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

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Hà Nội - Năm 2016

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

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. Lê Quang Minh

Hà Nội - Năm 2016

LỜI CAM ĐOAN

Tôi xin cam đoan, luận văn "Áp dụng Enterprise Architecture xây dựng khung kiến trúc bảo đảm toàn thông tin cho các tổ chức, doanh nghiệp tại Việt Nam" là do tôi thực hiện dưới sự hướng dẫn của TS. Lê Quang Minh. Trong toàn bộ nội dung của luận văn, những điều đã trình bày là của cá nhân tôi hoặc là được tôi tổng hợp từ nhiều nguồn tài liệu. Tất cả các nguồn tài liệu tham khảo có xuất xứ rõ ràng và được trích dẫn hợp pháp.

Hà Nội, ngày 28 tháng 10 năm 2016

Tác giả luận văn

Nguyễn Thanh Tuyền

LỜI CẢM ƠN

Trước tiên, tôi xin chân thành cảm ơn TS. Lê Quang Minh (Viện Công nghệ thông tin, Đại Học Quốc gia Hà Nội), người đã động viên, hướng dẫn giúp đỡ, chỉ bảo, đồng thời cung cấp các tài liệu trong quá trình tôi thực hiện đề tài.

Tôi xin cảm ơn ban chủ nhiệm Khoa cùng toàn thể các thầy, cô giáo trong Khoa Công nghệ thông tin – Trường Đại học Công nghệ đã tạo điều kiện giúp đỡ tôi trong thời gian học tập cũng như trong quá trình hoàn thành luận văn.

Cuối cùng, tôi xin được cảm ơn gia đình, bạn bè đã luôn ở bên cạnh, động viên, khuyến khích tôi trong quá trình học tập, nghiên cứu.

Mặc dù đã rất cố gắng trong quá trình thực hiện nhưng luận văn không thể tránh khỏi những thiếu sót. Tôi mong nhận được sự góp ý của các thầy, cô và các bạn học viên.

Xin trân trọng cảm ơn!

Tác giả luận văn

Nguyễn Thanh Tuyền

MỤC LỤC

BẢNG CÁC CHỮ CÁI VIẾT TẮT

Viết tắt	Tên đầy đủ
ATTT	An toàn thông tin
CNTT	Công nghệ thông tin
TCVN	Tiêu chuẩn Việt Nam
AMD	Phương pháp phát triển kiến trúc (Architecture Development Method)
CSAF	Khung kiến trúc an ninh không gian mạng (Cyber Security Architecture Framework)
CIO	Giám đốc Công Nghệ Thông Tin (Chief Information Officer)
Enterprise	Tổ chức, doanh nghiệp
EA	Kiến trúc tổng thể (Enterprise Architecture)
FEAF	Khung kiến trúc liên bang (Federal Enterprise Architecture Framework)
GAF	Khung kiến trúc tổ chức, doanh nghiệp (Government Architecture Framework)
ISO	Tổ chức quốc tế về tiêu chuẩn hóa (International Organization for Standardization)
IEC	Tổ chức quốc tế về tiêu chuẩn hóa (International Organization for Standardization)
ITI	Viện Công nghệ thông tin (Information Technology Institute)
NIST	Viện tiêu chuẩn và Công nghệ Quốc Gia (National Institute of Standards and Technology)

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC BẢNG

PHẦN MỞ ĐẦU

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

1.1. Về phương pháp luận xây dựng kiến trúc tổ chức, doanh 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 toàn thông tin cho các tổ chức, doanh nghiệp tại Việt Nam

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.

2. Đối tượng và phạm vi nghiên cứu

2.1. Đối tượng nghiên cứu

- Khung kiến trúc tổng thể tổ chức, doanh nghiệp; Phương pháp luận xây dựng khung kiến trúc tổ chức, doanh nghiệp.

- Cách áp dụng phương pháp luận xây dựng khung kiến trúc tổ chức, doanh nghiệp vào việc xây dựng khung kiến trúc bảo đảm an toàn thông tin cho các tổ chức, doanh nghiệp tại Việt Nam.

2.2. Phạm vi nghiên cứu

- Tổng quan về phương pháp luận xây dựng khung kiến trúc tổ chức, doanh nghiệp. Giới thiệu một số phương pháp nổi tiếng trên thế giới và một phương pháp của Việt Nam.

- Xây dựng khung kiến trúc bảo đảm toàn thông tin cho tổ chức, doanh nghiệp tại Việt Nam.

3. Phương pháp nghiên cứu

Nghiên cứu các tài liệu về phương pháp luận xây dựng kiến trúc.

Tham khảo một số kiến trúc đã xây dựng.

Tìm hiểu thêm các thông tin từ Internet.

Tham khảo ý kiến của Thầy hướng dẫn và các đồng nghiệp.

Lựa chọn các phương pháp thích hợp để giải quyết vấn đề đặt ra.

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. Các khái niệm

Khái niệm kiến trúc tổng thể (EA - Enterprise Architecture) được ra đời từ những năm 80 của thế kỷ trước. Tuy nhiên, vẫn chưa có một khái niệm rõ ràng, nhất quán và chính xác về khung kiến trúc tổng thể. Kiến trúc tổng thể đã được nhiều tổ chức đầu tư nghiên cứu, phát triển, trong mỗi nghiên cứu, khái niệm kiến trúc tổng thể cũng được định nghĩa theo các cách khác nhau. 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:

i) Các bộ phận cấu thành nên hệ thống đó,

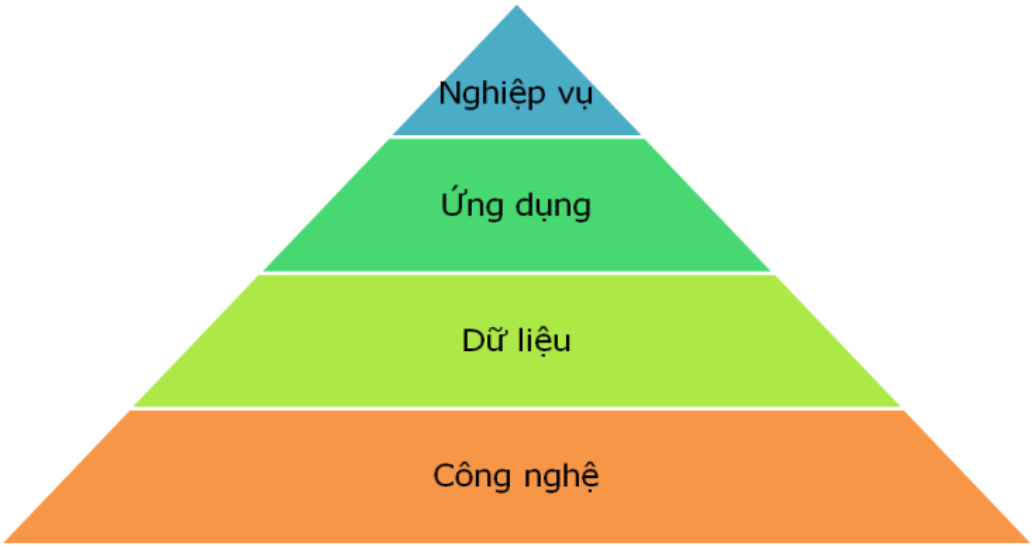
ii) Quan hệ giữa các bộ phận với nhau và với môi trường ngoài và

iii) 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:



Hình 1.1: Các thành phần của kiến trúc tổng thể

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

Cũng giống như vai trò của kiến trúc trong xây dựng, kiến trúc tổng thể đóng một vai trò vô cùng to lớn trong việc xây dựng, cải tổ, phát triển của mỗi tổ chức, cơ quan, doanh nghiệp. Kiến trúc tổng thể giúp cho các cơ quan tổ chức, doanh nghiệp có được cái nhìn rõ ràng, tổng thể về mình, biết được cơ quan, tổ chức đang đứng ở đâu, muốn đi tới đâu. Tổ chức còn thiếu gì, còn cần gì, các dự án

triển khai có thực sự nằm trong quy hoạch chung hay chỉ là tạm thời, chắp vá. Giữa các hệ thống có liên hệ, liên kết như thế nào….

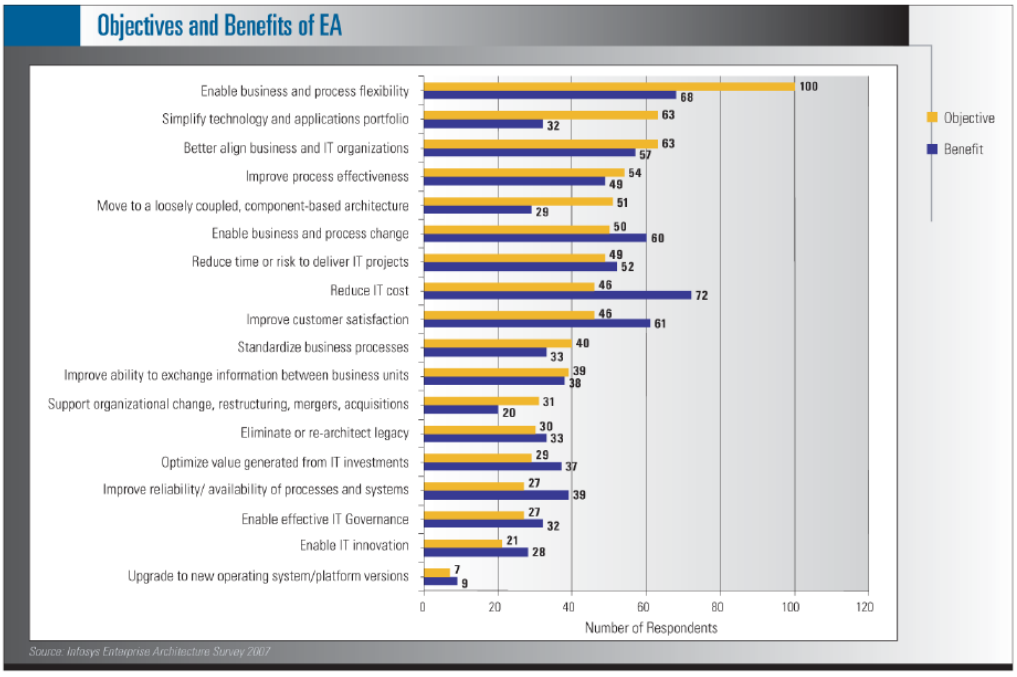
Khi quy mô tổ chức còn nhỏ, vài trò của kiến trúc tổng thể là chưa rõ ràng, tất cả các nguồn lực cũng như các vấn đề phát sinh đều với số lượng không đáng kể, trực quan và không quá khó để kiểm soát. Tuy nhiên, khi một tổ chức phát triển lới hơn, quy mô hoạt động được mở rộng thì vai trò của kiến trúc 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…



Hình 1.2: Mục đích và lợi ích của kiến trúc tổng thể

1.1.4 Quy trình xây dựng kiến trúc tổng thể

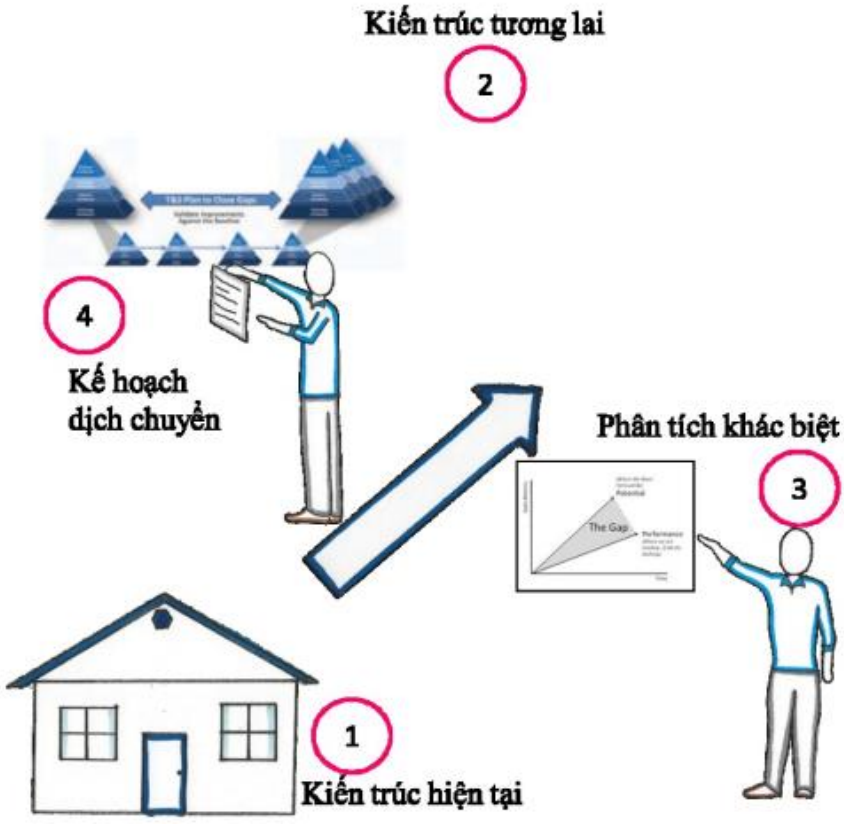
Hình 1. 3 cho ta thấy quy trình xây dựng kiến trúc tổng thể của một đơn vị, tổ chức. Bao gồm 04 bước sau:

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.



Hình 1.3: Quy trình xây dựng kiến trúc tổng thể

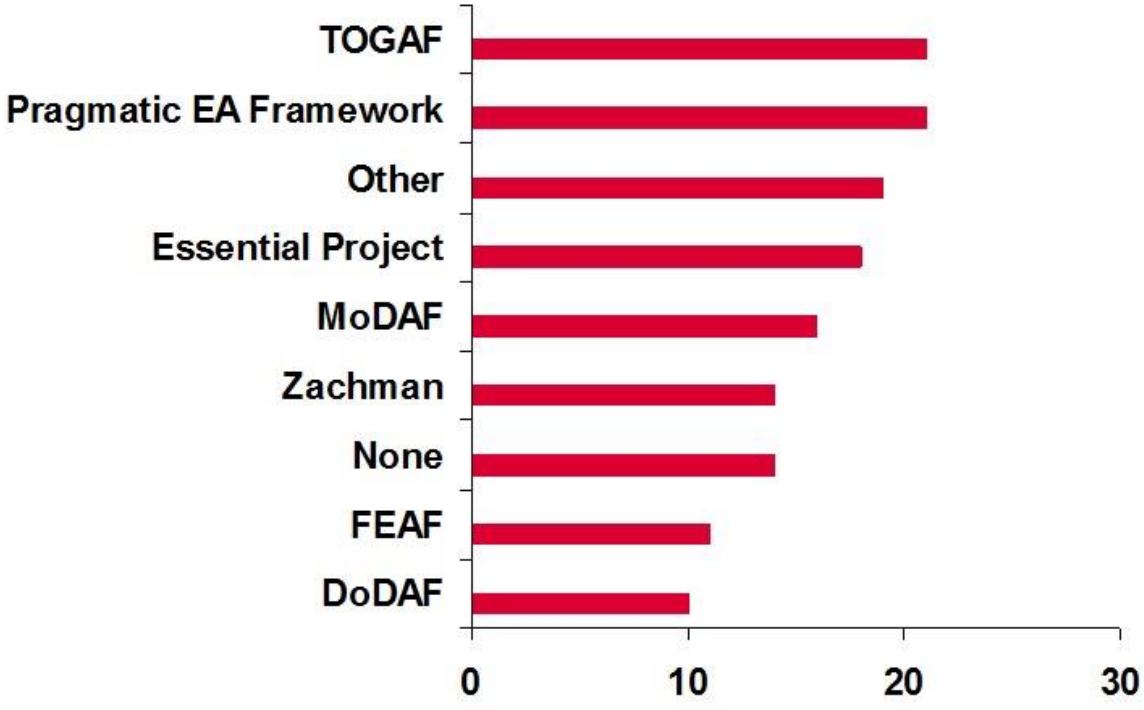
1.2. Tổng quan về khung kiến trúc tổng thể

1.2.1 Khung kiến trúc tổng thể là gì?

Kiến trúc tổng thể của mỗi tổ chức, đặc biệt là các tổ chức lớn, bao gồm nhiều thành phần nhỏ, thậm chí mỗi đơn vị của tổ chức đó cũng có kiến trúc tổng thể của riêng mình, cho nên để tạo ra sự thống nhất, đảm bảo tính tương thích cao giữa các thành phần, các hệ thống con trong một tổ chức cần có khung kiến trúc

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".

