PHỤ LỤC 3. HƯỚNG DẪN KỸ THUẬT TRIỂN KHAI KIẾN TRÚC CHÍNH QUYỀN ĐIỆN TỬ TỈNH BÌNH PHƯỚC

1. Hướng dẫn kỹ thuật triển khai Kiến trúc ứng dụng

1.1. Khung ứng dụng nền tảng cổng

Khung ứng dụng nền tảng cổng sẽ dùng công nghệ mới nhất của: Javascript, HTML5, CSS3, J2EE, .NET/C#, RESTFull, Web Service (SOAP) và Web2.0.

- **Tiêu chuẩn**: tuân thủ các chuẩn công nghệ mở về nội dung (content), portlets, web-service và ứng dụng giao diện người dùng (front-end) để giảm chi phí phát triển và đảm bảo tính linh động giữa các cổng, máy chủ ứng dụng, CSDL, và các hệ điều hành. Các đặc tả thông số kỹ thuật cần cân nhắc tuân thủ bao gồm: JSR-168/JSR-286, Web-Service for Remote Portlet (WSRP 2.0), JSR 170/JSR 283...

- Khung ứng dụng nền tảng cổng phục vụ quản lý nhận dạng và tích hợp xác thực SSO cho người dùng để sử dụng các ứng dụng dịch vụ trong hệ thống.

- **Kiểm soát truy nhập**: Khung ứng dụng nền tảng cổng cung cấp phân quyền người dùng truy nhập vào các nội dung và dịch vụ dựa vào danh sách vai trò (Role-Based) của người dùng trong hệ thống. Ví dụ, công dân không thể truy nhập và sử dụng các chức năng dành cho công chức và các cán bộ chuyên viên.

- **Tích hợp**: Khung ứng dụng nền tảng cổng được thiết kế và triển khai dựa trên nền tảng hướng dịch vụ (SOA), do đó cho phép việc tương tác và tích hợp chức năng và dữ liệu giữa các thành phần, ứng dụng dịch vụ trong hệ thống.

- **Cá nhân hoá**: cho phép người dùng có thể cá nhân hoá các trang trên cổng thông tin phù hợp với sở thích và mục đích riêng, bằng cách thêm, loại bỏ, và định vị lại các vùng hiển thị thông tin.

- **Tìm kiếm**: cho phép tìm kiếm tất cả các nội dung được phép truy nhập thông qua cổng (bao gồm: nội dung trong cổng thông tin, các ứng dụng dịch vụ, các CSDL quốc gia...)

- **Quản trị nội dung và quản lý tài liệu**: cung cấp kho lưu trữ tài liệu và nội dung để lưu trữ, quản lý, tích hợp và xuất bản tài liệu và nội dung đa phương tiện như là: âm thanh, hình ảnh, video và các kiểu dữ liệu khác. Và các nội dung và tài liệu này được sử dụng và chia sẻ giữa các người dùng và nhóm người dùng trong hệ thống.

- **Quản lý quy trình/luật**: cung cấp cơ chế quản lý và thiết lập các quy trình/luật phục vụ cho việc triển khai quy trình nghiệp vụ.

- **Lưu vết**: cung cấp khả năng lưu vết và quản lý các hoạt động của người dùng trong hệ thống.

- **Giám sát hiệu năng**: cho phép giám sát hiệu năng của cổng, để tối ưu hoá việc sử dụng tài nguyên của hệ thống.

- **Một số nền tảng cổng có thể sử dụng hiện nay**:
  - Mã nguồn mở: Liferay Portal, Jetspeed-2, GateIn Portal (JBoss Portal).
  - Sản phẩm thương mại: Oracle WebCenter, Oracle Weblogic Portal, IBM Websphere Portal, Microsoft SharePoint.

1.2. Kiến trúc và thiết kế các chức năng của ứng dụng dịch vụ

- Áp dụng kiến trúc module hoá (modular architecture), và kiến trúc phân tầng/lớp (tiered/layered architecture), phù hợp với quy trình nghiệp vụ, và phù hợp với các tiêu chuẩn

mở với vai trò và trách nhiệm rõ ràng. Xem xét việc phát triển các thành phần dịch vụ dùng chung và tái sử dụng khi cần thiết.

- Các công nghệ và tiêu chuẩn ứng dụng web sẽ được lựa chọn cho tất cả giải pháp ứng dụng mới.

- Tận dụng các chuẩn công nghiệp dựa trên các giải pháp phần mềm thương mại có sẵn (COST) về quản lý nội dung (content) và cổng (portals), chú ý việc sử dụng các giải pháp và công nghệ mã nguồn mở khi có thể. Việc sử dụng giải pháp COST giúp cho việc phát triển và triển khai nhanh hơn.

- Hợp nhất và đơn giản hoá các ứng dụng công nghệ ở bất cứ nơi nào có thể để giảm thiểu độ phức tạp của hệ thống.

- Lựa chọn các tiêu chuẩn mở dựa trên công nghệ, sản phẩm, công cụ, thiết kế, ứng dụng, và phương pháp phát triển.

1.3. Lựa chọn đúng các khung phát triển ứng dụng cho việc phát triển các ứng dụng web

- Các kiến trúc khung (framework architecture) nên áp dụng các kinh nghiệm thực tế trong quá trình phát triển ứng dụng, và các mẫu kiến trúc (architecture patterns) như là Model-View-Control (MVC) hỗ trợ việc tách bạch mô hình dữ liệu (Model) với các luật/quy tắc nghiệp vụ (Controller) từ giao diện người dùng (View). Những mô hình kiến trúc như vậy sẽ hỗ trợ, và thúc đẩy việc tái sử các module. Trong ứng dụng web, mô hình kiến trúc MVC này cho phép sử dụng một logic chương trình để hỗ trợ các giao diện người dùng khách nhau từ thiết bị di động (mobile), máy tính để bàn (desktop), máy tính cá nhân (laptop), KIOS...

- Một số khung kiến trúc MVC hiện tại có thể sử dụng như là: Spring MVC, Struts1, Struts2, Ruby and Rails, ASP.NET MVC....

- Khung kiến trúc ứng dụng áp dụng mô hình N-tầng (n-tier), với kiến trúc tối thiểu 3-tầng (gồm: tầng trình diễn, tầng nghiệp vụ, và tầng CSDL).

- Khung kiến trúc cung cấp khả năng sử dụng lại các thành phần và dịch vụ có sẵn.

- Khung kiến trúc sẽ bao gồm thành phần xác thực và phân quyền, tương thích với các chuẩn bảo mật. Khung kiến trúc bảo mật sẽ cho phép máy chủ web xác định người dùng của ứng dụng, và hạn chế truy cập vào các chức năng dựa trên một số tiêu chí xác định trước - Kiến trúc Bảo mật.

- Khung kiến trúc cung cấp khả năng kết nối với CSDL thông qua API, sử dụng cấu hình cho kết nối CSDL.

- Khung kiến trúc hỗ trợ khả năng quản lý giao dịch (transaction management) với CSDL.

- Khung kiến trúc hỗ trợ khả năng tạo các web-service và tương tích với các chuẩn áp dụng cho web-service.

- Khung kiến trúc hỗ trợ bộ nhớ đệm (cache) để tăng hiệu suất cho ứng dụng web.

- Một số khung kiến trúc phổ biến:

a) Java - JEE, Spring, Stripes, Struts, Sling, Tapestry, Wicket, JBoss Seam, Oracle ADF, Google Web Toolkit, OpenXava...

b) Ruby - Ruby On Rails...

c) ASP - ASP.NET MVC framework, CSL...

d) PHP - Symfony, Yii, Opendelight, Melt, Codeigniter...

- Lựa chọn các tiêu chuẩn mở dựa trên công nghệ, sản phẩm, công cụ, thiết kế, ứng dụng, và phương pháp phát triển. Các tiêu chuẩn mở tạo ra một nền tảng độc lập không phụ thuộc vào các nhà cung cấp giải pháp, cho phép việc sử dụng nhiều nhà phát triển khác nhau, và hỗ trợ việc trao đổi thông tin, liên thông, tính linh hoạt, duy trì dữ liệu, cũng như tự do hơn trong việc lựa chọn công nghệ và giải pháp từ các nhà cung cấp.

2. Hướng dẫn kỹ thuật triển khai Kiến trúc dữ liệu

Các Sở, ban, ngành của tỉnh có thể biểu diễn cấu trúc và ngữ nghĩa dữ liệu theo các khái niệm sau:

Khái niệm	Mô tả
Lược đồ dữ liệu (data schema)	Mô tả một tập dữ liệu được cấu trúc hóa và biểu diễn dữ liệu mô tả của nó. Các mô hình dữ liệu cho lược đồ dữ liệu có thể là các mô hình dữ liệu khái niệm và logic
Thực thể dữ liệu (data entity)	Sự trừu tượng hóa cho người, vật, địa điểm, sự kiện hoặc khái niệm được mô tả (hoặc đặc tính hóa) thông qua các thuộc tính/ phần tử thông dụng. Ví dụ "Người" và "công ty" là các thực thể dữ liệu. Một phiên bản của thực thể thể hiện một biểu diễn của thực thể dữ liệu, ví dụ công dân, người đóng thuế, vv…
Các phần tử/ thuộc tính dữ liệu (data elements/ attributes)	Các thuộc tính của một thực thể dữ liệu mà chứa đựng các thông tin về trạng thái của nó
Kiểu dữ liệu (data type)	Ràng buộc về kiểu biểu diễn vật lý mà một phiên bản của đối tượng/ thuộc tính dữ liệu có thể giữ (ví dụ "string" hay "integer")
Các quan hệ dữ liệu (data relationships)	Mô tả mối quan hệ giữa 2 thực thể dữ liệu. Ví dụ thực thể "Person" liên quan tới thực thể "Person name" bởi mối quan hệ "được biết bởi"

Có hai kiểu dữ liệu mô tả được đề xuất:

- Các mô hình dữ liệu logic để mô tả các tài nguyên dữ liệu được cấu trúc

- Dữ liệu mô tả nguồn tài nguyên số (ví dụ các phần tử tiêu chuẩn dữ liệu mô tả Dublin) để mô tả các nguồn dữ liệu bán cấu trúc và phi cấu trúc

Việc cài đặt nhóm khái niệm lược đồ dữ liệu có thể dưới dạng các sơ đồ quan hệ - thực thể, sơ đồ lớp, .. Việc cài đặt tài nguyên dữ liệu số có thể dưới dạng các bản ghi trong hệ thống quản lý nội dung hoặc mục lục dữ liệu mô tả.

