WHEN TRUST MATTERS

Các khía cạnh của Quy định an ninh mạng

Quản lý an ninh mạng trong ngành điện

DNV Singapore

07 August 2025



Chương trình

Thứ Năm- ngày 7/8/2025

SÁNG

- Giới thiệu các Quy định về An ninh mạng
  - Singapore
  - Chương trình Bảo vệ hạ tầng trọng yếu của Tập đoàn điện lực Bắc Mỹ (NERC CIP)
  - Liên minh châu Âu

CHIỀU

- Khía cạnh quy định về An ninh mạng
  - Cấu trúc quy định
  - Các yêu cầu quy định bắt buộc

Thứ Sáu- ngày 8/8/2025

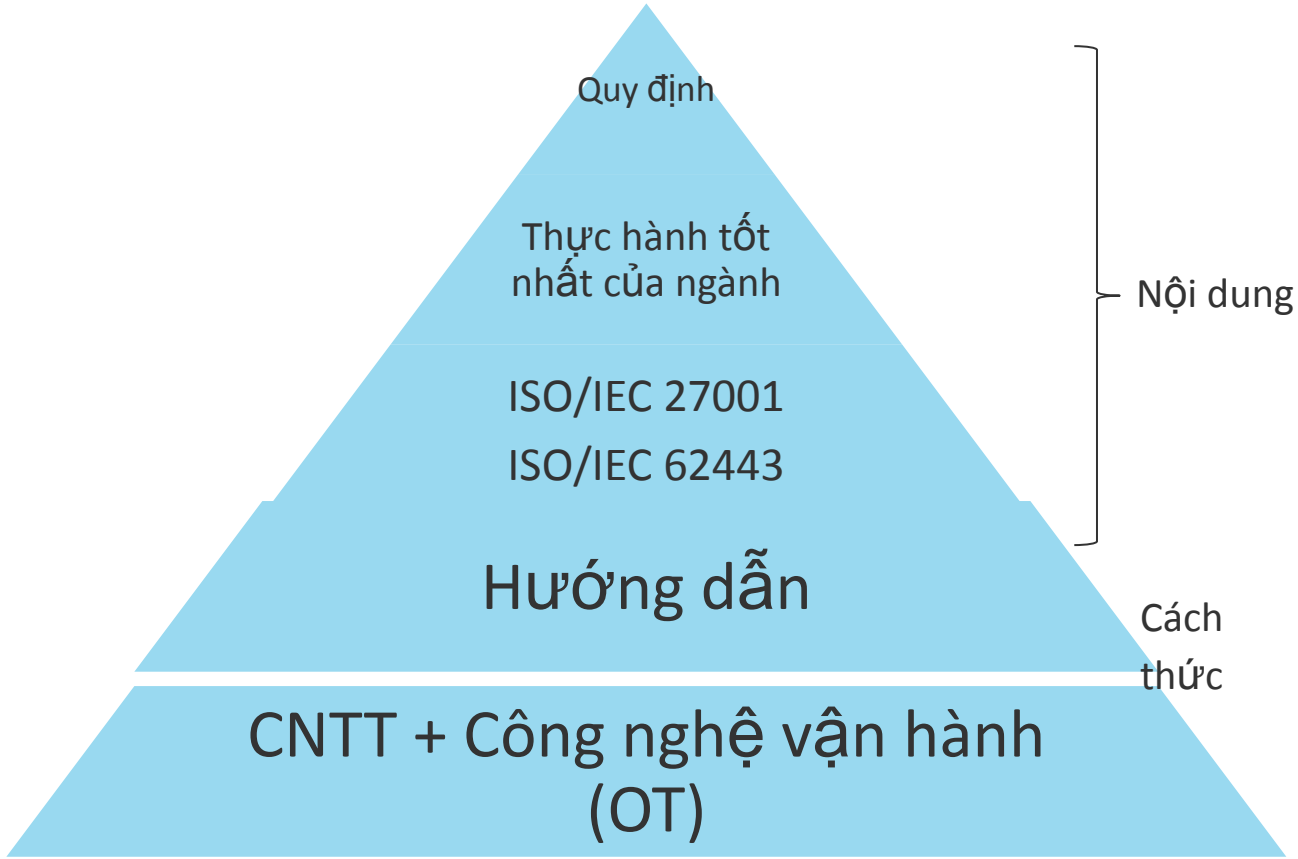
SÁNG

- Yêu cầu quy định về an ninh mạng (1)
  - Quản trị (Kiểm toán)
  - Quản lý tài sản
  - Bảo vệ

CHIỀU

- Yêu cầu quy định về an ninh mạng (2)
  - Phát hiện
  - Ứng phó và Phục hồi
- Tóm tắt

Quy định, Thực hành tốt, Tiêu chuẩn ngành, Hướng dẫn?



DNV ©

Quy định

- Luật áp dụng ở một quốc gia
- Được chính phủ giám sát
- Bắt buộc và có tính cưỡng chế thực thi
- Nhằm mục đích thiết lập mức tiêu chuẩn bảo mật tối thiểu kỳ vọng đạt được
- Mặc dù không phụ thuộc vào tiêu chuẩn ngành, quy định có thể áp dụng một phần của nhiều tiêu chuẩn ngành
- Không tuân thủ sẽ bị phạt

Tiêu chuẩn quốc tế

- Hướng dẫn dựa trên các thông lệ tốt nhất của ngành
- Được chấp nhận bởi các công ty lớn trong ngành
- Thực hiện tự nguyện
- Chứng nhận dựa trên các tiêu chuẩn ngành có sẵn

DNV

Nội dung

1. Cơ cấu và các yêu cầu quy định bắt buộc
2. Tóm tắt

1. Cơ cấu và các yêu cầu quy định bắt buộc

DNV ©

Hạ tầng thông tin trọng yếu (CII)

** 11 lĩnh vực CII được chỉ định tại Singapore*



- Định nghĩa - *hệ thống máy tính trực tiếp tham gia cung cấp các dịch vụ thiết yếu.*
- Mỗi quốc gia có định nghĩa khác nhau về các lĩnh vực CII

DNV ©

Hạ tầng thông tin trọng yếu (CII)

** 11 lĩnh vực CII quốc gia tại Malaysia*

Năng lượng	Nước	Ngân hàng và Tài chính
Nông nghiệp	Y tế	Giao thông Vận tải
CNTT&TT	Thương mại, Công nghiệp	An ninh
Khoa học công nghệ	Chính phủ	