Khung kiến trúc không phải là 1 kiến trúc duy nhất mà là một công cụ được sử dụng để xây dựng và phát triển kiến trúc. Từ một khung kiến trúc người ta có thể tạo ra nhiều kiến trúc khác nhau. Theo thống kê của Iso-enterprise architecture, có khoảng 57 khung kiến trúc trên toàn thế giới và nổi tiếng nhất, được áp dụng phổ biến nhất phải kể đến khung kiến trúc TOGAF, ZACHMAN, FEAF... Hình 1.4 cho ta thấy tỷ lệ áp dụng các khung kiến trúc đối với các tổ chức, doanh nghiệp trên toàn thế giới. Phần sau chúng ta sẽ tìm hiểu kỹ hơn về các khung kiến trúc này.

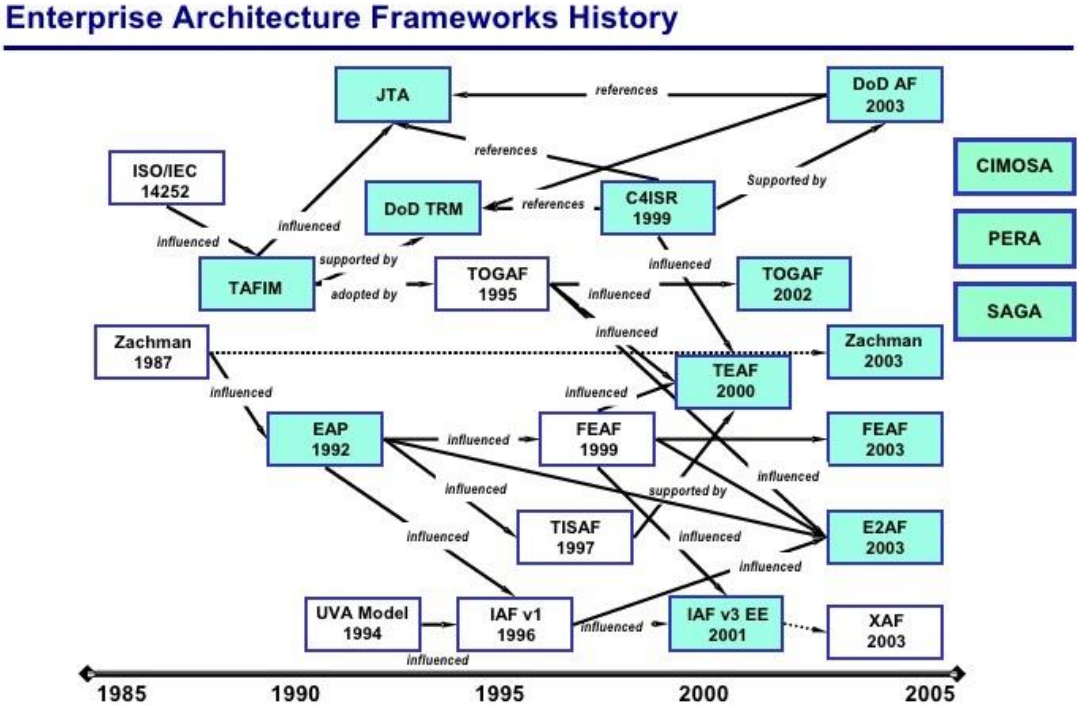


Hình 1.4: Tỷ lệ áp dụng các khung kiến trúc

2.2.2 Lịch sử và phát triển của khung kiến trúc EA

Kiến trúc hệ thống có thể coi như bắt đầu vào năm 1987 khi J.A Zachman viết bài báo "A Framework for Information Systems Architecture - Khung cho kiến trúc các hệ thống thông tin". Năm 1994, Bộ Quốc phòng Mỹ phát triển khung kiến trúc kỹ thuật cho quản lý thông tin (TAFIM) – khung kiến trúc bị ảnh hưởng nhiều bởi tư tưởng của Zachman. Đạo luật Clinger-Cohen được thông qua năm 1996 của Quốc hội Hoa Kỳ trong đó quy định các cơ quan liên bang phải nâng cao hiệu quả của đầu tư công nghệ thông tin đã tạo điều kiện chính thức cho sự phát triển của EA. Hội đồng CIO của Mỹ được thành lập và kết quả cho ra đời Khung Kiến trúc liên bang (FEAF). Phiên bản 1.1 của khung kiến trúc này được phát hành năm 1999. FEAF cuối cùng phát triển thành các kiến trúc doanh nghiệp liên bang (FEA) dưới sự kiểm soát của Văn phòng Quản lý và Ngân sách (OMB). Năm 1998, bốn năm sau khi TAFIM được giới thiệu và hai năm sau khi nó được hệ thống hóa bởi Clinger-Cohen, TAFIM đã chính thức ngừng hoạt động và công việc thực hiện được chuyển giao cho Tập đoàn Open. Họ đã thay đổi và phát triển phiên bản khung kiến trúc mở (TOGAF) đầu tiên từ dựa trên khung TAFIM đó.

Các kiến trúc E2AF, TEAF sau này đều chịu ảnh hưởng ít nhiều TOGAF. Hình 1.5 đưa ra một vài mốc phát triển của một vài phương pháp luận EA phổ biến:



Hình 1.5: Lịch sử khung kiến trúc tổng thể

Sau gần 30 năm phát triển đến nay đã có hàng chục khung, phương pháp luận kiến trúc hệ thống ra đời và có thể thấy hầu hết các khung kiến trúc ngày nay đều có chung lịch sử và được xây dựng trên tinh hoa và các yếu tố có giá trị của các khung kiến trúc cũ.

1.2.3 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

1.3.1.1 Giới thiệu chung

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).

Ở phiên bản đầu tiên, khung cơ bản của Zachman được xây dựng trên 3 cột chính: dữ liệu, chức năng và mạng. Sau đó, ông phát triển mở rộng thêm 3 cột nữa: con người, thời gian và động lực, và đổi tên thành "Khung kiến trúc" – đây chính là khung Zachman được biết đến và sử dụng rộng rãi ngày nay.

1.3.1.2. Phương pháp luận

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 1.6: Lược đồ khung Zachman

Xuất phát từ tư tưởng trên, Khung Zachman đưa ra 6 quan điểm cơ bản sau:

Quan điểm ở mức ngữ cảnh (Contextual): đây là quan điểm liên quan đến khía cạnh chiến lược của tổ chức hay doanh nghiệp. Nó cho phép xác định các mục tiêu, phạm vi và đánh giá thực thi. Quan điểm này thường được đứng trên góc độ của người lập kế hoạch, xác định các nội dung:

– Danh sách các lớp dữ liệu ở mức cao (WHAT)

– Danh sách các quy trình nghiệp vụ (HOW)

– Danh sách địa điểm triển khai (WHERE)

– Danh sách các đơn vị quan trọng (WHO)

– Danh sách các sự kiện liên quan (WHEN)

– Danh sách các mục tiêu và chiến lược của hệ thống (WHY)

Quan điểm ở mức khái niệm (Conceptual): quan điểm này mô hình hóa quy trình nghiệp vụ bao gồm cấu trúc, chức năng và tổ chức liên quan đến các quy trình. Quan điểm này được gọi là khung nhìn nghiệp vụ, cho phép xác định các nội dung:

– Mô hình đối tượng/ dữ liệu mức khái niệm (WHAT)

– Mô hình quy trình nghiệp vụ (HOW)

– Hệ thống nghiệp vụ (WHERE)

– Mô hình luồng công việc (WHO)

– Chương trình tổng thể (WHEN)

– Kế hoạch nghiệp vụ (WHY)

Quan điểm ở mức Logic/ hệ thống (Logical): quan điểm này làm rõ các quy trình nghiệp vụ ở mức khái niệm. Nếu mức khái niệm mới chỉ dừng lại ở việc định nghĩa các chức năng nghiệp vụ thì mức này đặc tả cụ thể hơn các mô hình dữ liệu liên quan tới các chức năng. Quan điểm này còn là quan điểm dành cho đội ngũ nhân viên thiết kế, cho phép xác định các nội dung tương ứng sau:

– Mô hình dữ liệu logic (WHAT)

– Mô hình kiến trúc hệ thống (HOW)

– Kiến trúc các hệ thống phân tán (WHERE)

– Kiến trúc giao diện (WHO)

– Cấu trúc xử lý (WHEN)

– Mô hình quy tắc nghiệp vụ (WHY)

Quan điểm ở mức vật lý/ công nghệ (Physical/ Technology): quan điểm này xác định các mô hình vật lý, quản lý về mặt công nghệ, định nghĩa và phát triển các giải pháp công nghệ. Ở mức này, cho phép xác định các tiêu chí của các chương trình ứng dụng, các yêu cầu về hệ thống CSDL, ngôn ngữ, cấu trúc, chương trình, giao diện người sử dụng. Quan điểm này còn gọi là khung nhìn vật lý (dành cho đội ngũ nhân viên phát triển)

– Mô hình lớp/ dữ liệu vật lý (WHAT)

– Mô hình thiết kế công nghệ (HOW)

– Kiến trúc công nghệ (WHERE)

– Kiến trúc trình diễn (WHO)

– Cấu trúc điều khiển (WHEN)

– Thiết kế quy tắc (WHY)

Quan điểm ở tích hợp hệ thống (Out-of-context/ Intergrator/ As Built): quan điểm này thể hiện việc xây dựng, quản lý cấu hình và triển khai hệ thống, cho phép xác định các nội dung:

– Định nghĩa dữ liệu (WHAT)

– Chương trình (HOW)

– Kiến trúc mạng (WHERE)

– Kiến trúc bảo mật (WHO)

– Định nghĩa thời hạn (WHEN)

– Dự đoán quy tắc, luật (WHY)

Quan điểm ở mức vận hành (Functioning): quan điểm này thể hiện các chức năng của hệ thống hoàn chỉnh, quản lý việc vận hành và đánh giá hệ thống. Quan điểm này cho phép người sử dụng xác định các đặc tính vận hành, hướng dẫn, dữ liệu trong hệ thống, các đối tượng vận hành và sử dụng hệ thống, các thông điệp dữ liệu và thời gian của các hoạt động.

– Dữ liệu sử dụng (WHAT)

– Chức năng làm việc (HOW)

– Mạng lưới sử dụng (WHERE)

– Chức năng tổ chức (WHO)

– Kế hoạch cài đặt (WHEN)

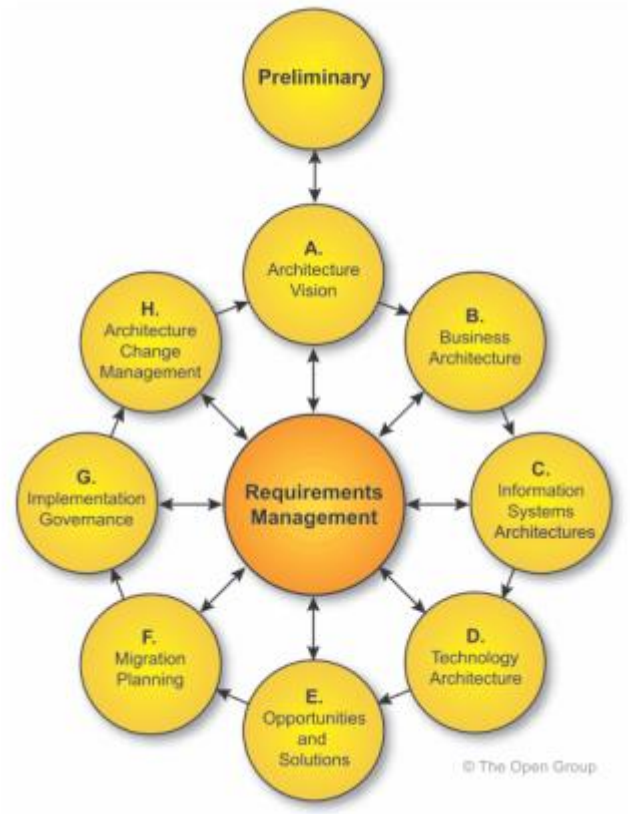
– Chiến lược hoạt động (WHY)

Qua tìm hiểu khung Zachman bên trên cho thấy ưu điểm của khung kiến trúc Zachman là cho phép tiếp cận một cách có hệ thống và đầy đủ mô tả về chức năng, nhiệm vụ, quy trình nghiệp vụ của cơ quan tổ chức. Đó là cách nhìn trung lập, toàn diện, hệ thống tất cả các mô hình của cơ quan, tổ chức. Đồng thời, nó cũng cung cấp hệ thống các câu hỏi hướng dẫn cho các nhà phát triển khi xây dựng hệ thống.

Tuy nhiên, nhược điểm của khung Zachman là không tập trung vào nghiệp vụ, không có sự đồng bộ hóa giữa IT và nghiệp vụ dẫn tới việc tập trung quá mức vào IT và không xây dựng quy trình để tiến hành mô tả khung. Hơn nữa, trong thực tế, rất hiếm khi ta cần trả lời đầy đủ các câu hỏi hay mô tả về hệ thống theo các quan điểm của khung kiến trúc Zachman đưa ra.

1.3.2. Khung kiến trúc TOGAF

Đây là phần cốt lõi của TOGAF, hướng dẫn các phương pháp để phát triển kiến trúc. ADM gồm 9 pha như mô tả trong Hình 1.7:



Hình 1.7: Phương pháp phát triển kiến trúc (ADM) – TOGAF

1.3.2.1. Các thành phần chính của TOGAF

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

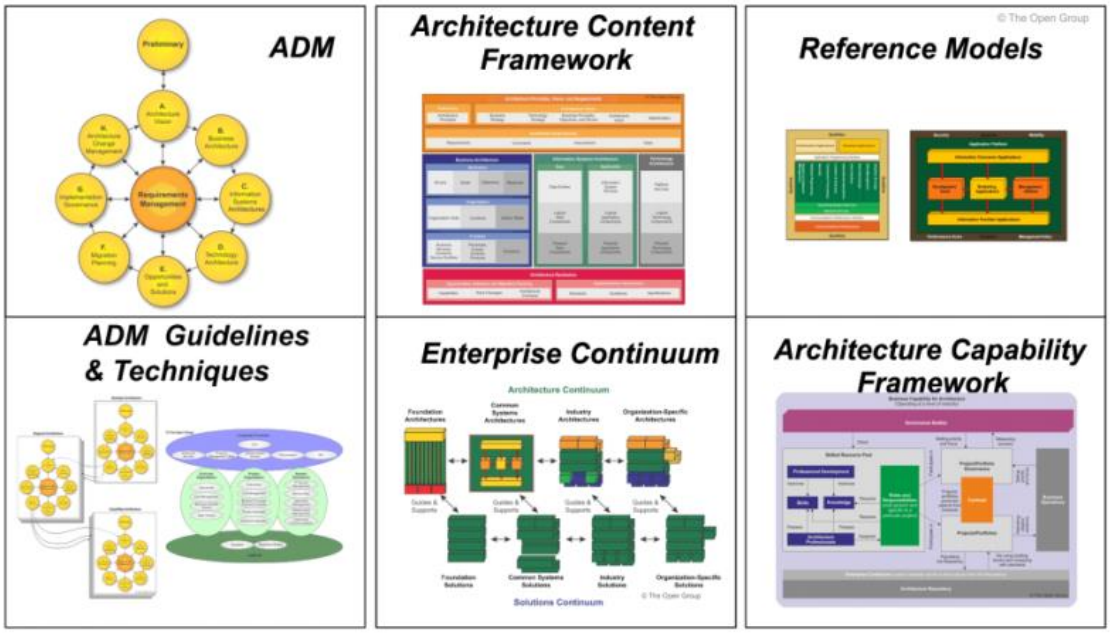
- Các kỹ thuật và các hướng dẫn sử dụng ADM (ADM Guidelines & Techniques).

