

BỘ CÔNG AN
CÔNG AN THÀNH PHỐ HÀ NỘI



SỔ TAY
HƯỚNG DẪN TUÂN THỦ QUY ĐỊNH PHÁP LUẬT
VÀ TĂNG CƯỜNG BẢO ĐẢM AN TOÀN HỆ
THỐNG THÔNG TIN THEO CẤP ĐỘ

(Ban hành theo Công văn số 5351/CAHN-ANM&PCTPSDCNC
ngày 01 / 8 / 2025 của Công an thành phố Hà Nội)

Hà Nội, 2025

Mục lục

Lời nói đầu	1
Chương 1. Tổng quan về bảo đảm an toàn hệ thống thông tin theo cấp độ	3
1. Bảo đảm an toàn hệ thống thông tin theo cấp độ là gì?	3
1.1. Khái niệm	3
1.2. Phân loại	3
1.3. Nguyên tắc thực hiện	4
2. Căn cứ pháp lý và một số văn bản chỉ đạo quan trọng liên quan	5
2.1. Các văn bản quy phạm pháp luật chính	5
2.2. Tiêu chuẩn, quy chuẩn kỹ thuật	6
3. Phạm vi đối tượng áp dụng quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ	9
4. Trách nhiệm quản lý nhà nước	10
5. Kinh phí bảo đảm an toàn hệ thống thông tin theo cấp độ	11
Chương 2. Xác định các chủ thể có liên quan	13
1. Chủ quản hệ thống thông tin	13
1.1. Định nghĩa	13
1.2. Trách nhiệm của chủ quản hệ thống thông tin	14
1.3. Xác định chủ quản hệ thống thông tin	15
1.4. Ủy quyền trách nhiệm chủ quản hệ thống thông tin	17
2. Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin ...	18
2.1. Định nghĩa	18
2.2. Trách nhiệm của đơn vị chuyên trách về an toàn thông tin	18
2.3. Chỉ định, thành lập đơn vị chuyên trách về an toàn thông tin	18
3. Đơn vị vận hành hệ thống thông tin	20
3.1. Định nghĩa	20
3.2. Trách nhiệm của đơn vị vận hành hệ thống thông tin	20
3.3. Trường hợp hệ thống thông tin gồm nhiều hệ thống thành phần hoặc phân tán, có nhiều hơn một đơn vị vận hành hệ thống thông tin	20
4. Trách nhiệm của chủ đầu tư dự án, hoạt động ứng dụng công nghệ thông tin phục vụ xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin	20
4.1. Trong các giai đoạn chuẩn bị đầu tư, thực hiện đầu tư xây dựng dự án, hoạt động ứng dụng công nghệ thông tin	20
4.2. Trong giai đoạn vận hành cho đến khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin	21
5. Xác định các chủ thể khi thuê dịch vụ công nghệ thông tin không có sẵn trên thị trường	22

Chương 3. Thẩm định, phê duyệt cấp độ an toàn hệ thống thông tin	23
1. Thẩm quyền thẩm định, phê duyệt cấp độ.....	23
1.1. Đối với hệ thống thông tin đề xuất cấp độ 1 hoặc cấp độ 2.....	23
1.2. Đối với hệ thống thông tin đề xuất cấp độ 3	23
1.3. Đối với hệ thống thông tin đề xuất cấp độ 4 hoặc cấp độ 5	23
2. Tổ chức thẩm định hồ sơ đề xuất cấp độ	23
2.1. Thành phần Hồ sơ đề nghị thẩm định	23
2.2. Thẩm định hồ sơ đề xuất cấp độ.....	22
2.3. Hội đồng thẩm định độc lập	22
2.4. Thời gian thẩm định hồ sơ đề xuất cấp độ	27
3. Quy trình thẩm định, phê duyệt cấp độ.....	27
3.1. Đối với hệ thống thông tin đề xuất cấp độ 1 hoặc cấp độ 2.....	27
3.2. Đối với hệ thống thông tin đề xuất cấp độ 3	27

Lời nói đầu

Thực hiện Quyết định số 3614/QĐ-UBND ngày 01/7/2025 của UBND thành phố Hà Nội về việc phân công Công an Thành phố là đơn vị chuyên trách an toàn thông tin mạng của Ủy ban nhân dân thành phố Hà Nội, để tăng cường áp dụng một cách thống nhất, phát huy hiệu quả các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ, hỗ trợ các đơn vị Sở, Ban, Ngành, cơ quan ngang Sở, UBND phường, xã trực thuộc UBND Thành phố triển khai một cách hiệu quả, Công an Thành phố biên soạn "*Sổ tay Hướng dẫn tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ*" để các cơ quan, đơn vị có căn cứ, dễ dàng hơn trong quá trình triển khai.

- Về cấu trúc, Sổ tay gồm 03 Chương, cụ thể:

- *Chương 1. Tổng quan về bảo đảm an toàn hệ thống thông tin theo cấp độ:* Cung cấp các thông tin chung về khái niệm, căn cứ pháp lý, phạm vi áp dụng, trách nhiệm quản lý nhà nước và kinh phí triển khai công tác bảo đảm an toàn hệ thống thông tin theo cấp độ;

- *Chương 2. Xác định các chủ thể có liên quan:* Tập trung hướng dẫn, làm rõ trách nhiệm và cách thức xác định các chủ thể có liên quan đến hệ thống thông tin gồm (1) chủ quản hệ thống thông tin; (2) đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin; (3) đơn vị vận hành hệ thống thông tin; (4) chủ đầu tư dự án, hoạt động ứng dụng công nghệ thông tin hoặc đơn vị chủ trì thuê dịch vụ công nghệ thông tin phục vụ xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin, với những ví dụ minh họa trong các tình huống cụ thể;

- *Chương 3. Thẩm định, phê duyệt cấp độ an toàn hệ thống thông tin:* Hướng dẫn chi tiết các nội dung có liên quan đến quy trình thẩm định hồ sơ đề xuất cấp độ và phê duyệt cấp độ an toàn hệ thống thông tin. Đặc biệt, sẽ thống nhất hướng dẫn đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin cụ thể các nội dung cần thuyết minh, làm rõ khi cho ý kiến thẩm định hồ sơ đề xuất cấp độ.

- Đầu mối liên hệ, hỗ trợ của Công an thành phố Hà Nội:

Đồng chí Thượng úy Hoàng Triều Dương, Cán bộ Đội 5, Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao; số điện thoại: 0986.837.519./.

Hà Nội, tháng 07 năm 2025.

Chương 1.

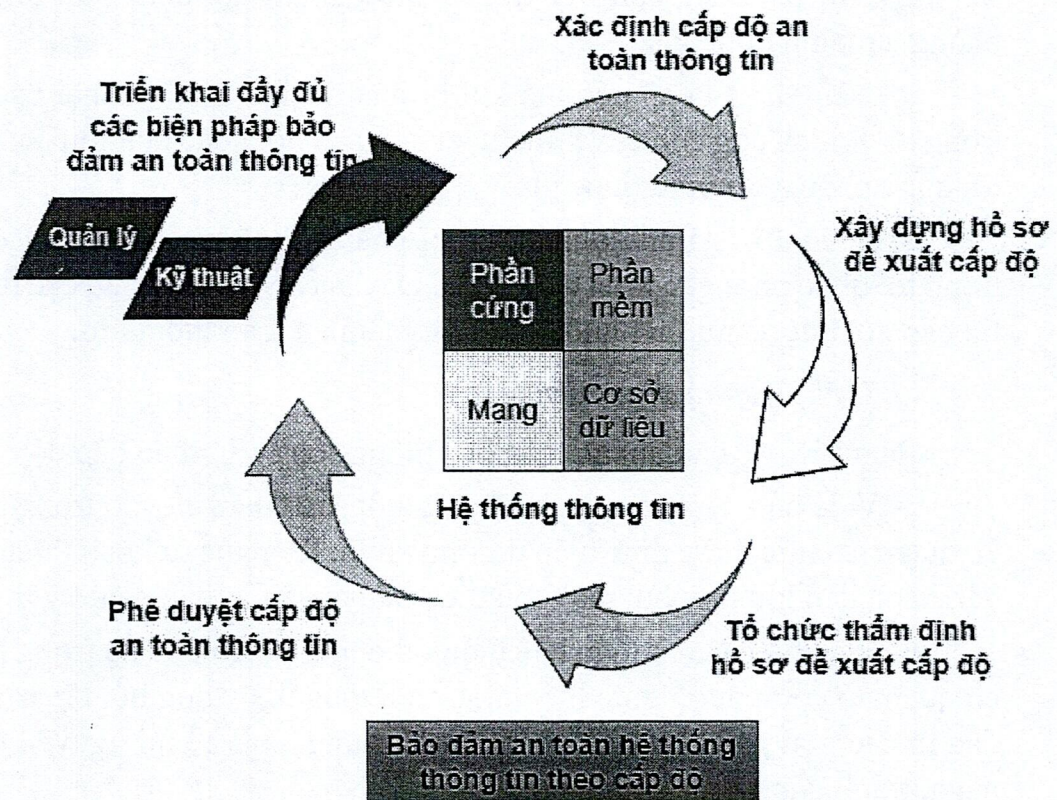
Tổng quan về bảo đảm an toàn hệ thống thông tin theo cấp độ

1. Bảo đảm an toàn hệ thống thông tin theo cấp độ là gì?

1.1. Khái niệm

Bảo đảm an toàn hệ thống thông tin theo cấp độ là các hoạt động xác định cấp độ, xây dựng, **thẩm định hồ sơ đề xuất cấp độ, phê duyệt cấp độ an toàn thông tin cho các hệ thống thông tin** và *triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin* (bao gồm các biện pháp quản lý và kỹ thuật) nhằm bảo vệ hệ thống thông tin phù hợp theo cấp độ.

Bảo đảm an toàn hệ thống thông tin theo cấp độ là biện pháp trọng tâm, cốt lõi để bảo vệ các hệ thống thông tin được quy định tại Luật An toàn thông tin mạng năm 2015.



