ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

NGUYỄN THANH TUYỀN

ÁP DỤNG ENTERPRISE ARCHITECTURE XÂY DỰNG KHUNG KIẾN TRÚC BẢO ĐẢM AN TOÀN THÔNG TIN CHO CÁC TỔ CHỨC DOANH NGHIỆP TẠI VIỆT NAM

Ngành: Công nghệ thông tin

Chuyên ngành: Quản lý Hệ thống thông tin

Mã số: Chuyên ngành đào tạo thí điểm

TÓM TẮT LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Hà Nội - Năm 2016

PHẦN MỞ ĐẦU

1. Cơ sở khoa học và thực tiễn của đề tài

1.1. Về phương pháp luận xây dựng kiến trúc cơ quan xí nghiệp

Ngày nay, ứng dụng công nghệ thông tin (CNTT) vào mọi mặt của đời sống xã hội và hoạt động sản xuất kinh doanh là một xu thế tất yếu, CNTT đã và đang làm biến đổi sâu sắc đời sống, kinh tế, văn hoá xã hội của mỗi quốc gia, vùng lãnh thổ trên toàn thế giới. Việc ứng dụng CNTT tại các tổ chức doanh nghiệp đang được đẩy mạnh hơn bao giờ hết. Tuy nhiên, trong quá trình phát triển, bất kỳ một tổ chức, hệ thống nào khi phát triển tự phát đến một quy mô nhất định cũng gặp một số vấn đề nảy sinh như:

- Hệ thống thông tin càng ngày càng phức tạp, tốn kém, khó điều hành. Chi phí và mức độ phức tạp của hệ thống tăng theo cấp lũy thừa;

- Mức độ hệ thống thông tin đáp ứng nhu cầu của tổ chức càng ngày càng kém đi. Mỗi khi có nhu cầu mới hoặc thay đổi, rất khó điều chỉnh một hệ thống thông tin cồng kềnh, đắt tiền đáp ứng được các nhu cầu mới đó.

Không chỉ ở Việt Nam mà cả ở các nước phát triển việc xây dựng các hệ thống thông tin phần lớn chưa có một kiến trúc toàn diện dẫn đến các hệ thống được đầu tư xây dựng chắp vá, thiếu đồng bộ, không toàn diện, khả năng tích hợp kém… đặc biệt là nhiều hệ thống sau khi xây dựng xong không đưa vào sử dụng được hoặc sử dụng kém hiệu quả do không đáp ứng được nhu cầu thực tế. Trong bối cảnh đó nhu cầu đặt ra là phải có các phương pháp luận xây dựng kiến trúc (hay còn gọi là "khung kiến trúc") để giúp cho các cơ quan, doanh nghiệp có thể vận dụng, xây dựng kiến trúc CNTT cho mình. Trên thế giới, đã có nhiều khung kiến trúc được xây dựng và áp dụng đem lại hiệu quả cao như: khung kiến trúc Zachman, khung kiến trúc nhóm mở - TOGAF, khung kiến trúc tổng thể liên bang Mỹ - FEAF…

Thời gian qua, nhóm chuyên gia của Viện Công nghệ thông tin - Đại học Quốc gia Hà Nội đã nghiên cứu, xây dựng và hoàn thiện khung kiến trúc ITI-GAF (Information Technology Institute - Government Architecture Framework) với mục đích tạo một khung kiến trúc dễ hiểu và dễ áp dụng cho các cơ quan, tổ chức Việt Nam trong việc xây dựng kiến trúc CNTT phù hợp với đặc trưng về nghiệp vụ, cơ sở hạ tầng, khung pháp lý, trình độ phát triển CNTT của mình.

1.2. Xây dựng khung kiến trúc bảo đảm an an toàn thông tin cho các nước đang phát triển

Trong thời đại Internet như hiện nay, hầu như mọi dữ liệu thông tin đều được trao đổi qua không gian mạng. Sự xuất hiện của những xu hướng công nghệ mới như dữ liệu lớn, điện toán đám mây, sự tích hợp và hội tụ của truyền thông xã hội, di động, Internet vạn vật đang tạo ra những cơ hội to lớn cho người sử dụng nhưng mặt khác cũng nảy sinh những nguy cơ mất an ninh, an toàn thông tin và tội phạm mạng. Theo báo cáo của Global Risk 2015 của diễn đàn kinh tế thế giới công bố tháng 2/2015, thừa nhận mình chưa được chuẩn bị kỹ càng, đầy đủ để tự bảo vệ trước các cuộc tấn công mạng. Thiệt hại do tội phạm mạng gây ra cho nền kinh tế toàn cầu lên tới hơn 400 tỉ đô la Mỹ trong một năm. Ngoài ra, xu hướng mới của các cuộc tấn công mạng ngày nay nhằm tới các cơ sở hạ tầng trọng yếu và có thể gây ra hàng loạt hậu quả nghiêm trọng không thua kém các cuộc tấn công bằng vũ khí như bom đạn hay tên lửa. Nguy cơ và rủi ro mất an toàn thông tin đang trở lên hiện hữu, ảnh hưởng sâu rộng tác động đến các vấn đề trong mọi hoạt động kinh tế, xã hội, quốc phòng, an ninh và là một vấn đề đối với mỗi quốc gia trên toàn thế giới

Công tác bảo đảm an toàn thông tin tại các tổ chức, doanh nghiệp Việt Nam thời gian qua đã nhận được sự quan tâm, đầu tư nhất định của tổ chức, doanh nghiệp, tuy nhiên, thời gian qua vẫn chưa có một giải pháp, khung kiến trúc tổng thể bảo đảm an toàn thông tin cho các tổ chức, doanh nghiệp, công tác bảo đảm an toàn thông tin đang được phát triển một cách tự phát, độc lập giữa các tổ chức, doanh nghiệp. Thực trạng này đặt ra nhu cầu cần xây dựng một khung kiến trúc chung cho các tổ chức, doanh nghiệp trong việc kiểm tra, đánh giá cũng như xây dựng các chính sách, giải pháp bảo đảm an ninh, an toàn thông tin cho mình để tăng cường công tác bảo đảm an ninh, an toàn thông tin của các tổ chức, doanh nghiệp.

CHƯƠNG I: TỔNG QUAN VỀ KIẾN TRÚC TỔNG THỂ, KHUNG KIẾN TRÚC TỔNG THỂ

1.1. Tổng quan về kiến trúc tổng thể

1.1.1. Kiến trúc tổng thể

Khái niệm về kiến trúc tổng thể được hiểu theo một số khái niệm như sau:

+ Kiến trúc tổng thể bao gồm tầm nhìn, nguyên tắc và các tiêu chuẩn hướng dẫn việc mua, triển khai công nghệ trong doanh nghiệp (Theo Forrester, Gene Leganza,2001)

+ Kiến trúc tổng thể là quá trình dịch chuyển tầm nhìn và chiến lược kinh doanh làm thay đổi doanh nghiệp một cách hiệu quả bằng cách tạo ra, truyền tải, và cải thiện các nguyên tắc và các mô hình mô tả trạng thái cơ bản của doanh nghiệp trong tương lai và cho phép nó hoạt động (Theo Gartner Group).

+ Kiến trúc tổng thể là sự quản lý một cách tối đa sự đóng góp của các nguồn lực, đầu tư công nghệ thông tin và các hoạt động phát triển hệ thống để đạt được một mục đích chung. Kiến trúc mô tả rõ ràng mối quan hệ giữa mục tiêu chiến lược và các mục tiêu cụ thể thông qua việc đầu tư cải thiện đo lường hiệu suất cho toàn bộ doanh nghiệp hay một phần doanh nghiệp (Theo US Federal EA).

+ Thiết kế nghiệp vụ và sự gắn kết hệ thống CNTT là một phần của Kiến trúc tổng thể. Các nhà kiến trúc tìm kiếm sự gắn kết giữa quy trình và cấu trúc doanh nghiệp để CNTT hỗ trợ hiệu quả. (Wegmann et al. 2005).

+ Mục đích chính của Kiến trúc tổng thể là thông báo, hướng dẫn và hạn chế các quyết định của doanh nghiệp đặc biệt là các đầu tư cho công nghệ thông tin (US Chief Information Officer Council) .

+ Kiến trúc tổng thể là sự hiểu biết về tất cả các thành phần khác nhau mà tạo nên doanh nghiệp và cách các thành phần này tương tác với nhau. (Innstitute For Enterprise Architecture Developments).

+ Kiến trúc tổng thể bao gồm tầm nhìn, nguyên tắc, các chuẩn và các quy trình nhằm hướng dẫn việc mua, thiết kế và triển khai công nghệ trong doanh nghiệp (Forrester Research).

