm:

- Hệ thống phải có giao diện thân thiện với người sử dụng.

- Hệ thống phải có các giao diện tiêu chuẩn được xác định rõ ràng giữa các thành phần bên trong hệ thống.

- Hệ thống phải có các giao diện tiêu chuẩn được xác định rõ ràng để giao tiếp giữa các tầng khác nhau của hệ thống

- Hệ thống phải có các giao diện tiêu chuẩn được xác định rõ ràng cho tất cả các giao tiếp với các hệ thống bên ngoài

- Hệ thống không cho phép các thành phần / ứng dụng, người sử dụng hệ thống cả bên trong và bên ngoài truy cập trực tiếp vào cơ sở dữ liệu. Tất cả các tương tác sẽ được thực hiện thông qua các giao diện tiêu chuẩn được xác định rõ ràng

- Hệ thống không cho phép các thành phần / ứng dụng, người dùng của hệ thống cả bên trong và bên ngoài truy cập trực tiếp vào bất kỳ tệp hoặc tài nguyên nào của hệ thống một cách trực tiếp trừ khi thông qua chức năng được phép, thông qua các giao diện tiêu chuẩn và được xác định rõ.

- Đối với các nghiệp vụ được quy định là thủ tục hành chính, cho phép người sử dụng truy cập để sử dụng sau khi đã xác thực điện tử thông qua Cổng dịch vụ công quốc gia.

1.8. Yêu cầu về tính toàn vẹn dữ liệu

Các yêu cầu về tính toàn vẹn dữ liệu của hệ thống bao gồm:

- Hệ thống chỉ cho phép nhập dữ liệu qua các kênh giao tiếp của nó (bao gồm dữ liệu do người dùng nhập vào và các dữ liệu nhận được từ các hệ thống khác)

- Hệ thống sẽ xác nhận rằng dữ liệu được nhập ở định dạng được chỉ định và tự động phát hiện bất kỳ định dạng dữ liệu không hợp lệ nào

- Hệ thống phải đảm bảo rằng tất cả dữ liệu nhận được là hoàn chỉnh theo các đặc tả của bản ghi dữ liệu

- Hệ thống sẽ ngăn chặn việc cập nhật, thay thế, xóa trái phép bất kỳ dữ liệu nào

- Hệ thống sẽ lưu trữ tiến trình lịch sử của tất cả các hoạt động cập nhật, sửa đổi và xóa bất kỳ dữ liệu nào

- Hệ thống sẽ lưu trữ ở mức tối thiểu các lịch sử của việc cập nhật dữ liệu: Ai đã thực hiện thay đổi, những gì đã được thay đổi (bao gồm cả giá trị ban đầu và giá trị mới), lý do thực hiện thay đổi và nếu có thể thì ai đã ủy quyền thay đổi

- Hệ thống sẽ lưu trữ ở mức tối thiểu lịch sử xóa dữ liệu: Ai đã thực hiện xóa, những gì đã bị xóa (bao gồm cả giá trị), lý do xóa được thực hiện và nếu có thể thì ai cho phép xóa

- Hệ thống sẽ ngăn chặn việc xóa bất kỳ dữ liệu quan trọng nào

- Hệ thống sẽ yêu cầu việc kiểm tra và phê duyệt của người thứ hai đối với các hành động quan trọng và cập nhật dữ liệu quan trọng

- Hệ thống sẽ cho phép tạo ra các báo cáo theo dõi các cập nhật dữ liệu quan trọng

- Hệ thống phải đảm bảo rằng các thay đổi đối với dữ liệu chỉ được thực hiện khi cần thiết và bởi người dùng được cấp/giao quyền. Dữ liệu gốc (không thay đổi) phải được giữ lại ở dạng gốc.

- Hệ thống sẽ cung cấp một cơ chế lưu trữ dữ liệu. Tất cả dữ liệu được lưu trữ sẽ được kiểm tra lịch sử lưu trữ và các tham chiếu. Việc lưu trữ sẽ được thực hiện định kỳ theo chính sách đã được xây dựng.

- Hệ thống sẽ chỉ lưu trữ dữ liệu theo "Chính sách lưu trữ" của Tổng cục Hải quan

- Hệ thống cho phép cấu hình để lưu trữ dữ liệu trong một khoảng thời gian

- Hệ thống sẽ cho phép người dùng được cấp/giao quyền truy cập dữ liệu đã lưu trữ trước đó.

1.9. Yêu cầu về quy trình phát triển phần mềm

Quy trình phát triển phần mềm bao gồm:

- Quản lý tạo lập mô tả dịch vụ;

- Quản lý phát triển ứng dụng và thực thi dịch vụ;

- Quản lý công bố dịch vụ đã phát triển;

- Quản lý kiểm thử dịch vụ;

- Quản lý đóng gói và triển khai dịch vụ.

1.10. Yêu cầu về kiến trúc

- Phù hợp với kiến trúc chính phủ điện tử 2.0

- Phù hợp với kiến trúc tổng thể hệ thống CNTT ngành Tài chính hướng tới tài chính số.

- Phù hợp với kiến trúc tổng thể hệ thống CNTT cơ quan Hải quan hướng tới Hải quan số

Cụ thể:

- Kiến trúc ứng dụng được thiết kế cho phép tích hợp, chia sẻ dữ liệu và

xây dựng ứng dụng một cách linh hoạt thông qua cơ chế tích hợp có tính đến các giải pháp tích hợp, chia sẻ dữ liệu qua trục tích hợp (ESB) và các công nghệ tích hợp phân tán.

- Hệ thống thông tin xây dựng theo hướng tiếp cận kiến trúc hướng dịch vụ

- Hệ thống xây dựng theo mô hình đa lớp (lớp giao diện, lớp nghiệp vụ, lớp cơ sở dữ liệu…)

- Kiến trúc dữ liệu: Tuân thủ kiến trúc dữ liệu trong kiến trúc tổng thể hệ thống CNTT cơ quan Hải quan hướng tới Hải quan số.

- Việc tích hợp, chia sẻ dữ liệu với Bộ Tài chính và các đơn vị trực thuộc Bộ Tài chính thông qua nền tảng tích hợp, chia sẻ dữ liệu của Bộ tài chính. Việc tích hợp, chia sẻ dữ liệu với các đơn vị ngoài Bộ Tài chính sẽ thực hiên theo phương thức tích hợp, chia sẻ dữ liệu được quy định trong kiến trúc tổng thể hệ thống CNTT cơ quan Hải quan hướng tới Hải quan số.

1.11. Yêu cầu về kênh giao tiếp

Kênh giao tiếp là các phương thức mà hệ thống trao đổi thông tin với người sử dụng. Người dùng giao tiếp với hệ thống thông qua các kênh: Giao tiếp số (Mobile, Tablet, PC) và giao tiếp qua cổng/trang thông tin của Tổng cục Hải quan, giao tiếp qua dịch vụ công trực tuyến hoặc trao đổi trực tiếp giữa hệ thống của người sử dụng với hệ thống của cơ quan hải quan. Dữ liệu trao đổi qua kênh giao tiếp cần được mã hóa.

Trường hợp người sử dụng giao tiếp qua kênh giao tiếp số hoặc qua cổng/trang thông tin của Tổng cục Hải quan, giao tiếp qua dịch vụ công trực tuyến: Lớp này sẽ giao tiếp với xử lý liền kề thông qua kiểu dữ liệu có cấu trúc (JSON...)

Giao tiếp giữa hệ thống của người sử dụng và hệ thống của cơ quan hải quan được thực hiện thông qua các thông điệp dữ liệu xml hoặc json tủy thuộc quy định về chuẩn dữ liệu.

Đối với kênh trao đổi thông tin dành cho người sử dụng thiết bị di động thông minh (smartphone, Tablet): Hệ thống cần được thiết kế phù hợp với các đặc thù của thiết bị di động: kích thước màn hình của các thiết bị di động tối thiểu 6 inch, các phương thức nhập liệu, tốc độ và tính không ổn định của kết

nối Internet di động, đặc điểm sử dụng của người dùng thiết bị di động.

1.12. Yêu cầu danh mục điện tử dùng chung

Sử dụng danh mục điện tử dùng chung với hệ thống công nghệ thông tin hướng tới hải quan số của Tổng cục Hải quan.

2. Yêu cầu về phần mềm nền tảng

2.1. Yêu cầu lớp ứng dụng

- Sử dụng và triển khai trên nền tảng công nghệ web-based.

- Áp dụng công nghệ phát triển ứng dụng, dịch vụ hướng đối tượng, nên áp dụng kiến trúc dịch vụ nhỏ (microservice architecture) để tạo tập các dịch vụ nhỏ, độc lập, kết nối với nhau qua giao thức RESTful, gRPC...

- Ưu tiên áp dụng các công nghệ dựa trên các nền tảng mã nguồn mở để tận dụng ưu thế cho phép mở rộng và phát triển thêm khi có thay đổi về nghiệp vụ. Các phần mềm nguồn mở cũng cho phép đảm bảo an ninh thông tin hơn với lợi thế nắm được mã nguồn cũng như sự đóng góp, cập nhật liên tục của các cộng đồng mở.

- Ưu tiên áp dụng các công nghệ di động đa nền tảng để có thể triển khai được trên nhiều nền tảng di động mà không cần phải phát triển ứng dụng cho từng nền tảng di động.

- Ngôn ngữ và phương pháp phát triển ứng dụng nên được thống nhất về mặt công nghệ nhằm đảm bảo tính tối ưu cho công tác vận hành, duy trì, mở rộng hệ thống và đào tạo nguồn nhân lực. Đề xuất sử dụng các ngôn ngữ hướng đối tượng như .NET, java, Python... Phương pháp phát triển ứng dụng (như Agile Scrum, RUP,...) nên được áp dụng trong tất cả các bước của quy trình phát triển ứng dụng để đảm bảo chất lượng phần mềm đáp ứng nhu cầu nghiệp vụ.

2.2. Yêu cầu lớp dịch vụ

- Công nghệ tuân theo mô hình kiến trúc ứng dụng hướng dịch vụ và đa tầng.

