



BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG
CỤC CÔNG NGHỆ THÔNG TIN VÀ DỮ LIỆU TÀI NGUYÊN MÔI TRƯỜNG

BÁO CÁO THAM LUẬN

Hướng dẫn triển khai ATTT theo cấp độ

Bùi Công Thịnh
Phòng KH&CN&ATTT
Cục CNTT & DLTNMT

Nội dung trình bày

- Tổng quan về đảm bảo ATTT theo cấp độ tại Bộ TNMT
 - Hướng dẫn lập, thẩm định và trình phê duyệt hồ sơ đề xuất cấp độ ATTT
 - Một số kinh nghiệm triển khai đảm bảo ATTT theo cấp độ
-

Tổng quan về đảm bảo ATTT theo cấp độ tại Bộ TNMT

Hiện trạng về pháp lý về ATTT

- Quyết định số 674/QĐ-BTNMT của Bộ Tài nguyên và Môi trường ngày 31/3/2017 về Kiện toàn Ban chỉ đạo ứng cứu khẩn cấp hoặc ban chỉ đạo ứng dụng công nghệ thông tin
 - Quyết định số 3210/QĐ-BTNMT ngày 24/10/2018 của Bộ Tài nguyên và Môi trường Ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng Bộ Tài nguyên và Môi trường
 - Quyết định 2555/QĐ-BTNMT ngày 24/12/2021 về việc thành lập Đội Ứng cứu sự cố an toàn thông tin mạng của Bộ và Quy chế hoạt động của Đội Ứng cứu sự cố an toàn thông tin mạng
 - Quyết định số 2686/QĐ-BTNMT ngày 04/01/2022 Ban hành Kế hoạch phát triển Chính phủ số và bảo đảm an toàn thông tin mạng giai đoạn 2021- 2025 của Bộ Tài nguyên và Môi trường
 - Quyết định số 1194/QĐ-TCMT ngày 11/9/2019 của Tổng cục Môi trường Ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng của Tổng cục Môi trường
-

Hiện trạng về pháp lý (các văn bản liên quan)

- **Quyết định số 3196/QĐ-BTNMT** của Bộ Tài nguyên và Môi trường ngày 16 tháng 12 năm 2019 Ban hành Kiến trúc Chính phủ điện tử ngành tài nguyên và môi trường (Phiên bản 2.0)
 - **Quyết định số 964/QĐ-BTNMT** của Bộ Tài nguyên và Môi trường ngày 17/04/2019 về kế hoạch hành động thực hiện Nghị quyết 17/NQ-CP về nhiệm vụ, giải pháp trọng tâm phát triển chính phủ điện tử giai đoạn 2019-2020, định hướng đến 2025
 - **Thông tư 14/2020/TT-BTNMT** ngày 27/11/2020 của Bộ trưởng Bộ Tài nguyên và Môi trường ban hành quy trình và định mức kinh tế - kỹ thuật xây dựng, duy trì, vận hành hệ thống thông tin ngành tài nguyên và môi trường
 - **Quyết định số 417/QĐ-BTNMT** ngày 10/3/2021 của Bộ trưởng Bộ Tài nguyên và Môi trường Phê duyệt Chương trình chuyển đổi số tài nguyên và môi trường đến năm 2025, định hướng đến năm 2030.
-

Hiện trạng công tác đánh giá cấp độ cho các HTTT trong Bộ TNMT

- Tổng số 69 hệ thống thông tin đã được lên danh sách để lập hồ sơ đề xuất cấp độ
- Trong đó 06 hệ thống cấp độ 1, 25 hệ thống cấp độ 2, 21 hệ thống cấp độ 3, 01 hệ thống cấp độ 4 và 01 hệ thống cấp độ 5
- Đã tiến hành đánh giá và ban hành được 13 hồ sơ đề xuất cấp độ bao gồm 01 hồ sơ cấp độ cấp độ 5, 08 hồ sơ đề xuất cấp độ 3, và 04 hệ thống đề xuất cấp độ 2.

Tổng số HTTT	Số lượng HTTT cấp độ 1,2	Số lượng HTTT cấp độ 3	Số lượng HTTT cấp độ 4	Số lượng HTTT cấp độ 5	Tổng số đã lập HSDXCĐ
69	31	21	01	01	13

Hướng dẫn lập, thẩm định và trình phê duyệt hồ sơ đề xuất cấp độ ATTT

Căn cứ pháp lý

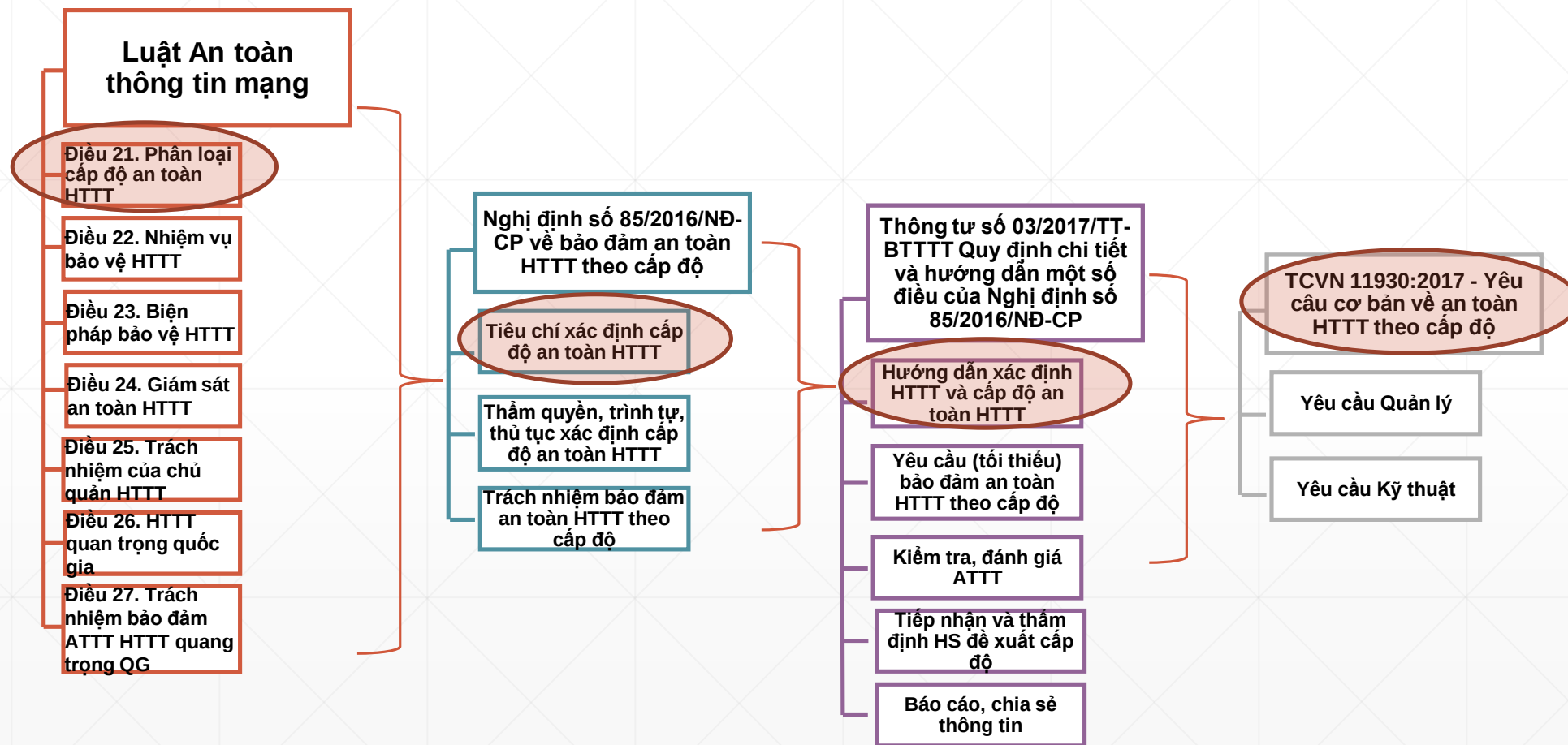
- Luật An an toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015;
 - Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018;
 - Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;
 - Thông tư 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ
 - Tiêu chuẩn quốc gia TCVN 11930:2017 về yêu cầu cơ bản đảm bảo an toàn HTTT theo cấp độ
 - Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 quy định chi tiết một số điều của Luật An ninh mạng
-