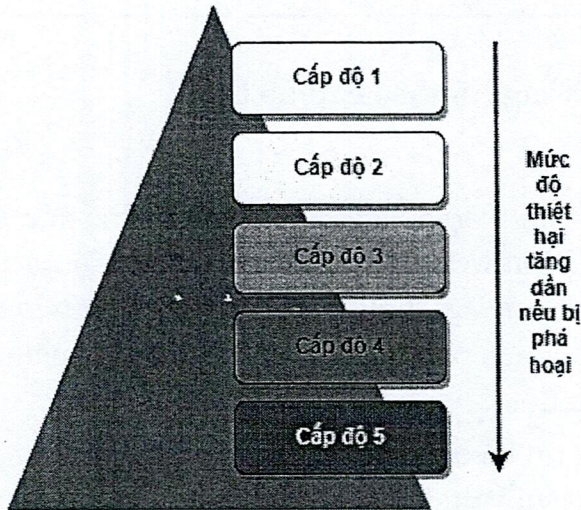
Hình 1. Hoạt động bảo đảm an toàn hệ thống thông tin theo cấp độ

Đối với các hệ thống thông tin do UBND thành phố Hà Nội là chủ quản, Công an thành phố Hà Nội với vai trò là đơn vị chuyên trách về an toàn thông tin mạng sẽ chủ trì:

- Thẩm định và phê duyệt đối với hệ thống thông tin cấp độ 1, 2.
- Thẩm định đối với hệ thống thông tin cấp độ 3.
- Cho ý kiến chuyên môn đối với hệ thống thông tin cấp độ 4, 5.

1.2. Phân loại

Hệ thống thông tin được phân loại theo 05 cấp độ an toàn như sau¹:



a) *Cấp độ 1* là cấp độ mà khi bị phá hoại sẽ làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân nhưng không làm tổn hại tới lợi ích công cộng, trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia;

b) *Cấp độ 2* là cấp độ mà khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng nhưng không làm tổn hại tới trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia;

c) *Cấp độ 3* là cấp độ mà khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia;

d) *Cấp độ 4* là cấp độ mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia;

đ) *Cấp độ 5* là cấp độ mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia. Đây là cấp độ cao nhất, các hệ thống thông tin cấp độ 5 được ưu tiên nguồn lực bảo đảm an toàn thông tin.

1.3. Nguyên tắc thực hiện

Nguyên tắc bảo đảm an toàn hệ thống thông tin theo cấp độ²:

- Việc bảo đảm an toàn hệ thống thông tin theo cấp độ trong hoạt động của cơ quan, tổ chức được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, vận hành đến khi hủy bỏ; tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật;
- Việc bảo đảm an toàn hệ thống thông tin theo cấp độ trong hoạt động của cơ quan, tổ chức được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.
- Việc phân bổ, bố trí nguồn lực để bảo đảm an toàn hệ thống thông tin thực hiện theo thứ tự ưu tiên từ cấp độ cao xuống cấp độ thấp.

2. Căn cứ pháp lý và một số văn bản chỉ đạo quan trọng liên quan

2.1. Các văn bản quy phạm pháp luật chính

Các văn bản quy phạm pháp luật chính quy định về bảo đảm an toàn thông tin theo cấp độ gồm:

¹ Quy định tại Khoản 2 Điều 21 Luật An toàn thông tin mạng năm 2015.

² Quy định tại Điều 4, Nghị định 85/2016/NĐ-CP

a) ***Luật An toàn thông tin mạng*** số 86/2015/QH13 do Quốc hội Việt Nam khóa 13 ban hành ngày 19/11/2015, có hiệu lực thi hành từ ngày 01/7/2016 (sau đây gọi tắt là Luật An toàn thông tin mạng):

Luật An toàn thông tin mạng quy định một số nội dung cơ bản về bảo đảm an toàn hệ thống thông tin theo cấp độ tại Mục 3. Bảo vệ hệ thống thông tin thuộc Chương II. Bảo đảm an toàn thông tin mạng, gồm 7 Điều, cụ thể: (1) Điều 21 quy định về việc phân loại cấp độ an toàn hệ thống thông tin; (2) Điều 22 quy định các nhiệm vụ bảo vệ hệ thống thông tin; (3) Điều 23 quy định về các biện pháp bảo vệ hệ thống thông tin; (4) Điều 24 quy định về giám sát an toàn hệ thống thông tin; (5) Điều 25 quy định trách nhiệm của chủ quản hệ thống thông tin; (6) Điều 26 quy định về hệ thống thông tin quan trọng quốc gia; (7) Điều 27 quy định về trách nhiệm bảo đảm an toàn thông tin mạng cho hệ thống thông tin quan trọng quốc gia.

b) ***Nghị định số 85/2016/NĐ-CP*** ngày 01/7/2016 của Chính phủ về bảo đảm an toàn thông tin theo cấp độ, có hiệu lực thi hành từ ngày 01/7/2016 (sau đây gọi tắt là Nghị định số 85/2016/NĐ-CP):

Nghị định này quy định chi tiết về tiêu chí, thẩm quyền, trình tự, thủ tục xác định cấp độ an toàn hệ thống thông tin và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ. Căn cứ các quy định tại Nghị định, các cơ quan, tổ chức thuộc đối tượng áp dụng tại Điều 2 Nghị định phải thực hiện quy trình, thủ tục xác định cấp độ và phương án bảo đảm an toàn thông tin cho các hệ thống thông tin do mình quản lý. Trên cơ sở đó, căn cứ vào các quy định về quyền và trách nhiệm bảo đảm an toàn thông tin theo cấp độ tương ứng, chủ quản hệ thống thông tin và đơn vị vận hành hệ thống thông tin sẽ triển khai các biện pháp về quản lý và kỹ thuật phù hợp để thực thi công tác bảo đảm an toàn thông tin.

c) ***Thông tư số 12/2022/TT-BTTTT*** ngày 12/8/2022 quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ, có hiệu lực thi hành từ ngày 01/10/2022 (sau đây gọi tắt là Thông tư số 12/2022/TT-BTTTT).

d) ***Thông tư 31/2017/TT-BTTTT*** ngày 15/11/2017 quy định về hoạt động giám sát an toàn hệ thống thông tin.

đ) ***Chỉ thị 14/CT-TTg*** ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại.

e) ***Chỉ thị 14/CT-TTg*** ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam.

*** Lưu ý:** Cho đến khi có văn bản quy phạm pháp luật mới quy định về bảo đảm an toàn thông tin theo cấp độ, các cơ quan, đơn vị tiếp tục căn cứ, triển khai theo các văn bản quy phạm pháp luật có hiệu lực hiện hành (ví dụ như các văn bản do Bộ Thông tin & Truyền thông ban hành).

2.2. Tiêu chuẩn, quy chuẩn kỹ thuật

Hệ thống tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ hiện chỉ có duy nhất *Tiêu chuẩn quốc gia TCVN 11930:2017* về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ (sau đây gọi tắt là Tiêu chuẩn quốc gia TCVN 11930:2017), trong đó:

Tiêu chuẩn này quy định các yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ, bao gồm hai nhóm yêu cầu quản lý và yêu cầu kỹ thuật. Nhóm các yêu cầu quản lý là cơ sở để cơ quan, tổ chức xây dựng chính sách, quy trình quản lý an toàn thông tin cho hệ thống thông tin của mình trong quá trình thiết kế, xây dựng, vận hành, khai thác và sử dụng. Nhóm yêu cầu kỹ thuật là cơ sở để cơ quan, tổ chức thiết kế, thiết lập cấu hình hệ thống trong quá trình xây dựng hệ thống thông tin.

3. Phạm vi đối tượng áp dụng quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ

Căn cứ quy định tại Điều 2 Nghị định số 85/2016/NĐ-CP, việc triển khai các nhiệm vụ bảo đảm an toàn hệ thống thông tin theo cấp độ đối với các hệ thống thông tin là bắt buộc đối với:

(1) Các cơ quan, tổ chức nhà nước gồm các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp nhà nước theo quy định tại khoản 11 Điều 4 Luật Doanh nghiệp 2020 và các cơ quan, tổ chức nhà nước khác;

(2) Các cơ quan, doanh nghiệp, cá nhân, tổ chức khác (như ngân hàng, tổ chức tài chính, doanh nghiệp tư nhân...) có triển khai các ứng dụng công nghệ thông tin cung cấp dịch vụ trực tuyến phục vụ người dân và doanh nghiệp.

(3) *Đối với các hệ thống thông tin khác, không thuộc phạm vi nêu trên:* Khuyến khích các cơ quan, tổ chức triển khai áp dụng để bảo vệ các hệ thống thông tin do mình xây dựng, quản lý, vận hành.

4. Trách nhiệm quản lý nhà nước

Ngày 28/2/2025, Công an thành phố Hà Nội tiếp nhận chức năng, nhiệm vụ quản lý nhà nước về an toàn thông tin mạng từ Sở Thông tin và Truyền thông (nay là Sở Khoa học & Công nghệ). Căn cứ Quyết định số 3614/QĐ-UBND ngày 01/7/2025 của UBND thành phố Hà Nội; theo đó, UBND Thành phố phân công Công an Thành phố là đơn vị chuyên trách an toàn thông tin mạng của UBND Thành phố và có trách nhiệm: *“Tổ chức triển khai bảo đảm an toàn hệ thống thông tin theo cấp độ; thẩm định về an toàn thông tin mạng trong hồ sơ thiết kế hệ thống thông tin, cấp độ an toàn hệ thống thông tin theo quy định của pháp luật”*.

5. Kinh phí bảo đảm an toàn hệ thống thông tin theo cấp độ

Theo quy định tại Điều 24 Nghị định số 85/2016/NĐ-CP, kinh phí thực hiện yêu cầu về an toàn thông tin theo cấp độ trong hoạt động của cơ quan, tổ chức nhà nước do Ngân sách nhà nước bảo đảm. Do đó, có thể xem xét sử dụng Ngân sách

nhà nước để chỉ cho các hoạt động bảo đảm an toàn hệ thống thông tin theo cấp độ. Việc sử dụng kinh phí phải tuân thủ các quy định của pháp luật về ngân sách và các quy định có liên quan.