- Các công nghệ theo kiến trúc này giúp cho việc tạo hệ thống linh hoạt bằng một tập các dịch vụ, trong đó các dịch vụ này có thể thêm mới, thay thế, xóa bỏ... mà không ảnh hưởng đến vận hành chung của hệ thống.

- Các dữ liệu trao đổi tuân thủ các chuẩn mở, ví dụ như XML, ebXML...

- Công nghệ tích hợp và chia sẻ dữ liệu qua trục tích hợp (ESB)...

- Công nghệ ETL (Extracts, Transforms and Load) để chuyển đổi mục đích, tối ưu hóa mục đích sử dụng dữ liệu nghiệp vụ, từ đó xây dựng được các thông tin hữu ích cho việc hoạch định chiến lược, kế hoạch,... của tổ chức.

2.3. Yêu cầu lớp giao diện

- Sử dụng nền tảng Client-side Rendering để xây dựng lớp giao diện nhằm chuyển gánh nặng biên dịch, sinh mã html về phía trình duyệt

- Sử dụng các framework phổ biến như VueJS, Angular, ReactJS… để xây dựng giao diện người sử dụng

2.4. Yêu cầu với ứng dụng di động

- Với những ứng dụng đi động bình thường, ưu tiên xây dựng ứng dụng hybrid (sử dụng chung một bộ mã nguồn sản phẩm và biên dịch ra các ứng dụng cho từng hệ điều hành)

- Với những ứng dụng yêu cầu hiệu năng cao hoặc cần những truy cập sâu vào thiết bị thì xây dựng các native app (mỗi hệ điều hành dùng một bộ mã nguồn riêng)

- Các ứng dụng hybrid được xây dựng bằng các công nghệ Flutter hoặc React-Native

2.5. Yêu cầu lớp xử lý nghiệp vụ

- Khuyến nghị sử dụng ngôn ngữ lập trình Java để hỗ trợ đa nền tảng

2.6. Yêu cầu xử lý thông điệp

Các yêu cầu về xử lý thông điệp của hệ thống bao gồm:

- Đảm bảo xử lý thông điệp theo nhiều định dạng khác nhau như JSON, XML, AVRO …

- Tốc độ xử lý thông điệp nhanh chóng, xử lý tốt với số lượng thông điệp lớn trong một khoảng thời gian ngắn

- Thông điệp được lưu giữ bền vững, an toàn, và có thể xử lý lại các thông điệp khi cần thiết

- Thông điệp được định tuyến dễ dàng phục vụ những mục đích nghiệp vụ khác nhau

- Một thông điệp phải đảm bảo được sử dụng cho nhiều dịch vụ khác nhau

- Dịch vụ xử lý thông điệp phải cung cấp tính năng tính toán song song trên nhiều node của hạ tầng máy chủ, dễ dàng mở rộng để tăng hiệu năng xử lý khi cần thiết

- Dịch vụ xử lý thông điệp phải được đảm bảo tính sẵn sàng cao, thời gian hoạt động 24/7.

- Các thông điệp trao đổi cần được ký số. Chứng thư số sử dụng để ký số được cung cấp bởi cơ quan có thẩm quyền hoặc đơn vị cung cấp dịch vụ chữ ký số được cấp phép. Phải có phương án đảm bảo an toàn trong việc sử dụng chữ ký số.

2.7. Yêu cầu giao tiếp giữa các dịch vụ

Các yêu cầu về giao tiếp giữa các dịch vụ bao gồm:

- Việc giao tiếp, phân phối thông tin giữa các dịch vụ phải nhanh chóng, dễ dàng và giảm thiểu sự phụ thuộc lẫn nhau giữa các dịch vụ riêng lẻ.

- Có khả năng tích hợp, liên thông nhiều loại ứng dụng khác nhau

- Các dịch vụ có thể giao tiếp với nhau không phụ thuộc vào nền tảng phát triển, định dạng thông điệp và giao thức.

- Có khả năng định tuyến, lưu nhật ký, lưu trữ thông tin mà không cần chỉnh sửa dịch vụ

- Có khả năng kiểm tra, xác thực thông điệp là hợp lệ, ngăn chặn các thông điệp bất thường. Có chức năng kiểm soát lỗi, thông báo lỗi từ ứng dụng, dịch vụ.

- Có khả năng thiết lập các luồng thông điệp hoặc sự kiện mới, từ các thông điệp, sự kiện, có thể thiết lập các sự kiện khác phức tạp hơn.

- Việc giao tiếp giữa các dịch vụ phải đảm bảo tính toàn vẹn trong việc xử lý thông điệp. Nếu như trong luồng xử lý thông điệp, một tiến trình xử lý bị lỗi thì toàn bộ quá trình sẽ được huỷ bỏ và khôi phục về như ban đầu

- Khi giao tiếp giữa các dịch vụ phải xây dựng một cơ chế xác thực truy cập, ủy nhiệm truy cập, và cung cấp tính năng mã hóa và giải mã thông điệp.

- Đáp ứng việc triển khai từng phần; không nhất thiết phải chuyển toàn bộ dịch vụ, ứng dụng trong một lần triển khai…

2.8. Yêu cầu về cơ sở dữ liệu (có cấu trúc, phi cấu trúc, bigdata)

2.8.1. Yêu cầu chung

- Hệ quản trị cơ sở dữ liệu được lựa chọn cần đảm bảo khả năng xử lý dữ liệu lớn, đảm bảo các quy định về an ninh, an toàn đồng thời phù hợp với công nghệ phát triển ứng dụng đã lựa chọn.

- Hệ quản trị cơ sở dữ liệu cho phép dễ dàng mở rộng quy mô lưu trữ, thay đổi (tăng/giảm) tài nguyên xử lý (RAM, CPU), hỗ trợ lưu trữ trên ổ SSD hoặc các loại ổ cứng tốc độ cao khác; hỗ trợ các tính năng truy xuất dữ liệu nhanh; hỗ trợ các giải pháp đồng bộ dữ liệu tức thời giữa DC và DR;

2.8.2. Yêu cầu về khả năng mở rộng

Khả năng mở rộng là khả năng của cơ sở dữ liệu hoặc hệ quản trị cơ sở dữ liệu để xử lý việc tăng hoặc giảm khối lượng công việc mà không ảnh hưởng đến năng suất, hiệu quả xử lý công việc của nó. Các yêu cầu về khả năng mở rộng đối với cơ sở dữ liệu gồm:

- Cơ sở dữ liệu và hệ quản trị cơ sở dữ liệu của hệ thống cần có khả năng mở rộng và xử lý các khối lượng công việc khác nhau.

- Khi các thành phần phần cứng hoặc phần mềm mới được thêm vào để mở rộng hệ thống nhằm xử lý tốt hơn khối lượng công việc lớn hơn, sẽ có ít nhất hoặc không có thời gian chết.

2.8.3. Yêu cầu về tính linh hoạt

Tính linh hoạt là khả năng của cơ sở dữ liệu hoặc hệ quản trị cơ sở dữ liệu để phân bổ tài nguyên có sẵn với số lượng cần thiết cho mỗi dịch vụ. Khả năng mở rộng liên quan đến cơ sở dữ liệu hoặc khả năng của hệ quản trị cơ sở dữ liệu để xử lý khối lượng công việc, trong khi khả năng linh hoạt liên quan đến mức độ linh hoạt khi hoàn thành nhiệm vụ đó. Để xử lý dữ liệu nhanh nhất có thể, hệ thống cấp phát và thu hồi tài nguyên dựa trên nhu cầu hiện tại, đó là khả năng

linh hoạt. Các tài nguyên được cung cấp và bị thu hồi nhằm cung cấp vừa đủ năng lực xử lý để thực thi các dịch vụ. Yêu cầu về tính linh hoạt như sau:

- Cơ sở dữ liệu và hệ quản trị cơ sở dữ liệu của hệ thống cần có khả năng phân bổ tài nguyên hệ thống phù hợp với nhu cầu cần thiết của mỗi dịch vụ, không hơn không kém.

- Cơ sở dữ liệu và hệ quản trị cơ sở dữ liệu của hệ thống cần có khả năng quản lý theo nhóm/cụm.

2.8.4. Yêu cầu về tính sẵn sàng

+ Tính sẵn sàng của cơ sở dữ liệu và hệ quản trị cơ sở dữ liệu là khả năng cho phép người dùng/phần mềm/phần cứng/ truy cập nếu có quyền.

+ Tính sẵn sàng của cơ sở dữ liệu và hệ quản trị cơ sở dữ liệu phải đảm báo 4 yếu tố sau:

++ Có khả năng cung cấp các dịch vụ đáng tin cậy (Reliability) trong một khoảng thời gian cụ thể.

++ Có khả năng phục hồi (Recoverability) nhanh chóng khi một thành phần bị lỗi hoặc ngắt kết nối khỏi máy chủ.

++ Có khả năng tạo và duy trì một môi trường (Manageability) hiệu quả để cung cấp dịch vụ cho người dùng.

++ Có khả năng phát hiện lỗi, xác định nguyên nhân và sửa chữa lỗi (Serviceability) để dịch vụ chỉ bị gián đoạn ở mức tối thiểu.

2.8.5. Yêu cầu về giám sát, vận hành cơ sở dữ liệu

- Dữ liệu phải được giám sát 24/7, có khả năng hỗ trợ phát hiện sớm các sự cố, tự động thông báo cho cán bộ giám sát;

- Có khả năng giám sát được các truy cập bất hợp pháp vào hệ quản trị cơ sở dữ liệu;

- Cảnh báo các hoạt động bất thường của cơ sở dữ liệu có thể ảnh hưởng tới hoạt động chung của hệ thống:

+ Cảnh báo về tài nguyên của máy chủ (RAM, CPU, HDD, I/O..);

+ Cảnh báo các thông tin cấu hình của cơ sở dữ liệu: Thời gian hiệu lực của

mật khẩu; dung lượng data file trên cơ sở dữ liệu; tài nguyên sử dụng của các tài khoản...

