



GIỚI THIỆU

- ❑ Một số quy định mới của Thông tư số 12/2022/TT-BTTTT
- ❑ Khung phát triển phần mềm an toàn

Quảng Ninh, ngày 14 tháng 4 năm 2023

QUAN ĐIỂM CHỈ ĐẠO



- ❖ *An toàn, an ninh mạng là trọng tâm của quá trình chuyển đổi số, là trụ cột quan trọng tạo lập niềm tin số và sự phát triển thịnh vượng trong kỷ nguyên số.*
- ❖ *Chủ quản hệ thống thông tin: Thực hiện nghiêm túc các quy định pháp luật về bảo vệ an ninh mạng; xác định cấp độ và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ và triển khai mô hình bảo vệ 4 lớp trước khi đưa vào sử dụng.*
 - ❑ *Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030 [964/QĐ-TTg]*



Nội dung trình bày

1

Hiện trạng phân loại,
xác định và phê
duyet HSĐXCĐ an
toàn HTTT



2

Công tác đơn đốc các Bộ,
ngành, địa phương hoàn
thành phân loại, phê
duyet HSĐXCĐ



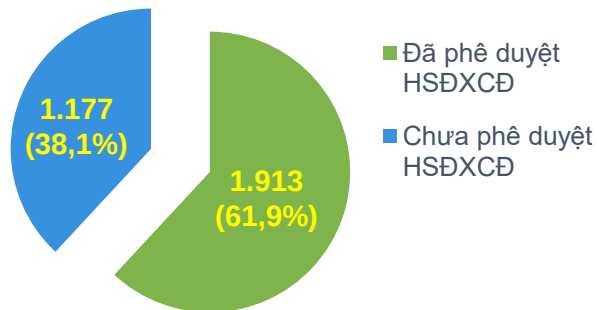
3

Một số quy định mới
của Thông tư số
12/2022/TT-BTTTT

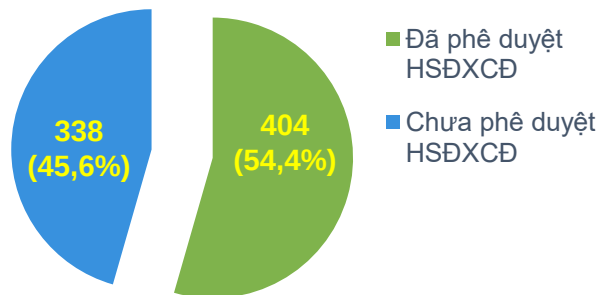
4

Khung Phát triển
phần mềm an toàn

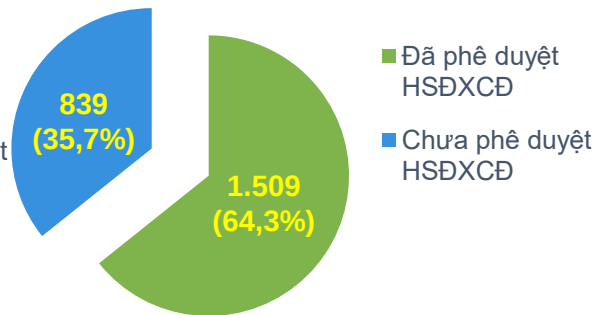
Hiện trạng phân loại, xác định và phê duyệt cấp độ an toàn HTTT (đến giữa T3/2023) | Trang 02/18



Toàn quốc: **3.090** HTTT đang vận hành



Bộ, ngành: **742** HTTT đang vận hành



Địa phương: **2.348** HTTT đang vận hành

❑ 15 Bộ, ngành có tỷ lệ phê duyệt HSDXCĐ **thấp, $\leq 50\%$.**

❑ 17 Địa phương có tỷ lệ phê duyệt HSDXCĐ **thấp, $\leq 50\%$.**

- Chủ quản HTTT chưa làm tròn trách nhiệm tại **Điều 20** Nghị định 85/2016/NĐ-CP;
- Đơn vị chuyên trách ATTT chưa làm tròn trách nhiệm tại **Điều 21** Nghị định 85/2016/NĐ-CP;
- Đơn vị vận hành HTTT chưa làm tròn trách nhiệm tại **Điều 22** Nghị định 85/2016/NĐ-CP.

➤ Việc này **có thể bị xử phạt** theo quy định tại Điều 88 của Nghị định số 15/2020/NĐ-CP.