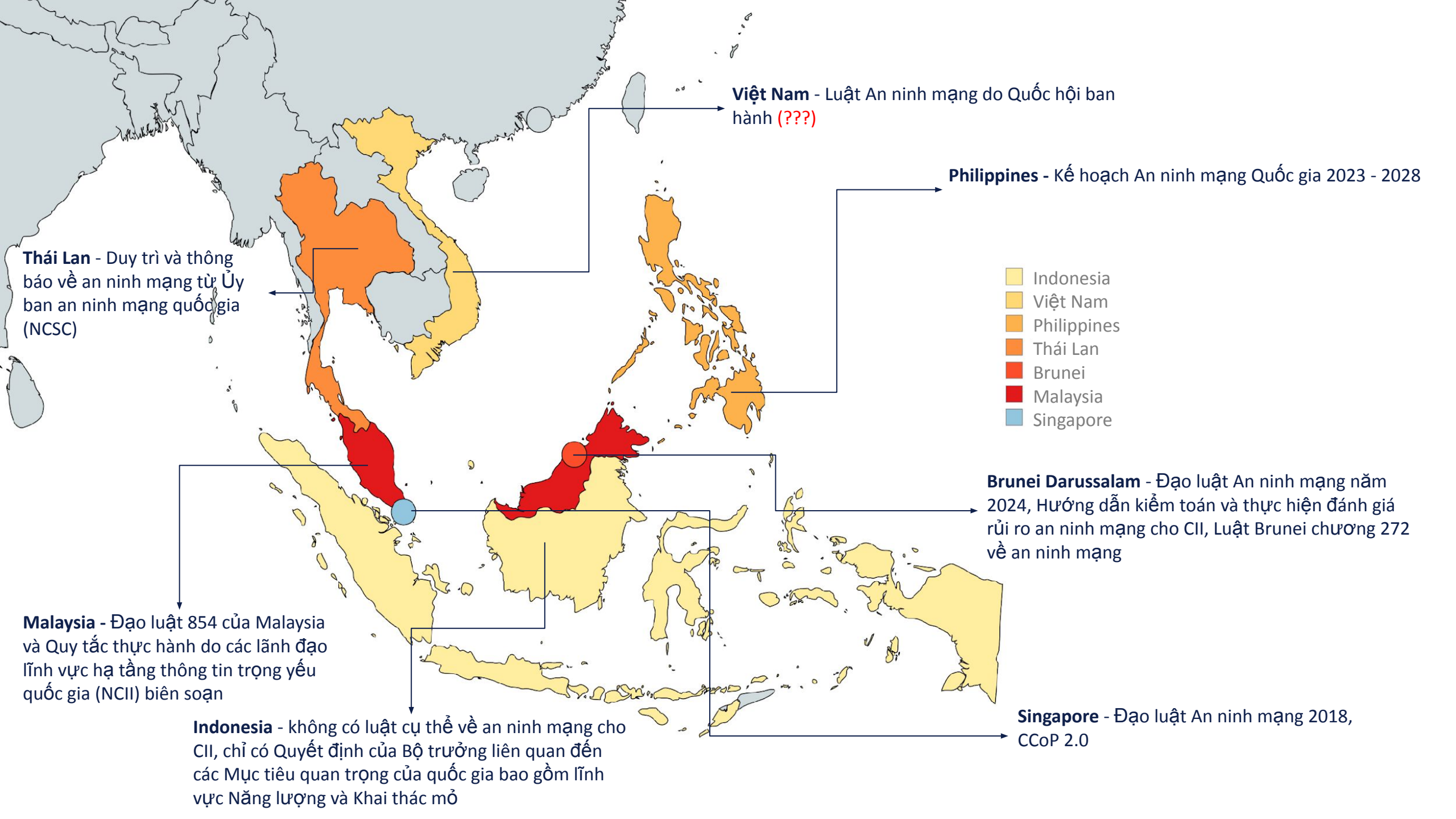
** Xếp hạng tác động theo NERC-CIP*

BES tác động cao

BES tác động trung bình

BES tác động thấp

DNV ©



Việt Nam - Luật An ninh mạng do Quốc hội ban hành (???)

Philippines - Kế hoạch An ninh mạng Quốc gia 2023 - 2028

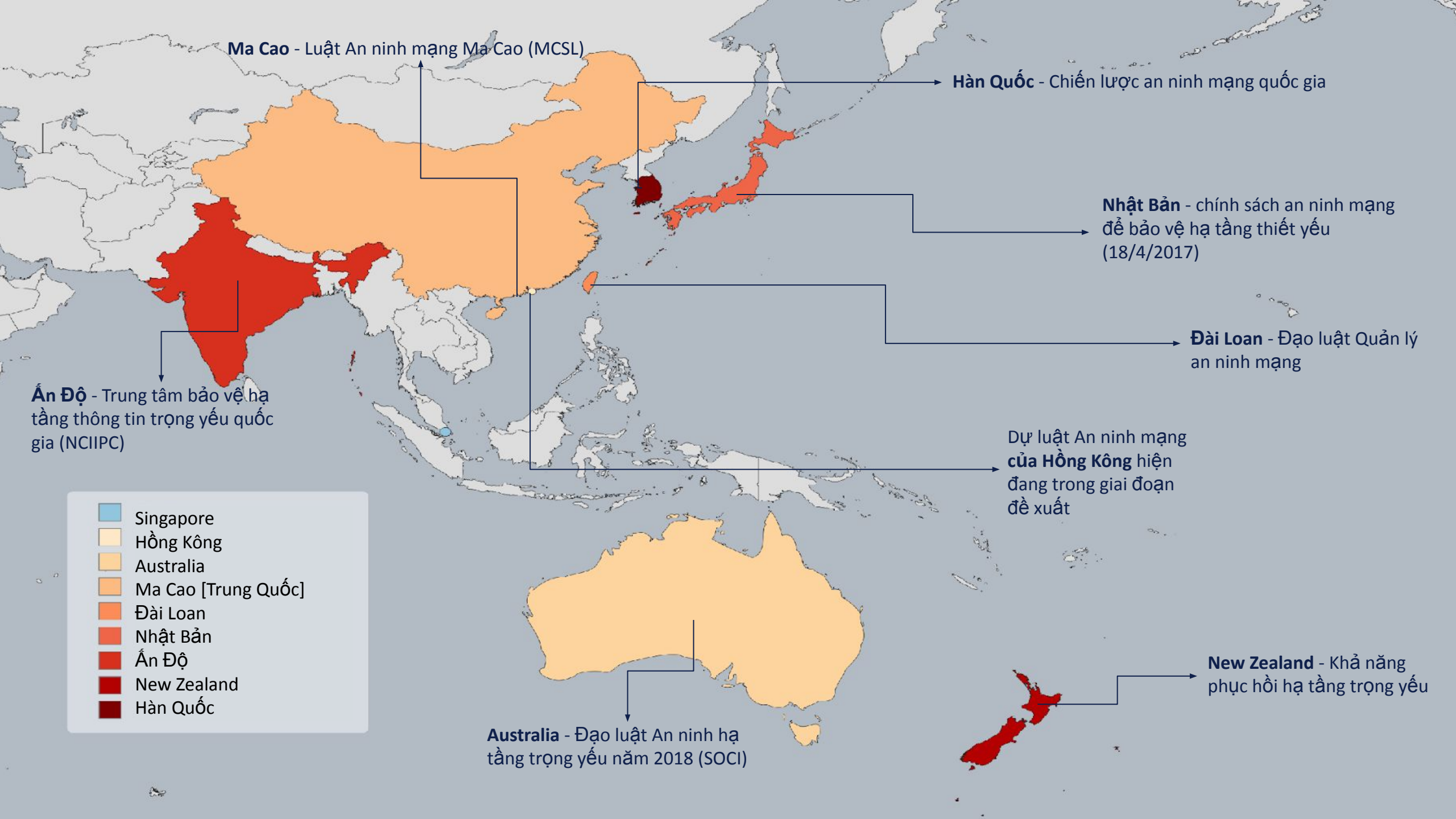
Thái Lan - Duy trì và thông báo về an ninh mạng từ Ủy ban an ninh mạng quốc gia (NCSC)