- Cảnh báo sự cố, rủi ro trong quá trình vận hành của hệ thống cơ sở dữ liệu.

- Có kế hoạch chuyển đổi hoạt động của dữ liệu của DC – DR;

- Có kế hoạch backup dữ liệu và khôi phục thử các dữ liệu đã backup;

- Hệ quản trị CSDL có cung cấp tính năng kiểm tra dữ liệu thay đổi. Hệ thống phải đảm bảo lưu vết các hoạt động trong hệ thống.

- Hệ quản trị CSDL có cung cấp các tính năng để hạn chế các cán bộ quản trị cơ sở dữ liệu hoặc những người sử dụng có đặc quyền khác truy cập vào dữ liệu ứng dụng nghiệp vụ hoặc thực hiện những thay đổi không được phép

Phụ lục II

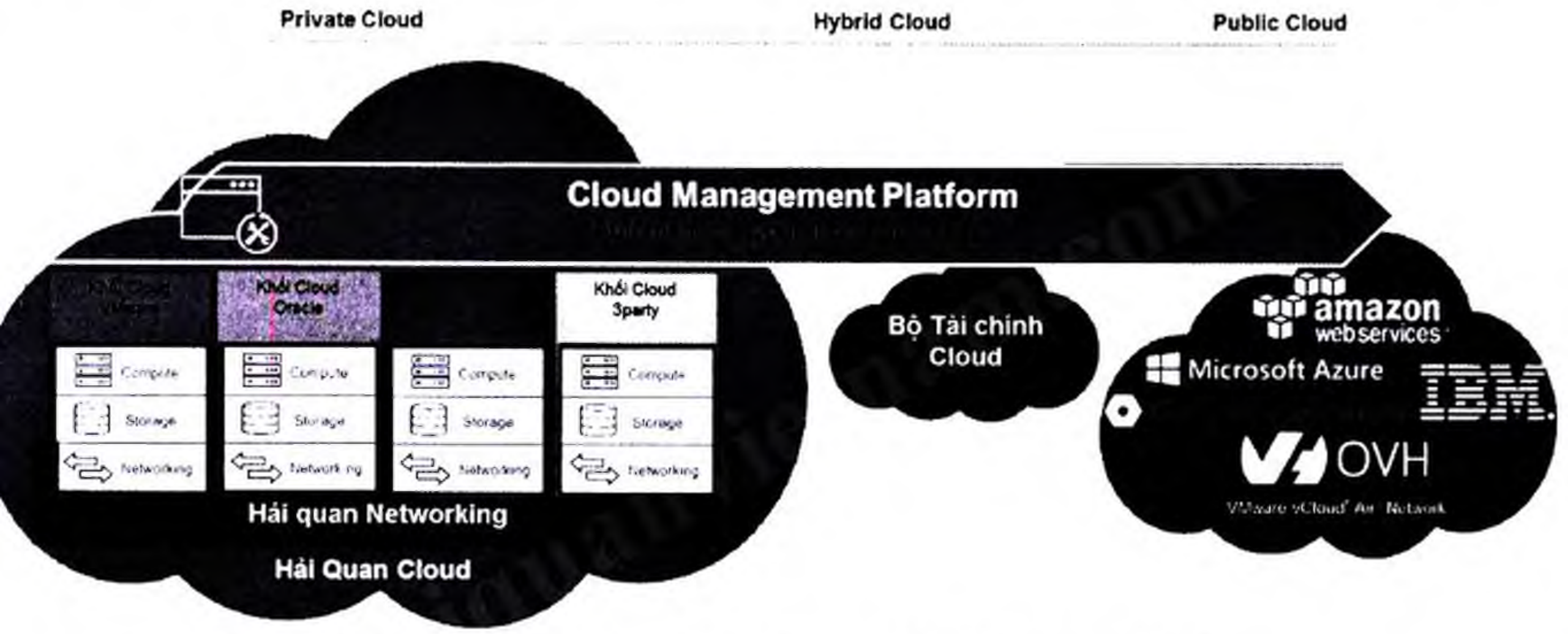
MÔ HÌNH PHẦN CỨNG HẢI QUAN SỐ

(ban hành kèm theo công văn số 1806/TCHQ-TXNK ngày 20/5/2022 của Tổng cục Hải quan)

Kiến trúc Điện toán đám mây ngành Hải quan đang hướng tới

. Mô hình kiến trúc

Kiến trúc điện toán đám mây ngành Hải quan đang hướng tới được xây ựng theo mô hình điện toán đám mây (Private Cloud), có khả năng giao tiếp, kết ối được với đám mây Bộ Tài chính và các đám mây công cộng (Public Cloud)



Hình 1: Kiến trúc điện toán đám mây Tổng cục Hải quan

- Đám mây công cộng: Cơ sở hạ tầng đám mây được cung cấp để sử dụng ở bởi công chúng.

- Đám mây riêng: Cơ sở hạ tầng đám mây được cung cấp để sử dụng riêng ởi một cơ quan, tổ chức duy nhất bao gồm nhiều người dùng.

- Đám mây lai (Hybrid Cloud): Cơ sở hạ tầng đám mây là một kết hợp của ai hoặc nhiều cơ sở hạ tầng đám mây khác nhau (riêng, cộng đồng hoặc công ộng).

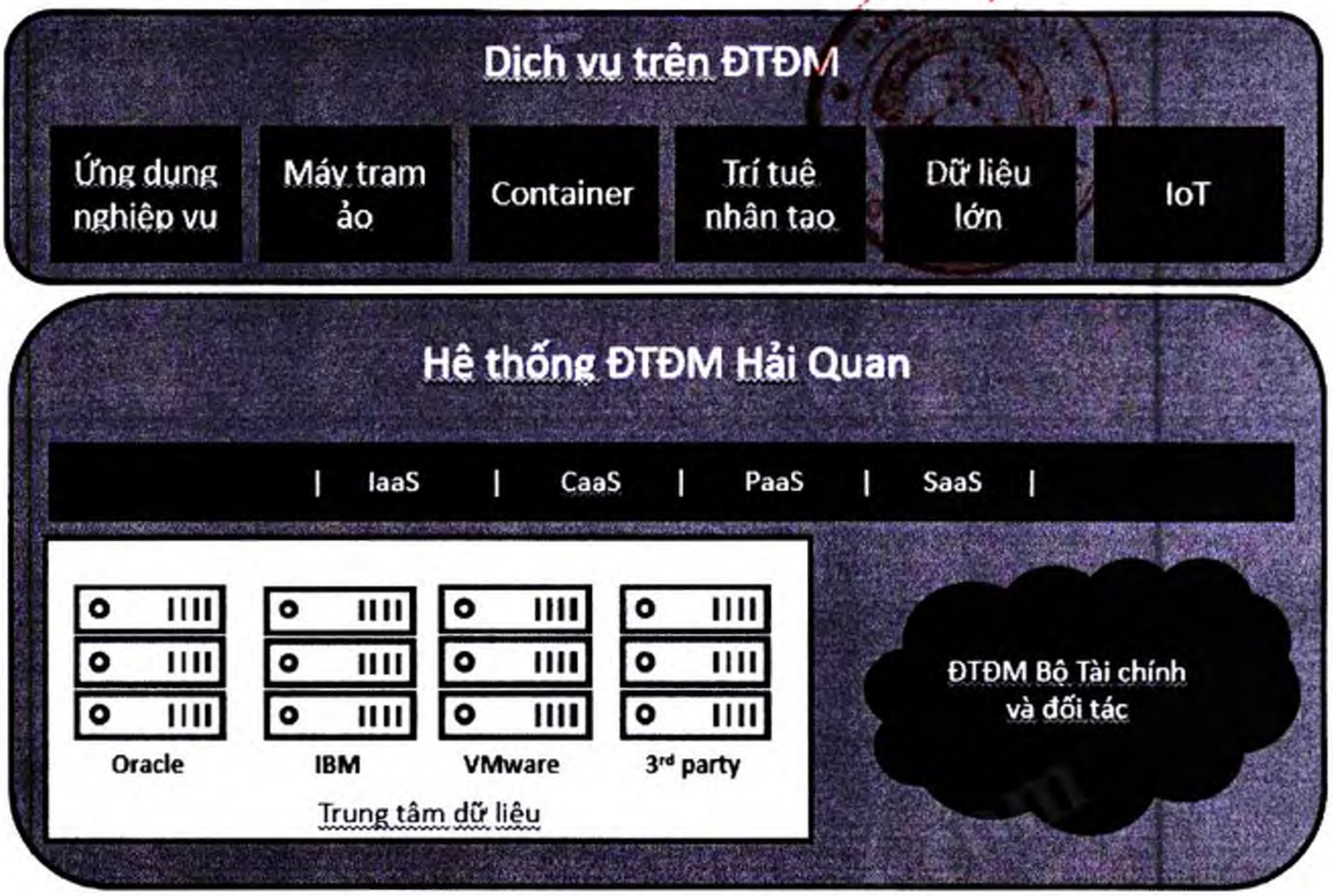
- Nền tảng điện toán đám mây (Cloud Management Platform)

- Automation: Khả năng tự động hóa

- Operation: Công cụ quản trị vận hành

- Business: Quản lý quy trình

Thiết kế Kiến trúc tổng quan hệ thống Điện toán đám mây ngành Hải quan hư sau:



Hình 1: Các thành phần trong Kiến trúc điện toán đám mây

- **Trung tâm dữ liệu:** hạ tầng trung tâm dữ liệu của Tổng cục Hải quan, bao gồm ba nhóm công nghệ ảo hoá chính là Oracle VM, IBM Power VM và VMware vSphere đã và đang triển khai, cùng nhóm công nghệ ảo hóa của hãng khác (3rd Party); được kế thừa và mở rộng để cung cấp dịch vụ Điện toán đám mây như:

+ ***Hạ tầng như một dịch vụ (IaaS)***: Quản trị việc cấp phát hạ tầng tự động trên Điện toán đám mây. Các dịch vụ có khả năng tự động cung cấp bao gồm các thành phần như: máy ảo, kết nối mạng, lưu trữ và các dịch vụ tương tác với hạ tầng điện toán.