Dù được định nghĩa như thế nào thì về cơ bản Kiến trúc tổng thể cũng bao gồm các thành phần chính sau:

1. Các bộ phận cấu thành nên hệ thống đó,

2. Quan hệ giữa các bộ phận với nhau và với môi trường ngoài và

3. Các nguyên tắc chỉ đạo việc thiết kế và phát triển các bộ phận đó (Theo ANSI/IEEE Std 1471-2000)

Hay hiểu đơn giản: "*kiến trúc của một tổ chức là bản thiết kế, quy hoạch tổng thể thống nhất từ đầu đến cuối cho toàn bộ quá trình xây dựng, phát triển của tổ chức, hệ thống đó sau này*", bao gồm toàn bộ các thành tố xây dựng nên cơ cấu tổ chức, hệ thống thông tin, các quy trình nghiệp vụ, các ứng dụng, hệ thống phần cứng và tất cả các thành phần khác cấu thành nên hệ thống đó.

1.1.2 Thành phần của kiến trúc tổng thể:

Kiến trúc tổng thể được nhiều tổ chức nghiên cứu và đưa ra các khái niệm khác nhau nhưng xét về thành phần, hầu hết các kiến trúc tổng thể đều bao gồm những thành phần sau:

Kiến trúc Nghiệp vụ (Bussiness Architecture): bao gồm chiến lược phát triển, hệ thống quản lý, cơ cấu tổ chức và các quy trình nghiệp vụ chủ yếu của một hệ thống.

Kiến trúc Dữ liệu (Data Architecture): cấu trúc các tài sản dữ liệu vật lý (văn bản, sách…) và logic (dữ liệu số hóa) của hệ thống và công cụ để quản lý các tài sản đó.

Kiến trúc Ứng dụng (Application Architecture): các phần mềm ứng dụng phải được sử dụng, tương tác giữa chúng với nhau và quan hệ của chúng với các quy trình nghiệp vụ chủ yếu của hệ thống.

Kiến trúc Công nghệ (Technology Architecture): mô tả hạ tầng phần cứng và phần mềm cần thiết để triển khai ba lớp kiến trúc nói trên, bao

gồm: hạ tầng CNTT, các phần mềm lớp giữa, mạng truyền thông và các chuẩn.

1.1.3 Tầm quan trọng của kiến trúc tổng thể

Khi quy mô tổ chức còn nhỏ, vài trò của kiến trúc tổng thể là chưa rõ ràng, tất cả các nguồn lực cũng như các vấn đề phát sinh đều với số lượng không đáng kể, trực quan và không quá khó để kiểm soát. Tuy nhiên, khi một tổ chức phát triển lới hơn, quy mô hoạt động được mở rộng thì vai trò của kiến trúc tổng thể được thể hiện một cách rõ ràng. Lúc này, số lượng nguồn lực tăng cao, các vấn đề phát sinh trong nghiệp vụ nhiều và dễ dàng gây ra sự quá tải, mất kiểm soát; hệ thống thông tin ngày càng trở nên phức tạp, tốn kém, khó điều hành, khả năng đáp ứng kém. Kiến trúc tổng thể giúp cho tổ chức:

- Đồng bộ hóa CNTT với nghiệp vụ, mang lại sức mạnh tổng hợp từ các nguồn khác nhau, các bộ phận khác nhau của một tổ chức.

- Tránh được việc đầu tư trùng chéo, lặp lại

- Xây dựng được bộ tiêu chuẩn cho toàn bộ hệ thống, nên dễ dàng phối hợp, chia sẻ giữa các dự án cũng như mở rộng hệ thống.

- Xây dựng được quy trình đầu tư rõ ràng, giảm bớt thời gian thực hiện đầu tư…

1.1.4 Quy trình xây dựng kiến trúc tổng thể

Bao gồm 04 bước sau:

Mô tả kiến trúc hiện tại (As-Is): Qua quá trình khảo sát và đánh giá hiện trạng, ta dựng lại kiến trúc hiện tại của hệ thống. Qua đó có thể xác định được vấn đề của hệ thống hiện tại.

Mô tả kiến trúc tương lại (To-Be): Là kiến trúc cần đạt tới của tổ chức dựa trên Khung Kiến trúc, tầm nhìn của tổ chức và sự lựa chọn công nghệ.

Phân tích khác biệt: Bằng việc so sánh kiến trúc hiện tại và kiến trúc tương lai, chúng ta tìm và phân tích các điểm khác biệt giữa chúng. Các điểm khác biệt là căn cứ để chúng ta lập kế hoạch chuyển đổi.

Kế hoạch chuyển đổi (Transition Plan): Từ kiến trúc hiện tại và kiến trúc tương lai, xây dựng các bước bao gồm các giải pháp, và trình tự, độ ưu tiên cần thực hiện để chuyển từ hiện tại sang kiến trúc tương lai.

1.2. Tổng quan về khung kiến trúc tổng thể

1.2.1 Khung kiến trúc tổng thể là gì?

Cũng giống như khái niệm kiễn trúc tổng thể, khái niệm khung kiến trúc cũng được hiểu theo nhiều cách khác nhau: Zachman định nghĩa khung như "một sơ đồ phân loại"; TOGAF lại coi khung là "một phương pháp chi tiết và bộ công cụ hỗ trợ để phát riển một kiến trúc" Roger Sessions coi khung kiến trúc "là một cấu trúc khung xương – skeleton structure", Schekkerman coi đó là bộ phận thiết yếu "có thể phối hợp nhiều khía cạnh tạo nên bản chất cơ bản của doanh nghiệp một cách toàn diện", hay trong định nghĩa của ISO/IEC/IEEE 42010 là "xác lập các quy định chung để tạo lập, giải thích, phân tích và sử dụng các kiến trúc trong một lĩnh vực phần mềm riêng biệt hoặc trong cộng đồng những người có liên quan".

1.2.2 Phân loại

Khung kiến trúc có thể được phân loại thành ba nhóm chính:

a. Khung kiến trúc phát triển bởi chính phủ và độc quyền:

Một trong những nơi áp dụng kiến trúc tổng thể mạnh nhất là các hệ thống chính phủ điện tử. Nước Mỹ có Khung Kiến trúc Liên bang (FEAF) và Kiến trúc Hành chính Liên bang (FEA) áp dụng cho các cơ quan quản lý nhà nước. Chính phủ Đức có Chuẩn và Kiến trúc cho Chính phủ điện tử SAGA. Canada có ban hành tài liệu về kiến trúc hướng dịch vụ Chính phủ GC SOA. Chính phủ Úc và nhiều nước khác cũng có khung kiến trúc chính phủ điện tử của mình. Ngoài ra, Bộ Quốc Phòng các nước cũng bắt đầu xây dựng kiến trúc tổng thể như một xu thế cho hoạt động quân sự đa quốc gia. Bộ Quốc phòng Mỹ lại có kiến trúc riêng DoDAF, Bộ quốc phòng Anh xây dựng khung MODAF, NATO cũng phát triển khung NAF cho riêng mình. Các khung kiến trúc ZACHMAN hay TOGAF cũng được xếp vào nhóm này

b. Khung kiến trúc phát triển bởi các tập đoàn

Đây là những khuôn khổ chủ yếu được phát triển bởi các nhà cung cấp phần mềm. Họ cung cấp kinh nghiệm và các phương pháp thực hành tốt nhất thu được từ các dự án kiến trúc trong quá khứ, dưới hình thức của các khung kiến trúc. Trong danh sách 27 công ty được giải "Annual Enterprise & IT Architecture Excellence Award 2012" có thể thấy những tên tuổi lớn như Credit Suisse, Intel, v.v... Trong các công ty lớn hiện có một chức danh: Nhà kiến trúc doanh nghiệp (Enterprise Architect). Các công ty tin học, tư vấn lớn cũng có các sản phẩm là các khung kiến trúc, phương pháp luận, giải pháp phần mềm, dịch vụ tư vấn xây dựng kiến trúc: IBM, Microsoft, Gartner...

c. Các khung kiến trúc khác

Nhóm này bao gồm nhiều khuôn khổ tập trung vào các ngành công nghiệp đặc biệt, cung cấp thêm các tính năng và chức năng như khung kiến trúc NIH..

1.3. Các phương pháp xây dựng khung kiến trúc tổng thể

1.3.1. Khung kiến trúc ZACHMAN

Khung kiến trúc được đặt theo tên tác giả John Zachman, người đầu tiên phát triển các khái niệm kiến trúc tổng thể trong những năm 1980 tại IBM. Ông xác định sự cần thiết phải có một kế hoạch chi tiết để xác định và kiểm soát sự tích hợp của hệ thống và các thành phần của hệ thống đó. Năm 1987 ông giới thiệu "Khung kiến trúc các hệ thống thông tin" (Framework for Information Systems).