Brunei Darussalam - Đạo luật An ninh mạng năm 2024, Hướng dẫn kiểm toán và thực hiện đánh giá rủi ro an ninh mạng cho CII, Luật Brunei chương 272 về an ninh mạng

Malaysia - Đạo luật 854 của Malaysia và Quy tắc thực hành do các lãnh đạo lĩnh vực hạ tầng thông tin trọng yếu quốc gia (NCII) biên soạn

Indonesia - không có luật cụ thể về an ninh mạng cho CII, chỉ có Quyết định của Bộ trưởng liên quan đến các Mục tiêu quan trọng của quốc gia bao gồm lĩnh vực Năng lượng và Khai thác mỏ

Singapore - Đạo luật An ninh mạng 2018, CCoP 2.0

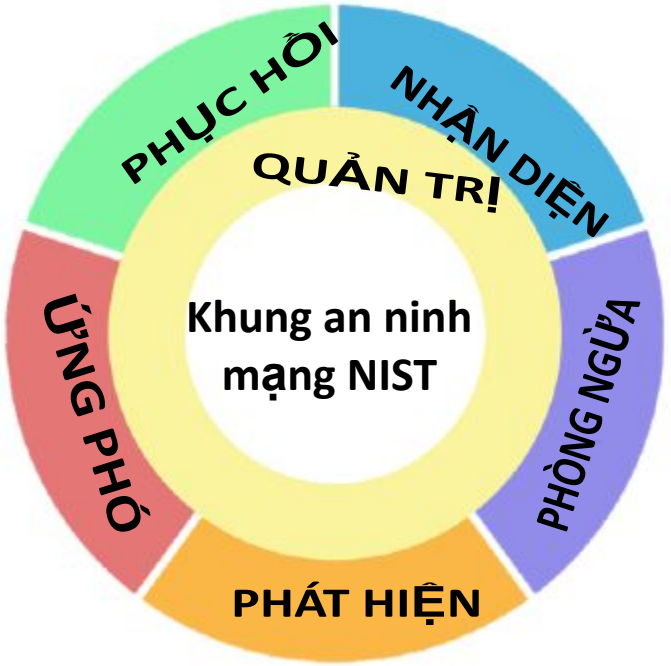

Ma Cao - Luật An ninh mạng Ma Cao (MCSL)
Hàn Quốc - Chiến lược an ninh mạng quốc gia
Nhật Bản - chính sách an ninh mạng để bảo vệ hạ tầng thiết yếu (18/4/2017)
Đài Loan - Đạo luật Quản lý an ninh mạng
Ấn Độ - Trung tâm bảo vệ hạ tầng thông tin trọng yếu quốc gia (NCIIPC)
Dự luật An ninh mạng **của Hồng Kông** hiện đang trong giai đoạn đề xuất
Singapore
Hồng Kông
Australia
Ma Cao [Trung Quốc]
Đài Loan
Nhật Bản
Ấn Độ
New Zealand
Hàn Quốc
Australia - Đạo luật An ninh hạ tầng trọng yếu năm 2018 (SOCI)
New Zealand - Khả năng phục hồi hạ tầng trọng yếu

Khung an ninh mạng (CSF) 2.0 của Viện tiêu chuẩn và công nghệ quốc gia (NIST)

Tổng quan về NIST CSF 2.0

Tham khảo: https://doi.org/10.6028/NIST.CSWP.29

- Cung cấp hướng dẫn để quản lý rủi ro an ninh mạng khi các tổ chức bắt đầu chương trình an ninh mạng
- Mô tả kết quả mong muốn, bao gồm tính linh hoạt, để giải quyết các rủi ro và khả năng chịu rủi ro của từng tổ chức
- Sử dụng để hiểu và đánh giá các khoảng trống, ưu tiên hành động và chia sẻ thông tin về các rủi ro an ninh mạng
- Áp dụng chung cho CNTT, IoT và OT
- Thành phần
  - ***CSF Cốt lõi*** – kết quả an ninh mạng cấp cao
  - ***Hồ sơ CSF*** – mô tả hiện trạng và mục tiêu an ninh mạng
  - ***Các tầng CSF*** – mô tả các hoạt động quản lý và quản trị rủi ro an ninh mạng



NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

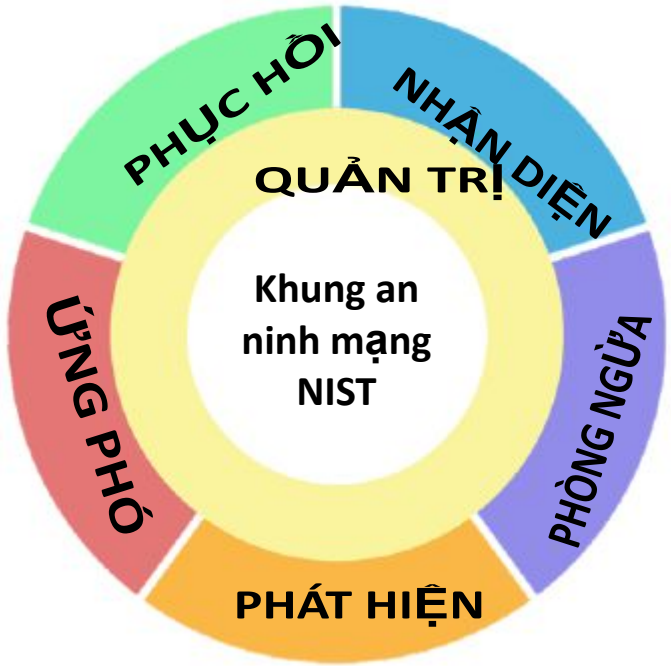
DNV

Tóm tắt về lõi CSF

bối cảnh tổ chức, chiến lược an ninh mạng, quản lý chuỗi cung ứng, vai trò, trách nhiệm và quyền hạn, chính sách

trao đổi thông tin nội bộ và với bên ngoài, kế hoạch phục hồi cập nhật, quan hệ công chúng

quy trình và tài sản trọng yếu, luồng dữ liệu, kiểm kê phần cứng/phần mềm, lỗ hổng/mối đe dọa/rủi ro



biện pháp ứng phó đã được kiểm thử và cập nhật, phối hợp nội bộ và với bên ngoài

quyền truy cập, tiếp cận tài sản và dữ liệu, sao lưu thường xuyên, thiết bị bảo vệ, đào tạo nâng cao nhận thức

kiểm tra và cập nhật quy trình phát hiện, lập đường cơ sở, giám sát nhật ký, nhận biết tác động

QUẢN TRỊ

Quy định an ninh mạng nói gì về quản trị

- Lãnh đạo và Giám sát
- Quản lý rủi ro
- Chính sách, Tiêu chuẩn, Hướng dẫn và Quy trình
- Lồng ghép an ninh mạng từ thiết kế
- Nguyên tắc thiết kế an ninh mạng
- Quản lý thay đổi
- Sử dụng Hệ thống và Dịch vụ điện toán đám mây
- Gia công phần mềm và quản lý nhà cung cấp

