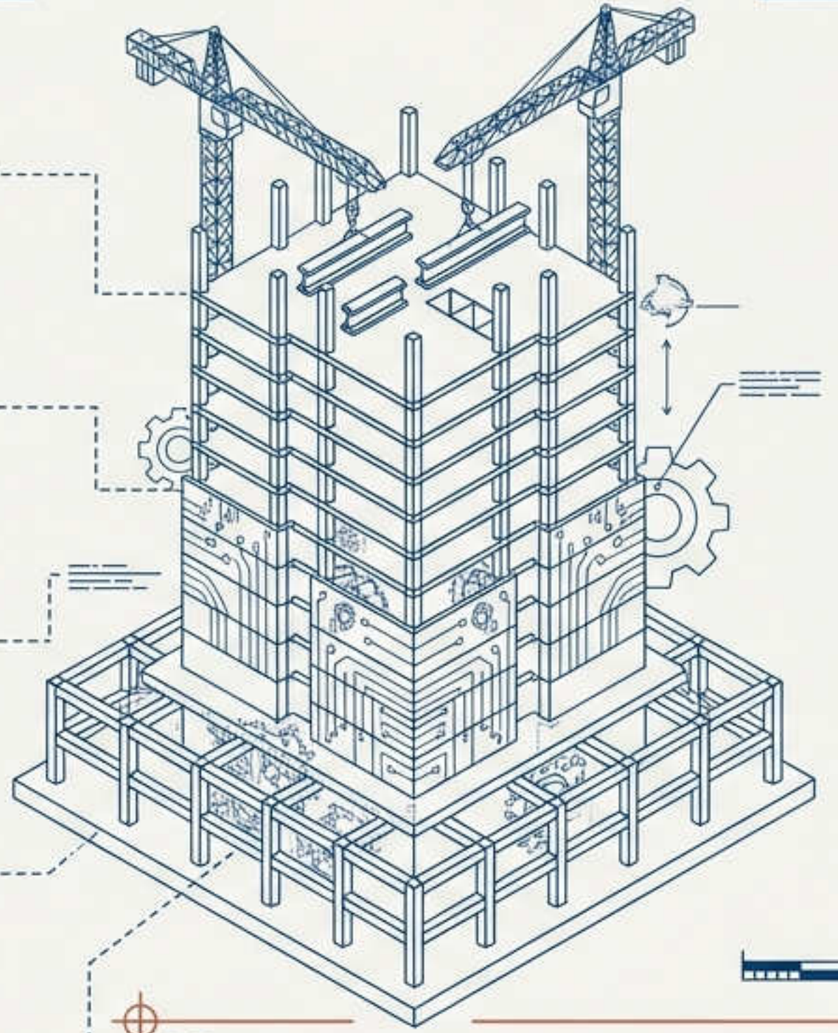
Quản trị Tổ chức & Rủi ro CNTT

Xây dựng nền tảng cho sự liên kết chiến lược và tạo ra giá trị

1. Chiến lược & Mục tiêu
2. Cơ cấu & Vai trò
3. Văn hóa & Đạo đức
4. Chính sách & Tiêu chuẩn
5. Quy trình & Tài sản



> **Quản trị (Governance)** là hệ thống đánh giá, chỉ đạo và giám sát để tạo ra giá trị cho các bên liên quan.

Nguồn: CRISC© Official Review Manual, 8th Edition - Chapter 1, Part A

Mục đích của Quản trị: Bốn câu hỏi cốt lõi

Quản trị (Governance)

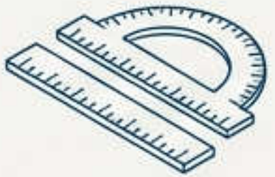
• Đánh giá (Evaluate) • Định hướng (Direct)
• Giám sát (Monitor)

Quản lý (Management)

Lập kế hoạch (Plan) • Xây dựng (Build)
• Vận hành (Run) • Theo dõi (Monitor)

The Four Are's

Are we doing the right things?
(Chúng ta có đang làm đúng việc không?) - Liên kết chiến lược.



Are we doing them the right way?
(Chúng ta có làm đúng cách không?) - Kiến trúc và tuân thủ.

Are we getting them done well?
(Chúng ta có hoàn thành tốt không?) - Hiệu suất hoạt động.

Are we seeing expected benefits?
(Chúng ta có đạt được lợi ích kỳ vọng không?) - Giá trị mang lại.

Thiết lập Định hướng: Các mô hình Chiến lược Doanh nghiệp

Chiến lược xác định khẩu vị rủi ro. Rủi ro CNTT phải hỗ trợ trực tiếp cho mô hình chiến lược đã chọn.

Tăng trưởng/ Thâu tóm

Tập trung vào tăng trưởng doanh thu.
Khẩu vị rủi ro cao để nắm bắt cơ hội.

Đổi mới/ Khác biệt hóa

Cung cấp sản phẩm khác biệt.
Chấp nhận rủi ro thử nghiệm công nghệ mới.

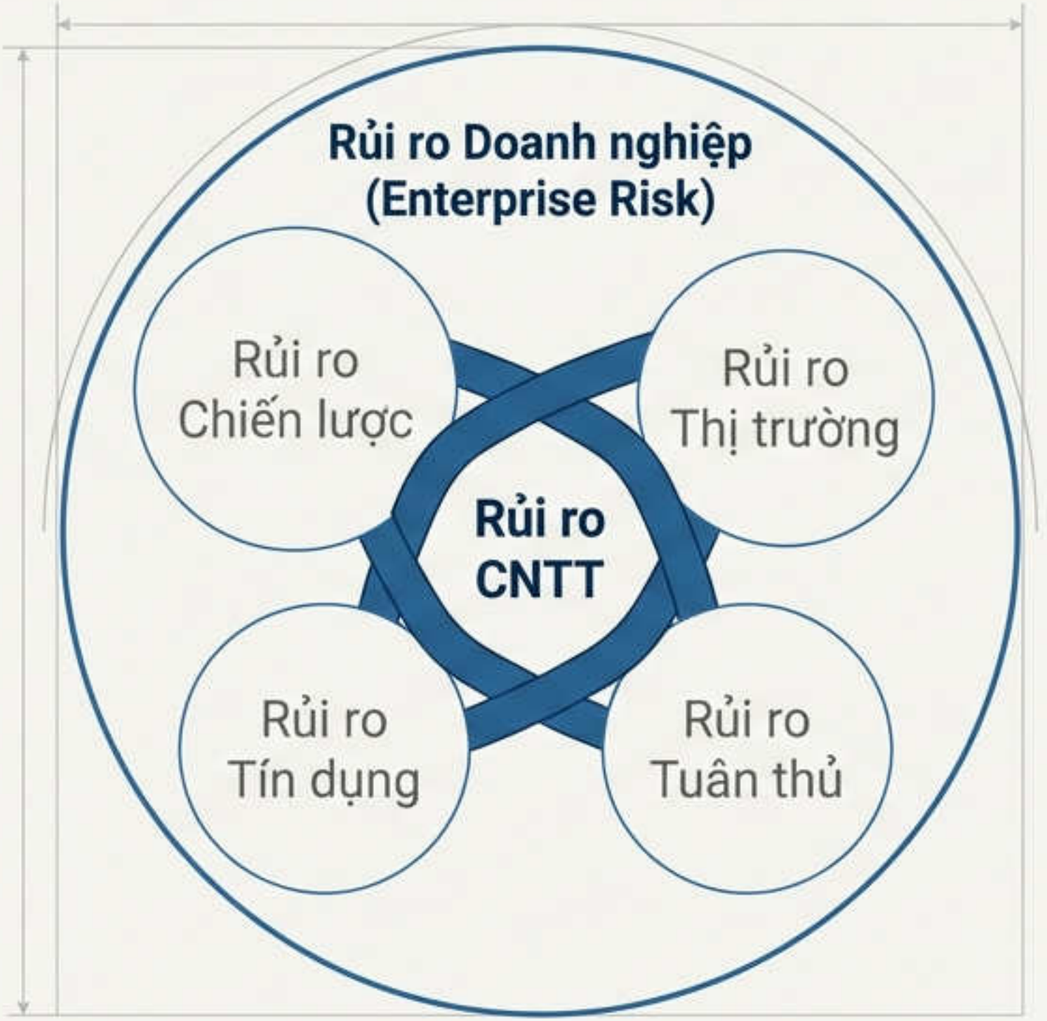
Dẫn đầu về chi phí

Giảm thiểu chi phí ngắn hạn.
Ưu tiên hiệu quả vận và kiểm soát chi tiêu.

Dịch vụ khách hàng/Sự ổn định

Tập trung vào sự ổn định.
Ưu tiên rủi ro uy tín và chất lượng dịch vụ.

Bối cảnh: Rủi ro CNTT chính là Rủi ro Kinh doanh



Bản chất kép của Rủi ro

Rủi ro là ảnh hưởng của sự không chắc chắn lên mục tiêu. Nó bao gồm cả mối đe dọa (tiêu cực) và cơ hội bị bỏ lỡ (tích cực).

Rủi ro hỗ trợ giá trị (Benefit Enablement)

Dự án không tạo ra giá trị kỳ vọng.

Rủi ro chuyển giao (Program Delivery)

Vượt ngân sách, chậm tiến độ.

Rủi ro vận hành (Service Delivery)

Hệ thống ngừng hoạt động, lỗi dịch vụ.

Tổ chức để Thành công: Cấu trúc & Trách nhiệm (RACI)

	Vai trò	Định nghĩa	Ai thường nắm giữ?
	**R - Responsible** (Người thực hiện)	Cá nhân trực tiếp làm việc để hoàn thành nhiệm vụ.	Chuyên gia rủi ro / Nhân viên
	**A - Accountable** (Người chịu trách nhiệm giải trình)	Người duy nhất chịu trách nhiệm cuối cùng và phê duyệt. Không thể chuyển giao.	Lãnh đạo cấp cao / Chủ sở hữu rủi ro
	**C - Consulted** (Người tham vấn)	Cung cấp thông tin đầu vào, ý kiến chuyên môn (Giao tiếp hai chiều).	Chuyên gia pháp lý / HR / IT
	**I - Informed** (Người được thông báo)	Cần được cập nhật về tiến độ hoặc kết quả (Giao tiếp một chiều).	Các bên liên quan khác

Nguyên tắc vàng: Chỉ nên có MỘT người chịu trách nhiệm giải trình (A) cho mỗi nhiệm vụ.

Các vai trò then chốt trong Quản lý Rủi ro

Chủ sở hữu rủi ro (Risk Owner)

- Có thẩm quyền ra quyết định.
- Chịu trách nhiệm giải trình (Accountability).
- “Sở hữu” tổn thất nếu rủi ro xảy ra.
- Thường là quản lý cấp cao đơn vị kinh doanh.

Chủ sở hữu kiểm soát (Control Owner)

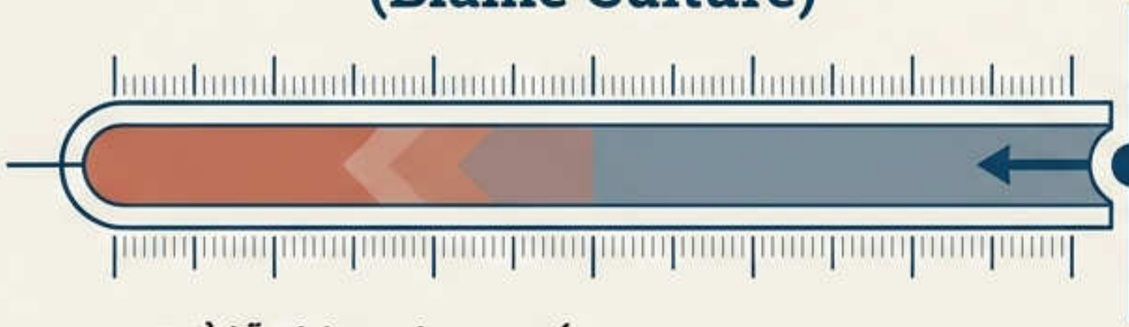
- Chịu trách nhiệm thiết kế và triển khai kiểm soát.
- Đảm bảo kiểm soát vận hành hiệu quả.
- Bảo trì và giám sát hoạt động kiểm soát.

Chuyên gia rủi ro (Risk Practitioner)

- Cung cấp dữ liệu và phân tích.
- Tư vấn và hỗ trợ ra quyết định.
- KHÔNG ra quyết định thay cho doanh nghiệp.

Yếu tố con người: Văn hóa Rủi ro & Đạo đức

Văn hóa tiêu cực (Blame Culture)



- Đổ lỗi khi có sự cố
- Che giấu thông tin (“Don’t Care”)
- Tuân thủ hình thức (“Compliance-driven”)

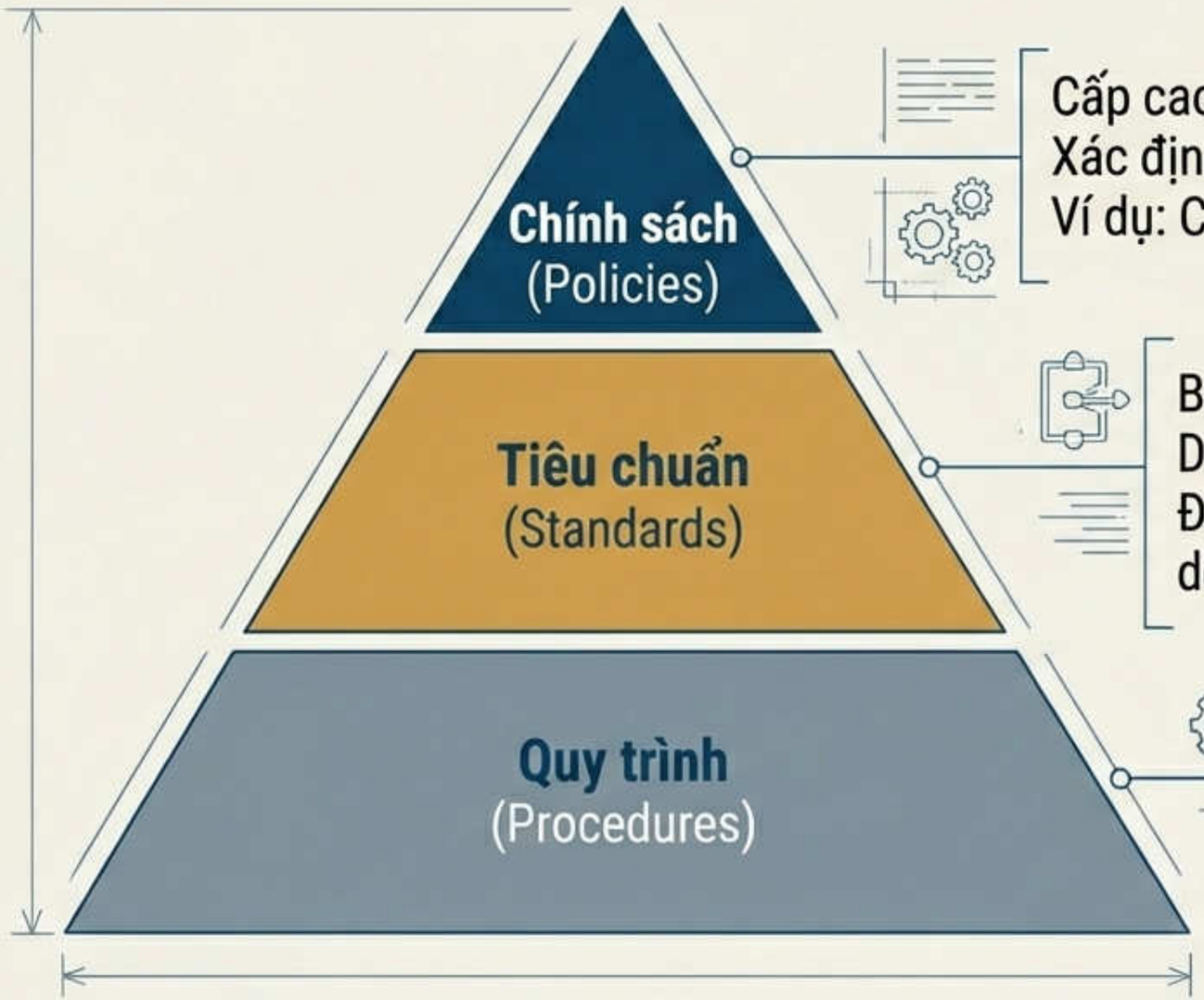
Văn hóa tích cực (Risk-Aware Culture)

- Giao tiếp **cởi mở, không sợ trả đũa**
- Rủi ro được **tích hợp** vào **quyết định**
- **Giải quyết nguyên nhân gốc rễ**

Đạo đức nghề nghiệp (ISACA Code of Ethics)

Khách quan, cẩn trọng (*due diligence*), và luôn phục vụ lợi ích của các bên liên quan.

Thiết lập Quy tắc: Chính sách & Tiêu chuẩn



Cấp cao nhất. Thể hiện ý chí lãnh đạo.
Xác định "Cái gì" (What) và "Tại sao" (Why).
Ví dụ: Chính sách An toàn thông tin.

Bắt buộc.
Dựa trên khung ISO/NIST.
Đảm bảo tính nhất quán trên toàn doanh nghiệp.

Chi tiết từng bước (Step-by-step).
Xác định "Làm thế nào" (How), "Khi nào" (When), "Ai" (Who).
Ví dụ: Quy trình xử lý sự cố.

Các khung quản lý & Tiêu chuẩn rủi ro

Áp dụng các khung tiêu chuẩn đã được công nhận để đảm bảo tính toàn diện.

ISO Standards

- **ISO 31000:2018**: Nguyên tắc quản lý rủi ro chung.
- **IEC 31010:2019**: Kỹ thuật đánh giá rủi ro.
- **ISO/IEC 27001 & 27005**: Quản lý rủi ro An toàn thông tin.

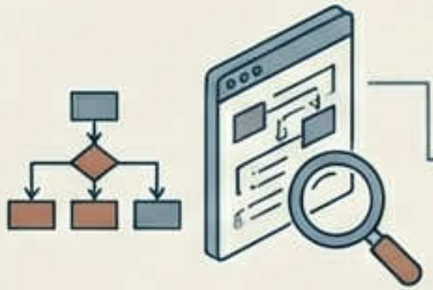
NIST

- **NIST SP 800-39**: Quản lý rủi ro ATTT (Từ chiến lược đến vận hành).

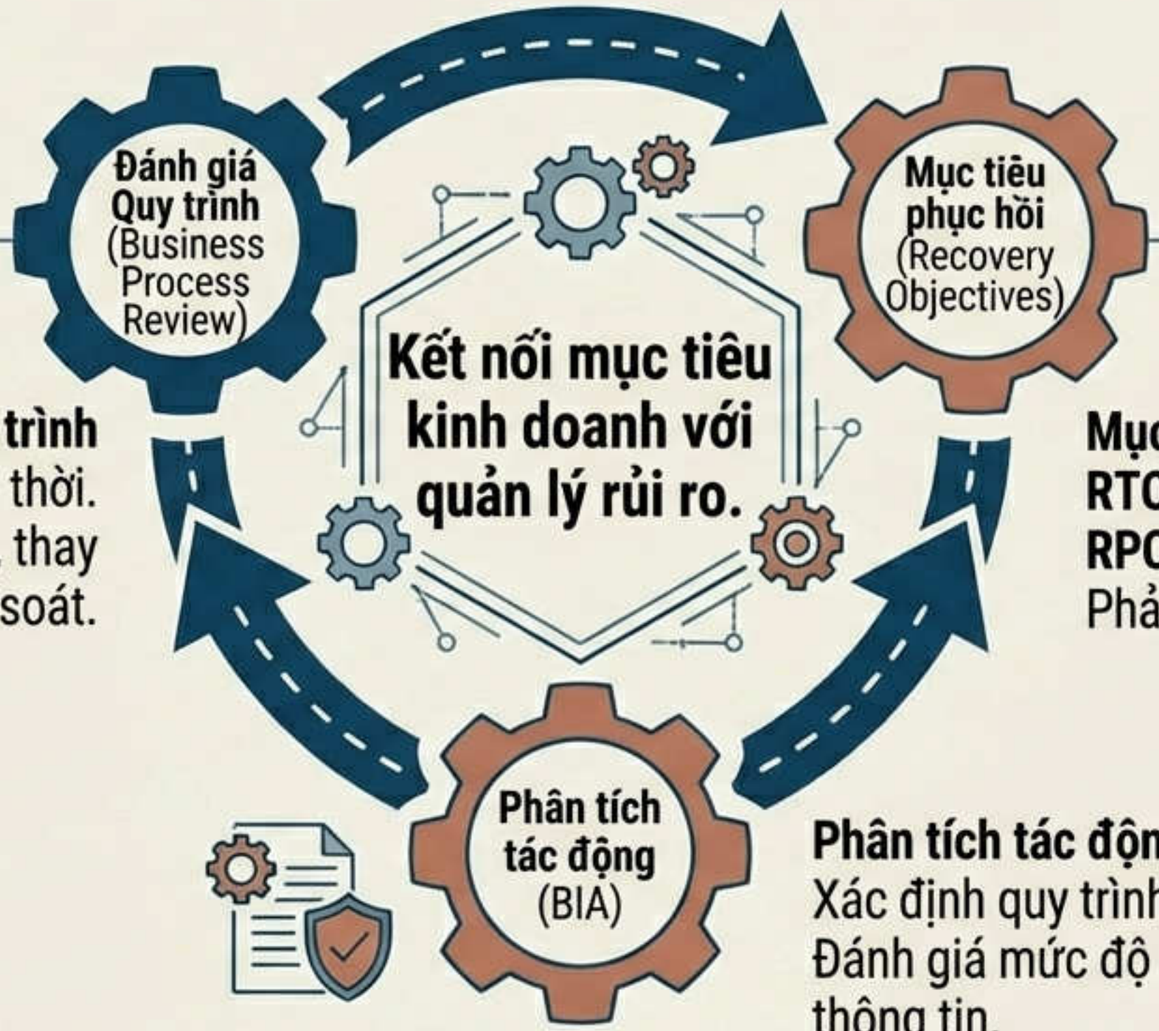
COBIT

- **COBIT**: Khung quản trị CNTT, liên kết rủi ro CNTT với mục tiêu kinh doanh.

Hiện thực hóa Vận hành: Quy trình & Khả năng phục hồi



Đánh giá Quy trình
Rủi ro nằm ở quy trình lỗi thời. Đánh giá rủi ro dự án, thay đổi và kiểm soát.



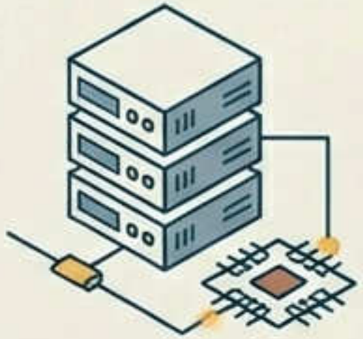
Mục tiêu phục hồi
RTO (Thời gian phục hồi mục tiêu).
RPO (Điểm phục hồi mục tiêu).
Phải dựa trên yêu cầu kinh doanh.

Phân tích tác động (BIA)
Xác định quy trình quan trọng. Đánh giá mức độ nhạy cảm của thông tin.

Quản lý Tài sản Tổ chức

Để quản lý rủi ro, doanh nghiệp phải biết mình đang sở hữu và bảo vệ cái gì.

Con người (People)
Kỹ năng, kiến thức, tính sẵn sàng.



Công nghệ (Technology)
Phần cứng, phần mềm, hạ tầng mạng.

Dữ liệu (Data)
Thông tin khách hàng, dữ liệu tài chính, dữ liệu vận hành.

Sở hữu trí tuệ (IP)
Bí mật thương mại, mã nguồn, thương hiệu.

Định giá Tài sản: Không chỉ là chi phí mua mới, mà bao gồm chi phí gián đoạn, pháp lý và danh tiếng.

Tổng hợp: Mô hình Thác đổ Chiến lược

Mục đích & Định hướng
Chiến lược - Mục tiêu - 4 Are's

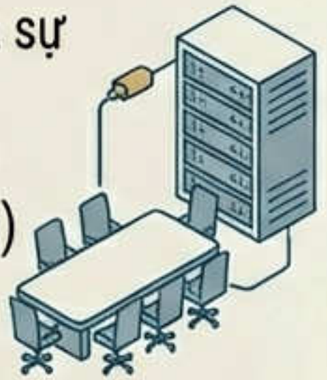
Trật tự & Cấu trúc
Mô hình RACI - 3 Tuyến phòng thủ

Hành vi & Văn hóa
Văn hóa rủi ro - Đạo đức nghề nghiệp

Quy tắc
Chính sách - Tiêu chuẩn

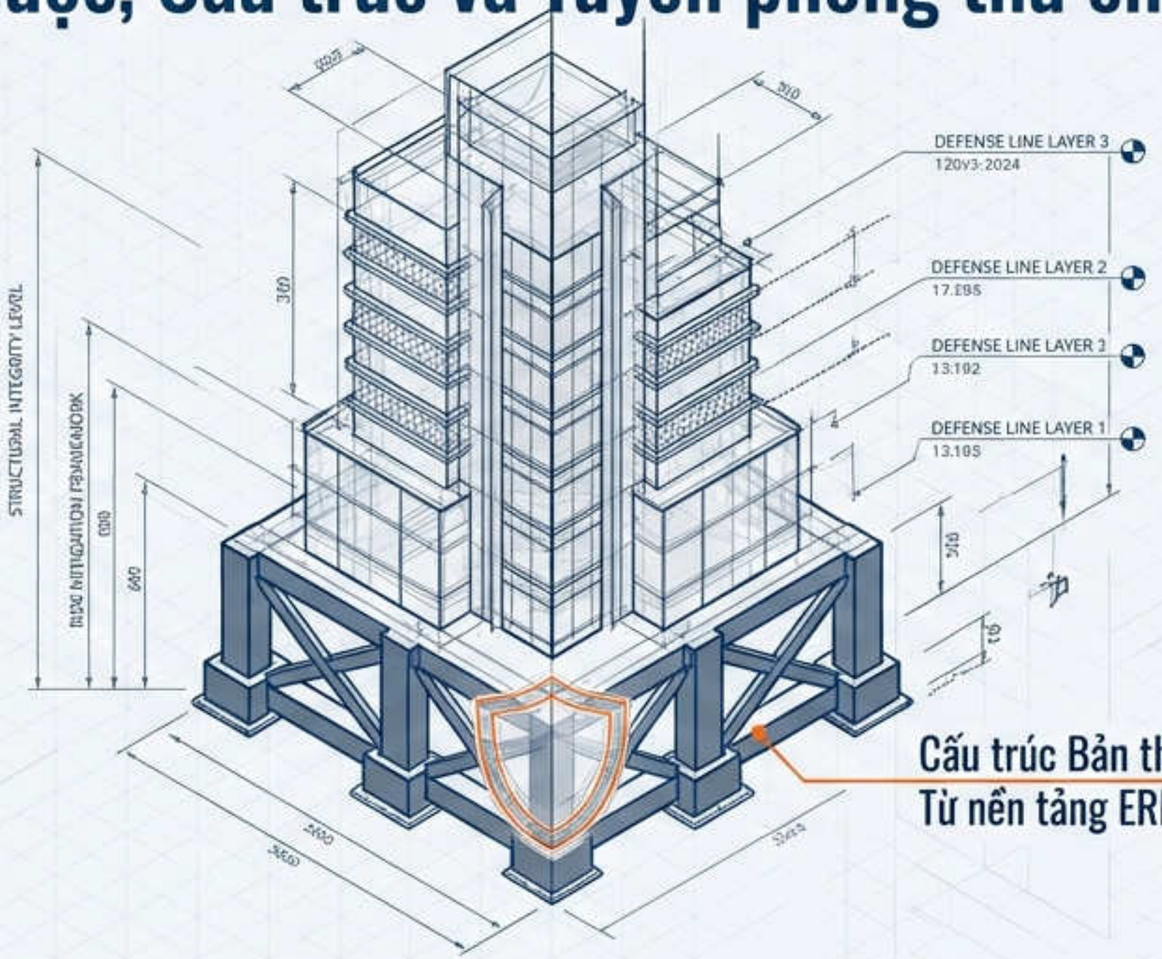
Thực thi
Quy trình - Tài sản - Dữ liệu

Quản trị hiệu quả là sự liên kết chặt chẽ từ phòng họp hội đồng quản trị (Boardroom) đến phòng máy chủ (Server room).



Chương 1 - Phần B: Quản trị Rủi ro

Xây dựng Chiến lược, Cấu trúc và Tuyến phòng thủ cho Doanh nghiệp

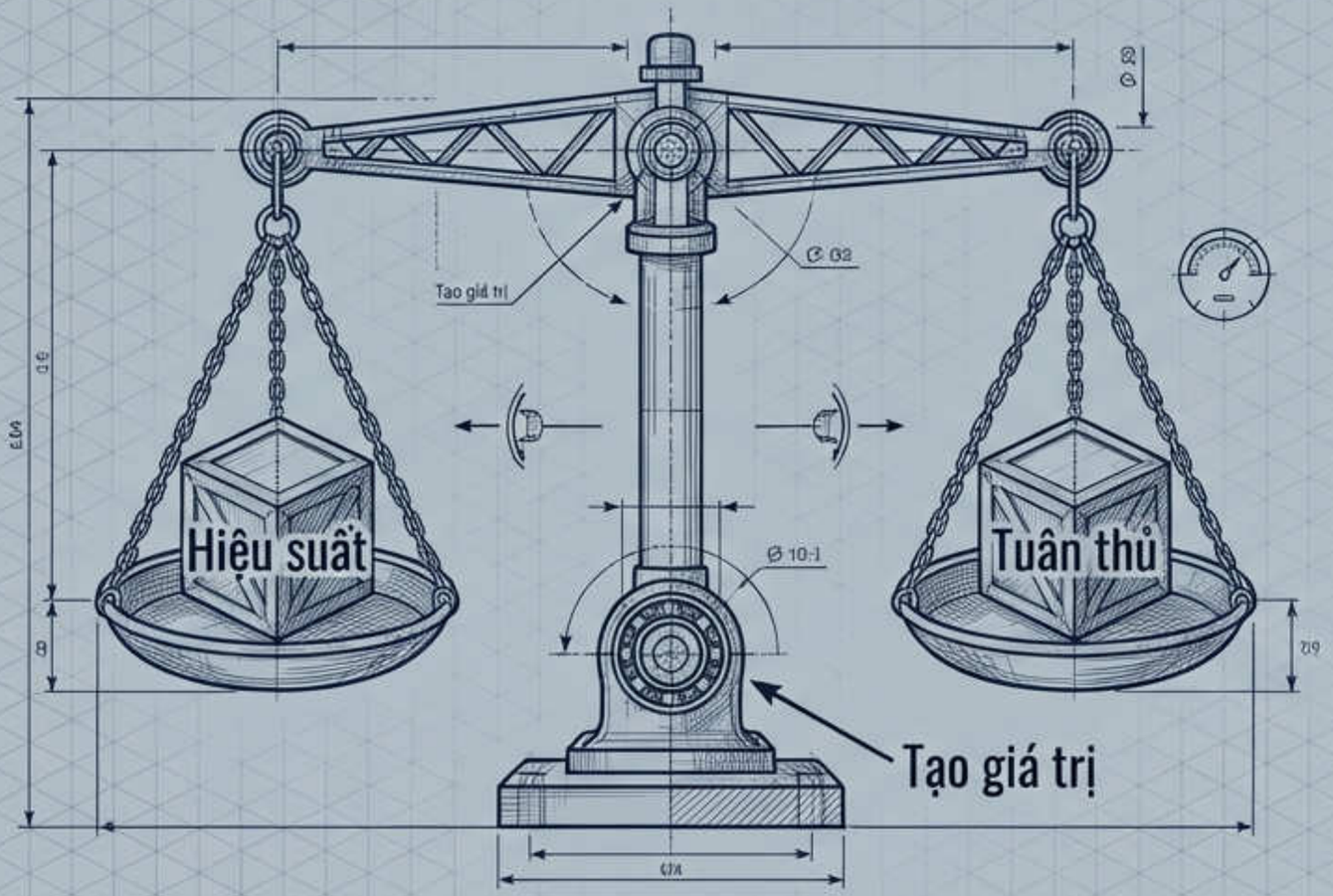


Cấu trúc Bản thiết kế:
Từ nền tảng ERM đến các giới hạn rủi ro

PROJECT:	ENTERPRISE RISK MGMT	
DRAWING NO:	C1-B-001	
DATE: OCT 26, 2024	SCALE: NTS	

Dựa trên tài liệu CRISC® Official Review Manual, 8th Edition

Quản trị Rủi ro: Cân bằng giữa Hiệu suất và Tuân thủ



Quản trị (Governance) vs. Quản lý (Management)

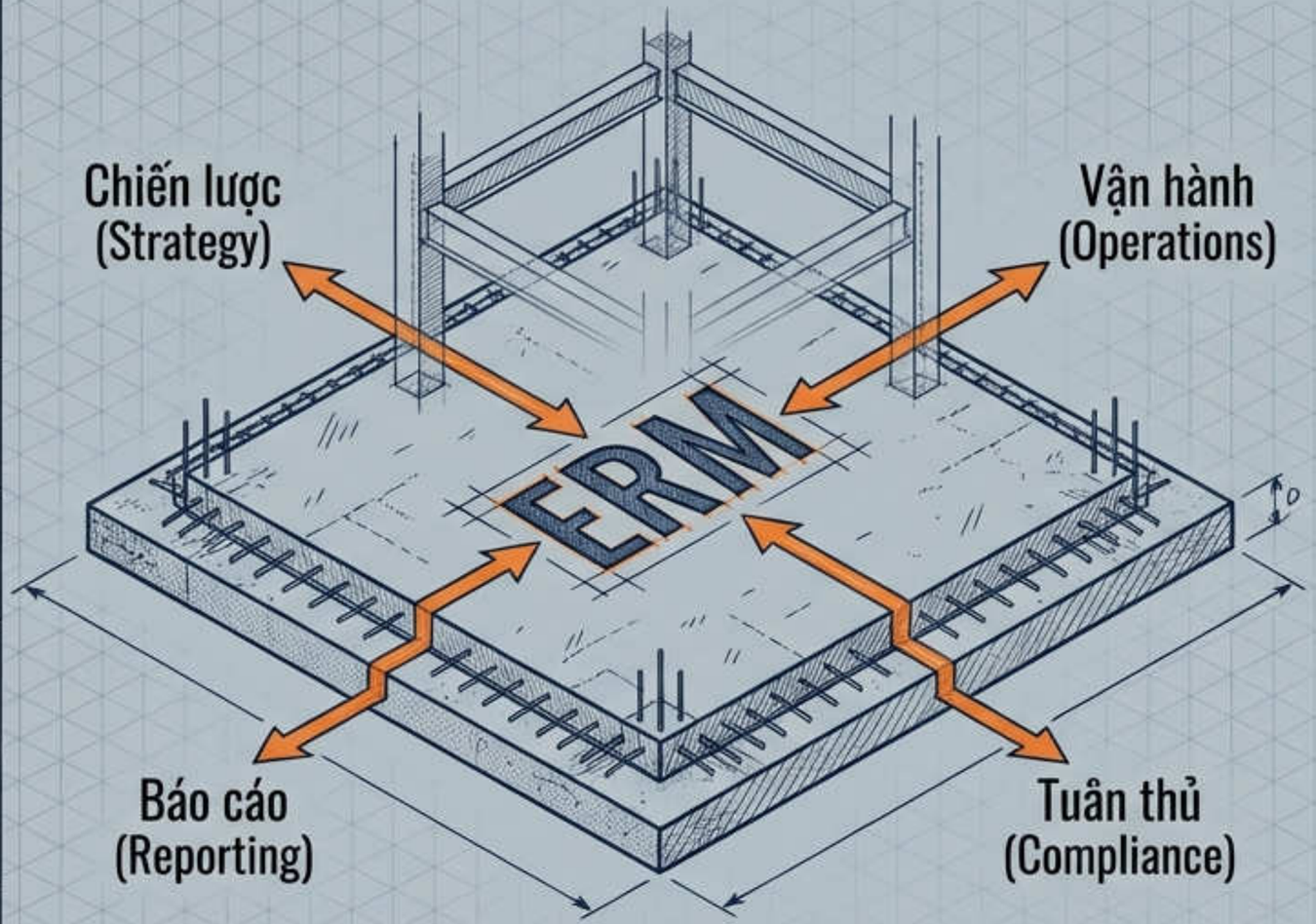
- **Quản trị:** Đánh giá, định hướng và giám sát.
- **Quản lý:** Lập kế hoạch, xây dựng, vận hành và theo dõi.