+ ***Container như một dịch vụ (CaaS):*** Cung cấp môi trường triển khai, quản lý các ứng dụng và dịch vụ container trên nền tảng Kubernetes.

+ ***Nền tảng như một dịch vụ (PaaS):*** Cung cấp các dịch vụ phần mềm nền tảng như Môi trường runtime, cơ sở dữ liệu, hệ điều hành web server, môi trường DevOps, các công cụ và thư viện được mô hình, tạo dịch vụ và triển khai ứng dụng.

+ ***Phần mềm như một dịch vụ (SaaS):*** Cung cấp các ứng dụng, dịch vụ phần mềm của Tổng cục Hải quan tới người dùng cuối.

- **Điện toán đám mây Bộ Tài chính và đối tác:** hệ thống Điện toán đám mây ngành Hải quan cung cấp khả năng kết nối sang dịch vụ Điện toán đám mây

của Bộ Tài chính và các đối tác cùng công nghệ hoặc tuân theo các chuẩn phổ biến của dịch vụ Điện toán đám mây công cộng

Dịch vụ trên Điện toán đám mây: hạ tầng Điện toán đám mây ngành Hải quan cung cấp nền tảng thống nhất để triển khai nhiều mô hình ứng dụng từ truyền thống tới hiện đại như các ứng dụng nghiệp vụ hiện có tới các ứng dụng ảo hoá máy trạm, ứng dụng container, các dịch vụ trí tuệ nhân tạo, xử lý dữ liệu lớn hoặc xử lý dữ liêu Internet vạn vật.

. Kiến trúc thành phần (nâng cấp từ hệ thống ảo hóa hiện tại)

2.1.Khối ảo hóa VMWare:

Kiến trúc chi tiết phần giải pháp Điện toán đám mây thuộc khối ảo hóa của Vmware như sau:

Hình 2: Kiến trúc chi tiết Điện toán đám mây khối VMware

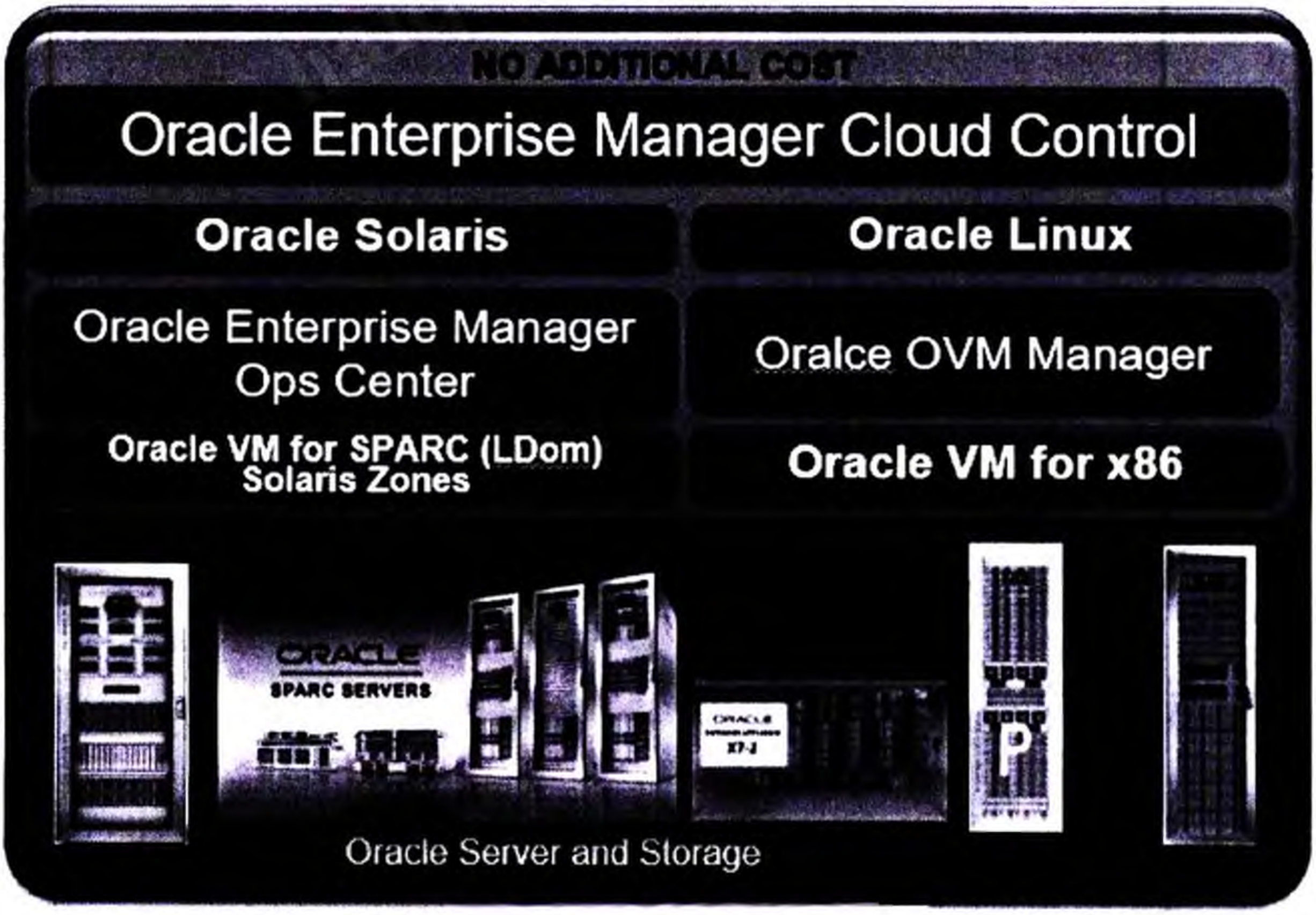
Giải pháp Điện toán đám mây của VMware triển khai dựa trên nền Máy chủ 86. Trong đó:

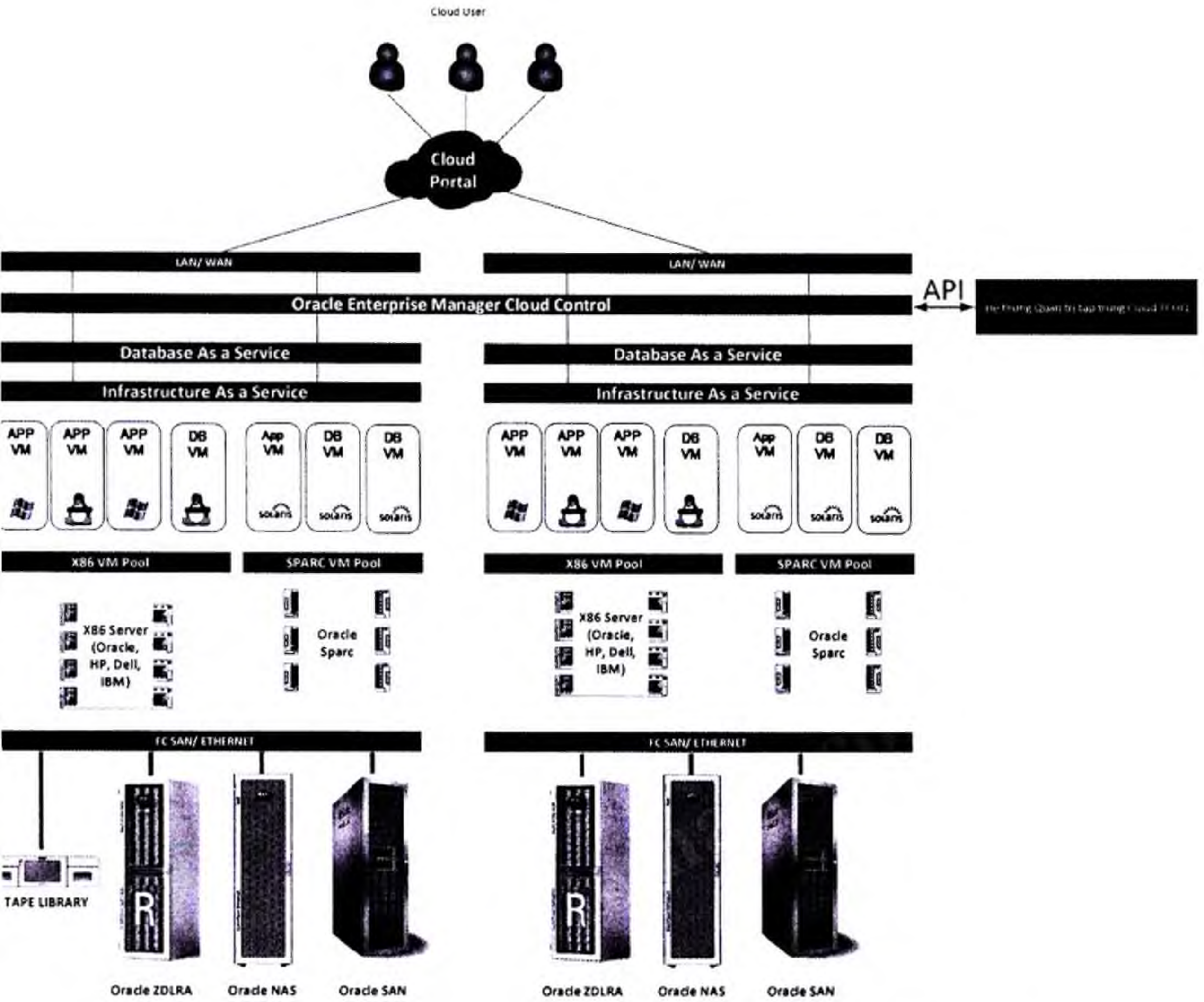
Khối cung cấp dịch vụ Điện toán đám mây: là khối quản trị và vận hành chính các dịch vụ Điện toán đám mây, cấp pháp dich vụ IaaS, PaaS và CaaS; cung cấp công cụ quản trị hiệu năng hạ tầng đám mây; công cụ thu nhận và xử lý log tập trung cho toàn bộ hạ tầng; thành phần triển khai, quản trị, nâng cấp và vá lỗi cho toàn bộ các thành của các khối.