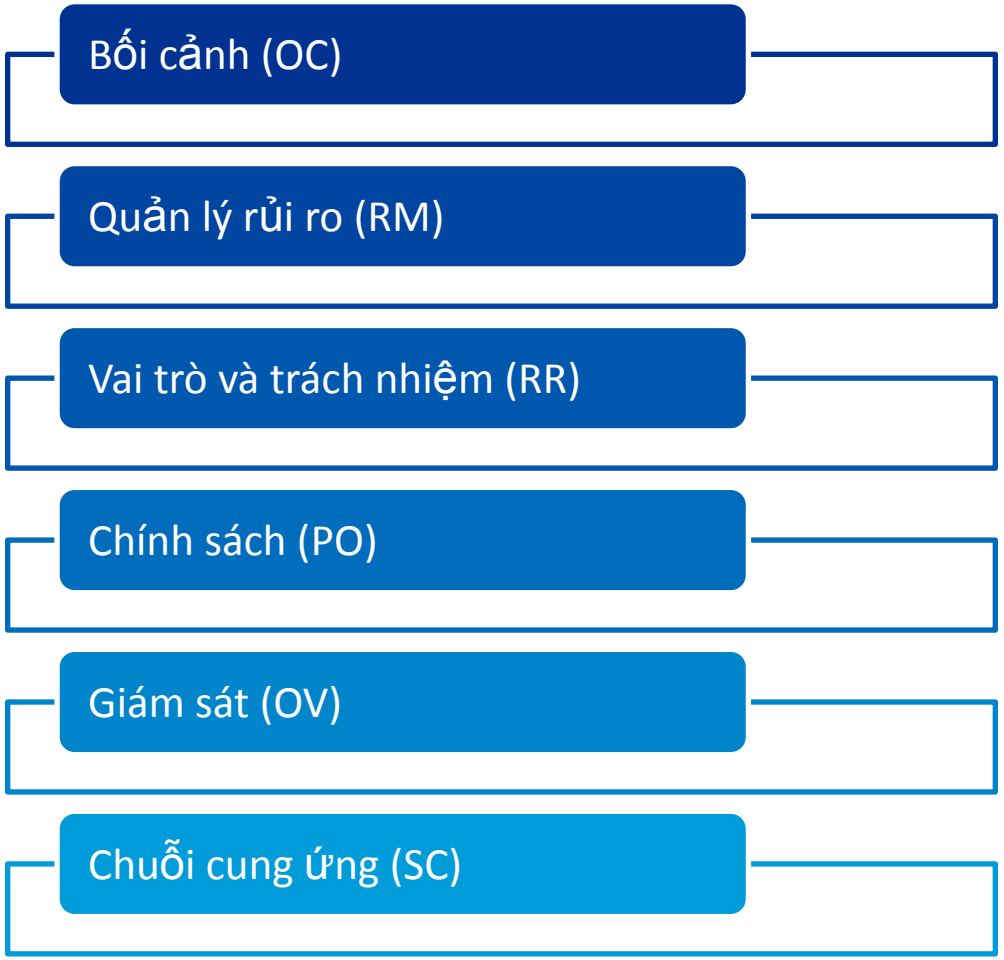


QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

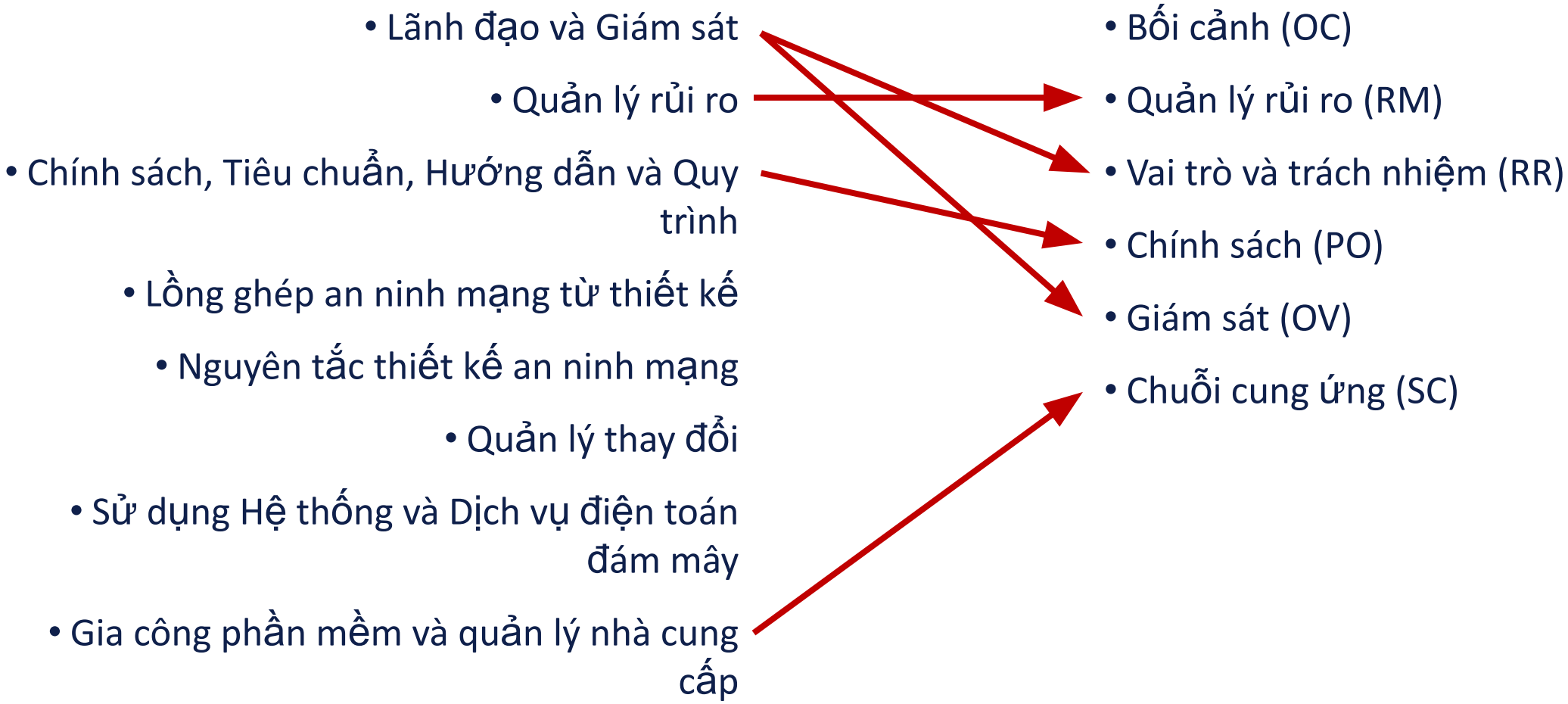
ĐẠO LUẬT AN NINH MẠNG 2018

NIST CSF 2.0 nói gì về quản trị

- Thiết lập, truyền đạt và giám sát
  - Chiến lược quản lý rủi ro an ninh mạng
  - Kỳ vọng
  - Chính sách



Kết nối Quy định với NIST CSF 2.0



DNV ©

NHẬN DIỆN

DNV ©

Quy định an ninh mạng nói gì về nhận diện

- Quản lý tài sản

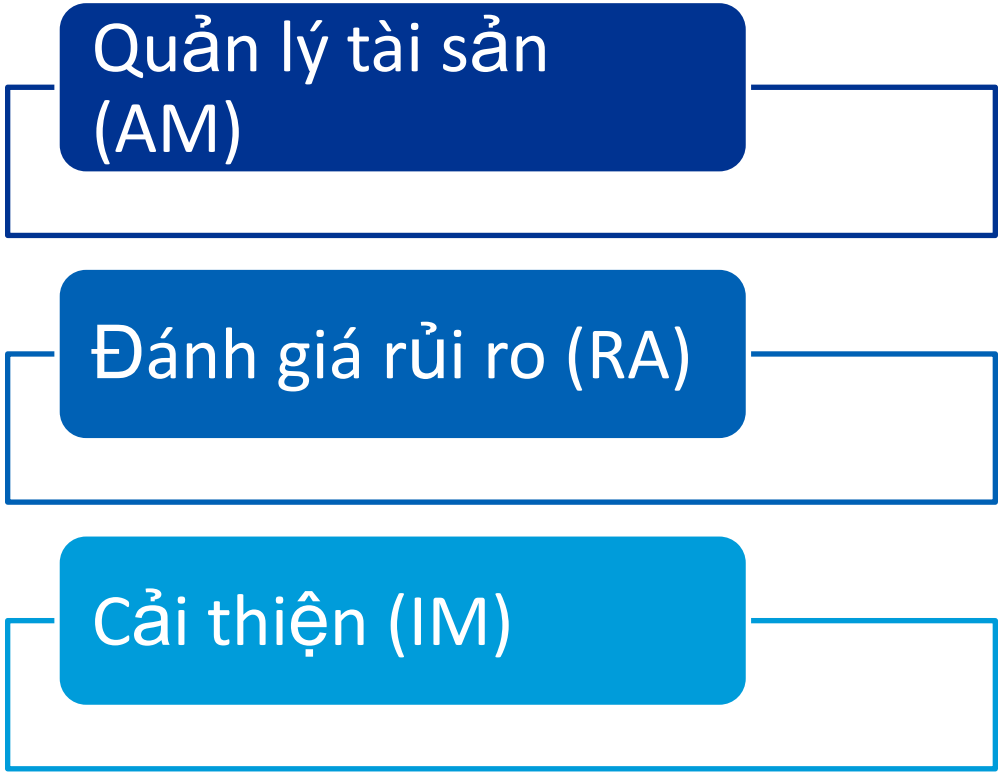


QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

NIST CSF 2.0 nói gì về nhận diện

- Hiểu các rủi ro an ninh mạng hiện tại



DNV ©

Kết nối Quy định với NIST CSF 2.0

- Quản lý tài sản →
  - Quản lý tài sản (AM)
  - Đánh giá rủi ro (RA)
  - Cải thiện (IM)

DNV ©

BẢO VỆ

Quy định an ninh mạng nói gì về bảo vệ (1/2)

- Kiểm soát truy cập, tiếp cận
- Quản lý tài khoản
- Quản lý quyền truy cập đặc biệt
- Bộ điều khiển miền
- Phân đoạn mạng
- Bảo mật mạng
- Kết nối từ xa
- Truyền thông không dây
- Tăng cường hệ thống
- Quản lý bản vá



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Quy định an ninh mạng nói gì về bảo vệ (2/2)

- Thiết bị máy tính di động và phương tiện lưu trữ di động
- Bảo mật ứng dụng
- Bảo mật cơ sở dữ liệu
- Đánh giá lỗ hổng
- Kiểm thử xâm nhập
- Mô phỏng tấn công đối kháng
- Quản lý khóa mật mã



QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

Quy định an ninh mạng nói gì về đào tạo và nâng cao nhận thức

- Chương trình nâng cao nhận thức về an ninh mạng
- Đào tạo và kỹ năng an ninh mạng

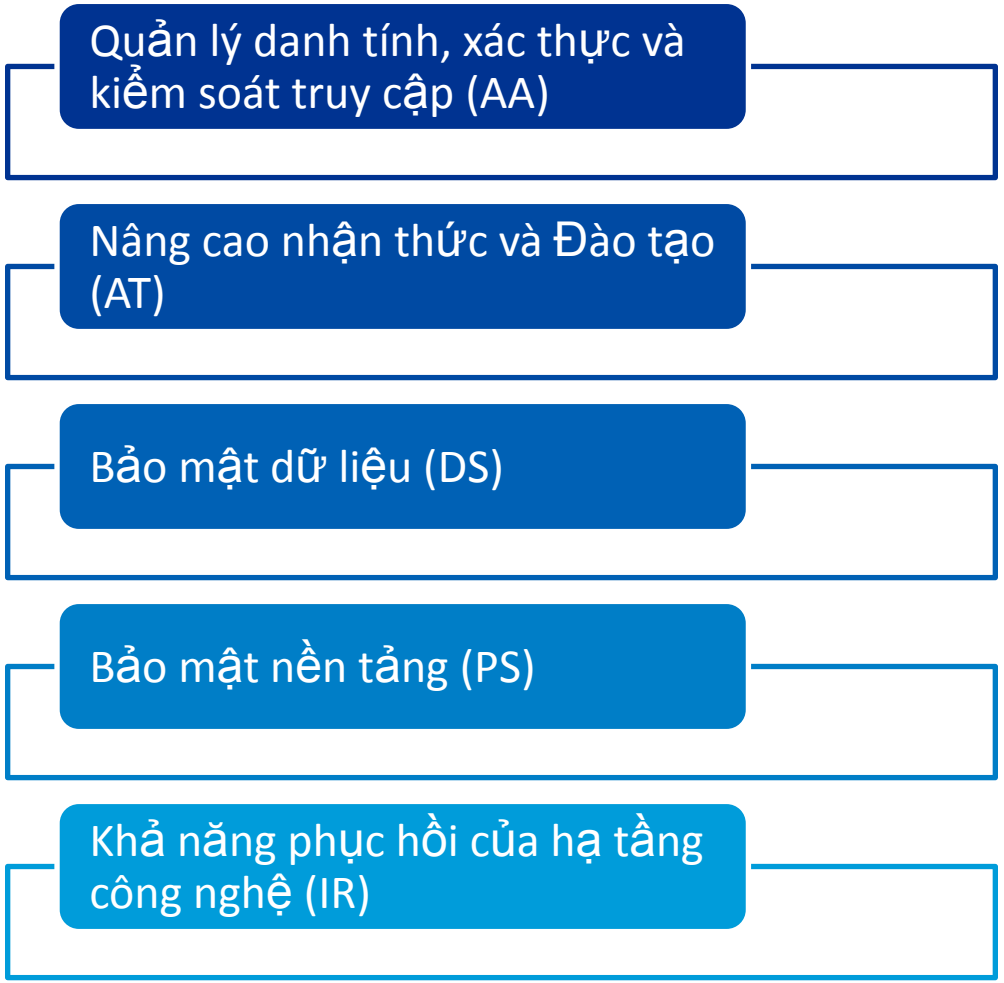


QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

NIST CSF 2.0 nói gì về bảo vệ

- Sử dụng các biện pháp bảo vệ để quản lý rủi ro an ninh mạng của tổ chức



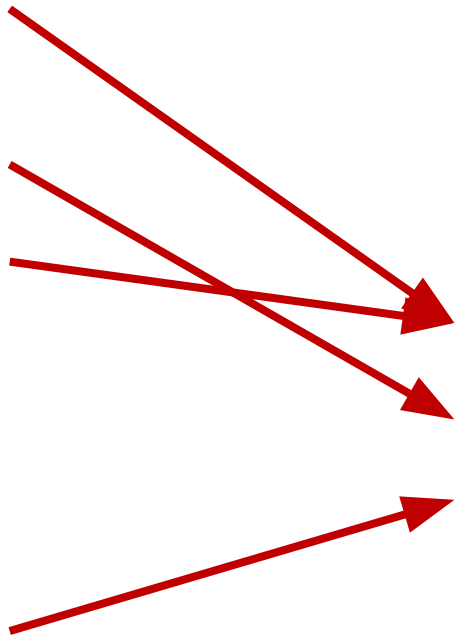
Kết nối Quy định với NIST CSF 2.0 (1/3)



DNV ©

Kết nối Quy định với NIST CSF 2.0 (2/3)

- Thiết bị máy tính di động và phương tiện lưu trữ di động
- Bảo mật ứng dụng
- Bảo mật cơ sở dữ liệu
- Đánh giá lỗ hổng
- Kiểm thử xâm nhập
- Mô phỏng tấn công đối kháng
- Quản lý khóa mật mã

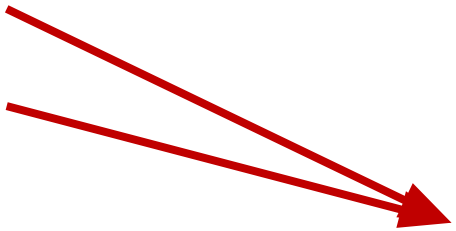


- Quản lý danh tính, xác thực và kiểm soát truy cập (AA)
- Nâng cao nhận thức và Đào tạo (AT)
- Bảo mật dữ liệu (DS)
- Bảo mật nền tảng (PS)
- Khả năng phục hồi của hạ tầng công nghệ (IR)

DNV ©

Kết nối Quy định với NIST CSF 2.0 (3/3)

- Chương trình nâng cao nhận thức về an ninh mạng
- Đào tạo và kỹ năng an ninh mạng



- Quản lý danh tính, xác thực và kiểm soát truy cập (AA)
- Nâng cao nhận thức và Đào tạo (AT)
- Bảo mật dữ liệu (DS)
- Bảo mật nền tảng (PS)
- Khả năng phục hồi của hạ tầng công nghệ (IR)

PHÁT HIỆN

DNV ©

Quy định an ninh mạng nói gì về việc phát hiện

- Ghi nhật ký
- Giám sát và Phát hiện
- Săn tìm mối đe dọa
- Chia sẻ thông tin và dữ liệu xử lý về mối đe dọa mạng