Mục tiêu: Tạo giá trị qua 3 trụ cột

1. Hiện thực hóa lợi ích (Benefit Realization)
2. Tối ưu hóa rủi ro (Risk Optimization)
3. Tối ưu hóa nguồn lực (Resource Optimization)

Quản trị hiệu quả không phải là loại bỏ rủi ro, mà là đảm bảo rủi ro được tối ưu hóa để đạt mục tiêu doanh nghiệp.

Nền tảng: Quản trị Rủi ro Doanh nghiệp (ERM)



Định nghĩa:

ERM là hoạt động điều phối để chỉ đạo và kiểm soát doanh nghiệp liên quan đến rủi ro. Kết nối rủi ro CNTT với mục tiêu kinh doanh.

Nguyên tắc cốt lõi (Good Practices)

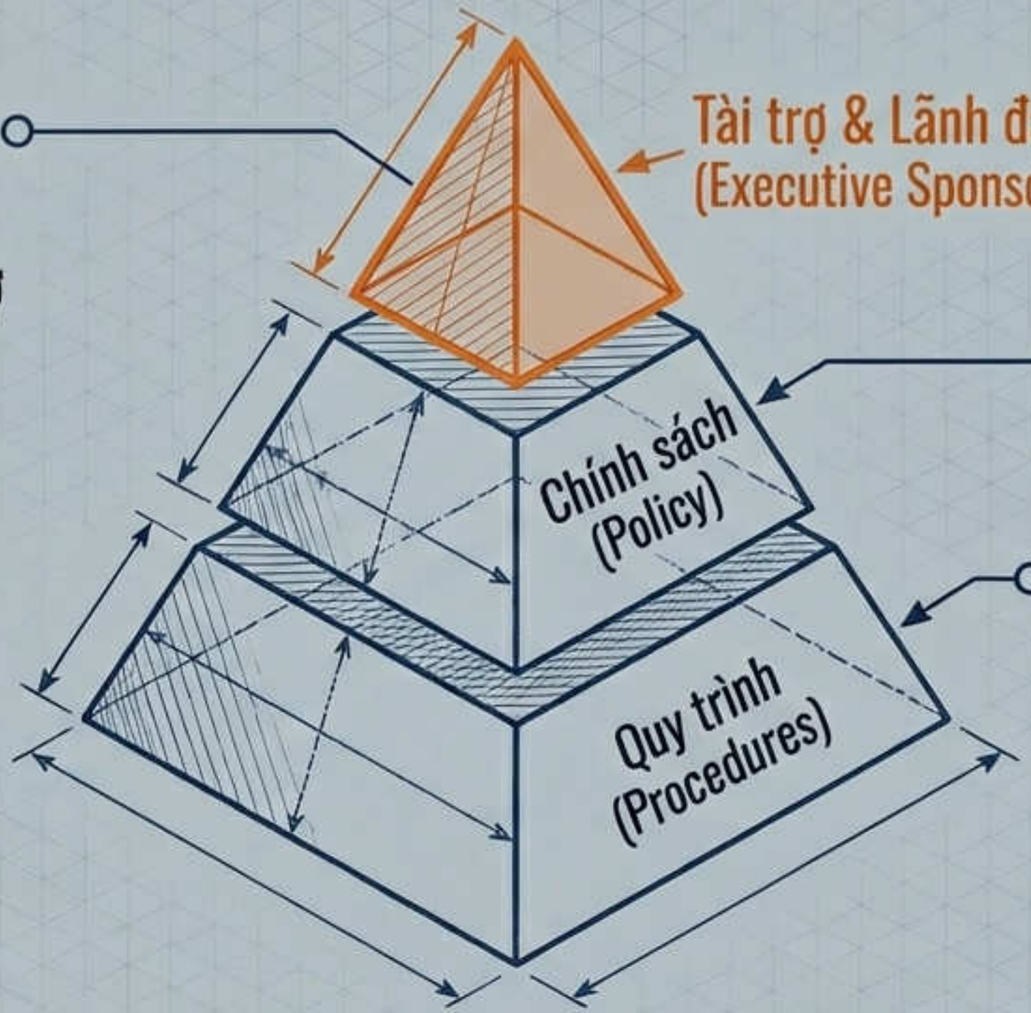
- **Toàn diện (Comprehensive)**: Bao phủ mọi khía cạnh, không chỉ CNTT.
- **Có thể kiểm toán (Auditable)**: Quyết định và quy trình được ghi lại.
- **Có thể biện minh (Justifiable)**: Dựa trên lý luận và dữ liệu.
- **Tuân thủ (Compliant)**: Tuân theo chính sách nội bộ và luật pháp bên ngoài.

Cảnh báo: Quản lý rủi ro rời rạc (Silos) tạo ra 'Sự an tâm giả tạo'.

Thiết lập Phương pháp Tiếp cận: Tông giọng từ Cấp lãnh đạo

Tone at the Top (Tông giọng từ cấp lãnh đạo):

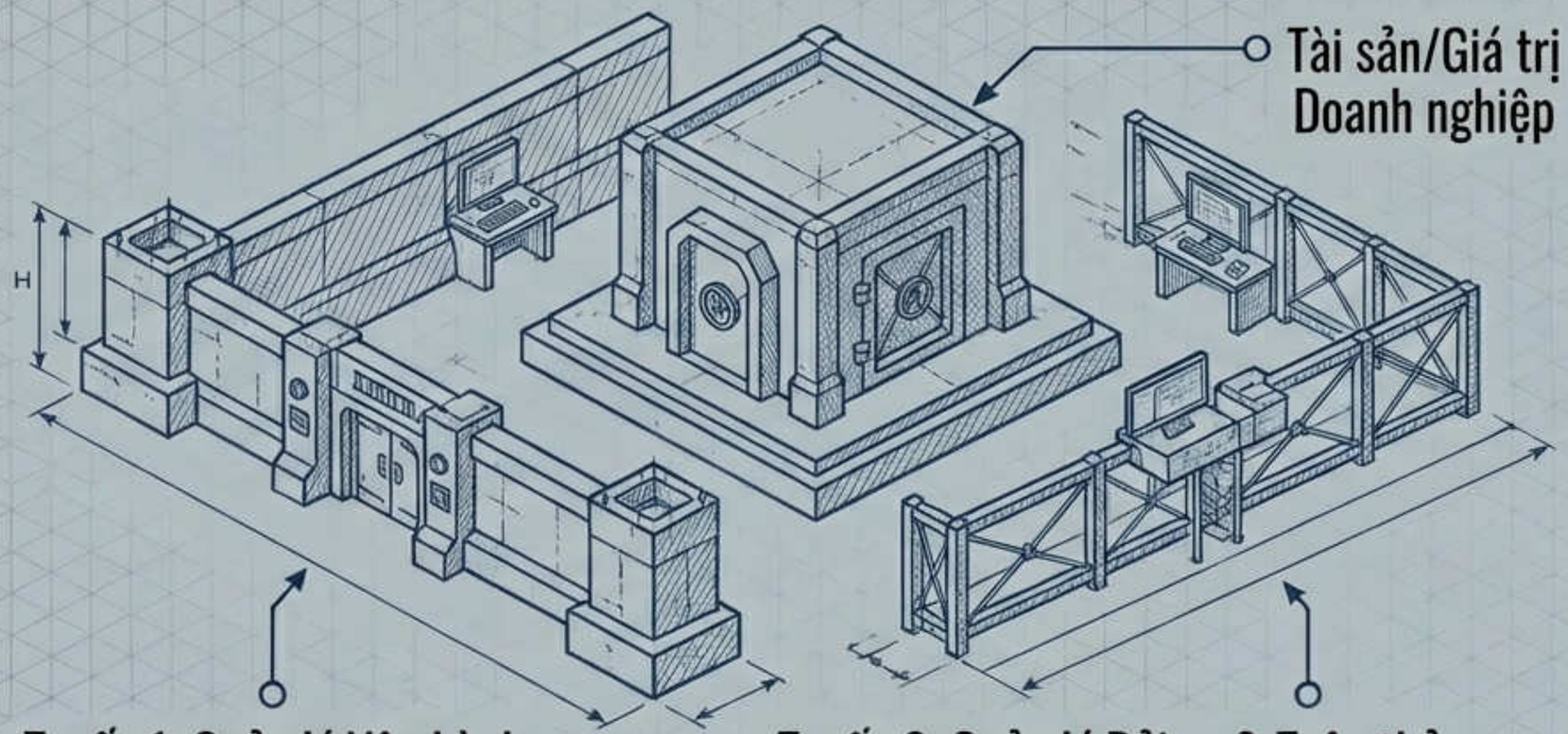
- Lãnh đạo cấp cao phải hỗ trợ rõ ràng.
- Phê duyệt 'Khẩu vị rủi ro'.
- Không có sự hỗ trợ này, chương trình thiếu thẩm quyền và ngân sách.

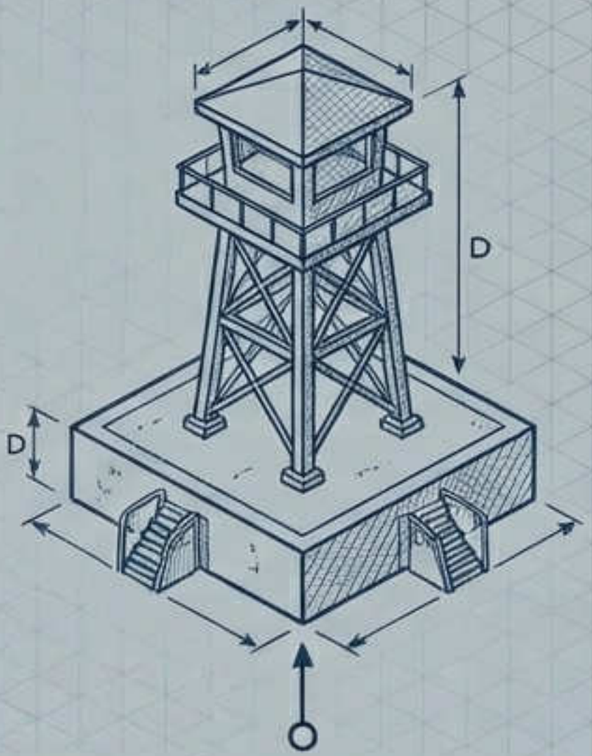


Chính sách (Policy):

- Tuyên bố ý định ngắn gọn.
- Giải thích LÝ DO quản lý rủi ro.
- Xác định trách nhiệm giải trình.
- Cam kết cải tiến liên tục.

Mô hình Ba Tuyến phòng thủ (The Three Lines of Defense)





Tuyến 1: Quản lý Vận hành

- Chức năng: Sở hữu và quản lý rủi ro.
- Trách nhiệm: Quản lý hàng ngày.

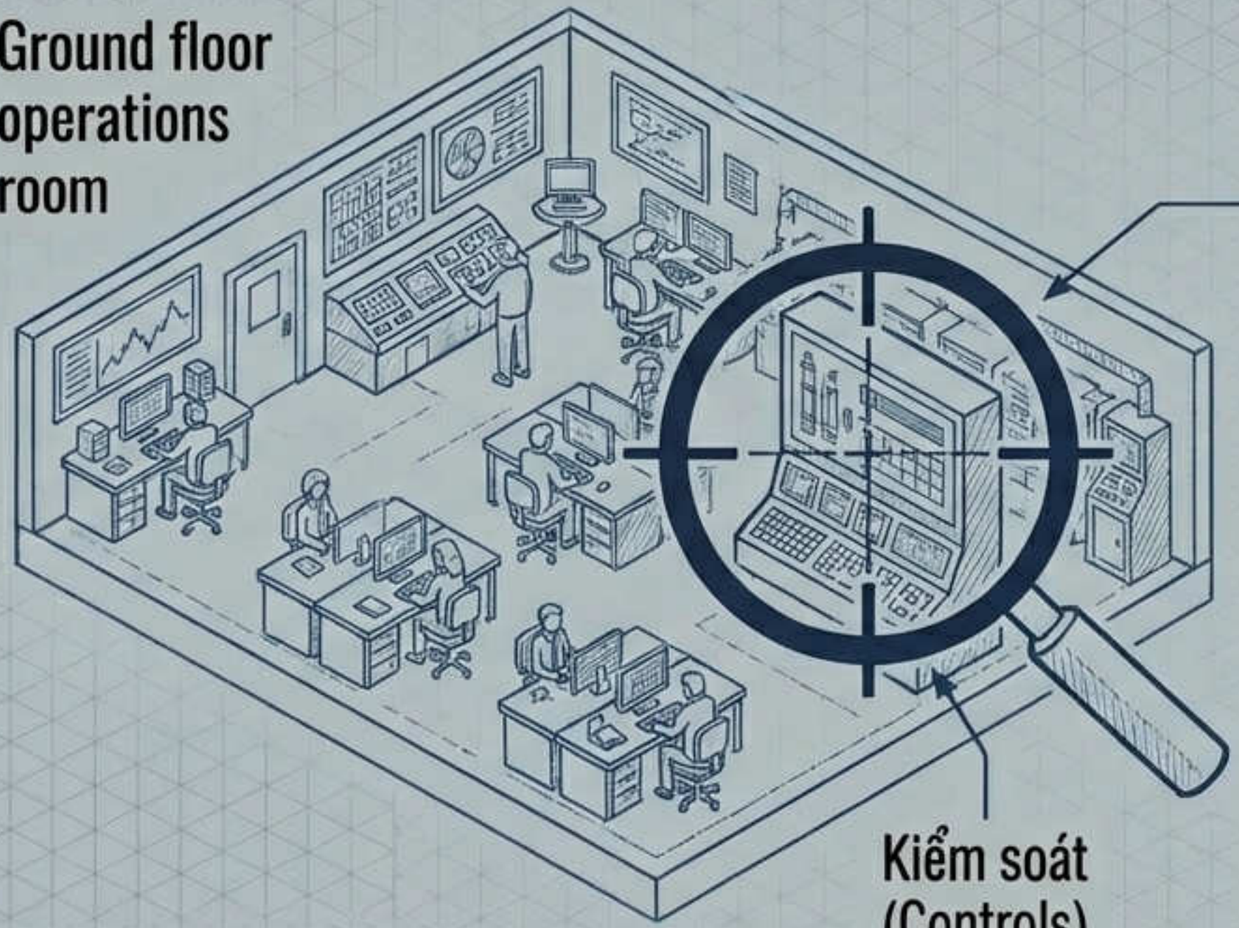
Tuyến 2: Quản lý Rủi ro & Tuân thủ

- Chức năng: Giám sát rủi ro.
- Trách nhiệm: Thiết lập khung và theo dõi.

Tuyến 3: Kiểm toán Nội bộ

- Chức năng: Đảm bảo độc lập.
- Trách nhiệm: Báo cáo trực tiếp lên HĐQT.

Tuyến 1: Quản lý Vận hành - Chủ sở hữu Rủi ro



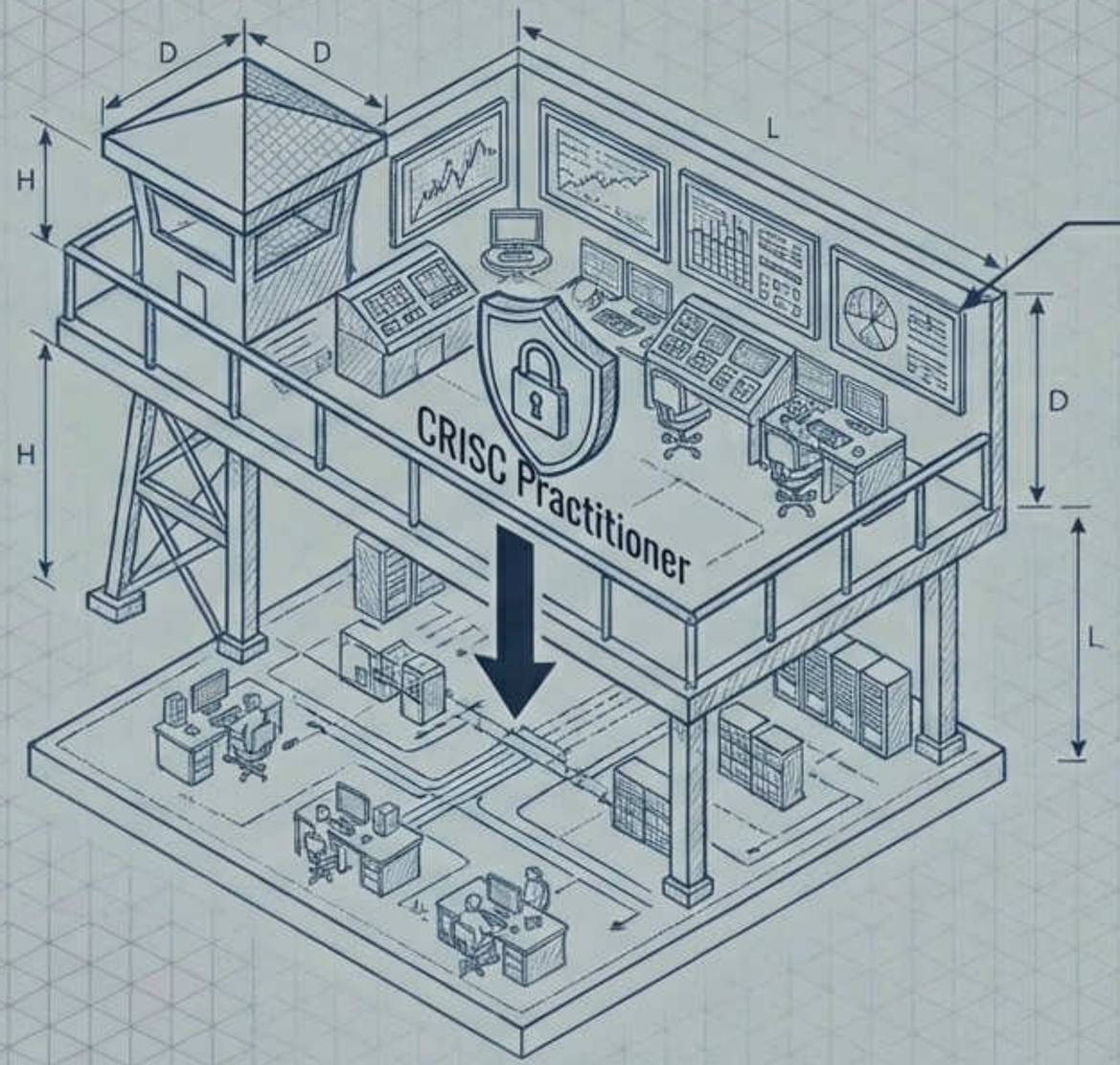
Vai trò: Quản lý vận hành (Operational Management).

Trách nhiệm chính:

- Chủ sở hữu rủi ro (Risk Owners): Chịu trách nhiệm giải trình về rủi ro trong hoạt động hàng ngày.
- Hành động: Phát hiện và xử lý rủi ro ngay lập tức.
- Thực thi: Chịu trách nhiệm thực hiện các biện pháp kiểm soát nội bộ.

Họ là những người phản ứng đầu tiên. Nếu kiểm soát thất bại, họ là người chịu trách nhiệm sửa chữa.

Tuyến 2: Giám sát - Quản lý Rủi ro & Tuân thủ



Vai trò: Chức năng Quản lý Rủi ro & Tuân thủ.

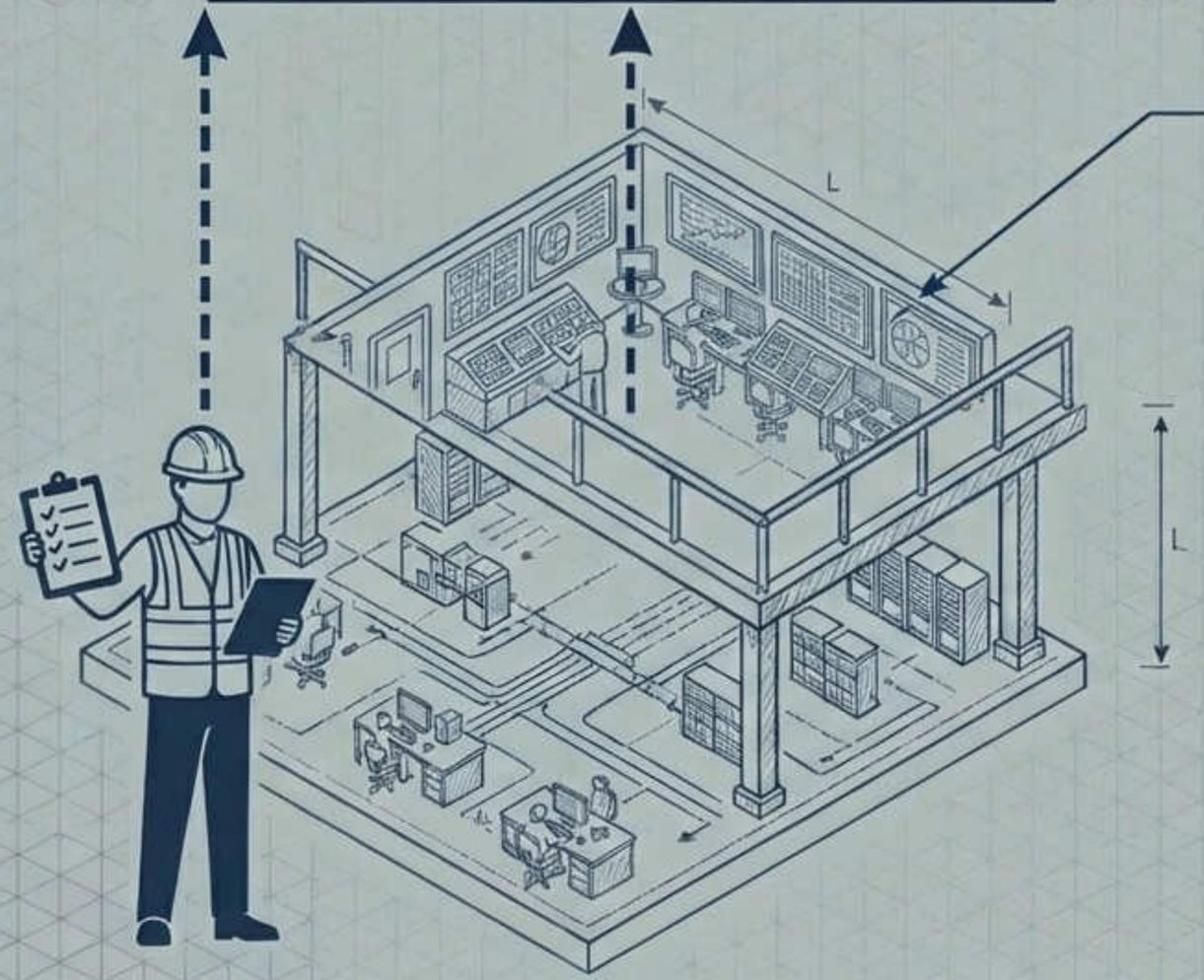
Trách nhiệm chính:

- Khung quản trị: Thiết lập chính sách và khung rủi ro.
- Giám sát: Theo dõi Tuyến 1 để đảm bảo tuân thủ.
- Báo cáo: Tổng hợp báo cáo rủi ro cho lãnh đạo cấp cao.
- Hỗ trợ: Giúp Tuyến 1 xác định rủi ro nhưng vẫn giữ sự độc lập.

Đây là vị trí làm việc thường thấy của chuyên gia CRISC.

Tuyến 3: Đảm bảo - Kiểm toán Nội bộ

Hội đồng Quản trị / Ủy ban Kiểm toán



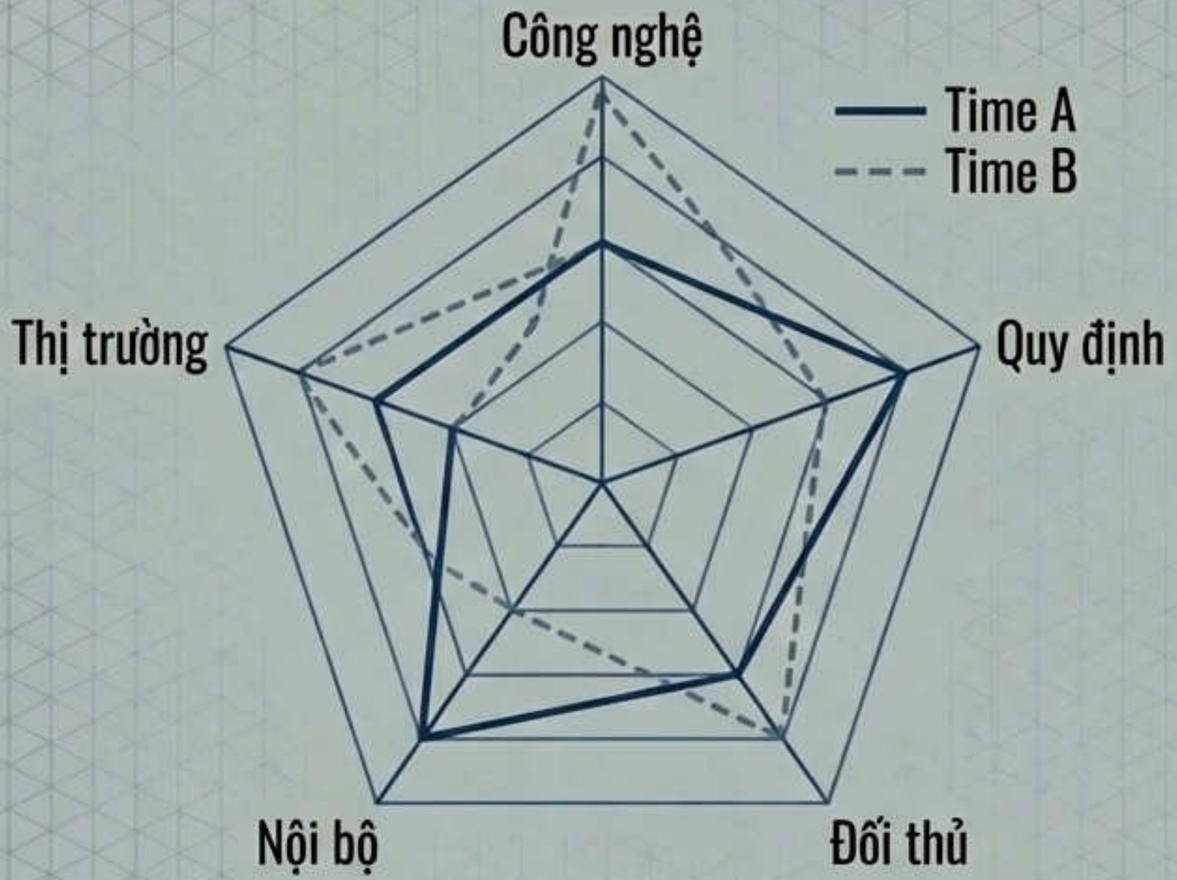
Vai trò: Kiểm toán Nội bộ (Internal Audit).
Đặc điểm cốt lõi: Độc lập và Khách quan.

Trách nhiệm chính:

- Đảm bảo độc lập về hiệu quả của quản trị và kiểm soát.
- Đánh giá: Họ KHÔNG thiết kế hay thực hiện kiểm soát (để tránh xung đột lợi ích), họ chỉ ĐÁNH GIÁ chúng.
- Báo cáo: Báo cáo trực tiếp lên cơ quan quản trị cao nhất.

Kiểm toán nội bộ kiểm tra xem Tuyến 1 và Tuyến 2 có đang làm tốt công việc của họ hay không.

Hồ sơ Rủi ro (Risk Profile) và Các yếu tố Thay đổi



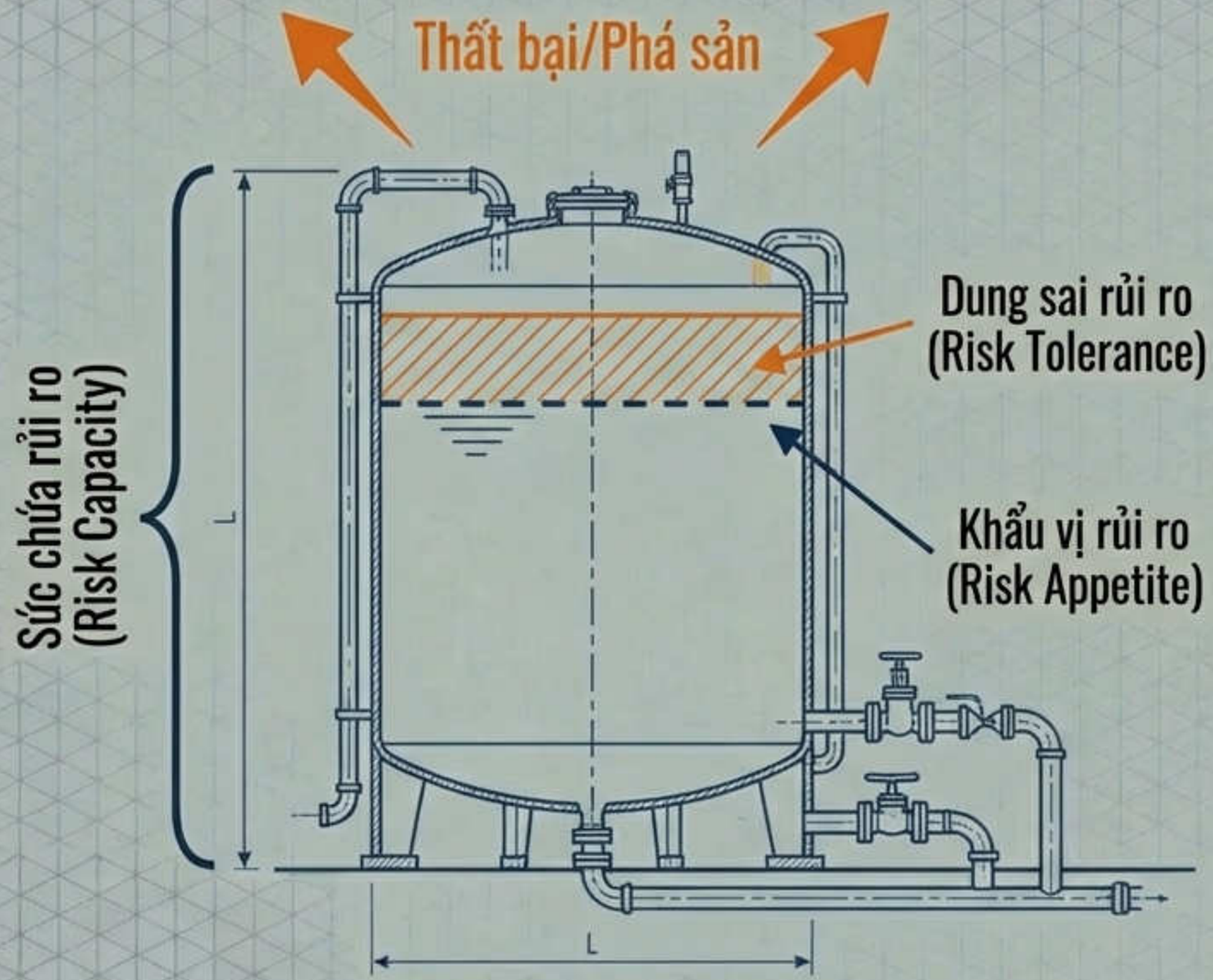
Định nghĩa: Hồ sơ rủi ro là bức tranh toàn cảnh về mức độ tiếp xúc rủi ro của doanh nghiệp tại một thời điểm cụ thể.