Ngữ cảnh của dữ liệu được thu thập theo các khái niệm sau:

Khái niệm	Mô tả
Nguyên tắc phân loại (taxonomy)	Nguyên tắc phân loại cung cấp cách thức phân lớp và phân loại thông tin trong một cấu trúc phân cấp kết hợp được định nghĩa rõ ràng hợp lý mà có thể được dùng để mô tả các thực thể dữ liệu. Ví dụ, phân loại dữ liệu

Khái niệm	Mô tả
	dựa trên khu vực đối tượng như "dịch vụ quản lý giao thông", "các dịch vụ quản lý thuế", "các dịch vụ đăng ký xây dựng", v..v. Nguyên tắc phân loại có thể được phân loại rộng hơn tới đề tài (topic)
Chủ đề/ đề tài (topic)	Chủ đề là một loại trong nguyên tắc phân loại. Chủ đề là khái niệm chính để áp dụng ngữ cảnh vào dữ liệu. Một chủ đề phân loại một tài sản dữ liệu, nghĩa là một phân nhóm nhỏ dữ liệu dựa trên các phần dữ liệu logic trong miền đề tài (subject area). Ví dụ, "đăng ký VAT" là một chủ đề trong miền đề tài "Dịch vụ quản lý thuế"
Tài sản dữ liệu (data asset)	Nơi chứa dữ liệu được quản lý. Trong nhiều trường hợp, nó là cơ sở dữ liệu. Tuy nhiên, một tài sản dữ liệu có thể là website, kho văn bản, dịch vụ dữ liệu và thư mục, vv..

Cài đặt các quy tắc phân loại thực hiện dưới dạng sơ đồ chủ đề XML (XML Topic Maps), hệ thống phân cấp OWL (web ontology language) hoặc lược đồ phân loại ISO 11179. Việc cài đặt bảng kiểm kê tài sản dữ liệu có thể dưới dạng các bản ghi trong sổ dữ liệu mô tả.

Mô hình trừu tượng chia sẻ dữ liệu được biểu diễn bởi:

Khái niệm	Mô tả
Gói trao đổi (exchange package)	Mô tả việc trao đổi dữ liệu định kỳ cụ thể giữa nhà cung cấp và sử dụng dịch vụ. Một gói trao đổi gồm thông tin, (dữ liệu mô tả) liên quan tới việc trao đổi (ví dụ ID nhà cung cấp dịch vụ, ID người sử dụng dịch vụ, thời hạn có hiệu lực đối với dữ liệu, vv..), cũng như tham chiếu tới nội dung bản tin (payload) cho việc trao đổi. Ví dụ, mô tả trao đổi dữ liệu giữa phòng ban cung cấp dịch vụ và sử dụng dịch vụ để có được thông tin
Trọng tải (payload)	Một định nghĩa kiểu điện tử sẽ xác định rõ các yêu cầu về trọng tải dữ liệu được trao đổi giữa bên cung cấp và sử dụng dịch vụ. Ví dụ, một tập tin cụ thể biểu diễn dưới dạng XML chứa thông tin về một thực thể
Nhà cung cấp dịch vụ (Service Producer)	Một thực thể (người hoặc tổ chức) mà cung cấp dữ liệu cho người sử dụng
Người sử dụng dịch vụ (service consumer)	Một thực thể (người hoặc tổ chức) sử dụng dữ liệu được cung cấp bởi một nhà cung cấp
Điểm truy vấn (query point)	Một điểm cuối mà cung cấp giao diện để truy cập và truy vấn tới một tài sản dữ liệu. Một biểu diễn cụ thể của điểm truy vấn có thể là URL cụ thể mà tại đó một truy vấn dịch vụ web có thể được kích hoạt

Tiêu chuẩn hóa chia sẻ dữ liệu được hỗ trợ bởi các miền tiêu chuẩn hóa ngữ cảnh dữ liệu và mô tả dữ liệu theo các cách sau:

- Mô tả dữ liệu (data description): định nghĩa thống nhất các gói trao đổi và các điểm truy vấn giúp khả năng chia sẻ hiệu quả bên trong hệ thống và giữa các sở, ban, ngành.

- Ngữ cảnh dữ liệu (data context): việc phân loại các gói trao đổi và các điểm truy vấn hỗ trợ việc phát hiện ra chúng và sử dụng tiếp theo của chúng trong việc truy cập và trao đổi dữ liệu.

Cài đặt/ thực hiện các gói trao đổi là các bản tin XML chuẩn hoặc tập giao dịch EDI. Cài đặt các điểm truy cập có thể là các mô tả trong một mô tả toàn bộ (Universal description), phát hiện và tích hợp (UDDI), hoặc đăng ký XML của một dịch vụ web truy cập dữ liệu.

Các sở ban ngành xác định các thành phần của kiến trúc dữ liệu như sau:

- Thiết lập các nguyên tắc về kiến trúc dữ liệu mà hoạt động như đầu vào kiến trúc quan trọng hoặc bộ điều khiển (drivers) đối với các sở ban ngành để thiết kế kiến trúc dữ liệu tương lai
- Thiết lập trục tích hợp (ESB) dựa trên cơ sở hạ tầng tích hợp, sẽ cung cấp nền tảng cho việc trao đổi dữ liệu giữa các ban ngành. Việc này sẽ loại bỏ các hầm chứa thông tin và cho phép truy cập và chia sẻ dữ liệu không giới hạn/ ngăn cách giữa các sở ban ngành.
- Xác định các thực thể dữ liệu chung cốt lõi và mô hình dữ liệu mà biểu diễn các thực thể dữ liệu chung quan trọng được sử dụng trong các sở ban ngành để chia sẻ và trao đổi dữ liệu.
- Thiết lập các tiêu chuẩn dữ liệu mô tả cho các thực thể dữ liệu cốt lõi thông dụng để sử dụng trong suốt các sở ban ngành sẽ cho phép trao đổi và xử lý dữ liệu dễ hơn, hiệu quả hơn. Nó cũng xóa bỏ sự nhập nhằng và không đồng nhất trong việc sử dụng dữ liệu giữa các ban ngành. Các tiêu chuẩn này áp dụng cho tất cả các hệ thống và có thể áp dụng để sử dụng trong các giao tiếp/ giao diện với các khu vực công khai.
- Hoàn thành mô hình dữ liệu đích dựa trên các tiêu chuẩn và các hướng dẫn bên trên để hợp nhất các thực thể dữ liệu thêm mà có thể được yêu cầu quá hoặc trên các thực thể dữ liệu cơ sở để hỗ trợ cho các quá trình thực hiện.
- Định nghĩa lược đồ dữ liệu dưới dạng XML để chia sẻ và trao đổi dữ liệu thông qua khung có khả năng tương tác dựa trên các đặc tả dữ liệu thông dụng phía trên. Tất cả các sở ban ngành phải đưa ra các dịch vụ nghiệp vụ của mình dưới dạng các dịch vụ điện tử, và tuân theo mô tả trao đổi dữ liệu thông dụng đã khuyến nghị để cho phép luồng thông tin không bị tách rời.
- Chính thức hóa mô hình quản trị và quản lý dữ liệu để điều khiển các tiêu chuẩn về dữ liệu và dữ liệu mô tả.
- Đưa ra giải pháp quản lý dữ liệu chía sẻ tập trung (Master Data Management Hub) để cố gắng tập trung hóa và tiêu chuẩn hóa tập dữ liệu chính của tỉnh, bằng cách hợp nhất chính xác, dọn sạch, xóa các bản sao và điều hòa dữ liệu chính đang được lưu tại các nơi lưu trữ tách biệt. Việc này sẽ giúp duy trì các bản ghi/ hồ sơ công dân và công việc/ doanh nghiệp (business) duy nhất, tin tưởng, chính xác, trọn vẹn và đồng bộ suốt các ban ngành, nhờ đó cho phép định danh các công dân nhanh chóng và dễ dàng tại bất kỳ nơi nào.

Thiết lập các khả năng về chia sẻ thông tin và tích hợp dữ liệu như sau:

- Xác định một chiến lược tích hợp dữ liệu hiệu quả dựa trên ETL mà hỗ trợ cả quá trình phân tích, thực hiện và dữ liệu.
- Nên sử dụng một giải pháp tích hợp dữ liệu toàn thể mà hỗ trợ các vấn đề kiến trúc sau:

- Tách, biến đổi và tải (ETL: Extract, Transform and Load): ETL được dùng trong tất cả các chương trình tích hợp dữ liệu để truy cập dữ liệu từ một hệ thống, biến đổi và tải nó vào hệ thống đích. Công nghệ ETL nhóm/gộp tất cả các dịch vụ cơ sở lại, thường qua một giao diện thiết kế, để xây dựng các dịch vụ có thể dùng lại được và hỗ trợ cho các bước đầu của tích hợp dữ liệu.
- Chất lượng dữ liệu (data quality): kiểm tra chất lượng dữ liệu rất cần thiết khi dữ liệu được tải từ nguồn tới đích. Đảm bảo giải pháp tích hợp dữ liệu cung cấp môi trường đồ họa (có hình vẽ, sơ đồ) cho quản lý dữ liệu để cho phép chúng gộp nhóm các dịch vụ cơ sở để làm mẫu (profile), phân tích, làm phong phú (enrich), làm gọn (cleanse) và làm khớp (match) dữ liệu để tạo các luật nghiệp vụ (business rules) áp dụng theo thời gian thực hoặc theo đợt như một phần của quá trình tích hợp/ dịch chuyển/ đồng bộ hóa dữ liệu.
- Đồng bộ hóa dữ liệu (data synchronization): đảm bảo quá trình đồng bộ hóa dữ liệu cho phép dữ liệu được giữ nguyên vị trí, và được tích hợp, truy cập khi cần. Vì tính chất động của nó, kỹ thuật này thích hợp để giải quyết các vấn đề tiềm tàng nơi mà cần truy cập lượng dữ liệu lớn hoặc dữ liệu từ nhiều hệ thống cơ sở.
- Ánh xạ dữ liệu mô tả (metadata mapping): đảm bảo khả năng ánh xạ dữ liệu mô tả cho phép nhập dữ liệu mô tả từ nhiều hệ thống khác nhau và trao đổi dữ liệu mô tả với các hệ thống khác.
- Kết nối doanh nghiệp (enterprise connectivity): một phần của bước đầu việc kết nối dữ liệu đảm bảo tính kết nối với các hệ thống giao diện là cần thiết để cho phép truyền dữ liệu giữa các hệ thống. Đảm bảo giải pháp tích hợp dữ liệu hỗ trợ một loạt các kỹ thuật kết nối khác nhau như truy cập tự nhiên bằng cách sử dụng các tiện ích chuẩn và truy cập chuẩn mở rộng (như ODBC) tới tất cả các nguồn dữ liệu cấu trúc hóa lớn, gồm cơ sở dữ liệu quan hệ, các file, hệ thống ERP, ngôn ngữ đánh dấu như XML để đọc và viết. Hỗ trợ cho việc kết nối tới, và đọc viết dữ liệu từ các hàng đợi tin. Giải pháp cũng hỗ trợ khả năng nhận và gửi dữ liệu từ và tới các dịch vụ web để cung cấp khả năng kết nối trọn vẹn.