Nội dung trình bày

1

Hiện trạng phân loại,
xác định và phê
duyet HSĐXCĐ an
toàn HTTT



2

Công tác đơn đốc các Bộ,
ngành, địa phương hoàn
thành phân loại, phê
duyet HSĐXCĐ

Công tác đơn đốc các Bộ, ngành, địa phương hoàn thành phân loại, phê duyệt cấp độ

Trang 04/18

Thủ tướng Chính phủ yêu cầu

- ✓ Hoàn thành phân loại, xác định và phê duyệt đề xuất cấp độ HTTT **trước 01/12/2022**;
- ✓ Triển khai đầy đủ phương án BDATHTTT theo cấp độ các HTTT đang vận hành **trước 01/6/2023**.

Chỉ thị số 02/CT-TTg
ngày 26/4/2022

Văn bản số 1598/BTTTT-CATTT
ngày 28/4/2022

Bộ TT&TT đề nghị

- ✓ Hoàn thành phê duyệt HSDXCĐ cho tất cả các HTTT **trước ngày 30/6/2022**;
- ✓ Triển khai đầy đủ phương án BDATHTTT theo cấp độ **trước ngày 15/11/2022**;
- ✓ **Cho dừng** các HTTT không BDATTT mạng theo quy định của pháp luật **từ ngày 01/01/2023**.

Bộ TT&TT đề nghị

- ✓ Tập trung rà soát, hoàn thành phân loại, xác định và phê duyệt đề xuất cấp độ ATTT **100% HTTT đang vận hành trước 31/3/2023**;
- ✓ Triển khai đầy đủ phương án bảo đảm ATHTTT theo cấp độ cho **100% HTTT đang vận hành trước ngày 30/9/2023**.

Văn bản số 652/BTTTT-CATTT
ngày 28/02/2023

Mẫu HSDXCĐ: <https://ais.gov.vn/thong-tin-tham-khao/mau-hsdxcd.htm>



Nội dung trình bày

1

Hiện trạng phân loại,
xác định và phê
duyet HSĐXCĐ an
toàn HTTT



2

Công tác đôn đốc các Bộ,
ngành, địa phương hoàn
thành phân loại, phê
duyet HSĐXCĐ

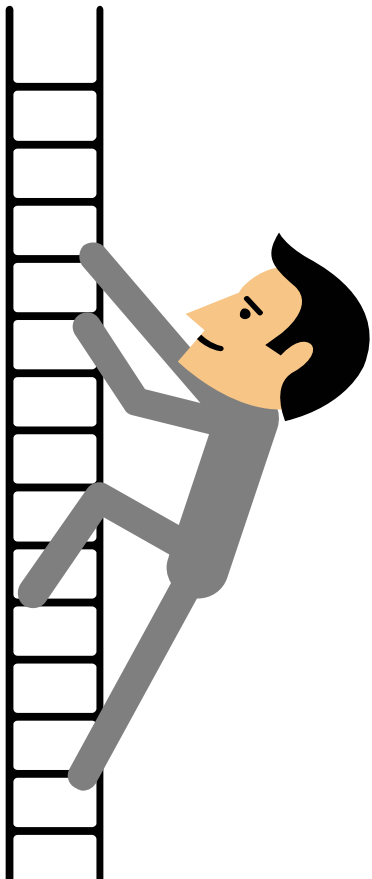


3

Một số quy định mới
của Thông tư số
12/2022/TT-BTTTT

Một số quy định mới của Thông tư số 12/2022/TT-BTTTT

| Trang 06/18



01 Về xác định các
chủ thể có liên quan
Điều 4, 5, 6

02 Thuyết minh cấp độ
an toàn hệ thống thông tin
Điều 7, 8, 9, 10

03 Kiểm tra, đánh giá
an toàn thông tin
Điều 11, 12

04 Chế độ báo cáo
Điều 13, 14

05 Các biện pháp bảo vệ
hệ thống thông tin
Phụ lục I, II, III, IV, V

06 Thời điểm phê duyệt
HSĐXCĐ
Điều 15

Xác định các chủ thể có liên quan



Chủ quản HTTT: Làm rõ quy định việc quyết định chủ quản HTTT là cấp có thẩm quyền quyết định đầu tư dự án thì phải bảo đảm điều kiện cơ quan, tổ chức được giao nhiệm vụ chủ quản HTTT có đủ năng lực để thực thi đầy đủ các quy định tại Điều 20 Nghị định 85/2016/NĐ-CP.