Các yếu tố kích hoạt thay đổi (Cần giám sát):

- Công nghệ mới (AI, Cloud): Cơ hội đi kèm đe dọa.
- M&A: Sáp nhập mang lại hệ thống và văn hóa mới.
- Quy định: Luật pháp mới (GDPR, Luật An ninh mạng).
- Đối thủ cạnh tranh: Thay đổi thị trường.
- Bên thứ ba: Chuỗi cung ứng.

Hồ sơ rủi ro không bao giờ tĩnh. Cần Giám sát liên tục (Continuous Monitoring).

Định nghĩa Giới hạn: Khẩu vị, Dung sai và Sức chứa



Sức chứa (Capacity):

- Điểm giới hạn tuyệt đối. Vượt quá mức này đồng nghĩa với thất bại.
- Dựa trên vốn và thanh khoản.

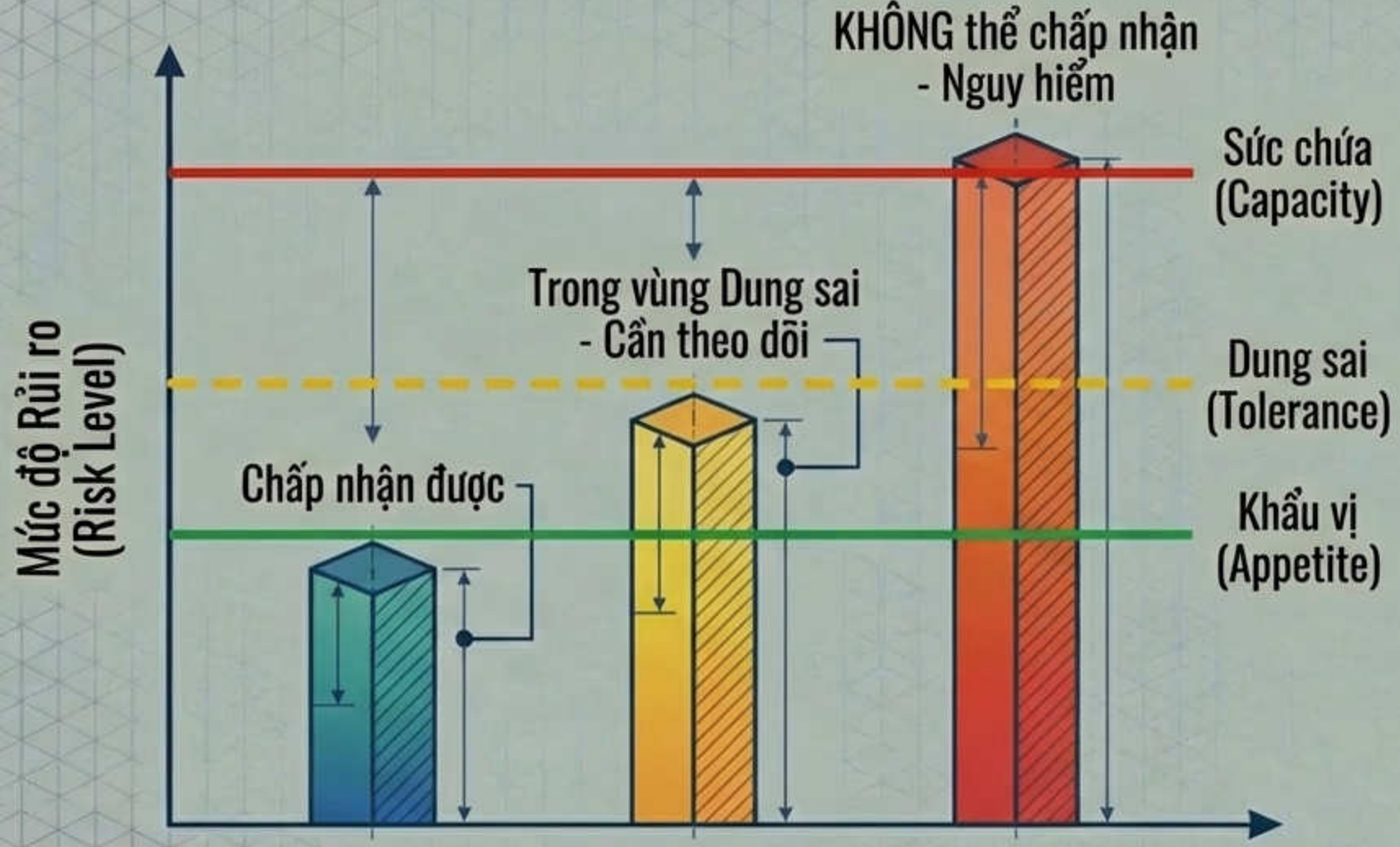
Khẩu vị (Appetite):

- Mức rủi ro mong muốn chấp nhận để đạt mục tiêu.
- Được thiết lập bởi HĐQT.

Dung sai (Tolerance):

- Mức độ sai lệch chấp nhận được so với khẩu vị.
- Mang tính chiến thuật (ví dụ: dự án vượt ngân sách 10%).

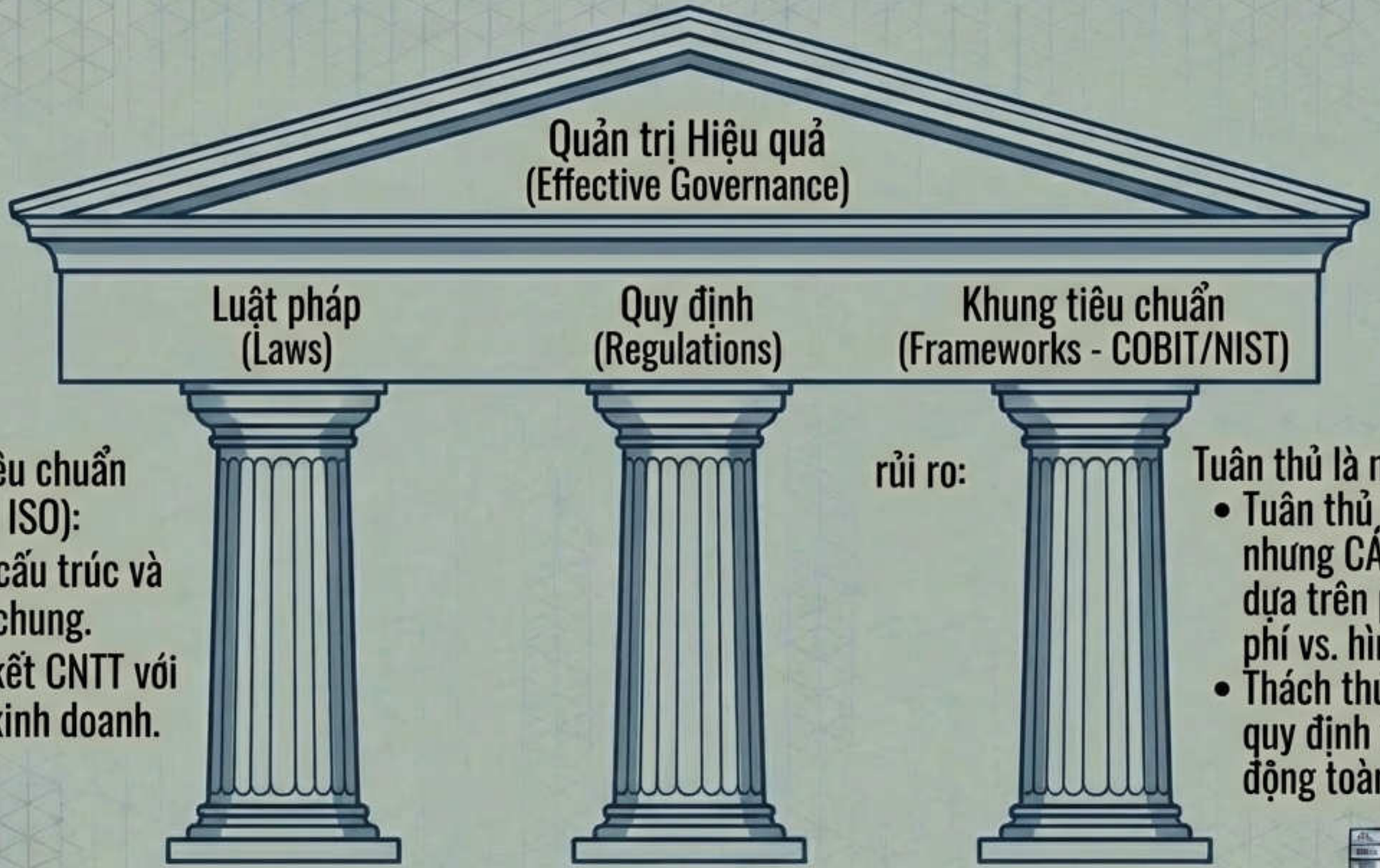
Trực quan hóa Các giới hạn Rủi ro



Quy tắc Quản trị:

- Rủi ro thực tế < Sức chứa.
- Lý tưởng: Rủi ro thực tế tiệm cận Khẩu vị.
- Các giới hạn này phải được phê duyệt và truyền thông rõ ràng.

Khung quản trị, Luật pháp và Quy định



Các Khung tiêu chuẩn (COBIT, NIST, ISO):

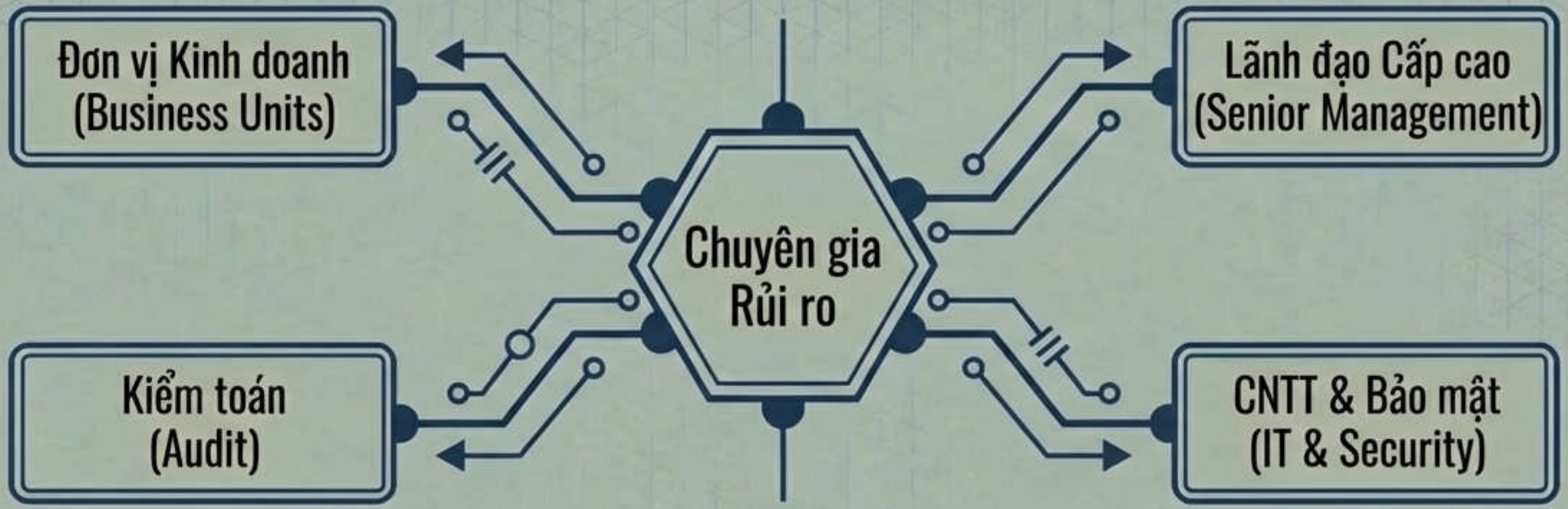
- Cung cấp cấu trúc và ngôn ngữ chung.
- Giúp liên kết CNTT với mục tiêu kinh doanh.

rủi ro:

Tuân thủ là một quyết định

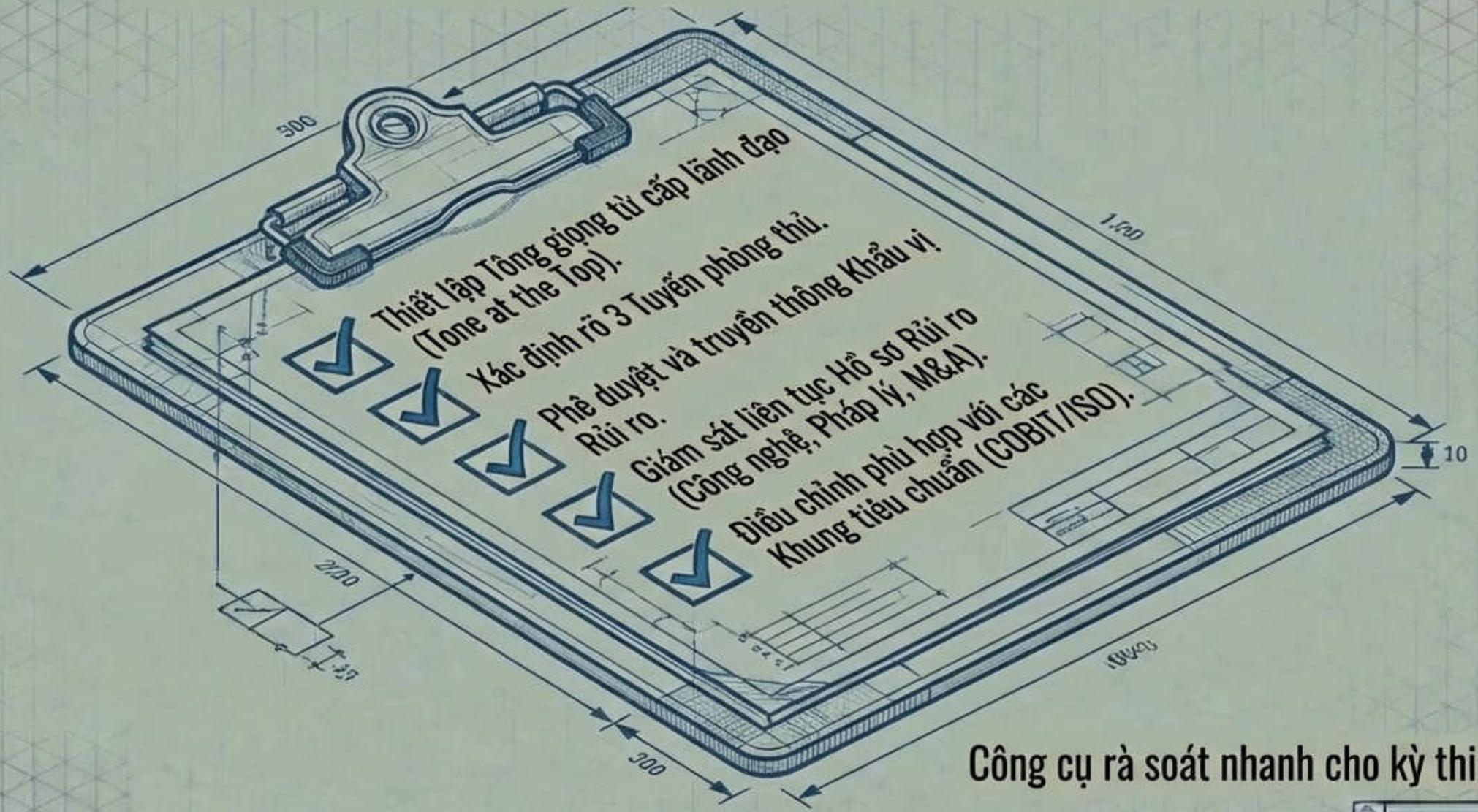
- Tuân thủ là bắt buộc, nhưng CÁCH tuân thủ dựa trên phân tích chi phí vs. hình phạt.
- Thách thức: Mâu thuẫn quy định trong hoạt động toàn cầu.

Vai trò của Chuyên gia Rủi ro (Risk Practitioner)



1. **Cố vấn (Advisor):** Tư vấn về các mối đe dọa và phản ứng rủi ro.
2. **Điều phối viên (Facilitator):** Hỗ trợ quản lý chọn khẩu vị và dung sai rủi ro.
3. **Người báo cáo (Reporter):** Duy trì Sổ đăng ký rủi ro (Risk Register).
4. **Cầu nối (Bridge):** Dịch thuật rủi ro kỹ thuật sangngôn ngữ kinh doanh.

Danh sách Kiểm tra Quản trị Rủi ro (Checklist)



Công cụ rà soát nhanh cho kỳ thi CRISC.

Kết luận: Từ Quản trị đến Giá trị

Quản trị rủi ro hiệu quả không phải là loại bỏ rủi ro, mà là hiểu rõ rủi ro để đưa ra quyết định kinh doanh sáng suốt.

Hiểu rõ rủi ro = Tăng cường khả năng phục hồi + Tối ưu hóa nguồn lực.

Risk Identification: Xây dựng nền móng cho Quản trị Rủi ro

Chapter 2 - Part A: Từ Nhận diện Mối đe dọa đến Xây dựng Kịch bản Rủi ro

Based on CRISC® Official Review Manual, 8th Edition

Tầm quan trọng của Nhận diện Rủi ro (Risk Identification)

Khái niệm cốt lõi: Nhận diện rủi ro là quá trình xác định các kịch bản sự kiện tổn thất (loss-event scenarios) có thể ảnh hưởng đến mục tiêu chiến lược. Nếu không nhận diện đúng, khả năng phục hồi của doanh nghiệp bị đe dọa.

Mục tiêu chính:

1. Hiểu Bối cảnh (Context): Làm việc với chủ sở hữu quy trình để hiểu vận hành.
2. Không chỉ là IT: Bao gồm yếu tố bên ngoài và giả định kinh doanh.
3. Đầu vào quan trọng: Bắt buộc cho bước Đánh giá và Phản hồi.

IT Risk Management Life Cycle

Phân biệt Cốt lõi: Threat Event và Risk Event

Hiểu đúng sự khác biệt giữa hành động và hậu quả

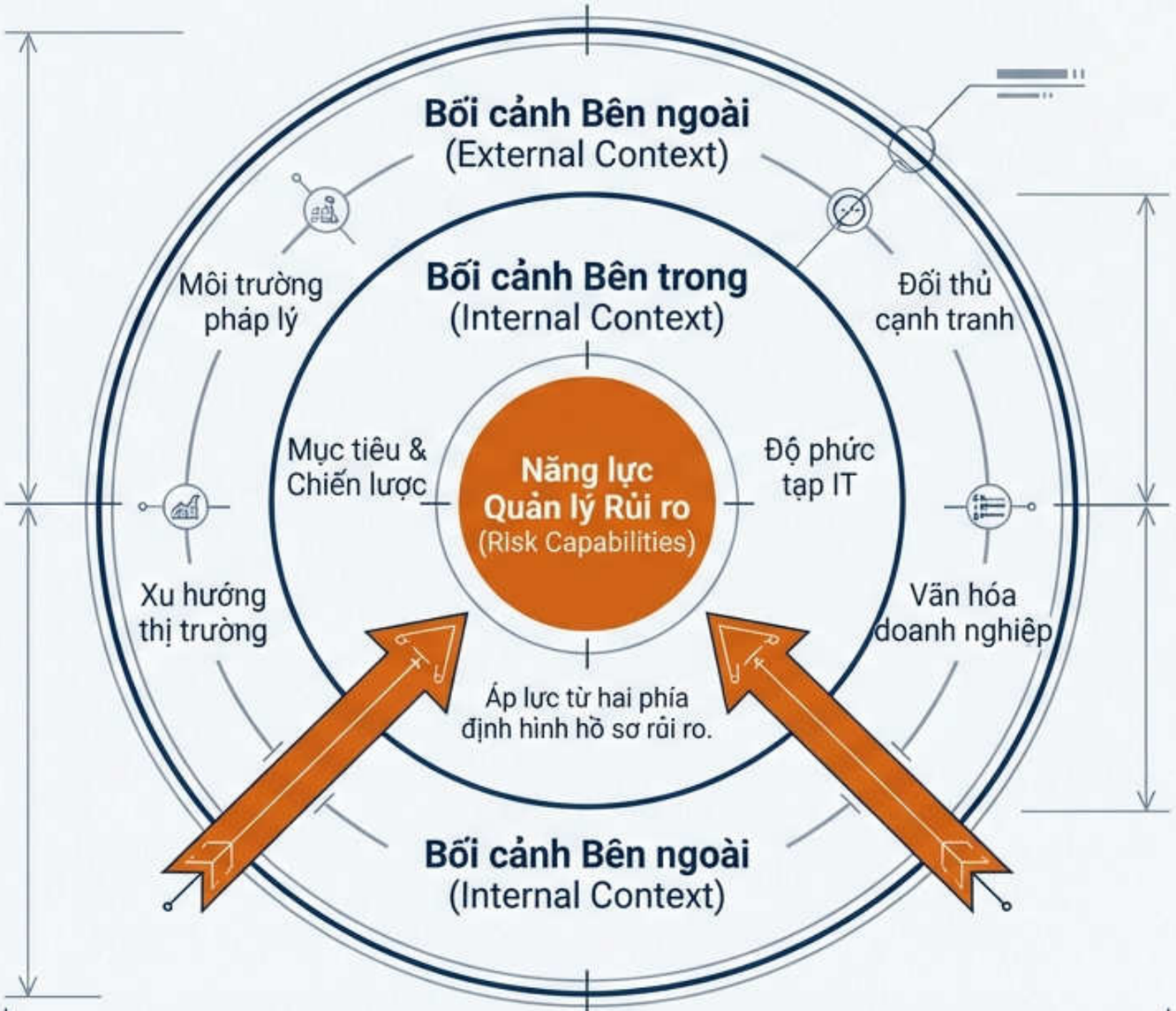
Định nghĩa:

- **Threat Event**: Hành động có tiềm năng gây hại (VD: Hacker tấn công).
- **Risk Event**: Hậu quả cụ thể khi mối đe dọa khai thác thành công lỗ hổng (VD: Mất dữ liệu).

Kịch bản 1: Ransomware (Threat)	-> Hoạt động bị ngưng trệ (Risk Event/Impact)
Kịch bản 2: Nhân viên bấm link độc hại (Threat)	-> Rò rỉ dữ liệu (Risk Event/Impact)

"Nếu không có tổn thất (loss), thì không có rủi ro (risk)."

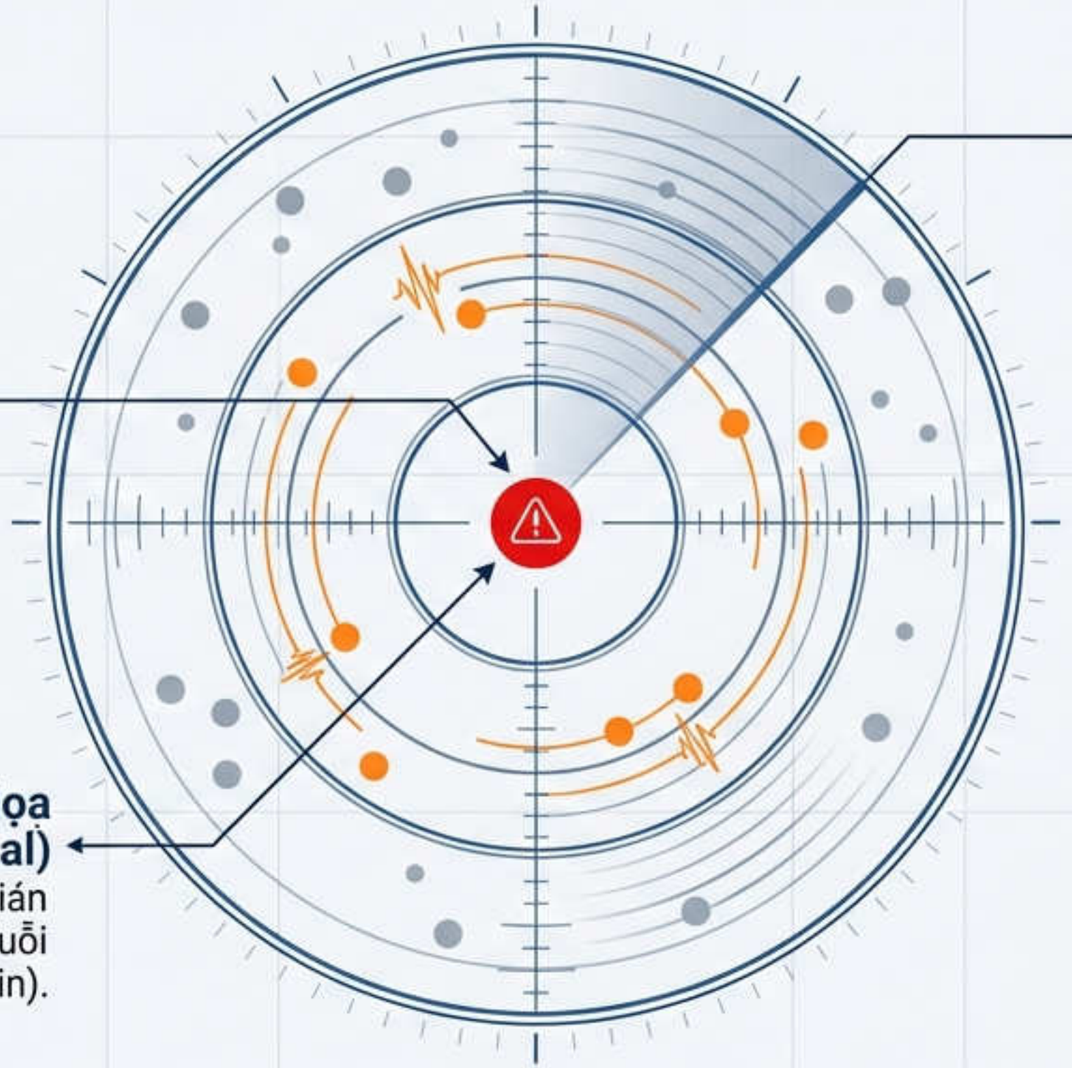
Các Nhân tố Rủi ro (Risk Factors): Bối cảnh và Năng lực



3 Phương pháp Tiếp cận để Nhận diện Rủi ro

Kết hợp cả 3 phương pháp để không bỏ sót rủi ro mới nổi

Bức tranh Mối đe dọa (Threat Landscape)



Mối đe dọa Mới nổi (Emerging)
Dấu hiệu bất thường, Công nghệ chưa kiểm chứng.

Mối đe dọa Nội bộ (Internal)
Nhân viên bất mãn, sơ suất, thiếu đào tạo. (Insider Threat)

Mối đe dọa Bên ngoài (External)
Tội phạm mạng, Gián điệp, Thiên tai, Chuỗi cung ứng (Supply Chain).

Lưu ý: Rủi ro Chuỗi cung ứng (Supply Chain Risk) đã tăng mạnh từ năm 2020 (Ví dụ: SolarWinds).

Mô hình hóa Mối đe dọa (Threat Modeling)

Tư duy như kẻ tấn công để xác định mục tiêu và động cơ

STRIDE

Tập trung kỹ thuật (Spoofing, Tampering...). Do Microsoft phát triển.

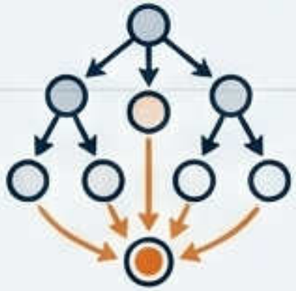
PASTA

Tập trung rủi ro (Risk-centric). Liên kết mục tiêu kinh doanh với kỹ thuật.

LINDDUN

Tập trung vào quyền riêng tư (Privacy concerns).

Attack Trees

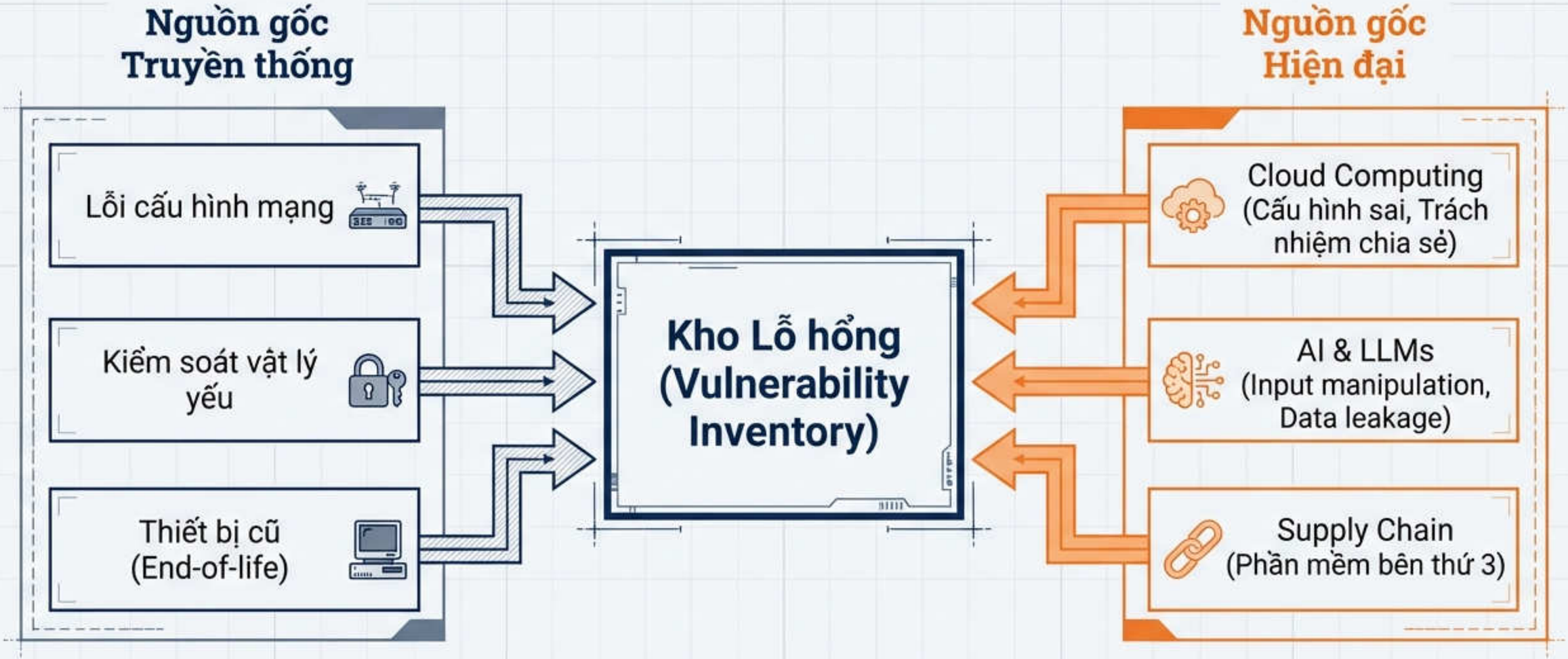


Sơ đồ cây mô tả các bước tấn công để đạt mục tiêu.

Persona non Grata

Tập trung vào động cơ và kỹ năng của con người.

Quản lý Lỗ hổng: Nguồn gốc và Công nghệ mới



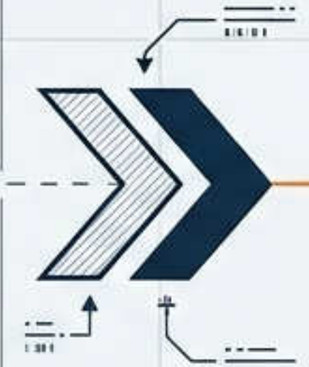
Đánh giá Lỗ hổng vs. Kiểm thử Xâm nhập

Gap Analysis: So sánh hiện trạng và trạng thái mong muốn

Vulnerability Assessment

Rộng nhưng Nông

- Rà quét tự động tìm lỗ hổng đã biết.
- Xác định cổng mở, thiếu bản vá.
- Mục tiêu: Liệt kê và xếp hạng (CVSS).



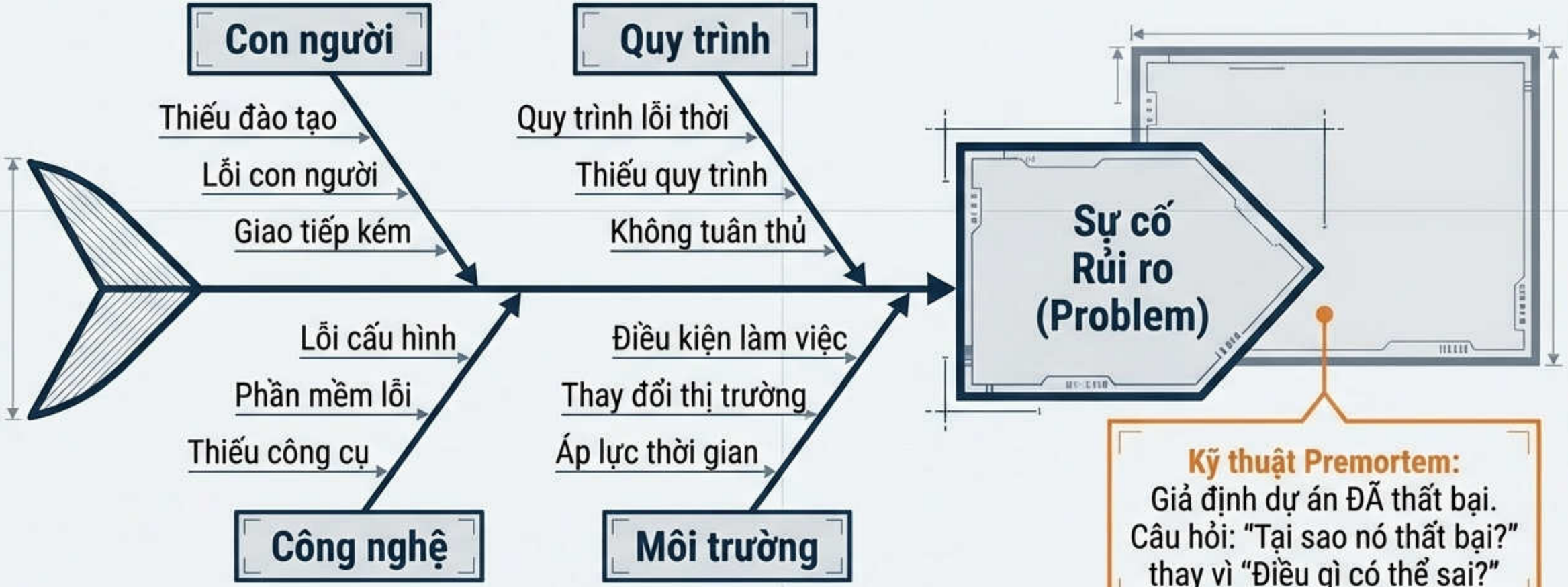
Penetration Testing

Hẹp nhưng Sâu

- Mô phỏng tấn công thực tế (Adversarial).
- Khai thác lỗ hổng để xem mức độ thiệt hại.
- Mục tiêu: Xác nhận tính khả thi của tấn công.