- 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 1.8: Các thành phần chính của TOGAF

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

Pha trù bị (Preliminary): Khung công việc và các nguyên tắc. Pha trù bị (hay dẫn nhập) bao gồm việc diễn giải khung công việc và định nghĩa các nguyên tắc cơ bản của kiến trúc. Nội dung của pha trù bị gồm:

- Mô hình tổ chức cho kiến trúc
- Khung kiến trúc đã được "may đo"
- Khởi tạo kho tư liệu kiến trúc
- Khung giám quản kiến trúc
- Danh mục các qui tắc (nội dung này không bắt buộc)

Pha A: Tầm nhìn kiến trúc (Architecture Vision) Tầm nhìn kiến trúc xác định phạm vi của kiến trúc được tạo, tổng thể như thế nào và các nguyên tắc đạt được. Đây là pha thực hiện khởi động mỗi vòng lặp của qui trình phát triển kiến trúc. Nội dung của tầm nhìn kiến trúc gồm:

- Xác định quy mô, hạn chế và kỳ vọng
- Xác định mục tiêu của kiến trúc

- Xác định các bên liên quan

- Tạo ra đề cương công việc

Pha B: Kiến trúc nghiệp vụ (Business Architecture) Kiến trúc nghiệp vụ mô tả các quy trình nghiệp vụ và con người, mối quan hệ của chúng với nhau và với môi trường, các nguyên tắc chi phối thiết kế và phát triển. Ngoài ra đưa ra cách thức để tổ chức có thể đạt được các mục tiêu nghiệp vụ. Nội dung của kiến trúc nghiệp vụ gồm:

- Cấu trúc tổ chức

- Mục tiêu nghiệp vụ

- Chức năng nghiệp vụ

- Dịch vụ nghiệp vụ

- Quy trình nghiệp vụ

- Các tác nhân và vai trò nghiệp vụ

- Tương quan của tổ chức và các chức năng nghiệp vụ

Pha C: Kiến trúc các hệ thống thông tin (Information Systems Architectures)

Kiến trúc các hệ thống thông tin bao gồm Kiến trúc dữ liệu và Kiến trúc ứng dụng:

- Kiến trúc dữ liệu (Data Architecture): Mô tả cấu trúc logic và vật lý của dữ liệu cũng như cách thức tổ chức quản lý, chuyển đổi, giám quản, lưu trữ và trao đổi dữ liệu.

- Kiến trúc ứng dụng (Applications Architecture): Mô tả các ứng dụng được triển khai nhằm phục vụ các qui trình nghiệp vụ và quá trình trao đổi, chia sẻ thông tin giữa các ứng dụng với nhau.

Pha D: Kiến trúc công nghệ (Technology Architecture) Kiến trúc công nghệ xác định các thành phần công nghệ, nền tảng công nghệ, các yêu cầu về cơ sở hạ tầng phục vụ việc xây dựng và triển khai hệ thống. Nội dung của kiến trúc công nghệ gồm:

- Phần cứng, phần mềm và công nghệ kết nối.

- Quan hệ của chúng với nhau và với môi trường.

- Các nguyên tắc chi phối việc thiết kế và phát triển

Pha E: Các cơ hội và giải pháp (Opportunities and Solutions) Pha này thực hiện phân tích các cơ hội và lựa chọn các giải pháp để tạo ra phiên bản hoàn chỉnh đầu tiên của lộ trình kiến trúc. Nội dung của pha này gồm:

- Lập kế hoạch triển khai.

- Xác định các dự án triển khai chính.

- Nhóm các dự án vào các Kiến trúc chuyển tiếp (Transition Architecture)

- Xác định cách tiếp cận: Tự xây dựng, mua hay sử dụng lại; Thuê ngoài; Sử dụng sản phẩm thương mại hay nguồn mở…

- Đánh giá ưu tiên.

- Xác định các phụ thuộc.

Pha F: Lập kế hoạch chuyển đổi (Migration Planning) Pha này đưa ra kế hoạch xây dựng và chuyển đổi trong quá trình hợp tác với các bên tham gia. Nội dung của pha này gồm:

- Đối với mỗi dự án đã xác định trong Pha E, thực hiện:

  Ước lượng chi phí, yêu cầu về tài nguyên của việc chuyển đổi.

  Phân tích lợi ích của việc chuyển đổi.

  Đánh giá rủi ro của việc chuyển đổi

  Xác định các mốc thời gian thực hiện chuyển đổi.

  Xây dựng cấu trúc phân việc thực hiện chuyển đổi.

  Xác định các rủi ro và sự phụ thuộc.

- Đưa ra các yêu cầu cho việc lặp lại qui trình xây dựng kiến trúc

- Xây dựng mô hình giám quản.

- Thay đổi các yêu cầu đối với năng lực kiến trúc.

Pha G: Giám quản triển khai (Implementation Governance) Pha này sẽ đưa ra hương thức quản lý, giám sát việc triển khai kiến trúc. Nội dung của pha này gồm:

- Cung cấp cách thức giám sát kiến trúc đối với việc triển khai các dự án.

- Xác định các ràng buộc của kiến trúc đối với việc triển khai các dự án.

- Theo dõi việc tuân thủ kiến trúc đối với việc triển khai các dự án.

Pha H: Quản lý sự thay đổi kiến trúc (Architecture Change Management) Pha này thiết lập nên các thủ tục để quản lý thay đổi tới kiến trúc mới. Nội dung của pha này gồm:

- Cung cấp cách thức theo dõi thường xuyên và đưa ra một quy trình quản lý thay đổi

- Bảo đảm rằng các thay đổi kiến trúc được quản lý chặt chẽ và có phương pháp.

- Thiết lập và hỗ trợ một kiến trúc linh hoạt có khả năng phát triển nhanh theo các thay đổi về công nghệ hoặc môi trường nghiệp vụ.

- Theo dõi quản lý nghiệp vụ và năng lực

1.3.2.3. *Các kỹ thuật và hướng dẫn áp dụng ADM (ADM Guidelines & Techniques)*

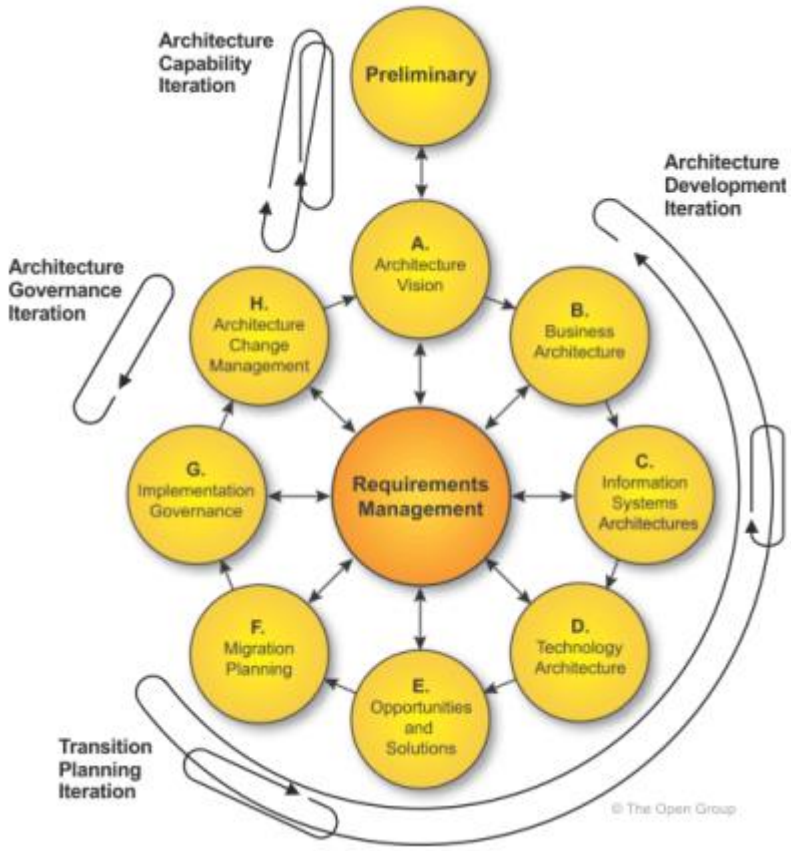
Áp dụng lặp trong ADM: Khi áp dụng ADM thì có thể thực hiện các vòng lặp để hoàn thiện kiến trúc. Các vòng lặp khi áp dụng ADM (Hình 1.9) gồm:

- Lặp năng lực kiến trúc (Architecture Capability Iteration).

- Lặp phát triển kiến trúc (Architecture Development Iteration).

- Lặp lập kế hoạch chuyển tiếp (Transition Planing Iteration).

- Lặp giám quản kiến trúc (Architecture Governance Iteration).



Hình 1.9: Các vòng lặp trong ADM

Kiến trúc an toàn, an ninh (Security Architecture) và ADM:

Khi áp dụng ADM có những vấn đề về an toàn, an ninh cần phải được giải quyết. Khi xây dựng EA kiến trúc sư EA cần phải đưa ra các các vấn đề an toàn, an ninh quan trọng cần phải được giải quyết để phối hợp với kiến trúc sư an toàn, an ninh xây dựng kiến trúc an toàn, an ninh. Các nội dung của kiến trúc an toàn, an ninh gồm:

- Xác thực (Authentication).
- Phân quyền (Authorization).
- Kiểm soát (Audit)
- Đảm bảo (Assurance).
- Tính sẵn sàng (Availability)
- Bảo vệ tài sản (Asset Protection).
- Quản trị (Administration).

- Quản lý rủi ro (Risk Management).

Kiến trúc an toàn, an ninh có thể được áp dụng vào từng pha của ADM

Các hướng dẫn và kỹ thuật áp dụng ADM khác:

- Xác định và giám quản các Kiến trúc hướng dịch vụ (SOA).

- Các nguyên tắc để phát triển kiến trúc.

- Quản lý bên liên quan.

- Các mẫu kiến trúc.

- Các kịch bản nghiệp vụ.

- Phân tích khoảng cách.

- Các kỹ thuật lập kế hoạch chuyển đổi.

- Các yêu cầu tương hợp

- Đánh giá sự sẵn sàng thay đổi nghiệp vụ

- Quản lý rủi ro

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

Khung nội dung kiến trúc cung cấp một cấu trúc chuẩn của nội dung kiến trúc, cho phép định nghĩa và trình bày các thành phần chính của kiến trúc được nhất quán, có cấu trúc. Khung nội dung kiến trúc chuẩn (Hình 1.10) gồm các thành phần chính:

- Dẫn nhập và tầm nhìn kiến trúc: Bao gồm các nguyên tắc, chiến lược nghiệp vụ, chiến lược công nghệ, các qui tắc nghiệp vụ, tầm nhìn kiến trúc, các bên liên quan, các yêu cầu, các ràng buộc...

- Kiến trúc nghiệp vụ: Bao gồm các yếu tố tác động, các mục tiêu, mục đích, độ đo, mô hình tổ chức, vị trí, các tác nhân / vai trò, các chức năng nghiệp vụ, các dịch vụ nghiệp vụ, các ràng buộc, chất lượng dịch vụ, các xử lý, sự kiện, sản phẩm…

- Kiến trúc hệ thống thông tin:

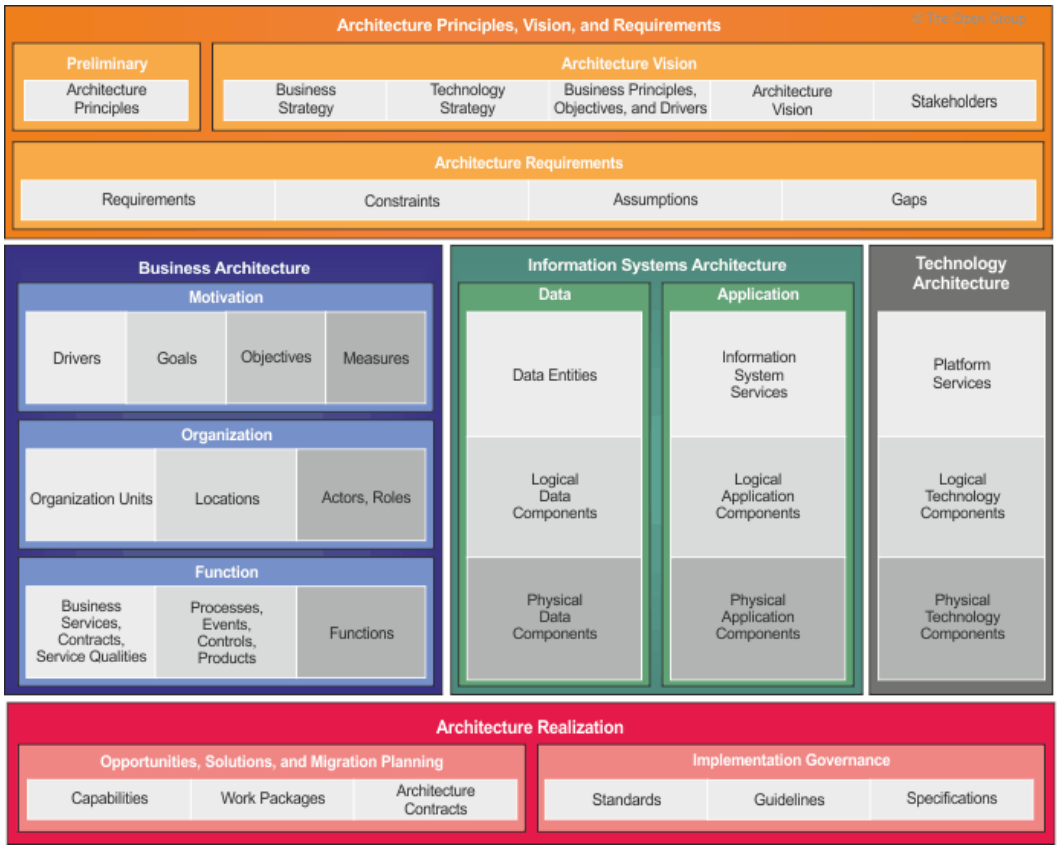
+ Kiến trúc dữ liệu: Bao gồm các thực thể dữ liệu, các thành phần dữ liệu mức logic, các thành phần dữ liệu mức vật lý.

+ Kiến trúc ứng dụng: Bao gồm các dịch vụ hệ thống thông tin, các thành phần ứng dụng mức logic, các thành phần ứng dụng mức vật lý.

- Kiến trúc công nghệ: Bao gồm các dịch vụ nền tảng, các thành phần công nghệ mức logic, các thành phần công nghệ mức vật lý. - Sự thực hiện kiến trúc:

+ Các cơ hội, các giải pháp và kế hoạch chuyển đổi: Các khả năng, các gói công việc, các ràng buộc kiến trúc.