Căn cứ pháp lý liên quan khác

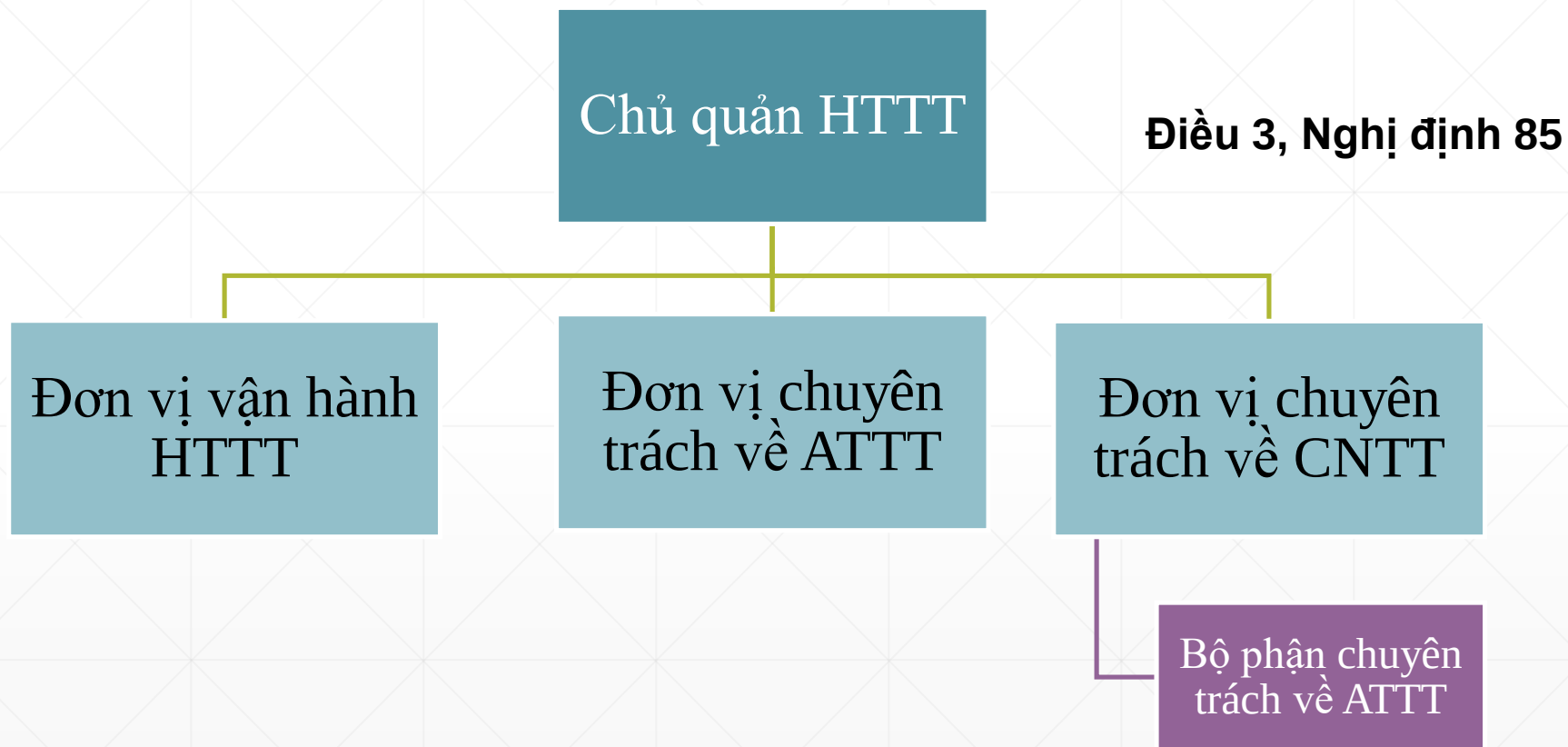
- Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại;
 - Chỉ thị số 14/CT-TTG ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;
 - Quyết định số 632/QĐ-TTg của Thủ tướng Chính phủ ngày 10 tháng 5 năm 2017 về việc Ban hành Danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia;
 - Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 03 năm 2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;
 - Thông tư số 20/2017/TT-BTTTT của Bộ Thông tin và Truyền thông ngày 12 tháng 9 năm 2017 quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;
 - Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;
-

HỆ THỐNG VĂN BẢN

Văn bản quy phạm pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ



Tổ chức, bộ máy



Phân loại thông tin

Phân loại thông tin theo thuộc tính bí mật

1

Thông tin công cộng

2

Thông tin riêng

3

Thông tin cá nhân

4

Thông tin bí mật nhà nước

Phân loại Hệ thống thông tin

Hướng dẫn xác định hệ thống thông tin cụ thể (Thông tư 03/2017/TT-BTTTT)

- 1 HTTT phục vụ hoạt động nội bộ
 - 2 HTTT phục vụ người dân, doanh nghiệp
 - 3 Hệ thống cơ sở hạ tầng thông tin
 - 4 HTTT điều khiển công nghiệp
-