Đơn vị vận hành HTTT: Xác định đơn vị vận hành trong trường hợp thuê DVCNTT với 3 giai đoạn: Chưa xác định được đơn vị cung cấp dịch vụ, đã xác định được đơn vị cung cấp dịch vụ, hết thời hạn cung cấp dịch vụ.



Tổ chức thẩm định HSĐXCĐ trong trường hợp Đơn vị chuyên trách về ATTT đồng thời là Đơn vị vận hành, tiến hành tổ chức thẩm định theo 01 trong 02 phương án: giao một đơn vị trực thuộc có đủ năng lực chủ trì hoặc tổ chức thẩm định hoặc thành lập Hội đồng thẩm định độc lập.



Về xác định hệ thống thông tin

Định kỳ hàng quý (ngày đầu tiên của quý), Cục An toàn thông tin sẽ cập nhật, bổ sung danh mục các hệ thống thông tin theo quy định tại Điều 7 và công bố trên Cổng thông tin điện tử của Bộ Thông tin và Truyền thông.



Hướng dẫn thuyết minh cấp độ ATHTTT

Yêu cầu đối với HTTT được đầu tư xây dựng mới hoặc mở rộng, nâng cấp cần **đồng bộ phương án kỹ thuật** trong các tài liệu Báo cáo kinh tế - kỹ thuật / Thiết kế cơ sở thuộc BCNCKT / Kế hoạch thuê DVCNTT / Đề cương và dự toán chi tiết **với các yêu cầu của phương án BĐATTT theo cấp độ được đề xuất**, được thuyết minh trong HSĐXCĐ.



Yêu cầu cơ bản BĐATTT về quản lý

Bổ sung yêu cầu về **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**. **Quy chế bảo đảm ATHTTT** đáp ứng các yêu cầu an toàn về quản lý cần được ban hành **trước khi** HSĐXCĐ được phê duyệt.