+ Thực hiện giám quản: Các chuẩn, các hướng dẫn, các đặc tả



Hình 1.10: Khung nội dung kiến trúc chuẩn

Các thành phần trong khung nội dung kiến trúc chuẩn lại được chi tiết bằng các danh mục (Catalog), các ma trận/bảng (Matrix) hoặc các biểu đồ (Diagrams). Theo từng thành phần chính của khung kiến trúc sẽ có các thành phần chi tiết được mô tả như trong Hình 1. 11 bao gồm:

- Dẫn nhập và tầm nhìn kiến trúc:

+ Danh mục: Nguyên tắc
+ Ma trận: Các bên liên quan.
+ Biểu đồ: Chuỗi giá trị, giải pháp.

- Kiến trúc nghiệp vụ:

+ Danh mục: Tổ chức / tác nhân, động lực / mục tiêu / mục đích, vai trò, chức năng nghiệp vụ, dịch vụ nghiệp vụ, vị trí, qui trình, sự kiện, sản phẩm, độ đo.
+ Ma trận: Tương tác nghiệp vụ, tác nhân / vai trò.
+ Biểu đồ: Qui trình nghiệp vụ, dịch vụ nghiệp vụ / thông tin, phân rã chức năng, vòng đời sản phẩm, UC nghiệp vụ, phân cấp tổ chức, luồng qui trình, sự kiện.

- Kiến trúc dữ liệu:

+ Danh mục: Thực thể dữ liệu, thành phần dữ liệu o Ma trận: Thực thể dữ liệu / chức năng nghiệp vụ, ứng dụng / dữ liệu.
+ Biểu đồ: Dữ liệu (mức khái niệm, mức logic), phân phối dữ liệu, bảo mật dữ liệu, chuyển đổi dữ liệu, vòng đời dữ liệu.

- Kiến trúc ứng dụng:

+ Danh mục: Ứng dụng, giao diện
+ Ma trận: Ứng dụng / tổ chức, vai trò / ứng dụng, ứng dụng / chức năng, tương tác ứng dụng.
+ Biểu đồ: Giao tiếp giữa các ứng dụng, ứng dụng và vị trí người sử dụng, UC ứng dụng, qui trình / ứng dụng, phân bổ phần mềm.

- Kiến trúc công nghệ:

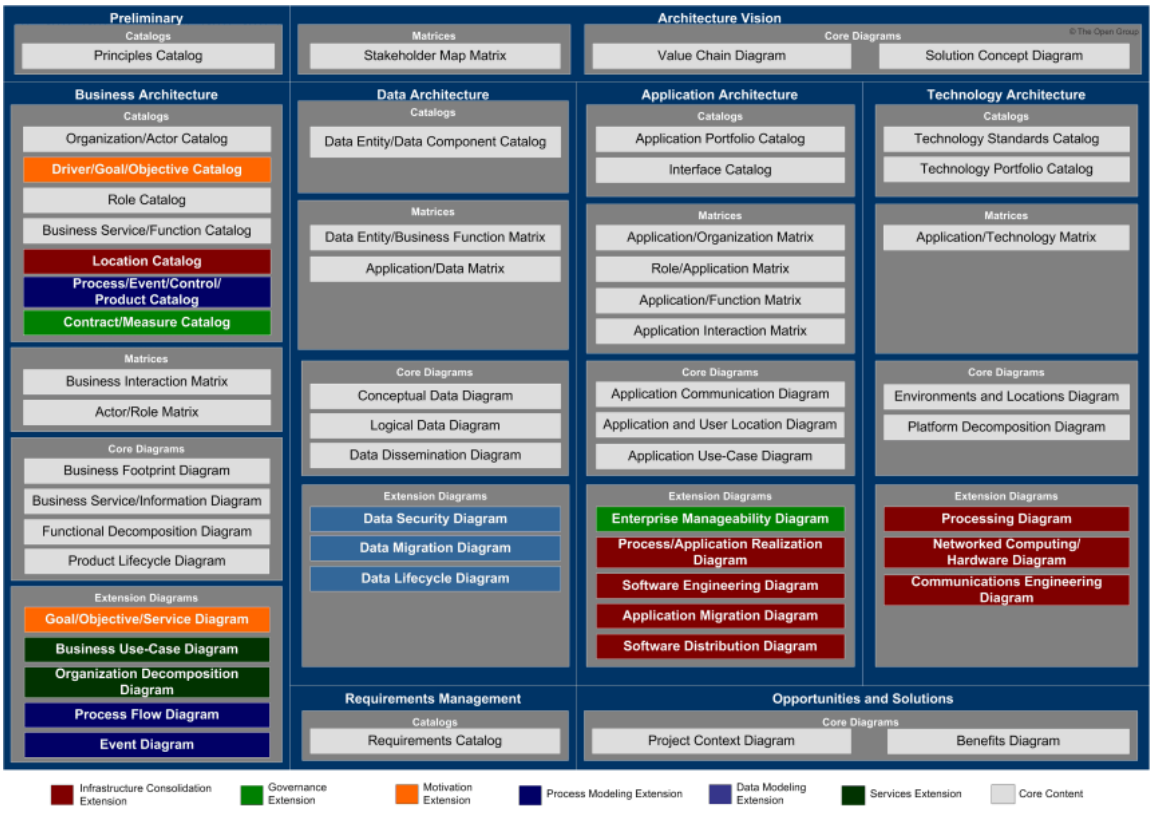
+ Danh mục: Các chuẩn công nghệ, đầu tư công nghệ.
+ Ma trận: Ứng dụng / công nghệ.
+ Biểu đồ: Môi trường và vị trí, phân cấp nền tảng, mạng máy tính / phần cứng.

- Quản lý các yêu cầu:

+ Danh mục: Các yêu cầu.

- Các cơ hội và các giải pháp:

+ Biểu đồ: Khung cảnh dự án, lợi ích.



Hình 1.11: Cách mô tả các thành phần của khung nội dung kiến trúc chuẩn

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

Bao gồm các cách thức phân loại phù hợp, các hướng dẫn, các mẫu, các mô hình, tài nguyên phục vụ cho việc phát triển kiến trúc trong một tổ chức.

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

Bao gồm cơ cấu tổ chức, các quy trình, các kỹ năng, các vai trò và trách nhiệm cần thiết để xây dựng và vận hành một chức năng kiến trúc trong tổ chức.

1.3.2.7. Các mô hình tham chiếu (Reference Models)

Các mô hình tham chiếu sử dụng để mô tả kỹ hơn về một thành phần nào đó của kiến trúc. Một thành phần kiến trúc có thể có một hoặc nhiều mô hình tham

chiếu. TOGAF cung cấp hai mô hình tham chiếu là mô hình tham chiếu công nghệ và mô hình tham chiếu cơ sở hạ tầng thông tin tích hợp.

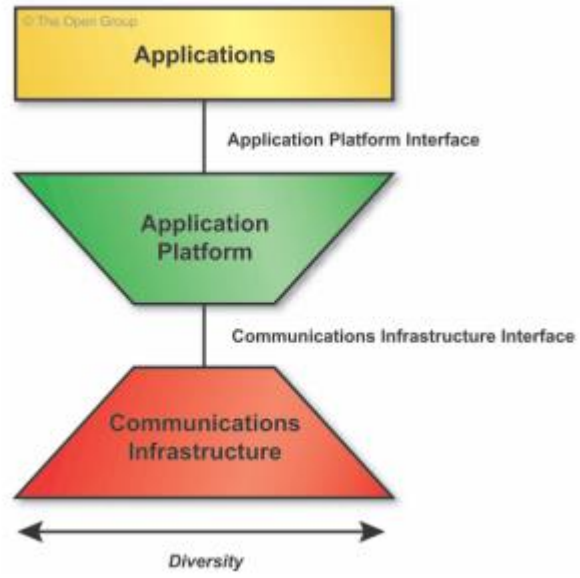
Mô hình tham chiếu công nghệ (Technical Reference Model - TRM):

Mô hình tham chiếu công nghệ cung cấp cách mô tả mạch lạc, cách trình diễn trực quan các thành phần và cấu trúc khái niệm của một hệ thống thông tin. Mô hình tham chiếu công nghệ (Hình 1.12) gồm ba thành phần:

- Cơ sở hạ tầng truyền thông (Communications Infrastructure): Cung cấp các dịch vụ cơ bản để liên thông các hệ thống và các biện pháp kỹ thuật cơ bản để truyền dữ liệu một cách trong suốt.

- Nền tảng ứng dụng (Application Platform): Cung cấp phần "nền" cho các ứng dụng phần mềm.

- Các ứng dụng (Applications): Là các ứng dụng phần mềm xây dựng trên nền tảng ứng dụng. Các thành phần đều có các giao diện (Interface) để thực hiện giao tiếp với nhau.



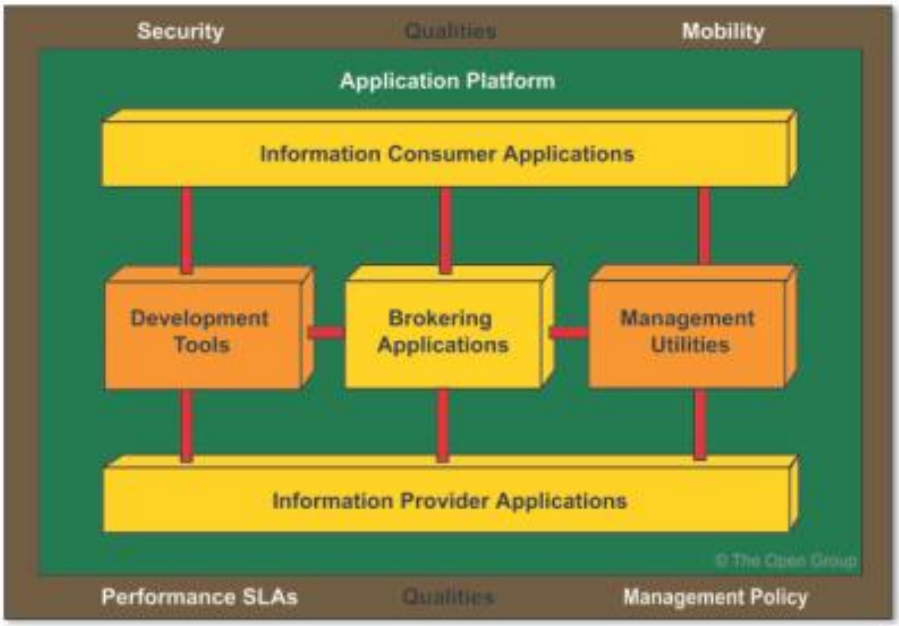
Hình 1.12: Mô hình tham chiếu công nghệ

Mô hình tham chiếu cơ sở hạ tầng thông tin tích hợp (Intergrated Information Infrastructure Reference Model – III- RM):

Mô hình tham chiếu cơ sở hạ tầng thông tin tích hợp cung cấp cách mô tả mạch lạc, cách trình diễn trực quan các thành phần và cấu trúc khái niệm của một

cơ sở hạ tầng thông tin tích hợp. Mô hình tham chiếu cơ sở hạ tầng thông tin tích hợp là một tập hợp các TRM trên phạm vi toàn cục nhưng cũng mở rộng một số phần của TRM trong các trường hợp cụ thể. Mô hình tham chiếu cơ sở hạ tầng thông tin tích hợp (Hình 1.13) gồm các thành phần sau:

- Các ứng dụng nghiệp vụ (Business Applications): Gồm ba loại:
  + Các ứng dụng trung gian (Brokering Applications)
  + Các ứng dụng cung cấp thông tin (Information Provider Applications)
  + Các ứng dụng thụ hưởng thông tin (Information Consumer Applications)
- Các ứng dụng hạ tầng (Infrastructure Applications): Gồm hai loại:
  + Các công cụ phát triển (Development Tools)
  + Các tiện ích quản lý (Management Utilities)
- Một nền tảng ứng dụng (Application Platform): cung cấp các dịch vụ hỗ trợ cho các ứng dụng ở trên như lưu trữ, luồng công việc, quản lý và trao đổi dữ liệu.
- Các giao diện (Interfaces) được sử dụng giữa các thành phần: Các interfaces bao gồm định dạng, giao thức, API…
- Chất lượng (Qualities): Qui định các chính sách, các yêu cầu về chất lượng.



Hình 1.13: Mô hình tham chiếu cơ sở hạ tầng thông tin tích hợp

TOGAF là phương pháp mang tính linh hoạt cao. TOGAF cho phép các giai đoạn được thực hiện không đầy đủ, có thể bỏ qua, kết hợp, sắp xếp lại, hoặc điều chỉnh lại các giai đoạn để phù hợp với nhu cầu của tình hình. Vì vậy, không nên ngạc nhiên nếu hai có 2 nhà tư vấn TOGAF khác nhau cho ra hai quá trình rất khác nhau, ngay cả khi làm việc với cùng một tổ chức. TOGAF thậm chí còn linh hoạt hơn về kiến trúc thực tế tạo ra. Kiến trúc được xây dựng tốt hay không tốt, hoạt động hiệu quả hay không hiệu quả phụ thuộc nhiều vào kinh nghiệm của nhân viên và tư vấn TOGAF. Tuy nhiên, điều này lại là yếu điểm của TOGAF bởi phương pháp này không chỉ ra cách làm thế nào xây dựng một kiến trúc tốt, cho nên kết quả có thể không như mong muốn. Bởi vậy, một tổ chức, đơn vị muốn áp dụng phương pháp TOGAF cần phải có những tiêu chí lựa chọn nhất định.

1.3.3. Khung kiến trúc ITI-GAF

Các nghiên cứu của các tổ chức quốc tế nổi tiếng và có uy tín khác nhau bao gồm Standish, Gartner ... đã chỉ ra rằng tỷ lệ thất bại của các dự án triển khai công nghệ thông tin là rất cao. Các nguyên nhân hàng đầu của thất bại không phải là kỹ thuật, mà chủ yếu do quản lý yếu kém, hành chính, sự hiểu biết về mục tiêu dự án, liên kết sai giữa kinh doanh và công nghệ, lựa chọn sai công nghệ, cam kết của lãnh đạo và nhận thức của người sử dụng...

Được thôi thúc bởi những thực tế này, Chính phủ Mỹ đã phát triển các FEA dựa trên khung kiến trúc ZACHMAN, nhằm đưa ra một kế hoạch tổng thể hướng dẫn các bước triển khai dự án công nghệ thông tin từng bước một. Ngày nay, có nhiều khung kiến trúc Chính phủ, đó là phương pháp cơ bản để xây dựng kiến trúc doanh nghiệp của Chính phủ nhằm đảm bảo khả năng tương tác, giảm thiểu sự thất bại. Khung kiến trúc phổ biến nhất TOGAF do Tập đoàn Open Consortium xây dựng bằng cách thu thập những kinh nghiệm thực tiễn từ hàng nghìn dự án công nghệ thông tin của hơn 350 công ty trên toàn cầu. Đây là một khung kiến trúc rất có giá trị đối với thực tiễn triển khai công nghệ thông tin.

Chi phí dành cho các dự án kiến trúc doanh nghiệp cao tới hàng vài triệu đô la Mỹ (USD) cho mỗi Bộ. Đối với một tổ chức, doanh nghiệp, chi phí này không chỉ khó để có thể đáp ứng nổi. Sẽ là rất hữu ích để bắt đầu với một khung nhỏ và sau đó khi có đầy đủ các điều kiện hơn tổ chức, doanh nghiệp có thể xây dựng EA như là kiến trúc ban đầu bằng những công cụ tinh vi dựa trên khung này.