Cụ thể: Bộ Tài chính có trách nhiệm hướng dẫn Mục chi cho công tác bảo đảm an toàn thông tin trong dự toán ngân sách, hướng dẫn quản lý và sử dụng kinh phí sự nghiệp chỉ cho công tác bảo đảm an toàn thông tin trong hoạt động của các cơ quan, tổ chức nhà nước. Đối với nhiệm vụ này, Bộ Tài chính đã ban hành Thông tư số 121/2018/TT-BTC ngày 12/12/2018 quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí để thực hiện công tác ứng cứu sự cố, bảo đảm an toàn thông tin mạng, trong đó các nội dung chi và mức chi được quy định cụ thể tại Điều 5 và Điều 6 của Thông tư;

(1) Kinh phí đầu tư cho an toàn thông tin sử dụng vốn đầu tư công thực hiện theo quy định của Luật Đầu tư công. Đối với dự án đầu tư công để xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin, kinh phí đầu tư cho an toàn thông tin theo cấp độ được bố trí trong vốn đầu tư của dự án tương ứng;

(2) Kinh phí thực hiện giám sát, đánh giá, quản lý rủi ro an toàn thông tin; đào tạo ngắn hạn, tuyên truyền, phổ biến nâng cao nhận thức; diễn tập an toàn thông tin và ứng cứu sự cố của cơ quan, tổ chức nhà nước được cân đối bố trí trong dự toán ngân sách hàng năm của cơ quan, tổ chức nhà nước đó theo phân cấp của Luật Ngân sách nhà nước;

(3) Bộ Tài chính có trách nhiệm hướng dẫn Mục chi cho công tác bảo đảm an toàn thông tin trong dự toán ngân sách, hướng dẫn quản lý và sử dụng kinh phí sự nghiệp chỉ cho công tác bảo đảm an toàn thông tin trong hoạt động của các cơ quan, tổ chức nhà nước. Đối với nhiệm vụ này, Bộ Tài chính đã ban hành Thông tư số 121/2018/TT-BTC ngày 12/12/2018 quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí để thực hiện công tác ứng cứu sự cố, bảo đảm an toàn thông tin mạng, trong đó các nội dung và mức chi được quy định cụ thể tại Điều 5 và Điều 6 của Thông tư;

(4) Căn cứ nhiệm vụ được giao, cơ quan, tổ chức nhà nước thực hiện lập dự toán, quản lý, sử dụng và quyết toán kinh phí thực hiện nhiệm vụ bảo đảm an toàn thông tin theo quy định của Luật Ngân sách nhà nước;

(5) Tỷ lệ kinh phí chi cho hoạt động bảo đảm an toàn thông tin:

- Tại Chỉ thị số 14/CT-TTg năm 2019, Thủ tướng Chính phủ chỉ đạo: “e) **Bảo đảm tỷ lệ kinh phí chi cho các sản phẩm, dịch vụ an toàn thông tin mạng đạt tối thiểu 10% trong tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin hàng năm, giai đoạn 5 năm và các dự án công nghệ thông tin (trong trường hợp chủ đầu tư chưa có hệ thống kỹ thuật hoặc thuê dịch vụ bảo đảm an toàn thông tin mạng chuyên biệt đáp ứng được các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ);**”;

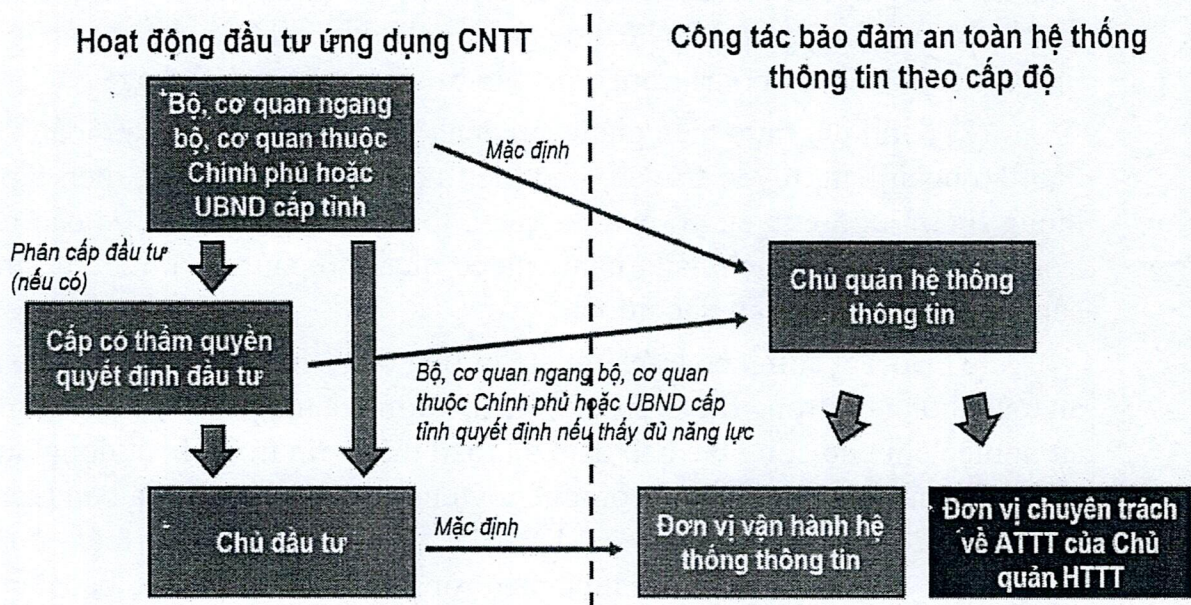
- Tại Chiến lược an toàn, an ninh mạng quốc gia, Thủ tướng Chính phủ tiếp tục chỉ đạo về đầu tư nguồn lực và bảo đảm kinh phí thực hiện: “đ) **Bố trí kinh phí chi cho an toàn, an ninh mạng đạt tối thiểu 10% kinh phí chi cho khoa học công nghệ, chuyển đổi số, ứng dụng công nghệ thông tin.**”.

Chương 2.

Xác định các chủ thể có liên quan

Để thực hiện tốt việc quản lý nhà nước về bảo đảm an toàn hệ thống thông tin theo cấp độ, phải xác định đúng các chủ thể liên quan đến mỗi hệ thống thông tin.

Các chủ thể có liên quan đến mỗi hệ thống thông tin bao gồm: (1) Chủ quản hệ thống thông tin; (2) Đơn vị chuyên trách về an toàn thông tin **của chủ quản hệ thống thông tin**; (3) Đơn vị vận hành hệ thống thông tin; (4) Chủ đầu tư dự án, hoạt động ứng dụng công nghệ thông tin hoặc đơn vị chủ trì thuê dịch vụ công nghệ thông tin phục vụ xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.



Hình 2. Xác định các chủ thể có liên quan

1. Chủ quản hệ thống thông tin

1.1. Định nghĩa

Định nghĩa về chủ quản hệ thống thông tin được quy định tại khoản 5 Điều 3 Luật An toàn thông tin mạng, sau đó được làm rõ chi tiết tại khoản 1 Điều 3 Nghị định số 85/2016/NĐ-CP, cụ thể:

Chủ quản hệ thống thông tin là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

Đối với cơ quan, tổ chức nhà nước, chủ quản hệ thống thông tin là các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương hoặc là cấp **có thẩm quyền** quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin đó.

1.2. Trách nhiệm của chủ quản hệ thống thông tin

Khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP quy định trách nhiệm của chủ quản hệ thống thông tin:

a) Chỉ đạo đơn vị vận hành hệ thống thông tin lập hồ sơ đề xuất cấp độ; tổ chức thẩm định, phê duyệt hồ sơ đề xuất cấp độ;

b) Chỉ đạo, tổ chức thực hiện phương án bảo đảm an toàn hệ thống thông tin theo cấp độ đối với hệ thống thông tin thuộc phạm vi mình quản lý theo quy định tại Điều 25, 26 và 27 Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP và quy định của pháp luật liên quan;

c) Chỉ đạo, tổ chức thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin trong phạm vi cơ quan, tổ chức mình, cụ thể như sau:

- Định kỳ 02 năm thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin tổng thể trong hoạt động của cơ quan, tổ chức mình;

- Định kỳ hàng năm thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin đối với các hệ thống cấp độ 3 và cấp độ 4;

- Định kỳ 06 tháng (hoặc đột xuất khi thấy cần thiết hoặc theo yêu cầu, cảnh báo của cơ quan chức năng) thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin đối với hệ thống cấp độ 5;

- Việc kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro an toàn thông tin đối với hệ thống từ cấp độ 3 trở lên phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép; tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp hoặc do tổ chức chuyên môn được cấp có thẩm quyền chỉ định thực hiện.

d) Chỉ đạo, tổ chức thực hiện đào tạo ngắn hạn, tuyên truyền, phổ biến, nâng cao nhận thức và diễn tập về an toàn thông tin, cụ thể như sau:

- Đào tạo, bồi dưỡng theo các chương trình đào tạo ngắn hạn nâng cao kiến thức, kỹ năng về an toàn thông tin cho cán bộ, công chức, viên chức làm về an toàn thông tin trong cơ quan, tổ chức mình;

- Tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin cho cán bộ, công chức, viên chức trong cơ quan, tổ chức mình;

- Diễn tập bảo đảm an toàn thông tin trong hoạt động của cơ quan, tổ chức mình; tham gia diễn tập quốc gia và diễn tập quốc tế do Bộ Công an tổ chức.

đ) Chỉ đạo đơn vị vận hành hệ thống thông tin phối hợp với đơn vị chức năng liên quan của Bộ Công an trong việc triển khai thiết bị, kết nối tới hệ thống kỹ thuật xử lý, giảm thiểu tấn công mạng, hỗ trợ giám sát an toàn thông tin cho hệ thống thông tin cung cấp dịch vụ công trực tuyến, phát triển Chính phủ điện tử.

* Về việc phê duyệt cấp độ: Chủ quản hệ thống thông tin có trách nhiệm: (1) Phê duyệt cấp độ an toàn thông tin của hệ thống thông tin được đề xuất cấp độ 3, 4; (2) Phê duyệt phương án bảo đảm an toàn thông tin của hệ thống thông tin được đề xuất cấp độ 5.

1.3. Xác định chủ quản hệ thống thông tin

Căn cứ quy định tại khoản 1 Điều 3 Nghị định số 85/2016/NĐ-CP và Điều 4 Thông tư số 12/2022/TT-BTTTT, chủ quản hệ thống thông tin xác định như sau:

1.3.1. Đối với các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban

nhân dân các tỉnh, thành phố trực thuộc trung ương

a) **Mặc định:** Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương (sau đây gọi chung là Ủy ban nhân dân cấp tỉnh) là chủ quản hệ thống thông tin của các hệ thống thông tin do các đơn vị (bao gồm đơn vị tham mưu, đơn vị hành chính, đơn vị sự nghiệp công lập và doanh nghiệp nhà nước) thuộc phạm vi quản lý làm chủ đầu tư.

b) Theo cấp có thẩm quyền quyết định đầu tư: Căn cứ quy định tại điểm c khoản 1 Điều 4 Thông tư số 12/2022/TT-BTTTT, đơn vị thuộc hoặc trực thuộc được bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh quyết định là chủ quản hệ thống thông tin đối với các hệ thống thông tin do đơn vị tự quyết định đầu tư, nếu đáp ứng hai điều kiện sau đây:

- Một là, có đủ năng lực thực thi quy định tại khoản 1 Điều 20 Nghị định số 85/2016/NĐ-CP, cụ thể:

+ Người đứng đầu đơn vị phải chỉ định được đơn vị trực thuộc làm đơn vị chuyên trách về an toàn thông tin theo quy định tại khoản 5 Điều 3 và điểm b khoản 1 Điều 20 Nghị định số 85/2016/NĐ-CP;

+ Đơn vị trực thuộc được chỉ định là đơn vị chuyên trách về an toàn thông tin phải đáp ứng các điều kiện được nêu tại Mục 2.3.2 Chương 2;

- Hai là, có đủ năng lực để thực thi đầy đủ các quy định tại khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP.