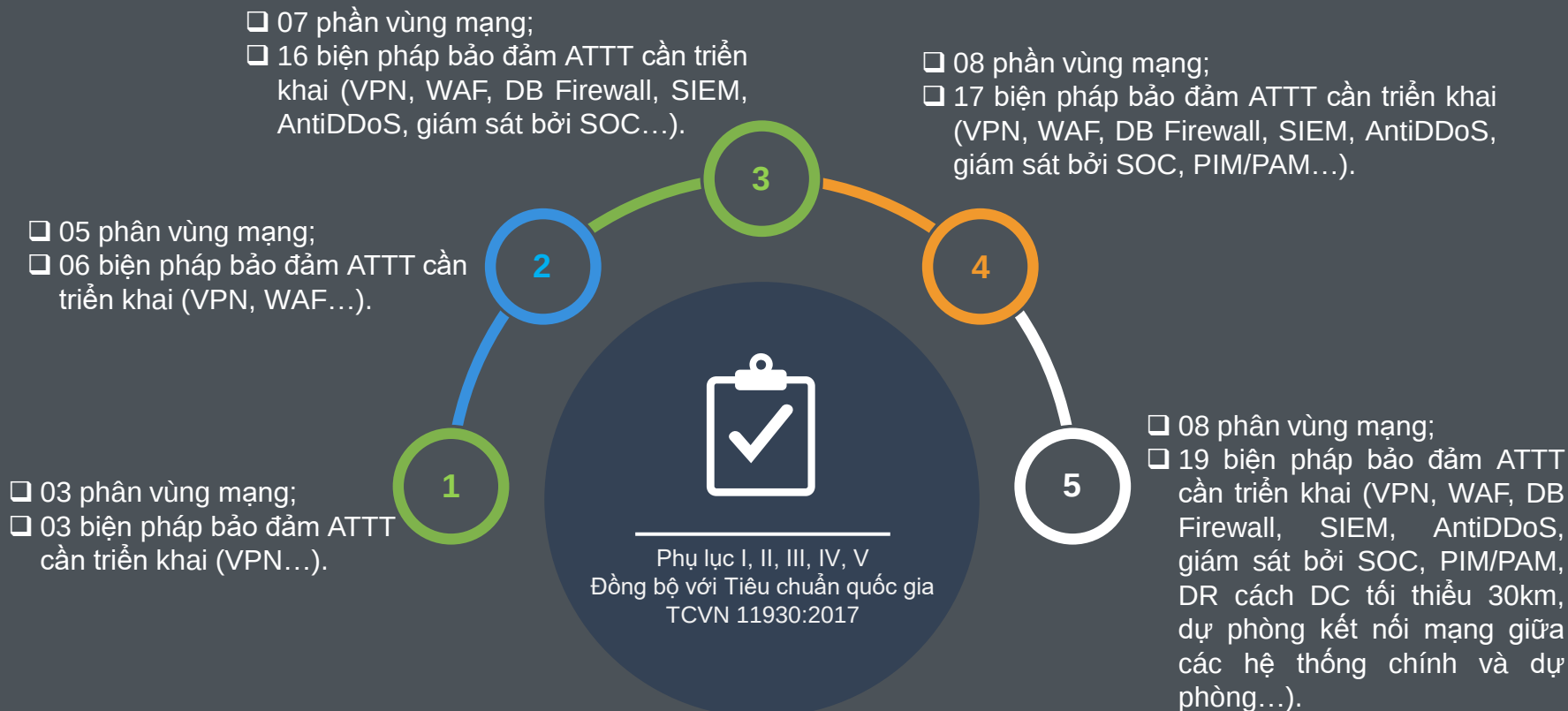


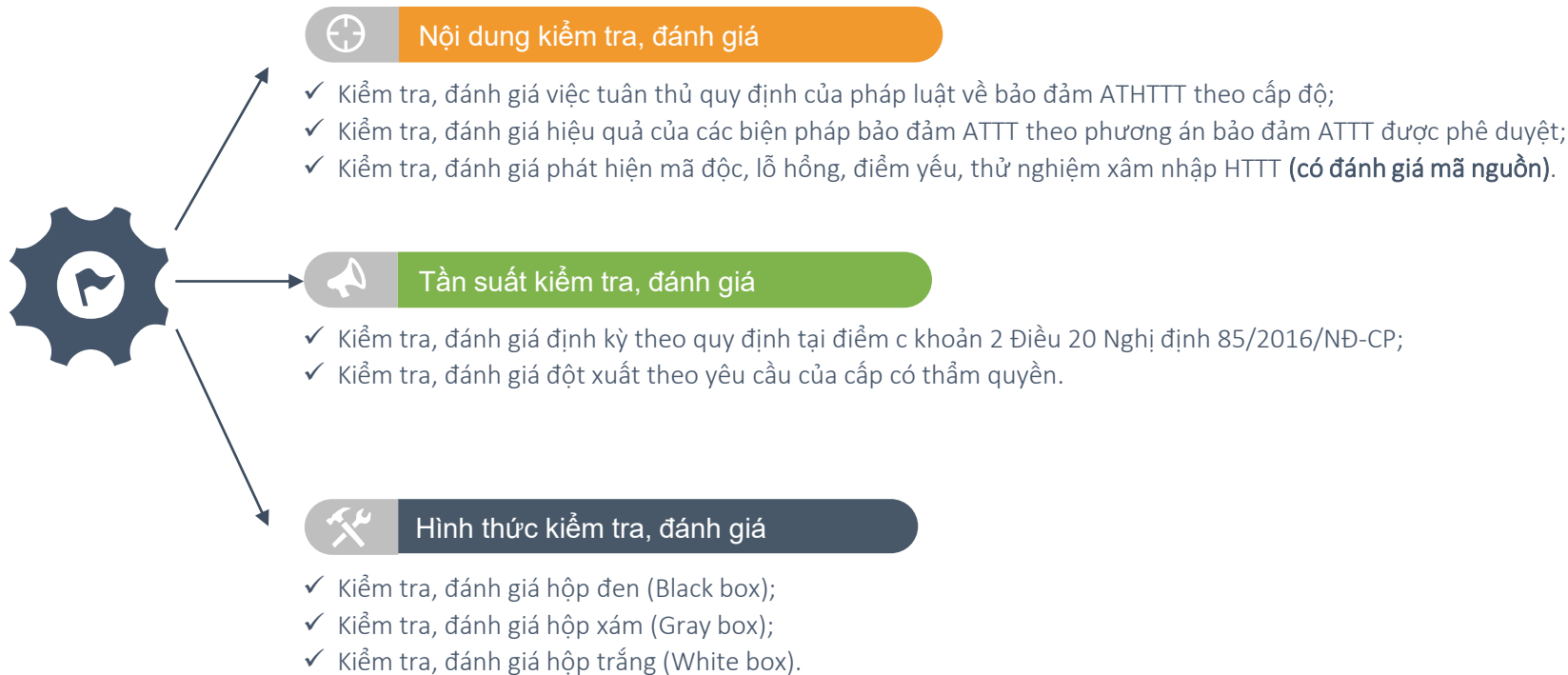
Yêu cầu cơ bản BĐATTT về kỹ thuật

Triển khai đầy đủ **phương án bảo đảm ATTT** đã được phê duyệt tại HSĐXCĐ và đáp ứng các yêu cầu an toàn **trước khi đưa vào vận hành, khai thác**. Yêu cầu về phần mềm nội bộ **tuân thủ Khung phát triển phần mềm an toàn...**

Phương án thiết kế hệ thống thông tin

| Trang 09/18







Phương thức gửi, nhận báo cáo

Phần mềm QLVB&ĐH, Hệ thống phần mềm báo cáo do Bộ TT&TT triển khai, Hệ thống thư điện tử...



Tần suất thực hiện báo cáo

- ✓ Định kỳ hàng năm;
- ✓ Đợt xuất theo đề nghị của cơ quan có thẩm quyền.



Thời gian chốt số liệu báo cáo định kỳ hàng năm

Tính từ ngày **15 tháng 12 năm trước** kỳ báo cáo đến **ngày 14 tháng 12 của kỳ báo cáo**.



Thời hạn gửi báo cáo định kỳ hàng năm