- Khối quản trị: là một cụm máy chủ triển khai trên nền hạ tầng ảo hoá VMware vSphere. Khối quản trị bao gồm các thành phần quản trị giải pháp ảo hoá vSphere và các thành phần cần thiết xây dựng lên cụm Điện toán đám mây như máy ảo ở dạng appliance gồm: vCenter Server, NSX Manager, SDDC Manager, ….
- Khối Production, Khối Test/Dev, Khối 3-Party: là các cụm máy chủ để triển khai các dịch vụ đám mây trên nền tảng ảo hoá VMware vSphere. Các máy chủ trong cụm này có thể sử dụng đồng thời nhiều loại lưu trữ, từ hệ thống lưu trữ sử dụng công nghệ vSAN, tới các hệ thống lưu trữ vật lý như SAN Storage, NAS, iSCSI. Trên cụm này có vCenter Server riêng để quản lý tài nguyên các khối Production, Khối Test/Dev, Khối 3-Party. Trên cụm này triển khai đồng thời dịch vụ ảo hoá mang NSX-T, từ cấp phát các dịch vụ mạng ảo L2, L3 tới dịch vụ tường lửa phân tán, tường lửa biên và dịch vụ định tuyến. Đồng thời trên cụm này cũng triển khai môi trường chạy container tích hợp vào vSphere.

2.2.Khối ảo hóa Oracle

Kiến trúc chi tiết phần giải pháp Điện toán đám mây thuộc khối ảo hóa của Oracle như sau:





Hình 3: Kiến trúc chi tiết Điện toán đám mây khối Oracle

Giải pháp Điện toán đám mây của Oracle triển khai dựa trên nền Máy chủ Oracle x86 và Máy chủ Oracle Sparc. Trong đó:

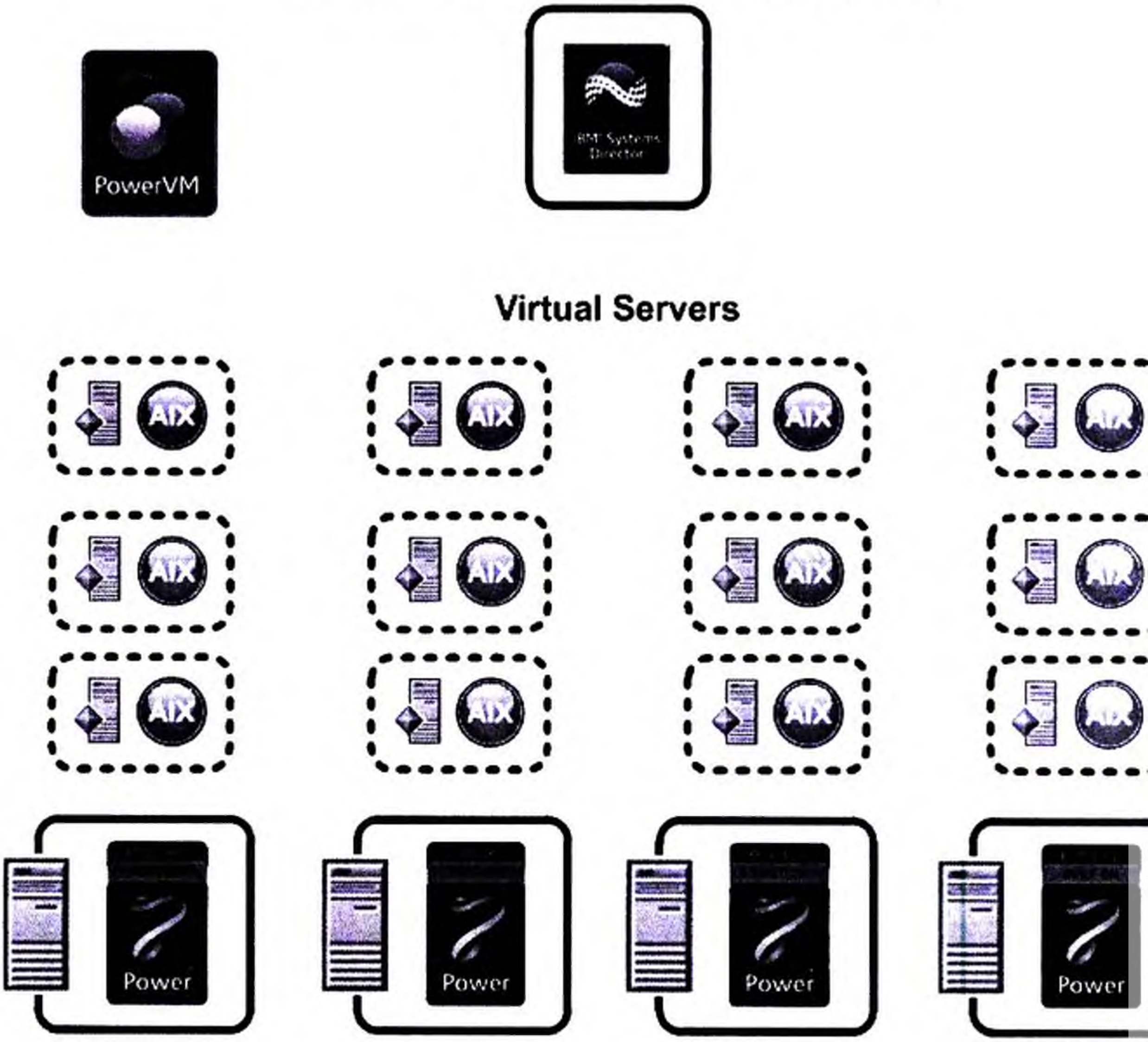
Nền tảng quản trị tập trung Oracle EMCC: Quản trị tập trung cả phần cứng và phần mềm cho hệ thống. Là Hệ thống quản trị tập trung cho điện toán đám mây bao gồm các dịch vụ IaaS, DbaaS (Database as a Service), Mwaas (Midleware as a Service);

Khối Oracle Solaris: cung cấp nền tảng ảo hóa cho các máy chủ chuyên dụng sử dụng Chip Sparc/RISC;

Khối Oracle Linux: cung cấp nền tảng ảo hóa cho các máy chủ Oracle sử dụng Chip x86;

2.3.Khối ảo hóa IBM:

Kiến trúc chi tiết phần giải pháp Điện toán đám mây thuộc khối ảo hóa của IBM như sau:



Hình 4: Kiến trúc chi tiết Điện toán đám mây khối IBM

Giải pháp Điện toán đám mây của IBM triển khai dựa trên nền Máy chủ IBM Power Series chạy Chip RISC. Trong đó:

- Nền tảng quản trị tập trung HMC: Là Hệ thống quản trị tập trung cho điện toán đám mây của IBM, quản trị tập trung cả phần cứng và phần mềm cho hệ thống.
- Khối Máy chủ P Series: cung cấp nền tảng ảo hóa cho các máy chủ chuyên dụng sử dụng Chip Sparc chạy Hệ điều hành AIX;

. Kiến trúc khối tài nguyên trong hệ thống Điện toán đám mây ngành Hải quan

Kiến trúc khối tài nguyên của hạ tầng Điện toán đám mây ngành Hải quan ương ứng với các nền tảng công nghệ Oracle, IBM, Vmware và 3rd Party được hiết kế với các khối chức năng như sau:

Khối quản trị: khối quản trị triển khai các cấu phần quản trị của giải pháp Điện toán đám mây.

Khối Production: là một hoặc nhiều cụm máy chủ cung cấp năng lực tính toán để cung cấp môi trường triển khai các dịch vụ IaaS, PaaS và CaaS.

Khối Test/Dev: là một hoặc nhiều cụm máy chủ để cung cấp môi trường cho quá trình thử nghiệm sản phẩm trước khi được triển khai trên môi trường Production.

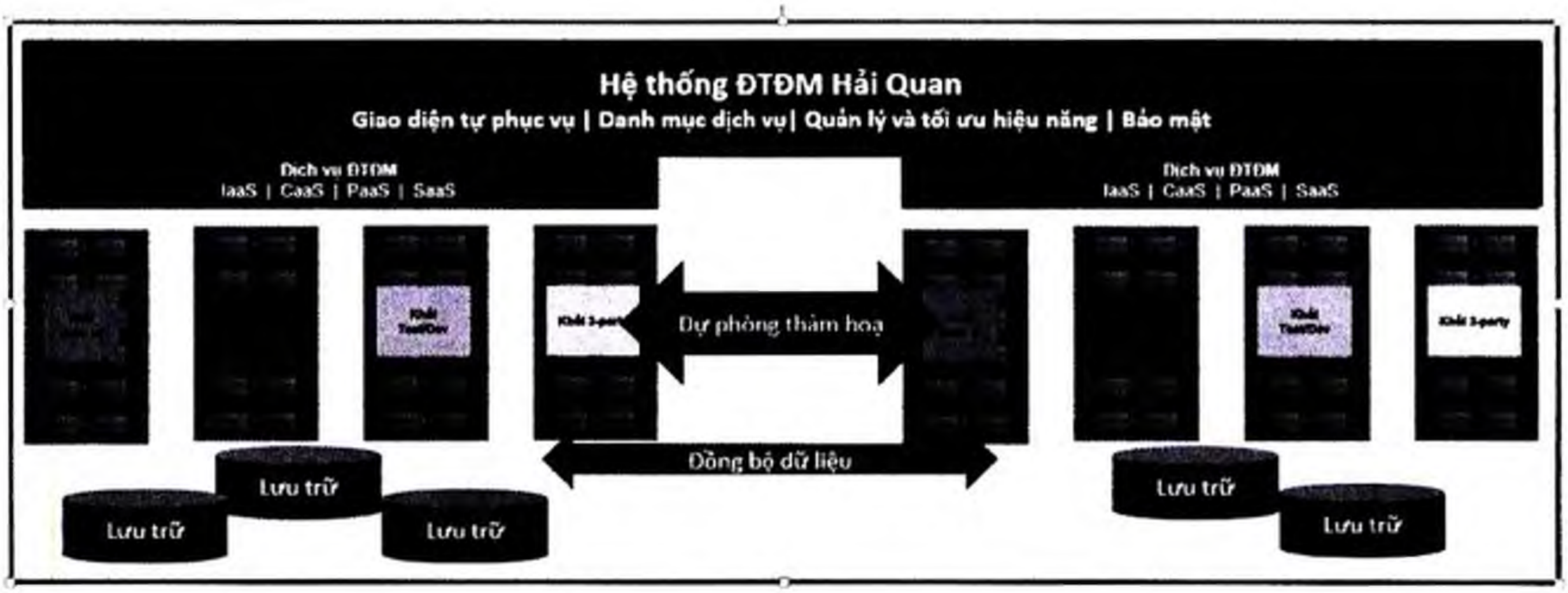
Khối 3-party: là một hoặc nhiều cụm máy chủ cung cấp môi trường riêng cho các đối tác, bộ/ban/ngành có các dịch vụ kết nối tới hệ thống của ngành Hải quan sẽ được cấp phát quyền triển khai hoặc giao diện kết nối tới.