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.

ITI-GAF được xây dựng trên cơ sở mô hình ITI-GAF có các yếu tố sau đây:

- Một mô hình doanh nghiệp chung;
- Một mô hình đánh giá sự trưởng thành doanh nghiệp;
- Các tiêu chuẩn của phát triển doanh nghiệp và một lộ trình để thực hiện chúng;
- Khuyến nghị hành động và các dự án chủ chốt;
- Mô hình quản trị;
- Cơ chế tài chính.

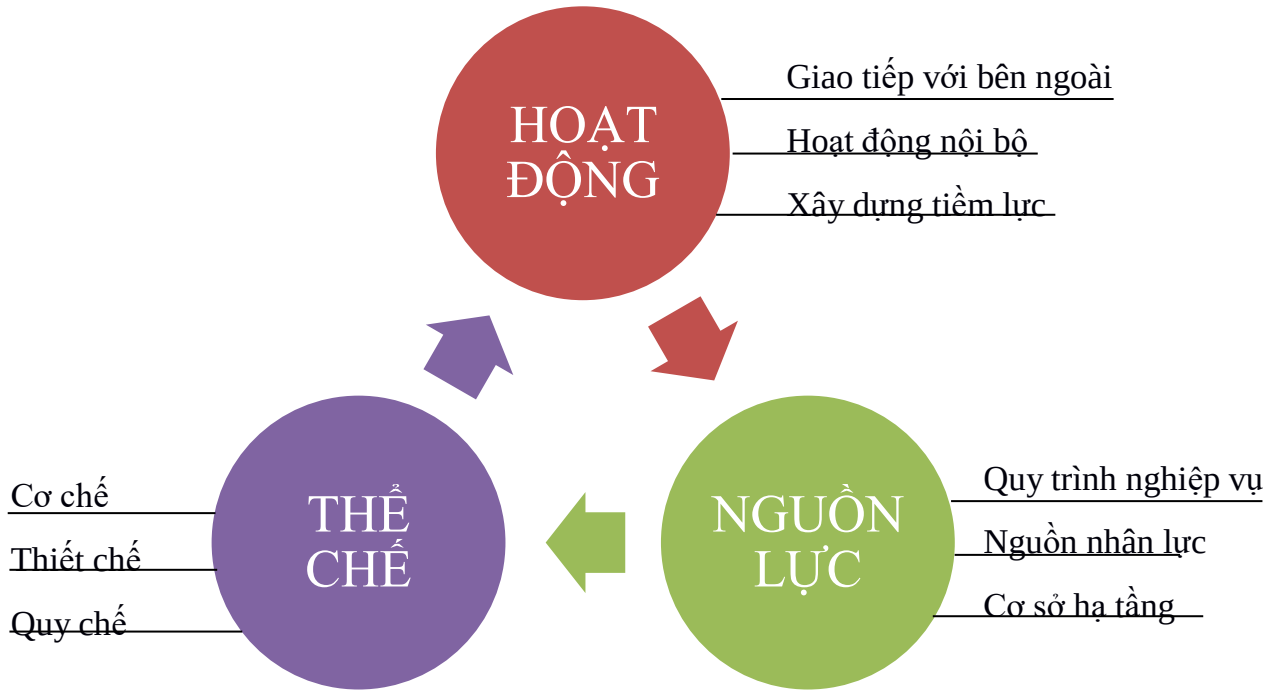
ITI-GAF đã được áp dụng thành công trong vài dự án tư vấn của Viện Công nghệ thông tin như mô hình Quốc hội điện tử, Mô hình cơ quan điện tử 3 cấp độ của Thành phố Hà Nội và hệ thống công nghệ thông tin của Cơ quan Quản lý

Dược phẩm và Mỹ phẩm Quốc gia. Dưới đây trình bày ngắn gọn các yếu tố đầu tiên của ITI-GAF:

Trong thiết kế hệ thống thực tế, phân tích các thành phần và hoạt động doanh nghiệp là rất quan trọng. Trong TOGAF, có một số bước phức tạp trong Phương pháp Phát triển kiến trúc (ADM) từ tầm nhìn đến hoạt động nghiệp vụ, hệ thống thông tin, ứng dụng, dữ liệu và kiến trúc công nghệ. Những phương pháp này được thiết kế cho các doanh nghiệp công nghệ thông tin và môi trường kinh doanh tiên tiến. Một số khái niệm trong phần này thì thực sự khó để tìm phần truy cập, điều này lại có ý nghĩa trong các môi trường thấp hơn.

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 1.14: 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.

Xây dựng các hoạt động nội bộ là để cơ quan hoạt động bước đầu. Về phương diện CNTT đó chính là bước Tin học hóa với các ứng dụng Văn phòng. Phối hợp hoạt động nội bộ tốt sẽ dẫn tới việc hoạt động với bên ngoài (quan hệ với các cơ quan ngoài hệ thống, với xã hội và quan hệ quốc tế) tốt. Bên cạnh các hoạt động mang tính nghiệp vụ, còn có các hoạt động mang tính hỗ trợ và xây dựng tiềm lực. Ba thành phần trong cách nhìn này có quan hệ chặt chẽ với nhau, thay đổi hoạt động trong một thành phần sẽ dẫn tới thay đổi trong các thành phần còn lại

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, ...

Trong cách nhìn này ba thành phần cũng có mối quan hệ hữu cơ với nhau: cơ chế là để phục vụ cho các hoạt động tạo ra sản phẩm. Các chế tài là để cơ cấu tổ chức có cơ sở pháp lý hoạt động có hiệu quả nhất. Cơ chế cũng cho phép tổ chức hoạt động có thể điều chỉnh để phục vụ tốt nhất cho hoạt động. Những cơ chế mới có thể dẫn tới các tổ chức mới cùng với các chế tài mới.

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

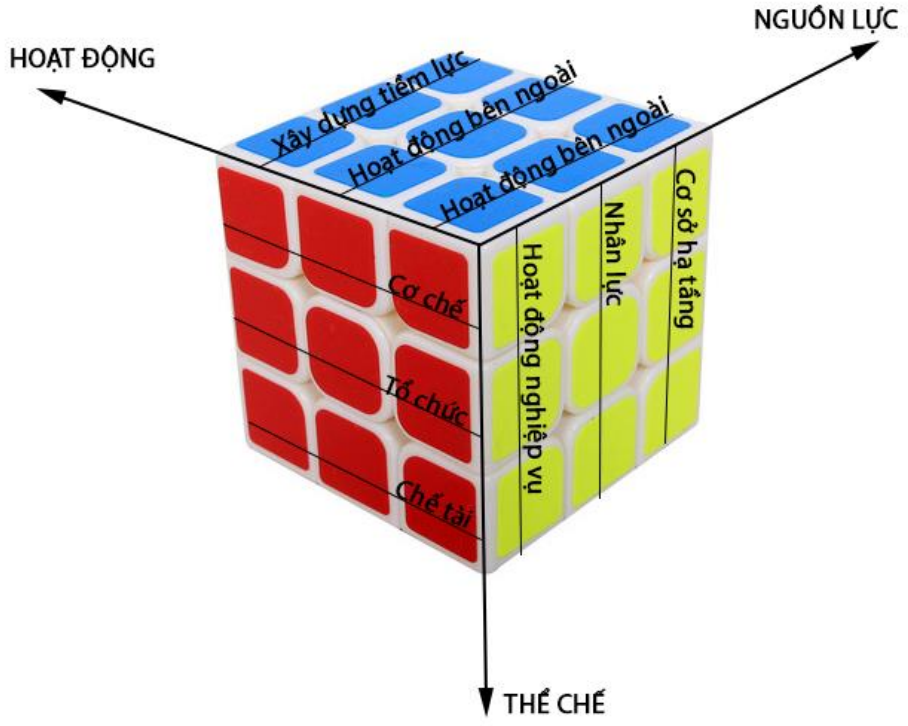
– *Hoạt động nghiệp vụ:* Đây là thế mạnh của doanh nghiệp và phải được thích nghi với sự thay đổi nhanh chóng của môi trường kinh doanh bằng cách tái cấu trúc liên tục, nhưng đôi khi không được hỗ trợ bởi các nguồn lực khác, vì không có cơ chế để thoát khỏi người không đủ năng lực cũng như các quy định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

Mối quan hệ giữa 3 thành phần của nguồn lực: nhân lực (con người) cần có cơ sở hạ tầng mới thực hiện được các yêu cầu nghiệp vụ mới. Con người cần có năng lực nghiệp vụ đáp ứng yêu cầu cải cách hành chính thay đổi quy trình nghiệp vụ và năng lực vận hành cơ sở hạ tầng ngày một hiện đại. Ứng dụng công nghệ hiện đại cho phép cải cách quy trình nghiệp vụ theo hướng tốt hơn. Nhờ các mối quan hệ trên, bất cứ một thay đổi nào trong mỗi thành phần cũng sẽ kéo theo thay đổi trong các thành phần còn lại. Quy hoạch trong một thành phần sẽ kéo theo quy hoạch trong các thành phần còn lại. Nếu không có quy hoạch, ba thành phần này sẽ dễ có nguy cơ không đồng bộ tạo ra lãng phí tiền bạc, thời gian hoặc cơ hội phát triển.

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 1.15: Mô hình 3x3x3

Thể chế / Nguồn lực-Hoạt động	Cơ chế	Tổ chức	Chế tài
Hoạt động nghiệp vụ với bên ngoài	Cơ chế hoạt động nghiệp vụ với bên ngoài	Tổ chức hoạt động nghiệp vụ với bên ngoài	Chế tài hoạt động nghiệp vụ với bên ngoài
Hoạt động nghiệp vụ nội bộ	Cơ chế hoạt động nghiệp vụ nội bộ	Tổ chức hoạt động nghiệp vụ nội bộ	Chế tài hoạt động nghiệp vụ nội bộ
Hoạt động nghiệp vụ xây dựng tiềm lực	Cơ chế hoạt động nghiệp vụ xây dựng tiềm lực	Tổ chức hoạt động nghiệp vụ xây dựng tiềm lực	Chế tài hoạt động nghiệp vụ xây dựng tiềm lực
Nhân lực hoạt động bên ngoài	Cơ chế đối với nhân lực bên ngoài	Tổ chức đối với nhân lực bên ngoài	Chế tài đối với nhân lực bên ngoài
Nhân lực hoạt động nội bộ	Cơ chế đối với nhân lực nội bộ	Tổ chức đối với nhân lực nội bộ	Chế tài đối với nhân lực nội bộ
Nhân lực hoạt động xây dựng tiềm lực	Cơ chế xây dựng tiềm lực về nguồn nhân lực	Tổ chức xây dựng tiềm lực về nguồn nhân lực	Chế tài xây dựng tiềm lực về nguồn nhân lực
Cơ sở hạ tầng bên ngoài	Cơ chế xây dựng cơ sở hạ tầng bên ngoài	Tổ chức xây dựng cơ sở hạ tầng bên ngoài	Chế tài xây dựng cơ sở hạ tầng bên ngoài
Cơ sở hạ tầng nội bộ	Cơ chế xây dựng cơ sở hạ tầng nội bộ	Tổ chức xây dựng cơ sở hạ tầng nội bộ	Chế tài xây dựng cơ sở hạ tầng nội bộ
Cơ sở hạ tầng xây dựng tiềm lực	Cơ chế xây dựng tiềm lực về cơ sở hạ tầng	Tổ chức xây dựng tiềm lực về cơ sở hạ tầng	Chế tài xây dựng tiềm lực về cơ sở hạ tầng

Bảng 1.1: 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….;

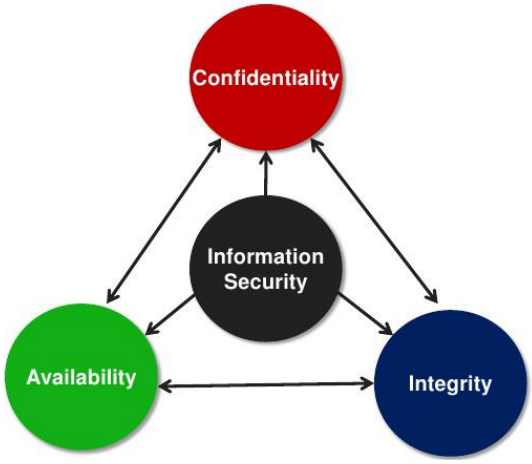
- An toàn thông tin cho các tài sản phần mềm: cơ sở dữ liệu, hệ điều hành, các phần mềm nghiệp vụ…;

- 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.



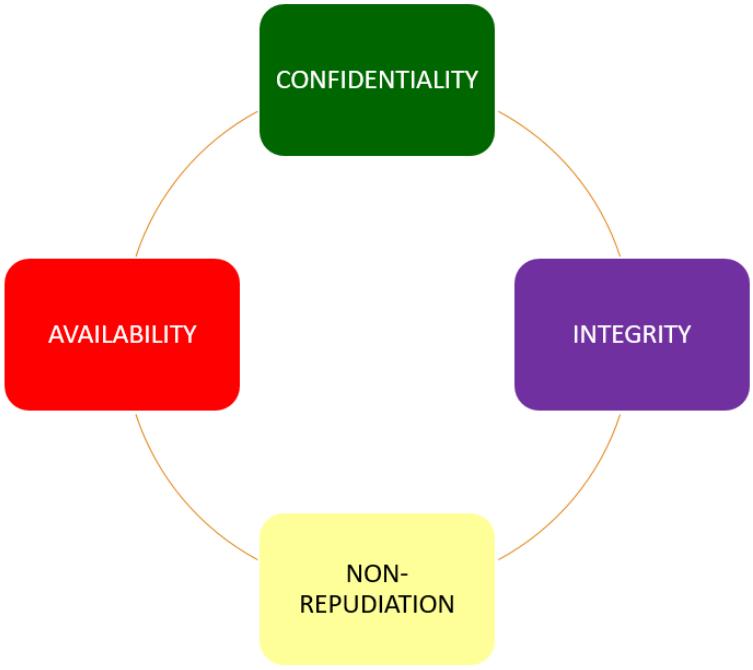
Hình 2.1: Mô hình tam giác an toàn thông tin CIA

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).



Hình 2.2: Các thuộc tính của an toàn thông tin

Tính không chối bỏ (Non-repudiation) phải có biện pháp giám sát, đảm bảo một đối tượng khi tham gia trao đổi thông tin thì không thể từ chối, phủ nhận việc mình đã phát hành hay sửa đổi thông tin.

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

Theo Cục An toàn thông tin – Bộ Thông tin và Truyền thông, qua khảo sát, đánh giá an toàn thông tin mạng một số cơ quan, doanh nghiệp trong thời gian qua ghi nhận một số đơn vị đã có sự quan tâm, đầu tư cho công tác đảm bảo an toàn thông tin mạng, bước đầu áp dụng các tiêu chuẩn kỹ thuật về an toàn thông tin; triển khai các thiết bị bảo vệ, phát hiện, cảnh báo xâm nhập; thành lập đơn vị quản trị hệ thống kiêm đảm bảo an toàn thông tin mạng. Tuy nhiên, tại hầu hết các đơn vị được kiểm tra đều phát hiện hệ thống mạng có lỗ hổng bảo mật, bị tấn công xâm nhập, chiếm đoạt thông tin, tài liệu, nhiều máy chủ và hệ thống thông tin quan trọng bị kiểm soát, gây nguy cơ tấn công mạng rất nghiêm trọng như: kiểm soát toàn bộ các liên lạc nội bộ qua thư điện tử, chiếm đoạt dữ liệu quan trọng trên máy tính và hệ thống mạng nội bộ; biến các máy tính, điện thoại thông minh bị kiểm soát trở thành thiết bị gián điệp, bí mật ghi âm, ghi hình.