Phân loại và xác định cấp độ

Cấp độ an toàn HTTT được phân loại tăng dần từ **cấp độ 1** đến **cấp độ 5** để áp dụng biện pháp quản lý và kỹ thuật nhằm bảo vệ HTTT phù hợp theo cấp độ

Cấp độ 1

Quyền và lợi ích hợp pháp của tổ chức, cá nhân

Cấp độ 2

Quyền và lợi ích hợp pháp của tổ chức, cá nhân, lợi ích công cộng

Cấp độ 3

Sản xuất, lợi ích công cộng, trật tự an toàn xã hội, quốc phòng, an ninh quốc gia

Cấp độ 4

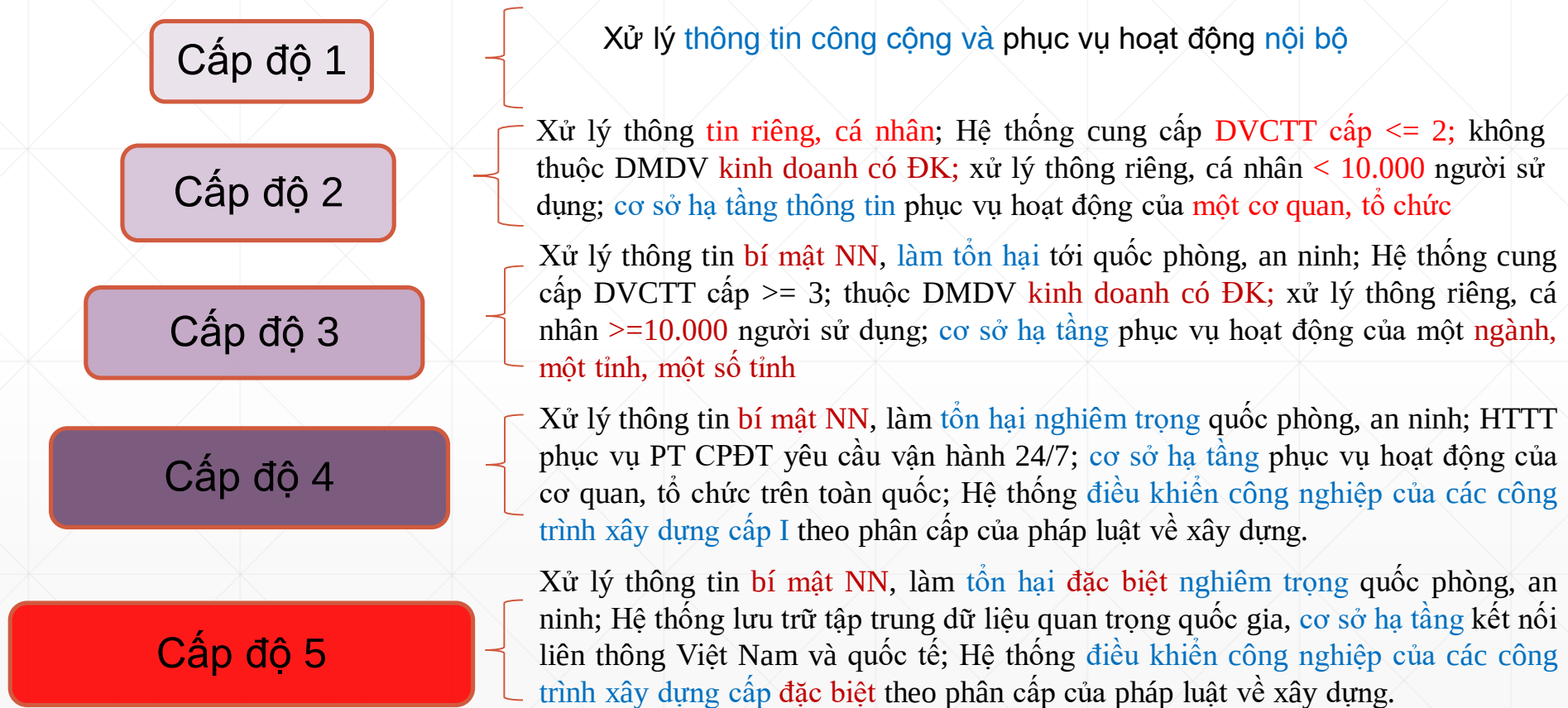
Lợi ích công cộng, trật tự an toàn xã hội, quốc phòng, an ninh quốc gia

Cấp độ 5

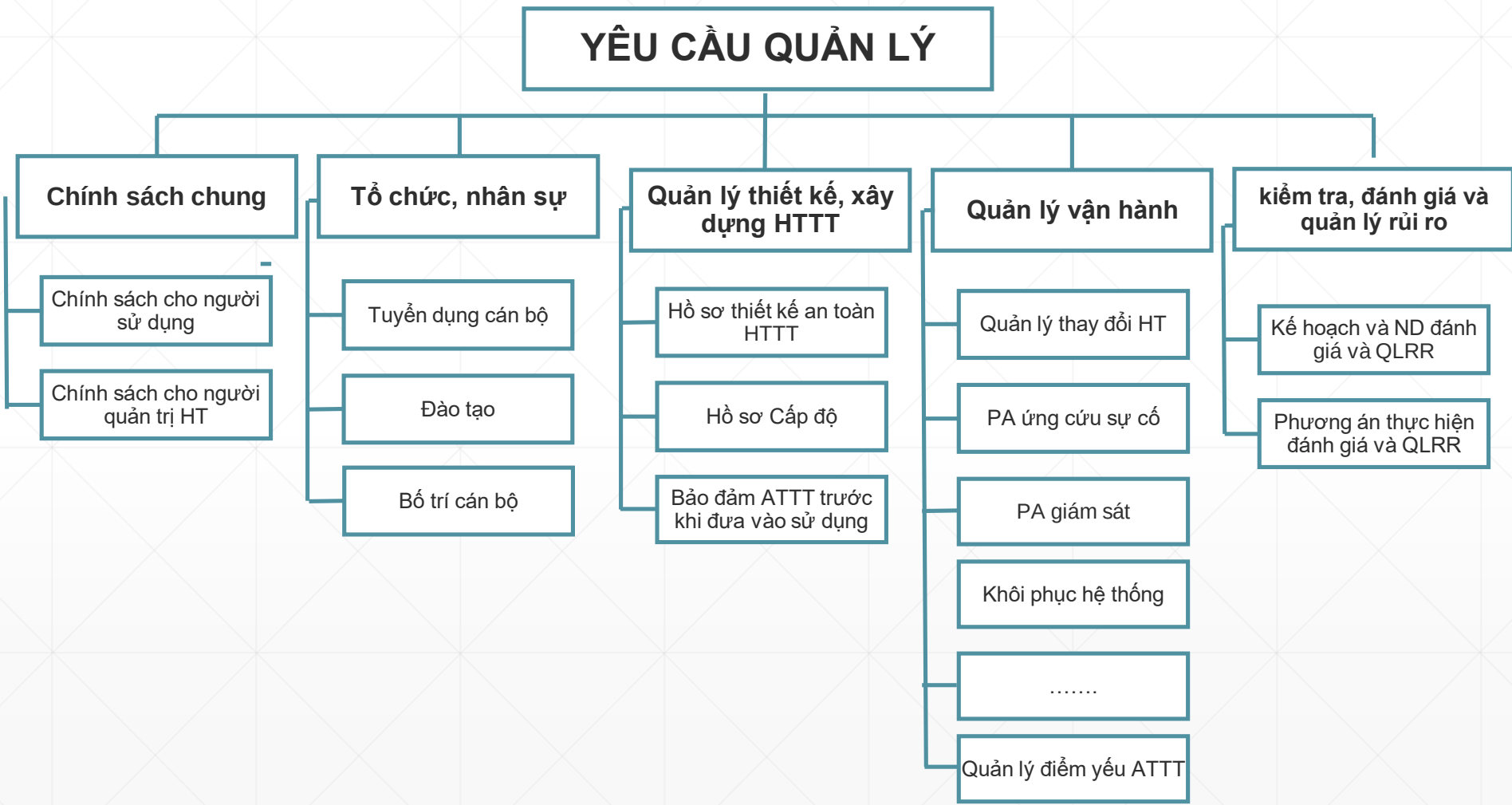
Quốc phòng an ninh, quốc gia (tổn hại đặc biệt nghiêm trọng)