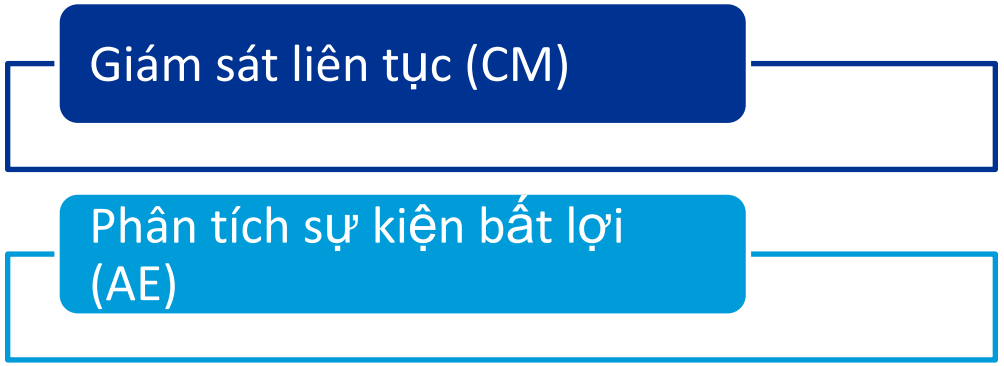


QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

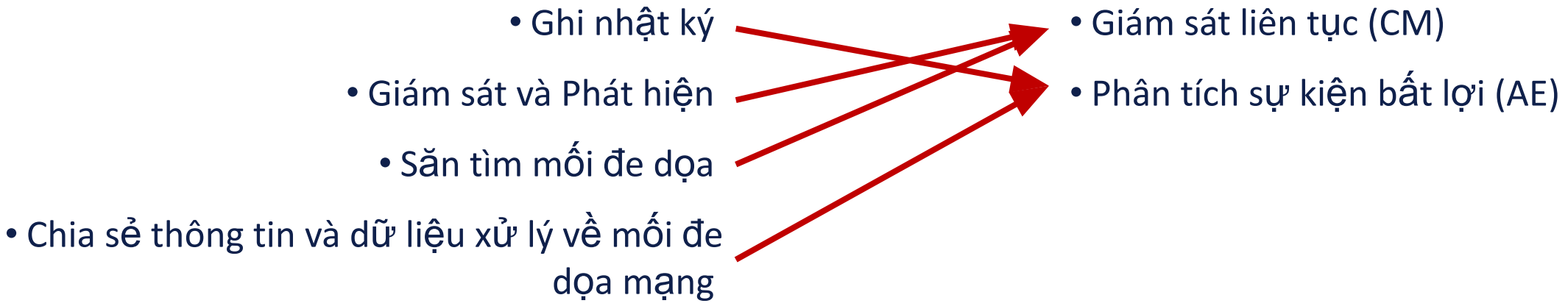
NIST CSF 2.0 nói gì về phát hiện

- Tìm và phân tích các cuộc tấn công và xâm phạm an ninh mạng có thể xảy ra



DNV ©

Kết nối Quy định với NIST CSF 2.0



ỨNG PHÓ

Quy định về an ninh mạng nói gì về ứng phó

- Quản lý sự cố
- Kế hoạch truyền thông khủng hoảng
- Diễn tập an ninh mạng

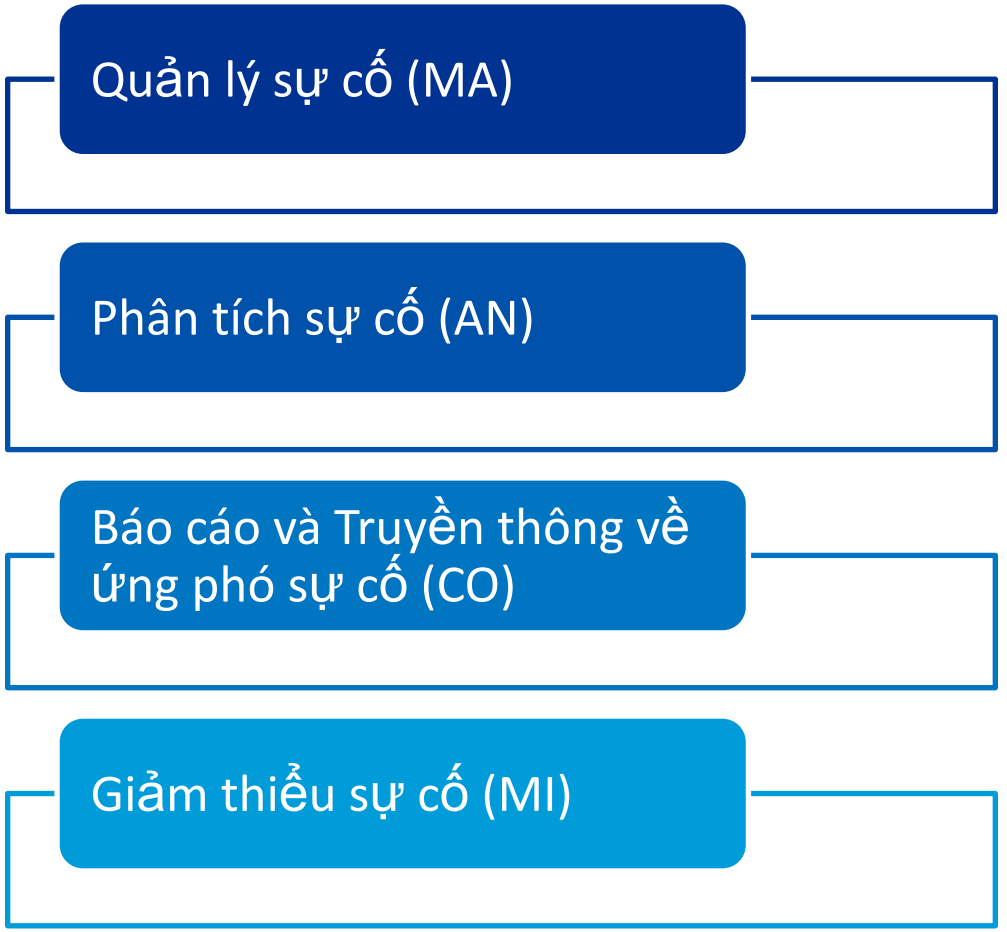


QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

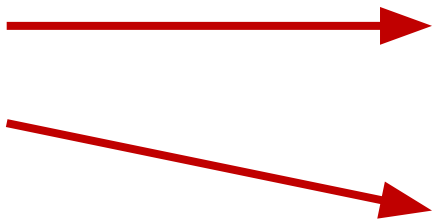
NIST CSF 2.0 nói gì về ứng phó

- Thực hiện hành động liên quan đến sự cố an ninh mạng được phát hiện



Kết nối Quy định với NIST CSF 2.0

- Quản lý sự cố
- Kế hoạch truyền thông khủng hoảng
- Diễn tập an ninh mạng



- Quản lý sự cố (MA)
- Phân tích sự cố (AN)
- Báo cáo và Truyền thông về ứng phó sự cố (CO)
- Giảm thiểu sự cố (MI)