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.

2.2.2. Hoạt động tấn công mạng vào các tổ chức, doanh nghiệp thời gian qua

Trong thời gian qua, hoạt động tấn công mạng vào các tổ chức, doanh nghiệp Việt Nam có sự gia tăng mạnh cả về số lượng và mức độ nguy hiểm, xuất hiện ngày càng nhiều cuộc tấn công có quy mô lớn nhằm vào mục tiêu quan trọng, kể cả những đơn vị được đầu tư mạnh về bảo đảm an toàn thông tin. Cụ thể:

* Vụ tấn công vào Công ty Cổ phần Truyền thông Việt Nam (VCCorp): Vụ tấn công bắt đầu vào đêm 12, rạng sáng 13/10/2014, hệ thống các trang web do VCCorp phụ trách dữ liệu và kỹ thuật, bao gồm những website được nhiều người biết đến như Dân trí, Kênh 14, Vneconomy, CafeF, Người lao động và trang web bán hàng như Muachung…đều không thể truy cập được và thông báo "lỗi bảo trì hệ thống", "505 – service unavailable". Qua kiểm tra, quản trị hệ thống phát hiện tình trạng các dịch vụ bị dừng trên hàng loạt máy chủ, một số máy chủ đã dừng hoạt động hoàn toàn, không thể truy cập do đã bị xóa dữ liệu trên ổ cứng. Theo số liệu thống kê: tổng số máy chủ bị chiếm quyền điều khiển và xóa dữ liệu là khoảng 900 máy, dẫn đến các dịch vụ trực tuyến được các công ty thuê đặt tại VDC.

Chiều ngày 15/10, VCCorp đã thông báo tất cả các báo điện tử đối tác và website của VCCorp mới hoạt động bình thường trở lại, các dữ liệu cũ cũng đã được phục hồi. Thế nhưng, đến sáng 18/10/2014, tình trạng các trang dantri.com.vn và một số website khác của VCCorp tiếp tục bị tấn công vào máy chủ Web và máy chủ lưu trữ khiến đồng thời chuyển hướng truy cập của các website này sang một blog. Theo thống kê trung bình có khoảng hơn 6 triệu truy cập của người dùng đã không thể sử dụng các dịch vụ chạy trên các máy chủ này

như tin tức, giao dịch trực tuyến…Qua phân tích sơ bộ cho thấy, nhiều khả năng đối tượng đã chiếm được quyền điều khiển các máy chủ từ trước, chỉnh sửa mã nguồn hệ thống, sau đó toàn bộ hệ thống sẽ tự động thực hiện cuộc tấn công khi đến thời điểm định trước. Đây là vụ việc tấn công hệ thống máy chủ quy mô lớn nhất từ trước đến thời điểm đó nhằm vào một đơn vị chuyên về cung cấp dịch vụ công nghệ thống tin , khiến hàng loạt trang tin, truyền hình trực tuyến, thương mại điện tử, cổng thanh toán trực tuyến lớn bị dừng hoạt động, gây hậu quả vô cùng nghiêm trọng.

* Trang web Google Việt Nam (google.com.vn) bị tấn công: Ngày 23/02/2015, trang Web tìm kiếm Google Việt Nam xuất hiện thông báo đã bị tấn công bởi nhóm hacker Lizard Squad. Ngay sau khi phát hiện sự cố, Google đã chặn hướng truy cập tới website nhằm sửa lỗi và khắc phục. Hậu quả là trong gần một ngày, người dùng không thể kết nối tới trang google.com.vn để tìm kiếm thông tin.

* Hơn 50.000 tài khoản VNPT bị công khai thông tin: Ngày 12/3/2015 nhóm hacker DIE Group đã tiến hành khai thác lỗ hổng SQL Injection của môđun tra cứu thông tin khách hàng trên một máy chủ cũ tại chi nhánh VNPT Sóc Trăng và công bố thông tin 50.000 tài khoản VNPT. Thông tin tài khoản bị công khai bao gồm: mã số khách hàng, họ tên, địa chỉ, số điện thoại (di động và cố định)...

* Tấn công mạng vào ngân hàng TPBank: Ngày 15/5, Ngân hàng Thương mại Cổ phần Tiên Phong (TPBank), thông báo đã từ chối yêu cầu chuyển hơn 1 triệu euro (1,13 triệu USD) vào cuối năm 2015. Yêu cầu chuyển tiền này đến từ một dịch vụ của bên thứ ba mà các ngân hàng sử dụng để kết nối với hệ thống tin nhắn liên ngân hàng SWIFT, TPBank đã nhanh chóng phát hiện ra lỗi này, chặn đứng việc chuyển tiền đến nhóm tội phạm. TPBank cũng cho biết có thể phần mềm độc hại (malware) đã được cài đặt vào ứng dụng mà bên thứ ba sử dụng.

* Việt nam Airline bị tấn công: Tin tặc nước ngoài đã thực hiện một cuộc tấn công có chủ đích (APT) vào hệ thống mạng của Tổng công ty Hàng không Việt Nam (VNA), hãng hàng không Vietjet, Jetstar và các cảng hàng không quốc tế như Nội Bài, Tấn Sơn Nhất, Phú Quốc. Tin tặc đã chiếm quyền điều khiển, hiển thị hình ảnh biểu tượng của nhóm tin tặc 1937CN kèm theo thông điệp xúc phạm Việt Nam và Philippin liên quan đến vấn đề Biển Đông lên trang điện tử chính

thức Vietnamairlines.com và 04 website khác của VNA; thông tin của 411000 khách hàng thường xuyên của VNA bị đánh cắp, công bố trên mạng Internet; nhiều máy chủ quản lý, máy chủ cơ sở dữ liệu thông tin chuyến bay của các cảng bị xóa hoặc mã hóa dữ liệu. Hơn 100 máy tính phục vụ check-in và màn hình hiển thị các chuyến bay bị kiểm soát, hiện thị hình ảnh phát tán nội dung xuyên tạc. Hậu quả để lại là uy tín của Viet Nam Airline bị ảnh hưởng nghiêm trọng, hơn 100 chuyến bay và hàng nghìn hành khách bị chậm vì tin tặc tấn công, nhà chức trách phải tắt toàn bộ mạng nội bộ, nhân viên làm thủ tục check in bằng tay thay vì máy và Việt Nam Airline xin lỗi khách hàng sau sự cố.

* Tấn công từ chối dịch vụ sử dụng các thiết bị IoTs: Tháng 6/2016, hãng bảo mật securi phát hiện "mạng máy tính ma" khổng lồ, khai thác lỗ hổng bảo mật, chiếm quyền điều khiển của 25.513 camera CCTV của 105 quốc gia, trong đó có trên 5000 camera CCTV của Việt Nam bị chiếm quyền điều khiển và tham gia hoạt động tấn công DdoS quy mô lớp và hệ thống mạng quốc gia trên thế giới và cả hệ thống mạng Việt Nam.

* Tấn công vào ngân hàng Vietcombank: Đầu tháng 8/2016, khách hàng của Vietcombank bỗng dưng bị người khác chuyển 500 triệu đồng từ tài khoản của mình sang tài khoản khác chỉ sau một đêm. Nguyên nhân của vụ việc nhiều khả năng khách hàng đã bị tội phạm lừa đảo lấy thông tin mã kích hoạt dịch smart OTP (tin nhắn thông báo mã OTP kích hoạt dịch vụ Smart OTP đã được gửi tới khách hàng) để sử dụng thực hiện các giao dịch chuyển khoản qua thẻ và tài khoản ngân hàng khác.

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).

2.3.2. Cấu trúc của tiêu chuẩn TCVN ISO/IEC 27002:2011

STT	Nội dung
1.	**Phạm vi áp dụng**
2.	**Phạm vi áp dụng**
3.	**3. Đánh giá và xử lý rủi ro**
3.1.	Đánh giá rủi ro an toàn thông tin
3.2.	Xử lý các rủi ro an toàn thông tin
4.	**Chính sách an toàn thông tin**
4.1.	Chính sách an toàn thông tin
5.	**Tổ chức đảm bảo an toàn thông tin**
5.1.	Tổ chức nội bộ
5.2.	Các bên tham gia bên ngoài
6.	**Quản lý tài sản**
6.1.	Trách nhiệm đối với tài sản
6.2.	Phân loại thông tin

7.	**Đảm bảo an toàn thông tin từ nguồn nhân lực**
7.1.	Trước khi tuyển dụng
7.2.	Trong thời gian làm việc
7.3.	Chấm dứt hoặc thay đổi công việc
8.	**Đảm bảo an toàn vật lý và môi trường**
8.1.	Các khu vực an toàn
8.2.	Đảm bảo an toàn trang thiết bị
9.	**Quản lý truyền thông và vận hành**
9.1.	Các trách nhiệm và thủ tục vận hành
9.2.	Quản lý chuyển giao dịch vụ của bên thứ ba
9.3.	Lập kế hoạch và chấp nhận hệ thống
9.4.	Bảo vệ chống lại mã độc hại và mã di động
9.5.	Sao lưu
9.6.	Quản lý an toàn mạng
9.7.	Xử lý phương tiện
9.8.	Trao đổi thông tin
9.9.	Các dịch vụ thương mại điện tử
9.10.	Giám sát
10.	**Quản lý truy cập**
10.1.	Yêu cầu nghiệp vụ đối với quản lý truy cập
10.2.	Quản lý truy cập người dùng
10.3.	Các trách nhiệm của người dùng
10.4.	Quản lý truy cập mạng
10.5.	Quản lý truy cập hệ điều hành
10.6.	Điều khiển truy cập thông tin và ứng dụng

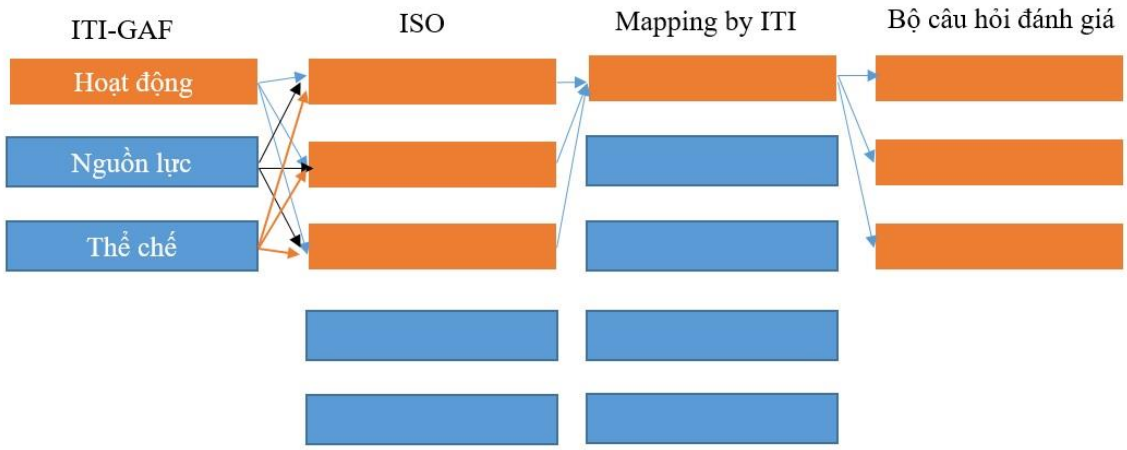
10.7.	Tính toán di động và làm việc từ xa
11.	**Tiếp nhận, phát triển và duy trì các hệ thống thông tin**
11.1.	Yêu cầu đảm bảo an toàn cho các hệ thống thông tin
11.2.	Xử lý đúng trong các ứng dụng
11.3.	Quản lý mã hóa
11.4.	An toàn cho các tệp tin hệ thống
11.5.	Bảo đảm an toàn trong các quy trình hỗ trợ và phát triển
11.6.	Quản lý các điểm yếu kỹ thuật
12.	**Quản lý các sự cố an toàn thông tin**
12.1.	Báo cáo về các sự kiện an toàn thông tin và các điểm yếu
12.2.	Quản lý các sự cố an toàn thông tin và cải tiến
13.	**Quản lý sự liên tục của hoạt động nghiệp vụ**
13.1.	Các khía cạnh an toàn thông tin trong quản lý sự liên tục của hoạt động nghiệp vụ
14.	**Sự tuân thủ**
14.1.	Sự tuân thủ các quy định pháp lý
14.2.	Sự tuân thủ các chính sách và tiêu chuẩn an toàn, và tương thích kỹ thuật
14.3.	Xem xét việc đánh giá các hệ thống thông tin
	Thư mục tài liệu tham khảo

Bảng 2.1: Cấu trúc tiêu chuẩn TCVN ISO/IEC 27002:2011

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

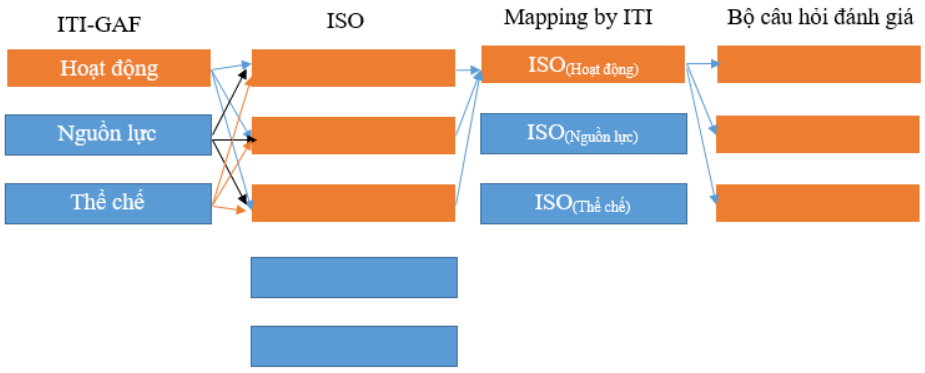
Hình 3.1 mô tả các bước để xây dựng mô hình đánh giá an toàn thông tin của tổ chức, doanh nghiệp. Các quan điểm về hoạt động, nguồn lực và thể chế được của tổ chức được ánh xạ đến các điểm, yêu cầu của các tiêu chuẩn về an ninh, an toàn thông tin và phân cụm các tiêu chuẩn đó thành các cụm là các thành 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

Trong mô hình này, chúng ta phải phải giải quyết 03 nhóm câu hỏi lớn sau:

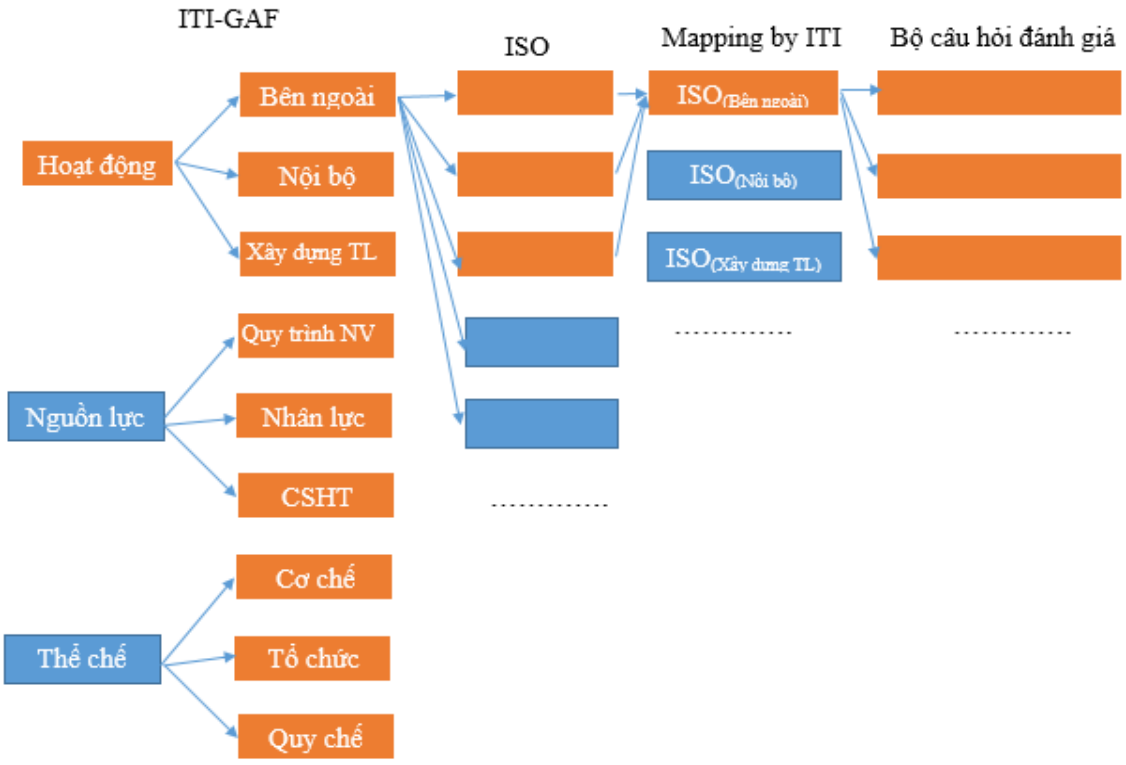
– An toàn thông tin cho các hoạt động của tổ chức, doanh nghiệp, đây chính là việc đảm bảo an toàn thông tin cho các hoạt động của tổ chức như các hoạt động giao tiếp, hoạt động xây dựng tổ chức.