Về bản chất, khung Zachman không phải là một khung kiến trúc như các khái niệm, định nghĩa chúng ta đã tìm hiểu, mà là một dạng lược đồ. Nó không cung cấp phương pháp luận để xây dựng kiến trúc, mà cung cấp một phương pháp luận để mô tả kiến trúc cần xây dựng.

Lược đồ mô tả Zachman là một ma trận sáu hàng sáu cột. Trong đó, sáu cột dựa trên sáu nội dung cơ bản trong trao đổi và giao tiếp: Cái gì (What), Như thế nào (How), Ở đâu (Where), Ai (Who), Khi nào (When) và Tại sao (Why). Việc lồng ghép các câu hỏi này cho phép mô tả các hệ

thống phức tạp như Kiến trúc Tổng thể. Các hàng thể hiện các khung nhìn theo quan điểm của sáu chủ thể trong tổ chức: Người lập kế hoạch (Planner) với mối quan tâm về Phạm vi (Scope), Chủ đầu tư (Owner) với mối quan tâm về Mô hình nghiệp vụ (Bussiness Model), Người thiết kế hệ thống (Designer) với mối quan tâm về Mô hình hệ thống (System Model), Người xây dựng hệ thống (Builder) với mối quan tâm về Mô hình công nghệ (Technology Model), Các nhà thầu phụ (Subcontractor) hoặc các nhà lập trình (Programmer) với mối quan tâm về Thuyết minh chi tiết (Detailed Presentation), và các Người sử dụng (Users) với mối quan tâm về Chức năng (Functioning Enterprise).

	What (Data)	How (Function)	Where (Locations)	Who (People)	When (Time)	Why (Motivation)
Scope {contextual} Planner	List of things important to the business	List of processes that the business performs	List of locations in which the business operatses	List of organizations important to the business	List of events/ cycles important to the business	List of business goals/strategies
Enterprise Model {conceptual} Business Owner	e.g. Semantic Model	e.g. Business Process Model	e.g. Business Logistics System	e.g. Workflow Model	e.g. Master Schedule	e.g. Business Plan
System Model {logical} Designer	e.g. Logical Data Model	e.g. Application Architecture	e.g. Distributed System Architecture	e.g. Human Interface Architecture	e.g. Process Structure	e.g. Business Rule Model
Technology Model {physical} Implementer	e.g. Physical Data Model	e.g. System Design	e.g. Technology Architecture	e.g. Presentation Architecture	e.g. Control Structure	e.g. Rule Design
Detailed Representation {out-of-context} Subcontractor	e.g. Data Definition	e.g. Program	e.g. Network Architecture	e.g. Security Architecture	e.g. Timing Definition	e.g. Rule Definition
Functioning System	e.g. Data	e.g. Function	e.g. Network	e.g. Organization	e.g. Schedule	e.g. Strategy

Hình 1. 1: Lược đồ khung Zachman

1.3.2. Khung kiến trúc TOGAF

Các thành phần chính của TOGAF

- Phương pháp phát triển kiến trúc (Architecture Development Method – ADM).

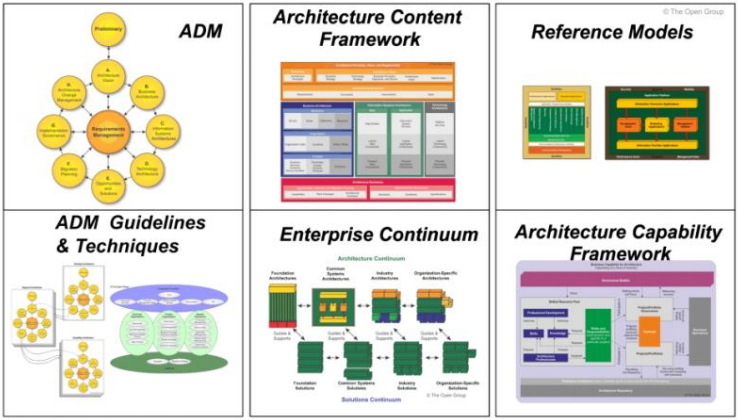
- Các kỹ thuật và các hướng dẫn sử dụng ADM (ADM Guidelines & Techniques).

- Khung nội dung kiến trúc (Architecture Content Framework).

- Kho tư liệu kiến trúc và giải pháp của tổ chức (Enterprise Continuum).

- Các mô hình tham chiếu (Reference Models).

- Khung năng lực kiến trúc (Architecture Capability Framework).



Hình 1. 2: Các thành phần chính của TOGAF

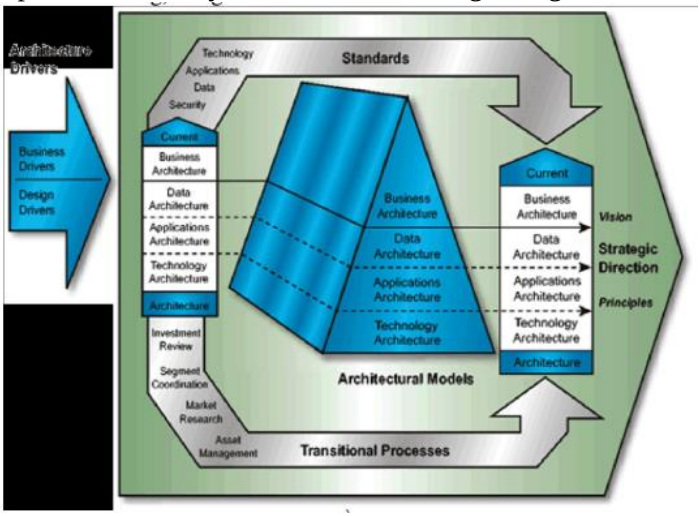
1.3.3. Khung kiến trúc FEAF

FEAF được phát triển bởi Hội đồng CIO nhằm tăng cường khả năng tương tác, sự phát triển của các quy trình chung và chia sẻ dữ liệu giữa các cơ quan thuộc chính phủ liên bang và các tổ chức chính phủ khác. FEAF được coi là một công cụ cho phép Chính phủ liên bang:

– Tổ chức thông tin trong toàn liên bang
– Tăng cường chia sẻ dữ liệu trong các cơ quan của Liên bang
– Giúp cho các tổ chức liên bang phát triển kiến trúc của mình
– Giúp các tổ chức liên bang phát triển nhanh chóng quy trình đầu tư IT của mình
– Phục vụ nhu cầu công chúng và khách hàng tốt hơn, nhanh hơn và giá thành hợp lý hơn.

FEAF được xây dựng dựa trên mô hình kiến trúc của Viện tiêu chuẩn và Công nghệ Quốc Gia (NIST). Mô hình NIST cho phép tổ chức, lập kế hoạch và xây dựng tập các thông tin tích hợp và kiến trúc CNTT. Nó bao gồm 5 lớp xác định riêng biệt nhưng có quan hệ với nhau bao gồm: kiến trúc nghiệp vụ, kiến trúc thông tin, kiến trúc hệ thống thông tin, kiến trúc dữ liệu và kiến trúc hệ thống cung cấp (phần cứng, phần mềm và thông tin liên lạc)

Khi thiết kế khung kiến trúc, hội đồng CIO đã xác định 8 thành phần cơ bản cho phát triển và duy trì kiến trúc liên bang, bao gồm:



Hình 1.3: Các thành phần cơ bản của khung FEAF

1. Trình điều khiển kiến trúc: có 2 nhân tố gây ra thay đổi cho kiến trúc đó là nghiệp vụ và thiết kế. Điều khiển nghiệp vụ có thể là sáng kiến điều hành mới, các luật mới được sửa đổi hoặc các yêu cầu thay đổi của thị trường... Điều khiển thiết kế bao gồm phần mềm hoặc phần cứng mới và sự kết hợp của chúng với các hướng tiếp cận triển khai mới...

2. Hướng chiến lược: đảm bảo các thay đổi phù hợp với kiến trúc và bao gồm tầm nhìn, nguyên tắc, mục đích và mục tiêu.

3. Kiến trúc hiện tại: Định nghĩa kiến trúc hiện tại và bao gồm 2 phần: nghiệp vụ hiện tại và kiến trúc thiết kế (bao gồm dữ liệu, ứng dụng và công nghệ).