Phân tích Nguyên nhân Gốc rễ (Root Cause Analysis)

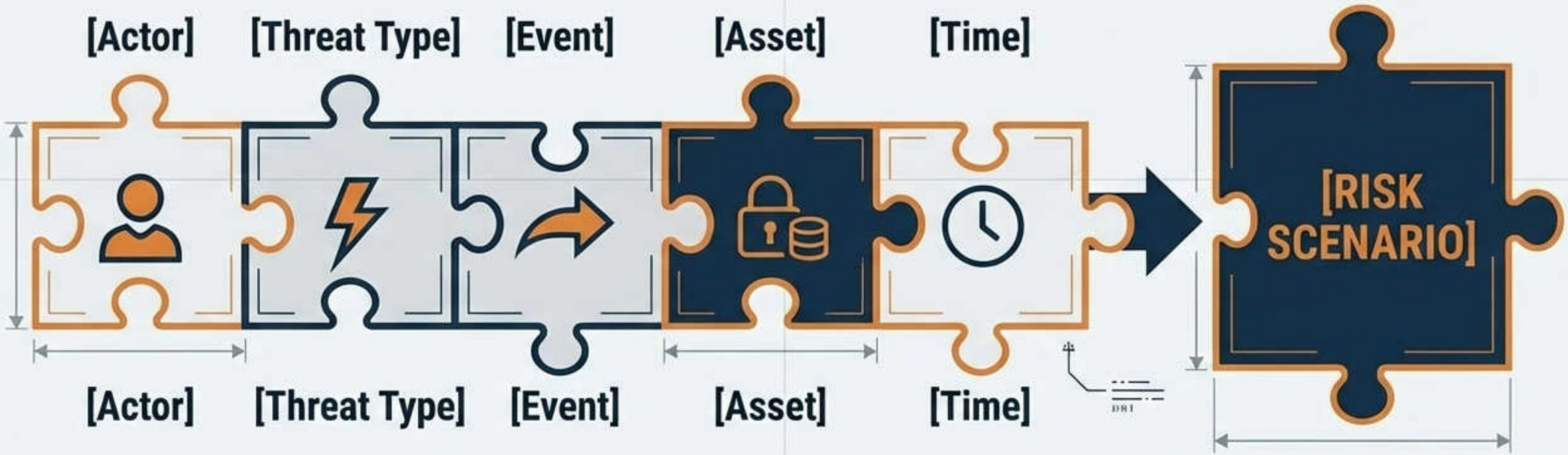
Không chỉ sửa lỗi (symptom), phải tìm nguyên nhân để ngăn chặn tái diễn.



Kỹ thuật Premortem:
Giả định dự án ĐÃ thất bại.
Câu hỏi: "Tại sao nó thất bại?"
thay vì "Điều gì có thể sai?"

Kịch bản Rủi ro (Risk Scenario) - Mảnh ghép hoàn chỉnh

Kịch bản giúp chuyển ngôn ngữ kỹ thuật sangngôn ngữ kinh doanh.



Ví dụ: Một nhân viên bất mãn (Actor) cố ý (Threat Type) sao chép dữ liệu (Event) từ CRM (Asset) trước khi nghỉ việc (Time).

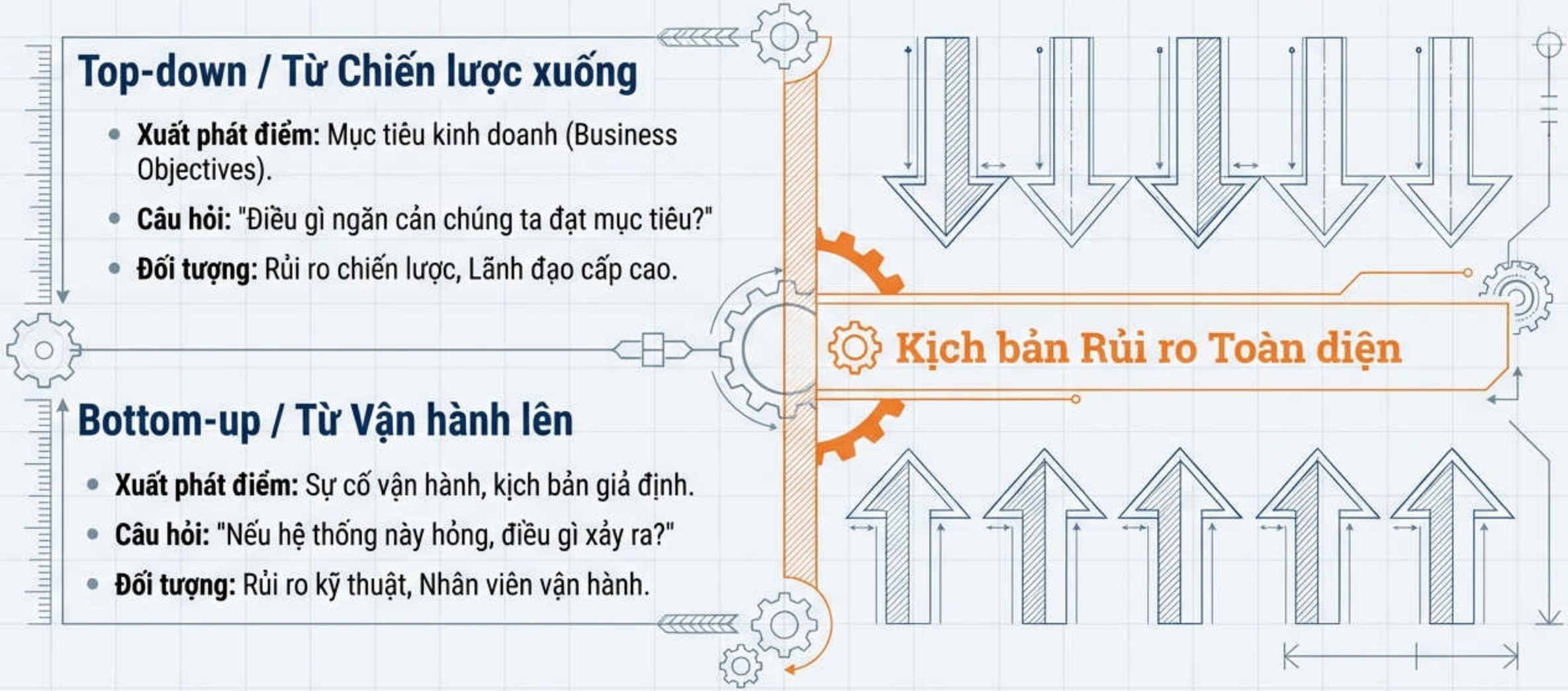
Phương pháp Phát triển Kịch bản

Top-down / Từ Chiến lược xuống

- **Xuất phát điểm:** Mục tiêu kinh doanh (Business Objectives).
- **Câu hỏi:** "Điều gì ngăn cản chúng ta đạt mục tiêu?"
- **Đối tượng:** Rủi ro chiến lược, Lãnh đạo cấp cao.

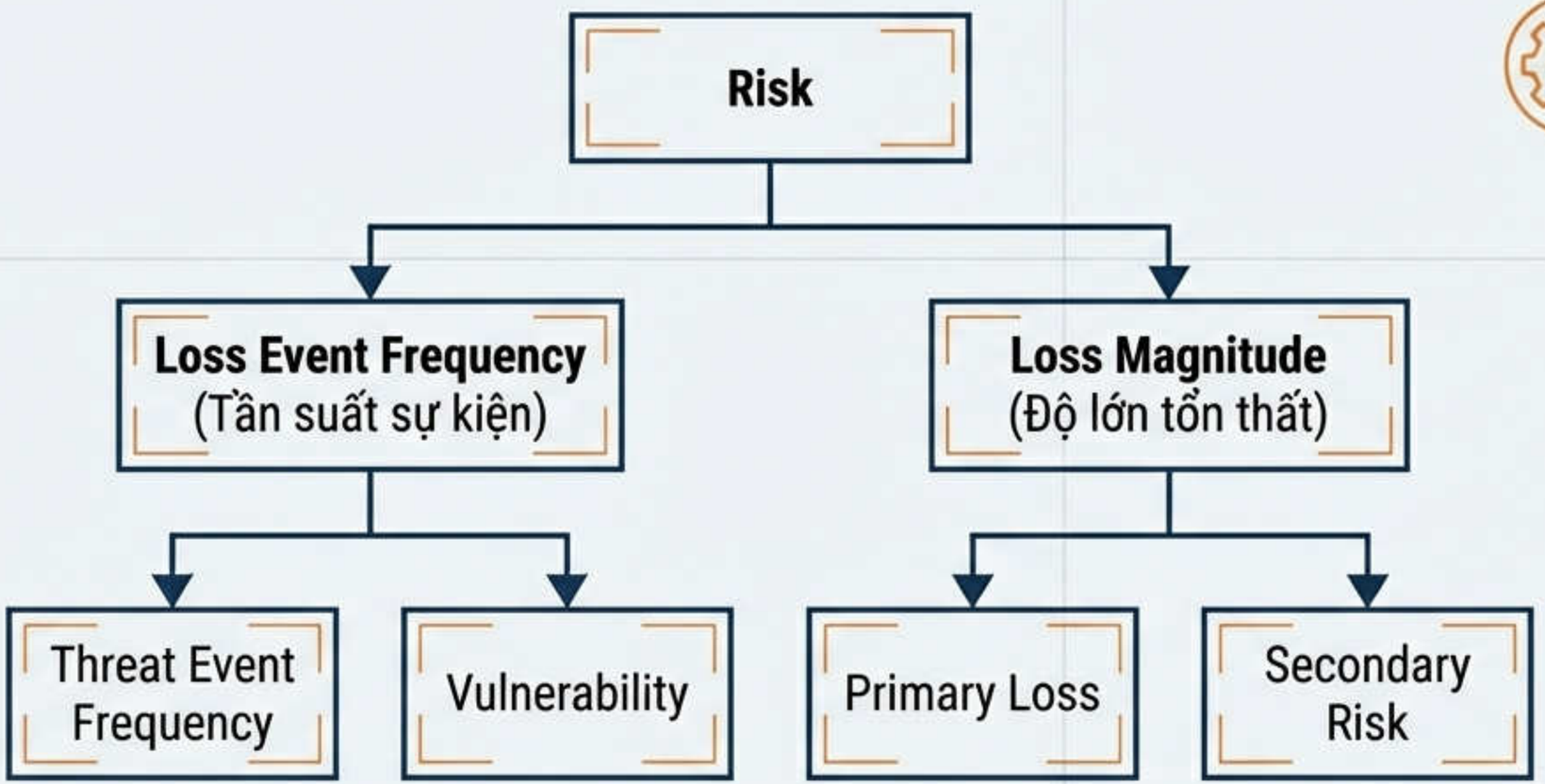
Bottom-up / Từ Vận hành lên

- **Xuất phát điểm:** Sự cố vận hành, kịch bản giả định.
- **Câu hỏi:** "Nếu hệ thống này hỏng, điều gì xảy ra?"
- **Đối tượng:** Rủi ro kỹ thuật, Nhân viên vận hành.



Công cụ Phân tích Kịch bản: FAIR và HARM

Chuyển đổi kịch bản thành định lượng



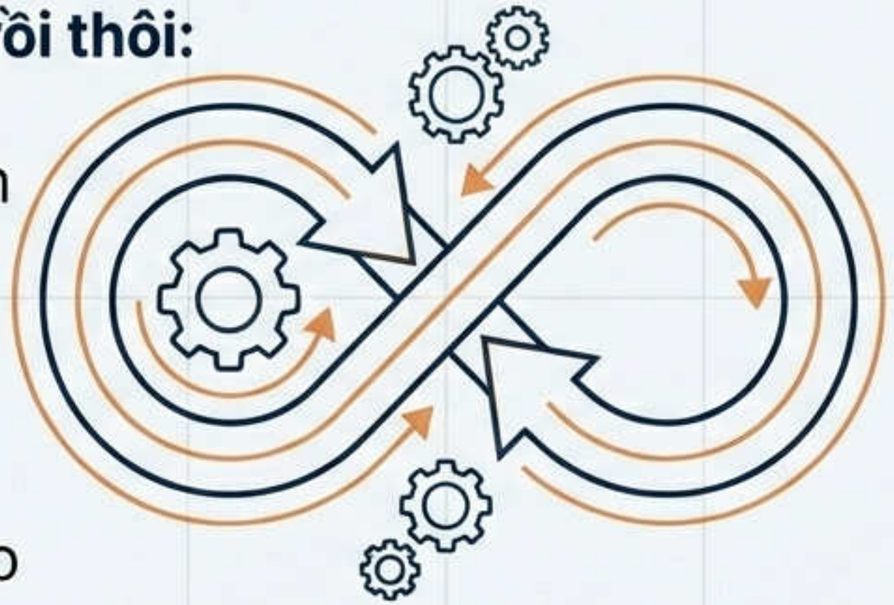
HARM Model: Mở rộng từ FAIR. Xem xét thêm "Độ trưởng thành của kiểm soát" (Control Maturity) và năng lực kẻ tấn công.

Những Cạm bẫy thường gặp (Common Pitfalls)

- **Nhầm lẫn Threat và Risk:** Chỉ liệt kê mối đe dọa mà quên tác động kinh doanh.
- **Bỏ qua Shadow IT:** Không thấy rủi ro từ công nghệ do nghiệp vụ tự triển khai.
- **Thiếu cập nhật (Stale Context):** Không cập nhật hồ sơ khi quy trình thay đổi.
- **Quá tải dữ liệu:** Nhiều chỉ số nhưng thiếu phân tích bối cảnh.
- **Chỉ tập trung kỹ thuật:** Bỏ qua yếu tố con người và quy trình.

Thông điệp cốt lõi: Nhận diện là Quy trình Liên tục

- **Không làm một lần rồi thôi:** Risk Identification là chu trình liên tục cần giám sát thay đổi.
- **Kết nối IT với Kinh doanh:** Risk Scenario là cầu nối ngôn ngữ chung.



- **Tư duy Phản biện:** Dùng Root Cause Analysis và Threat Modeling để tìm rủi ro ẩn.

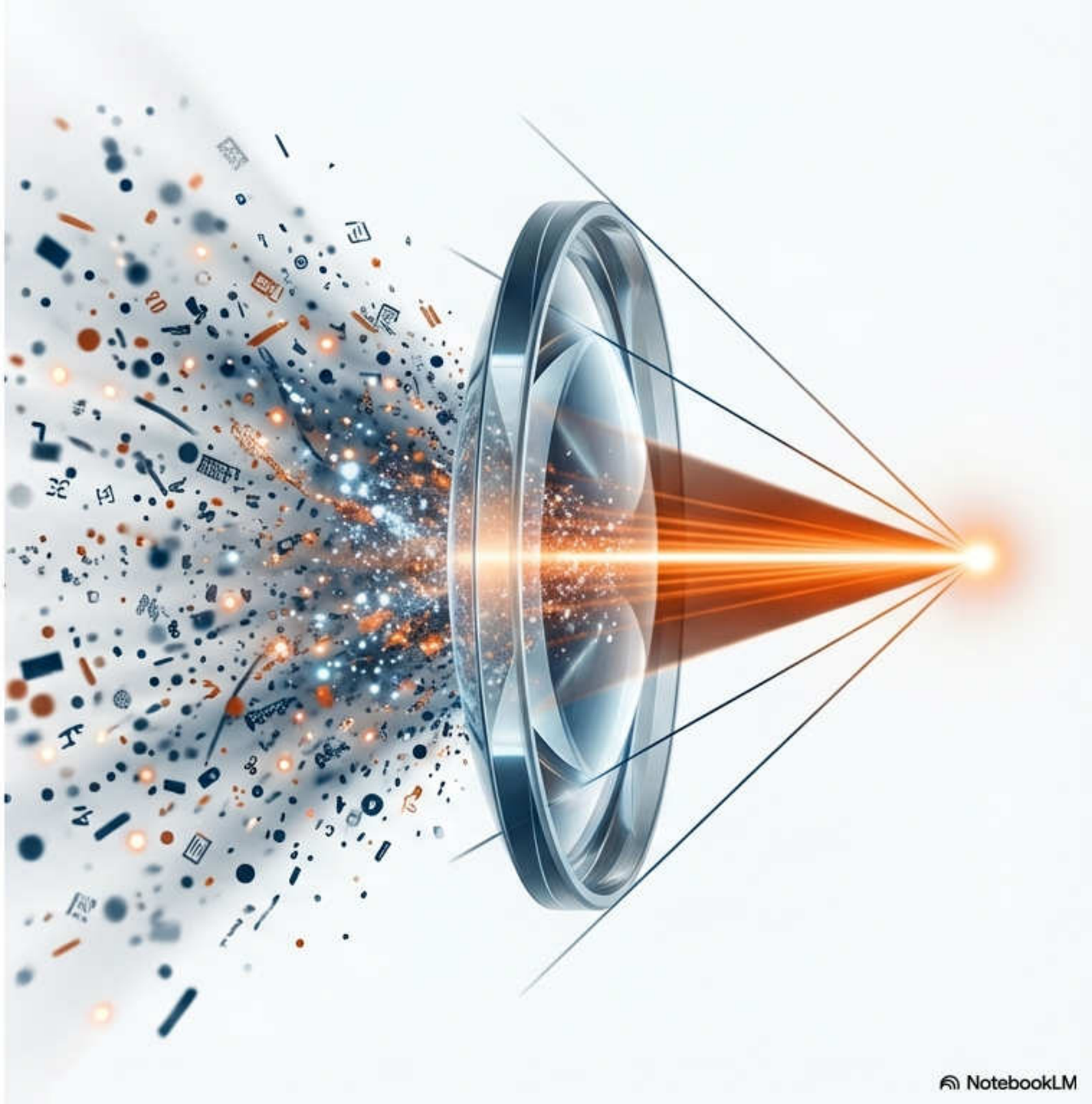
Tiếp theo: Part B - Risk Analysis

Phân tích Rủi ro CNTT

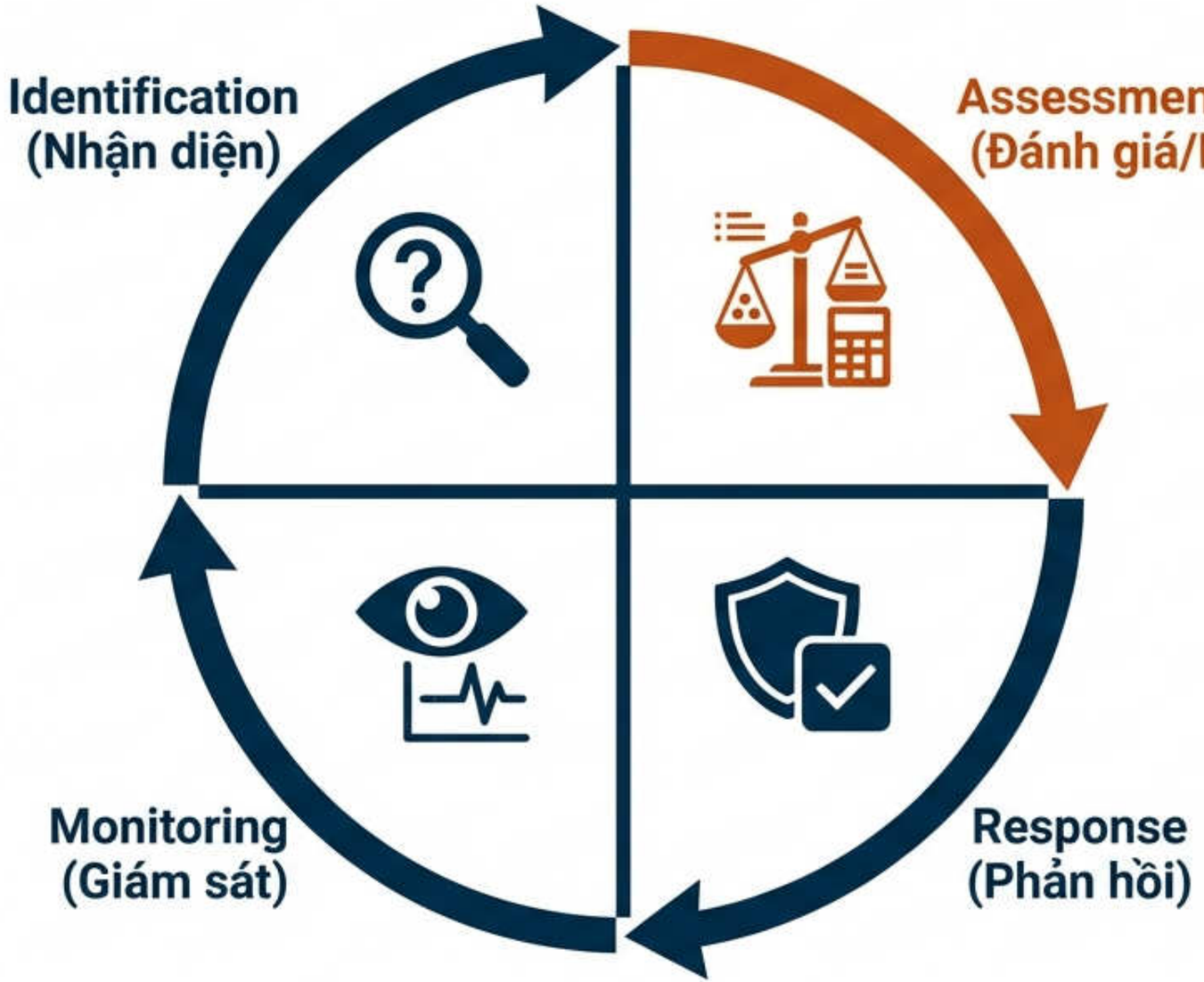
Từ Dữ liệu đến Quyết định

CRISC Official Review Manual, 8th Edition - Chapter 2, Part B

Based on ISACA® CRISC™ Curriculum



Vị trí của Phân tích trong Vòng đời Quản lý Rủi ro



Assessment/Analysis:

Giai đoạn trọng tâm. Đây là cầu nối xử lý dữ liệu để hiểu rõ khả năng xảy ra **(Likelihood)** và **tác động (Impact)**.

Key Insight: Phân tích **không phải là đích đến**, mà là **công cụ hỗ trợ ra quyết định**.

Khái niệm Đánh giá Rủi ro (Risk Assessment Concepts)

Risk Analysis (Phân tích) + **Risk Evaluation (Đánh giá)** = **Risk Assessment**

Risk Analysis (Phân tích)

Phân tách rủi ro để ước tính:
- Xác suất (Probability)
- Mức độ tổn thất (Loss Magnitude)

Risk Evaluation (Đánh giá)

So sánh kết quả phân tích với:
- Khẩu vị rủi ro (Risk Appetite)
- Ngưỡng chấp nhận rủi ro (Risk Tolerance)

Mục tiêu cốt lõi: Hiểu rõ sự phụ thuộc hệ thống, xác định kiểm soát hiện có, và ưu tiên hóa rủi ro.

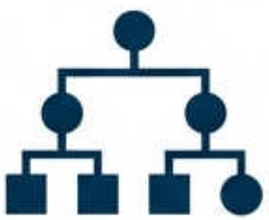
Các Kỹ thuật Đánh giá Rủi ro

Bow Tie Analysis: Liên kết nguyên nhân, sự kiện trung tâm và hậu quả.

Monte Carlo Analysis: Mô phỏng thống kê dự đoán kết quả định lượng

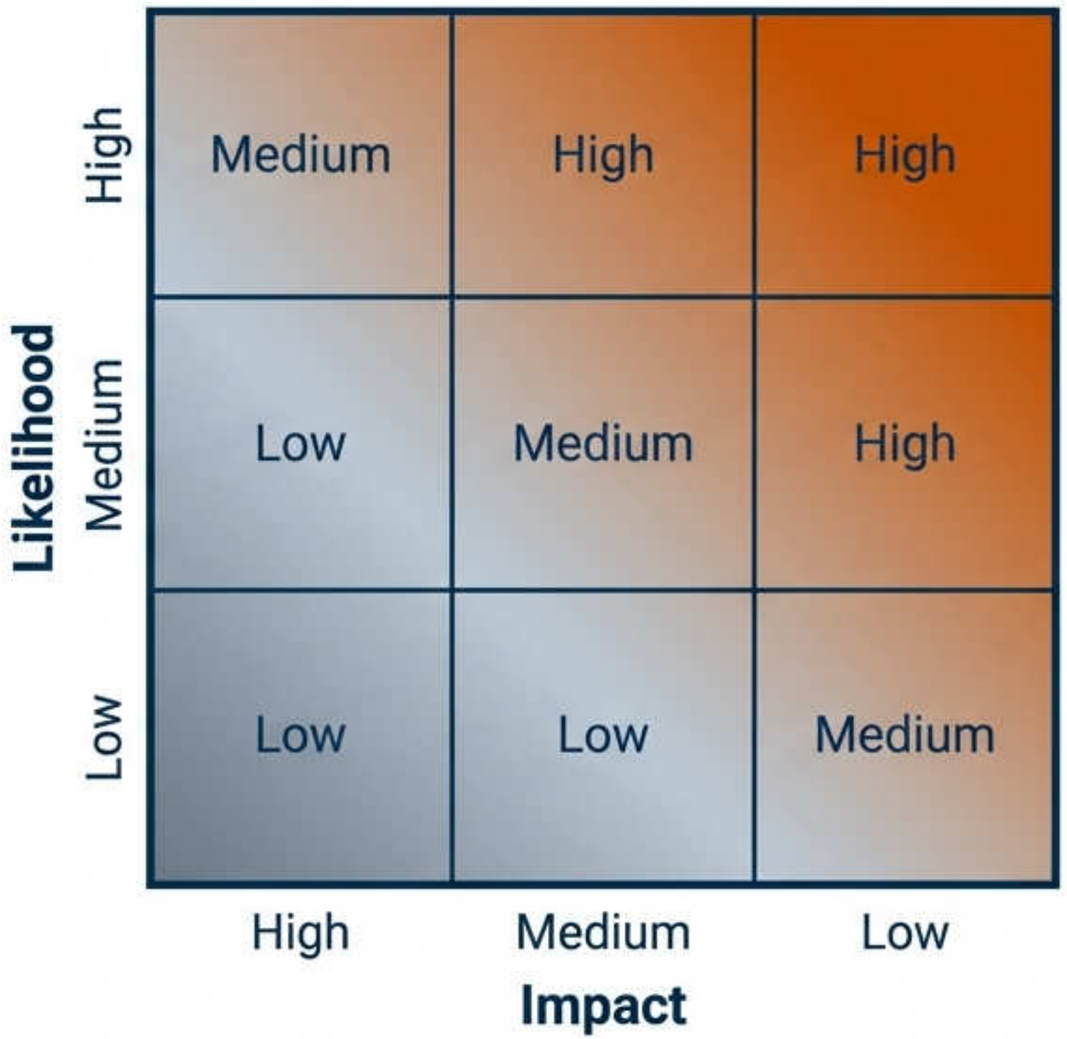
Delphi Method: Thu thập ý kiến chuyên gia ẩn danh để đạt đồng thuận.

Root Cause Analysis: Xác định nguyên nhân gốc rễ (Fault tree)



Decision Tree: Mô hình hóa các kết quả từ một sự kiện khởi đầu.

Phương pháp Phân tích Định tính (Qualitative Assessment)



Định nghĩa:
Sử dụng thang đo xếp hạng (Cao/Trung bình/Thấp) hoặc thang điểm (1-10) dựa trên ý kiến chuyên gia.

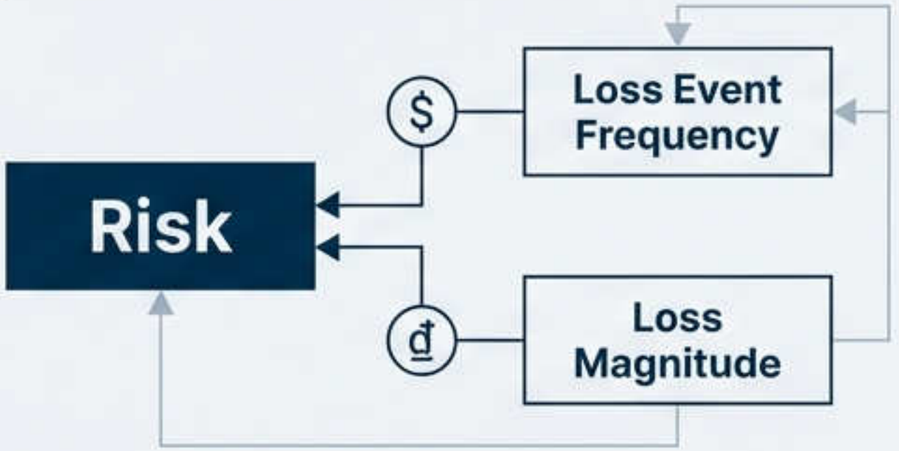
Cách tiếp cận:
- Dựa trên mối đe dọa (Kịch bản tấn công)
- Dựa trên tài sản (Giá trị và độ nhạy cảm CIA)

Ưu điểm:
Nhanh chóng, dễ hiểu, tốt cho ưu tiên ban đầu.

Nhược điểm: Chủ quan (Subjective), khó bảo vệ trước ban lãnh đạo, khó theo dõi xu hướng.

Phương pháp Phân tích Định lượng (Quantitative Assessment)

Định nghĩa: Sử dụng tính toán số học và xác suất thống kê để gán giá trị tiền tệ cho rủi ro.
Mô hình tiêu biểu: Factor Analysis of Information Risk (FAIR).



Ứng dụng:
- Tính toán ROI cho kiểm soát.
- So sánh chi phí rủi ro vs. chi phí phòng ngừa.

Thách thức:
Đòi hỏi dữ liệu lịch sử chất lượng cao, phức tạp và tốn kém.

So sánh & Phương pháp Bán định lượng

Định tính (Qualitative)

- Chủ quan
- Nhanh
- Dễ giao tiếp

Bán định lượng (Hybrid/Semiquantitative)

- Kết hợp thang đo định tính với giá trị số (ví dụ: 0-100).
- Mục tiêu: Tăng độ chi tiết mà không cần dữ liệu hoàn hảo.
- Lưu ý: Không nhầm lẫn với dữ liệu thực nghiệm.

Định lượng (Quantitative)

- Khách quan
- Chính xác
- Tốn kém dữ liệu

Phân tích Tác động Kinh doanh (BIA)

Mục đích: Xác định mức độ quan trọng của quy trình kinh doanh và hậu quả nếu gián đoạn.

Đầu ra chính:
- Xác định quy trình trọng yếu (**Critical processes**).
- Thiết lập RTO và RPO.

Vai trò: Nền tảng cho Chiến lược Duy trì Hoạt động Kinh doanh (**BCP**).

Phân biệt BIA và Đánh giá Rủi ro

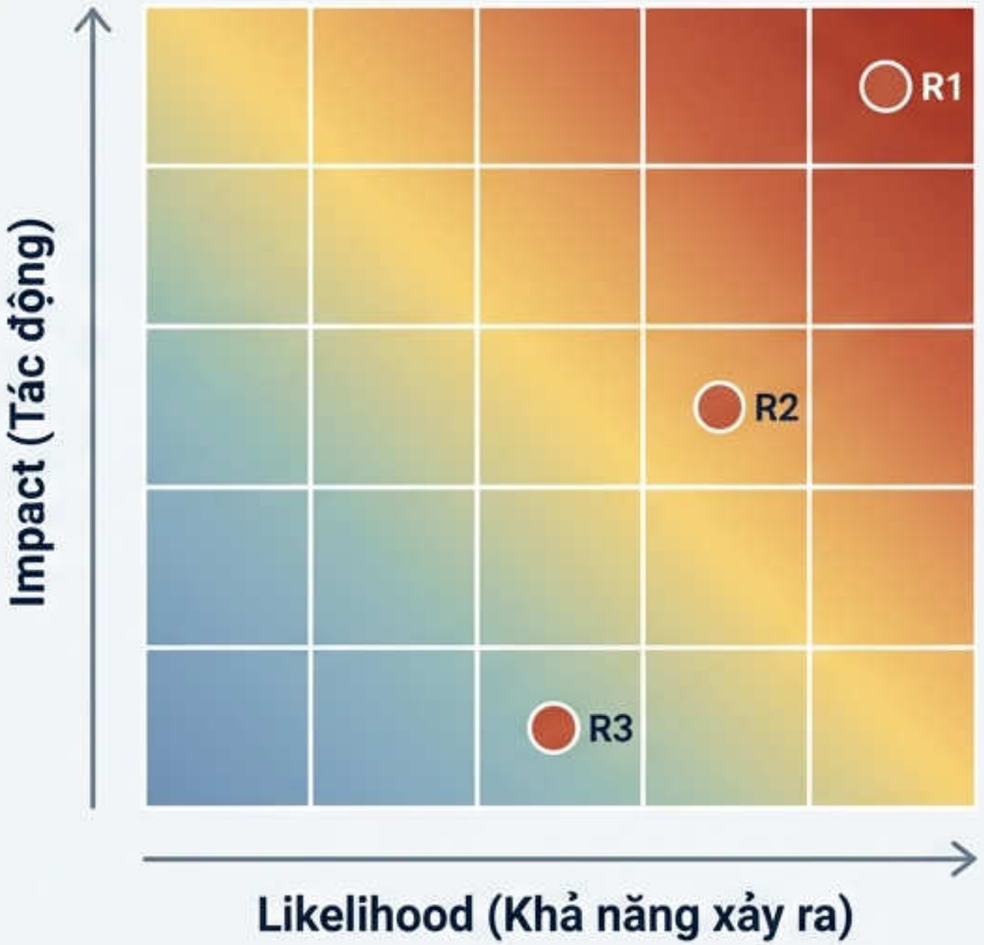
Risk Assessment (Đánh giá Rủi ro)

- Đầu vào: Mối đe dọa, Lỗ hổng.
- Trọng tâm: Xác suất (Likelihood) & Tác động (Impact).
- Mục tiêu: Giảm thiểu khả năng xảy ra.