BI (Business Intelligence) nói tới tập các khả năng giúp việc tách, kết hợp và biểu diễn dữ liệu để làm thuận lợi quá trình phân tích quyết định. Nó cung cấp thông tin liên quan tới quá khứ, trạng thái hiện tại, và dự thảo tương lai của chính phủ để giúp phân tích dữ liệu cho mục đích đánh giá rủi ro và các truy vấn đặc biệt. BI bao gồm các khả năng rộng sau:

- Nhu cầu và dự báo (demand and forecasting): làm thuận lợi cho việc dự đoán các sản phẩm hữu ích đáp ứng được nhu cầu của sở ban ngành về dịch vụ.
- Phiếu ghi điểm cân bằng (balanced scorecard): hỗ trợ khung hiệu năng chiến lược hòa hợp với dữ liệu tài chính và phi tài chính.
- Hỗ trợ và lập quyết định (decision support and planning): hỗ trợ việc phân tích thông tin và dự đoán sự ảnh hưởng của các quyết định trước khi nó được tạo ra.
- Khai thác dữ liệu (data mining): cung cấp sự khám phá hiệu quả các mẫu không rõ ràng, có giá trị và các mối quan hệ trong tập dữ liệu khổng lồ.

Tìm kiếm cung cấp khả năng xác định các nguồn dữ liệu cụ thể (nghĩa là, có cấu trúc, thường trong các hệ thống đang vận hành), hoặc thông tin (không cấu trúc, có trong các kho nội dung hoặc các nơi lưu trữ trên mạng internet/ intranet). Các sở ban ngành tuân theo các

hướng dẫn kỹ thuật sau cho khả năng tìm kiếm:

- Web search: khả năng xác định và lấy được nội dung trên internet/ intranet.
- Enterprise search: khả năng tạo danh sách hợp nhất được xếp hạng bởi nhiều kiểu nội dung trên nhiều nguồn khác nhau.
- Federated search: khả năng tìm kiếm trên nhiều ứng dụng hoặc sử dụng nhiều chương trình tìm kiếm.
- Tìm kiếm ứng dụng cụ thể: khả năng tìm kiếm một ứng dụng cụ thể.

Việc báo cáo cung cấp khả năng báo cáo và truy vấn dữ liệu có trong BI. Nó cũng có thể được sử dụng để chỉ đạo việc báo cáo hoạt động trên các hệ thống nguồn nơi việc sử dụng dịch vụ được coi là thích hợp. Sở ban ngành tuân theo các hướng dẫn kỹ thuật sau cho vấn đề báo cáo:

- Báo cáo được định nghĩa trước (pre - defined reporting): các báo cáo định nghĩa trước được tạo để người dùng đạt được các yêu cầu thường xuyên.
- Báo cáo đặc biệt (ad hoc reporting): tạo báo cáo cho các yêu cầu không thường xuyên và hỗ trợ sử dụng các báo cáo thay đổi trên cơ sở theo nhu cầu.
- Truy vấn và phân tích (query and analysis): cho phép người dùng truy vấn và phân tích dữ liệu.
- Báo cáo cụ thể từng ứng dụng (application specific reporting): hạn chế tới hoặc trong một ứng dụng.

Các sở ban ngành sẽ tuân theo các hướng dẫn sau trong quá trình lựa chọn công cụ báo cáo:

Công cụ có kĩ thuật biểu diễn toàn diện, ví dụ biểu đồ, đồ thị, truy vấn, text, v..v, để cho phép người dùng gọi các báo cáo định nghĩa trước hoặc tạo các báo cáo đặc biệt. Công cụ cũng nên có khả năng tùy biến để cho phép người dùng tùy đổi và thiết lập trước cách biểu diễn báo cáo để đảm bảo tuân theo các tiêu chuẩn của ban ngành.

- Công cụ có các kỹ thuật chuyển đổi, hỗ trợ logic nghiệp vụ để chuyển đổi từ dữ liệu thô thành thông tin hữu dụng.
- Công cụ hỗ trợ việc tạo các báo cáo theo nhiều định dạng khác nhau như rtf, CSV, XML…
- Công cụ báo cáo có khả năng kết nối nguồn dữ liệu và hỗ trợ kỹ thuật truy cập chuẩn. Công cụ cũng nên có tính linh hoạt để giúp việc tích hợp dữ liệu từ nhiều cơ sở dữ liệu, các dịch vụ web, các file, đối tượng…
- Công cụ có đặc tính bảo mật cần thiết để ngăn cản truy cập trái phép. Công cụ cũng nên có khả năng tích hợp không hạn chế với xác thực người dùng bên ngoài và các khung sign on duy nhất.
- Công cụ có khả năng kết xuất theo các định dạng như excel, file, pdf
- Công cụ độc lập với nền tảng phần cứng.
- Cần có các đặc tính giám sát phiên bản và giám sát thay đổi.
- Khả năng lập lịch và phân phối của công cụ báo cáo là các tính năng tăng thêm giá trị
- Lập kế hoạch để báo cáo được chạy hàng ngày, hàng tuần và phân phát báo cáo được tạo ra tới người nhận bằng email hoặc các phương thức trên web.

Các sở ban ngành sử dụng các tài liệu điện tử để làm thuận tiện quá trình trao đổi thông tin và nâng cao khả năng cộng tác giữa các ban ngành trong tỉnh. Chuyển các kho văn bản giấy sang dạng điện tử sẽ giúp việc truy cập và đạt được thông tin dễ dàng đối với công chức và người dân, giúp cải thiện hiệu năng công việc và giảm chi phí vận hành. Sở ban ngành xem xét các khả năng quản lý tài liệu, nội dung, tri thức sau:

- Cân nhắc việc chuyển các dạng văn bản trên giấy sang dạng điện tử sẽ cho phép người dân điền dữ liệu online sẽ giảm lỗi và giảm công sức thao tác với dữ liệu
- Đối với các tài liệu dạng giấy đang tồn tại, tiến hành quét và nhận dạng OCR/ICR nội dung là cách nhanh để lấy nội dung với hiệu quả tốt hơn làm thủ công và ít lỗi hơn
- Sử dụng giải pháp quản lý tài liệu điện tử (DMS) cho phép tỉnh chia sẻ thông tin cho các ban ngành
- Xem xét việc sử dụng một kho tài liệu tập trung mức tỉnh để hợp nhất tài liệu giữa các ban ngành để làm thuận lợi cho việc tìm kiếm tài liệu dựa trên nội dung một cách nhanh chóng. Phải thực hiện các giám sát về bảo mật để ngăn cản các truy cập trái phép tới các tài liệu mật. Trong trường hợp nhiều DMS đưa ra trong các sở ban ngành khác nhau, một cổng tài liệu hợp nhất duy nhất có thể được khái niệm hóa, thống nhất tất cả DMS các ban ngành
- Sử dụng các tiêu chuẩn công nghiệp dựa trên các giải pháp quản lý tài liệu (tốt nhất là mã nguồn mở, tránh các giải pháp và công nghệ bản quyền bất cứ khi nào có thể) sẽ làm cho việc triển khai các giải pháp nhanh hơn với thời gian quay vòng tối thiểu và ít công sức phát triển hơn
- Cùng với việc xem xét công nghệ, cần thay đổi về văn hóa với một thay đổi hình mẫu trong tri thức của người sử dụng nó (nghĩa là các công dân, công chức chính phủ, …). Việc tập huấn thích hợp nên được tiến hành cho tất cả các mức công chức của chính phủ
- Một vài xu hướng quản lý tri thức nổi trội:
    - Triển khai cổng tri thức cho nội bộ công chức chính phủ để chia sẻ thông tin và các cổng quốc gia cho người dân truy cập để truyền bá thông tin cũng như sử dụng dịch vụ.
    - Hướng tới sử dụng công nghệ 4.0, ví dụ các khảo sát, thăm dò, diễn đàn thảo luận.
    - Sử dụng các phương tiện và mạng xã hội để tương tác sâu sắc hơn giữa chính phủ với người dân bằng việc dịch chuyển mô hình quảng bá truyền thống sang cam kết tích cực trên các vấn đề, chương trình và tạo quyết định.
    - Tích hợp các thiết bị di động vào kế hoạch truyền thông (ví dụ gửi tin nhắn văn bản cho các thông báo và giao dịch).