4. Kiến trúc tương lai: Xác định kiến trúc tương lai, bao gồm nghiệp vụ và kiến trúc thiết kế trong tương lai, biểu diễn khả năng và công nghệ đạt được từ việc hỗ trợ thay đổi của nhu cầu kinh doanh

5. Quá trình chuyển đổi: hỗ trợ chuyển đổi từ hiện tại sang tương lai. Các tiến trình chính trong kiến trúc liên bang là các kế hoạch đầu tư CNTT, kế hoạch chuyển đổi quản lý cấu hình và quản trị thay đổi...

6. Phân đoạn kiến trúc:

7. Các mô hình kiến trúc: xác định mô hình thiết kế và nghiệp vụ

8. Các chuẩn: tham chiếu tới tất cả các chuẩn, hướng dẫn...

1.3.4 Khung kiến trúc GARTNER

Không giống như khung ZACHMAN là lược đồ mô tả kiến trúc, TOGAF là phương pháp xây dựng, FEAF là phương pháp tổng hợp thì GARTNER là một phương pháp thiên về thực hành. GARTNER là một sản phẩm của tập đoàn Gartner - tập đoàn tư vấn và cung cấp công nghệ thông tin hàng đầu thế giới. Khung kiến trúc GARTNER cung cấp một mô hình thẩm định nghiệp vụ, thông tin, yêu cầu công nghệ và các mối quan tâm trong sự kết hợp của cả hai kiến trúc doanh nghiệp và kinh doanh. Trong khi nó không có nhiều tài liệu tham khảo hướng dẫn như một số khung kiến trúc khác, nhưng nó được hỗ trợ bởi hệ thống nhân viên phát triển rộng khắp của tập đoàn GARTNER.

Khung GARTNER cung cấp 4 quan điểm chính:

- Enterprise business architecture (EBA): kiến trúc kinh doanh

- Enterprise information architecture (EIA): kiến trúc thông tin

- Enterprise technology architecture (ETA): kiến trúc kỹ thuật

- Enterprise solution architecture (ETA): kiến trúc giải pháp

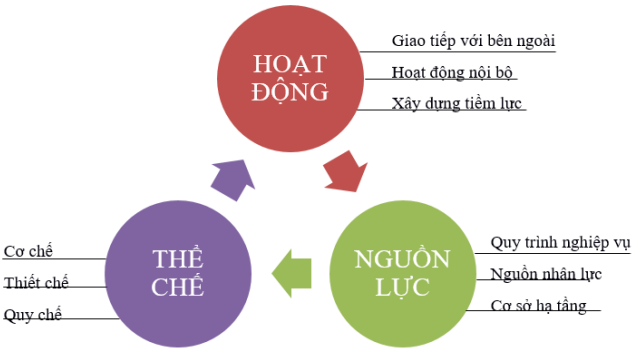
Trong đó, kiến trúc giải pháp được xây dựng bởi sự kết hợp và đối chiếu của 3 kiến trúc trên

1.3.5. Khung kiến trúc ITI-GAF

Bắt đầu từ năm 2009, Viện Công nghệ thông tin – Đại học Quốc gia Hà Nội đã phát triển ITI-GAF (Information Technology Institute Government Architecture Framework, ITI-GAF), một khung kiến trúc Chính phủ nhỏ và đơn giản, dựa trên EGIF được phát triển trước đây bởi một nhóm của UNDP và các tính năng chính của TOGAF.

Mô hình doanh nghiệp của ITI-GAF đơn giản hoá các giai đoạn tinh vi trên, hướng dẫn phân tích hệ thống một cơ quan, tổ chức theo ba cách nhìn, quan điểm khác nhau: quan điểm nguồn lực, quan điểm thể chế và quan điểm hoạt động. Mỗi quan điểm đều có các thành phần quan hệ ràng buộc hữu cơ với nhau, để đảm bảo tính bền vững.

Theo định nghĩa, doanh nghiệp là một tổ chức thực hiện các mục tiêu bằng cách cung cấp hoạt động, sử dụng các nguồn lực và thể chế.



Hình 1.4: Mô hình ITI-GAF

Quan điểm về "hoạt động": Các doanh nghiệp chung có thể có ba loại hoạt động khác nhau, có thể dưới các hình thức dịch vụ trong các doanh nghiệp tiên tiến. Điều này thay thế các mô hình kinh doanh của doanh nghiệp bằng một quan điểm chung mà sẽ dễ dàng hơn để phân tích.

– Các hoạt động bên ngoài: Hoạt động kinh doanh liên quan, các dịch vụ tương tác với khách hàng và đối tác kinh doanh.

– Các hoạt động nội bộ: Giúp giữ cho sự hợp tác và hành động bình thường trong doanh nghiệp và chủ yếu giữa công nhân của các doanh nghiệp như tuyển dụng, đề bạt, khen thưởng, kỷ luật.

– Xây dựng tiềm lực: Các hoạt động và dịch vụ cải thiện chất lượng của các nguồn lực hiện có.

Quan điểm về "thể chế": Khác với quan điểm truyền thống, một hệ thống tổ chức sinh ra và tìm cách hoạt động để phục vụ cho sự tồn tại của chính nó, quan điểm hiện đại cho rằng mục tiêu tối hậu là tạo ra sản phẩm cho xã hội theo đúng chức năng của hệ thống. Mọi hoạt động, cơ cấu hoặc quy định không phục vụ cho việc tạo ra, nâng cao năng suất và chất lượng sản phẩm, đều phải thay đổi. Đó chính là bản chất của cải cách hành chính.Thể chế là những yếu tố chính của một doanh nghiệp. Nó bao gồm:

– *Cơ chế:* Cơ chế bao gồm các hành động trên cơ sở thường xuyên, bao gồm các hành động dựa trên xử lý thông tin về hướng dẫn cơ sở thực tiễn. Đôi khi không được xác định rõ ràng trong các quy định, bởi vì các thủ tục của hành động đã thay đổi đáng kể. Tuy nhiên, đôi khi một cơ chế phải trở thành một quy định nếu nó trở nên ổn định và không nên bị vi phạm.

– *Tổ chức:* Bao gồm các định nghĩa vai trò và mục tiêu của tất cả các vị trí và đơn vị trong doanh nghiệp và các mối quan hệ giữa chúng phải được xác định và thiết lập trong phần này. Vai trò được xác định kém với các mục tiêu mơ hồ cần được củng cố bằng các biện pháp khác nhau hoặc cắt bỏ hoàn toàn bằng cách đánh giá thường xuyên với các chỉ số định lượng.

– *Chế tài:* Tất cả các quy tắc phải được xác định bằng văn bản trong các hình thức khác nhau: theo pháp luật, chính sách, quyết định, hướng dẫn, ...

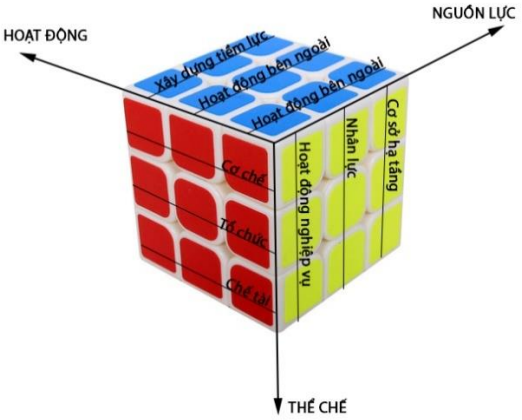
Quan điểm về "Nguồn lực": Các nguồn lực của doanh nghiệp phải được cân đối giữa các thành phần sau:

– *Hoạt động nghiệp vụ:* Đây là thế mạnh của doanh nghiệp và phải được thích nghi với sự thay đổi nhanh chóng của môi trường kinh doanh bằng cách tái cấu trúc liên tục, nhưng đôi khi không được hỗ trợ bởi các nguồn lực khác, vì không có cơ chế để thoát khỏi người không đủ năng lực cũng như các quy định đã lỗi thời.

– *Nhân lực:* Giải quyết vấn đề này là quan trọng nhất và khó khăn nhất. Mặc dù mọi người nói rất nhiều về nó, nhưng thường bị lãng quên trong các dự án công nghệ thông tin. Như kết quả, trang thiết bị cao cấp mới hoặc quá trình kinh doanh không thể được vận hành bởi nguồn nhân lực hiện tại.

– *Cơ sở hạ tầng:* Sai lầm thường gặp nhất là coi nó phụ thuộc vào các nguồn lực tài chính sẵn có. Trong thực tế, nó được xác định bởi các doanh nghiệp và nguồn nhân lực.

Từ những phân tích dựa trên các quan điểm trên, các yếu tố doanh nghiệp có thể được sắp xếp thành 27 khối của một mô hình Rubic. Vì tất cả các khối liên quan với nhau, một sự thay đổi nhỏ trong một khối sẽ ảnh hưởng đến những cái khác. Sự phụ thuộc này phản ánh khả năng tương tác, mà được giữ bởi các tiêu chuẩn.