Business Impact Analysis (BIA)

- Đầu vào: Quy trình kinh doanh, Tài nguyên.
- Trọng tâm: Tính cấp thiết (Urgency) & Thời gian phục hồi.
- Mục tiêu: Ưu tiên phục hồi dịch vụ.

Bản đồ Rủi ro (Heat Maps)



Trực quan hóa: Biểu diễn mối quan hệ Tần suất - Tác động.

Vùng Xanh: Chấp nhận, giám sát.

Vùng Đỏ: Hành động ngay lập tức.

Mục đích: Giúp Ban lãnh đạo nhận diện điểm nóng (hotspots).

Sổ đăng ký Rủi ro (Risk Register)

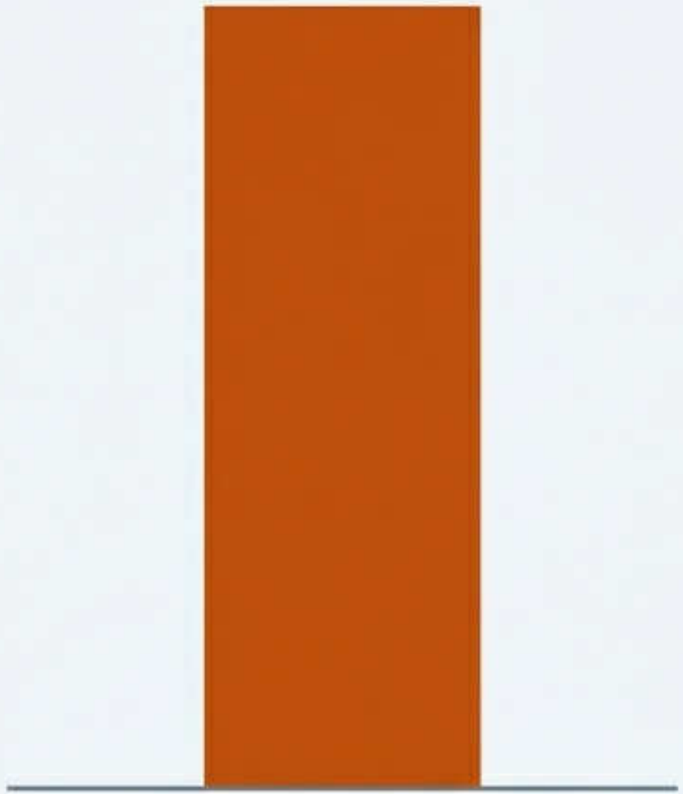
ID	Risk Scenario	Risk Owner	Risk Score	Response
R01	Server Failure	IT Ops	**High**	Mitigate
R02	Data Leak	CISO	**Critical**	Avoid
R03	Power Outage	Facility	Low	Accept

Định nghĩa: Kho lưu trữ trung tâm của tất cả rủi ro.

Thành phần bắt buộc:
- Chủ sở hữu rủi ro (Risk Owner)
- Mô tả kịch bản
- Điểm số rủi ro (Likelihood x Impact)
- Phản ứng đề xuất

Tính chất: Tài liệu sống (**Living document**), cập nhật liên tục.

Rủi ro Tiềm tàng (Inherent Risk)



Gross Risk (Rủi ro thô)

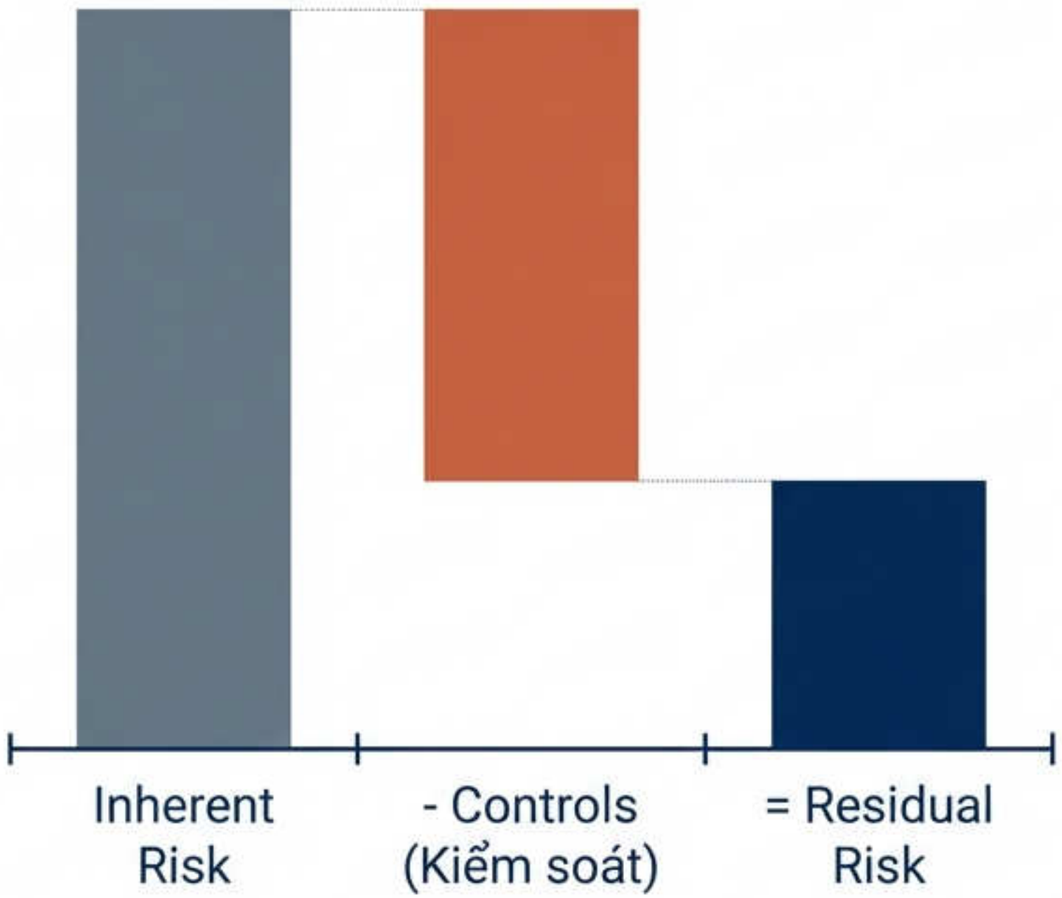
Định nghĩa: Mức độ rủi ro khi chưa có bất kỳ biện pháp kiểm soát nào.

Bản chất: Phơi nhiễm thô (**Gross risk**) của hoạt động kinh doanh.

Ví dụ: Truyền tải dữ liệu qua internet mà không có mã hóa.

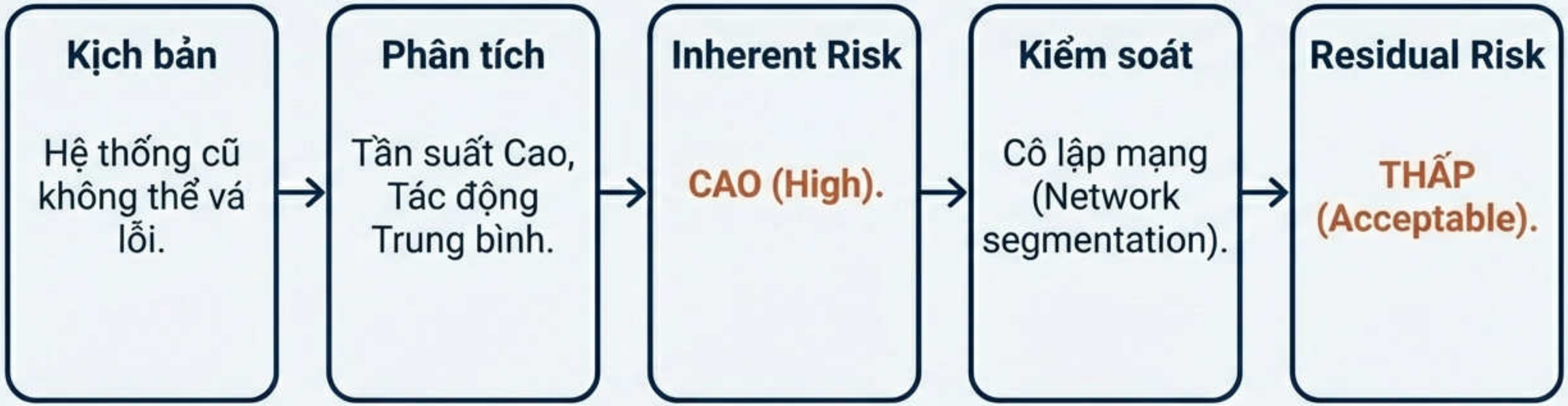
Ý nghĩa: Giúp quyết định xem có nên tham gia vào hoạt động đó ngay từ đầu hay không.

Rủi ro Còn lại (Residual) & Hiện tại (Current)



- **Công thức: Inherent Risk - Controls = Residual Risk.**
- **Quyết định**: Nếu **Residual Risk ≤ Risk Appetite** → Chấp nhận.
- **Rủi ro Hiện tại (Current Risk):** Rủi ro tại thời điểm đánh giá, tính đến kiểm soát hiện có và kế hoạch chưa hoàn thành.
- **Lưu ý:** Không thể loại bỏ rủi ro về 0.

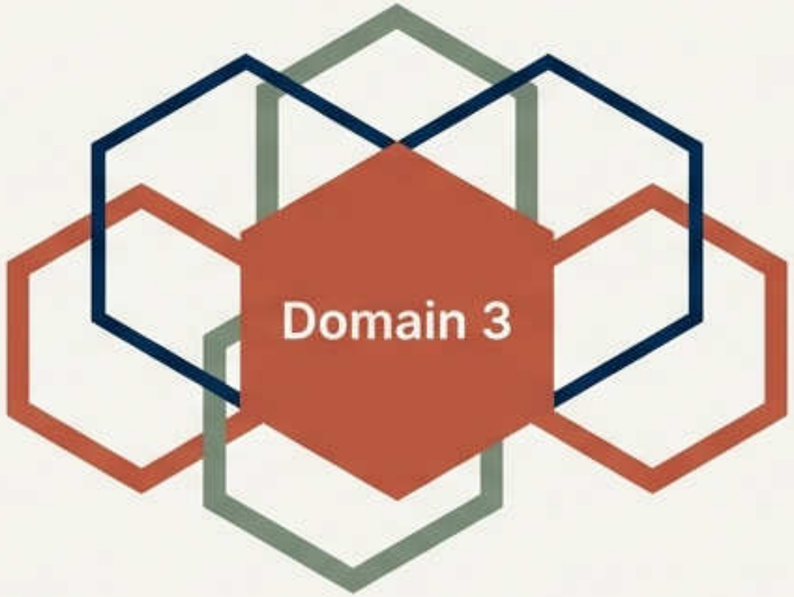
Case Study: Quy trình Phân tích Thực tế



Quyết định cuối cùng: Chấp nhận rủi ro còn lại và tiếp tục giám sát.

Điểm chính cần ghi nhớ (Key Takeaways)

- **Dữ liệu & Quyết định:** Phân tích phải hỗ trợ ra quyết định kinh doanh, không chỉ là bài tập kỹ thuật.
- **Chất lượng Dữ liệu:** 'Rác vào, rác ra" (GIGO). Kết quả phụ thuộc vào đầu vào.
- **Phân biệt Rủi ro:** Hiểu rõ Inherent vs. Residual để đánh giá hiệu quả kiểm soát.
- **Liên kết BIA:** Sử dụng BIA để xác định tính cấp thiết phục hồi.



CRISC Domain 3 - Part A: Chiến lược & Thực thi Phản ứng Rủi ro

Biến Đánh giá thành Hành động: Các phương án, Quyền sở hữu và Quản lý Ngoại lệ

Based on ISACA CRISC Review Manual, 8th Edition - Chapter 3

Từ Đánh giá đến Hành động: Cầu nối Phản ứng

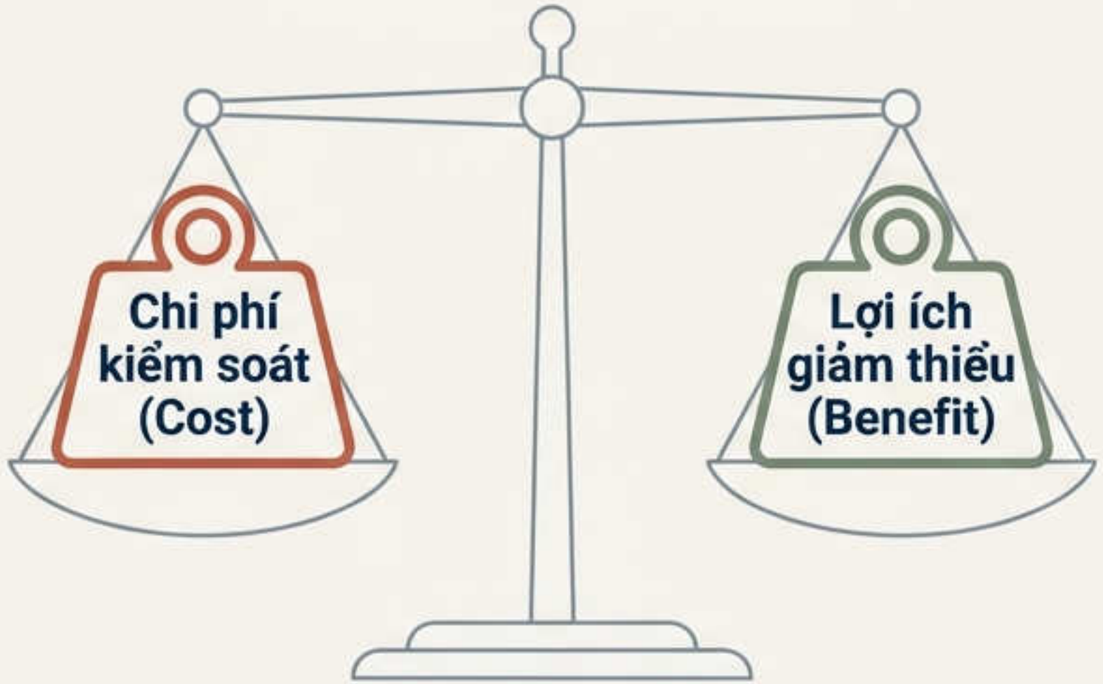
Context

Bối cảnh: Đầu ra của quy trình Đánh giá Rủi ro là danh sách các rủi ro đã được xếp hạng. Bước tiếp theo là xác định phản ứng phù hợp.

Mục tiêu cốt lõi: Đưa rủi ro hiện tại về mức phù hợp với **Khẩu vị rủi ro (Risk Appetite)** và **Dung sai rủi ro (Risk Tolerance)** của doanh nghiệp.

Lưu ý: Rủi ro không bao giờ biến mất hoàn toàn. Mục tiêu không phải là loại bỏ rủi ro bằng mọi giá, mà là quản lý nó một cách hiệu quả về chi phí.

Nguyên tắc Chiến lược của Phản ứng Rủi ro



Chi phí (Cost)

Chi phí kiểm soát không được vượt quá giá trị của tài sản hoặc tổn thất dự kiến.

Hiệu suất (Performance)

Kiểm soát không được làm chậm quy trình kinh doanh quá mức cho phép.

Tuân thủ (Conformance)

Phản ứng phải đáp ứng đầy đủ các yêu cầu luật pháp và quy định.

Hiệu quả đầu tư (ROI) trong bảo mật là việc giảm thiểu tổn thất tiềm tàng so với chi phí bỏ ra.

4 Phương án Phản ứng Chiến lược

1. Chấp nhận (Risk Acceptance)

Nhận thức rủi ro và quyết định không hành động thêm (chỉ giám sát). Thường dùng khi chi phí xử lý cao hơn tổn thất.

2. Giảm thiểu (Risk Mitigation)

Thực hiện các biện pháp kiểm soát để giảm khả năng xảy ra hoặc tác động. Đây là phương án phổ biến nhất.

3. Chuyển giao (Risk Transfer)

Chuyển gánh nặng tài chính sang bên thứ ba (bảo hiểm, đối tác). Lưu ý: Không chuyển giao được trách nhiệm giải trình.

4. Tránh né (Risk Avoidance)

Ngừng hoàn toàn hoạt động gây ra rủi ro. Dùng khi không có phương án nào khác đưa rủi ro về mức chấp nhận được.

Đi sâu vào: Chấp nhận Rủi ro (Risk Acceptance)

Định nghĩa & Điều kiện

- Một quyết định có ý thức của ban lãnh đạo để giữ nguyên mức rủi ro hiện tại.
- Rủi ro phải nằm trong **Khẩu vị rủi ro (Risk Appetite)**.
- Chi phí xử lý vượt quá lợi ích mang lại.
- Phải có Risk Owner ký duyệt chính thức.

Tự bảo hiểm (Self-insurance): Doanh nghiệp dành riêng ngân sách để chi trả tổn thất thay vì mua bảo hiểm.

Chấp nhận (Acceptance) vs. Phớt lờ (Ignorance)

Chấp nhận		Được ghi lại, được giám sát, có kế hoạch.
Phớt lờ		Không biết rủi ro tồn tại, không có sự chuẩn bị.

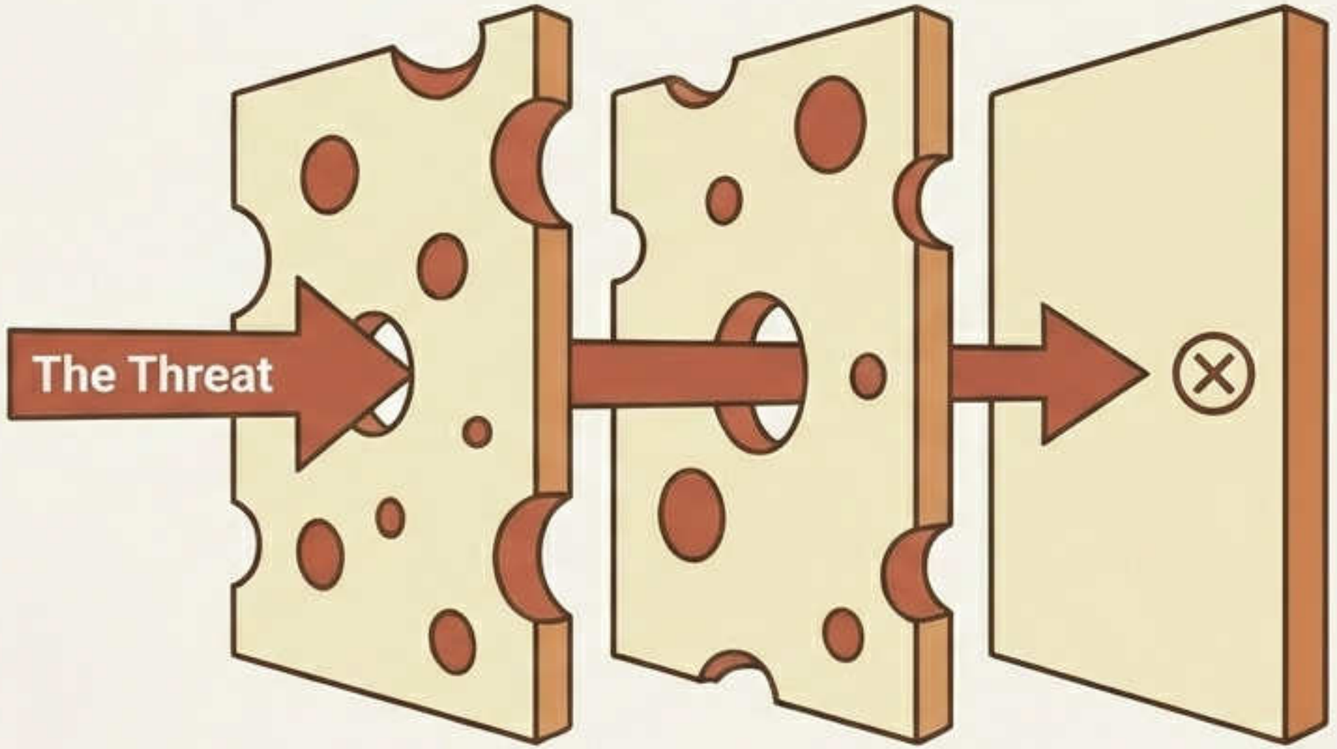
Cảnh báo: Chấp nhận rủi ro không phải là hành động một lần. Cần xem xét lại định kỳ.

Đi sâu vào: Giảm thiểu Rủi ro (Risk Mitigation)

Mục tiêu: Giảm **Rủi ro Tiềm ẩn (Inherent Risk)** xuống mức **Rủi ro Còn lại (Residual Risk)** thông qua các biện pháp kiểm soát.

Chiến thuật

- Phòng ngừa (Preventive): Ngăn chặn sự cố.
- Phát hiện (Detective): Nhận biết sớm.
- Khắc phục (Corrective): Giảm thiểu thiệt hại.



1. Kỹ thuật (Technical): Firewall, Encryption

2. Hành chính (Administrative): Policy, Training

3. Vật lý (Physical): Locks, CCTV

Đi sâu vào: Chuyển giao & Tránh né

Chuyển giao (Transfer/Sharing)

- **Cơ chế:** Bảo hiểm (Insurance) hoặc Thuê ngoài (Outsourcing).
- **Quan trọng:** Bạn có thể chuyển giao rủi ro tài chính, nhưng **KHÔNG** thể chuyển giao trách nhiệm giải trình (accountability) hoặc uy tín.

Tránh né (Avoidance)

- **Cơ chế:** Loại bỏ hoàn toàn nguyên nhân gây rủi ro (ngừng hoạt động, rút khỏi thị trường).
- **Khi nào dùng?** Khi không có kiểm soát nào khả thi hoặc chi phí quá cao.
- **Cái giá:** Mất đi cơ hội kinh doanh (Opportunity Cost).

Khung Ra Quyết định (Decision Framework)

Làm thế nào để chọn phương án đúng? Quyết định dựa trên dữ liệu, không phải cảm tính.

$$\textbf{Value of Control} = (\textbf{ALE}_{\textbf{before}} - \textbf{ALE}_{\textbf{after}}) - \textbf{Cost of Control}$$

Annualized Loss Expectancy
(Tổn thất dự kiến hàng năm)

Phân tích Chi phí - Lợi ích (CBA)

So sánh chi phí triển khai với mức độ tổn thất giảm được.

Nếu Chi phí Kiểm soát > Giá trị Tài sản, phương án tốt nhất là Chấp nhận.

Hồ sơ Kinh doanh (Business Case)

Tài liệu đề xuất phương án, bao gồm phân tích rủi ro, chi phí, lợi ích và ROI để ban lãnh đạo phê duyệt.

Quyền sở hữu & Trách nhiệm Giải trình

Chủ sở hữu Rủi ro (Risk Owner)	Chủ sở hữu Kiểm soát (Control Owner)
	
Là ai? Lãnh đạo doanh nghiệp, trưởng bộ phận nghiệp vụ (Business Manager). **Trách nhiệm:** • Có quyền ra quyết định chấp nhận rủi ro. • Chịu trách nhiệm giải trình cuối cùng. • Phê duyệt ngân sách.	**Là ai?** Trưởng phòng IT, quản lý bảo mật, nhân viên vận hành. **Trách nhiệm:** • Thiết kế và triển khai kiểm soát. • Đảm bảo kiểm soát hoạt động hiệu quả. • Báo cáo cho Risk Owner.

Risk Practitioner chỉ tư vấn, **KHÔNG** phải là người ra quyết định chấp nhận rủi ro.

Định nghĩa Vai trò Quản trị

- Thiết lập "Tone at the Top".
- Xác định Khẩu vị rủi ro (Risk Appetite).
- Chịu trách nhiệm (Accountable) cuối cùng.

- Xác định và đánh giá rủi ro.
- Tư vấn các phương án phản ứng.
- Giám sát và báo cáo.
- Giám sát và báo cáo.
- Đảm bảo quyết định phù hợp mục tiêu kinh doanh.

Quản lý Rủi ro Bên thứ ba & Chuỗi cung ứng

Nguyên tắc: Thuê ngoài dịch vụ (Outsourcing) không có nghĩa là thuê ngoài trách nhiệm.

Thẩm định (Due Diligence)

Đánh giá năng lực bảo mật đối tác trước khi ký hợp đồng.

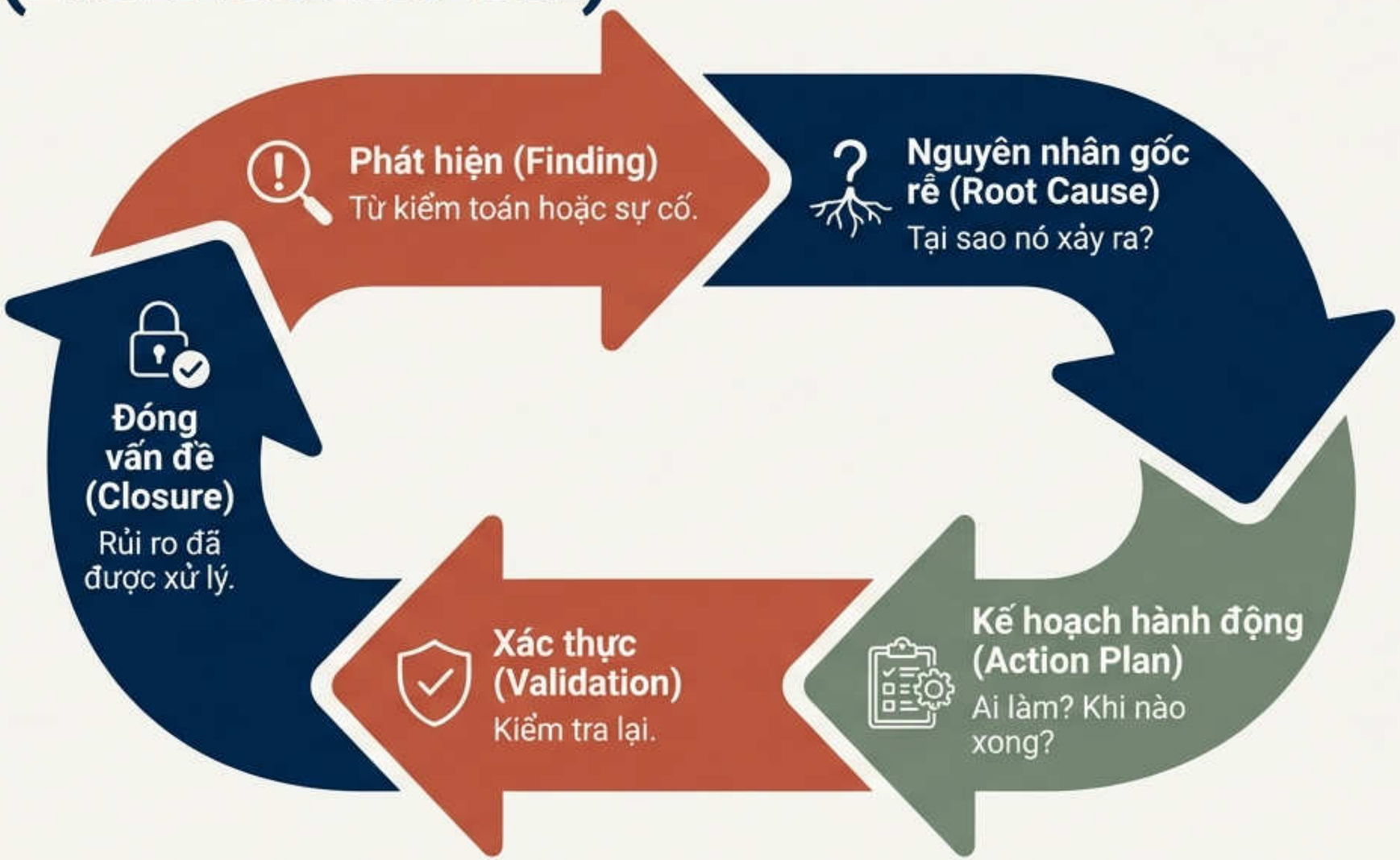
Hợp đồng (Contracts/SLAs)

Quy định rõ yêu cầu bảo mật và "Right to Audit" (Quyền kiểm toán).

Giám sát (Monitoring)

Đánh giá định kỳ hiệu suất và tuân thủ của nhà cung cấp.

Quản lý Vấn đề & Phát hiện (Remediation)



Mục tiêu là giải quyết triệt để nguyên nhân, không chỉ chữa trị triệu chứng.

Quản lý Ngoại lệ (Exception Management)

Quy trình chính thức cho phép tạm thời không tuân thủ chính sách vì lý do nghiệp vụ.

Permit

Phê duyệt (Approval):
Bởi Risk Owner hoặc cấp quản lý.

Có thời hạn (Time-bound):
Ngoại lệ phải có ngày hết hạn.

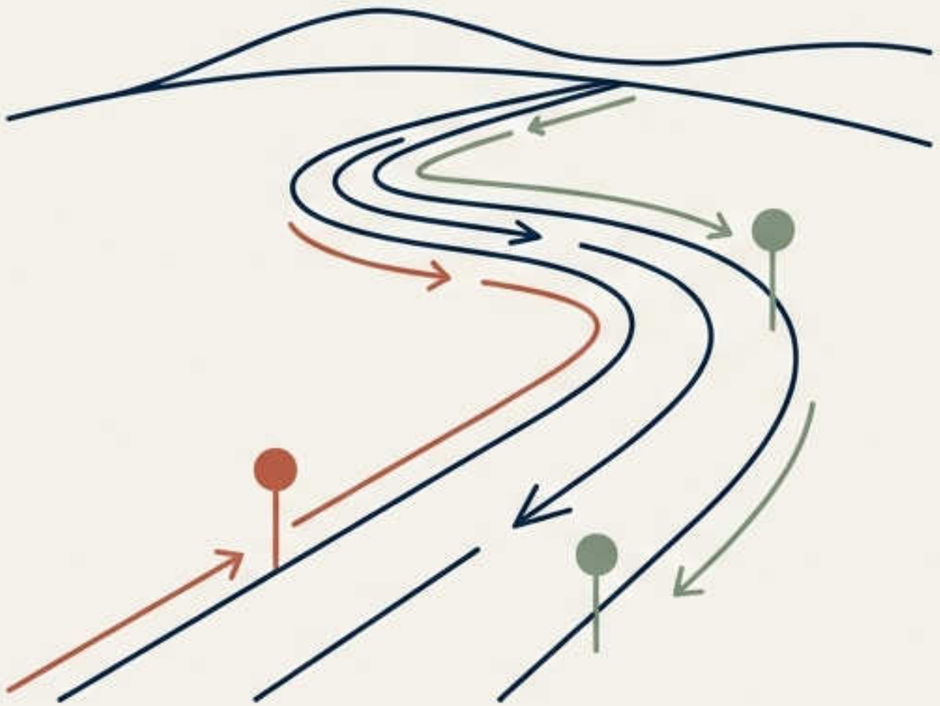
Kiểm soát bù đắp (Compensating Controls):
Biện pháp giảm thiểu rủi ro bổ sung.

Rủi ro: Nếu không quản lý tốt, ngoại lệ sẽ tích tụ thành "nợ kỹ thuật".

Tóm tắt: Danh mục Kiểm tra Phản ứng Rủi ro

- [x] Đã liên kết phản ứng rủi ro với mục tiêu kinh doanh và khẩu vị rủi ro chưa?
- [x] Đã thực hiện phân tích chi phí – lợi ích (CBA) cho các biện pháp kiểm soát chưa?
- [x] Đã xác định rõ Chủ sở hữu Rủi ro (người ra quyết định) và Chủ sở hữu Kiểm soát (người thực hiện) chưa?
- [x] Rủi ro còn lại (Residual Risk) có nằm trong ngưỡng chấp nhận không?
- [x] Có quy trình chính thức để quản lý nhà cung cấp và các ngoại lệ chính sách không?