DNV ©

PHỤC HỒI

Quy định về an ninh mạng nói gì về ứng phó

- Kế hoạch sao lưu và khôi phục
- Kế hoạch duy trì hoạt động và Kế hoạch phục hồi sau thảm họa

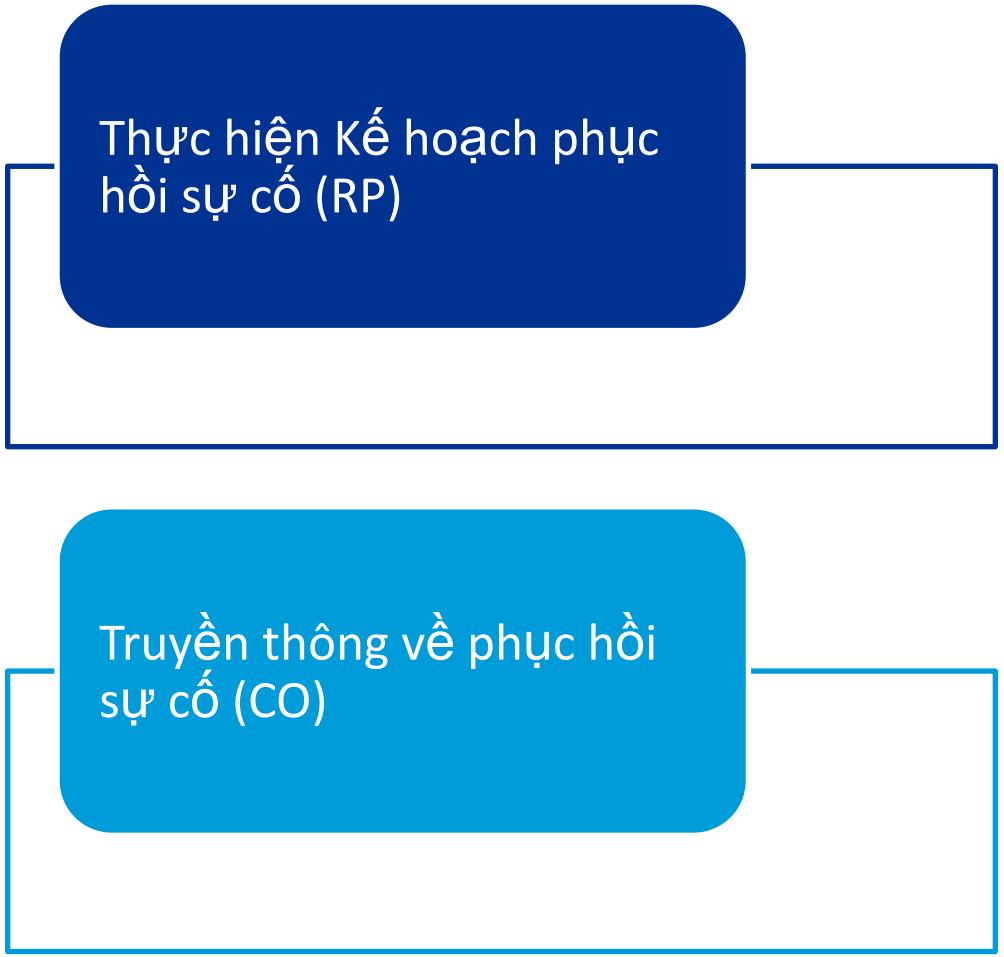


QUY TẮC THỰC HÀNH AN NINH MẠNG CHO HẠ TẦNG THÔNG TIN TRỌNG YẾU – ẤN BẢN THỨ HAI

ĐẠO LUẬT AN NINH MẠNG 2018

NIST CSF 2.0 nói gì về phục hồi

- Khôi phục tài sản và hoạt động bị ảnh hưởng bởi sự cố an ninh mạng



Kết nối Quy định với NIST CSF 2.0

- Kế hoạch sao lưu và khôi phục
- Kế hoạch duy trì hoạt động và Kế hoạch phục hồi sau thảm họa



- Thực hiện Kế hoạch phục hồi sự cố (RP)
- Truyền thông về phục hồi sự cố (CO)

2. Tóm tắt

DNV ©

Những điểm chính

- Phạm vi của quy định an ninh mạng chủ yếu áp dụng các khái niệm chính theo tiêu chuẩn quốc tế
- Quy định được điều chỉnh và hoàn thiện theo bối cảnh của quốc gia/lĩnh vực
  - Việc tuân thủ các tiêu chuẩn quốc tế không đồng nghĩa với việc tuân thủ quy định
- Tiêu chuẩn bảo mật theo quy định càng cao thì chi phí triển khai của chủ sở hữu CII càng lớn.
  - Chi phí kinh doanh cũng sẽ bị ảnh hưởng
- Việc tuân thủ quy định một cách mù quáng có thể dẫn đến cảm giác an toàn giả



Bao nhiêu là đủ?

Yêu cầu theo quy định (mức cơ sở)	Yêu cầu có thể bổ sung
Đánh giá rủi ro	Hoạt động bảo mật
Kiểm kê tài sản	Lồng ghép an ninh mạng từ thiết kế
Kiểm toán tuân thủ	Săn tìm mối đe dọa
Đánh giá lỗ hổng	Bài tập nhóm Xác định vùng tím
Kiểm thử xâm nhập	Thông tin xử lý về mối đe dọa
Đào tạo nâng cao nhận thức	

Lưu ý: mọi yêu cầu bổ sung trong quy định sẽ làm tăng gánh nặng cho chủ sở hữu CII (bao gồm cả chi phí!)

Các khía cạnh của Quy định an ninh mạng

Quản lý an ninh mạng trong ngành điện

ivan.christian@dnv.com

+65 9728 2143

www.dnv.com

DNV ©