3. Hướng dẫn kỹ thuật triển khai Kiến trúc bảo mật

Khung kiến trúc bảo mật, bảo mật mạng

1. *Giám sát truy cập mạng*: người dùng được cung cấp quyền truy cập tới mạng và các dịch vụ mạng mà được xác thực một cách cụ thể việc sử dụng thông qua các kỹ thuật giám sát truy cập mạng thích hợp.
2. *Truy cập từ xa (VPN):* thực thi các chính sách và tiêu chuẩn bảo mật hỗ trợ để bảo vệ việc truy cập thông tin qua các kết nối từ xa.
3. *Mạng IPS/IDS*: bảo vệ kiến trúc mạng thông qua việc sử dụng IPS/IDS tuân thủ những điều sau:

   a. Các hệ thống IDS/IPS phải được đặt tại các ranh giới mạng các ban ngành.
   b. Thực hiện cập nhật các chữ ký và mẫu IDS/IPS đúng lúc để phát hiện các hành động có hại dựa trên các mẫu và chữ ký.
   c. Phân chia vai trò và trách nhiệm rõ ràng cho các thao tác vận hành liên quan tới việc quản lý hệ thống IDS/IPS.
4. Các ban ngành sẽ cài đặt tường lửa để tách biệt các hệ thống, ứng dụng dịch vụ mà các dịch vụ bên ngoài hoặc người dùng nội bộ có thể truy cập
5. *Quét và giám sát WLAN*: sử dụng mã hóa kiên cố và giám sát việc xác thực trên các mạng truy cập cục bộ không dây (WLAN) để ngăn chặn các truy cập trái phép tới mạng

Xác thực ứng dụng: Tuân thủ theo các tiêu chuẩn liên quan tới định danh, xác thực và quyền hạn

1. Xây dựng và duy trì một tập các chính sách và thủ tục nhất quán bao gồm các vấn đề định danh, xác thực và phân quyền cho các người dùng hệ thống
2. Duy trì để tất cả người dùng hệ thống là:
   a. Định danh duy nhất để đảm bảo trách nhiệm
   b. Được xác thực mỗi lần truy cập vào hệ thống
   c. Biết các chính sách và thủ tục giám sát truy cập
3. Sở ban ngành phân tích các kỹ thuật xác thực khác nhau và xác định cái nào có khả năng thực tế để sử dụng trong việc cấp phát dịch vụ điện tử. Trong dịch vụ điện tử, kỹ thuật xác thực được sử dụng dựa trên mức độ rủi ro của dịch vụ. Trước khi xác định một kỹ thuật xác thực cụ thể, ban ngành sẽ đánh giá kiểu xác thực cho mỗi dịch vụ cụ thể. Thêm đó, các mức xác thực khác nhau cũng được xác định dựa trên nhu cầu.
   a. *Xác thực mức 0*: ở mức này, không cần xác thực người dùng. Dữ liệu được coi như sử dụng công cộng và chúng thường là các tài liệu có thông tin (informational material). Bất kỳ người dùng hoặc thực thể nào đều có thể truy cập thông tin này. Tại mức này, không yêu cầu xác nhận định danh của người dùng. Tuy nhiên, cho các mục đích theo dõi, các sở ban ngành có thể log địa chỉ IP
   b. *Xác thực mức 1*: ở mức này, xác thực yêu cầu có độ phức tạp vừa phải. Các định danh của người dùng được lập bởi ban ngành nhằm đảm bảo các dịch vụ được truy cập bởi người dùng hoặc các thực thể được phép. Kỹ thuật xác thực đưa ra ở mức này là khóa xác thực một hệ số (one factor) dưới dạng mật khẩu. Thực hiện các chính sách về độ phức tạp mật khẩu chắc chắn để đảm bảo độ tin cậy và toàn vẹn của dữ liệu
   c. *Xác thực mức 2*: kỹ thuật xác thực mức này yêu cầu độ chắc chắn cao về tính chính xác của định danh người dùng hoặc thực thể. Nó là yếu tố cốt yếu cho các sở ban ngành quyết định , chỉ những người được xác thực được truy cập vào dịch vụ đề nghị. Điều này bao gồm cả dịch vụ online mà xử lý các dữ liệu cá nhân nhạy cảm hay thực hiện các giao dịch tài chính. Kỹ thuật xác thực đưa ra cho mức này là xác thực 2 hệ số (two factor authentication), nghĩa là, mật khẩu cụ thể cho người dùng và mật khẩu mỗi lần cho mỗi phiên để tránh việc bị lợi dụng, bị chặn hoặc các tấn công khác

Xây dựng mô hình xác thực của tỉnh phù hợp và an toàn. Nói chung, mô hình xác thực

quản lý định danh là một trong 3 kiểu như yêu cầu

1. *Mô hình hầm chứa (Silo Model):* trong mô hình này, nhà cung cấp định danh và cung cấp dịch vụ là một.
2. *Mô hình tập trung (Centralised model):* trong mô hình này, một ứng dụng riêng biệt hoặc hệ thống hoạt động như một nhà cung cấp ủy nhiệm người dùng chuyên biệt cho tất cả các nhà cung cấp dịch vụ
3. *Mô hình liên đoàn (Federated model)*: cung cấp dịch vụ logon duy nhất cho nhiều ứng dụng với một định danh duy nhất

Giao diện và bảo mật SOA (Interface and SOA security): xem xét các vấn đề bảo mật dưới đây khi sử dụng các dịch vụ web

1. SSL/TSL
2. Bảo mật dữ liệu XML
3. Ngôn ngữ đánh dấu xác nhận bảo mật (Security Assertion Mark-up language)
4. Bảo mật thông điệp SOAP

Giám sát truy cập ứng dụng: tuân thủ chặt chẽ các chính sách giát sát việc truy cập ứng dụng sau

1. Việc truy cập tới các chức năng của hệ thống ứng dụng được giới hạn phù hợp với các chính sách giám sát truy cập của các sở ban ngành
2. Việc truy cập ứng dụng dựa trên nhu cầu để biết truy cập cơ bản và hình thức từ chủ ứng dụng (owner)
3. Các hạn chế truy cập phải dựa trên các yêu cầu về nghiệp vụ cụ thể của ứng dụng
4. Xem xét các vấn đề sau để hỗ trợ các yêu cầu về hạn chế truy cập:
    a. Cung cấp giao diện người dùng để giám sát việc truy cập các chức năng hệ thống ứng dụng
    b. Giám sát việc dữ liệu được truy cập bởi 1 người dùng cụ thể
    c. Giám sát các quyền truy cập của người dùng, ví dụ đọc, viết, xóa, chạy
    d. Giám sát quyền truy cập của các ứng dụng khác
    e. Hạn chế thông tin đầu ra
    f. Quy định các giám sát truy cập vật lý và logic cho việc cô lập các ứng dụng, dữ liệu các ứng dụng hoặc các hệ thống nhạy cảm

Tường lửa các ứng dụng web (Web Application Firewalls - WAF): tuân thủ các tiêu chuẩn sau khi cài đặt tường lửa cho các ứng dụng web

1. Hầu hết các WAF có một tập các chính sách xây dựng sẵn (pre -built) để đảm bảo các thiết bị được bảo vệ an toàn khỏi các rủi ro về bảo mật ứng dụng thông thường đã được xác định . Tỉnh sẽ cấu hình các thiết bị ở "chế độ học", nhờ đó các thiết bị sẽ học các lời gọi ứng dụng được xác thực trong suốt các quá trình thiết lập/cài đặt và kiểm thử.
2. WAF sẽ được cấu hình để phân tích các dữ liệu đến và đi và tạo quyết định khóa hay cho phép các phần tử cụ thể

Truyền file (file transfer): xác định các phương thức truyền file, cân nhắc tới các vấn đề:

1. Để bảo vệ thông tin được truyền khỏi việc bị chặn, sao chép, thay đổi, định tuyến sai và phá hủy
2. Sử dụng kỹ thuật mã hóa để đảm bảo tính bảo mật, toàn vẹn và chính xác của thông tin

3. Các thỏa thuận giữa sở ban ngành và các bên liên quan phải nhằm tới vấn đề bảo mật việc truyền dẫn thông tin nghiệp vụ

Lọc nội dung web (web content filtering): cấu hình tường lửa để đảm bảo rằng lưu lượng mạng đến và đi được an toàn

Mã hóa (encryption): tạo thủ tục chuẩn hóa để mã hóa thông tin bao gồm những công việc sau:

1. Phân tích các rủi ro của việc không sử dụng các chiến lược mã hóa và băm hiệu quả thích hợp để bảo vệ thông tin giữa ứng dụng khác
2. Xác định mã hóa tối thiểu và độ dài/thuật toán/ hàm khóa băm được sử dụng
3. Tham khảo các kiến nghị được đưa ra bởi viện tiêu chuẩn và công nghệ quốc gia.
4. Phân tích yêu cầu sử dụng chữ ký điện tử trên ứng dụng khác nhau
5. Sửa đổi các ứng dụng để sử dụng các tiêu chuẩn mã hóa mới

Quét ứng dụng (application scanning): sử dụng các công cụ tự động xác thực để quét và báo cáo. Việc quét ứng dụng lý tưởng có thể được thực hiện ở mức code (code based level - phân tích code cơ bản) và tại mức sản phẩm cuối (end product level - kiểm thử sự xâm nhập) nên được thực hiện trên tất cả các ứng dụng và sản phẩm trước và sau khi triển khai trên môi trường sản phẩm thực tế. Việc quét các ứng dụng web là cần thiết và quan trọng để phát hiện các vấn đề về bảo mật có thể xảy ra.

Các chính sách về việc sử dụng mạng internet (Internet Usage Policies): Đưa ra các chính sách sử dụng chấp nhận được để giúp người dùng hiểu được cái gì được chấp nhận và không được chấp nhận trong việc sử dụng tài nguyên của các sở ban ngành. Nó sẽ đưa ra các hành động và cách xử lý theo yêu cầu khi sử dụng thiết bị sở ban ngành, tài sản có tính trí tuệ, hoặc phần mềm như việc sử dụng có tính chất cá nhân ngẫu nhiên các hệ thống, địa chỉ email và internet.

Sinh trắc học (Biometrics): sử dụng các kỹ thuật sinh trắc học phù hợp với yêu cầu về luật pháp liên quan tới vấn đề bảo mật thông tin cá nhân.

Hạ tầng mã hóa công khai (Public Key Infrastructure): sử dụng các chức năng của hạ tầng PKI.