Hình 1.5: Mô hình 3x3x3

CHƯƠNG II: CƠ SỞ LÝ LUẬN VỀ AN TOÀN THÔNG TIN, HỆ THỐNG QUẢN LÝ AN TOÀN THÔNG TIN

2.1. An toàn thông tin

2.1.1. Khái niệm

* Khái niệm về thông tin

Thông tin được hiểu là kết quả của hoạt động trí óc mang tính chất vô hình. Thông tin tồn tại dưới nhiều hình thức khác nhau như được in ra, được viết ra, được lưu trữ trong các thiết bị điện tử, được truyền tải thông qua các phương tiện thông tin, truyền thông hay được chuyển qua các thiết bị đa phương tiện…Trong mọi tình huống thì thông tin đều có tính chất là tài sản có giá trị (hữu hình hoặc vô hình). Theo định nghĩa của ISO 27000, thông tin là một loại tài sản, cũng như các loại tài sản quan trọng khác của một doanh nghiệp, có giá trị cho một tổ chức và do đó, cần có nhu cầu để bảo vệ thích hợp.

An toàn thông tin là bảo vệ thông tin trước nguy cơ mất an toàn nhằm đảm bảo tính liên tục trong hoạt động kinh doanh của doanh nghiệp; giảm thiểu các thiệt hại do sự hư hỏng hay cố ý phá hoại; gia tăng tới mức tối đa các cơ hội kinh doanh và đầu tư phát triển.

Nhưng cho dù thông tin tồn tại dưới dạng nào đi chăng nữa, thông tin được đưa ra với 2 mục đích chính là chia sẻ và lưu trữ, nó luôn luôn cần sự bảo vệ nhằm đảm bảo sự an toàn thích hợp.

* Khái niệm về an toàn thông tin

An toàn thông tin mạng" là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm đảm bảo tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin. (Theo Luật an toàn thông tin mạng của Chính phủ đã ban hành năm 2015)

An toàn thông tin là một khái niệm bao hàm nhiều vấn đề, trong đó có:

- An toàn thông tin cho các tài sản vật lý: máy chủ, máy trạm; thiết bị an ninh mạng, đường truyền internet….;

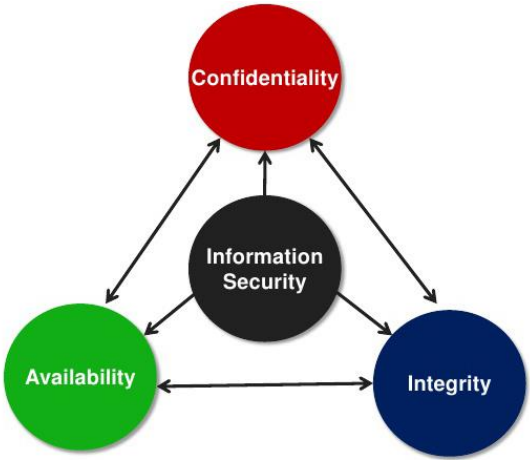
- An toàn thông tin cho các tài sản phần mềm: cơ sở dữ liệu, hệ điều hành, các phần mềm nghiệp vụ…;

- An toàn thông tin cho tài sản thông tin: bí mật kinh doanh; chính sách của một tổ chức hay chiến lược phát triển của đơn vị…);

- An toàn thông tin cho tài sản dịch vụ: các dịch vụ tổ chức cung cấp ra bên ngoài cũng như các dịch vụ mà bên ngoài cung cấp cho tổ chức của mình….

- An toàn thông tin cho tải sản con người: Lãnh đạo và nhân viên trong tổ chức…..

Có nhiều cách tiếp cận về an toàn thông tin, trong đó mô hình tam giác bảo mật CIA là cách tiếp cận dựa trên các thuộc tính của an toàn thông tin, bao gồm 03 thuộc tính: Confidentiality – tính bí mật hay tính bảo mật, Integrity – tính toàn vẹn hay tính nguyên vẹn và Availability – tính sẵn sàng hay tính khả dụng. Hình 2.1 là một thể hiện về các thuộc tính và mối quan hệ của các thuộc tính trong an toàn thông tin.



Hình 2.2: Mô hình tam giác an toàn thông tin CIA

Tính bảo mật hay tính bí mật (Confidentiality) của thông tin thể hiện việc thông tin được bảo vệ khỏi việc bị tiết lộ, sử dụng bởi các cá nhân hoặc hệ thống trái phép. Tính bảo mật của thông tin bảo đảm rằng chỉ có những người dùng đã được phân quyền thì mới có thể truy cập, sử dụng thông tin. Tính bí mật của thông tin có thể đạt được bằng cách giới hạn truy cập về cả mặt vật lý, ví dụ như tiếp cận trực tiếp tới thiết bị lưu trữ thông tin đó hoặc logic, ví dụ như truy cập thông tin đó từ xa qua môi trường mạng.

Tính toàn vẹn hay tính nguyên vẹn (Integrity) của thông tin là thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi. Tính toàn vẹn thông tin được coi là nền tảng của hệ thống thông tin, bởi thông tin sẽ không còn giá trị sử dụng nếu người dùng không thể xác minh tính toàn vẹn của nó. Nhiều mã độc hại (virus, worm…) máy tính được thiết kế với mục đích làm hỏng dữ liệu.

Tính sẵn sàng (Availability) tính sẵn sàng cho phép người dùng hợp pháp - người dùng hay hệ thống máy tính - có thể truy cập thông tin mà không bị can thiệp hay cản trở. Một ví dụ về tính sẵn sàng của thông tin đó chính là việc một website phải hoạt động một cách liên tục để đảm bảo bất cứ người dùng hợp pháp nào có thể truy nhập và tìm kiếm thông tin trên website đó.

Ngày nay, mô hình tam giác bảo mật CIA còn được bổ sung thêm các yếu tố khác là Non-Repudiation (Tính không chối bỏ).

2.1.2. Các yếu tố ảnh hưởng đến an toàn thông tin

Các yếu tố ảnh hưởng đến an toàn thông tin gồm các yếu tố sau:

- Con người (People);

- Quy trình (Procedure);

- Công nghệ (Technology);

** Con người (People)*

Con người (People) mặc dù luôn bị bỏ qua nhưng con người lại là mối đe dọa lớn đối với an toàn thông tin. Theo thông tin của "Tạp chí an toàn thông tin" số liệu khảo sát năm 2015, tỷ lệ các tổ chức, doanh nghiệp có lãnh đạo, hoặc cán bộ chuyên trách/bán chuyên trách về ATTT là 34% (giảm so với 73% của năm 2014). Điều này cho thấy tổ chức, bộ máy và nhân sự cho ATTT ở các doanh nghiệp vừa và nhỏ còn rất nhiều khoảng trống và chưa được quan tâm chú trọng. Chỉ có 25,6% các đơn vị được khảo sát cho biết, có kế hoạch đào tạo các kỹ năng cơ bản về ATTT cho nhân lực của đơn vị mình, trong đó đa phần là các kế hoạch đào tạo dài hạn.

Về vấn đề đào tạo, tuyên truyền nâng cao nhận thức về ATTT cho cán bộ, nhân viên, các tổ chức doanh nghiệp cũng chưa chú trọng nhiều. Khoảng 30,8% các đơn vị được khảo sát cho biết có đào tạo, tuyên truyền, trong đó chủ yếu là hình thức đào tạo tập trung (35,5%), đào tạo từ xa (qua website - 19,9%), tập huấn thông qua giải quyết sự cố ATTT (16,6%).

Cũng theo báo cáo khảo sát, trong các nguy cơ tiềm ẩn có khả năng ảnh hưởng đến ATTT của các tổ chức doanh nghiệp, thì chính nhân viên đang làm việc tại đơn vị là "nguy cơ" lớn nhất, chiếm 55,4%; xếp thứ hai là các loại tin tặc, tội phạm máy tính; thứ ba là nhân viên đã nghỉ việc. Mối đe dọa đến từ đối tượng "Đối thủ cạnh tranh" chỉ xếp thứ tư.

Nguy cơ mất ATTT do phía con người có thể xuất phát từ các hành vi vô ý (lỗi nhập liệu,..) hay cố tình (thực hiện các hành vi tấn công mạng, sử dụng công cụ tấn công là các phần mềm có hại, truy cập trái phép thông tin mật,…). Các hành vi đó bao gồm:

- Kẻ tấn công thực hiện các hành vi xâm nhập hệ thống, truy cập hệ thống trái phép, sử dụng phương thức tấn công lừa đảo bằng các kỹ nghệ xã hội (Social Engineering).