Kết luận: Hướng tới Sự Bền vững



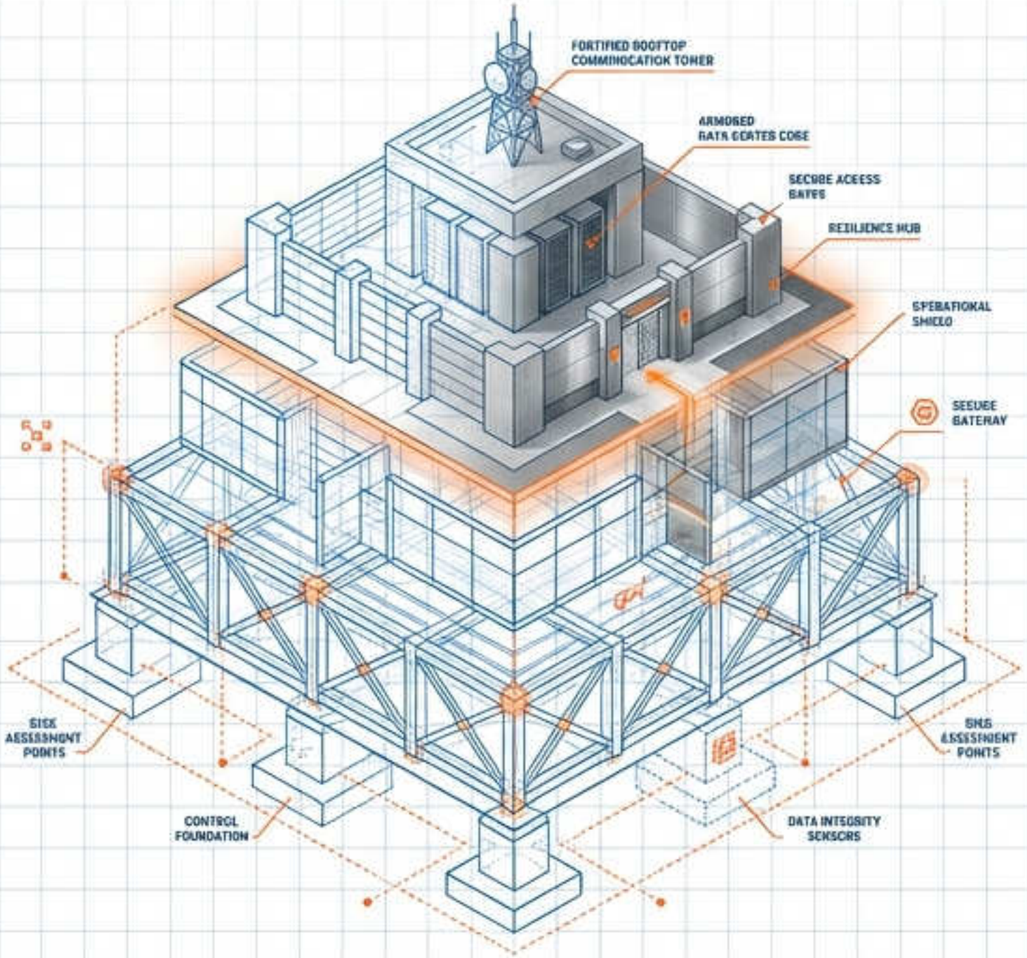
Quản lý rủi ro không phải là đích đến, mà là một hành trình liên tục.

Mục tiêu cuối cùng: Không chỉ là tuân thủ, mà là xây dựng một doanh nghiệp có khả năng chống chịu (Resilient Enterprise).

End of Chapter 3, Part A. Next: Part B - Control Design and Implementation.

Thiết kế và Triển khai Kiểm soát Kỹ thuật cho sự Kiên cường

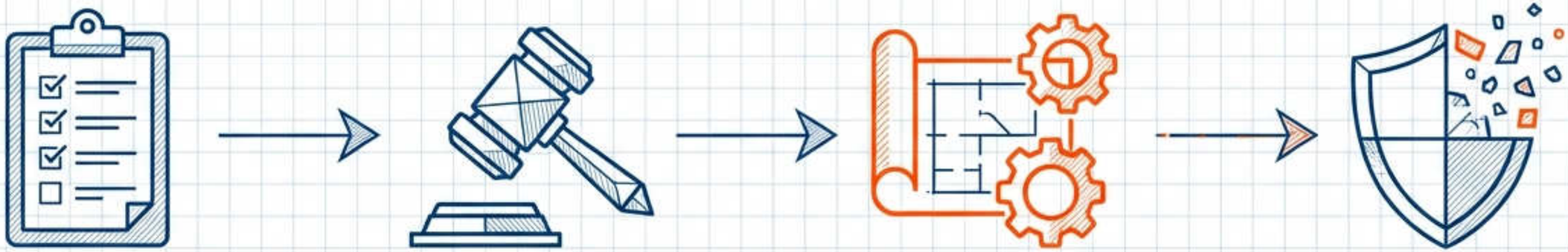
Chương 3 - Phần B: CRISC® Review Manual, 8th Edition



Từ Lý thuyết Rủi ro đến Thực tế Vận hành

PROJECT: CRISC RESILIENCE ARCHITECTURE

Vai trò của Kiểm soát trong Quản lý Rủi ro



Đánh giá Rủi ro

Quyết định Ứng phó

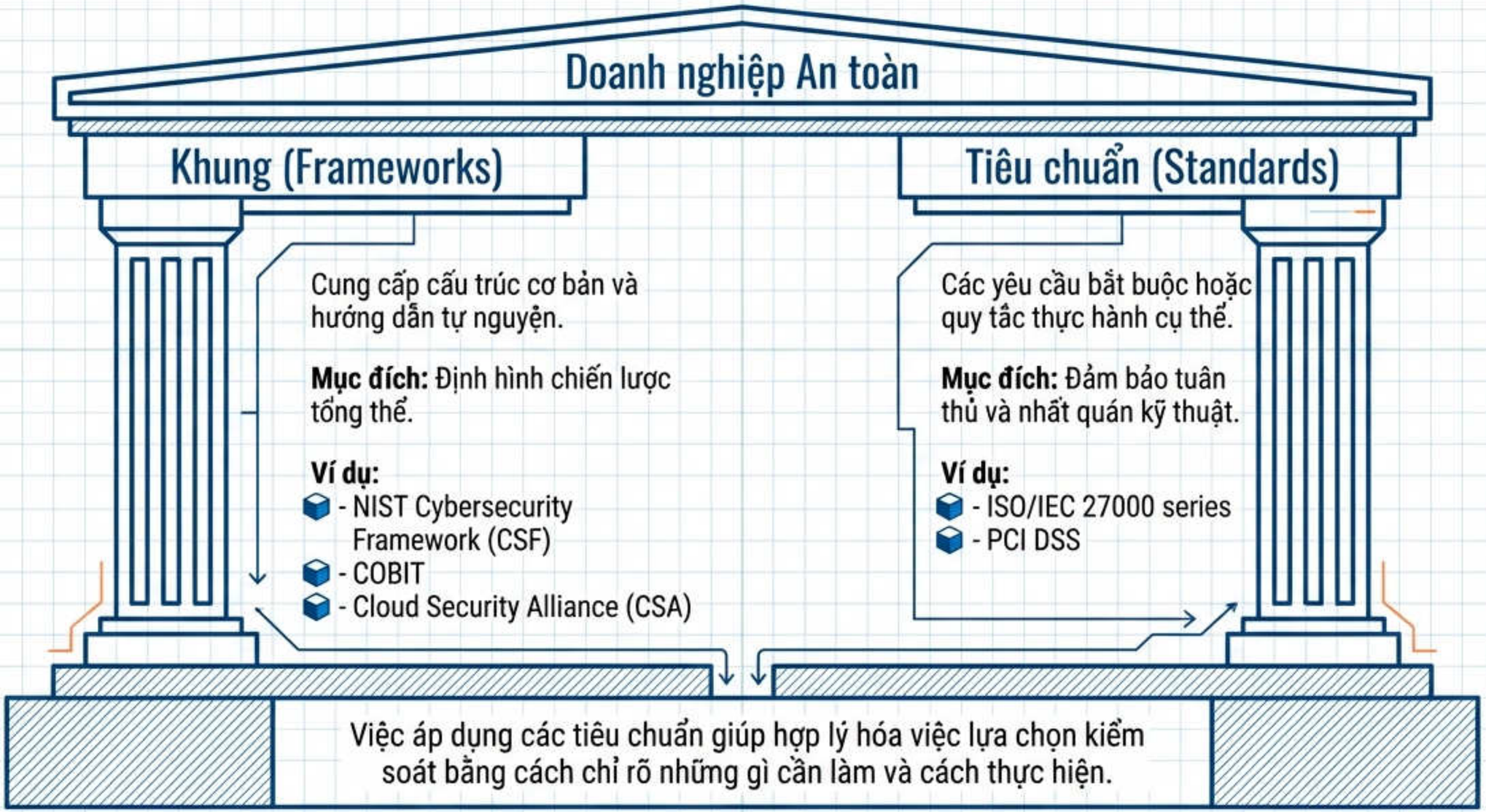
Thiết kế & Triển khai Kiểm soát

Giảm thiểu Rủi ro Còn lại

Key Insight: Kiểm soát là cầu nối giữa các quyết định "Ứng phó Rủi ro" và thực tế vận hành. Nếu không có kiểm soát hiệu quả, các quyết định quản lý rủi ro chỉ là lý thuyết.

Hiệu quả = Hoạt động như dự định + Quản lý được rủi ro mục tiêu.

Quy chuẩn và Khung kiểm soát: Nền móng của Thiết kế



Phân loại Kiểm soát theo Thời gian

Trước sự cố

Sự cố (Incident)

Sau sự cố

Kiểm soát Răn đe (Deterrent)

Cảnh báo, làm nản lòng. (VD: Biển báo, chính sách).

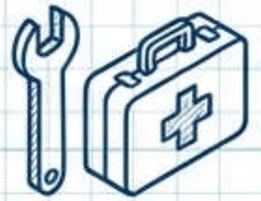
Kiểm soát Phòng ngừa (Preventive)

Ngăn chặn hành vi. (VD: Tường lửa, mã hóa).

Trong sự cố

Kiểm soát Phát hiện (Detective)

Cảnh báo vi phạm. (VD: IDS, logs).



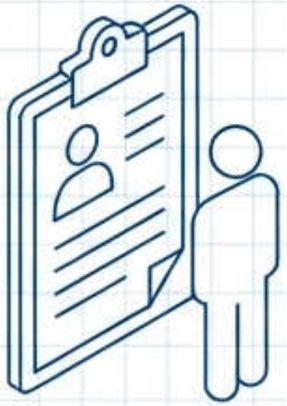
Kiểm soát Khắc phục (Corrective)

Sửa chữa, khôi phục. (VD: Backups, vá lỗi).

Kiểm soát Bù đắp (Compensating Controls): Được sử dụng khi các kiểm soát chính không thể thực hiện được (VD: Giám sát con người thay cho hệ thống).

Ba Phương pháp Thực thi Kiểm soát

Hành chính / Quản lý



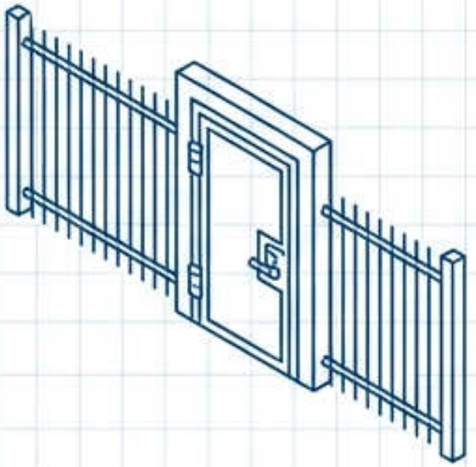
- Dựa vào con người và quy trình.
- Phụ thuộc vào sự phán đoán.
- Bao gồm: Chính sách, đào tạo, quy trình thay đổi.

Thiếu kiểm soát hành chính (như đào tạo) có thể vô hiệu hóa kiểm soát kỹ thuật.

Kỹ thuật / Logic

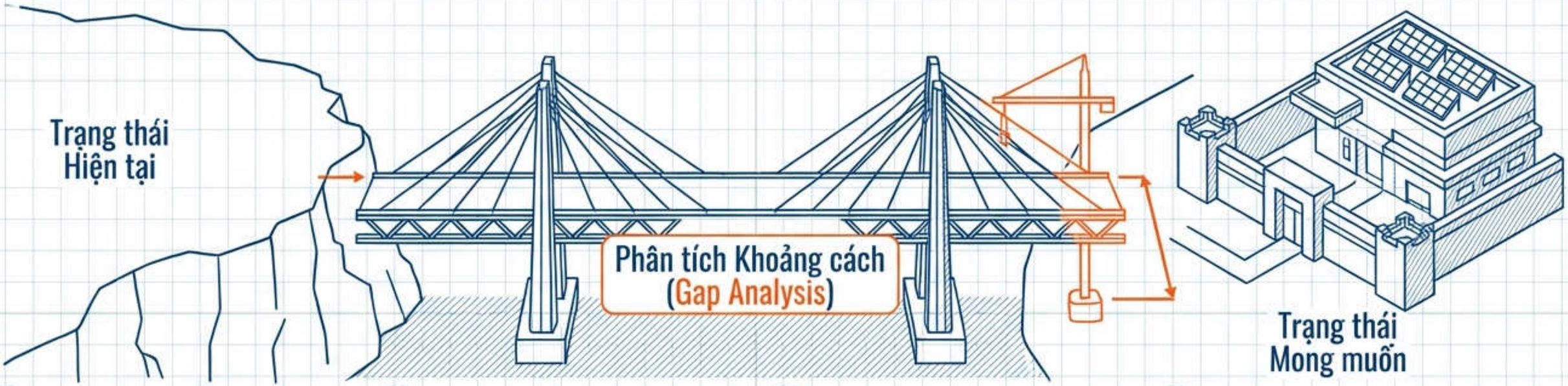
- Thực hiện qua công nghệ.
- Cần cấu hình và bảo trì.
- Bao gồm: Tường lửa, mã hóa, Antivirus.

Vật lý



- Hạn chế tiếp cận thế giới thực.
- Bảo vệ con người và phần cứng.
- Bao gồm: Khóa cửa, hàng rào, Camera CCTV.

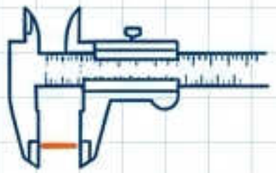
Thiết kế và Lựa chọn: Phân tích Khoảng cách



1 Đánh giá Hiện trạng

Hiểu rõ kiểm soát hiện có qua audit, logs.

2 Xác định Khoảng cách



So sánh hiện trạng với mức rủi ro chấp nhận được.

3 Lựa chọn Kiểm soát

Quyết định dùng safeguards hay countermeasures.

4 Củng cố Hệ thống (Hardening)

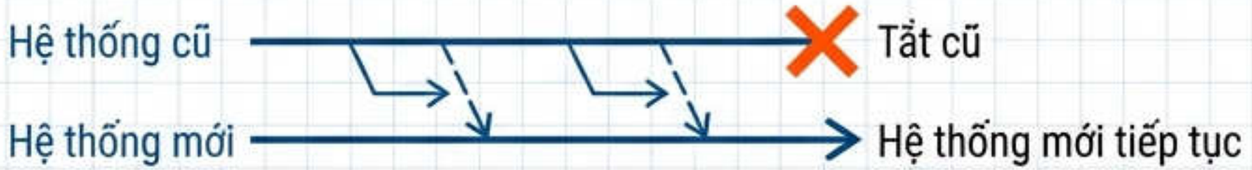
Tắt dịch vụ không cần thiết, giảm bề mặt tấn công.

Chiến lược Triển khai và Chuyển đổi

Chuyển đổi Song song (Parallel)

Chạy hệ thống cũ và mới cùng lúc.

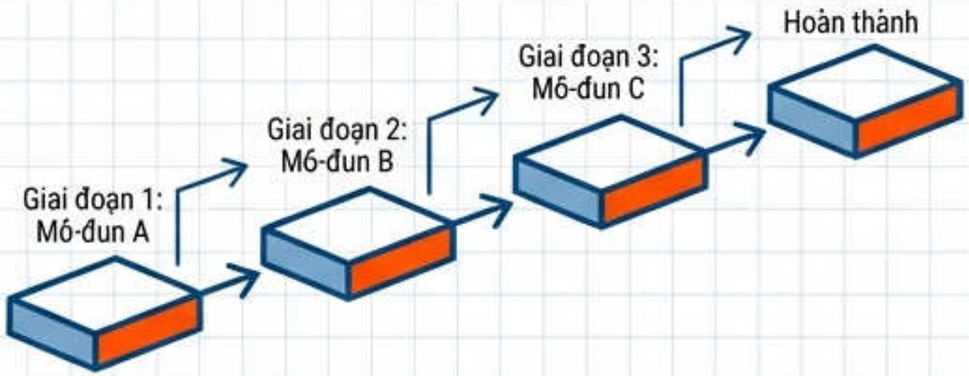
Ghi chú: An toàn nhất, chi phí cao nhất.



Chuyển đổi theo Giai đoạn (Phased)

Triển khai từng mô-đun/khu vực.

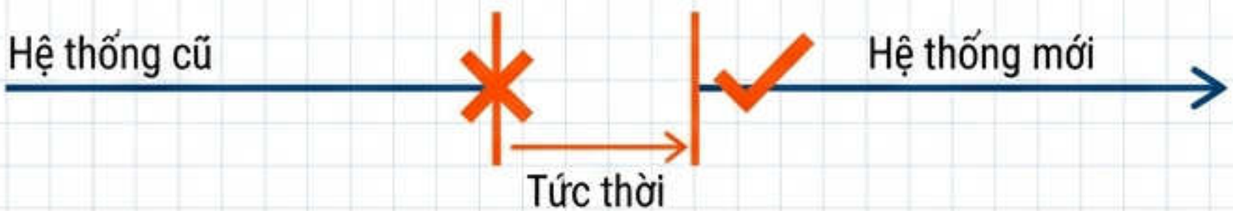
Ghi chú: Giảm rủi ro tác động lớn, tích hợp phức tạp.



Chuyển đổi Tức thời (Cutover)

Tắt cũ, bật mới ngay lập tức.

Ghi chú: Nhanh, rẻ, nhưng rủi ro cao nhất.



Đánh giá Sau Triển khai

Thời điểm thực hiện:

1. Ngay sau khi hoàn thành dự án.
2. Sau khi vận hành ổn định.

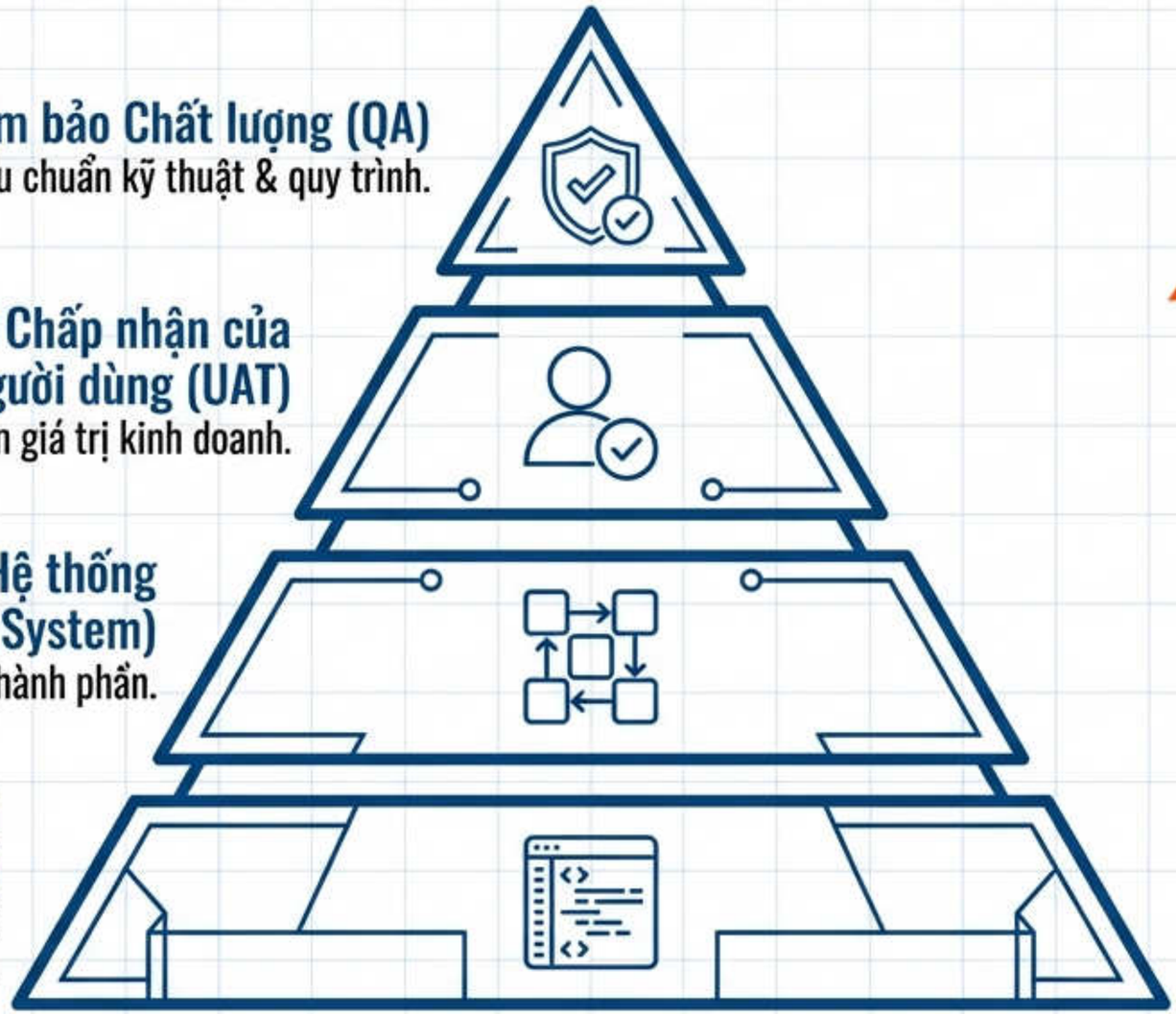
Phương pháp Kiểm thử: Từ Mã nguồn đến Người dùng

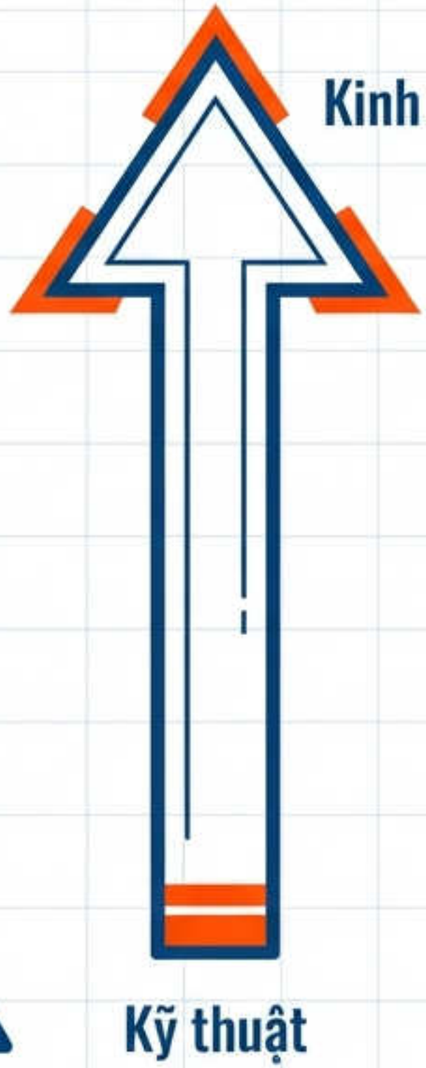
Đảm bảo Chất lượng (QA)
Tuân thủ tiêu chuẩn kỹ thuật & quy trình.

Kiểm thử Chấp nhận của Người dùng (UAT)
Người dùng cuối xác nhận giá trị kinh doanh.

Kiểm thử Tích hợp/Hệ thống (Integration/System)
Kiểm tra tương tác giữa các thành phần.

Kiểm thử Đơn vị (Unit Testing)
Kiểm tra từng mô-đun/đoạn mã riêng lẻ.



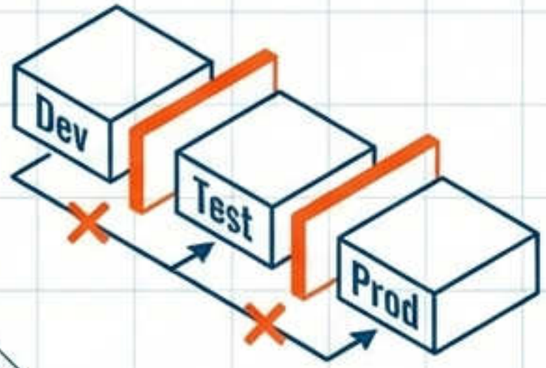


Thực hành Tốt nhất trong Kiểm thử

Dữ liệu Kiểm thử (Test Data)

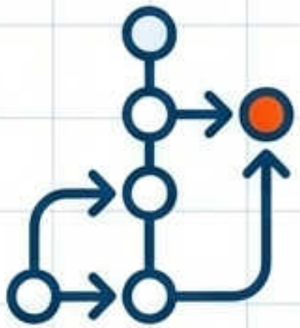
Không dùng dữ liệu sản xuất (trừ khi đã làm sạch).
Sử dụng Fuzzing để test giá trị lạ.

Phân tách Môi trường



Tách biệt vật lý/logic Dev, Test, Prod để ngăn lây nhiễm chéo.

Kiểm soát Phiên bản

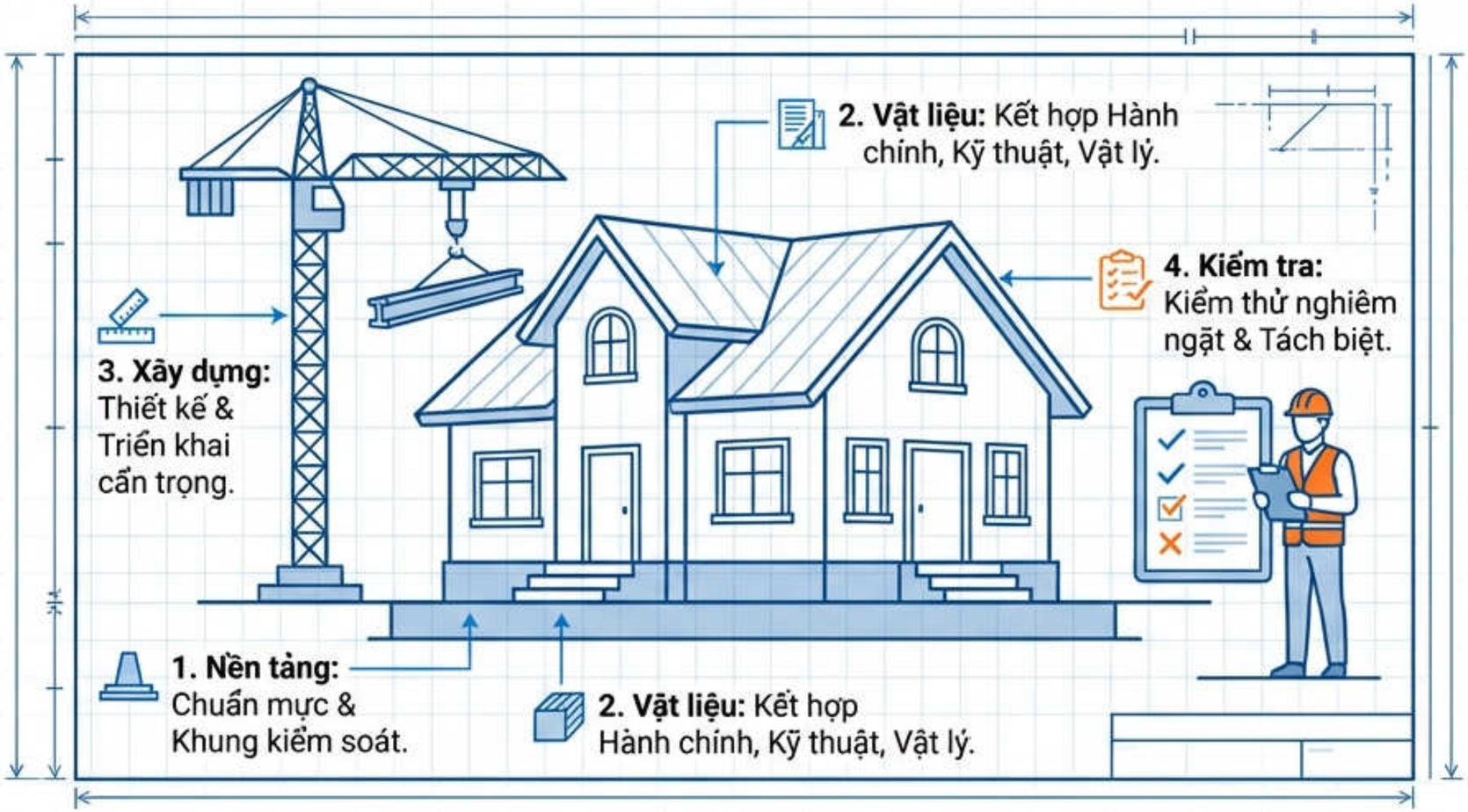


Theo dõi thay đổi mã nguồn, đảm bảo khả năng năng rollback.

Tính Khách quan

Người viết mã không nên là người duy nhất kiểm thử mã đó.

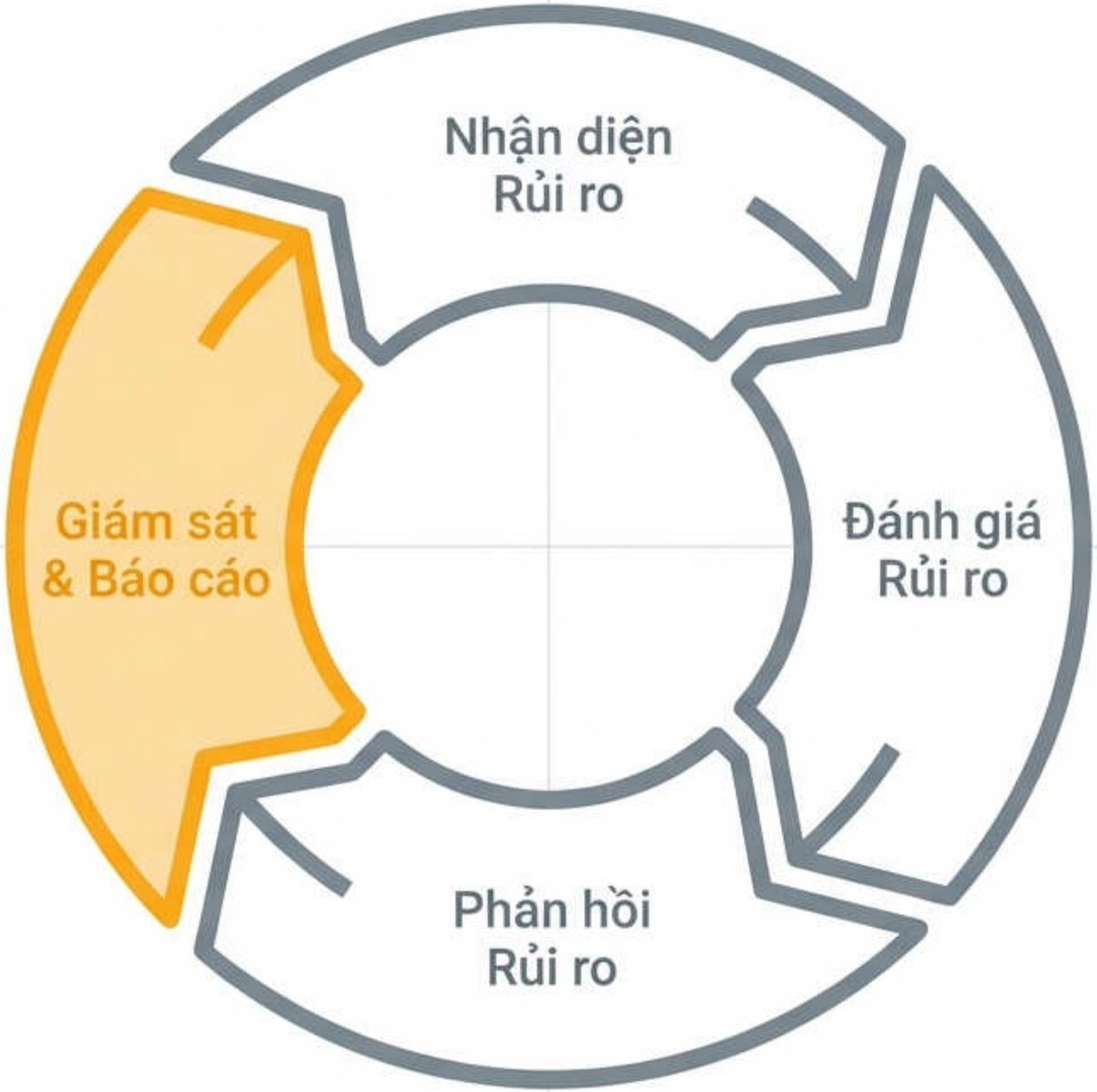
Tổng kết: Tư duy Kỹ thuật cho Sự Kiên cường



"Kiểm soát không chỉ là rào cản, chúng là nền tảng cho phép doanh nghiệp vận hành an toàn và phát triển bền vững."