- ✓ Đơn vị chuyên trách về ATTT, Đơn vị vận hành: báo cáo tới Chủ quản HTTT **trước ngày 20 tháng 12 hàng năm**;
- ✓ Chủ quản HTTT gửi báo cáo Bộ TT&TT **trước ngày 25 tháng 12 hàng năm**.



Thời điểm phê duyệt HSĐXCĐ



Thời điểm phê duyệt HSĐXCĐ

Khuyến khích phê duyệt HSĐXCĐ an toàn thông tin **trước khi cấp có thẩm quyền phê duyệt** Báo cáo kinh tế - kỹ thuật hoặc thiết kế cơ sở thuộc BCNCKT hoặc Kế hoạch thuê DVCNTT hoặc Đề cương và dự toán chi tiết tương ứng.



HTTT đang vận hành, khai thác, đã được phê duyệt cấp độ

Chủ quản hệ thống thông tin cần tiến hành rà soát HSĐXCĐ và Phương án đảm bảo ATTT đã được phê duyệt, hoàn thành việc điều chỉnh, phê duyệt lại HSĐXCĐ và Phương án bảo đảm ATTT (nếu cần) **trước 01/6/2023**.



Nội dung trình bày

1

Hiện trạng phân loại,
xác định và phê
duyet HSĐXCĐ an
toàn HTTT



2

Công tác đơn đốc các Bộ,
ngành, địa phương hoàn
thành phân loại, phê
duyet HSĐXCĐ