- Tội phạm máy tính sử dụng các hình thức giả mạo thông tin, mua chuộc để lấy cắp thông tin nhằm mục đích phá hủy, sửa đổi dữ liệu trái phép, phổ biến các thông tin trái phép.

- Các tổ chức khủng bố thâm nhập, tấn công hệ thống thông tin nhằm phá hoại, gây ra các cuộc chiến tranh thông tin.

- Các tổ chức tình báo sử dụng các biện pháp ăn cắp thông tin, thâm nhập hệ thống nhằm ăn cắp các thông tin giá trị của đối thủ cạnh tranh, của quốc gia khác phục vụ mục đích kinh doanh, chính trị.

- Các hành vi do chính các nhân viên bên trong tổ chức thực hiện như lạm dụng quyền truy cập, ăn trộm các thông tin kinh doanh, bán thông tin bí mật, sửa đổi các thông tin,.. Các nguy cơ này là do nhân viên cẩu thả hoặc chưa được đào tạo huấn luyện về ATTT, do nhân viên bất mãn hoặc cố tình muốn ăn cắp thông tin, phá hoại hoạt động sản xuất, kinh doanh, điều hành của tổ chức, hoặc do chính cơ chế quản lý, bảo vệ của tổ chức.

Với rủi ro lớn nhất là từ con người nên tổ chức phải có những chính sách, chế tài, chương trình đào tạo và nâng cao nhận thức công nghệ hợp lý để tránh việc con người vô tình làm tổn hại hoặc thất thoát thông tin . Kỹ nghệ xã hội dựa trên các sai sót do lỗi hoặc tâm lý người dùng, nó có thể được sử dụng để lợi dụng các thao tác của người dùng để chiếm quyền truy cập thông tin bất hợp pháp.

** Quy trình (Procedure)*

Là một yếu tố có thể gây ảnh hưởng đến an toàn hệ thống mà thường hay bị tổ chức chưa được quan tâm đúng mức. Quy trình ở đây được hiểu là các văn bản có tính định hướng của tổ chức và các văn bản cụ thể hướng dẫn thực thi một tập các nhiệm vụ được thiết kế để xác định, giới hạn, quản lý và kiểm soát các nguy cơ đối với dữ liệu, hệ thống để đảm bảo tính bí mật, tính toàn vẹn và tính sẵn sàng của hoạt động hệ thống. Khi kẻ tấn công hiểu được quy trình của một tổ chức thì hắn có thể lợi dụng để tìm ra các kẽ hở gây ảnh hưởng tính toàn vẹn của thông tin. Ví dụ: một nhà tư vấn ngân hàng biết được quy trình chuyển tiền qua hệ thống máy tính của ngân hàng, người này lợi dụng nó để ra lệnh chuyển hàng triệu đô la vào tài khoản của mình qua các điểm yếu an ninh (thiếu xác thực) trong quy trình này. Hầu hết các tổ chức đều phổ biến các quy trình để nhân viên có thể truy cập hợp pháp vào hệ thống thông tin nhằm thực hiện các nhiệm vụ của mình.

Theo thông tin của "Tạp chí an toàn thông tin" số liệu khảo sát năm 2015, số các tổ chức doanh nghiệp có phê duyệt và ban hành chính sách về ATTT cũng giảm còn 23,7% (so với 30% năm 2014 và 25% năm 2013). Số lượng các tổ chức doanh nghiệp ban hành quy định về an toàn thông tin, ATTT cá nhân cũng chiếm tỷ lệ khá khiêm tốn, là 22,7% (trong đó, số tổ chức doanh nghiệp tuân theo các chuẩn ATTT quốc tế như 2700x hay PCI… chiếm chưa đến 13%).

Như vậy việc xây dựng các chính sách, quy định, quy trình và tuân thủ đúng văn bản an toàn thông tin đóng vai trò quan trọng trong việc bảo vệ thông tin, do vậy những kiến thức, hiểu biết về văn bản cần phải được phổ biến rộng rãi cho tất cả các thành viên trong tổ chức.

** Công nghệ (Technology)*

Là việc sử dụng các giải pháp, biện pháp kỹ thuật (theo sự phát triển của khoa học công nghệ nói chung và CNTT nói riêng) nhằm đảm bảo ATTT. Ngày nay, các giải pháp kỹ thuật đảm bảo ATTT thường bao gồm: hệ thống tường lửa (Firewall), hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS), phần mềm phòng chống virus, giải pháp mã hóa (Encryption), chữ kí số (CA),..

Theo thông tin của "Tạp chí an toàn thông tin" số liệu khảo sát năm 2015, về sử dụng biện pháp kỹ thuật để đảm bảo ATTT: Con số ấn tượng nhất của đợt khảo sát năm nay là việc các doanh nghiệp tăng cường sử dụng hệ thống kiểm soát truy cập khi đi vào/ra các khu vực quan trọng bằng thẻ từ, bảo vệ… là 15% so với 7,3% năm 2014. Ngoài ra, việc sử dụng chữ ký số trong giao dịch điện tử lên tới 43,1%. Các con số này chứng tỏ, các biện pháp bảo vệ đơn giản, dễ dùng sẽ được các tổ chức ưu tiên áp dụng.

Mặc dù vậy, các tổ chức doanh nghiệp vẫn chưa quan tâm đúng mức tới việc đảm bảo an toàn dữ liệu. Việc mã hóa và sao lưu dữ liệu được thực hiện ở mức thấp, chỉ có 12,3% tổ chức được hỏi có sử dụng mã hóa

Ba yếu tố chính là Quy trình, Con người và Công nghệ có mối quan hệ chặt chẽ với nhau, hỗ trợ và bổ sung cho nhau. Một hệ thống muốn đảm bảo ATTT thành công phải coi trọng cả ba yếu tố nói trên.

2.2. Thực trạng an toàn thông tin tại Việt Nam

2.2.1. Thực trạng an toàn thông tin tại các tổ chức doanh nghiệp

Trong năm 2015, các cuộc tấn công mạng có quy mô và mức độ lớn gia tăng dẫn đến gây mất mát dữ liệu, thiệt hại về kinh tế. Theo thống kê của VNCERT, xu hướng tấn công lừa đảo, mã độc, thay đổi giao diện trở nên phổ biến. Cụ thể, đã có 4.484 sự cố tấn công lừa đảo, 6.122 sự cố thay đổi giao diện, 14.115 sự cố về mã độc và 3.257 sự cố khác được ghi nhận trong 11 tháng đầu năm. Bên cạnh đó, trong các trang web/cổng thông tin điện tử của Cơ quan nhà nước đã có 9 website bị tấn công thay đổi giao diện với 144 đường dẫn bị thay đổi; 106 website bị cài mã độc với 227 đường dẫn phát tán mã độc, 1 website bị tấn công cài mã lừa đảo. Các hình thức lừa đảo trực tuyến gia tăng, bao gồm lừa đảo chiếm đoạt thẻ cào điện thoại di động và tài khoản mạng xã hội, lấy cắp thông tin cá nhân. Các hình thức quảng cáo rác, tin nhắn rác vẫn chưa được kiểm soát. Đặc biệt, tấn công có chủ đích vào các cơ quan nhà nước chiếm 2,5% Quý I và gia tăng 7,1% trong Quý II.

Theo đánh giá của các hãng bảo mật trên thế giới, Việt Nam tiếp tục nằm trong nhóm những quốc gia kém bảo mật trên thế giới, nằm trong số các nước có số người dùng di động bị mã độc tấn công nhiều nhất thế giới. Gần 50% người dùng có nguy cơ nhiễm mã độc khi sử dụng Internet trên máy tính, số lượng thiết bị lây nhiễm virus qua các hoạt đông trực tuyến chiếm khoảng 65% tổng số người dùng. Đứng thứ 4 về tỉ lệ về tỷ lệ lây nhiễm mã độc với 30% thiết bị bị lây nhiễm, đứng thứ 3 thế giới và thứ 2 châu Á về mức độ phát tán thư rác, đáng chú ý, trong thời gian gần đây, mã độc mã hóa dữ liệu (Ramsomeware) đã lây lam rộng rãi qua một số dịch vụ.

2.3. Quản lý an toàn thông tin theo tiêu chuẩn TCVN ISO/IEC 27002:2011

2.3.1. Tổng quan tiêu chuẩn TCVN ISO/IEC 27002:2011

TCVN ISO/IEC 27002:2011 là tiêu chuẩn Việt Nam được xây dựng dựa theo phương pháp chấp thuận nguyên vẹn tiêu chuẩn quốc tế

ISO/IEC 27002:2005. Tiêu chuẩn này thiết lập các hướng dẫn và nguyên tắc chung cho hoạt động khởi tạo, triển khai, duy trì và cải tiến công tác quản lý an toàn thông tin trong một tổ chức. Mục tiêu của tiêu chuẩn này là đưa ra hướng dẫn chung nhằm đạt được các mục đích chung đã được chấp nhận trong quản lý an toàn thông tin.