Lưu ý quan trọng: Việc xác định chủ quản hệ thống thông tin đối với các hệ thống thông tin *không xác định theo phân cấp hành chính*:

(1) Trường hợp theo phân cấp đầu tư, một đơn vị thuộc phạm vi quản lý của bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ hoặc Ủy ban nhân dân cấp tỉnh là cấp có thẩm quyền quyết định đầu tư xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin *nhưng không đủ năng lực* làm chủ quản hệ thống thông tin hoặc *có đủ năng lực nhưng không được* bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ hoặc Ủy ban nhân dân cấp tỉnh **quyết định** là chủ quản hệ thống thông tin thì chủ quản hệ thống thông tin được xác định là bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ hoặc Ủy ban nhân dân cấp tỉnh tương ứng;

(2) Trường hợp cần phân cấp chủ quản hệ thống thông tin, bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh cần chỉ đạo đơn vị chuyên trách về an toàn thông tin có đánh giá cụ thể về năng lực của từng tổ chức để xác định những tổ chức có đủ năng lực làm chủ quản hệ thống thông tin, đặc biệt là đối với hệ thống thông tin được đề xuất cấp độ 4 và cấp độ 5.

Ví dụ 2.1. Một số trường hợp điển hình:

(i) Đối với các hệ thống thông tin (nếu có) do Ủy ban nhân dân cấp xã, Chi cục/Trung tâm thuộc Sở, cơ sở y tế công lập thuộc Sở Y tế, cơ sở giáo dục công lập thuộc Sở Giáo dục và Đào tạo, Sở, ban, ngành, doanh nghiệp nhà nước... tại địa phương quyết định đầu tư nhưng đơn vị *không đủ năng lực làm chủ quản hệ thống thông tin* thì chủ quản hệ thống thông tin được xác định là Ủy ban nhân

dân cấp tỉnh;

(ii) Đối với các hệ thống thông tin (nếu có) do Văn phòng, Thanh tra, Cục, Chi cục/Trung tâm thuộc Cục, Chi cục thuộc Cục, Ban, Trung tâm, Viện, Học viện, doanh nghiệp nhà nước... thuộc bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ quyết định đầu tư nhưng đơn vị ***không đủ năng lực làm chủ quản hệ thống thông tin*** thì chủ quản hệ thống thông tin được xác định là bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;

(iii) Trường hợp Cục (và tương đương) thuộc bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ ***có đủ năng lực làm chủ quản hệ thống***. Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ ***ủy quyền Cục làm chủ quản hệ thống thông tin*** thì thực hiện theo quy định tại khoản 3 Điều 4 Thông tư số 12/2022/TT-BTTTT và hướng dẫn chi tiết tại Mục 1.5 Chương 2 bên dưới.

1.3.2. Đối với doanh nghiệp và các tổ chức khác (không phải bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh, như cơ quan Đảng, Đoàn thể, Quốc hội, Hội đồng nhân dân các cấp; tổ chức chính trị, chính trị-xã hội...)

Chủ quản hệ thống thông tin được xác định là cấp có thẩm quyền quyết định đầu tư xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin.

Trường hợp một đơn vị là cấp có thẩm quyền quyết định đầu tư xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin ***nhưng không đủ năng lực*** làm chủ quản hệ thống thông tin, đơn vị đó cần báo cáo cơ quan, tổ chức cấp trên trực tiếp và đề nghị cơ quan, tổ chức cấp trên trực tiếp làm chủ quản hệ thống thông tin.

Ví dụ 2.2. Đối với hệ thống thông tin (nếu có) do các cơ quan Đảng xây dựng, triển khai, việc tổ chức bảo đảm an toàn hệ thống thông tin theo cấp độ được thực hiện theo Luật An toàn thông tin mạng và các văn bản quy định, hướng dẫn của Đảng, trong đó có thể tham khảo phương án thực hiện như sau:

Đối với hệ thống thông tin (nếu có) do các cơ quan Đảng bộ khối, Văn phòng tỉnh ủy và các ban của Đảng tại địa phương quyết định đầu tư, tuy nhiên các đơn vị này ***không đủ năng lực làm chủ quản hệ thống thông tin*** thì khi đó, chủ quản hệ thống thông tin được xác định là Đảng bộ cấp tỉnh. Ban Thường vụ Đảng bộ tỉnh hoặc Ban chấp hành Đảng bộ tỉnh (theo thẩm quyền) cần chỉ định một đơn vị trực thuộc làm nhiệm vụ đơn vị chuyên trách về an toàn thông tin của Đảng bộ tỉnh theo quy định (thường là Văn phòng tỉnh ủy);

1.4. Ủy quyền trách nhiệm chủ quản hệ thống thông tin

Trường hợp áp dụng khoản 3 Điều 4 Thông tư số 12/2022/TT-BTTTT, bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh có văn bản ủy quyền cho một đơn vị trực thuộc có đủ năng lực để thay mặt thực hiện trách nhiệm của chủ quản hệ thống thông tin theo quy định tại khoản 2 Điều 20 Nghị định 85/2016/NĐ-CP thì khi đó, theo quy định của pháp luật về dân sự:

(1) Đơn vị được ủy quyền không phải chủ quản hệ thống thông tin mà chỉ thực hiện các nhiệm vụ được chủ quản hệ thống thông tin ủy quyền (theo phạm vi

nhiệm vụ được nêu trong văn bản ủy quyền);

(2) Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh vẫn là chủ quản hệ thống thông tin và đơn vị chuyên trách về an toàn thông tin của bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh vẫn thực hiện trách nhiệm của mình đối với hệ thống thông tin;

(3) Trường hợp có hệ thống thông tin được đề xuất cấp độ 3 trở lên thì khi phê duyệt cấp độ an toàn thông tin (cấp độ 3, 4) hoặc phê duyệt phương án bảo đảm an toàn thông tin (cấp độ 5), Người đứng đầu đơn vị được ủy quyền ký quyết định của đơn vị ủy quyền (chủ quản hệ thống thông tin) với tư cách *thừa ủy quyền*.

2. Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin

2.1. Định nghĩa

*Đơn vị chuyên trách về an toàn thông tin*³ là đơn vị có chức năng, nhiệm vụ bảo đảm an toàn thông tin của chủ quản hệ thống thông tin.

2.2. Trách nhiệm của đơn vị chuyên trách về an toàn thông tin

Theo quy định tại Điều 21 Nghị định số 85/2016/NĐ-CP, đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin có trách nhiệm:

- Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, giám sát công tác bảo đảm an toàn thông tin;

- Thẩm định hồ sơ đề xuất cấp độ 1, 2, 3, phê duyệt cấp độ an toàn thông tin đối với các hệ thống thông tin được đề xuất cấp độ 1, 2 hoặc cho ý kiến về mặt chuyên môn đối với hồ sơ đề xuất cấp độ 4, 5 theo thẩm quyền quy định tại khoản 1, khoản 2 Điều 12 và Khoản 5 Điều 15 Nghị định số 85/2016/NĐ-CP.

Đơn vị chuyên trách về an toàn thông tin của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ và Ủy ban nhân dân cấp tỉnh còn đảm nhận vai trò là đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

* Về công tác thẩm định, phê duyệt cấp độ: Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin có trách nhiệm: (1) Thẩm định hồ sơ đề xuất cấp độ của hệ thống thông tin được đề xuất cấp độ 1, 2, 3; (2) Phê duyệt cấp độ an toàn thông tin của hệ thống thông tin được đề xuất cấp độ 1, 2; (3) Cho ý kiến chuyên môn đối với hồ sơ đề xuất cấp độ của hệ thống thông tin được đề xuất cấp độ 4, 5.

Theo đó, Công an tỉnh sẽ thực hiện thẩm định và phê duyệt hồ sơ đề xuất cấp độ hệ thống thông tin cấp độ 1, 2; thẩm định hồ sơ đề xuất cấp độ và tham mưu UBND phê duyệt cấp độ đối với hệ thống thông tin cấp độ 3; cho ý kiến chuyên môn đối với hồ sơ đề xuất cấp độ của hệ thống thông tin được đề xuất cấp độ 4, 5, tham mưu gửi hồ sơ về Bộ Công an để thẩm định.

³ Theo khoản 5 Điều 3 Nghị định số 85/2016/NĐ-CP

2.3. Chỉ định, thành lập đơn vị chuyên trách về an toàn thông tin

2.3.1. Trường hợp các cơ quan, tổ chức được xác định là chủ quản hệ thống thông tin, chưa có đơn vị chuyên trách về an toàn thông tin độc lập nhưng đã có đơn vị chuyên trách về công nghệ thông tin

Theo quy định tại điểm b khoản 1 Điều 20 Nghị định số 85/2016/NĐ-CP, Người đứng đầu cơ quan, tổ chức là chủ quản hệ thống thông tin có trách nhiệm:

- Chỉ định đơn vị chuyên trách về công nghệ thông tin làm nhiệm vụ đơn vị chuyên trách về an toàn thông tin;
- Thành lập hoặc chỉ định bộ phận chuyên trách về an toàn thông tin trực thuộc đơn vị chuyên trách về công nghệ thông tin.

Bộ phận chuyên trách về an toàn thông tin⁴ là bộ phận do chủ quản hệ thống thông tin thành lập hoặc chỉ định (thuộc đơn vị chuyên trách về công nghệ thông tin) để (tham mưu giúp đơn vị chuyên trách về công nghệ thông tin) thực thi nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an toàn thông tin mạng (nhiệm vụ của đơn vị chuyên trách về an toàn thông tin).

2.3.2. Điều kiện xác định đơn vị chuyên trách về an toàn thông tin

Đơn vị được xác định là đơn vị chuyên trách về an toàn thông tin phải đáp ứng các điều kiện sau đây:

(1) Là một đơn vị trực thuộc của chủ quản hệ thống thông tin, có chức năng, nhiệm vụ bảo đảm an toàn thông tin hoặc được giao nhiệm vụ là đơn vị chuyên trách về công nghệ thông tin của chủ quản hệ thống thông tin;

(2) Có năng lực để bảo đảm thực thi các quy định tại Điều 21 Nghị định số 85/2016/NĐ-CP, trong đó: có nhân sự đáp ứng yêu cầu chuyên môn, đảm bảo tổ chức thẩm định hồ sơ đề xuất cấp độ; có tư cách pháp nhân để ban hành quyết định phê duyệt cấp độ an toàn thông tin đối với các hệ thống thông tin được đề xuất cấp độ 1, 2 theo thẩm quyền được giao tại khoản 1 Điều 12 Nghị định số 85/2016/NĐ-CP, phù hợp các quy định của pháp luật về dân sự và các quy định của pháp luật có liên quan.