Xác định cấp độ an toàn HTTT

Cấp độ an toàn HTTT được phân loại tăng dần từ **cấp độ 1** đến **cấp độ 5** để áp dụng biện pháp quản lý và kỹ thuật nhằm bảo vệ HTTT phù hợp theo cấp độ



Các yêu cầu đảm bảo ATTT



Các yêu cầu đảm bảo ATTT



Hướng dẫn xây dựng Thuyết minh đề xuất cấp độ ATTT cho HTTT

Hồ sơ đề xuất cấp độ

STT	Tên tài liệu	Ghi chú
I	Thuyết minh đề xuất cấp độ	
1.1	Nội dung mô tả, thuyết minh tổng quan về hệ thống thông tin	Mục 1 Điều 15 Nghị định 85/2016/NĐ-CP
1.2	Nội dung thuyết minh về đề xuất cấp độ	Mục 3 Điều 15 Nghị định 85/2016/NĐ-CP
1.3	Nội dung thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng	Mục 4 Điều 15 Nghị định 85/2016/NĐ-CP
II	Các tài liệu thiết kế	Mục 2 Điều 15 Nghị định 85/2016/NĐ-CP

Thuyết minh Hồ sơ đề xuất cấp độ

PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN THUỘC PHẠM VI QUẢN LÝ

1. Thông tin Chủ quản hệ thống thông tin

2. Thông tin Đơn vị vận hành

3. Mô tả phạm vi, quy mô của hệ thống

3.1 Phạm vi

3.2 Quy mô

4. Mô tả cấu trúc của hệ thống

4.1 Sơ đồ logic tổng thể

4.2 Sơ đồ kết nối vật lý

4.3 Danh mục thiết bị sử dụng trong hệ thống

4.4 Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

4.5 Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ

I. Mô tả tổng quan về HTTT

- Chủ quản Hệ thống thông tin (Đ5 – TT03)
- Đơn vị vận hành (Đ6 – TT03)
- Quy mô, phạm vi của hệ thống (phạm vi, đối tượng sử dụng, danh mục ứng dụng dịch vụ cung cấp...)
- Cấu trúc vật lý và logic của hệ thống, quy hoạch các vùng mạng chức năng của hệ thống
- Mô tả Chức năng của các thành phần/hệ thống thành phần

II. Thuyết minh đề xuất cấp độ

1. Thông tin về các hệ thống thông tin thuộc phạm vi quản lý

STT	Tên HTTT	Loại hình HTTT (Đ4 - TT03)	Thông tin xử lý	Cấp độ đề xuất
1	Hệ thống A	Phục vụ hoạt động nội bộ	Công khai	1
2	Hệ thống B	Phục vụ người dân và doanh nghiệp	Thông tin cá nhân	2
3	Hệ thống C	Hệ thống cơ sở hạ tầng thông tin	Thông tin công khai	3
4	Hệ thống D	Hệ thống thông tin điều khiển công nghiệp	Thông tin riêng	3
...				

2. Thuyết minh đề xuất cấp độ đối với từng hệ thống cụ thể (Đ7-11 NDD85 & Đ7 TT03)

- Hệ thống thông tin A
- Thuyết minh về cơ sở xác định loại hình HTTT
- Thuyết minh về các loại thông tin hệ thống đó xử lý.
- Căn cứ theo tiêu chí xác định tại Điều X, Nghị định số 85 => Hệ thống thông tin được đề xuất cấp độ A.
- Hệ thống thông tin B...

Thuyết minh Hồ sơ đề xuất cấp độ

PHẦN II. THUYẾT MINH ĐỀ XUẤT CẤP ĐỘ AN TOÀN CHO HỆ THỐNG ABC

- 2.1. Danh mục hệ thống thông tin và cấp độ đề xuất tương ứng
- 2.2. Thuyết minh đề xuất cấp độ đối với Hệ thống ABC

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ

- I. Mô tả tổng quan về HTTT**
- Chủ quản Hệ thống thông tin (Đ5 – TT03)
 - Đơn vị vận hành (Đ6 – TT03)
 - Quy mô, phạm vi của hệ thống (phạm vi, đối tượng sử dụng, danh mục ứng dụng dịch vụ cung cấp...)
 - Cấu trúc vật lý và logic của hệ thống, quy hoạch các vùng mạng chức năng của hệ thống
 - Mô tả Chức năng của các thành phần/hệ thống thành phần

- II. Thuyết minh đề xuất cấp độ**
- 1. Thông tin về các hệ thống thông tin thuộc phạm vi quản lý**

STT	Tên HTTT	Loại hình HTTT (Đ4 - TT03)	Thông tin xử lý	Cấp độ đề xuất
1	Hệ thống A	Phục vụ hoạt động nội bộ	Công khai	1
2	Hệ thống B	Phục vụ người dân và doanh nghiệp	Thông tin cá nhân	2
3	Hệ thống C	Hệ thống cơ sở hạ tầng thông tin	Thông tin công khai	3
4	Hệ thống D	Hệ thống thông tin điều khiển công nghiệp	Thông tin riêng	3
...				