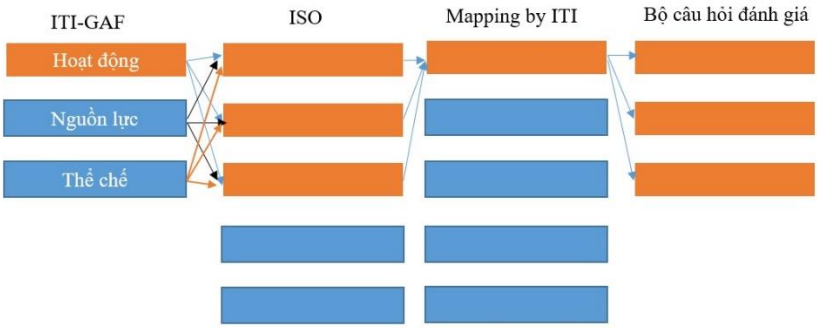
Các mục tiêu và biện pháp quản lý của tiêu chuẩn này được xây dựng nhằm đáp ứng các yêu cầu đã được xác định bởi quá trình đánh giá rủi ro. Tiêu chuẩn này có thể đóng vai trò như một hướng dẫn thực hành trong việc xây dựng các tiêu chuẩn an toàn thông tin cho tổ chức và các quy tắc thực hành quản lý an toàn thông tin hiệu quả và giúp tạo dựng sự tin cậy trong các hoạt động liên tổ chức.

Tiêu chuẩn này gồm 11 điều về kiểm soát an toàn thông tin với tất cả 39 danh mục an toàn chính và một điều giới thiệu về đánh giá và xử lý rủi ro. Mỗi điều gồm một số danh mục an toàn chính: Chính sách an toàn (1), Tổ chức thực hiện an toàn thông tin (2), Quản lý tài sản (2), An toàn nguồn nhân lực (3), An toàn vật lý và môi trường (2), Quản lý khai thác và truyền thông (10), Kiểm soát truy cập (7), Thu thập, phát triển và duy trì hệ thống thông tin (6), Quản lý sự cố an toàn thông tin (2), Quản lý tính liên tục về nghiệp vụ (1), Sự tuân thủ (3).

CHƯƠNG III: XÂY DỰNG KHUNG KIẾN TRÚC BẢO ĐẢM AN TOÀN THÔNG TIN CHO CÁC TỔ CHỨC DOANH NGHIỆP TẠI VIỆT NAM

3.1. Đề xuất khung kiến trúc bảo đảm an toàn thông tin

Khung kiến trúc bảo đảm an toàn thông tin được xây dựng dựa trên mô hình ITI-GAF là một mô hình đơn giản, dễ áp dụng có thể thể thích hợp cho mọi cấp độ của tổ chức khác nhau bằng việc phân tích, xem xét các khía cạnh của hệ thống bảo đảm an toàn thông tin của tổ chức, doanh nghiệp dưới 03 góc độ về nguồn lực, thể chế và hoạt động. Các thành phần của nguồn lực, thể thế, hoạt động được xem xét và kết hợp với các tiêu chuẩn về bảo đảm an ninh, an toàn hệ thống thông tin để cho ra một mô hình đánh giá – là xương sống, điểm chính của khung kiến trúc bảo đảm an toàn thông tin. Do các mô hình đánh giá dựa trên ITI-GAF nên cho phép các tổ chức để đánh giá mức độ an ninh của tổ chức một cách nhanh chóng, chính xác và toàn diện. Thông qua đánh giá, mỗi tổ chức sẽ xác định các điểm mạnh, điểm yếu của an toàn thông tin trong hệ thống của mình, xác định nhu cầu đầu tư trọng điểm, sau đó xây dựng một kế hoạch hành động để phát triển tổ chức và tăng cường bảo đảm an toàn thông tin cho tổ chức. Đây là một trong những bước quan trọng nhất để bảo đảm an toàn thông tin cho các tổ chức doanh nghiệp.



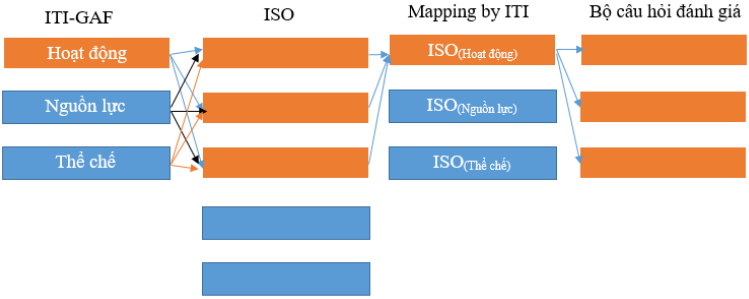
Hình 3.1: Mô hình an toàn thông tin cho các tổ chức, doanh nghiệp

Hình 3.1 mô tả các bước để xây dựng mô hình đánh giá an toàn thông tin của tổ chức doanh nghiệp. Các quan điểm về hoạt động, nguồn lực và thể chế được của tổ chức được ánh xạ đến các điểm, yêu cầu của các tiêu chuẩn về an ninh, an toàn thông tin và phân cụm các tiêu chuẩn đó thành các cụm là các thành phần của các quan điểm về hoạt động, nguồn lực và thể chế. Các tiêu chuẩn về an ninh, an toàn thông tin ở đây có thể là các tiêu các tiêu chuẩn quốc tế, hay Việt Nam về an ninh, an toàn thông tin như các bộ tiêu chuẩn ISO/IEC 27001, 27002, COBIT, TCVN… Sau quá trình phân cụm các quan điểm về hoạt động, nguồn lực, thể chế của tổ chức ứng với các điểm trong các tiêu chuẩn sẽ cho chúng ta một bảng liên kết các quản điểm đó với các tiêu chuẩn về an ninh, an toàn thông tin. Và sau cùng, dựa vào bảng này chúng ta sẽ xây dựng ra và bộ câu hỏi, tiêu chuẩn đánh giá theo cách tiếp cận của ITI-GAF.

Khung kiến trúc bảo đảm an toàn thông tin dựa trên mô hình ITI-GAF là đơn giản và phù hợp với mọi cấp độ của tổ chức, doanh nghiệp từ những tổ chức, doanh nghiệp với quy mô nhỏ đến tổ chức, doanh nghiệp có quy mô lớn. Đối với các tổ chức doanh nghiệp nhỏ, chúng ta có thể chỉ cần xem xét, đánh giá, xây dựng các tiêu chuẩn về an toàn thông tin tương ứng 3 góc độ là hoạt động, nguồn lực, thể chế. Đối với doanh nghiệp trung bình, chúng ta xem xét xem xét, đánh giá, xây dựng các tiêu chuẩn về an toàn thông tin tương ứng 9 góc độ là hoạt động giao tiếp với bên ngoài, hoạt động nội bộ, hoạt động xây dựng tiềm lực, cơ chế, thể chế, quy chế, quy trình nghiệp vụ, nguồn nhân lực và cơ sở hạ tầng. Đối với doanh nghiệp lớn chúng ta xem xét xem xét, đánh giá, xây dựng các tiêu chuẩn về an toàn thông tin tương ứng 27 góc độ đó là sự kết hợp của 3x3x3 thành phần của hoạt động, thể chế và nguồn lực.

3.1.1. Mô hình đơn giản

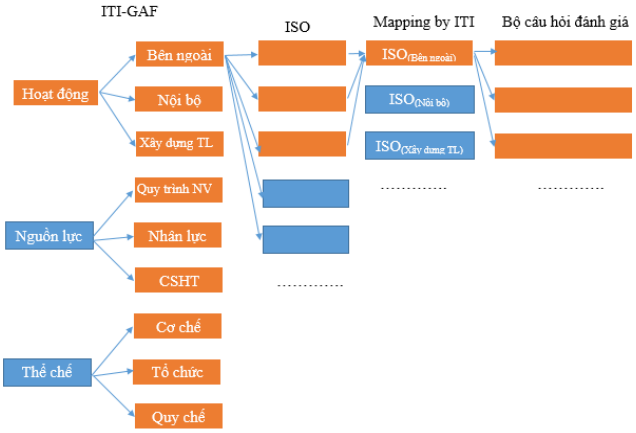
Là mô hình được áp dụng chủ yếu cho các doanh nghiệp nhỏ, đó là việc xem xét, đánh giá, xây dựng các tiêu chuẩn về an toàn thông tin tương ứng 03 góc độ: Hoạt động, thể chế và nguồn lực.