Phân loại dữ liệu (data classification): xác định một mức phân loại dữ liệu dựa trên việc điều chỉnh mỗi yêu cầu. Dữ liệu có thể được phân loại theo các điều kiện về yêu cầu theo luật định, giá trị, mức độ rủi ro, mức độ bị lộ và sửa đổi trái phép

Truyền dẫn, lưu trữ và loại bỏ dữ liệu (data transmission, storage, disposal): tuân thủ các chính sách xử lý dữ liệu dựa trên mức phân loai dữ liệu dựa trên các yếu tố quan trọng sau:

1. Lưu trữ dữ liệu: tất cả các dữ liệu đang "nghỉ ngơi" đâu đó trên máy trạm cục bộ, trên máy chủ hoặc có được ở bất cứ dạng nào sẽ được mã hóa một cách vật lý
2. Tập hợp và truyền dẫn dữ liệu (data collection and transmission): tất cả việc truyền dẫn dữ liệu phải được thực hiện trên các kênh đã mã hóa
3. Loại bỏ dữ liệu (data disposal): dữ liệu được loại bỏ một cách nhất quán với phân loại và vòng đời của nó, tuân theo các chính sách và thủ tục của sở ban ngành. Các kỹ thuật giám sát truy cập cũng được sử dụng để đảm bảo chỉ những người dùng được phép mới có thể truy cập dữ liệu mà họ được cấp quyền truy cập tường minh trong suốt quá trình sắp xếp này

Bảo mật cơ sở dữ liệu (database security): tiến hành xem xét các giám sát bảo mật khóa cài đặt trong cơ sở dữ liệu. Việc đánh giá bao gồm xem xét các thông số cấu hình máy chủ CSDL, các thao tác và các thủ tục liên quan tới:

1. Giám sát việc truy cập và cấp phát quyền
2. Sử dụng các tài khoản theo phân quyền
3. Kiểm tra, ghi nhật ký và giám sát
4. Cấu hình hệ quản trị cơ sở dữ liệu (DBMS)
5. Quản lý người dùng và truy cập hệ điều hành (OS)
6. Cấp phát các vai trò (roles)
7. Sao lưu và khôi phục
8. Quản lý mật khẩu
9. Quản lý việc vá lỗi bảo mật cơ sở dữ liệu
10. Vai trò và cấp quyền
11. Phương pháp và thực thi việc theo dõi người dùng
12. Cấu trúc tên người dùng và mật khẩu
13. Các tiêu chuẩn cho views và roles

Diệt virut, xóa spam (antivirus, anti-spam): thực hiện việc phát hiện, ngăn chặn thích đáng và các giám sát việc phục hồi để chống lại các phần mềm xâm nhập kết hợp với việc nhận biết người dùng thích hợp.

Quản lý việc vá/ sửa lỗi (patch managemet): đưa ra tiến trình quản lý việc sửa lỗi cần nhiều tài nguyên và lặp lại mà sự thành công có nó được đánh giá trong suốt các lần kiểm duyệt và không có thời gian chết ngoài ý muốn.

Thẻ truy cập, thẻ ID (Access card, ID card): việc truy cập tới cơ sở/ văn phòng của sở ban ngành cần được điều khiển thông qua các kỹ thuật xác thực và giám sát truy cập thích hợp. Tất cả các nhân viên phải được tạo thẻ định danh nhân viên/ thẻ truy cập và phải đeo mọi lúc.

Khóa và bảo vệ (Locks and safes): tất cả các phương tiện thiết bị chứa thông tin mật phải được giữ ở những nơi an toàn với việc giám sát chặt chẽ việc truy cập.

Hệ thống giám sát và báo động: cơ sở văn phòng của sở ban ngành cần trang bị các hệ thống giám sát báo động phù hợp mà hoạt động 24/7

Bảo vệ cơ sở vật chất: thiết kế và áp dụng các bảo mật vật lý cho cơ quan, các phòng, và mọi cơ sở vật chất

Thông báo vi phạm an toàn và xử lý: định rõ tiến trình để đảm bảo rằng phát hiện ra tất cả các vi phạm về an toàn bảo mật đúng lúc và có hành động kịp thời thích đáng ngay theo đó

Xử lý sự cố: tuân theo các hướng dẫn, chính sách và thủ tục quản lý sự cố thích hợp theo tiêu chuẩn chính quyền điện tử.

Quản lý lỗ hổng và đe họa (threat and vulnerability management): thực hiện đánh giá các lỗ hổng và mối đe dọa thường xuyên để phát hiện và có biện pháp sửa chữa các lỗ hổng bảo mật trên các thiết bị và ứng dụng dịch vụ, để chủ động ngăn chặn sự lan truyền của bất kì yếu tố đe dọa nào.

Quản lý cấu hình và tài sản (asset and configuration management): nhận dạng rõ ràng tất cả các tài sản và mục đích của từng loại. Thông tin này sẽ được ghi lại vào sổ sách và thường xuyên được cập nhật.

Đo lường đánh giá và báo cáo (mesuarement and reporting): chỉ ra các chỉ báo về hiệu năng bảo mật quan trọng mà sẽ được soạn và báo cáo lên nhóm quản lý thường xuyên. Nên xác định rõ ràng cấu trúc báo cáo này, nêu rõ vai trò và trách nhiệm tương ứng

Tuân theo hướng dẫn, tiêu chuẩn bảo mật để xây dựng chiến lược và chương trình bảo mật cụ thể của mỗi ban ngành mà cần theo đúng các tiêu chuẩn công nghiệp và khung bảo mật an toàn như ISO 27001 và ISO 27002, NIST 800 và ITIL. Nên kết hợp chặt chẽ vấn đề bảo mật qua các giai đoạn của quản lý danh mục và dự án.

Thực hiện đánh giá các rủi ro dựa trên các tiêu chuẩn nội bộ như ISO 31000 mà sẽ bao gồm (không bị hạn chế) lập kế hoạch bảo mật, xác định yêu cầu bảo mật, các tiêu chuẩn đánh giá bảo mật, nâng cấp và hỗ trợ liên tục.

Làm theo mẫu các chính sách bảo mật thông tin.

Tất cả các mục thiết bị đang bị loại bỏ (being disposed of) bao gồm phương tiện lưu trữ phải được thẩm tra để đảm bảo rằng bất kỳ dữ liệu nhạy cảm và phần mềm có bản quyền bị xóa hoặc ghi đè một cách an toàn trước khi loại bỏ hoặc dùng lại. Nên sử dụng chữ ký điện tử để xác nhận tính xác thực và độ toàn vẹn của thông báo hoặc văn bản số.

Cần cân nhắc xem xét triển khai kỹ thuật ngăn chặn việc mất dữ liệu để ngăn cản việc truy cập và phân tán thông tin trái phép.

Cần duy trì việc kiểm tra các vết và nhật ký (trails and logs). Thông tin nhật ký có tính chất quyết định trong việc xác định và theo dõi các đe dọa và tổn hại tới môi trường. Có một số thiết bị và phần mềm sẽ được ghi nhật ký bao gồm các phần cứng và phần mềm: tường lửa, máy chủ web, máy chủ ứng dụng, máy chủ cổng điện tử, máy chủ xác thực, bộ điều khiển trung tâm/ miền, máy chủ cơ sở dữ liệu, máy chủ mail, máy chủ file, router, máy chủ DHCP, v..v

Thiết lập thủ tục để quản lý việc ghi nhật ký. Trong quá trình xác định thủ tục này, chủ yếu quyết định hành động, sự kiện nào nên được ghi nhật ký. Các sự kiện lý tưởng cần phải lưu giữ lại bao gồm:

1. Tạo, đọc, cập nhật và xóa các bản ghi mật.
2. Các hành động xác thực và cấp phép người dùng, ví dụ người dùng login, logout.
3. Cấp, sửa đổi, thu hồi các quyền truy cập của người dùng, bao gồm thêm một người dùng hoặc nhóm, thay đổi mức đặc quyền người dùng, thay đổi các quyền hạn liên quan tới file, thay đổi các quyền tới đối tượng cơ sở dữ liệu, thay đổi các chính sách tường lửa, mật khẩu người dùng…
4. Thay đổi cấu hình dịch vụ, mạng, hệ thống, bao gồm cài đặt các vá lỗi hoặc cập nhật phần mềm, hoặc các thay đổi phần mềm đã cài đặt khác.
5. Bật, tắt, khởi động lại các chương trình ứng dụng, hủy bỏ, làm hỏng hoặc các kết thúc bất thường tiến trình, các thất bại dịch vụ mạng.
6. Phát hiện các hành động nghi ngờ ví dụ từ các hệ thống ngăn chặn và phát hiện tấn công, các chương trình diệt virut, phát hiện phần mềm xâm nhập…

Thiết lập một danh sách các thành phần/thông tin được chuẩn hóa mà nên được lưu giữ như một phần thông tin kiểm tra nhật ký. Các phần tử tiêu biểu được lưu giữ gồm:

1. Kiểu hành động: ví dụ tạo, đọc, xóa…
2. Hệ thống con thực hiện hành động: ví dụ tên giao dịch hoặc tiến trình, định danh giao dịch hoặc tiến trình.