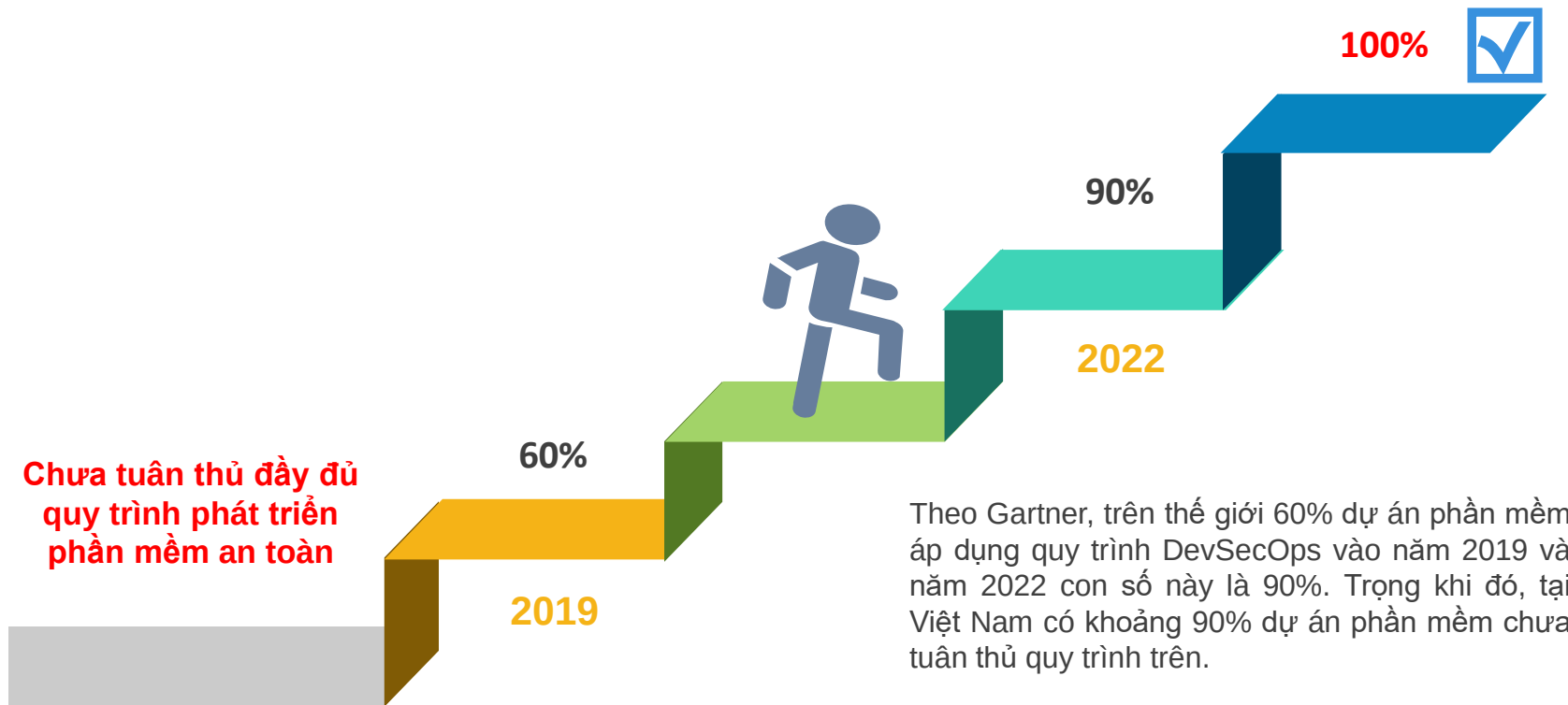
3

Một số quy định mới
của Thông tư số
12/2022/TT-BTTTT

4

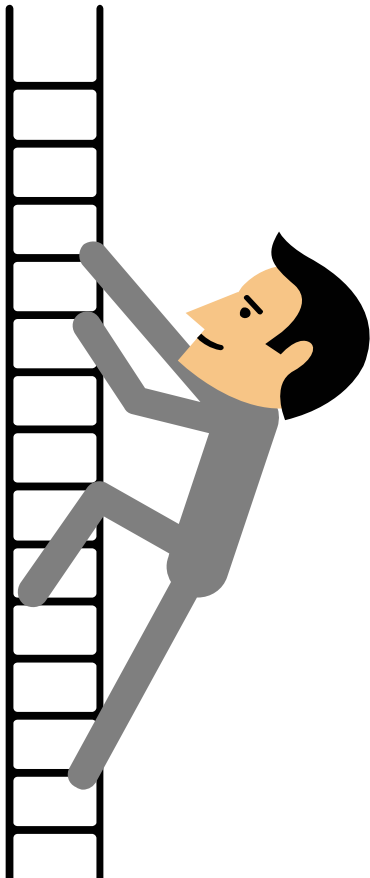
Khung Phát triển
phần mềm an toàn

Thực trạng về tuân thủ quy trình phát triển phần mềm an toàn



Tổng quan về Khung Phát triển phần mềm an toàn

| Trang 15/18



01

HÌNH THỨC BAN HÀNH

Phiên bản 1.0 – được ban hành ngày 10/02/2022, kèm theo Văn bản số 166/CATTT-ATHTTT của Cục An toàn thông tin.