Ví dụ 2.3. Đơn vị chuyên trách về an toàn thông tin tại các địa phương:

(i) Đối với Ủy ban nhân dân cấp tỉnh: Công an tỉnh được xác định là đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin;

(ii) Đối với Ủy ban nhân dân cấp xã: Ủy ban nhân dân cấp xã không có đơn vị trực thuộc nên không có đơn vị chuyên trách về an toàn thông tin.

3. Đơn vị vận hành hệ thống thông tin

3.1. Định nghĩa

Đơn vị vận hành hệ thống thông tin⁵ là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin.

⁴ Theo khoản 6 Điều 3 Nghị định số 85/2016/NĐ-CP.

⁵ Theo khoản 3 Điều 3 Nghị định số 85/2016/NĐ-CP.

3.2. Trách nhiệm của đơn vị vận hành hệ thống thông tin

Theo quy định tại Điều 22 Nghị định số 85/2016/NĐ-CP, đơn vị vận hành hệ thống thông tin có trách nhiệm:

- Thực hiện xác định cấp độ an toàn hệ thống thông tin theo quy định tại Điều 14 Nghị định số 85/2016/NĐ-CP;
- Thực hiện bảo vệ hệ thống thông tin theo quy định của pháp luật và hướng dẫn, tiêu chuẩn, quy chuẩn an toàn thông tin;
- Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin, báo cáo chủ quản hệ thống thông tin điều chỉnh nếu cần thiết;
- Định kỳ hoặc đột xuất báo cáo công tác thực thi bảo đảm an toàn hệ thống thông tin theo yêu cầu của chủ quản hệ thống thông tin hoặc cơ quan quản lý nhà nước chuyên ngành có thẩm quyền;
- Phối hợp, thực hiện theo yêu cầu của cơ quan chức năng trong công tác bảo đảm an toàn thông tin.

3.3. Trường hợp hệ thống thông tin gồm nhiều hệ thống thành phần hoặc phân tán, có nhiều hơn một đơn vị vận hành hệ thống thông tin

Theo quy định tại khoản 2 Điều 5 Thông tư số 12/2022/TT-BTTTT, chủ quản hệ thống thông tin có trách nhiệm chỉ định một đơn vị chủ trì thực hiện quyền và nghĩa vụ của đơn vị vận hành hệ thống thông tin theo quy định của pháp luật. Khi đó quy chế bảo đảm an toàn thông tin cần làm rõ trách nhiệm của đơn vị chủ trì và các đơn vị tham gia vận hành hệ thống thông tin.

4. Trách nhiệm của chủ đầu tư dự án, hoạt động ứng dụng công nghệ thông tin phục vụ xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin

4.1. Trong các giai đoạn chuẩn bị đầu tư, thực hiện đầu tư xây dựng dự án, hoạt động ứng dụng công nghệ thông tin

Mặc định chủ đầu tư được xác định là đơn vị vận hành hệ thống thông tin, chịu trách nhiệm:

(1) Lòng ghép thuyết minh đề xuất cấp độ vào nội dung báo cáo kinh tế - kỹ thuật (trường hợp dự án đầu tư áp dụng phương án thiết kế 01 bước), thiết kế cơ sở thuộc báo cáo nghiên cứu khả thi (trường hợp dự án đầu tư áp dụng phương án thiết kế 02 bước) hoặc đề cương và dự toán chi tiết (trong trường hợp đầu tư ứng dụng công nghệ thông tin không phải lập dự án)⁶;

(2) Xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin, đồng bộ với phương án kỹ thuật trong báo cáo kinh tế - kỹ thuật hoặc thiết kế cơ sở thuộc báo cáo nghiên cứu khả thi hoặc đề cương và dự toán chi tiết tương ứng⁷;

(3) Khuyến khích gửi đơn vị/trình cấp có thẩm quyền thẩm định và phê duyệt cấp độ an toàn hệ thống thông tin trước khi cấp có thẩm quyền phê duyệt

⁶ Khoản 1 Điều 13 Nghị định số 85/2016/NĐ-CP.

⁷ Khoản 1 Điều 8 Thông tư số 12/2022/TT-BTTTT.

báo cáo kinh tế - kỹ thuật hoặc thiết kế cơ sở thuộc báo cáo nghiên cứu khả thi hoặc đề cương và dự toán chi tiết tương ứng⁸.

Trường hợp chủ đầu tư đồng thời là cấp có thẩm quyền quyết định đầu tư, có đủ năng lực, được xác định là chủ quản hệ thống thông tin thì chủ đầu tư chỉ định một đơn vị hoặc bộ phận trực thuộc thực hiện nhiệm vụ đơn vị vận hành hệ thống thông tin. Khi đó, đơn vị hoặc bộ phận được xác định là đơn vị vận hành hệ thống thông tin sẽ chịu trách nhiệm thực hiện các nhiệm vụ (2) và (3) ở trên.

4.2. Trong giai đoạn vận hành cho đến khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin

Trên cơ sở từng tình huống cụ thể, chủ đầu tư có thể đóng vai trò:

(1) Chủ quản hệ thống thông tin nếu là cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin đó và có đủ năng lực để thực thi đầy đủ các quy định tại Điều 20 Nghị định 85/2016/NĐ-CP, được quyết định là chủ quản hệ thống thông tin, hoặc;

(2) Tiếp tục là đơn vị vận hành hệ thống thông tin nếu chủ quản hệ thống thông tin không có văn bản giao một đơn vị khác thực hiện nhiệm vụ đơn vị vận hành hệ thống thông tin, hoặc;

(3) Đơn vị tham gia sử dụng hệ thống thông tin nếu chủ quản hệ thống thông tin có văn bản giao một đơn vị khác thực hiện nhiệm vụ đơn vị vận hành hệ thống thông tin. Khi đó quy chế bảo đảm an toàn thông tin cho hệ thống cần làm rõ trách nhiệm giữa đơn vị vận hành hệ thống thông tin và đơn vị tham gia sử dụng hệ thống thông tin.

Ví dụ 2.4. Trong giai đoạn vận hành hệ thống thông tin, chủ đầu tư cài đặt, vận hành hệ thống thông tin tại Trung tâm dữ liệu của bộ/địa phương do đơn vị chuyên trách về công nghệ thông tin của bộ/địa phương quản lý hoặc chủ đầu tư thuê dịch vụ hạ tầng số và cài đặt, vận hành hệ thống thông tin tại Trung tâm dữ liệu hoặc dịch vụ điện toán đám mây của doanh nghiệp. Khi đó:

(i) Chủ đầu tư tiếp tục thực hiện nhiệm vụ là đơn vị vận hành hệ thống thông tin nếu chủ quản hệ thống thông tin không có văn bản giao đơn vị chuyên trách về công nghệ thông tin hoặc doanh nghiệp cung cấp dịch vụ hạ tầng số thực hiện nhiệm vụ đơn vị vận hành hệ thống thông tin;

(ii) Quy chế bảo đảm an toàn thông tin cho hệ thống cần làm rõ trách nhiệm giữa đơn vị vận hành hệ thống thông tin và đơn vị cung cấp dịch vụ hạ tầng số phục vụ vận hành hệ thống thông tin (hai đơn vị có thể ký quy chế phối hợp hoặc đồng trình chủ quản hệ thống thông tin ban hành).

5. Xác định các chủ thể khi thuê dịch vụ công nghệ thông tin không có sẵn trên thị trường

Khái niệm: *Dịch vụ công nghệ thông tin không sẵn có trên thị trường*⁹ là dịch vụ được thiết lập theo các yêu cầu riêng nhằm đáp ứng yêu cầu đặc thù của cơ quan, đơn vị.

⁸ Điều 15 Thông tư số 12/2022/TT-BTTTT.

⁹ Khoản 4 Điều 3 Nghị định số 73/2019/NĐ-CP ngày 05/9/2019 của Chính phủ quy định quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

Đặc điểm:

(1) Cơ quan, đơn vị thuê tổ chức, cá nhân thiết lập mới, mở rộng hoặc nâng cấp cho hệ thống hạ tầng kỹ thuật, phần mềm, cơ sở dữ liệu nhằm đáp ứng yêu cầu đặc thù của cơ quan, đơn vị;

(2) Có hình thành hệ thống thông tin riêng của cơ quan, đơn vị thuê;

(3) Sau khi hoàn thành hệ thống hoặc hạng mục của hệ thống công nghệ thông tin thì tổ chức, cá nhân được thuê sẽ tổ chức quản trị, vận hành để cung cấp dịch vụ cho cơ quan, đơn vị thuê hoặc bàn giao cho cơ quan, đơn vị thuê tự tổ chức quản trị, vận hành trong một thời hạn nhất định.

Tổ chức thực hiện: Trường hợp bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ hoặc Ủy ban nhân dân cấp tỉnh hoặc đơn vị trực thuộc lựa chọn hình thức thuê dịch vụ công nghệ thông tin để xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin theo yêu cầu đặc thù của cơ quan, đơn vị thì việc xác định các chủ thể có liên quan của hệ thống thông tin được xác định như trường hợp lập dự án hoặc xây dựng đề cương và dự toán chi tiết, cụ thể:

(1) Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh hoặc cấp có thẩm quyền quyết định đầu tư là chủ quản hệ thống thông tin.

(2) Khi chưa xác định được đơn vị cung cấp dịch vụ theo quy định pháp luật:

- Trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin (đồng thời là đơn vị chủ trì, trực tiếp ký hợp đồng thuê dịch vụ công nghệ thông tin): Chủ quản hệ thống thông tin giao một đơn vị trực thuộc tham mưu thực hiện (1) lồng ghép thuyết minh đề xuất cấp độ vào nội dung kế hoạch thuê dịch vụ¹⁰; (2) xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin, đồng bộ với phương án kỹ thuật trong kế hoạch thuê dịch vụ¹¹; (3) khuyến khích gửi đơn vị/trình cấp có thẩm quyền thẩm định và phê duyệt cấp độ an toàn hệ thống thông tin trước khi cấp có thẩm quyền phê duyệt kế hoạch thuê dịch vụ¹²;

- Trường hợp chủ quản hệ thống thông tin giao một đơn vị trực thuộc chủ trì thuê dịch vụ công nghệ thông tin: Đơn vị chủ trì thuê dịch vụ được xác định là đơn vị vận hành hệ thống thông tin, tiến hành (1) lồng ghép thuyết minh đề xuất cấp độ vào nội dung kế hoạch thuê dịch vụ¹³; (2) xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin, đồng bộ với phương án kỹ thuật trong kế hoạch thuê dịch vụ¹⁴; (3) khuyến khích gửi đơn vị/trình cấp có thẩm quyền thẩm định và phê duyệt cấp độ an toàn hệ thống thông tin trước khi cấp có thẩm quyền phê

¹⁰ Khoản 2 Điều 13 Nghị định số 85/2016/NĐ-CP.