3. Các định danh của các đối tượng yêu cầu hành động: ví dụ tên người dùng, tên máy tính, địa chỉ IP và địa chỉ MAC.
4. Định danh của các đối tượng mà hành động được thực hiện trên nó: ví dụ tên file bị truy cập, các định danh duy nhất của các bản ghi bị truy cập trong cơ sở dữ liệu, các tham số truy vấn được sử dụng để xác định bản ghi bị truy cập trong cơ sở dữ liệu, tên máy tính, địa chỉ IP, địa chỉ MAC.
5. Các giá trị trước và sau khi hành động liên quan tới việc cập nhật một phần tử dữ liệu, nếu có thể thực hiện được. Thời gian hành động xảy ra.
6. Các trạng thái hành động, ví dụ như hành động đó được phép hay bị từ chối bởi các kỹ thuật giám sát truy cập
7. Các dòng mã mô tả hoặc/ và giải thích tại sao hành động lại bị từ chối bởi kỹ thuật giám sát truy cập, nếu có thể áp dụng được

Cần đưa ra cân nhắc về việc thiết lập một kế hoạch để chuẩn hóa định dạng lưu trữ các nhật ký đã lưu lại để đảm bảo tính toàn vẹn của nhật ký và hỗ trợ cho việc phân tích, báo cáo mức doanh nghiệp. Các kỹ thuật được biết để hỗ trợ các mục tiêu trên bao gồm nhưng không bị giới hạn các mục sau:

1. Các nhật ký sự kiện được tập hợp bởi một hệ thống quản lý nhật ký tập trung. Nhật ký được lưu theo định dạng văn bản rõ ràng (well-documented)
2. Nhật ký được lưu trong cơ sở dữ liệu tập ký tự ANSI mà tự tạo các nhật ký kiểm tra phù hợp với các yêu cầu của tài liệu này

Chỉ cung cấp việc truy cập tới mạng và dịch vụ mạng cho những người dùng mà được xác thực cụ thể để sử dụng

Cần xem xét tới vấn đề phân tầng/chia tách cơ sở hạ tầng mạng ban ngành thành các phân đoạn VLANs riêng biệt dựa trên mức độ giới hạn của các hệ thống. Việc liên lạc truyền thông giữa mỗi đoạn mạng này có thể được điều khiển bởi tường lửa

Tiến hành xem xét thường xuyên để đảm bảo làm đúng theo các chính sách điều hành đã phê chuẩn, và các yêu cầu đúng luật pháp (nếu có). Bất cứ khi nào cần, nên thực hiện kiểm tra việc tuân thủ bởi các nhà kiểm duyệt độc lập

Chỉ định/ lựa chọn các nhà cung cấp bên ngoài để thực hiện các kiểm tra việc thâm nhập trên tất cả các ứng dụng internet

Giám sát truy cập mạng:

1. Định rõ các mạng, dịch vụ mạng được phép truy cập
2. Xác định các thủ tục cấp phép để xác định ai được phép truy cập mạng và dịch vụ mạng nào
3. Định rõ các thủ tục và giám sát việc quản lý để bảo vệ việc truy cập tới các kết nối và dịch vụ mạng, bao gồm:
    a. Các phương tiện được sử dụng để truy cập mạng và dịch vụ mạng (ví dụ sử dụng mạng ảo riêng hay mạng không dây)
    b. Các yêu cầu xác thực người dùng cho việc truy cập các dịch vụ mạng khác nhau
    c. Giám sát việc sử dụng các dịch vụ mạng

Truy cập từ xa (VPN)

1. Định rõ các yêu cầu bảo mật truyền thông, xem xét tới nhu cầu truy cập từ xa tới các hệ

thống nội bộ, mức độ nhạy cảm của thông tin sẽ được truy cập và truyền qua các kết nối truyền thông và mức độ nhạy cảm của hệ thống nội bộ

2. Cung cấp một định nghĩa công việc được phép, thời gian làm việc, việc phân loại thông tin có thể được nắm giữ, các hệ thống và dịch vụ nội bộ mà các bên liên quan được cấp phép truy cập

Cấu hình tường lửa tỉnh, sở, ban, ngành cần thực hiện như sau:

1. *Lọc gói (package filtering):* tường lửa lọc gói kiểm tra mỗi gói truyền qua nó lên trên tầng mạng. Điều này có nghĩa là, 4 tầng cao hơn (ứng dụng, biểu diễn, phiên, và vận chuyển) được phép vào mạng nội bộ. Tường lửa lọc gói xem xét mỗi gói và xác định sẽ làm gì với nó dựa trên một chính sách mà ban ngành đã đề ra
2. *Proxy cổng ứng dụng (application gateway proxy):* gateway tầng ứng dụng, hay thường gọi là proxy, hoạt động trên tầng ứng dụng. Các tường lửa của proxy đối mặt với thách thức là các mạng bên ngoài phát triển không ngừng và đưa ra các giao thức, dịch vụ, ứng dụng mới liên tục. Khi điều này xảy ra, proxy sẽ khó khăn để xử lý lượng truyền thông cực độ trên các mạng
3. *Kiểm soát tình trạng (stateful inspection):* kiểm soát tình trạng sẽ thu thập, lưu trữ và điều khiển thông tin liên quan tới các tầng truyền thông và từ các ứng dụng khác. Điều này có nghĩa là, các tường lửa trạng thái có thể xác định giai đoạn nào một kết nối TCP đang ở (mở, đã gửi kết nối, đồng bộ, xác nhận, hay thiết lập), các gói tin có bị phân mảnh hay không, v…v

Quét và giám sát WLAN

1. Duy trì việc bảo mật vật lý các điểm truy cập không dây để bảo vệ khỏi việc bị trộm và truy cập tới các cổng dữ liệu. Tất cả các điểm truy cập phải được giữ tại một nơi an toàn về mặt vật lý và chỉ có thể được truy cập bởi các cá nhân được cấp phép.
2. Đảm bảo rằng tất cả các bảng điều khiển quản lý được giữ ở một nơi an toàn về vật lý.
3. Định danh tập dịch vụ (service set identifier) của mỗi điểm truy cập được thay đổi từ cấu hình mặc định sang một định danh khó đoán và khó liên kết với các ban ngành.
4. Cấu hình cơ sở hạ tầng không dây đối với xác thực mạnh bằng việc sử dụng EAP (giao thức xác thực mở rộng).

Kỹ thuật xác thực: cần xem xét việc sử dụng các kỹ thuật xác thực sau:

1. Sử dụng tối thiểu hai nhân tố xác thực được coi là xác thực mạnh như mật khẩu, PIN…
2. Sử dụng thẻ thông minh, token bảo mật phần cứng, điện thoại cầm tay…
3. Sử dụng vân tay, quét võng mạc hoặc các phương pháp sinh trắc khác

Xác thực ứng dụng: các hệ thống xác thực tuân theo các ban ngành có thể được phân loại là một, hai hoặc đa chiều, phụ thuộc vào số lượng yếu tố được áp dụng để đảm bảo mức độ chắc chắn theo mong muốn về việc xác định một thực thể điện tử.

1. Mật khẩu: là cách thức xác thực được chấp nhận rộng rãi nhất khi người dùng chứng thực độ chính xác của định danh bằng cách sử dụng bí mật chỉ họ biết. Thông thường, các mật khẩu được lưu dưới định dạng mã hóa tại thiết bị người dùng.
2. Mật khẩu dùng một lần (disposable passwỏd): mật khẩu mỗi lần dùng là khác biệt là các thiết bị vật lý mà có thể dùng để tạo các mật khẩu chỉ được dùng 1 lần. Các mật khẩu này được tạo dựa trên các mật mã cụ thể. Trong phương pháp này, việc sử dụng

mã hoặc mật khẩu đối với việc xác thực người dùng trong tương lai là không thể.

3. Token mềm (soft tokens): chúng là các khóa bí mật được lưu một cách điện tử trên các thiết bị như ổ đĩa cứng, CD, thẻ USB... Các khóa này được lưu trữ dưới dạng mã hóa và việc chỉ được truy cập thông với khóa này.
4. Token cứng (hardware tokens): token cứng là thiết bị vật lý mà người dùng phải sử dụng trong quá trình xác thực. Token hoạt động như một khóa điện tử để truy cập thông tin.
5. Sinh trắc: nói tới các kỹ thuật xác thực dựa trên các đặc điểm vật lý có thể đo lường được và có thể được kiểm tra. Xác thực dựa trên sinh trắc học hiện được quan tâm rộng rãi như một phương pháp khó bắt chước và giả mạo nhất. Có một số phương pháp sinh trắc học như: nhận dạng vân tay, quét mắt, chữ ký tự động, mẫu chữ, hình dáng vân lòng bàn tay, nhận dạng giọng nói, nhận dạng mặt…

Các chính sách quản lý mật khẩu: tuân thủ các chính sách mật khẩu mạnh như sau:

1. Quy định bắt buộc các chính sách về mức độ phức tạp của mật khẩu mạnh mẽ, khóa tài khoản, các đặc điểm hết hạn và đặt lại mật khẩu. Người dùng cuối nên có khả năng để đặt lại mật khẩu của họ
2. Quy định bắt buộc các chính sách mật khẩu mạnh với độ dài mật khẩu tối thiểu 8 kí tự, bao gồm cả chữ in hoa, in thường, chữ số và các kí tự đặc biệt
3. Mật khẩu sẽ được tạo bởi người dùng ngoại trừ trường hợp mật khẩu ban đầu và đặt lại
4. Mật khẩu ban đầu sẽ được hệ thống sinh ra bằng cách sử thuật toán sinh mã tự động
5. Sau quá trình xác thực với mật khẩu đầu tiên, người dùng được yêu cầu thay đổi mật khẩu của họ
6. Cài đặt "Các dịch vụ quên mật khẩu" để cho phép người dùng đặt lại mật khẩu của họ bằng cách trả lời các câu hỏi xác thực
7. Không hiển thị mật khẩu lên màn hình
8. Người dùng có thể thay đổi mật khẩu bất cứ thời điểm nào. Trong khi thay đổi, người dùng sẽ nhập mật khẩu mới tối thiểu 2 lần. Nếu người dùng thay đổi mật khẩu, phải gửi thông báo hoặc email tới địa chỉ mail đã đăng kí hoặc SMS để chỉ báo có thay đổi vừa xảy ra trong hồ sơ người dùng
9. Đảm bảo tối đa 90 ngày mật khẩu phải được thay đổi một lần và cho phép sử dụng lại mật khẩu sau 8 lần thay đổi
10. Phải thực hiện các chính sách kết thúc phiên để tự động logout khỏi hệ thống sau một khoảng thời gian không làm gì xác định. Người dùng nên bị từ chối khả năng làm mất hiệu lực kỹ thuật timeout/ khóa hệ thống
11. Khóa tài khoản người dùng sau 5 lần cố gắng logon thất bại và chỉ cho phép người quản trị xác lập lại tài khoản người dùng đã bị khóa
12. Tài khoản người dùng bị treo ngay khi người dùng không còn nhu cầu truy cập vào hệ thống nữa (hoặc rời cơ quan, hoặc đổi vai trò)
13. Bảo vệ và lưu trữ dữ liệu xác thực nhạy cảm dưới dạng được mã hóa trong các phương tiện lưu trữ

Đối với vấn đề bảo mật SOA, tuân theo các hướng dẫn sau:

1. Xác thực: định danh người dùng được xác minh dựa trên các chứng nhận mà người dùng đưa ra, ví dụ tên truy cập/ mật khẩu, chữ ký điện tử, toke ngôn ngữ đánh dấu bảo mật chuẩn (SAML), token Kerberos. Đối với dịch vụ web, các chứng nhận được ứng

dụng client đưa ra thay mặt cho người dùng cuối

2. Độ toàn vẹn và không từ chối(integrity and non-repudiation)
    a. Tập trung tới việc làm thế nào để các tin (message) sẽ được giữ nguyên vẹn trong quá trình truyền dẫn trên các kiểu dịch vụ phương tiện trung gian khác nhau
    b. Đảm bảo chữ ký số đặc quyền cho tin đó, cũng có một chữ ký điện tử xác định tính hợp lệ của người gửi và cung cấp dấu thời gian để đảm bảo việc truyền dẫn không thể bị từ chối sau đó bởi hoặc người gửi hoặc người nhận
    c. Các tin XML được kí bằng cách sử dụng các chuẩn chữ ký XML
3. Mức độ bảo mật: đề cập , tập trung tới việc làm thế nào để bảo vệ các dữ liệu trong tin để nó không bị lộ cho phía nhận không được định hướng tới trong quá trình truyền dẫn. Cần mã hóa nội dung tin một cách độc lập với quá trình vận chuyển. Điều này đảm bảo rằng chỉ những người nhận được nhắm tới mới có thể truy cập vào dữ liệu được bảo vệ. Nên sử dụng mã hóa đối xứng hoặc không đối xứng, và thuật toán giải mã được nêu ra trong tiêu chuẩn bảo mật WS mã hóa XML tại mức tin
4. Độ sẵn sàng: tập trung vào việc làm thế nào để bản tin được phân phát ngay lập tức tới phía nhận mà người dùng chính đáng nhận dịch vụ họ đã được quyền

Cần xem xét vấn đề thiết kế bảo mật dịch vụ web để bao phủ các khía cạnh bảo mật cốt lõi sau:

1. Sử dụng SSL/TSL: SSL/TSL là giao thức cung cấp bảo mật cho việc truyền thông trên mạng. SSL/TSL cho phép các phiên bảo mật điểm tới điểm bằng cách cung cấp việc xác thực máy chủ cho các máy khách, xác thực máy khách tùy chọn cho máy chủ, xác thực tin dữ liệu, độ tin cậy và toàn vẹn dữ liệu
2. Liên quan tới SSL, TSL kết hợp kế hoạch lưu đệm một phiên tùy chọn để giảm số lượng kết nối cần để thiết lập từ ban đầu. Việc tối ưu như vậy nhằm giảm tải tính toán do các thao tác mã hóa
3. Đối với dịch vụ web, một tin được phát bởi một máy khách, ví dụ như trình duyệt hoặc ứng dụng, có thể được định tuyến và xử lý bởi một số các ứng dụng và dịch vụ trung gian trước khi tới đích nhận cuối cùng. SSL/TSL bảo vệ chỉ bảo vệ nội dung tin trong khi chúng đang được truyền giữa cặp đầu cuối biết nhau. Bản tin, khi được xử lý bởi SSL/TSL tại điểm cuối nhận, được cung cấp giải mã cho tầng ứng dụng
4. Bảo mật dữ liệu XML: XML là ngôn ngữ trao đổi dữ liệu giữa các dịch vụ web. Bảo mật dữ liệu XML bằng cách bảo vệ tính toàn vẹn và tin mật cũng như tính xác thực của chúng, là yêu cầu quan trọng cho bảo mật dịch vụ web. Có thể đạt được độ toàn vẹn và bảo mật bằng cách sử dụng các kỹ thuật mã hóa, trong khi đạt được được tính xác thực bằng cách sử dụng các chữ ký điện tử. Mã hóa và chữ ký XML là hai cách để xác định làm thế nào để mã hóa dữ liệu và làm thế nào để đảm bảo tính xác thực của bản tin bằng cách dùng chữ ký điện tử trong tài liệu XML
5. Mã hóa XML: cung cấp bảo mật điểm cuối tới cuối (end to end) cho các ứng dụng yêu cầu trao đổi dữ liệu có cấu trúc bảo mật. Nó xác định một mô hình chuẩn cho 2 phạm vi sau:
    a. Mã hóa phần dữ liệu đang được trao đổi
    b. Bảo mật phiên giữa hai hoặc nhiều bên

6. Với mã hóa XML cả dữ liệu bảo mật và không bảo mật có thể được trao đổi trong cùng tài liệu. Nó có thể xử lý cả dữ liệu kiểu XML và không XML. Trong khi SSL/TSl cung cấp chỉ cung cấp sự tin cẩn tại lớp truyền dẫn, thì mã hóa XML cung cấp độ bảo mật tại mức ứng dụng và do đó đảm bảo độ bảo mật các bản tin từ đầu cuối tới đầu cuối đi qua nhiều dịch vụ web
7. Đặc tả mã hóa XML mô tả làm thế nào sử dụng XML để biểu diễn các tài nguyên web được mã hóa bằng số (bao gồm dữ liệu XML). Thông tin mã hóa được lưu trữ tách biệt khỏi dữ liệu mã hóa. Thông tin mã hóa lưu trữ dữ liệu về khóa mã hóavà thuật toán mã hóa. Mã hóa XML có thể dùng PKI để mã hóa dữ liệu
8. Chữ ký XML: xác định cú pháp XML cho các chữ ký điện tử. Như mã hóa XML, nó áp dụng với cả dữ liệu XML và không XML. Các mục dữ liệu được ký có thể là các tài liệu toàn bộ XML, các phần tử XML, hoặc các file chứa bất kỳ mục dữ liệu số nào. Chữ ký XML cho phép ký nhiều dữ liệu với một chữ ký. Chữ ký XML thêm việc xác thực, độ toàn vẹn dữ liệu, và hỗ trợ việc không từ chối dữ liệu mà nó ký. Chữ ký XML cho phép các cấu trúc khác nhau, như chữ ký bao (enveloping), chữ ký được bao (enveloped) và chữ ký tách biệt (detached)
9. Ngôn ngữ đánh dấu xác nhận bảo mật (security assertion markup language): SAML là một tiêu chuẩn dựa trên XML cho việc trao đổi dữ liệu được xác thực và cấp phép giữa các miền (domain) bảo mật. Trong SAML, thông tin bảo mật được biểu diễn như các xác nhận về các đối tượng (subject), tại đó mỗi đối tượng là một thực thể (hoặc con người hoặc máy tính) mà có một định danh trong một miền bảo mật. Các xác nhận có thể mang thông tin về thuộc tính của các đối tượng, về các xác thực được đối tượng thực hiện trước đó, và có thể là các quyết định về việc cấp phép xem đối tượng đó có được phép truy cập vào tài nguyên nào đó hay không
10. SMAL hỗ trợ 3 kiểu xác nhận: thuộc tính, xác thực, và quyết định cấp phép. Một xác nhận SAML có thể gồm vài câu lệnh xác nhận về tính xác thực, sự cấp phép và các thuộc tính. SAML cũng có thể được sử dụng để tạo xác nhận về các ủy quyền
11. Nhà cung cấp cũng có thể cần thông tin chi tiết về kiểu và độ mạnh của việc xác thực bởi nhà cung cấp định danh khi nó được xác thực bởi người dùng; để mang thông tin này, SAML cung cấp ngữ cảnh xác thực, mà được truyền đạt (hoặc tham chiếu) trong câu lệnh xác thực của xác nhận
12. SAML có thể hỗ trợ cho các trường hợp sử dụng sau:
    a. Đăng nhập duy nhất (sign -on): sử dụng một SAML có thể xác thực một người dùng với ứng dụng mà người đó đã được xác thực bởi một ứng dụng khác. SAML sẽ mang thông tin xác thực cho người dùng từ ứng dụng thứ nhất sang cái thứ hai
    b. Việc cấp phép: cùng với việc xác thực, SAML có thể được dùng để quyết định việc cấp phép cho một thực thể. Dựa trên vai trò của thực thể, nó có thể quyết định xem một người dùng có thể truy cập vào tài nguyên cụ thể hay không
    c. Bảo mật các tin SOAP: có thể sử dụng các xác nhận SAML trong các tin SOAP để mang thông tin bảo mật và định danh giữa các thực thể trong các giao dịch của dịch vụ web
13. Bảo mật tin SOAP: SOAP là giao thức đặc tả cho việc trao đổi thông tin có cấu trúc trong thực thi các dịch vụ web. Khi một tin SOAP được truyền qua một tập dịch vụ hoặc

ứng dụng web, nó có thể có những lỗ hổng bảo mật (loopholes) nếu việc đo lường kiểm tra thích hợp không được thực hiện. Ví dụ, một tin có thể bị kẻ tấn công đọc, có thể làm giả một yêu cầu, vv… Do đó, cần cung cấp việc bảo mật từ đầu cuối tới đầu cuối qua nhiều bước nhảy để đảm bảo tính toàn vẹn và tin cậy của các tin SOAP, cũng như để xác minh định danh của các yêu cầu

14. Sử dụng mã hóa và chữ ký XML để đạt được các mục đích này
15. Cần chuẩn hóa việc biểu diễn các thông tin bảo mật thêm trong chính các tin SOAP, để các thành phần phần mềm xử lý chúng, nghĩa là, các bộ xử lý SOAP có thể quản lý thông tin bảo mật một cách đúng đắn
16. Xem xét việc tuân thủ các tiêu chuẩn sau:
    a. Bảo mật WS
    b. Chuyển đổi bảo mật WS (ws security conversions)
    c. Độ tin cậy WS

Tuân theo các hướng dẫn về tường lửa ứng dụng sau:

1. WAF được xem xét trên góc độ phân phối ứng dụng, dịch vụ web và bảo mật mạng
2. Các giải pháp WAF có thể là một phần hoặc cung cấp cả bộ đầy đủ các chức năng để cung cấp việc bảo vệ. Nó quan trọng cho tỉnh xác nhận yêu cầu và thực hiện đánh giá rủi ro chi tiết phù hợp khi cân nhắc giải pháp WAF thích hợp

Nhận thức và tập huấn vấn đề bảo mật (awareness and training): thành lập một chương trình nhận biết/ dạy vấn đề bảo mật thông tin tuân theo các chính sách bảo mật thông tin của các sở ban ngành và các thủ tục phù hợp, xem xét tới việc thông tin của các ban ngành được bảo vệ và giám sát để thực hiện việc bảo vệ thông tin