Toàn bộ việc triển khai, quản trị và vận hành hệ thống như mở rộng / thu ẹp tài nguyên, nâng cấp, vá lỗi trên các khối Production, khối Test/Dev, khối 3-arty được thực hiện từ khối quản trị.

. Kiến trúc dự phòng thảm hoạ cho hệ thống Điện toán đám mây ngành Hải quan

Hệ thống Điện toán đám mây ngành Hải quan triển khai cung cấp năng lực ự phòng sẵn sàng cao trên nhiều mức, từ dự phòng trong phạm vi nội tại của ung tâm dữ liệu tới dự phòng giữa các trung tâm dữ liệu.

Kiến trúc Điện toán đám mây ngành Hải quan cung cấp dự phòng thảm hoạ giữa Trung tâm dữ liệu chính (DC) và Trung tâm dữ liệu dự phòng (DR) như sau:



- **Dự phòng thảm họa cho khối tài nguyên:** Hệ thống Điện toán đám mây ngành Hải quan có thể cung cấp dịch vụ dựa trên tài nguyên tại DC hoặc sử dụng tài nguyên trên các khối của DC và DR.
- **Dự phòng thảm hoạ cho khối lưu trữ:** các dịch vụ quan trọng được thiết lập dự phòng giữa DC và DR, dữ liệu cần được đồng bộ giữa DC và DR.

Yêu cầu kỹ thuật để tích hợp với hệ thống Điện toán đám mây/ảo hóa ngành Hải quan

STT	Nội dung yêu cầu
1	Quản lý hạ tầng Điện toán đám mây
	Cung cấp giao diện quản lý tích hợp hạ tầng vật lý và hạ tầng ảo hoá và truy cập tập trung để quản lý tài nguyên vật lý và ảo hoá
	Tự động quản lý vòng đời của toàn hệ thống, từ giai đoạn triển khai ban đầu tới cấu hinh, triển khai, nâng cấp, vá lỗi, đơn giản hoá các công việc quản trị hàng ngày
2	Hệ thống ảo hoá
	Hỗ trợ khả năng di chuyển nóng máy ảo, không ảnh hưởng tới người dùng, hoặc dừng dịch vụ, loại bỏ sự cần thiết lập kế hoạch dừng dịch vụ để bảo trì máy chủ

	Hỗ trợ khả năng di chuyển máy ảo giữa các máy chủ với thế hệ CPU khác nhau
	Hỗ trợ khả năng sẵn sàng cao, khi máy chủ vật lý gặp sự cố thì tự động khởi động lại máy ảo lên máy chủ khác
	Hỗ trợ khả năng hoạt động liên tục cho máy ảo khi máy chủ vật lý gặp lỗi mà không làm ngừng dịch vụ và mất dữ liệu. Hỗ trợ máy ảo lên tới 8vCPU
	Hỗ trợ khả năng cân tải, cân bằng tải nguyên cấp phát cho các máy ảo /workloads trong một cụm máy chủ ảo hoá Tối ưu tài nguyên và có thể tắt máy chủ vào thời điểm hệ thống yêu cầu ít tài nguyên
	Hỗ trợ khả năng quản trị và cấu hình mạng tập trung trên hệ thống ảo hoá thông qua việc cấu hình ở mức cluster
	Hỗ trợ khả năng cân bằng tải tự động dựa trên đặc điểm của lưu trữ để xác định lưu trữ phù hợp cho lưu trữ máy ảo khi tạo ra và lưu trữ sau đó
	Tối ưu truy xuất lưu trữ và mạng thông qua việc theo dõi liên tục hoạt động vào ra trên một vùng lưu trữ và truy xuất trên mạng, tự động phân bổ truy xuất tài nguyên tới máy ảo theo nhu cầu
	Cung cấp giao diện quản trị tích hợp cho phép quản trị cả hệ thống máy chủ vật lý và máy ảo.
	Có thể triển khai máy chủ quản trị dưới dạng sẵn sàng cao active-standby dựa cơ chế sẵn sàng cao dựng sẵn
	Hệ thống lưu trữ
	Cung cấp cơ chế thiết lập chính sách lưu trữ linh hoạt
	Cung cấp cơ chế lưu trữ hỗ trợ ổ thế rắn (All Flash)
	Cung cấp cơ chế thiết lập chất lượng dịch vụ theo IOPS

	Cung cấp cơ chế nén và chống trùng lặp
	Cung cấp cơ chế RAID-5/6 Erasure Coding
	Cung cấp cơ chế điều khiển lưu trữ cho ứng dụng container
	Cung cấp nền tảng lưu trữ cho các dịch vụ lưu trữ đối tượng (object storage)
	Cung cấp giao diện tích hợp với phần mềm quản trị đám mây
4	Hệ thống mạng định nghĩa bởi phần mềm (SDN)
	Quản lý tập trung chính sách kết nối mạng, bảo mật, cân bằng tải
	Cung cấp cơ chế chuyển mạch phân tán trên môi trường ảo hoá, cho phép mở rộng mạng L2 trên mạng L3
	Cung cấp cơ chế định tuyến động giữa các mạng ảo, phân tán, tính hợp lõi hệ thống ảo hoá
	Cung cấp tường lửa biên, NAT, và mạng riêng ảo
	Cung cấp kết nối giữa mạng ảo hoá và VLAN vật lý
	Hỗ trợ định tuyến động
	Hỗ trợ tích hợp với nền tảng quản trị Điện toán đám mây
	Cung cấp tường lửa phân tán lên tới L7, tích hợp với nhân hệ thống ảo hoá, hỗ trợ cho máy ảo và container
	Cung cấp cân bằng tải từ L2 tới L7
	Cung cấp tính năng tích hợp tường lửa với định danh trên hệ thống Active Directory
	Cung cấp cân bằng tải cho các dịch vụ container
	Cung cấp kết nối mạng bảo mật giữa nhiều trung tâm dữ liệu

	Cung cấp tường lửa hiểu trạng thái, lọc theo URL
	Cung cấp công cụ giám sát luồng giao dịch giám sát mạng ảo hoá
	Hỗ trợ giám sát và lập kế hoạch quản lý tường lửa phân tán
	Hệ thống cân bằng tải ứng dụng web và phần mềm
	Cung cấp tính năng cân bằng tải hỗ trợ TLS 1.3, SSL termination, default gateway, GSLB, DNS, wildcard VIP và L4-L7
	Cung cấp khả năng chuyển luồng thông minh qua nhiều sites và trên nhiều hệ thống Điện toán đám mây
	Cung cấp khả năng giám sát hiệu năng và ghi lại và phát lại các sự kiện mạng bằng ghi nhật ký chi tiết
	Cung cấp khả năng mở rộng cân bằng tải cho ứng dụng dựa trên mẫu lưu lượng truy cập thời gian thực
	Cung cấp kết nối tới các hệ thống như VMware, SDN controller, OpenStack, AWS, GCP, Azure, Kubernetes, VMC
	Cung cấp thông tin chi tiết về ứng dụng từ dịch vụ proxy phân tán tới bảo mật ứng dụng web theo thời gian thực
	Cung cấp mô hình bảo mật tích cự và chế độ học cho tường lửa ứng dụng web
	Cung cấp cơ chế xác thực cho ứng dụng HTTP theo cơ chế SAML2.0
	Cung cấp giao diện cho tự động hoá và lập trình
	Cung cấp cơ chế phân tích từ xa hệ thống cân bằng tải phân tán dựa trên dữ liệu thời gian thực
	Cung cấp chức năng quản lý dựa trên chính sách và có khả năng chọn lựa nâng cấp

	Hợp nhất dịch vụ container như ingress, WAF, GSLB, DNS/IPAM trên một nền tảng mở rộng hỗ trợ nhiều cụm, site và nhiều vùng container
6	Hệ thống giám sát kết nối mạng
	Cung cấp cơ chế giám sát luồng giữa mạng ảo hoá - ảo hoá, ảo hoá - vật lý, và luồng mạng theo giao thức IPFIX
	Cung cấp cơ chế lập kế hoạch tường lửa phân đoạn mạng
	Cung cấp giao diện hiển thị ứng dụng được phát hiện
	Cung cấp giao diện vận hành về hình thái mạng, danh sách trạng thái, cân bằng tải
	Cung cấp hiển thị thông tin qua các thiết bị của bên thứ ba như thiết bị chuyển mạch, định tuyến, tường lửa và cân bằng tải
	Cung cấp cơ chế nhập thông tin DNS mạng vật lý vào hệ thống
	Cung cấp khả năng tích hợp với phần mềm giám sát hạ tầng đám mây
7	Hệ thống quản trị, triển khai dịch vụ đám mây
	Cung cấp môi trường đa chủ thể (multi tenant)
	Cung cấp hệ thống giao diện, cho phép người dùng tự yêu cầu cấp phát dịch vụ (self-service portal)
	Cung cấp hệ thống danh mục thống nhất nhiều dịch vụ kết hợp nhiều nền tảng và nhiều hệ thống Điện toán đám mây
	Cung cấp dịch vụ hạ tầng: máy ảo, kết nối mạng, lưu trữ
	Cung cấp công cụ để thiết lập qui trình phê duyệt cấp phát tài nguyên
	Cung cấp công cụ thiết lập thời hạn sử dụng tài nguyên
	Cung cấp công cụ định nghĩa các hành động được thực hiện bởi người dùng trên dịch vụ đã triển khai