Giám sát và Báo cáo Rủi ro

CRISC® Official Review Manual - Chapter 3, Part C



Chu trình Từ Dữ liệu đến Quyết định

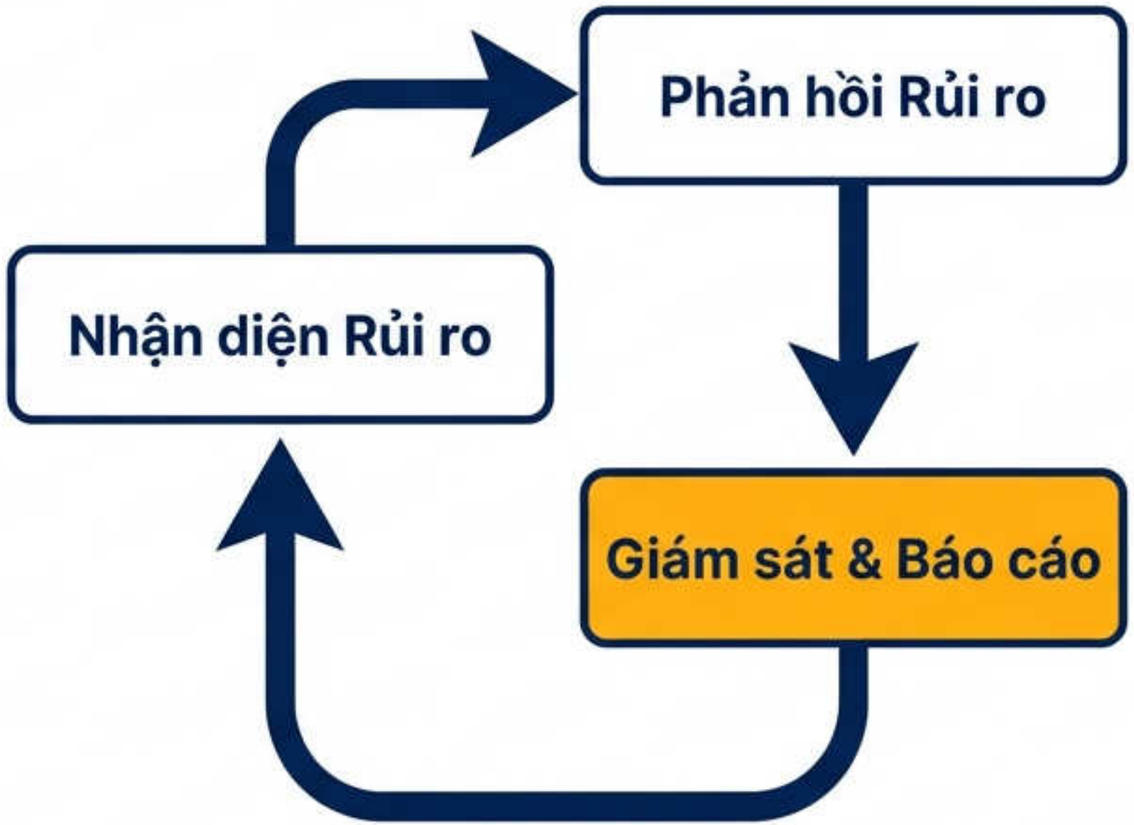
Vai trò của Giám sát trong Vòng đời Rủi ro

Mục đích Chính

Giám sát không phải là điểm kết thúc. Nó là "cảm biến" kích hoạt chu kỳ xác định rủi ro tiếp theo.

Chức năng

- Đảm bảo các biện pháp kiểm soát hoạt động hiệu quả.
- Phát hiện các thay đổi trong hồ sơ rủi ro (Risk Profile).
- Cung cấp dữ liệu cho việc ra quyết định của lãnh đạo.



Giám sát hiệu quả giúp doanh nghiệp chuyển từ trạng thái "Phản ứng" (Reactive) sang "Chủ động" (Proactive).

Kế hoạch Hành động Rủi ro

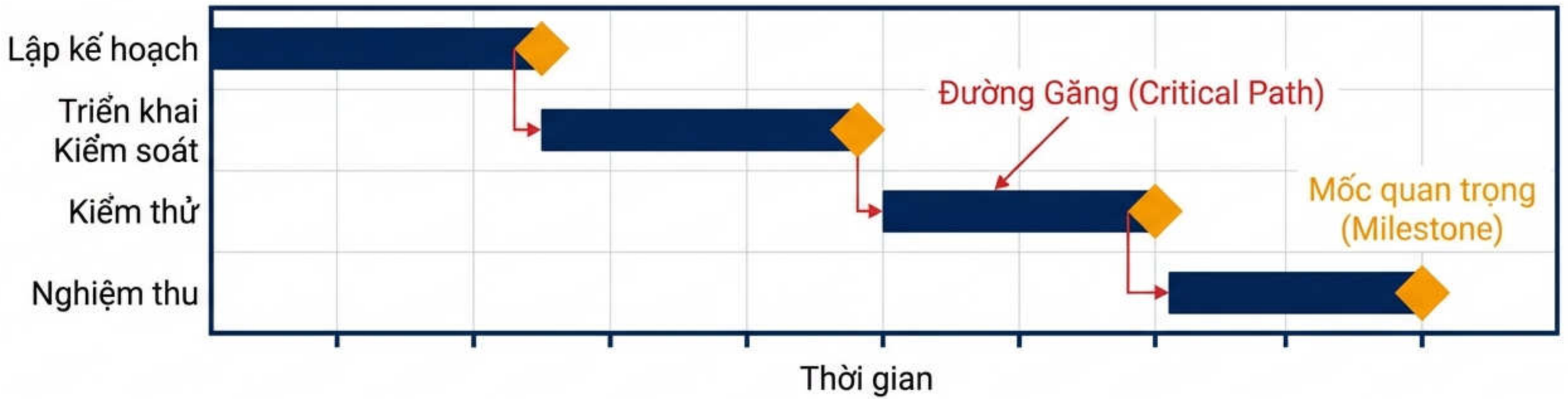
Định nghĩa: Một lộ trình cụ thể để triển khai các phản hồi rủi ro đã được chọn.

Phân tích khoảng cách (Gap Analysis)

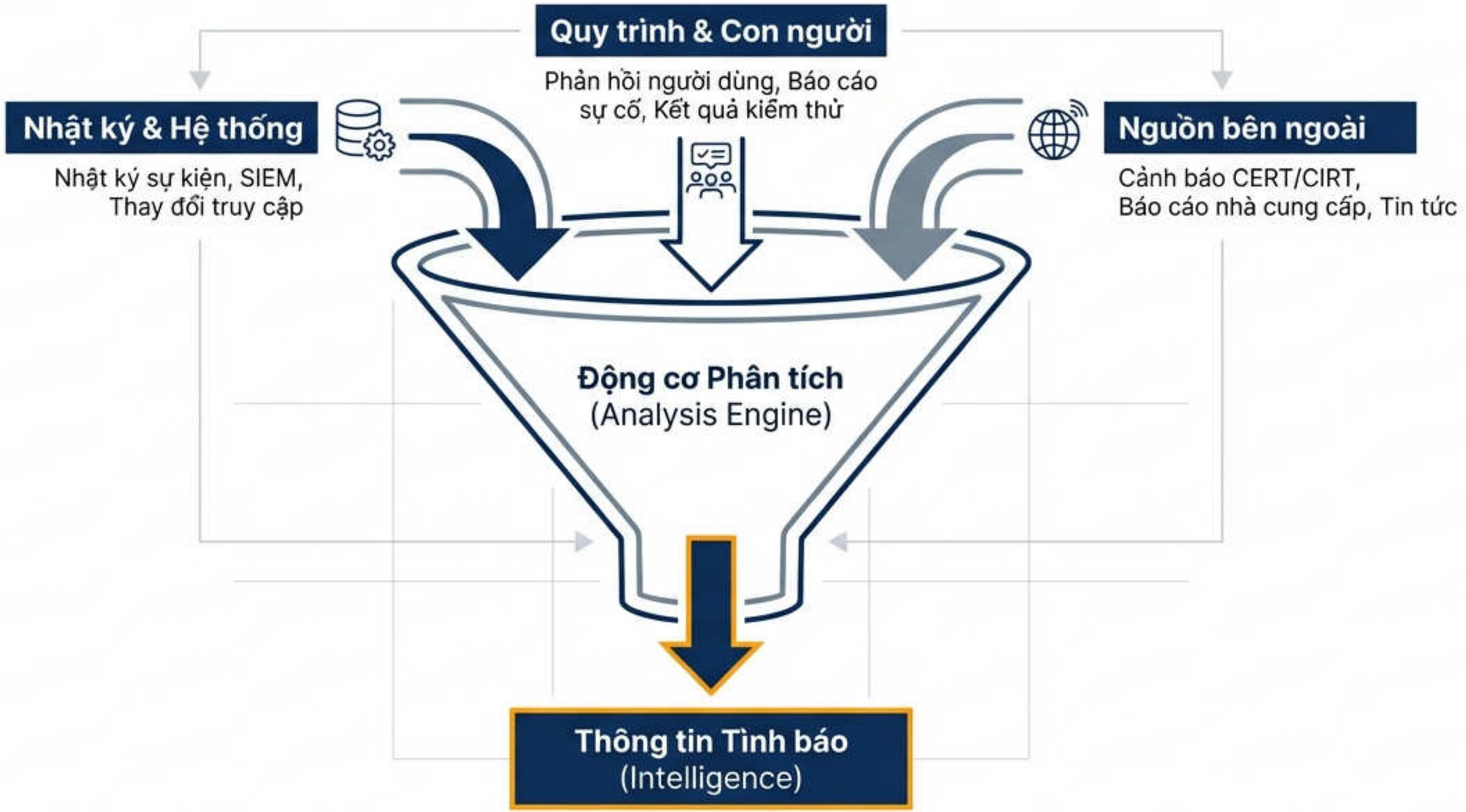
So sánh trạng thái hiện tại và trạng thái mong muốn.

Đường găng (Critical Path)

Các yếu tố dự án ảnh hưởng trực tiếp đến thời gian hoàn thành.



Thu thập Dữ liệu: Nền tảng của Giám sát



Bộ ba Chỉ số Đo lường: KPI, KRI, KCI

KPI

Chỉ số Hiệu suất Chính

Focus Question:
Chúng ta có đạt được mục tiêu không?

Example:
Thời gian trung bình để vá lỗi (MTTP).

KRI

Chỉ số Rủi ro Chính

Focus Question:
Rủi ro có đang gia tăng không?

Example:
Số lượng bản vá bảo mật quá hạn 30 ngày.

KCI

Chỉ số Kiểm soát Chính

Focus Question:
Biện pháp kiểm soát có hoạt động không?

Example:
Tỷ lệ máy chủ đã cài đặt antivirus.

Phân biệt KPI và KRI

KPI (Hiệu suất)

Chỉ số trễ (Lagging Indicator). Đo lường kết quả đã xảy ra.

Context: Xe đang chạy bao nhiêu km/h?

KRI (Rủi ro)

Chỉ số dẫn dắt (Leading Indicator). Cảnh báo sớm về sự cố tương lai.

Context: Động cơ có sắp quá nhiệt không?

KPI và KRI thường được sử dụng cùng nhau để cung cấp bức tranh toàn cảnh.

Tối ưu hóa Chỉ số Rủi ro Chính (KRI)

Nguyên tắc 'Goldilocks' trong việc chọn chỉ số

Quá ít
(Mù thông tin)

Tối ưu hóa
(Optimized)

Quá nhiều
(Nhiễu/Noise)

Độ nhạy (Sensitivity)
Chỉ số thay đổi ngay khi rủi ro thay đổi.

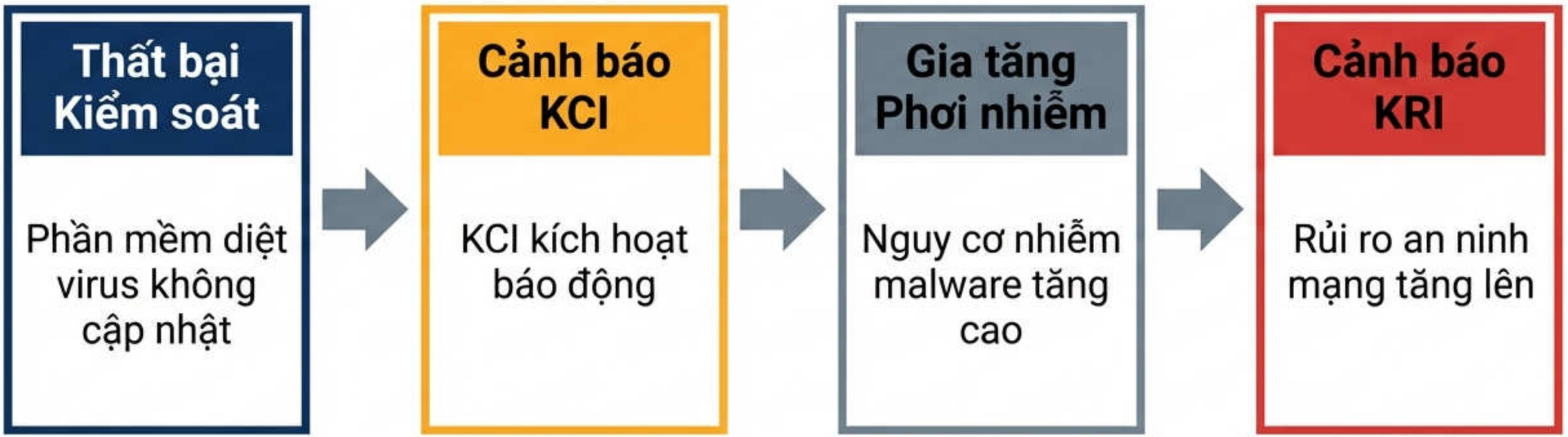
Độ tin cậy (Reliability)
Tương quan cao với rủi ro thực tế.

Dễ đo lường (Effort)
Dễ thu thập và duy trì dữ liệu.

Có thể lặp lại (Repeatable)
Đo lường nhất quán theo thời gian.

Chỉ số Kiểm soát Chính (KCI)

Hiệu ứng dây chuyền từ Kiểm soát đến Rủi ro



KCI thường là chỉ số dẫn dắt (Leading Indicator) cho KRI.

Kỹ thuật Giám sát và Đánh giá

Phương pháp và công cụ chính để đánh giá hiệu quả.

Tự đánh giá (Self-assessment)

Chủ sở hữu quy trình tự kiểm tra. Nhanh chóng nhưng có thể chủ quan.

Kiểm toán IS (IS Audit)

Đánh giá độc lập, khách quan. Bằng chứng mạnh mẽ nhưng tốn thời gian.

Đánh giá lỗ hổng (Vulnerability Assessment)

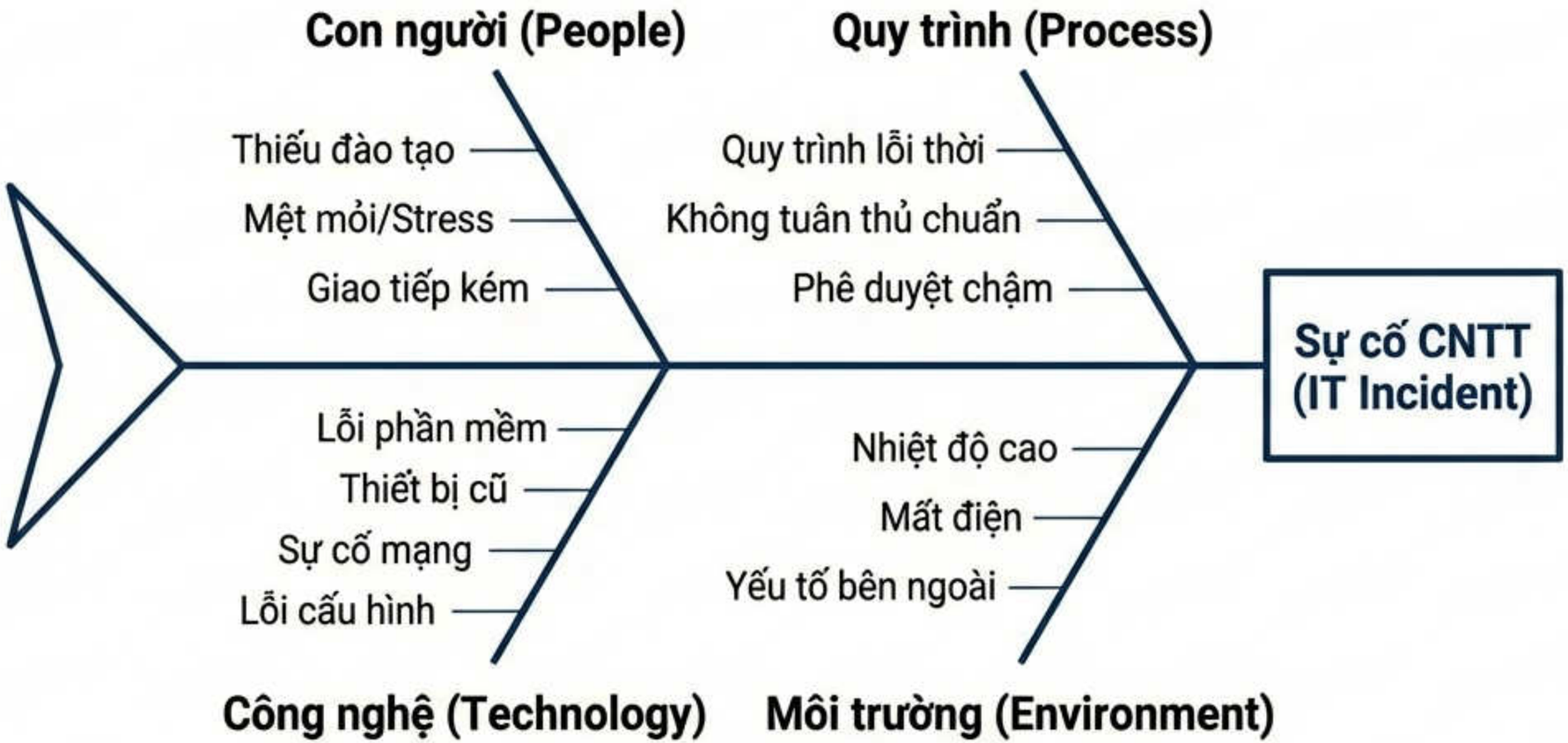
Quét hệ thống tự động để tìm điểm yếu đã biết.

Kiểm thử xâm nhập (Penetration Testing)

Mô phỏng tấn công thực tế (Black/White box). Rủi ro cao, ʁủi ro cao, cần phê duyệt.

Phương pháp Phân tích Dữ liệu

Phân tích Nguyên nhân Gốc rễ (Root Cause Analysis)



- Phân tích Cây Lỗi (Fault Tree Analysis)
- Phân tích Xu hướng (Trend Analysis)

Nguyên tắc Báo cáo Rủi ro

Chính xác - Kịp thời - Liên quan

Ban Lãnh đạo / HĐQT

Xu hướng chiến lược, Heat Maps, Tác động tài chính.

Quản lý cấp trung

Scorecards, KRI, Trạng thái dự án.

Vận hành / Kỹ thuật

Nhật ký chi tiết (Logs), Cảnh báo kỹ thuật, Sự cố cụ thể.

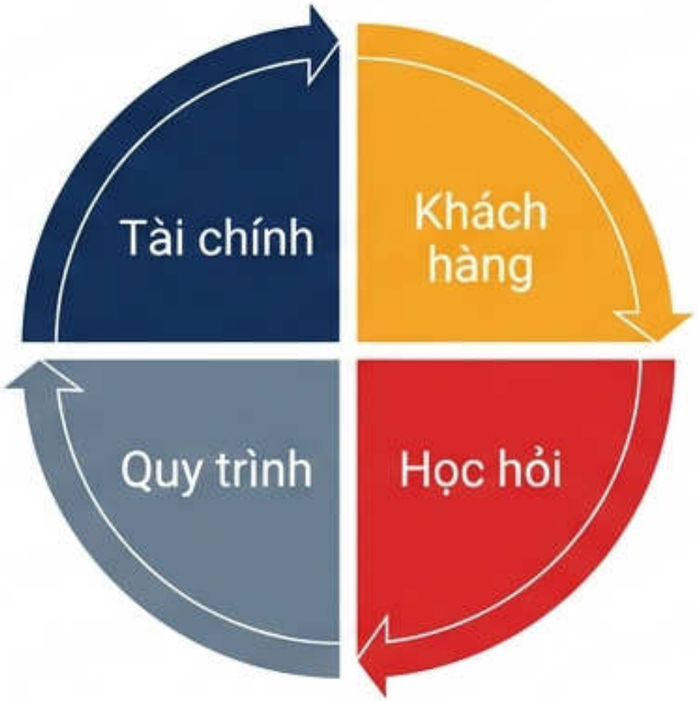
Trực quan hóa: Biểu đồ Nhiệt (Heat Maps)

Đặc điểm

- Công cụ tiêu chuẩn cho báo cáo cấp cao.
- Giúp ưu tiên tài nguyên vào vùng 'Đỏ'.
- Lưu ý: Thường dựa trên dữ liệu định tính, có thể mang tính chủ quan.

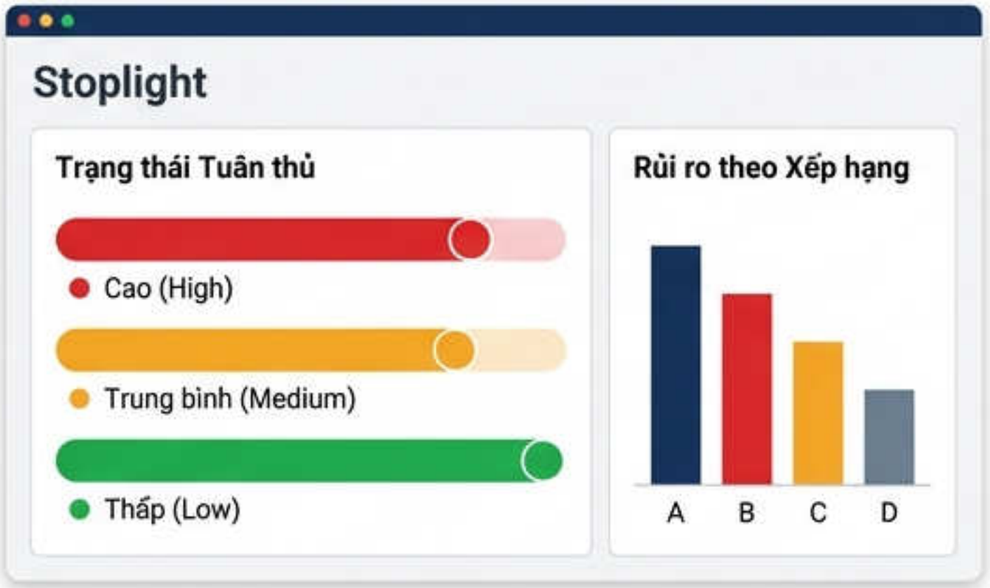
Bảng điều khiển và Thẻ điểm

Thẻ điểm cân bằng (Balanced Scorecard)



- Nhìn rủi ro trong bối cảnh chiến lược tổng thể.

Bảng điều khiển (Dashboard)



- Tập trung vào các ngoại lệ cần xử lý ngay (Real-time).

Giám sát Rủi ro Mới nổi

AI & Big Data

Rủi ro về quyền riêng tư và thiên kiến thuật toán.

Cloud & Shadow IT

Mất kiểm soát dữ liệu khi các đơn vị tự triển khai công nghệ.

Chuỗi cung ứng

Rủi ro từ nhà cung cấp thứ ba và đối tác.

Chiến lược: Tích hợp đánh giá rủi ro vào quy trình Quản lý Thay đổi (Change Management).

Tổng kết & Trọng tâm Kỳ thi

Thẻ điểm cân bằng (Balanced Scorecard)

- Nhìn rủi ro trong bối cảnh chiến lược tổng thể.

Danh sách Ghi nhớ (Exam Checklist)

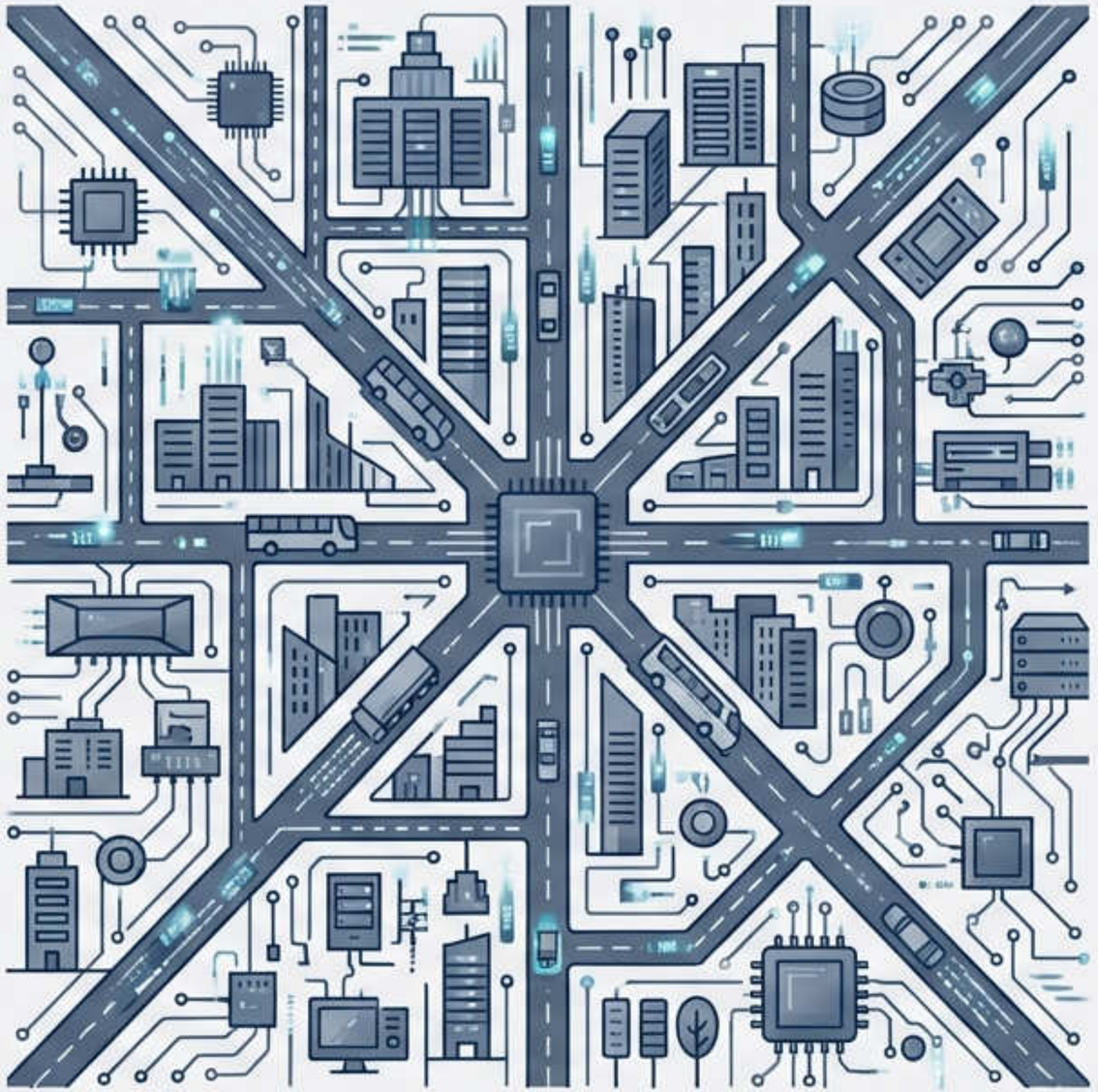
1. Phân biệt rõ KPI (Hiệu suất), KRI (Rủi ro), KCI (Kiểm soát).
2. Hiểu sự khác biệt giữa Kiểm toán (độc lập) và Tự đánh giá.
3. Biểu đồ nhiệt (Heat Map) thể hiện Tần suất vs. Tác động.
4. KCI thất bại là chỉ báo dẫn dắt (leading) cho KRI.

Kết thúc Chương 3 - Phần C

CRISC Review Manual - Chapter 4

Technology and Security

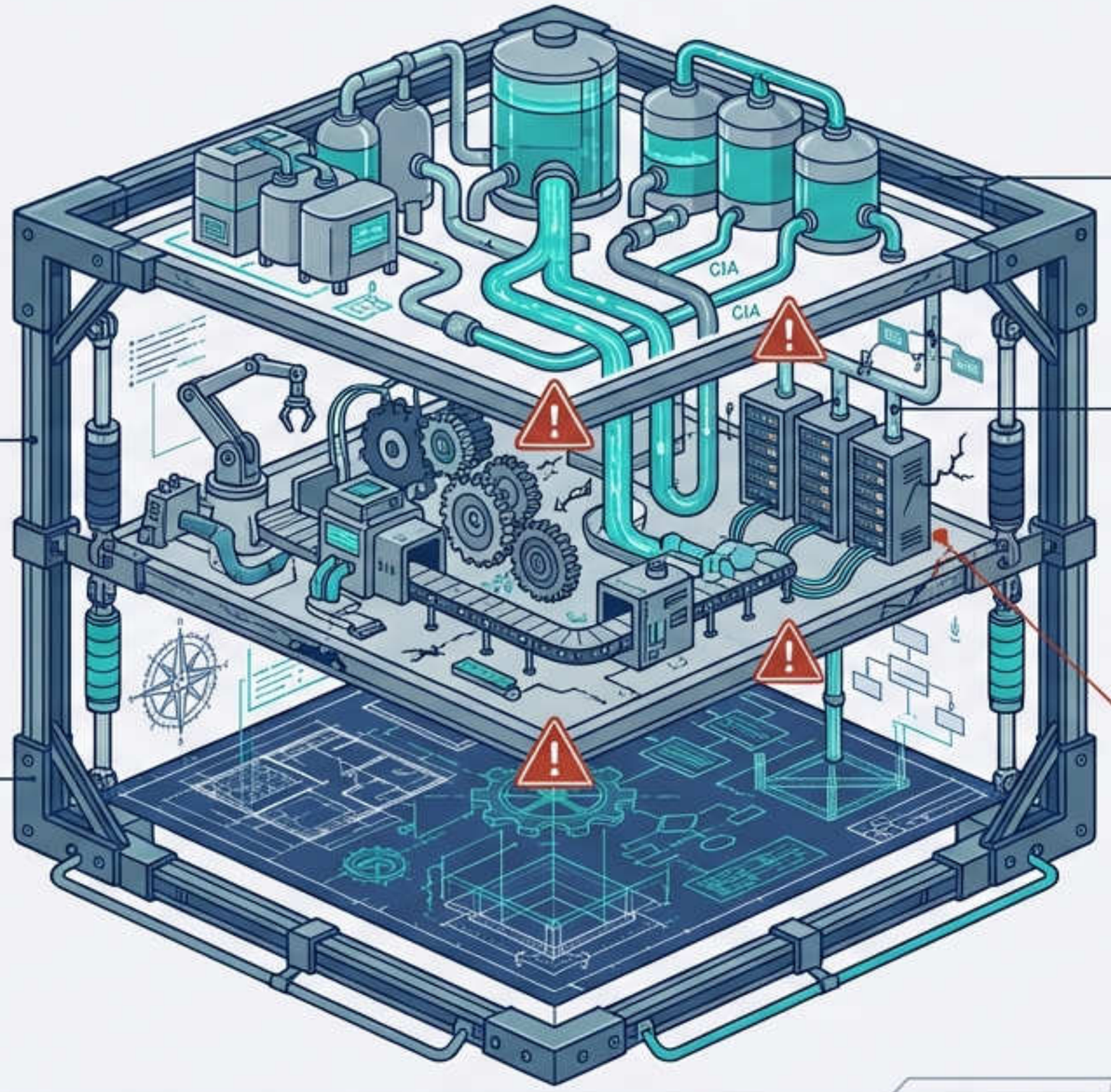
Part A: Technology Principles (Các Nguyên tắc Công nghệ)



Trọng tâm: Hiểu về các thành phần công nghệ để nhận diện rủi ro.
Mục tiêu: Đánh giá cách công nghệ hỗ trợ hoặc cản trở các mục tiêu kinh doanh.
Các lĩnh vực chính: Kiến trúc doanh nghiệp, Vận hành hệ thống, Vòng đời dữ liệu, và Công nghệ mới nổi.

Hệ sinh thái Rủi ro Công nghệ (The Technology Risk Ecosystem)

Roboto Slab



Dữ liệu (Data)
Tài sản cần bảo vệ (CIA).

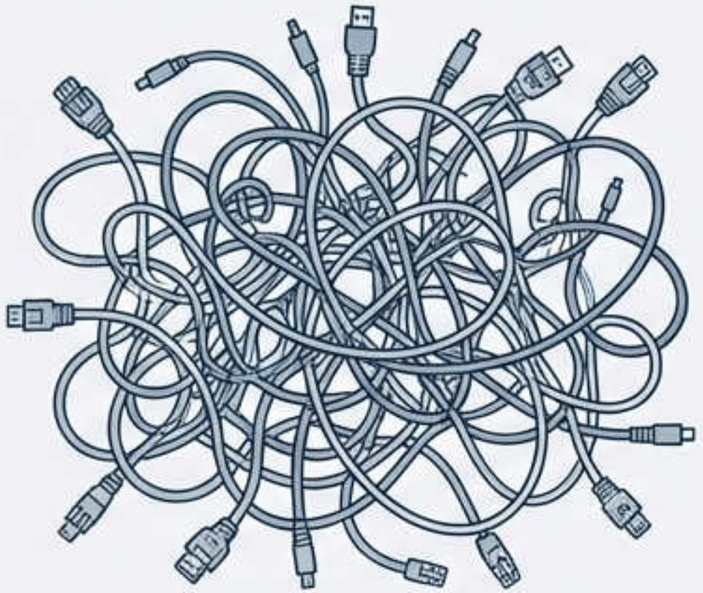
Vận hành (Operations)
Cỗ máy xử lý.
Nơi phát sinh lỗ hổng (Vulnerabilities).

Khả năng phục hồi (Resilience)
Lưới an toàn khi thất bại.

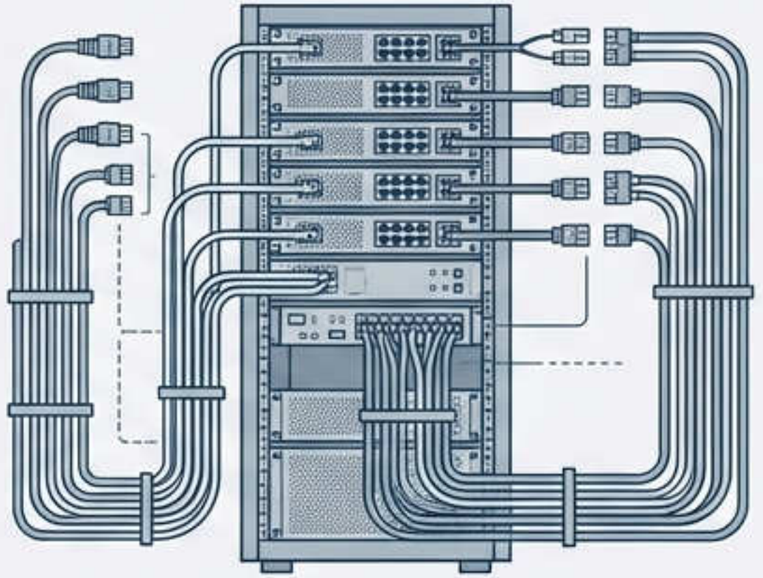
Chiến lược (Strategy)
Nền tảng của rủi ro. Kiến trúc sai = Bảo mật vô nghĩa.