- 2. Thuyết minh đề xuất cấp độ đối với từng hệ thống cụ thể (Đ7-11 NDD85 & Đ7 TT03)**
- Hệ thống thông tin A
 - Thuyết minh về cơ sở xác định loại hình HTTT
 - Thuyết minh về các loại thông tin hệ thống đó xử lý.
 - Căn cứ theo tiêu chí xác định tại Điều X, Nghị định số 85 => Hệ thống thông tin được đề xuất cấp độ A.
 - Hệ thống thông tin B...

Thuyết minh Hồ sơ đề xuất cấp độ

PHẦN III. THUYẾT MINH PHƯƠNG ÁN ĐẢM BẢO AN TOÀN HỆ THỐNG THÔNG TIN

3.1. Thuyết minh phương án bảo đảm an toàn thông tin đáp ứng các yêu cầu an toàn cơ bản về Quản lý

3.1.1. Xây dựng quy chế đảm bảo an toàn thông tin

- a) Quy chế đảm bảo an toàn thông tin
- b) Quy chế vận hành
- c) Phạm vi chính sách an toàn thông tin
- d) Xây dựng chính sách an toàn thông tin
- b) Xây dựng và công bố
- c) Rà soát, sửa đổi

3.1.2. Tổ chức bảo đảm an toàn thông tin

- a) Đơn vị chuyên trách về an toàn thông tin
- b) Phối hợp với những cơ quan/tổ chức có thẩm quyền

3.1.3. Đảm bảo nguồn nhân lực

- a) Tuyển dụng
- b) Trong quá trình làm việc
- c) Chấm dứt hoặc thay đổi công việc

3.1.4 Quản lý thiết kế, xây dựng hệ thống thông tin

- a) Thiết kế an toàn hệ thống thông tin
- b) Phát triển phần mềm thuê khoán
- c) Thử nghiệm và nghiệm thu hệ thống

3.1.5 Quản lý vận hành hệ thống thông tin

- a) Quản lý an toàn mạng
 - b) Quản lý an toàn máy chủ và ứng dụng
 - c) Quản lý an toàn dữ liệu
 - d) Quản lý an toàn thiết bị đầu cuối
 - f) Quản lý phòng chống phần mềm độc hại
 - g) Quản lý giám sát an toàn hệ thống thông tin
 - h) Quản lý điểm yếu an toàn thông tin
 - i) Quản lý sự cố an toàn thông tin
 - k) Quản lý an toàn người sử dụng đầu cuối
-

Thuyết minh Hồ sơ đề xuất cấp độ

PHẦN III. THUYẾT MINH PHƯƠNG ÁN ĐẢM BẢO AN TOÀN HỆ THỐNG THÔNG TIN

3.2. Thuyết minh phương án đáp ứng yêu cầu kỹ thuật

3.2.1. Bảo đảm an toàn mạng

- a) Thiết kế hệ thống
- b) Kiểm soát truy cập từ bên ngoài mạng
- c) Kiểm soát truy cập từ bên trong mạng
- d) Nhật ký hệ thống
- e) Phòng chống xâm nhập
- f) Phòng chống phần mềm độc hại trên môi trường mạng
- g) Bảo vệ thiết bị hệ thống

3.2.2. Bảo đảm an toàn máy chủ

- a) Xác thực
- b) Kiểm soát truy cập
- c) Nhật ký hệ thống
- d) Phòng chống xâm nhập
- e) Phòng chống phần mềm độc hại
- f) Xử lý máy chủ khi chuyển giao

3.2.3 Bảo đảm an toàn ứng dụng

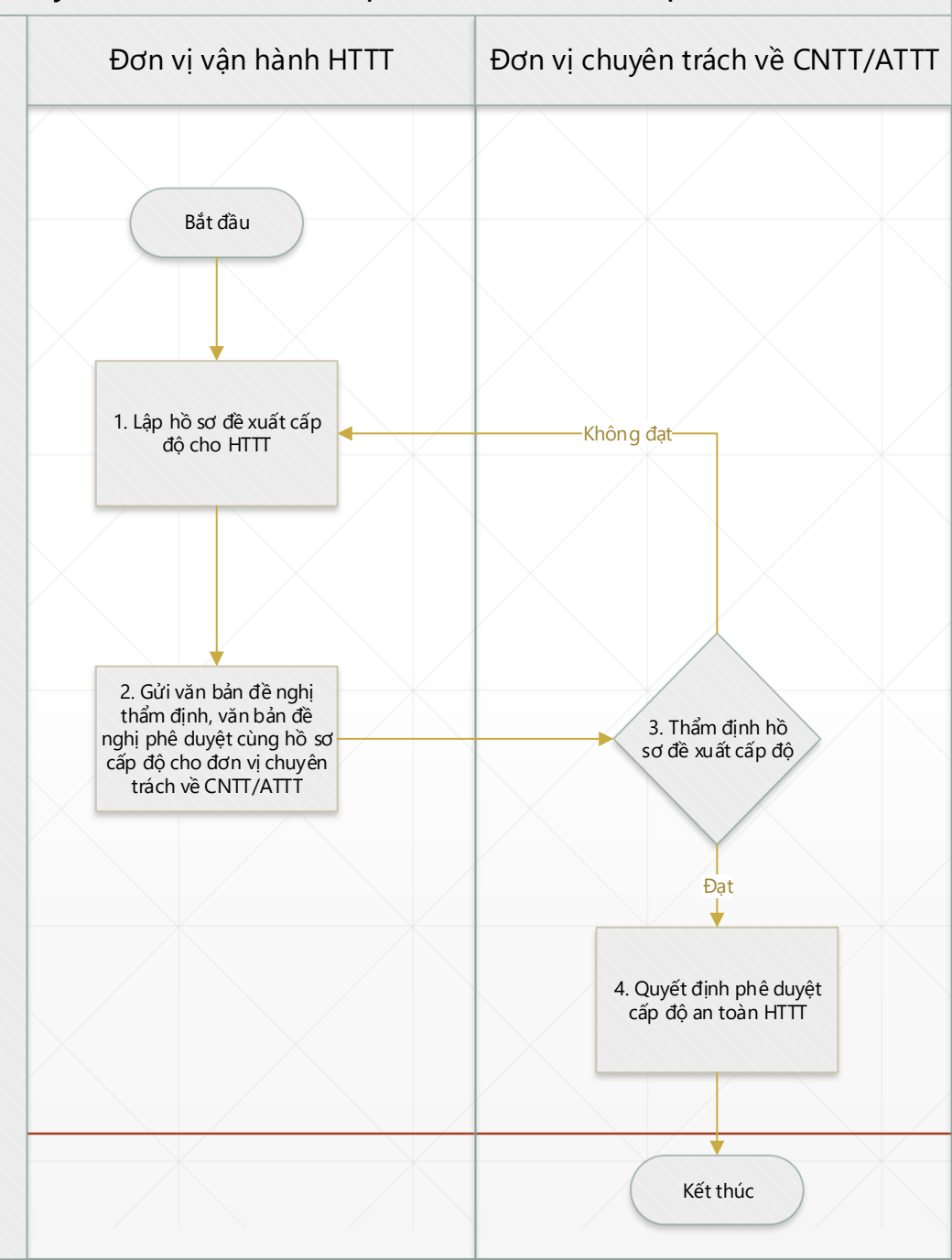
- a) Xác thực
- b) Kiểm soát truy cập
- c) Nhật ký hệ thống
- d) Bảo mật thông tin liên lạc
- e) Chống chối bỏ
- g) An toàn ứng dụng và mã nguồn