	Cung cấp công cụ kết nối tới nhiều hệ thống Điện toán đám mây khác
	Cung cấp kết nối tới hạ tầng Kubernetes
	Cung cấp công cụ kết nối tới nền tảng ảo hoá hiện có của ngành Hải quan như VMware vSphere, VMware NSX
	Cung cấp công cụ cho phép thiết kế dịch vụ trên giao diện trực quan
	Cung cấp công cụ cho phép thiết kế dịch vụ theo phương thức IaC (Infrastructure as Code) dựa trên YAML
	Cung cấp công cụ mở rộng dịch vụ dựa trên các ngôn ngữ lập trình Javascripts, Perl, NodeJS
	Hỗ trợ tích hợp các công cụ quản trị cấu hình như Terraform, SaltStack
	Hỗ trợ tích hợp với các hệ thống như Git, Ansible, Puppet và các hệ thống quản lý IP như Infoblox, Active Directory
	Hệ thống vận hành đám mây
	Cung cấp hệ thống giao diện, báo cáo, đồ thị nhiệt, biểu đồ hiệu năng hoạt động
	Cung cấp chức năng giám sát và phân tích hiệu năng
	Cung cấp khả năng giám sát tuân thủ hạ tầng ảo hoá theo các chuẩn DISA, FISMA, ISO, CIS, PCI, HIPAA, FIPS 140-2
	Quản lý dự báo hiệu năng thời gian thực bao gồm xu hướng, đo đếm tài nguyên, tính đúng tài nguyên yêu cầu và tối ưu
	Cung cấp tính năng tính toán chi phí tổng thể của trung tâm dữ liệu
	Cung cấp chức năng dự báo tài nguyên theo mô hình What-If cho thêm / bớt máy ảo
	Cung cấp chức năng cấu hình thủ công nhằm tối ưu hoạt động của máy

	ảo (workload) theo mục đích
	Cung cấp chức năng dự báo và quản lý cân bằng tài nguyên
	Cung cấp tính năng hướng dẫn khắc phục
	Tích hợp với phần mềm quản lý log
	Cung cấp giao diện tổng quan và di trú cho hệ thống lưu trữ siêu hội
	Tích hợp với giải pháp quản trị hiệu năng cho các ứng dụng trên hạ tầng đám mây
	Cơ chế sẵn sàng cao dựng sẵn (tự động chuyển sang node dự phòng)
	Cung cấp khả năng tuỳ biến bảng điều khiển, báo cáo và các khung nhìn
	Cho phép tạo ra công thức tính toán tuỳ biến (super metric) kết hợp nhiều thuộc tính khác nhau để giám sát đối tượng, tương quan số liệu, áp xạ các mối quan hệ
	Cho phép phân tích chi phí chi tiết để thu hồi, lập kế hoạch và so sánh chi phí đám mây công cộng
	Cung cấp mô hình dự báo tài nguyên What-If với các kịch bản: -đề xuất mua sắm bổ xung và loại bỏ phần cứng -thêm dung lượng lưu trữ cho hệ thống siêu hội tụ -dịch chuyển tới VMware Cloud trên AWS, AWS, Azure, Google. IBM, hoặc VMware Cloud Provider Program, và các hệ thống cloud khác
	Cho phép thiết lập hồ sơ máy ảo tuỳ biến để theo dõi số lượng máy ảo còn triển khai tiếp
	Cho phép kết hợp nhiều kịch bản được lưu và xếp chồng lên để xác định ảnh hưởng về tài nguyên và kết hoạch sử dụng hiệu quả
	Cung cấp chức năng tự động hoá dựa trên mục đích và cân bằng tải theo lịch
	Cho phép tích hợp với giải pháp quản lý đám mây, cho triển khai workload ở giai đoạn đầu và tối ưu liêu tục
	Cung cấp chức năng nhận diện cân bằng tải cho các workload vSAN
	Cung cấp chức năng đặt workload trên các máy chủ được chỉ định

	Cung cấp tính năng quản lý hiệu năng, năng lực và gỡ lỗi cho vSAN
	Cung cấp tính năng giám sát tài nguyên của hệ điều hành (CPU, Disk, Memory, Network)
	Tích hợp quản lý cho SDDC và Cloud Pod Health
	Cung các các mẫu tuân thủ tuỳ biến
	Tự động hoá khắc phục khi phát hiện không tuân thủ
	Tự động phát hiện và xây dựng ánh xạ cho các ứng dụng phụ thuộc
	Tích hợp với các giải pháp quản trị hạ tầng của bên thứ 3: lưu trữ, mạng, hệ thống hội tụ và siêu hội tụ
	Cơ chế phát hiện, giám sát và gỡ lỗi cho các ứng dụng đóng gói
	Cung cấp khả năng tích hợp với giải pháp vận hành thông minh mạng và bảo mật định nghĩa bởi phần mềm để giám sát trên mạng ảo hoá và mạng vật lý
	Quản trị giám sát các hệ thống đa đám mây AWS, Azure, Google Cloud
	Tích hợp giám sát các hệ thống cơ sở dữ liệu, lớp giữa và các ứng dụng đóng gói
	Hệ thống giám sát và phân tích log
	Cung cấp bảng điều khiển và phân tích tương tác
	Cung cấp khả năng thu thập log từ nền tảng ảo hoá
	Cung cấp khả năng tích hợp với phần mềm quản trị đám mây
	Cung cấp khả năng thu thập, truy vấn và phân tích cho nền tảng Kubernetes
	Cung cấp khả năng cảnh báo
	Cung cấp khả năng phân tích dựa trên máy học
	Cung cấp khả năng tích hợp với Active Directory
	Cung cấp khả năng thiết lập truy xuất dư trên vai trò

	Cung cấp khả năng thiết lập cụm, sẵn sàng cao, chuyển tiếp, lưu trữ và tuỳ biến lưu trữ dữ liệu
	Cung cấp khả năng tích hợp thông qua các trình cắm mở rộng (content packs)
0	Hệ thống container
	Cung cấp Container Registry
	Cung cấp khả năng giám sát container
	Cung cấp khả năng quản lý theo chính sách
	Cung cấp khả năng chuẩn đoán sự phù hợp
	Cung cấp mạng container
	Cung cấp cân bằng tải
	Cung cấp Ingress
	Cung cấp môi trường chạy Kubernetes
	Cung cấp quản lý định danh và truy cập
	Cung cấp cơ chế quản lý vòng đời
	Cung cấp hệ điều hành
	Cung cấp cơ chế bảo vệ dữ liệu
	Cung cấp cơ chế log cho container
	Hỗ trợ đa đám mây
	Hỗ trợ vSphere
1	Hệ thống giám sát tập trung
	Cung cấp giao diện giám sát thống nhất, đa nền tảng và tích hợp với phần mềm giám sát hạ tầng đám mây
	Cung cấp khả năng giám sát nền tảng IBM PowerVC, IBM HMC

	Cung cấp khả năng giám sát nền tảng Oracle Enterprise Manager,
	Cung cấp khả năng giám sát hạ tầng VMware vRealize Automation, VMware vCenter Server
12	Hệ thống phòng chống thảm hoạ
	Cung cấp hệ kịch bản khôi phục thảm hoạ tập trung
	Cung cấp cơ chế thực hiện kiểm thử liên tục
	Cung cấp cơ chế tự động thực hiện khôi phục thảm hoạ
	Cung cấp cơ chế lập kế hoạch dịch chuyển TTDL
	Tự động chuyển chiều bảo vệ và dự phòng
	Hỗ trợ đồng bộ dựa trên lưu trữ vật lý
	Tự động bảo vệ máy ảo
	Hỗ trợ đồng bộ tích hợp với hệ thống ảo hoá
	Hỗ trợ lưu trữ kéo dãn (stretched storage)
	Cung cấp cơ chế điều phối dịch chuyển giữa các TTDL

Phụ lục III

YÊU CẦU VỀ CẤP ĐỘ 4 AN NINH AN TOÀN ĐỐI VỚI HỆ THỐNG HOÀN THUẾ GTGT CHO NGƯỜI NƯỚC NGOÀI

(ban hành kèm theo công văn số 1806/TCHQ-TXNK ngày 20/5/2022 của Tổng cục Hải quan)

1. Yêu cầu về an ninh an toàn

Các thành phần, nội dung về đảm bảo an toàn thông tin (ATTT) đối với hệ thống thông tin phải tuân thủ đầy đủ các quy định pháp lý hiện hành, cụ thể: Luật An toàn thông tin mạng; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về việc bảo đảm an toàn hệ thống thông tin theo cấp độ; Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 về việc quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về việc bảo đảm an toàn hệ thống thông tin theo cấp độ; Tiêu chuẩn quốc gia TCVN 11930: 2017 về Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ; Quyết định số 201/QĐ-BTC ngày 12/2/2018 của Bộ Tài chính Ban hành Quy chế An toàn thông tin mạng Bộ Tài chính; Quyết định 1048/QĐ-TCHQ ngày 14/4/2020 của Tổng cục trưởng Tổng cục Hải quan về việc ban Quy chế bảo đảm an toàn, an ninh thông tin mạng Tổng cục Hải quan; Quyết định 1728/QĐ-TCHQ ngày 18/6/2019 của Tổng cục trưởng Tổng cục Hải quan về việc ban hành Kiến trúc và khung tiêu chuẩn an toàn bảo mật hệ thống công nghệ thông tin ngành Hải quan…