¹¹ Khoản 1 Điều 8 Thông tư số 12/2022/TT-BTTTT.

¹² Điều 15 Thông tư số 12/2022/TT-BTTTT.

¹³ Khoản 2 Điều 13 Nghị định số 85/2016/NĐ-CP.

¹⁴ Khoản 1 Điều 8 Thông tư số 12/2022/TT-BTTTT.

duyet kế hoạch thuê dịch vụ¹⁵.

(3) Khi đã xác định được đơn vị cung cấp dịch vụ theo quy định pháp luật:

- Trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin (đồng thời là đơn vị chủ trì, trực tiếp ký hợp đồng thuê dịch vụ công nghệ thông tin): Theo quy định tại khoản 3 Điều 3 Nghị định số 85/2016/NĐ-CP, đơn vị vận hành là đơn vị cung cấp dịch vụ;

- Trường hợp chủ quản hệ thống thông tin giao một đơn vị trực thuộc chủ trì thuê dịch vụ công nghệ thông tin: Đơn vị chủ trì thuê dịch vụ tiếp tục là đơn vị vận hành nếu chủ quản hệ thống thông tin không giao đơn vị cung cấp dịch vụ hoặc đơn vị khác thực hiện nhiệm vụ đơn vị vận hành hệ thống thông tin.

Đơn vị cung cấp dịch vụ có trách nhiệm phối hợp với chủ quản hệ thống thông tin/đơn vị chủ trì thuê dịch vụ cập nhật thông tin trong hồ sơ đề xuất cấp độ theo đúng hiện trạng hạ tầng đã cài đặt để tổ chức thẩm định, phê duyệt (nếu chưa phê duyệt) hoặc gửi đơn vị chuyên trách về an toàn thông tin để cập nhật.

(4) Khi hết thời hạn cung cấp dịch vụ, nếu hệ thống thông tin tiếp tục được duy trì hoạt động (có thể chuyển về vận hành tại hạ tầng của đơn vị chủ trì thuê dịch vụ hoặc của chủ quản hệ thống thông tin...), thì đơn vị chủ trì thuê dịch vụ được xác định là đơn vị vận hành hệ thống thông tin.

¹⁵ Điều 15 Thông tư số 12/2022/TT-BTTTT.

Chương 3.

Thẩm định, phê duyệt cấp độ an toàn hệ thống thông tin

1. Thẩm quyền thẩm định, phê duyệt cấp độ

Thẩm quyền thẩm định và phê duyệt cấp độ an toàn thông tin đối với các hệ thống thông tin được quy định tại Điều 12 Nghị định số 85/2016/NĐ-CP:

1.1. Đối với hệ thống thông tin đề xuất cấp độ 1 hoặc cấp độ 2

Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện thẩm định, phê duyệt hồ sơ đề xuất cấp độ đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2.

Ví dụ thực tế: Nếu UBND tỉnh là chủ quản hệ thống thông tin thì Công an tỉnh sẽ thực hiện thẩm định, và phê duyệt HSĐXCĐ đối với hệ thống thông tin được đề xuất là cấp độ 1 hoặc cấp độ 2.

1.2. Đối với hệ thống thông tin đề xuất cấp độ 3

a) Thẩm định: Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện thẩm định hồ sơ đề xuất cấp độ.

b) Phê duyệt: Chủ quản hệ thống thông tin phê duyệt cấp độ an toàn thông tin trên cơ sở ý kiến thẩm định của đơn vị chuyên trách về an toàn thông tin.

Ví dụ thực tế: Nếu UBND tỉnh là chủ quản hệ thống thông tin thì Công an tỉnh thực hiện thẩm định HSĐXCĐ đối với hệ thống thông tin được đề xuất là cấp độ 3; UBND thực hiện phê duyệt cấp độ.

1.3. Đối với hệ thống thông tin đề xuất cấp độ 4 hoặc cấp độ 5

a) Thẩm định:

Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) chủ trì, phối hợp với Bộ Quốc phòng và các bộ, ngành liên quan thực hiện thẩm định hồ sơ đề xuất cấp độ, trừ trường hợp hệ thống thông tin do Bộ Quốc phòng quản lý.

b) Phê duyệt:

- Chủ quản hệ thống thông tin phê duyệt cấp độ an toàn thông tin đối với hệ thống thông tin đề xuất cấp độ 4; phê duyệt phương án bảo đảm an toàn thông tin đối với hệ thống thông tin đề xuất cấp độ 5;

- Thủ tướng Chính phủ phê duyệt danh mục hệ thống thông tin cấp độ 5 (danh mục hệ thống thông tin quan trọng quốc gia).

2. Tổ chức thẩm định hồ sơ đề xuất cấp độ

2.1. Thành phần Hồ sơ đề nghị thẩm định

Căn cứ quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP và khoản 7 Điều 9 Thông tư số 12/2022/TT-BTTTT, hồ sơ đề xuất cấp độ gửi thẩm định gồm các tài liệu sau đây:

(1) Văn bản đề nghị thẩm định, phê duyệt hồ sơ đề xuất cấp độ theo Mẫu số 01 được ban hành kèm theo Nghị định số 85/2016/NĐ-CP (đối với hệ thống thông tin đề xuất cấp độ 1 hoặc cấp độ 2) hoặc Văn bản đề nghị thẩm định hồ sơ đề xuất cấp độ theo Mẫu số 02 được ban hành kèm theo Nghị định số 85/2016/NĐ-CP (đối với hệ thống thông tin đề xuất cấp độ 3 trở lên).

(2) Tài liệu hồ sơ đề xuất cấp độ bao gồm các tài liệu thành phần sau đây:

- Tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin, có đầy đủ các nội dung theo quy định tại khoản 3 Điều 8 Thông tư số 12/2022/TT-BTTTT;

- Tài liệu thuyết minh về việc đề xuất cấp độ, có đầy đủ các nội dung theo quy định tại khoản 4 Điều 8 Thông tư số 12/2022/TT-BTTTT. Trường hợp hệ thống thông tin được đề xuất cấp độ 4 hoặc cấp độ 5, cần làm rõ thêm các nội dung theo quy định tại khoản 5 Điều 8 Thông tư số 12/2022/TT-BTTTT;

- Tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng, có đầy đủ các nội dung thuyết minh đáp ứng các yêu cầu về quản lý và kỹ thuật ứng với cấp độ đề xuất, theo quy định tại khoản 6 Điều 8, Điều 9 và Điều 10 Thông tư số 12/2022/TT-BTTTT.

(3) Tài liệu thiết kế hệ thống thông tin.

(4) Dự thảo quy chế hoặc quy chế bảo đảm an toàn thông tin đã được cấp có thẩm quyền ban hành và các văn bản, quy chế được tham chiếu, áp dụng.

(5) Văn bản ý kiến chuyên môn của đơn vị chuyên trách về an toàn thông tin đối với hệ thống thông tin được đề xuất cấp độ 4 hoặc cấp độ 5.

2.2. Thẩm định hồ sơ đề xuất cấp độ

Sau khi nhận được đầy đủ hồ sơ hợp lệ theo quy định, cơ quan/đơn vị có thẩm quyền thẩm định hồ sơ đề xuất cấp độ (sau đây gọi tắt là đơn vị thẩm định) tiến hành thẩm định hồ sơ với các nội dung cụ thể như sau:

2.2.1. Nội dung thẩm định hồ sơ đề xuất cấp độ

Theo quy định tại khoản 1 Điều 16 Nghị định số 85/2016/NĐ-CP, nội dung thẩm định hồ sơ đề xuất cấp độ bao gồm:

(1) Sự phù hợp về việc đề xuất cấp độ;

(2) Sự phù hợp của phương án bảo đảm an toàn hệ thống thông tin trong thiết kế sơ bộ, thiết kế thi công hoặc tài liệu có giá trị tương đương theo cấp độ tương ứng (tài liệu thiết kế hệ thống thông tin);

(3) Sự phù hợp của phương án bảo đảm an toàn hệ thống thông tin trong quá trình vận hành hệ thống theo cấp độ tương ứng.

2.2.2. Thẩm định sự phù hợp về việc đề xuất cấp độ

a) Nội dung cần xem xét để làm rõ sự phù hợp đối với cấp độ đề xuất:

- Mô tả phạm vi, quy mô của hệ thống thông tin thuộc tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin;

- Nội dung tài liệu thuyết minh về việc đề xuất cấp độ;
- Các nội dung có liên quan mô tả, làm rõ phạm vi, quy mô của hệ thống thông tin thuộc tài liệu thiết kế hệ thống thông tin.

b) Ý kiến thẩm định cần làm rõ:

- Sự phù hợp giữa loại thông tin mà hệ thống thông tin xử lý, được thuyết minh trong tài liệu thuyết minh về việc đề xuất cấp độ với quy định tại khoản 1 Điều 6 Nghị định số 85/2016/NĐ-CP; sự phù hợp, đồng bộ với loại thông tin có tính bí mật cao nhất mà hệ thống thông tin xử lý được thuyết minh trong tài liệu thiết kế hệ thống thông tin;

- Sự phù hợp giữa loại hình hệ thống thông tin được thuyết minh trong tài liệu thuyết minh về việc đề xuất cấp độ với các quy định tại khoản 2 Điều 6 Nghị định số 85/2016/NĐ-CP; sự phù hợp, đồng bộ với các nội dung có liên quan mô tả, làm rõ phạm vi, quy mô của hệ thống thông tin thuộc tài liệu thiết kế hệ thống thông tin;

- Sự phù hợp giữa cấp độ được đề xuất, được thuyết minh trong tài liệu thuyết minh về việc đề xuất cấp độ với các tiêu chí xác định cấp độ được quy định từ Điều 7 đến Điều 11 Nghị định số 85/2016/NĐ-CP; sự phù hợp, đồng bộ với nội dung mô tả phạm vi, quy mô của hệ thống thông tin thuộc tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin và các nội dung có liên quan mô tả, làm rõ phạm vi, quy mô của hệ thống thông tin thuộc tài liệu thiết kế hệ thống thông tin;

- Trong trường hợp hệ thống thông tin được đề xuất cấp độ 4 hoặc 5: Cho ý kiến thêm về sự phù hợp đối với các nội dung đặc thù được thuyết minh trong tài liệu thuyết minh về việc đề xuất cấp độ theo quy định tại khoản 5 Điều 8 Thông tư số 12/2022/TT-BTTTT, đồng bộ với các nội dung có liên quan mô tả, làm rõ phạm vi, quy mô của hệ thống thông tin thuộc tài liệu thiết kế hệ thống thông tin.

c) Kết quả đánh giá:

- Nội dung thẩm định đánh giá là “Đạt” nếu tất cả các nội dung được cho ý kiến thẩm định theo hướng dẫn tại điểm b ở trên được đánh giá là phù hợp;

- Nội dung thẩm định đánh giá là “Không đạt” nếu có ít nhất một trong các nội dung được cho ý kiến thẩm định theo hướng dẫn tại điểm b ở trên được đánh giá là không phù hợp.