3.2.3. Bảo đảm an toàn dữ liệu

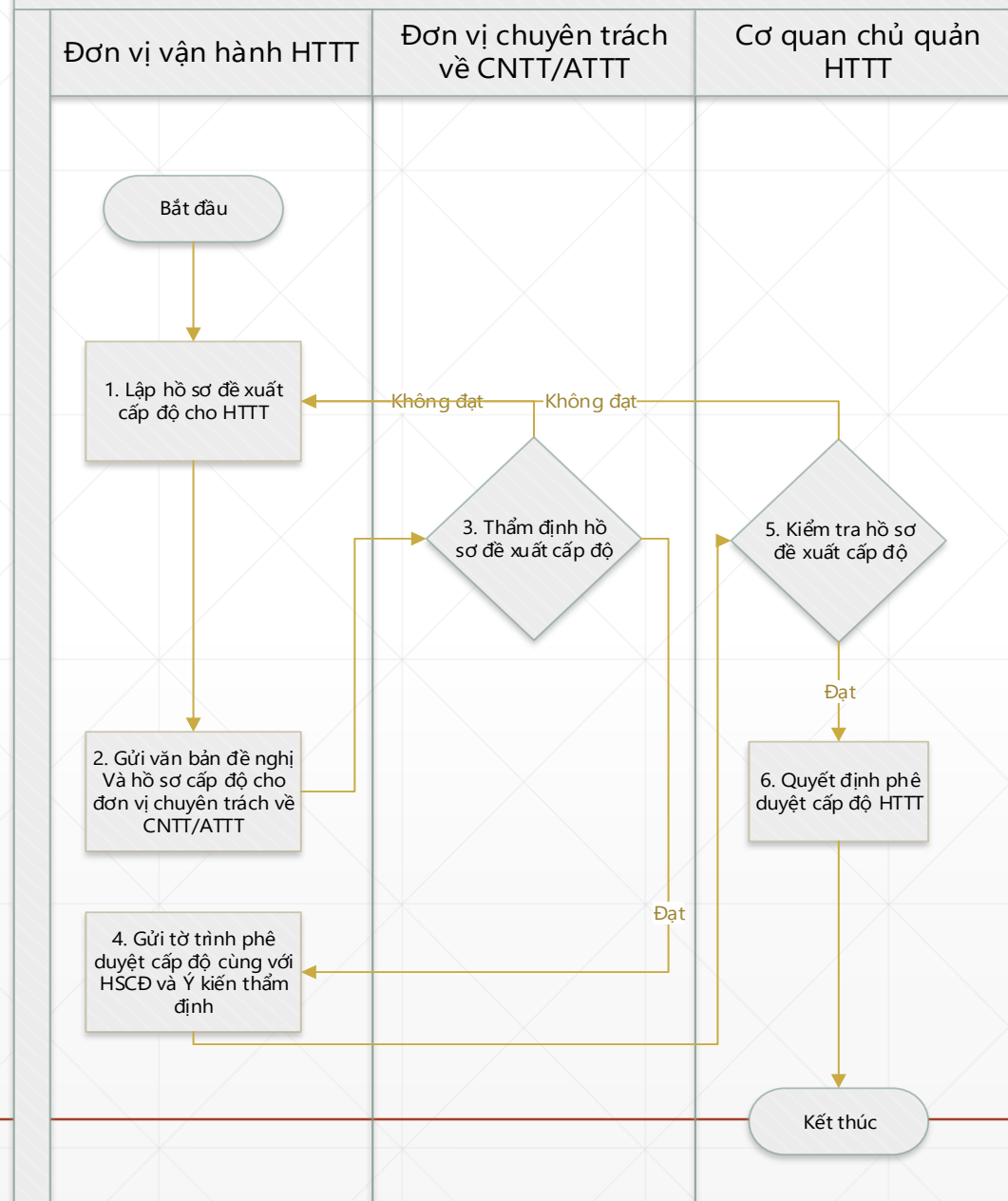
- a) Nguyên vẹn dữ liệu
 - b) Bảo mật dữ liệu
 - b) Sao lưu dự phòng
-