– An toàn thông tin cho thể chế của tổ chức, doanh nghiệp, là xây dựng có chế chính sách của tổ chức cho việc đảm bảo an toàn thông tin của tổ chức.

– An toàn thông tin cho nguồn lực doanh nghiệp, là việc xây dựng nguồn nhân lực, cơ sở hạ tầng cũng như các quy trình nghiệp vụ của tổ chức.

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

Trong mô hình này, chúng ta phải hỏi 09 nhóm câu hỏi sau:

– Bảo đảm an toàn thông tin cho các hoạt động giao tiếp với bên ngoài của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho các hoạt động giao tiếp trong nội bộ tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho các hoạt động xây dựng tiềm lực của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho các hoạt động nghiệp vụ của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho nguồn nhân lực của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho cơ sở hạ tầng của tổ chức, doanh nghiệp.

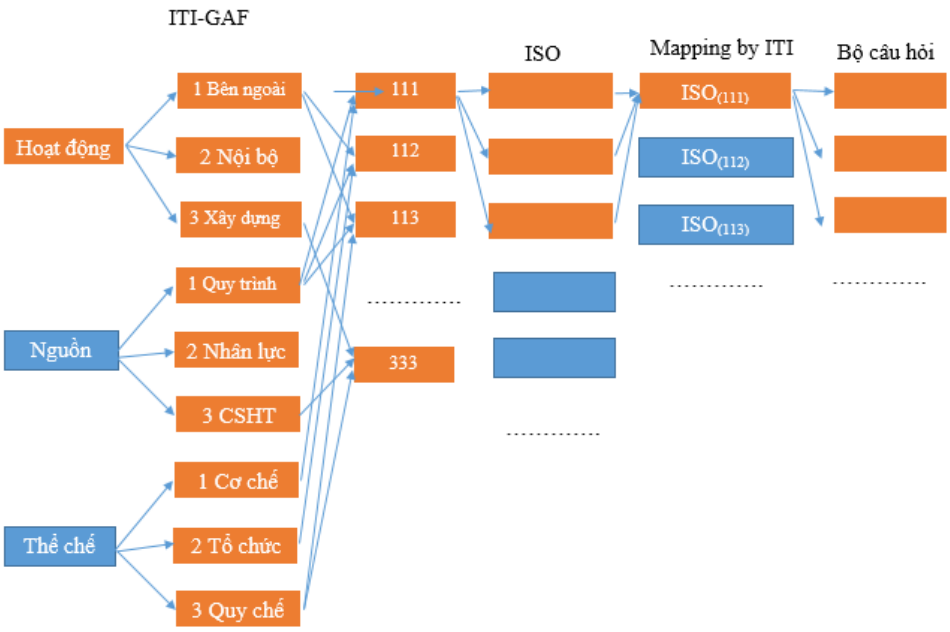
– Bảo đảm an toàn thông tin cho các cơ chế của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho các tổ chức của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin đối với các chế tài của tổ chức, doanh nghiệp.

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

Trong mô hình này, chúng ta phải hỏi 27 nhóm câu hỏi sau:

– Bảo đảm an toàn thông tin cho cho cơ chế hoạt động nghiệp vụ với bên ngoài của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho tổ chức hoạt động nghiệp vụ với bên ngoài của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho chế tài hoạt động nghiệp vụ với bên ngoài của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho cơ chế hoạt động nghiệp vụ nội bộ của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho tổ chức hoạt động nghiệp vụ nội bộ của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho chế tài hoạt động nghiệp vụ nội bộ của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho cơ chế hoạt động nghiệp vụ xây dựng tiềm lực của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho tổ chức hoạt động nghiệp vụ xây dựng tiềm lực của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho chế tài hoạt động nghiệp vụ xây dựng tiềm lực của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho cơ chế đối với nhân lực bên ngoài của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho tổ chức đối với nhân lực bên ngoài của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho chế tài đối với nhân lực bên ngoài của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho cơ chế đối với nhân lực nội bộ của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho tổ chức đối với nhân lực nội bộ của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho chế tài đối với nhân lực nội bộ của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho cơ chế xây dựng tiềm lực về nguồn nhân lực của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho tổ chức xây dựng tiềm lực về nguồn nhân lực của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho chế tài xây dựng tiềm lực về nguồn nhân lực của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho cơ chế xây dựng cơ sở hạ tầng bên ngoài của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho tổ chức xây dựng cơ sở hạ tầng bên ngoài của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho chế tài xây dựng cơ sở hạ tầng bên ngoài của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho cơ chế xây dựng cơ sở hạ tầng nội bộ của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho tổ chức xây dựng cơ sở hạ tầng nội bộ của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho chế tài xây dựng cơ sở hạ tầng nội bộ của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho cơ chế xây dựng tiềm lực về cơ sở hạ tầng của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho tổ chức xây dựng tiềm lực về cơ sở hạ tầng của tổ chức, doanh nghiệp.

– Bảo đảm an toàn thông tin cho chế tài xây dựng tiềm lực về cơ sở hạ tầng của tổ chức, doanh nghiệp.

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 được thể hiện như bảng dưới đây:

STT	Trọng số ITI	Thể chế	Nguồn lực	Hoạt động	Nội dung
1.	111	Cơ chế	Quy trình nghiệp vụ	Bên ngoài	−Thương mại điện tử (C9.9.1) −Xác định các rủi ro liên quan đến các bên tham gia bên ngoài (C5.2.1) −Giải quyết an toàn khi làm việc với khách hàng (C5.2.2) −Giải quyết an toàn trong các thỏa thuận với bên thứ ba (C5.2.3)
2.	112	Cơ chế	Quy trình nghiệp vụ	Nội bộ	−Hướng dẫn phân loại thông tin (C6.2.1) −Gán nhãn và xử lý thông tin (C6.2.2) −Phân tích và đặc tả các yêu cầu về an toàn (C11.1.1) −Kiểm tra tính hợp lệ của dữ liệu đầu vào (C11.2.1) −Kiểm soát việc xử lý nội bộ (C11.2.2) −Tính toàn vẹn thông điệp (C11.2.3) −Các thủ tục quản lý thay đổi (C11.5.1) −Sự rò rỉ thông tin(C11.5.4) −Quản lý thay đổi (9.1.2) −Quản lý thay đổi đối với các dịch vụ của bên thứ ba (C9.2.3) −Giám sát sử dụng hệ thống (C9.10.2)

					−Các trách nhiệm và thủ tục (C12.2.1) −Thu thập chứng cứ (C12.2.3) −Tính đến an toàn thông tin trong quản lý sự liên tục của hoạt động nghiệp vụ (C13.1.1) −Ngăn chặn việc lạm dụng phương tiện xử lý thông tin(C14.1.5) −Các biện pháp quản lý kiểm toán các hệ thống thông tin (C14.3.1) −Quy trình trao quyền cho phương tiện xử lý thông tin (C5.1.4) −Các thỏa thuận về bảo mật (C5.1.5) −Liên lạc với những cơ quan/tổ chức có thẩm quyền (C5.1.6) −Liên lạc với các nhóm chuyên gia (C5.1.7) −Tự soát xét về an toàn thông tin (C5.1.8)
3.	113	Cơ chế	Quy trình nghiệp vụ	Xây dựng tiềm lực	−Kiểm tra tính hợp lệ của dữ liệu đầu ra (C11.2.4) −Quản lý các điểm yếu về kỹ thuật (C11.6.1) −Giám sát và soát xét các dịch vụ của bên thứ ba (C9.2.2) −Đánh giá rủi ro và sự liên tục trong hoạt động của tổ chức (C13.1.2) −Xây dựng và triển khai các kế hoạch về tính liên tục, trong đó bao gồm vấn đề đảm bảo an toàn thông tin (C13.1.3) −Khung hoạch định sự liên tục trong hoạt động nghiệp vụ (C13.1.4) −Kiểm tra, duy trì và đánh giá các kế hoạch đảm bảo sự liên tục trong hoạt động của tổ chức (C13.1.5) −Quyền sở hữu trí tuệ (IPR) (C14.1.2)
4.	121	Cơ chế	Nguồn nhân lực	Bên ngoài	

5.	122	Cơ chế	Nguồn nhân lực	Nội bộ	−Thẩm tra (C7.1.2) −Hủy bỏ quyền truy cập (C7.3.3) −Trách nhiệm của ban quản lý (C7.2.1) −Xử lý kỷ luật (C7.2.3) −Quản lý mật khẩu người dùng (C10.2.3) −Soát xét các quyền truy cập của người dùng (C10.2.4) −Sử dụng mật khẩu (C10.3.1) −Phân tách nhiệm vụ (9.1.3)
6.	123	Cơ chế	Nguồn nhân lực	Xây dựng tiềm lực	−Nhận thức, giáo dục và đào tạo về an toàn thông tin (C7.2.2) −Đăng ký thành viên(C10.2.1) −Quản lý đặc quyền (C10.2.2)
7.	131	Cơ chế	Cơ sở hạ tầng	Bên ngoài	
8.	132	Cơ chế	Cơ sở hạ tầng	Nội bộ	−Kiểm kê tài sản (C6.1.1) −Quyền sở hữu tài sản (C6.1.2) −Kiểm soát cổng truy cập vật lý (C8.1.2) −Bảo dưỡng thiết bị (C8.2.4) −An toàn khi loại bỏ hoặc tái sử dụng thiết bị (C7.2.6) −Di dời tài sản (C8.2.7) −Quản lý truy cập đến mã nguồn chương trình (C11.4.3) −Phát triển phần mềm thuê khoán (C11.5.5) −Bàn giao tài sản (C7.3.2) −Các thiết bị không được quản lý (C10.3.2) −Xác thực người dùng cho các kết nối bên ngoài (C10.4.2) −Định danh thiết bị trong các mạng (C10.4.3) −Chuyển giao dịch vụ (C9.2.1) −Loại bỏ phương tiện (C9.7.2) −Các thủ tục xử lý thông tin (C9.7.3)

					−An toàn cho các tài liệu hệ thống (C9.7.4) −Báo cáo về các nhược điểm an toàn thông tin (C12.1.2) −Bảo vệ các hồ sơ của tổ chức (C14.1.3) −Bảo vệ các công cụ kiểm toán hệ thống thông tin (C14.3.2)
9.	133	Cơ chế	Cơ sở hạ tầng	Xây dựng tiềm lực	−Các tiện ích hỗ trợ (C8.2.2) −An toàn cho dây cáp (C8.2.3) −Quản lý các phần mềm điều hành (C11.4.1) −Bảo vệ dữ liệu kiểm tra hệ thống (C11.4.2) −Soát xét kỹ thuật các ứng dụng sau thay đổi của hệ thống điều hành (C11.5.2) −Hạn chế thay đối các gói phần mềm (C11.5.3) −Chuẩn đoán từ xa và bảo vệ cổng cấu hình (C10.4.4) −Phân tách trên mạng (C10.4.5) −Quản lý kết nối mạng (C10.4.6) −Quản lý định tuyến mạng (C10.4.7) −Các thủ tục đăng nhập an toàn (C10.5.1) −Định danh và xác thực người dùng (C10.5.2) −Hệ thống quản lý mật khẩu (C10.5.3) −Sử dụng các tiện ích hệ thống (C10.5.4) −Thời gian giới hạn của phiên làm việc (C10.5.5) −Giới hạn thời gian kết nối (C10.5.6) −Hạn chế truy cập thông tin (C10.6.1) −Cách ly hệ thống nhạy cảm (C10.6.2) −Tính toán và truyền thông qua thiết bị di động (C10.7.1)

					−Phân tách các chức năng phát triển, kiểm thử và vận hành (9.1.4) −Quản lý năng lực hệ thống (C9.3.1) −Chấp nhận hệ thống (C9.3.2) −Quản lý chống lại mã độc hại (C9.4.1) −Kiểm soát các mã di động (C9.4.2) −Sao lưu thông tin (C9.5) −Kiểm soát mạng (C9.6.1) −An toàn cho các dịch vụ mạng (C9.6.2) −Thông điệp điện tử (C9.8.4) −Các giao dịch trực tuyến (C9.9.2) −Thông tin công khai (C9.9.3) −Ghi nhật ký kiểm soát (C9.10.1) −Bảo vệ các thông tin nhật ký (C9.10.3) −Nhật ký của người điều hành và người quản trị (C9.10.4) −Ghi nhật ký lỗi (C9.10.5) −Đồng bộ thời gian (C9.10.6) −Báo cáo về các sự kiện an toàn thông tin (C12.1.1) −Rút bài học kinh nghiệm từ các sự cố an toàn thông tin (C12.2.2)
10.	211	Thiết chế	Quy trình nghiệp vụ	Bên ngoài	
11.	212	Thiết chế	Quy trình nghiệp vụ	Nội bộ	−Cam kết của ban quản lý về đảm bảo an toàn thông tin (5.1.1)
12.	213	Thiết chế	Quy trình nghiệp vụ		
13.	221	Thiết chế	Nguồn nhân lực	Bên ngoài	