1. Yêu cầu triển khai Phương án đảm bảo an toàn thông tin về mặt kỹ thuật

2.1. Bảo đảm an toàn máy chủ

a) Xác thực:

- Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ;

- Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng);

- Thiết lập cấu hình máy chủ để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau: Yêu cầu thay đổi mật khẩu mặc định; Thiết lập quy

tắc đặt mật khẩu về số ký tự, loại ký tự; Thiết lập thời gian yêu cầu thay đổi mật khẩu; Thiết lập thời gian mật khẩu hợp lệ;

- Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với một tài khoản nhất định;

- Thiết lập cấu hình để vô hiệu hóa tài khoản nếu tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định;

- Thiết lập cấu hình để chỉ cho phép đăng nhập hệ thống vào khoảng thời gian hợp lệ (theo quy định của Tổng cục Hải quan);

- Sử dụng cơ chế xác thực đa nhân tố để xác thực người sử dụng truy cập, quản trị vào các máy chủ quan trọng.

b) Kiểm soát truy cập:

- Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa;

- Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi máy chủ không nhận được yêu cầu từ người dùng;

- Thay đổi cổng quản trị mặc định của máy chủ;

- Không cho phép quản trị, cấu hình máy chủ trực tiếp từ các mạng bên ngoài, trường hợp bắt buộc phải quản trị theiet bị từ xa phải thực hiện gián tiếp thông qua các máy quản trị trong hệ thống và sử dụng kết nối mạng an toàn;:

- Phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau trên máy chủ với người sử dụng/ nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau;

- Cấp quyền tối thiểu (quyền truy cập, quản trị) cho tài khoản quản trị máy chủ theo quyền hạn.

c) Nhật ký hệ thống:

- Thiết lập ghi nhật ký hệ thống bao gồm các thông tin cơ bản: Thông tin kết nối mạng tới máy chủ (Firewall log); Thông tin đăng nhập vào máy chủ; Lỗi phát sinh trong quá trình hoạt động; Thông tin thay đổi cấu hình máy chủ; Thông tin truy cập dữ liệu và dịch vụ quan trọng trên máy chủ;

- Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống để không mất hoặc tràn nhật ký hệ thống;

- Quản lý và lưu trữ tập trung nhật ký hệ thống thu thập được từ máy chủ;

- Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 06 tháng:

- Lưu trữ dự phòng dữ liệu nhật ký hệ thống trên hệ thống lưu trữ riêng biết có mã hóa với dữ liệu nhật ký quan trọng;

d) Phòng chống xâm nhập:

- Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ;

- Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ;

- Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng;

- Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng;

- Quản lý tập trung việc cập nhật và xử lý bản vá, điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống:

- Thực hiện cấu hình tối ưu, tăng cường bảo mật cho máy chủ trước khi đưa vào sử dụng.

đ) Phòng chống phần mềm độc hại:

- Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật;

- Kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt;

- Quản lý tập trung các phần mềm phòng chống mã độc cài đặt trên máy chủ;

- Có cơ chế kiểm tra, xử lý mã độc của các phương tiện lưu trữ di động trước khi kết nối với máy chủ.

e) Xử lý máy chủ khi chuyển giao:

- Có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng;

- Sao lưu dự phòng thông tin, dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành;

- Có biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa.

3.2. Bảo đảm an toàn ứng dụng

a) Xác thực:

- Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng;

- Lưu trữ có mã hóa thông tin xác thực hệ thống;

- Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng: Yêu cầu thay đổi mật khẩu mặc định; Thiết lập đặt mật khẩu theo tiêu chí mật khẩu mạnh; Thời gian yêu cầu thay đổi mật khẩu; Thiết lập thời gian mật khẩu hợp lệ;

- Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định;

- Mã hóa thông tin xác thực trước khi gửi qua môi trường mạng;

- Thiết lập cấu hình ứng dụng để ngăn cản việc đăng nhập tự động đối với các ứng dụng, dịch vụ cung cấp và xử lý dữ liệu;

- Vô hiệu hóa tài khoản nếu đăng nhập sai nhiều lần vượt số lần quy định:

b) Kiểm soát truy cập:

- Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa;

- Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng;

- Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa;

- Phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của ứng

dụng với từng người/nhóm sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau;

- Giới hạn số lượng các kết nối đồng thời (kết nối khởi tạo và đã thiết lập) đối với các ứng dụng, dịch vụ máy chủ cung cấp;

- Cấp quyền tối thiểu cho tài khoản quản trị ứng dụng theo quyền hạn;

- Cấp quyền tối thiểu cho tài khoản kết nối cơ sở dữ liệu.

c) Nhật ký hệ thống:

- Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: (1) Thông tin truy cập ứng dụng; (2) Thông tin đăng nhập khi quản trị ứng dụng; (3) Thông tin các lỗi phát sinh trong quá trình hoạt động; (4) Thông tin thay đổi cấu hình ứng dụng;

- Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung;

- Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 06 tháng;

- Lưu trữ dự phòng dữ liệu nhật ký hệ thống trên hệ thống lưu trữ riêng biệt, có mã hóa đối với dữ liệu nhật ký quan trọng.

d) Bảo mật thông tin liên lạc:

- Mã hóa thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trước khi truyền đưa, trao đổi qua môi trường mạng; sử dụng phương án mã hóa theo quy định về bảo vệ bí mật nhà nước đối với thông tin mật;

- Sử dụng kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền;

- Sử dụng kết hợp các kết nối mạng an toàn hoặc biện pháp mã hoá để đảm bảo dữ liệu quan trọng được mã hoá 02 lần khi truyền qua môi trường mạng:

- Sử dụng kênh vật lý riêng khi truyền đưa, trao đổi qua môi trường mạng đối với dữ liệu quan trọng;

đ) Chống chối bỏ:

- Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu quan trọng:

- Chữ ký số được cung cấp bởi cơ quan có thẩm quyền hoặc đơn vị cung

cấp dịch vụ chữ ký số được cấp phép;

- Có phương án bảo đảm an toàn trong việc sử dụng chữ ký số.

e) An toàn ứng dụng và mã nguồn:

- Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý;

- Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu;

- Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF;

- Có chức năng kiểm soát lỗi, thông báo lỗi từ ứng dụng;

- Đảm bảo không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng;

- Có chức năng tạo lập, duy trì và quản lý phiên làm việc an toàn.

2.3. Bảo đảm an toàn dữ liệu

a) Nguyên vẹn dữ liệu:

- Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn;

- Có phương án giám sát, cảnh báo khi có thay đổi thông tin, dữ liệu lưu trữ trên hệ thống lưu trữ/phương tiện lưu trữ;

- Có phương án khôi phục tính nguyên vẹn của thông tin dữ liệu.

b) Bảo mật dữ liệu:

- Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ;

- Sử dụng các phương pháp mã hóa mạnh để mã hóa dữ liệu;

- Có phương án quản lý và bảo vệ dữ liệu mã hóa và khóa giải mã:

- Thiết lập phân vùng lưu trữ mã hóa, phân quyền truy cập chỉ cho phép người có quyền được truy cập, quản lý dữ liệu mã hóa.

c) Sao lưu dự phòng:

- Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ:

- Phân loại và quản lý các dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau;

- Có hệ thống/phương tiện lưu trữ độc lập để sao lưu dự phòng;

- Phương pháp sao lưu dự phòng có tính sẵn sàng cao, cho phép khôi phục dữ liệu nóng khi một thành phần trong hệ thống xảy ra sự cố.

2. Phải thực hiện kiểm tra, đánh giá an toàn thông tin hệ thống trước khi đưa vào vận hành chính thức

Hệ thống trước khi đưa vào vận hành chính thức phải được đánh giá an toàn thông tin và đánh giá rủi ro, tổ chức khắc phục lỗ hổng an toàn thông tin do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép hoặc tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp.

3.2.2. Yêu cầu triển khai Phương án đảm bảo an toàn thông tin về mặt quản lý ATTT

Tuân thủ Phương án đảm bảo an toàn thông tin theo cấp độ về mặt quản lý ATTT đã triển khai đối với Hệ thống cơ sở hạ tầng thông tin Trung tâm dữ liệu TCHQ đã/đang triển khai và Quyết định 1048/QĐ-TCHQ của Tổng cục Hải quan. Ngoài ra, với Hệ thống khi triển khai cần thực hiện:

3.2.2.1. Quản lý thiết kế, xây dựng hệ thống

- Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin;

- Có tài liệu mô tả phương án đảm bảo an toàn thông tin theo cấp độ;

- Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin;

- Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống;

- Có phương án quản lý và bảo vệ hồ sơ thiết kế;

3.2.2.2. Quản lý vận hành hệ thống

a) Quản lý an toàn máy chủ và ứng dụng

Xây dựng quy trình quản lý an toàn máy chủ và ứng dụng, trong đó phải bao gồm các nội dung:

- Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ;

- Có quy định về quản lý truy cập mạng của máy chủ;

- Có quy định về quản lý truy cập và quản trị máy chủ và ứng dụng;

- Có quy định về quản lý cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố;

- Có quy định về quản lý cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng;

- Có quy định về quản lý kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống;

- Có quy định về quản lý cấu hình tối ưu và tăng cường bảo mật cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

b) Quản lý an toàn dữ liệu

Xây dựng quy trình quản lý an toàn dữ liệu, trong đó phải bao gồm các nội dung:

- Có quy định về yêu cầu an toàn đối với phương pháp mã hóa;

- Có quy định về phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa;

- Có quy định về cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu;

- Có quy định về trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ;

- Có quy định về quản lý sao lưu dự phòng và khôi phục dữ liệu: tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ;

- Có quy định về cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ;

- Có quy định về việc định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các dữ liệu quan trọng khác trên hệ thống.

c) Quản lý phòng chống phần mềm độc hại

Xây dựng quy trình quản lý phần mềm độc hại, trong đó phải bao gồm các nội dung:

- Có quy định về cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy chủ;