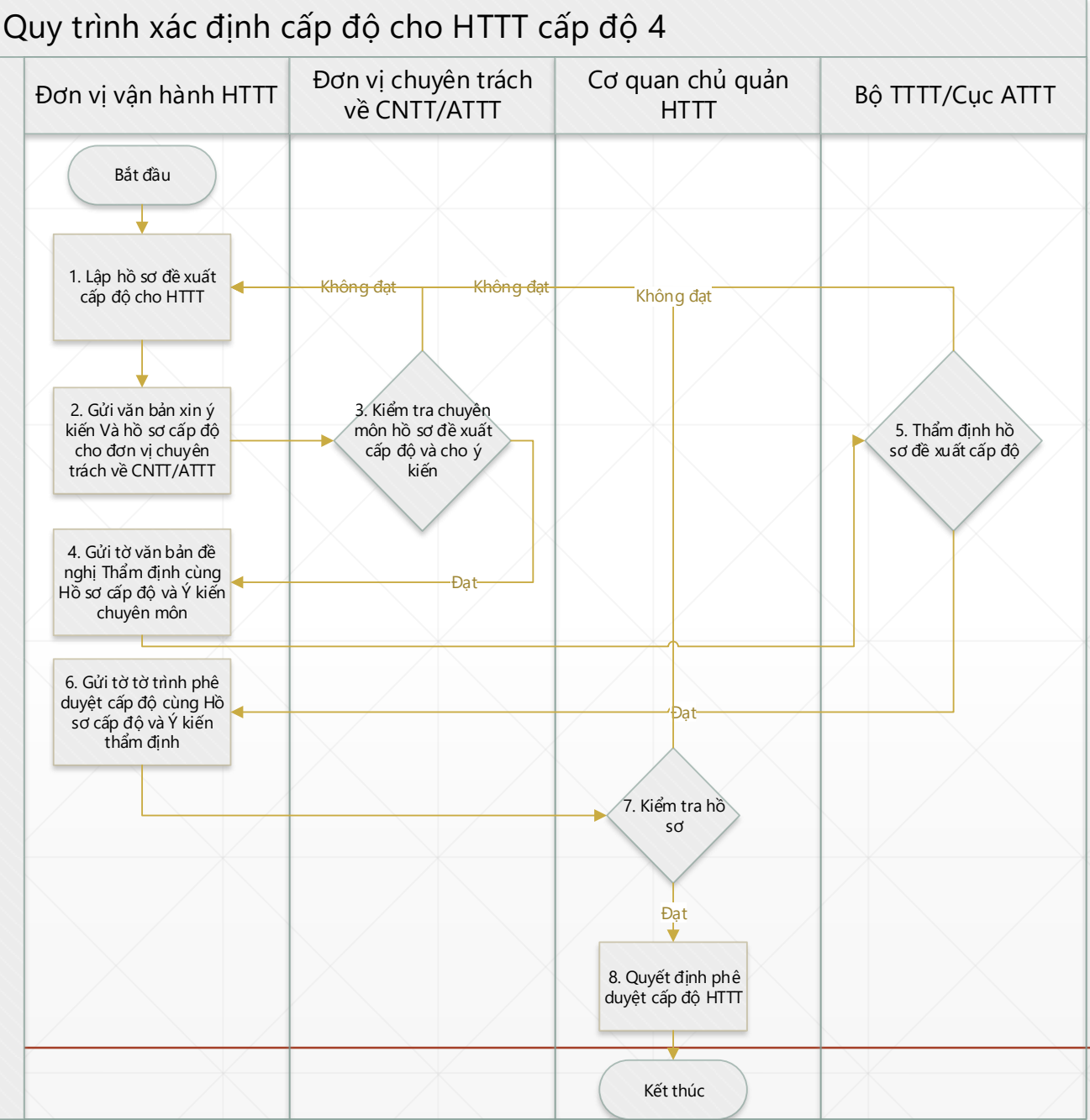
Quy trình thẩm định hồ sơ đề xuất cấp độ