2.2.3. Thẩm định sự phù hợp của phương án bảo đảm an toàn hệ thống thông tin trong tài liệu thiết kế hệ thống thông tin

a) Nội dung cần xem xét:

- Mô tả hiện trạng kiến trúc hệ thống (đối với hệ thống thông tin đang vận hành) hoặc kiến trúc hệ thống (đối với hệ thống thông tin được xây dựng mới hoặc nâng cấp, mở rộng) thuộc tài liệu mô tả, thuyết minh tổng quan hệ thống thông tin;

- Nội dung tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng;

- Dự thảo quy chế bảo đảm an toàn thông tin cho hệ thống thông tin hoặc

quy chế đã được cấp có thẩm quyền ban hành;

- Các nội dung có liên quan, mô tả, làm rõ mô hình kiến trúc tổng thể, mô hình lô-gic, mô hình vật lý của hệ thống, thuyết minh phương án bảo đảm an toàn thông tin (về quản lý và kỹ thuật) thuộc tài liệu thiết kế hệ thống thông tin.

b) Ý kiến thẩm định:

- Đối với nội dung phương án đáp ứng các yêu cầu về quản lý tương ứng với cấp độ đề xuất được thuyết minh trong tài liệu thuyết minh phương án bảo đảm an toàn thông tin:

- + Cho ý kiến tổng quan về sự phù hợp và đầy đủ giữa các nội dung được thuyết minh với các quy định tại Điều 9, Điều 10 và Phụ lục tương ứng với cấp độ đề xuất được ban hành kèm theo Thông tư số 12/2022/TT-BTTTT;

- + Cho ý kiến về sự phù hợp và đồng bộ giữa nội dung về quản lý thiết kế, xây dựng hệ thống được thuyết minh trong hồ sơ đề xuất cấp độ với các nội dung quy định, quy trình kèm theo dự thảo quy chế bảo đảm an toàn thông tin cho hệ thống thông tin hoặc quy chế đã được cấp có thẩm quyền ban hành;

- + Cho ý kiến về sự phù hợp, đồng bộ giữa nội dung thuyết minh về quản lý thiết kế, xây dựng hệ thống với các nội dung về chính sách quản lý trong tài liệu thiết kế hệ thống thông tin. Ví dụ: Chính sách về quyền sở hữu thông tin, dữ liệu hình thành trong quá trình thuê dịch vụ công nghệ thông tin với phương án quản lý rủi ro an toàn thông tin và phương án kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin theo quy định tại khoản 2 Điều 19 Nghị định số 85/2016/TT-BTTTT và khoản 3 Điều 9 Thông tư số 12/2022/TT-BTTTT.

- Đối với thuyết minh phương án đáp ứng các yêu cầu về kỹ thuật tương ứng với cấp độ đề xuất được thuyết minh trong tài liệu thuyết minh phương án bảo đảm an toàn thông tin:

- + Cho ý kiến về sự phù hợp giữa nội dung mô tả hiện trạng kiến trúc hệ thống hoặc mô tả kiến trúc hệ thống thuộc tài liệu mô tả, thuyết minh tổng quan về hệ thống thông tin với các quy định tại điểm d khoản 3 Điều 8, Điều 9, Điều 10 và Phụ lục tương ứng với cấp độ đề xuất được ban hành kèm theo Thông tư số 12/2022/TT-BTTTT; sự phù hợp, đồng bộ với các nội dung có liên quan, mô tả, làm rõ mô hình kiến trúc tổng thể, mô hình lô-gic, mô hình vật lý của hệ thống thuộc tài liệu thiết kế hệ thống thông tin;

- + Cho ý kiến về sự phù hợp, đầy đủ giữa nội dung thuyết minh phương án đáp ứng các yêu cầu về kỹ thuật với các quy định tương ứng tại Điều 9, Điều 10 và Phụ lục tương ứng với cấp độ đề xuất được ban hành kèm theo Thông tư số 12/2022/TT-BTTTT; sự phù hợp, đồng bộ với các nội dung thuyết minh về yêu cầu kỹ thuật đối với hệ thống thông tin tài liệu thiết kế hệ thống thông tin;

- + Tài liệu thiết kế hệ thống thông tin phải có thuyết minh, làm rõ các yêu cầu về phần mềm nội bộ được quy định tại khoản 8 Điều 9 Thông tư số 12/2022/TT-BTTTT, đồng bộ với nội dung thuyết minh phương án đáp ứng các yêu cầu về kỹ thuật trong tài liệu thuyết minh phương án bảo đảm an toàn thông tin;

+ Trường hợp hệ thống thông tin được đề xuất cấp độ 3, 4 hoặc 5 được triển khai dưới hình thức thuê dịch vụ công nghệ thông tin tại Trung tâm dữ liệu hoặc Điện toán đám mây: Thiết kế hệ thống phải đáp ứng quy định tương ứng tại khoản 9 và khoản 10 Điều 9 Thông tư số 12/2022/TT-BTTTT, đồng bộ với nội dung thuyết minh phương án đáp ứng các yêu cầu về kỹ thuật trong tài liệu thuyết minh phương án bảo đảm an toàn thông tin.

c) Kết quả đánh giá:

- Nội dung thẩm định đánh giá là “Đạt” nếu tất cả các nội dung được cho ý kiến thẩm định theo hướng dẫn tại điểm b ở trên được đánh giá là phù hợp;

- Nội dung thẩm định đánh giá là “Không đạt” nếu có ít nhất một trong các nội dung được cho ý kiến thẩm định theo hướng dẫn tại điểm b ở trên được đánh giá là không phù hợp.

2.2.4. Thẩm định sự phù hợp của phương án bảo đảm an toàn hệ thống thông tin trong quá trình vận hành hệ thống theo cấp độ tương ứng

a) Nội dung cần xem xét:

- Nội dung tài liệu thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng;

- Dự thảo quy chế bảo đảm an toàn thông tin cho hệ thống thông tin hoặc quy chế đã được cấp có thẩm quyền ban hành;

- Các nội dung có liên quan, mô tả, làm rõ thuyết minh phương án bảo đảm an toàn thông tin (về quản lý và kỹ thuật) thuộc tài liệu thiết kế hệ thống thông tin.

b) Nội dung thẩm định:

- Đối với thuyết minh phương án đáp ứng các yêu cầu về quản lý tương ứng với cấp độ đề xuất được thuyết minh trong tài liệu thuyết minh phương án bảo đảm an toàn thông tin: Cho ý kiến về sự phù hợp của các nội dung về quản lý (ngoài các nội dung về quản lý thiết kế, xây dựng hệ thống), khi đưa hệ thống thông tin vào vận hành khai thác.

- Đối với thuyết minh phương án đáp ứng các yêu cầu về kỹ thuật tương ứng với cấp độ đề xuất được thuyết minh trong tài liệu thuyết minh phương án bảo đảm an toàn thông tin, trên cơ sở hiện trạng các phương án bảo đảm an toàn thông tin về mặt kỹ thuật đang được triển khai, cho ý kiến về sự phù hợp của lộ trình triển khai đầy đủ phương án đáp ứng các yêu cầu về kỹ thuật trong quá trình vận hành hệ thống thông tin, bao gồm:

+ Trường hợp hạ tầng kỹ thuật phục vụ triển khai hệ thống thông tin chưa được thiết kế theo các phân vùng mạng đáp ứng yêu cầu tại Phụ lục tương ứng với cấp độ đề xuất được ban hành kèm theo Thông tư số 12/2022/TT-BTTTT: Cho ý kiến về sự phù hợp của lộ trình thực hiện phân tách các vùng mạng đáp ứng yêu cầu và phương án (về quản lý và kỹ thuật) tạm thời triển khai áp dụng trong giai đoạn phân vùng mạng chưa được thiết kế đáp ứng yêu cầu;

+ Đối với các yêu cầu về kỹ thuật hiện tại chưa đáp ứng: Cho ý kiến về sự

phù hợp của lộ trình dự kiến thực hiện phương án triển khai đáp ứng đầy đủ các yêu cầu về kỹ thuật và phương án (về quản lý và kỹ thuật) tạm thời triển khai áp dụng trong giai đoạn chưa triển khai đáp ứng đầy đủ các yêu cầu về kỹ thuật.

c) Kết quả đánh giá:

- Nội dung thẩm định đánh giá là “Đạt” nếu tất cả các nội dung được cho ý kiến thẩm định theo hướng dẫn tại điểm b ở trên được đánh giá là phù hợp;

- Nội dung thẩm định đánh giá là “Không đạt” nếu có ít nhất một trong các nội dung được cho ý kiến thẩm định theo hướng dẫn tại điểm b ở trên được đánh giá là không phù hợp;

- Đối với hệ thống thông tin đang vận hành: Trong trường hợp kết quả đánh giá là “Không đạt” và nhận thấy hệ thống thông tin chưa đáp ứng điều kiện để vận hành an toàn, đơn vị thẩm định có thể cho ý kiến nêu rõ các nguy cơ gây mất an toàn thông tin có thể xảy ra đối với hệ thống và yêu cầu đơn vị vận hành khẩn trương triển khai các biện pháp để bảo đảm an toàn thông tin trong quá trình vận hành hoặc báo cáo chủ quản hệ thống thông tin cho dừng hệ thống để triển khai các biện pháp bảo đảm an toàn thông tin.