1. Chương trình nhận thức bao gồm một số các hoạt động nâng cao việc nhận biết như các chiến dịch (ví dụ "ngày bảo mật thông tin"), phát hành các sổ tay hoặc thư tin
2. Đào tạo và huấn luyện bảo mật thông tin được thực hiện định kỳ

Phân loại bảo mật dữ liệu: Đảm bảo tuân theo khung phân loại dữ liệu sau:

1. Cung cấp tiến trình phân loại bảo mật dữ liệu chuẩn mà cho phép các sở ban ngành đánh giá các tài sản dữ liệu của họ và xác định mức phân loại bảo mật thích hợp áp dụng cho các tài sản dữ liệu đó, nhờ đó làm tăng khả năng tương tác. Xem xét việc sử dụng các tiếp cận sau:
    a. Định danh các tài sản thông tin
    b. Định danh người sở hữu tài sản thông tin
    c. Thực hiện đánh giá việc mức độ ảnh hưởng của tài sản thông tin
    d. Xác định lược độ phân loại bảo mật cho các tài sản thông tin
    e. Áp dụng các giám sát về bảo mật dựa trên việc phân loại bảo mật
    f. Lưu trữ tài liệu thông tin được phân loại bảo mật trong hồ sơ
2. Cung cấp lược đồ phân loại dữ liệu được định nghĩa rõ ràng mà biểu diễn tất cả các kiểu dữ liệu tồn tại hoặc có thể tồn tại trong môi trường. Bao gồm:
    a. Xây dựng tập tiêu chuẩn đơn giản và một lược đồ phân loại để đánh giá giá trị thông tin
    b. Khi phân loại thông tin, mỗi chủ sở hữu thông tin nên xem xét các yêu cầu về độ tin cẩn, nhạy cảm, bí mật, đúng luật, có thể kiểm soát, việc truy cập của thông tin

Tuân theo các hướng dẫn về các mức phân loại dữ liệu sau thêm vào các yêu cầu kiểm soát đang có:

1. Bí mật cao nhất: đây là mức phân loại tài sản dữ liệu cao nhất ở mức quốc gia. Các thông tin như vậy có thể gây ra "thiệt hại đặc biệt nghiêm trọng" tới vấn đề an ninh quốc gia nếu được công bố công khai
2. Bí mật: các thông tin này có thể gây ra "thiệt hại nghiêm trọng" nếu được công bố công khai
3. Kín: các thông tin này có thể gây ra "thiệt hại" nếu được công bố công khai
4. Hạn chế: các thông tin này có thể gây ra "hậu quả không mong muốn" nếu được công bố công khai
5. Không phân loại: thông tin hoặc văn bản này không có trong mức phân loại đưa ra có thể được đặt ở mức "không phân loại". Các tài liệu như vậy có thể được sử dụng công khai cộng đồng và không cần yêu cầu giám sát bảo mật để hạn chế truy cập

Tuân theo các hướng dẫn về chống virut và spam:

1. Lập các chính sách chính thức để ngăn chặn việc sử dụng các phần mềm trái phép
2. Thực hiện các giám sát để ngăn cản hoặc phát hiện việc sử dụng phần mềm trái phép (ví dụ danh sách trắng các ứng dụng)
3. Thực hiện các giám sát để ngăn cản hoặc phát hiện việc sử dụng các website nghi ngờ hoặc biết là có hại
4. Lập các chính sách chính thức để bảo vệ lại các rủi ro kết hợp với việc có được file và phần mềm hoặc từ/ qua các mạng ngoài hoặc trên bất kỳ một thiết bị khác, chỉ ra phương pháp đánh giá khả năng bảo vệ nào nên thực hiện
5. Giảm các lỗ hổng mà các phần mềm xâm nhập có thể khai thác, ví dụ thông qua việc quản lý lỗ hổng kỹ thuật
6. Tiến hành xem xét thường xuyên phần mềm và nội dung dữ liệu của các hệ thống hỗ trợ các tiến trình công việc nghiệp vụ quan trọng. Việc xuất hiện của bất kỳ các file không được chấp thuận hoặc các hiệu chỉnh trái phép phải được điều tra chính thức
7. Cài đặt và cập nhật thường xuyên các phần mềm phát hiện xâm nhập và phục hồi để quét các máy tính và thiết bị như một sự giám sát để phòng ngừa hoặc trên cơ sở hàng ngày. Việc thực hiện quét nên bao gồm:
    a. Quét bất kỳ file nào nhận trên mạng về hoặc qua bất kỳ thiết bị lưu trữ nào để phát hiện phần mềm xâm nhập trước khi sử dụng
    b. Quét các đính kèm và tải về trên mail điện tử trước khi dùng. Việc này có thể được thực hiện ở các nơi khác nhau, ví dụ máy chủ mail, các máy tính để bàn và khi vào mạng của sở ban ngành
    c. Quét các trang web để phát hiện sự xâm nhập

Quản lý lỗ hổng và mối đe dọa: Các sở ban ngành cần thực hiện các công việc sau:

1. Xác định rõ các lỗ hổng và mối đe dọa tiềm ẩn trong môi trường hệ thống thông tin tỉnh và xây dựng một tiến trình sửa chữa khắc phục cơ bản để giám sát tích cực và quản lý các hệ thống nội bộ quan trọng và bảo mật đường bao
2. Triển khai các phần mềm chống virut trên tất cả các máy chủ và máy trạm để giảm khả năng tấn công sự an toàn
3. Triển khai các thiết bị bảo mật nội bộ và đường bao (permeter), ví dụ các tường lửa

enterprise để giảm nguy cơ tấn công

4. Triển khai các giải pháp lọc nội dung web để ngăn chặn đe dọa từ các website làm hại để giúp xác định và khóa các trang web có nguy cơ rủi ro
5. Giảm lỗ hổng cho các chương trình giả mạo và email rác, cài đặt phần mềm bảo mật email mức doanh nghiệp mà kiểm tra các tin đến và đi để đảm bảo các tin rác không được truyền đi nếu hệ thống trở nên bị hại
6. Để giảm các rủi ro về bảo mật do việc dùng các ổ đĩa/ phương tiện có thể tháo rời, thực hiện các bước sửa chữa đơn giản, như hủy đặc tính "tự chạy" của hệ điều hành trên máy để bàn/ xách tay và huấn luyện người dùng quét virut các đĩa có thể tháo rời trước khi mở file
7. Quét định kỳ mạng để xác định các lỗ hổng mức hệ thống
8. Thông tin nhật ký rất quan trọng để xác định và theo dõi các đe dọa và làm hại tới môi trường. Độ chi tiết và các mức nhật ký được thiết lập để đáp ứng được các yêu cầu về quản lý bảo mật. Thiết lập các tiến trình cho việc xem nhật ký và cảnh báo
9. Triển khai các thiết bị để giám sát chủ động và quản lý an toàn thông tin nội bộ và bao quanh. Thiết lập các tiến trình quản lý và sửa chữa các tấn công về bảo mật để quản lý các mối đe dọa.
10. Triển khai hệ thống phát hiện xâm nhập mạng (IDS) trên các điểm quan trọng và bao quanh của mạng và tổ chức IDS trên các mạng nghiêm trọng
11. Triển khai tiến trình tập trung hóa để ràng buộc thông tin về đe dọa từ các nguồn khác biệt.

Quét và kiểm thử ứng dụng: Tuân theo các hướng dẫn sau:

1. Định nghĩa một ma trận mức độ rủi ro dựa trên OWASP (Open Web Application Security Project) để xác định các vấn đề thường xuyên nhất và nguy kịch nhất
    a. A1: phép nội xạ (injection)
    b. A2: Cross-site Scripting (XSS)
    c. A3: Quản lý phiên và xác thực lỗi (broken authentication and session management)
    d. A4: tham chiếu đối tượng trực tiếp không an toàn (insecure direct object references)
    e. A5: Cross-site Request Forgery (CSRF)
    f. A6: cấu hình sai bảo mật (security misconfigurations)
    g. A7: kho lưu trữ mã không bảo mật (insecure cryptographic storage)
    h. A8: thất bại khi truy cập URL hạn chế
    i. A9: bảo vệ tầng vận chuyển thiếu (Insufficient Transport Layer protection)
    j. A10: đổi hướng và gửi chuyển tiếp mất hiệu lực (invalidated redirects and forwards)
2. Xây dựng kế hoạch tạo một cơ sở hạ tầng tập trung hóa để hỗ trợ việc quét ứng dụng. Quét ứng dụng là một quá trình lặp lại. Vì vậy rất quan trọng để lưu giữ metrics như các vấn đề được nhận biết bởi phiên bản ứng dụng và giải pháp tại mức ứng dụng cũng như mức doanh nghiệp
3. Tạo một nguồn tin tưởng để chỉ báo các lập trình viên những việc làm và không được làm và các thủ tục tăng cường trong vòng đời phát triển phần mềm (SDLC)

4. Tiêu chuẩn xác nhận/ kiểm tra an toàn ứng dụng: tuân theo các tiêu chuẩn xác nhận an toàn mức ứng dụng (ASVS) từ OWASP. Mục tiêu chính của tiêu chuẩn xác nhận an toàn ứng dụng OWASP là để cung cấp một cơ sở cho việc kiểm thử các kỹ thuật giám sát bảo mật ứng dụng, cũng như bất kỳ giám sát bảo mật kỹ thuật nào trong môi trường, mà dựa trên việc chống lại các lỗ hổng như XSS và SQL injection. Có 3 phần chính với OWASP ASVS. Các yêu cầu trong ASVS:
    a. Các mức độ xác nhận/ kiểm tra độ an toàn mức ứng dụng tăng theo chiều rộng và sâu khi tăng lên mức cao hơn
    b. Các yêu cầu xác nhận quy định một giải pháp danh sách trắng (white - list) duy nhất để giám sát an toàn
    c. Các yêu cầu về báo cáo đảm bảo rằng các báo cáo đủ chi tiết để có thể thực hiện xác nhận lại, và để xác định xem việc kiểm tra đó có chính xác và đầy đủ không