14.	222	Thiết chế	Nguồn nhân lực	Nội bộ	−Phối hợp đảm bảo an toàn thông tin (C5.1.2) −Phân định trách nhiệm đảm bảo an toàn thông tin (C5.1.3)
15.	223	Thiết chế	Nguồn nhân lực	Xây dựng tiềm lực	
16.	231	Thiết chế	Cơ sở hạ tầng	Bên ngoài	−An toàn cho thiết bị hoạt động bên ngoài trụ sở của tổ chức (C8.2.5)
17.	232	Thiết chế	Cơ sở hạ tầng	Nội bộ	−Vành đai an toàn vật lý (C8.1.1) −Bảo vệ các văn phòng, phòng làm việc và vật dụng (C8.1.3) −Bảo vệ chống lại các mối đe dọa từ bên ngoài và từ môi trường (C8.1.4)
18.	233	Thiết chế	Cơ sở hạ tầng	Xây dựng tiềm lực	−Bố trí và bảo vệ thiết bị (C8.2.1)
19.	311	Quy chế	Quy trình nghiệp vụ	Bên ngoài	−Sự tuân thủ các tiêu chuẩn và chính sách an toàn (C14.2.1)
20.	312	Quy chế	Quy trình nghiệp vụ	Nội bộ	−Chính sách sử dụng các biện pháp quản lý mã hóa (C11.3.1) −Các thủ tục vận hành được ghi thành văn bản (C9.1.1) −Các chính sách và thủ tục trao đổi thông tin (C9.1.1) −Các thỏa thuận trao đổi (C9.8.1) −Các hệ thống thông tin nghiệp vụ (C9.8.5) −Bảo vệ dữ liệu và sự riêng tư của thông tin cá nhân (C14.1.4)
21.	313	Quy chế	Quy trình nghiệp vụ	Xây dựng tiềm lực	−Xác định các điều luật hiện đang áp dụng được (C14.1.1) −Quy định về quản lý mã hóa (C14.1.6) −Soát xét lại chính sách an toàn thông tin (C4.1.2)

22.	321	Quy chế	Nguồn nhân lực	Bên ngoài	
23.	322	Quy chế	Nguồn nhân lực	Nội bộ	−Các vai trò và trách nhiệm (C7.1.1) −Điều khoản và điều kiện tuyển dụng (C7.1.3) −Trách nhiệm kết thúc hợp đồng (C7.3.1) −Chính sách quản lý truy cập (C10.1)
24.	323	Quy chế	Nguồn nhân lực	Xây dựng tiềm lực	
25.	331	Quy chế	Cơ sở hạ tầng	Bên ngoài	−Các khu vực truy cập tự do, phân phối và chuyển hàng (C8.1.6) −Kiểm tra sự tương thích kỹ thuật (C14.2.2)
26.	332	Quy chế	Cơ sở hạ tầng	Nội bộ	−Làm việc trong các khu vực an toàn (C8.1.5) −Quản lý khóa (C11.3.2) −Chính sách màn hình sạch và bàn làm việc sạch (C10.3.2) −Chính sách sử dụng các dịch vụ mạng (C10.4.1) −Quản lý các phương tiện có thể di dời (C9.7.1) −Vận chuyển phương tiện vật lý (C9.8.3)
27.	333	Quy chế	Cơ sở hạ tầng	Xây dựng tiềm lực	−Sử dụng hợp lý tài sản (C6.1.3) −Làm việc từ xa (C10.7.2) −Tài liệu chính sách an toàn thông tin (C4.1.1)

Bảng 3.1: Phân cụm TCVN theo ITI-GAF

3.2.2. Xây dựng bộ câu hỏi đánh giá

Bộ câu hỏi đánh giá được xây dựng trên kết quả xây dựng trên nguyên tắc bộ câu hỏi sẽ bảo phủ hết nội dung của các tiêu chí của TCVN trong từng nhóm.

STT	Câu hỏi	Yes	No
1	Việc phân loại các mức độ đối với thông tin nghiệp vụ để đảm bảo an toàn thông tin trong nội bộ cơ quan đã được quy định hay chưa (C6.2.1)?		
2	Đã đưa ra các yêu cầu về an toàn đối với từng thành phần cụ thể trong hệ thống thông tin hay chưa (C11.1)?		
3	Có hay không các thủ tục rà soát tính đúng đắn của thông tin trong các hoạt động trao đổi thông tin (C11.2)?		
4	Có hay không các thủ tục kiểm soát và đánh giá sự thay đổi trong các thành phần và toàn bộ hệ thống thông tin (C9.1.2)?		
5	Có hay không việc thiết lập các thủ tục và phân công trách nhiệm nhằm đảm bảo xử lý sự cố về an toàn thông tin (C12.2.1)?		
6	Có hay không việc đưa các yêu cầu về an toàn thông tin vào trong quy trình quản lý hệ thống thông tin nhằm đảm bảo khả năng làm việc liên tục của hệ thống (C13.1.1)?		
7	Có hay không các thủ tục ngăn ngừa và giám sát khả năng sử dụng các phương tiện thông tin không đúng mục đích (C14.1.5)?		
8	Có hay không các yêu cầu và thỏa thuận về sở hữu thông tin và các phương tiện xử lý thông tin nhằm đảm bảo an toàn thông tin trong hệ thống (C5.1)?		

Bảng 3.2: Bộ câu hỏi với trọng số ITI là 112

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. Bộ Khoa học và Công nghệ (2010), *Đề tài "Nghiên cứu xây dựng kiến trúc Công nghệ thông tin & Truyền thông và các giải pháp công nghệ phù hợp cho việc triển khai Chính phủ điện tử ở Việt Nam"*, chương trình KH&CN trọng điểm cấp nhà nước, mã số KC.01/06-10
2. Nguyễn Minh Hồng (2010), *Nghiên cứu xây dựng kiến trúc công nghệ thông tin và truyền thông và các giải pháp công nghệ phù hợp cho việc triển khai Chính phủ điện tử ở Việt Nam,* Báo cáo tổng hợp Đề tài khoa học cấp Nhà nước mã số KC.01.18 ,Bộ Thông tin Truyền thông.
3. 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.
4. Viện CNTT – ĐHQG Hà Nội (2014), *Thuyết minh đề tài "Nghiên cứu xây dựng và thử nghiệm mô hình chứng thực điện tử văn bản pháp lý để thúc đẩy triển khai dịch vụ công trên địa bàn Thành phố Hà Nội"*, Đề tài nghiên cứu khoa học và phát triển công nghệ cấp thành phố, mã số 01C-07/02-2014-2.
5. 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

6. "Business Systems Planning and Business Information Control Study: A comparison". In:IBM Systems Journal, vol 21, no 3, 1982. p. 31-53.
7. 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.
8. J. A. Zachman (1987). "A Framework for Information Systems Architecture". In: IBM Systems Journal, vol 26, no 3. IBM Publication G321-5298.

9. The Open Group Architectural Framework, TOGAF 9.1 Online Documents (2012), URL: http://pubs.opengroup.org/architecture/togaf9-doc/arch/
10. National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (2014), URL: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
11. White House(2007), *FEA Consolidated Reference Model Document Version 2.3*, URL: http://www.whitehouse.gov/sites/default/files/omb/assets/fea_docs/FEA_CRM_v23_Final_Oct_2007_Revised.pdf
12. Roger Sessions(2007), *A Comparison of the Top Four Enterprise Architecture Methodologies*, ObjectWatch
13. USA (2013), *Federal Enterprise Architecture Framework, version 2.0*
14. The Open Group Architectural Framework, *TOGAF 9.1 Online Documents*, URL: http://pubs.opengroup.org/architecture/togaf9-doc/arch/

ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ
------🕮------

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

Hà Nội, ngày 26 tháng 11 năm 2016

QUYẾT NGHỊ
CỦA HỘI ĐỒNG CHẤM LUẬN VĂN THẠC SĨ

Căn cứ Quyết định số **981/QĐ-ĐT ngày 18 tháng 11 năm 2016** của Hiệu trưởng Trường Đại học Công nghệ về việc thành lập Hội đồng chấm luận văn thạc sĩ của học viên **Nguyễn Thanh Tuyền** ,Hội đồng chấm luận văn Thạc sĩ đã họp vào hồi 13h, thứ 7, ngày 26 tháng 11 năm 2016, tại Phòng 304, Nhà G2, Trường Đại học Công nghệ, ĐHQGHN.

Tên đề tài luận văn: **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:

Sau khi nghe học viên trình bày tóm tắt luận văn Thạc sĩ, các phản biện đọc nhận xét, học viên trả lời các câu hỏi, Hội đồng đã họp, trao đổi ý kiến và thống nhất kết luận:

1..Về tính cấp thiết, tính thời sự, ý nghĩa lý luận và thực tiễn của đề tài luận văn:

Đề tài có tính thời sự, có ý nghĩa lý luận và thực tiễn cao

2..Về bố cục, phương pháp nghiên cứu, tài liệu tham khảo, ... của luận văn:

Bố cục của luận văn hợp lý
phương pháp nghiên cứu phù hợp
Tài liệu tham khảo đầy đủ

3..Về kết quả nghiên cứu:

Nghiên cứu về quản trị rủi ro, về hệ thống chỉ số đo an toàn thông tin theo tiêu chuẩn ISO 27001.
Áp dụng ISO 27001 vào các bài toán thực tiễn;

đề xuất các mô hình (đơn giản, trung gian, nâng cao), khung tiêu chuẩn đảm bảo an toàn lưới điện

4. **Hạn chế của luận văn** *(nếu có)*:

- Đề xuất khung tiêu chuẩn chưa được nhiều nội dung
- chưa chỉ ra được khung tiêu chuẩn nào phù hợp với các tỉnh được đoàn giúp ở VN.

5. **Đánh giá chung và kết luận:**

Luận văn đáp ứng được yêu cầu của luận văn thạc sĩ ngành năng, đề nghị cấp bằng Thạc sĩ cho học viên.

Luận văn đạt 7.7 10 điểm. Quyết nghị này được 5 / 5 thành viên của Hội đồng nhất trí thông qua.

THƯ KÝ HỘI ĐỒNG

TS. Lê Đức

CHỦ TỊCH HỘI ĐỒNG

PGS. TS. Nguyễn Ngọc Hoà

XÁC NHẬN CỦA CƠ SỞ ĐÀO TẠO

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

BẢN NHẬN XÉT PHẢN BIỆN LUẬN VĂN THẠC SĨ

Họ và tên cán bộ phản biện: Trần Trọng Hiếu

Học hàm, học vị: TS.

Chuyên ngành: Công nghệ thông tin

Cơ quan công tác: Khoa CNTT, Trường ĐH Công nghệ, ĐHQGHN

Họ và tên học viên cao học: Nguyễn Thanh Tuyền

Tên đề tài luận văn: Áp dụng Enterprise Architecture xây dựng khung kiến thức trúc bảo đảm an toàn thông tin cho các tổ chức doanh nghiệp tại Việt Nam

Chuyên ngành: Quản lý Hệ thống thông tin Mã số:

Ý KIẾN NHẬN XÉT

- Việc đảm bảo an toàn thông tin cho các tổ chức, doanh nghiệp tại Việt Nam là vấn đề cấp thiết hiện nay nhất là sau khi các trang web của của chính phủ bị tấn công và các vụ bị rút trộm tiền từ các hệ thống ngân hàng. Xây dựng các chính sách và các kiến trúc làm chuẩn chung cho sự phát triển của các hệ thống thông tin là vấn đề cấp bách hiện nay.
- Luận văn đã tập trung nghiên cứu ứng dụng enterprise architecture nhằm xây dựng các hệ thống thông tin an toàn. Đây là đề tài nghiên cứu có tính thực tiễn cao.
- Luận văn đã đề xuất khung kiến trúc đảm bảo an toàn thông dựa trên mô hình ITI-GAF. Tuy nhiên nội dung mới dừng lại ở mức mô tả mà chưa có các phân tích và luận giải đầy đủ, chi tiết về các thành phần của khung kiến trúc này.
- Về hình thức, khóa luận đã được trình bày một cách rõ ràng, bố cục chặt chẽ theo đúng văn phong khoa học.

Tóm lại, luận văn đáp ứng các yêu cầu về nội dung và hình thức của một luận văn thạc sĩ Công nghệ thông tin. Đề nghị cho học viên được bảo vệ trước Hội đồng.

Hà Nội, ngày 22 tháng 11 năm 2016

XÁC NHẬN CỦA CƠ QUAN CÔNG TÁC **CÁN BỘ PHẢN BIỆN**

Trần Trọng Hiếu

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

BẢN NHẬN XÉT PHẢN BIỆN LUẬN VĂN THẠC SĨ

Họ và tên cán bộ phản biện: Nguyễn Hiếu Minh

Học hàm, học vị: PGS.TS

Chuyên ngành: Truyền thông và Mạng máy tính

Cơ quan công tác: Học viện Kỹ thuật Mật mã

Họ và tên học viên cao học: Nguyễn Thanh Tuyền

Tên đề tài luận văn: Áp dụng Enterprise Architecture xây dựng khung kiến trúc bảo đảm an toàn thông tin cho các tổ chức, doanh nghiệp tại Việt Nam.

Chuyên ngành: Hệ thống thông tin Mã số: 13025106

Ý KIẾN NHẬN XÉT

Việc ứng dụng CNTT vào mọi mặt của đời sống xã hội và các tổ chức doanh nghiệp là nhu cầu không thể thiếu. Tuy nhiên việc xây dựng các hệ thống thông tin còn có rất nhiều vấn đề vì còn thiếu hoặc chưa áp dụng đúng một kiến trúc tổng thể. Do đó các hệ thống xây dựng xong thường hoạt động không hiệu quả. Một trong các vấn đề đảm bảo triển khai kiến trúc tổng thể là bài toán đảm bảo an toàn thông tin. Vì thế việc xây dựng khung kiến trúc đảm bảo an toàn thông tin cho các tổ chức doanh nghiệp tại Việt Nam luôn mang tính thời sự và cấp thiết.

Luận văn bao gồm: Mở đầu; Chương 1: Tổng quan về kiến trúc tổng thể; Chương 2: Cơ sở lý luận về an toàn thông tin, hệ thống quản lý an toàn thông tin; Chương 3: Xây dựng khung kiến trúc đảm bảo an toàn thông tin cho các tổ chức doanh nghiệp; Kết luận.

Luận văn tập trung vào giải quyết một số nội dung sau:

- Tổng quan về kiến trúc tổng thể, khung kiến trúc tổng thể và một số khung kiến trúc (khung kiến trúc ZACHMAN, TOGAF, ITI-GAF).
- Nghiên cứu về cơ sở lý luận an toàn thông tin, hệ thống quản lý an toàn thông tin (tiêu chuẩn TCVN ISO/IEC 27002:2011).
- Xây dựng khuung kiến trúc đảm bảo an toàn thông tin cho các doanh nghiệp: đề xuất các mô hình (đơn giản, trung gian, nâng cao); khung kiến trúc bảo đảm an toàn thông tin; đánh giá kết quả đạt được.

Luận văn không trùng lặp của đề tài nghiên cứu so với các công trình khoa học, luận văn đã công bố ở trong và ngoài nước.

Kết cấu luận văn tương đối hợp lý.

Đảm bảo sự phù hợp giữa tên đề tài với nội dung nghiên cứu cũng như với chuyên ngành và mã số đào tạo.

Về cơ bản học viên đã giải quyết được mục tiêu đã đề ra, bao gồm các tìm hiểu lý thuyết và xây dựng chương trình thử nghiệm.

Học viên đã thể hiện được sự hiểu biết và nắm được vấn đề cần giải quyết.

Các kết quả nghiên cứu đảm bảo độ tin cậy.

Tuy nhiên, luận văn còn có một số nhược điểm sau:

- Đề xuất khung kiến trúc được mô tả chưa thực sự rõ ràng.
- Chưa thấy được bản chất và sự phù hợp với các tổ chức doanh nghiệp tại Việt Nam.

Với các kết quả đã đạt được, đồng ý cho học viên được bảo vệ trước hội đồng chấm luận văn để nhận học vị Thạc sĩ.

Hà Nội, ngày 24 tháng 11 năm 2016

XÁC NHẬN CỦA CƠ QUAN CÔNG TÁC

BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ

PHÓ GIÁM ĐỐC

Nguyễn Hồng Quang

CÁN BỘ PHẢN BIỆN

PGS.TS Nguyễn Hiếu Minh.