2.2.5. Kết quả thẩm định hồ sơ đề xuất cấp độ

a) Hình thức phát hành:

Đơn vị thẩm định hồ sơ đề xuất cấp độ phát hành Văn bản ý kiến thẩm định theo Mẫu số 04 được ban hành kèm theo Nghị định số 85/2016/NĐ-CP, gửi đơn vị vận hành hệ thống thông tin.

b) Kết luận thẩm định:

- Hồ sơ đề xuất cấp độ của hệ thống thông tin được thuyết minh là phù hợp với cấp độ đề xuất và đủ điều kiện trình cấp có thẩm quyền phê duyệt cấp độ an toàn thông tin hoặc phê duyệt phương án bảo đảm an toàn thông tin nếu tất cả các nội dung thẩm định được đánh giá là “Đạt”;

- Hồ sơ đề xuất cấp độ của hệ thống thông tin được thuyết minh là chưa phù hợp theo cấp độ đề xuất nếu trong ý kiến thẩm định có nội dung được đánh giá “Không đạt”. Khi đó, đơn vị vận hành hệ thống thông tin cần thuyết minh bổ sung hoặc giải trình, làm rõ đối với các nội dung được đánh giá không đạt, gửi lại hồ sơ cho đơn vị thẩm định để tiếp tục tiến hành quy trình thẩm định theo quy định.

2.3. Thời gian thẩm định hồ sơ đề xuất cấp độ

a) Đối với hệ thống thông tin được đề xuất cấp độ 1 hoặc 2: Theo quy định tại khoản 2 Điều 17 Nghị định số 85/2016/NĐ-CP, thời gian xử lý phê duyệt (trong đó có thẩm định) tối đa là 07 ngày làm việc kể từ ngày nhận đủ hồ sơ hợp lệ.

b) Đối với hệ thống thông tin được đề xuất cấp độ 3, 4 hoặc 5 theo quy định tại khoản 2 Điều 16 Nghị định số 85/2016/NĐ-CP:

- Đối với hệ thống thông tin đề xuất cấp độ 3: Thời gian thẩm định tối đa là 15 ngày kể từ ngày nhận đủ hồ sơ hợp lệ;

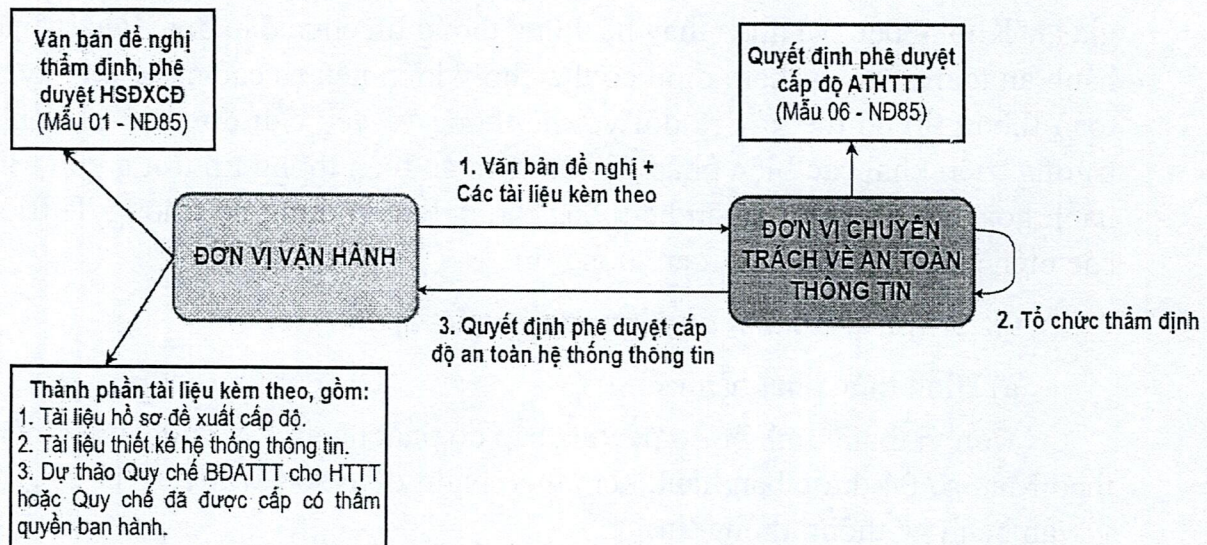
- Đối với hệ thống thông tin đề xuất cấp độ 4 hoặc cấp độ 5: Thời gian thẩm định tối đa là 30 ngày kể từ ngày nhận đủ hồ sơ hợp lệ.

Lưu ý: Trường hợp sau khi tổ chức thẩm định, hồ sơ đề xuất cấp độ của hệ thống thông tin được đánh giá chưa phù hợp, cần được điều chỉnh hoặc bổ sung, hoàn thiện, thời gian tổ chức thẩm định sẽ được tính lại kể từ thời điểm đơn vị thẩm định nhận được hồ sơ hoàn thiện.

3. Quy trình thẩm định, phê duyệt cấp độ

3.1. Đối với hệ thống thông tin đề xuất cấp độ 1 hoặc cấp độ 2

3.1.1. Sơ đồ quy trình



Hình 3. Quy trình thẩm định, phê duyệt cấp độ an toàn thông tin cấp độ 1, 2

3.1.2. Trình tự thực hiện

a) Bước 1. Gửi thẩm định hồ sơ đề xuất cấp độ:

Sau khi hoàn thành việc xây dựng hồ sơ đề xuất cấp độ, đơn vị vận hành hệ thống thông tin gửi hồ sơ đề nghị thẩm định, phê duyệt cấp độ an toàn thông tin tới đơn vị chuyên trách về an toàn thông tin hoặc đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ thẩm định, phê duyệt cấp độ an toàn thông tin để tổ chức thẩm định và phê duyệt.

b) Bước 2. Tổ chức thẩm định, phê duyệt cấp độ an toàn thông tin:

Đơn vị chuyên trách về an toàn thông tin hoặc đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ thẩm định, phê duyệt cấp độ an toàn thông tin:

- Thực hiện thẩm định hồ sơ đề xuất cấp độ theo quy định.
- Có Văn bản ý kiến thẩm định (theo Mẫu số 04 ban hành kèm theo Nghị định số 85/2016/NĐ-CP) gửi đơn vị vận hành hệ thống thông tin.

Trên cơ sở kết quả thẩm định:

- Trường hợp hồ sơ đề xuất cấp độ đã được thuyết minh phù hợp với cấp độ đề xuất và đủ điều kiện phê duyệt cấp độ an toàn thông tin, đơn vị đã thẩm định

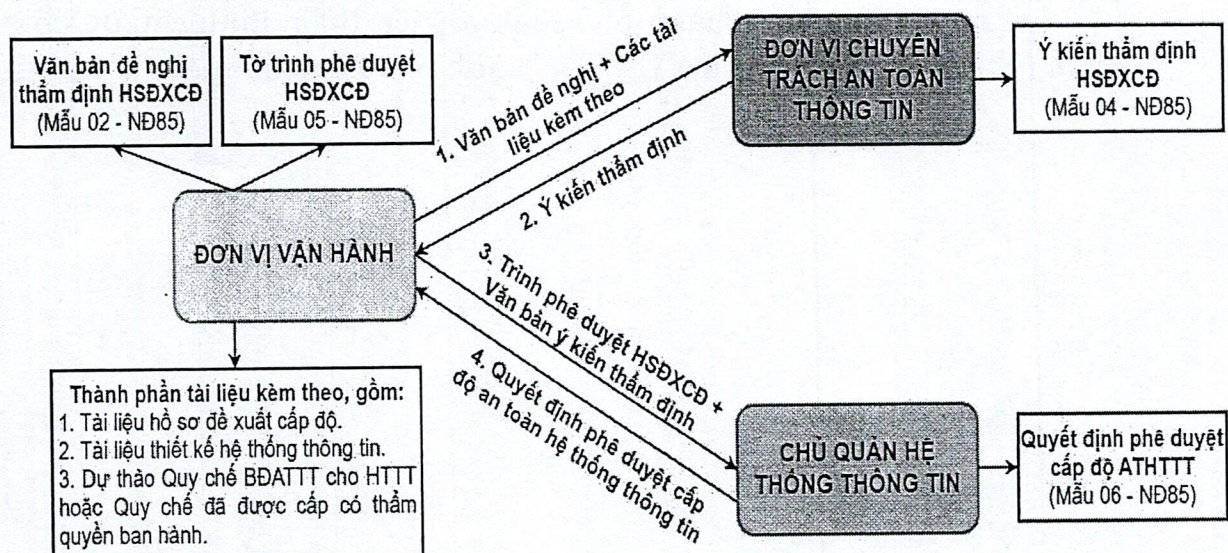
hồ sơ đề xuất cấp độ tiến hành ban hành quyết định phê duyệt cấp độ an toàn thông tin đối với hệ thống thông tin (theo Mẫu số 06 Nghị định số 85/2016/NĐ-CP), gửi báo cáo chủ quản hệ thống thông tin theo quy định;

- Trường hợp hồ sơ đề xuất cấp độ được thuyết minh chưa phù hợp với cấp độ đề xuất, đơn vị vận hành hệ thống thông tin cần thuyết minh bổ sung hoặc giải trình, làm rõ đối với các nội dung được đánh giá không đạt, gửi lại hồ sơ để đơn vị thẩm định để tiếp tục thực hiện. Thời gian giải quyết được tính lại kể từ thời điểm đơn vị thẩm định nhận được hồ sơ đầy đủ, hoàn thiện.

Lưu ý: Công an tỉnh sẽ thực hiện thẩm định, phê duyệt cấp độ đối với hệ thống thông tin cấp độ 1, 2 mà UBND tỉnh làm chủ quản hệ thống.

3.2. Đối với hệ thống thông tin đề xuất cấp độ 3

3.2.1. Sơ đồ quy trình



Hình 4. Quy trình thẩm định, phê duyệt cấp độ an toàn thông tin cấp độ 3

3.2.2. Trình tự thực hiện

a) Bước 1. Gửi thẩm định hồ sơ đề xuất cấp độ:

Sau khi hoàn thành việc xây dựng hồ sơ đề xuất cấp độ, đơn vị vận hành hệ thống thông tin gửi hồ sơ đề nghị thẩm định⁶² tới đơn vị chuyên trách về an toàn thông tin hoặc đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ thẩm định hồ sơ đề xuất cấp độ để tổ chức thẩm định.

b) Bước 2. Tổ chức thẩm định:

Đơn vị chuyên trách về an toàn thông tin hoặc đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ thẩm định hồ sơ đề xuất cấp độ an toàn thông tin:

- Thực hiện thẩm định hồ sơ đề xuất cấp độ theo quy định;
- Có Văn bản ý kiến thẩm định (theo Mẫu số 04 ban hành kèm theo Nghị định số 85/2016/NĐ-CP) gửi đơn vị vận hành hệ thống thông tin.

Trên cơ sở kết quả thẩm định, trường hợp hồ sơ đề xuất cấp độ được thuyết