02

PHẠM VI ÁP DỤNG

Khung phát triển phần mềm an toàn được ban hành nhằm khuyến nghị cơ quan, đơn vị, doanh nghiệp phát triển phần mềm có thể phát hiện lỗ hổng, điểm yếu bảo mật và kịp thời khắc phục trong quá trình phát triển phần mềm.

03

NGUỒN THAM KHẢO

Tài liệu NIST SP 800 – 218 “Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities” của Viện Tiêu chuẩn và Công nghệ Quốc gia thuộc Bộ Thương mại – Hoa Kỳ.

Ý tưởng



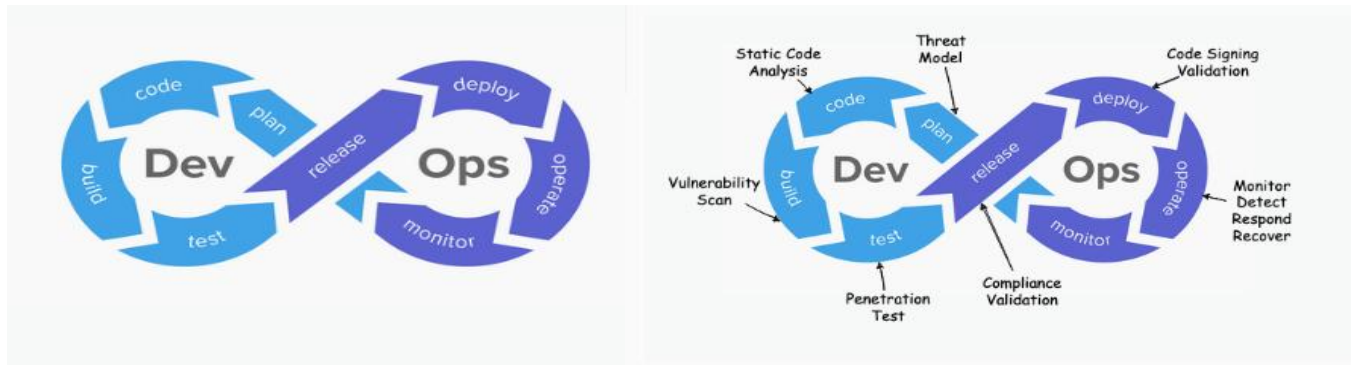
Các vòng đời phát triển phần mềm (SDLC - Software Development Life Cycle): Thác nước (Waterfall), V, Xoắn ốc (Spiral), Phát triển phần mềm linh hoạt (Agile Scrum)...

Có rất ít mô hình SDLC đề cập đến vấn đề an toàn phần mềm và các phương pháp phát triển phần mềm an toàn cần được tích hợp vào trong quá trình phát triển để giảm thiểu điểm yếu và tác động tiềm ẩn của các lỗ hổng bảo mật.



Nguyên tắc dịch chuyển sang trái (shift-left testing):

- Triển khai bảo đảm an toàn thông tin thường xuyên, liên tục, **ngay từ khâu thiết kế, xây dựng, vận hành**, cho đến khi hủy bỏ (khoản 1 Điều 4 Nghị định 85/2016/NĐ-CP) - DEVSECOPS.
- Lợi ích: giảm thiểu chi phí, thời gian thực hiện, giúp khắc phục các lỗi bảo mật sớm trong quá trình phát triển.



Nội dung chính - 4 nhóm nhiệm vụ

| Trang 17/18



Chuẩn bị của tổ chức (PO - Prepare the Organization)

Các tổ chức phải đảm bảo nhân sự, quy trình và công nghệ để thực hiện phát triển phần mềm an toàn tại cấp độ tổ chức. Giai đoạn này cũng có thể áp dụng cho quá trình phát triển phần mềm an toàn, như các nhóm phát triển riêng lẻ hoặc các dự án.



Bảo vệ phần mềm (PS - Protect the Software)

Các tổ chức cần bảo vệ tất cả các thành phần của phần mềm phòng chống giả mạo và truy cập trái phép.