Quy trình xác định cấp độ cho HTTT cấp độ 1 và 2

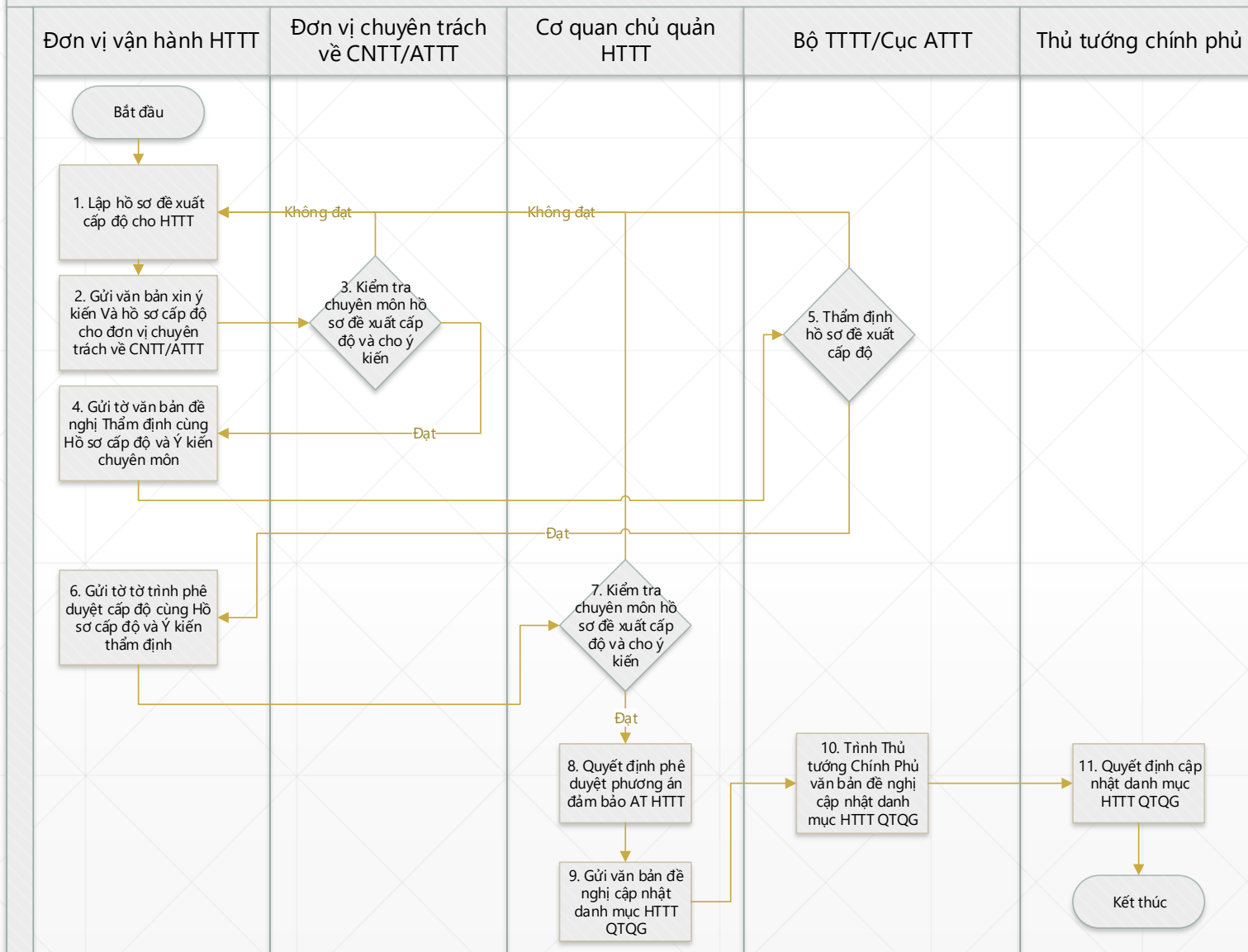


Quy trình xác định cấp độ cho HTTP cấp độ 3

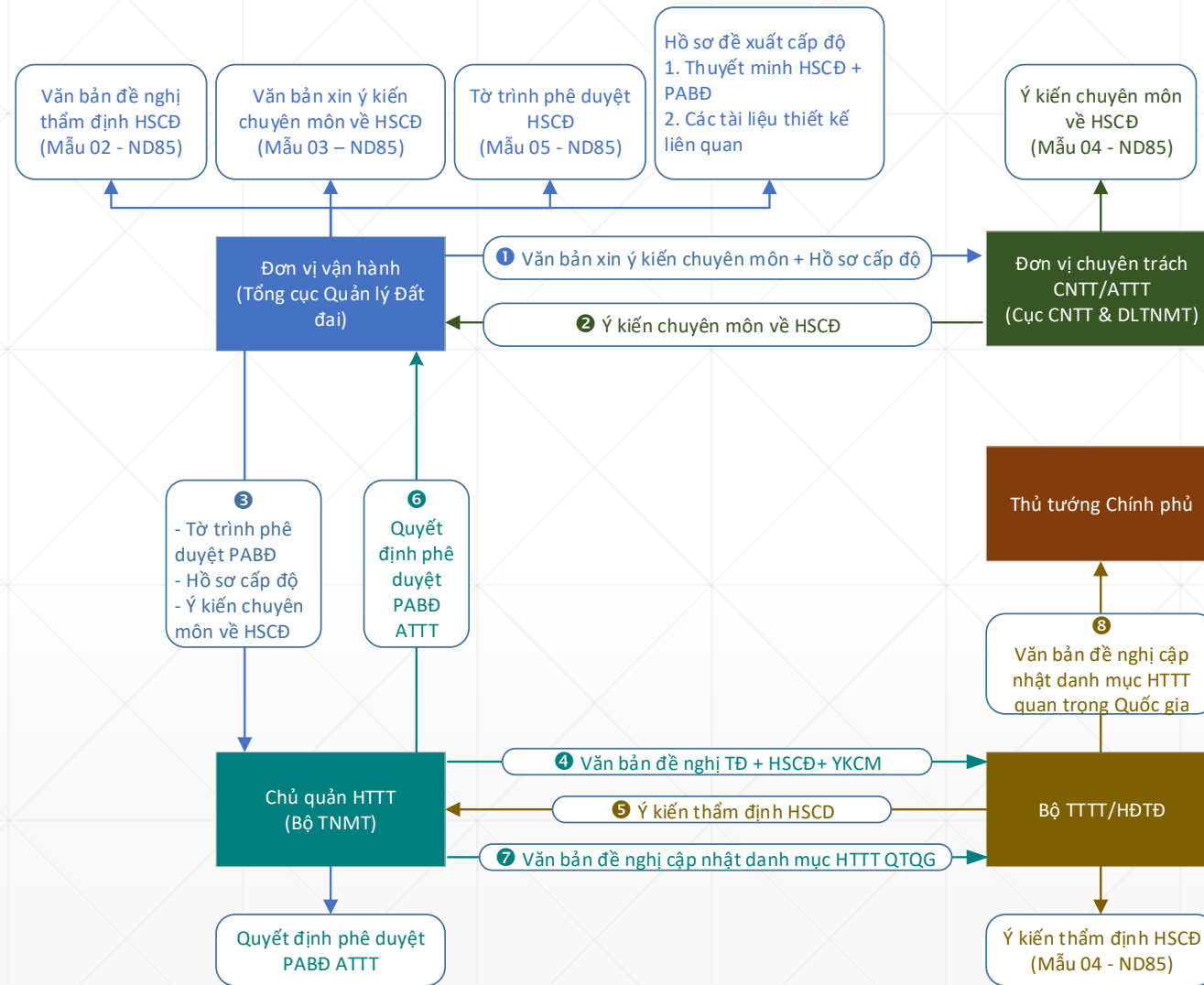




Quy trình xác định cấp độ cho HTTT cấp độ 5



Ví dụ minh họa cụ thể: Quy trình xác định cấp độ 5 cho hệ thống thông tin đất đai quốc gia



Ghi chú

- HSCĐ: Hồ sơ đề xuất cấp độ (Điều 15, ND85)
- PABĐ: hương án đảm bảo an toàn HTTT (Điều 19, ND85)

Một số kinh nghiệm triển khai đảm bảo ATTT theo cấp độ

Một số kinh nghiệm thực tiễn đẩy mạnh công tác đảm bảo ATTT theo cấp độ

1. Lập danh sách các HTTT

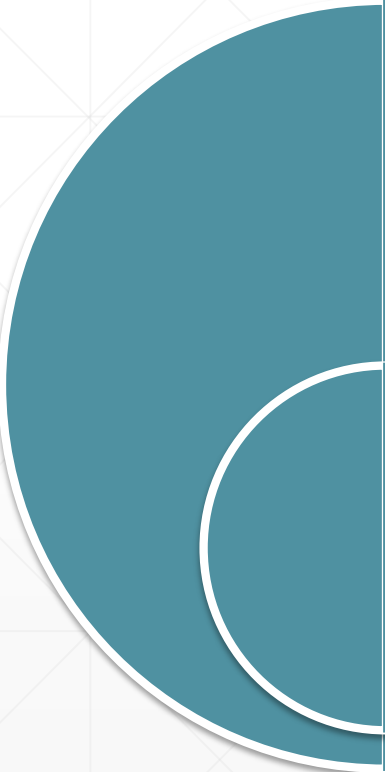


2. Phân loại các HTTT
(Khoản 3 Điều 4 TT 03/2017-TT-BTTTT)



3. Gom nhóm các hệ thống có cùng tính năng, công nghệ, đơn vị vận hành...

Một số kinh nghiệm thực tiễn đẩy mạnh công tác đảm bảo ATTT theo cấp độ



1. Lập và đánh giá cấp độ cho các hệ thống hạ tầng CNTT

2. Lập và đánh giá các hệ thống khác đặt trên hạ tầng CNTT: kế thừa được toàn bộ phần quy định về quản lý và một phần quản trị hạ tầng

Một số kỹ thuật đảm bảo an toàn thông tin chung cho tổ chức

1. Thường xuyên **tuyên truyền, cập nhật kiến thức, nâng cao nhận thức** cho người dùng về ATTT (Quy định, quy chế về ATTT của Bộ, các quy định pháp luật về đảm bảo an ninh thông tin mạng,...)

Cài đặt các phần mềm phòng chống mã độc.

Định kỳ dò quét, đánh giá, xử lý các vấn đề ATTT cho các hệ thống thông tin, thống mạng TTDL, mạng người dùng, ứng dụng (website, csdl, ...)

Cập nhật thông tin cảnh báo và khuyến nghị khắc phục nguy cơ ATTT từ Cục CNTT&DLTNMT (Cục ATTT, NCSC thuộc BTTTT; Ban Cơ yếu; CP Bộ Công an,)

Áp dụng, cập nhật các Giải pháp kỹ thuật phòng chống tấn công mức mạng (IPS, chặn lọc ứng dụng, anti-virus, anti-botnet, anti-spam, giám sát, ...)

Trân trọng cảm ơn!

Q&A