Hình 3.2: Mô hình an toàn thông tin cho các tổ chức, doanh nghiệp nhỏ

3.1.2. Mô hình trung gian

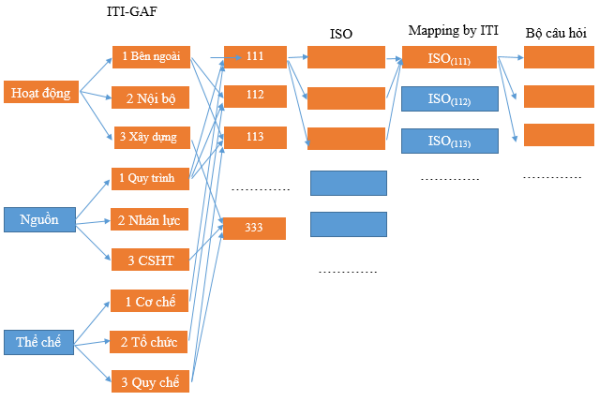
Được áp dụng chủ yếu cho các doanh nghiệp trung bình, đó là việc xem xét xem xét, đánh giá, xây dựng các tiêu chuẩn về an toàn thông tin tương ứng 9 góc độ là hoạt động giao tiếp với bên ngoài, hoạt động nội bộ, hoạt động xây dựng tiềm lực, cơ chế, thể chế, quy chế, quy trình nghiệp vụ, nguồn nhân lực và cơ sở hạ tầng.



Hình 3.3: Mô hình an toàn thông tin cho các tổ chức, doanh nghiệp trung bình

3.1.3. Mô hình nâng cao

Được áp dụng đối với doanh nghiệp lớn chúng ta xem xét xem xét, đánh giá, xây dựng các tiêu chuẩn về an toàn thông tin tương ứng 27 góc độ đó là sự kết hợp của 3x3x3 thành phần của hoạt động, thể chế và nguồn lực.



Hình 3.4: Mô hình an toàn thông tin cho các tổ chức, doanh nghiệp lớn

3.2. Khung kiến trúc bảo đảm an toàn thông tin dựa trên tiêu chuẩn Việt Nam TCVN ISO/IEC 27002:2011

Khung kiến trúc bảo đảm an toàn thông tin được xây dựng trên mô hình đánh giá bằng cách kết hợp mô hình ITI-GAF với các tiêu chuẩn về an ninh, an toàn thông tin, phân cụm các tiêu chuẩn thành các nhóm theo các tiếp cận của mô hình ITI-GAF để đưa ra các bộ câu hỏi tương ứng. Quá trình xây dựng Khung kiến trúc bảo đảm an toàn thông tin dựa trên tiêu chuẩn Việt Nam TCVN ISO/IEC 27002:2011 trải qua 02 bước chính đó là

3.2.1. Phân cụm tiêu chuẩn TCVN ISO/IEC 27002:2011 theo mô hình ITI-GAF

TCVN ISO/IEC 27002:2011 về *Công nghệ thông tin - các kỹ thuật An toàn - Quy tắc thực hành quản lý an toàn thông tin* gồm có 11 điều

về kiểm soát an toàn thông tin với tất cả 39 danh mục an toàn chính và 134 tiêu chuẩn. Quá trình phân cụm tiêu chuẩn TCVN ISO/IEC 27002:2011 theo mô hình ITI-GAF được tiến hành bằng việc xem xét 134 tiêu chuẩn của TCVN, gán cho mỗi tiêu chuẩn một trọng số ITI để phân chia tiêu chuẩn TCVN thành 27 nhóm

3.3. Đánh giá kết quả đạt được và hướng phát triển trong tương lai

3.3.1. Kết quả đạt được

- Đề xuất được khung kiến trúc bảo đảm an toàn thông tin cho các tổ chức doanh nghiệp dựa trên cách tiếp cận của khung kiến trúc ITI-GAF kết hợp với các tiêu chuẩn về bảo đảm an ninh, an toàn thông tin. Đây là khung kiến trúc có tính linh hoạt cao, để sử dụng có thể áp dụng cho mọi cấp độ của tổ chức, doanh nghiệp, là cơ sở xây dựng khung kiến trúc đảm bảo an ninh không giang mạng cho các quốc gia đang phát triển.

- Phân cụm được tiêu chuẩn TCVN ISO/IEC 27002:2011 ánh xạ sang mô hình ITI-GAF, đây là công việc tốn rất nhiều công sức bằng việc nghiên cứu, phân tích 134 tiêu chí của TCVN để đưa vào mô hình ITI-GAF.

- Bước đầu đưa ra bộ câu hỏi với hơn 100 câu hỏi tích hợp vào công cụ đánh giá làm cở sở để khảo sát, đánh giá thực trạng công tác bảo đảm an toàn thông tin cho các tổ chức, doanh nghiệp cũng như là căn cứ để triển khai các giải pháp khác nhằm nâng cao năng lực bảo đảm an toàn thông tin cho các tổ chức, doanh nghiệp.

3.3.2. Hướng phát triển trong tương lai

Trong tương khung kiến trúc bảo đảm an toàn thông tin cho tổ chức, doanh nghiệp cần phải kết hợp với nhiều tiêu chuẩn an ninh, an toàn thông tin khác bên cạnh TCVN ISO/IEC 27002:2011 như tiêu chuẩn ISO 272001, các Tiêu chuẩn của COBIT, NIST... nhằm đưa ra một khung kiến trúc toàn diện hơn.

KẾT LUẬN

Ngày nay, nguy cơ mất an ninh, an toàn thông tin ngày càng gia tăng mạnh mẽ, phức tạp và ảnh hưởng nhiều đến hoạt động của các tổ chức, doanh nghiệp. Ở các nước đang phát triển, cùng với sự của các doanh nghiệp hoạt động trên môi trường mạng dẫn đến các rủi ro có thể xảy ra là rất nghiêm trọng. Do đó, cần thiết để có một phương pháp xây dựng chính sách đảm bảo an toàn thông tin một cách toàn diện, dễ hiểu và dễ thực hiện cho các tổ chức doanh nghiệp. Khung kiến trúc bảo đảm an toàn thông tin là một hướng dẫn cho các biện pháp, chính sách đảm bảo an toàn thông tin.

Khung kiến trúc bảo đảm an toàn thông tin dựa trên ITI-GAF là giải pháp dễ thực hiện để để đáp ứng những yêu cầu trên. Một mặt, nó thừa hưởng tất cả các tính năng tốt của cách tiếp cận kiến trúc doanh nghiệp. Mặt khác, nó đã được đơn giản hóa để phù hợp với cơ sở hạ tầng và năng lực trong các tổ chức, doanh nghiệp. Các mô hình đánh giá có thể giúp các tổ chức, doanh nghiệp để xác định các những việc cần thực hiện. Dựa vào đó, nó cho phép các tổ chức, doanh nghiệp để xây dựng kế hoạch hành động dài hạn ngắn hạn và và giám sát, đánh giá lại và điều chỉnh các mục tiêu sau mỗi giai đoạn phát triển. Đây là điều kiện tiên quyết để xây dựng một hệ thống toàn diện đảm bảo an toàn thông tin.

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. Tiêu chuẩn TCVN ISO/IEC 27002:2011 Công nghệ thông tin – các kỹ thuật an toàn – quy tắc thực hành quản lý an toàn thông tin.
2. Nguyễn Văn Đoài, Lê Khắc Quyền (2015), "Nghiên cứu, tìm hiểu kiến trúc TOGAF và những ứng dụng của TOGAF trong các trường đại học", Tạp chí Công nghệ Thông tin và Truyền thông, kỳ 1 tháng 4/2015.

Tiếng Anh

3. "Business Systems Planning and Business Information Control Study: A comparison". In:IBM Systems Journal, vol 21, no 3, 1982. p. 31-53.
4. Nguyen Ai Viet (2016), TOWARD ASEAN-EU COOPERATION IN CYBER SECURITY: An analysis on alignment between EU and ASEAN priorities and objectives – Final Report of CONNECT2SEA project.
5. J. A. Zachman (1987). "A Framework for Information Systems Architecture". In: IBM Systems Journal, vol 26, no 3. IBM Publication G321-5298.
6. The Open Group Architectural Framework, TOGAF 9.1 Online Documents (2012), URL: http://pubs.opengroup.org/architecture/togaf9-doc/arch/
7. National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (2014), URL: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
8. Enterprise architecture framework, URL: https://en.wikipedia.org/wiki/Enterprise_architecture_framework