Sản xuất phần mềm đảm bảo an toàn (PW - Produce Well-Security Software)

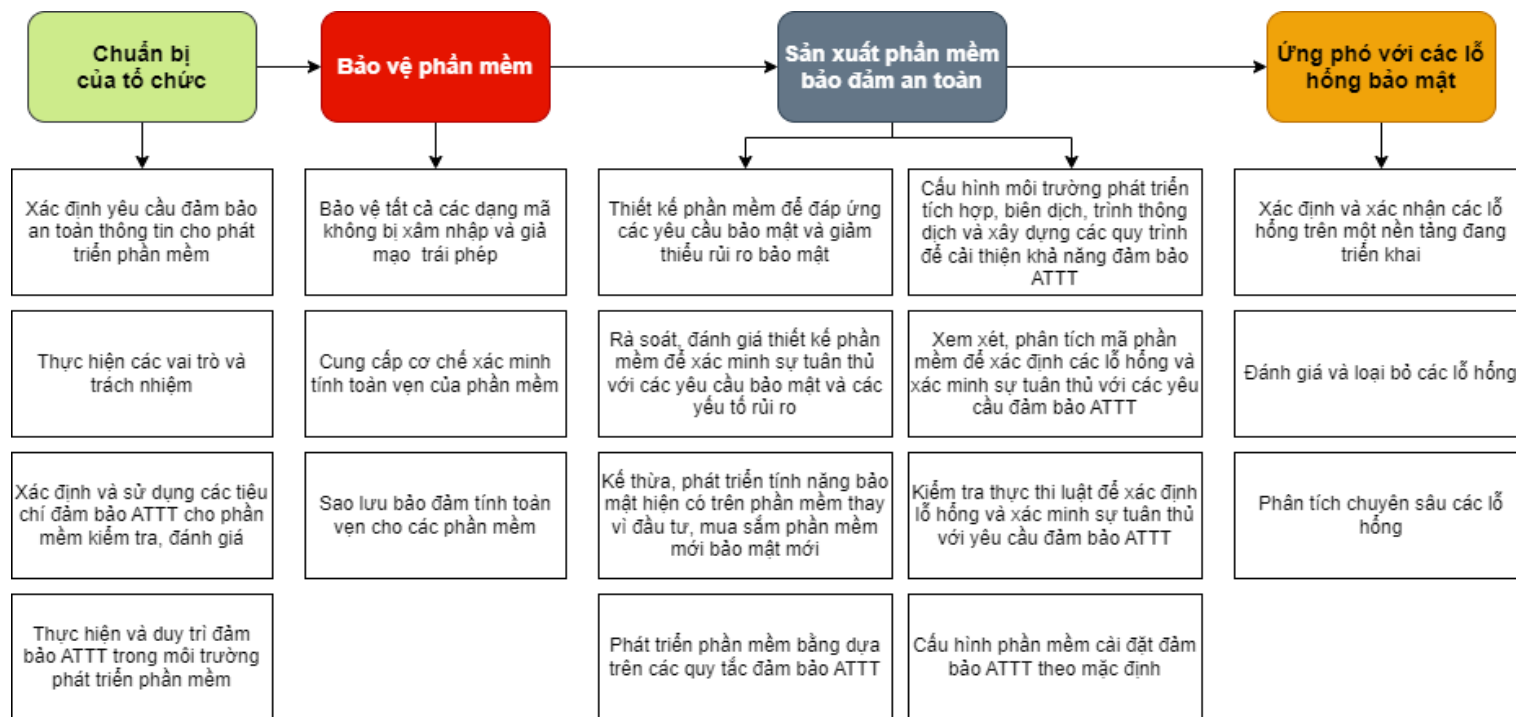
Các tổ chức cần sản xuất phần mềm đảm bảo an toàn với tối thiểu các điểm yếu tồn tại trong các phiên bản phát hành.



Ứng phó với các lỗ hổng bảo mật (RV – Respond to Vulnerabilities)

Các tổ chức phải xác định điểm yếu bảo mật còn tồn tại trong các phiên bản phần mềm phát hành và ứng phó tương ứng để xử lý những điểm yếu này và ngăn ngừa tương tự xảy ra trong tương lai.

Nội dung cụ thể





CỤC AN TOÀN THÔNG TIN
AUTHORITY OF INFORMATION SECURITY

Năm 2023
Năm dữ liệu số quốc gia

TRÂN TRỌNG CẢM ƠN!

Chi tiết liên hệ: **Nguyễn Minh Dũng**

- ❖ Phòng An toàn hệ thống thông tin, Cục An toàn thông tin, Bộ Thông tin và Truyền thông;
- ❖ Điện thoại: 0914.646.840;
- ❖ Email: dungnm@mic.gov.vn.