Insight: Rủi ro thường xuất hiện tại các điểm giao thoa (ví dụ: Chiến lược thay đổi nhưng Vận hành không theo kịp).

Chiến lược & Kiến trúc Doanh nghiệp (Enterprise Architecture - EA)



Poor EA



Good EA

Vai trò của EA: Đảm bảo CNTT hỗ trợ trực tiếp cho mục tiêu kinh doanh. Các khung phổ biến: TOGAF, Zachman.

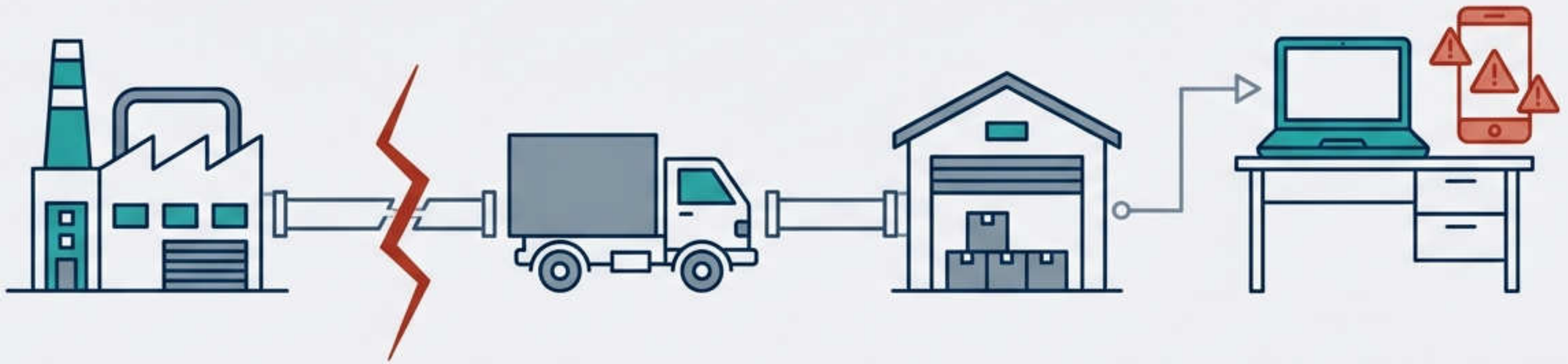
Lộ trình Công nghệ (Roadmaps): Dự báo thay đổi, tránh đầu tư vào công nghệ "chết" (Legacy systems).

Sự lệch pha (Misalignment): Giải pháp CNTT không giải quyết được vấn đề kinh doanh.

Nợ kỹ thuật (Technical Debt): Chi phí duy trì hệ thống cũ, thiếu bảo mật.

Shadow IT: Khi EA quá cứng nhắc, các bộ phận tự ý triển khai công nghệ ngoài tầm kiểm soát.

Quản lý Vận hành: Phần cứng & Chuỗi cung ứng



Quản lý Tài sản (Asset Management):

- Bạn không thể bảo vệ những gì bạn không biết mình đang sở hữu.
- **Rủi ro:** Thiết bị không được kiểm kê (**Unmanaged assets**) là điểm mù.

Chuỗi cung ứng (Supply Chain):

- **Rủi ro** từ bên thứ ba (**Third-party risk**).
- **Mối đe dọa:** Phần cứng bị cài cắm mã độc từ nhà sản xuất.

Bring Your Own Device (BYOD):

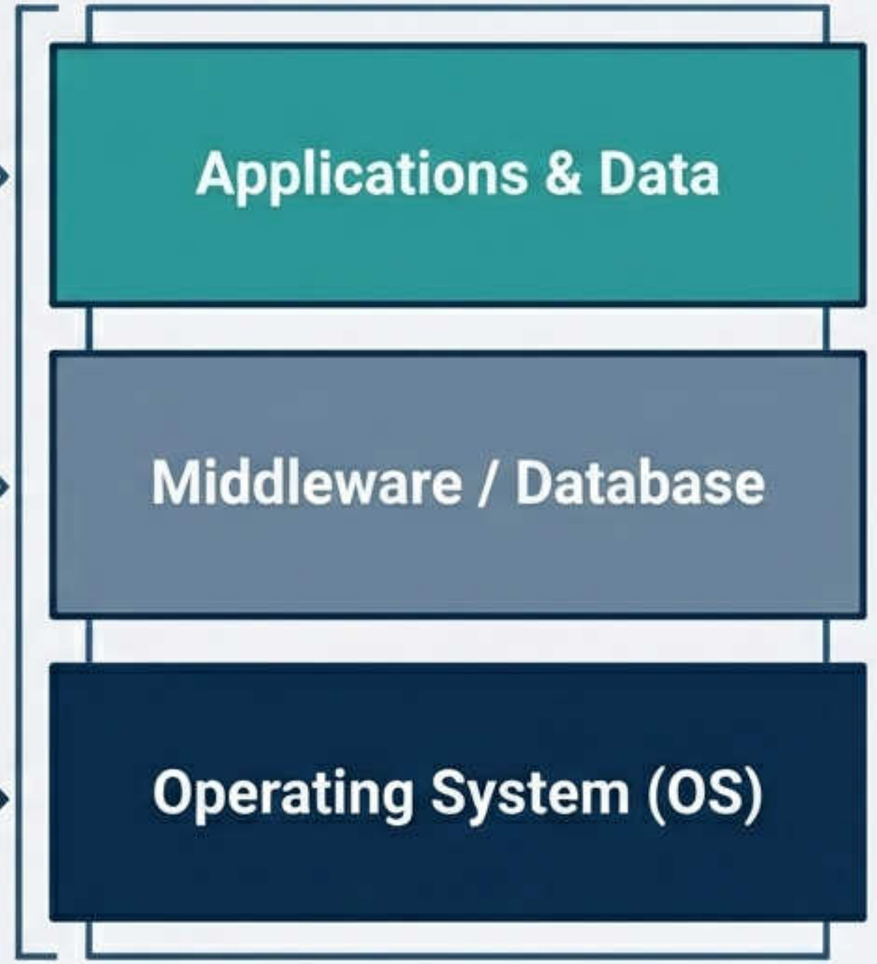
- **Lợi ích:** Linh hoạt, tiết kiệm.
- **Rủi ro:** Nguy cơ rò rỉ dữ liệu (**Data Exfiltration**) trên thiết bị cá nhân.

Quản lý Vận hành: Hệ điều hành & Ứng dụng

Ứng dụng: Xác thực đầu vào để tránh SQL Injection. Áp dụng Đặc quyền tối thiểu (Least Privilege).

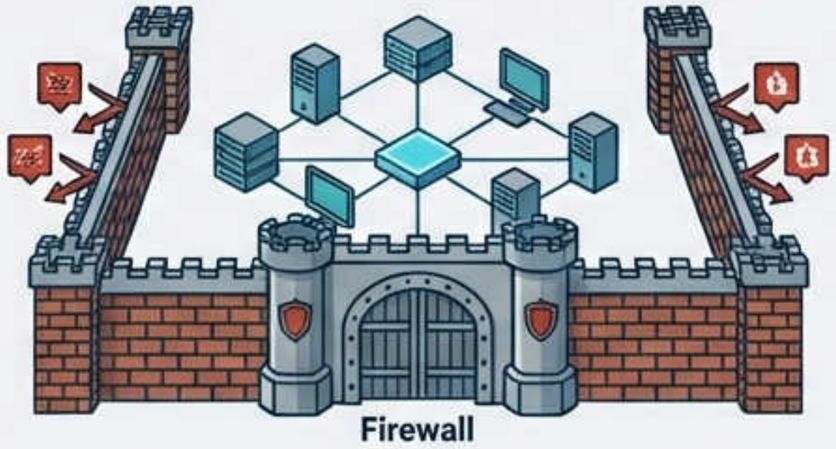
Hệ thống kế thừa (Legacy): Ngừng hỗ trợ (End-of-Life). Cần cô lập mạng (Network segmentation) nếu không thể thay thế.

Hệ điều hành: Rủi ro lỗ hổng chưa vá (Unpatched) và cấu hình mặc định không an toàn.



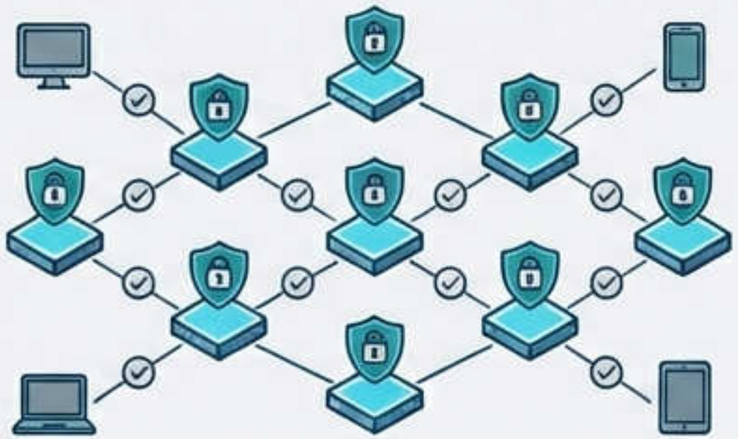
Kiến trúc Mạng & Bảo mật Đường truyền

Perimeter Defense



Vành đai truyền thống.

Zero Trust



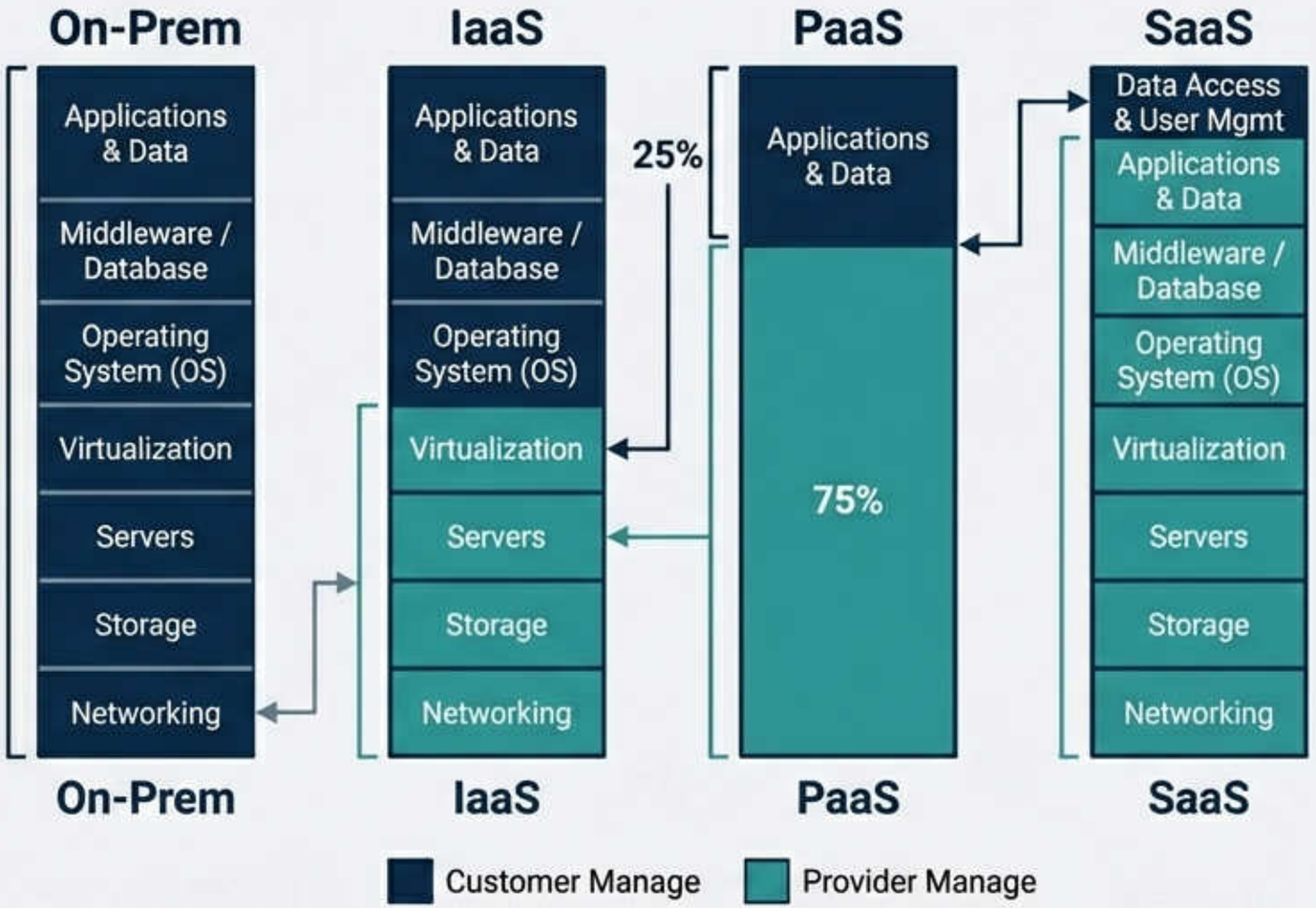
Identity-based Verification.

Cấu trúc mạng (Topologies): Star, Bus, Mesh ảnh hưởng đến tính sẵn sàng. Cần tránh Điểm lỗi đơn (Single Point of Failure).
Thiết bị bảo mật: Firewall, IDS/IPS, Proxy, DMZ.
Xu hướng Zero Trust:
- Nguyên tắc: “Không bao giờ tin tưởng, luôn luôn xác thực” (Never trust, always verify).
- Lý do: Làm việc từ xa và Cloud đã xóa nhòa vành đai mạng.

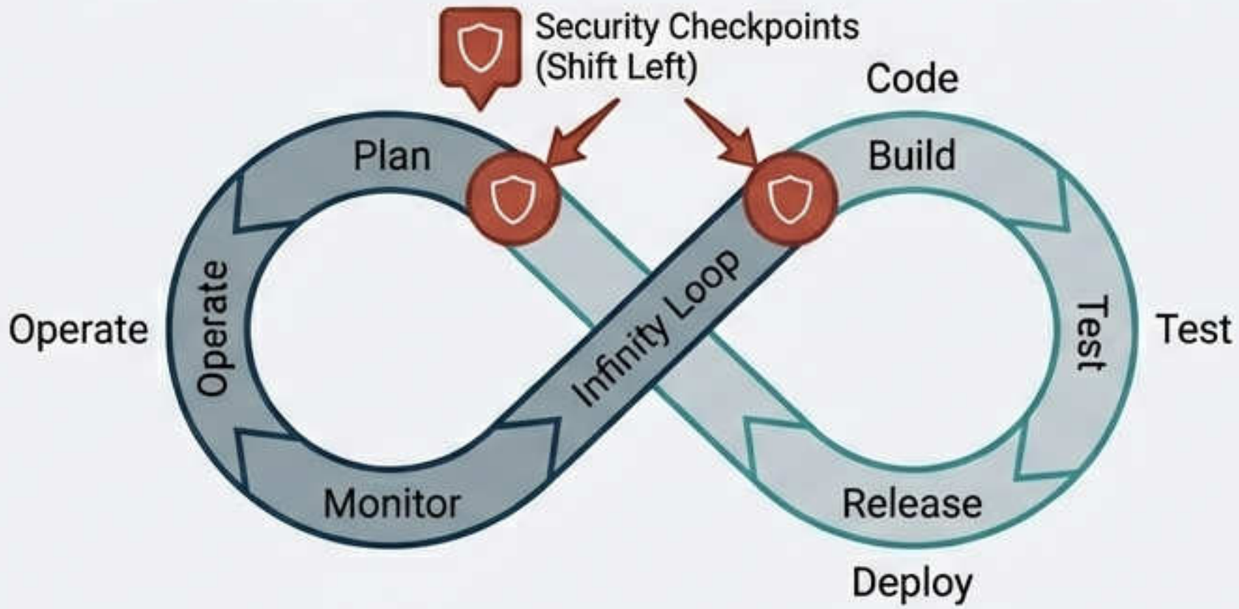
Ảo hóa & Điện toán Đám mây (Shared Responsibility)

Ảo hóa: Rủi ro 'VM Sprawl' (tăng trưởng máy ảo không kiểm soát).

Mô hình Trách nhiệm Chia sẻ:
- IaaS/PaaS/SaaS xác định ai quản lý OS, Ứng dụng, hay Dữ liệu.
- **Insight:** Bạn có thể thuê ngoài hạ tầng, nhưng **không thể thuê ngoài trách nhiệm giải trình (Accountability)**.

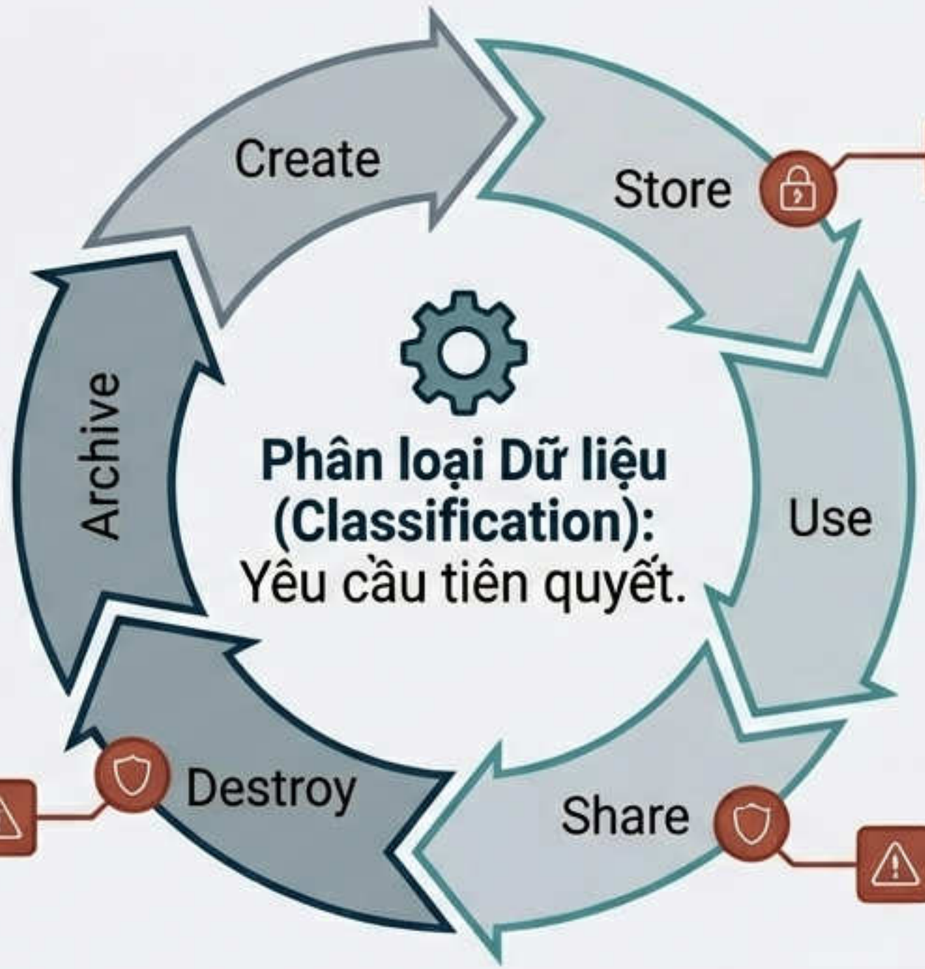


Vòng đời Phát triển Hệ thống (SDLC) & Quản lý Dự án



Waterfall vs. Agile: Waterfall dồn kiểm thử về cuối (rủi ro cao). **Agile** nhanh nhưng dễ bỏ qua quy trình.
Nguyên tắc Shift Left: Tích hợp bảo mật từ giai đoạn thiết kế.
Rủi ro Dự án:
- Scope Creep (Phạm vi phình to).
- Thiếu sự tham gia của các bên liên quan.
- Cạn kiệt ngân sách trước khi triển khai kiểm soát bảo mật.

Quản lý Vòng đời Dữ liệu (Data Lifecycle Management)



Rủi ro mã hóa kém.

Rủi ro phục hồi dữ liệu (Data Remanence).

Rủi ro mất kiểm soát (DLP).

Quyền riêng tư: Tuân thủ GDPR/CCPA cho dữ liệu cá nhân (PII).

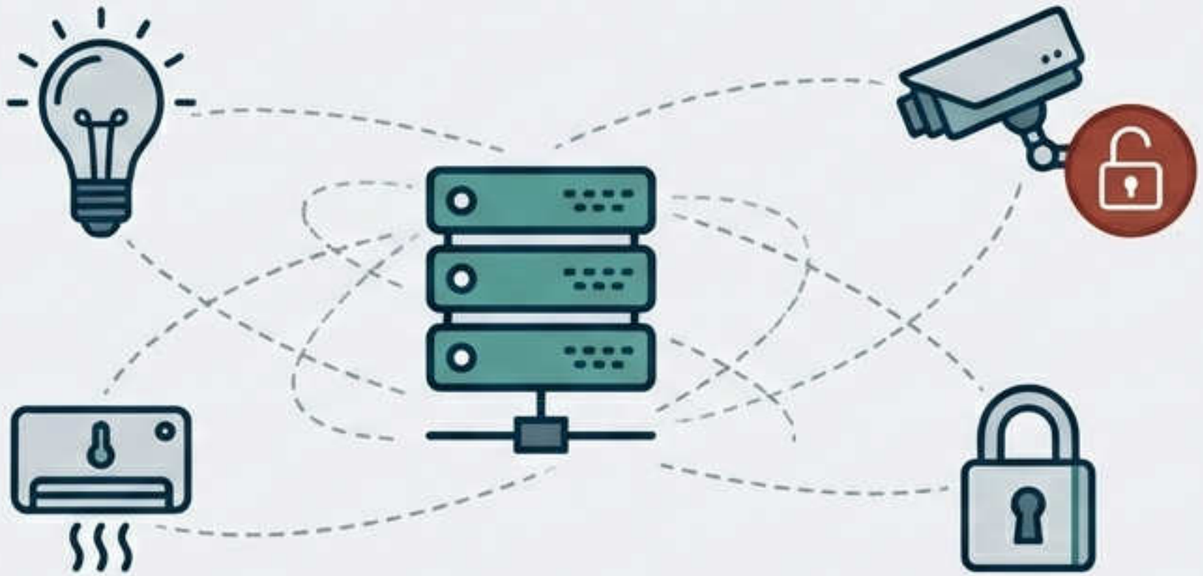
Khả năng Phục hồi: BCP vs. DR

BCP (Business Continuity): Duy trì kinh doanh.
DRP (Disaster Recovery): Khôi phục CNTT.

RPO (Recovery Point Objective): Chấp nhận mất dữ liệu tối đa (liên quan đến Backup).
RTO (Recovery Time Objective): Thời gian ngừng hoạt động tối đa (liên quan đến dự phòng).

Rủi ro: Khoảng cách giữa kỳ vọng Availability của doanh nghiệp và năng lực thực tế của CNTT.

Công nghệ Mới nổi: Kết nối Vạn vật (IoT)



- **Internet of Things (IoT):** Thiết bị năng lực xử lý thấp, khó cài agent bảo mật.
- **Rủi ro chính:** Mật khẩu mặc định, Firmware cũ không được vá.
- **Mở rộng bề mặt tấn công:** Mỗi thiết bị là một điểm thâm nhập tiềm năng.
- **Shadow IT:** Thiết bị được lắp đặt bởi bộ phận Facilities mà không qua CNTT kiểm duyệt.

Công nghệ Mới nổi: AI & Dữ liệu lớn (Big Data)

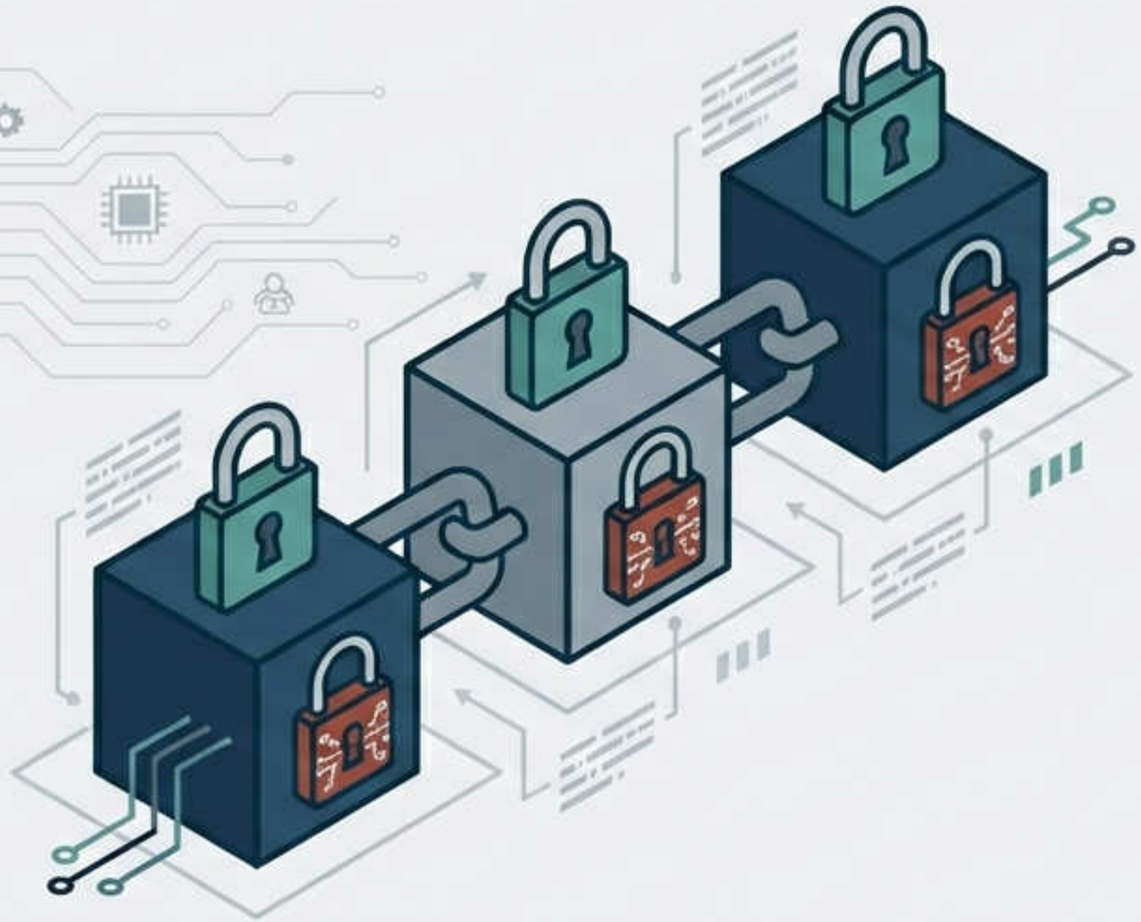
Generative AI:

- Rủi ro liêm chính (Integrity): "Ảo giác" (Hallucinations) và Thiên kiến (Bias).
- Deepfakes: Tấn công phi kỹ thuật (Social Engineering) bằng giả mạo danh tính.

Big Data:

- Rủi ro tập trung (Aggregation Risk): Gom tụ dữ liệu tạo thành mục tiêu giá trị cao cho tin tặc.
- Thách thức kiểm soát khối lượng dữ liệu khổng lồ.

Công nghệ Mới nổi: Blockchain



Bản chất: Sổ cái phân tán (Distributed Ledger), Bất biến (Immutable).

Ứng dụng: Hợp đồng thông minh (Smart Contracts), Chuỗi cung ứng.

Góc nhìn Rủi ro:

- **Tính toàn vẹn**: Rất cao, khó làm giả.
- **Khả năng sửa lỗi:** Hầu như không thể đảo ngược giao dịch sai.
- **Quản lý khóa:** Mất khóa tư (Private Key) = Mất tài sản vĩnh viễn.

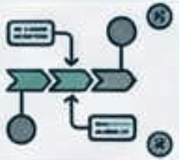
Danh mục Kiểm tra cho Chuyên gia Rủi ro (Checklist)

- [ ] **Nhận diện (Identify):** Đã kiểm kê đầy đủ tài sản phần cứng, phần mềm và luồng dữ liệu chưa?

- [ ] **Đánh giá (Assess):** Công nghệ có phù hợp với mục tiêu kinh doanh (Alignment) không?

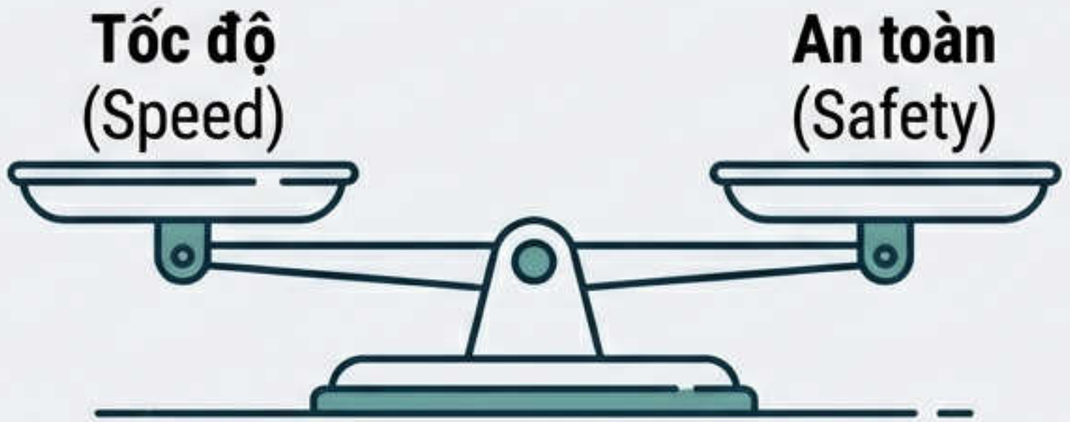
- [ ] **Dự báo (Forecast):** Đã xem xét rủi ro từ AI, IoT và Shadow IT chưa?

- [ ] **Kết nối (Connect):** Đảm bảo RTO/RPO của CNTT khớp với yêu cầu của BCP.



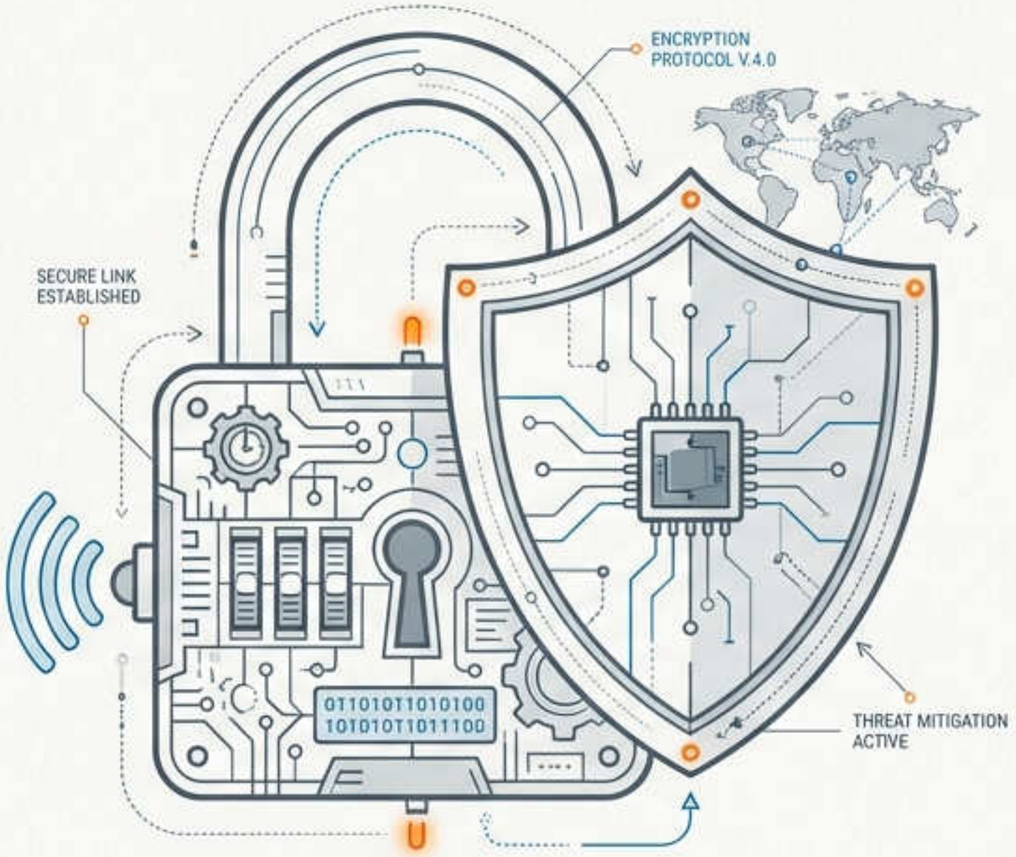
- [ ] **Vòng đời (Lifecycle):** Bảo mật có được tích hợp vào SDLC và mua sắm không?

Kết luận: Quản trị trong Môi trường Biến động



Công nghệ thay đổi liên tục, nhưng nguyên tắc quản lý rủi ro vẫn giữ nguyên: **Nhận diện -> Đánh giá -> Phản hồi**.

- Rủi ro công nghệ là rủi ro kinh doanh.
- Thách thức không phải là công nghệ mới, mà là sự tích hợp an toàn.
- **Thông điệp cuối:** Chuyển dịch từ người nói "Không" sang người kiến tạo giải pháp "Làm thế nào để an toàn".



Các Nguyên Tắc An Toàn Thông Tin

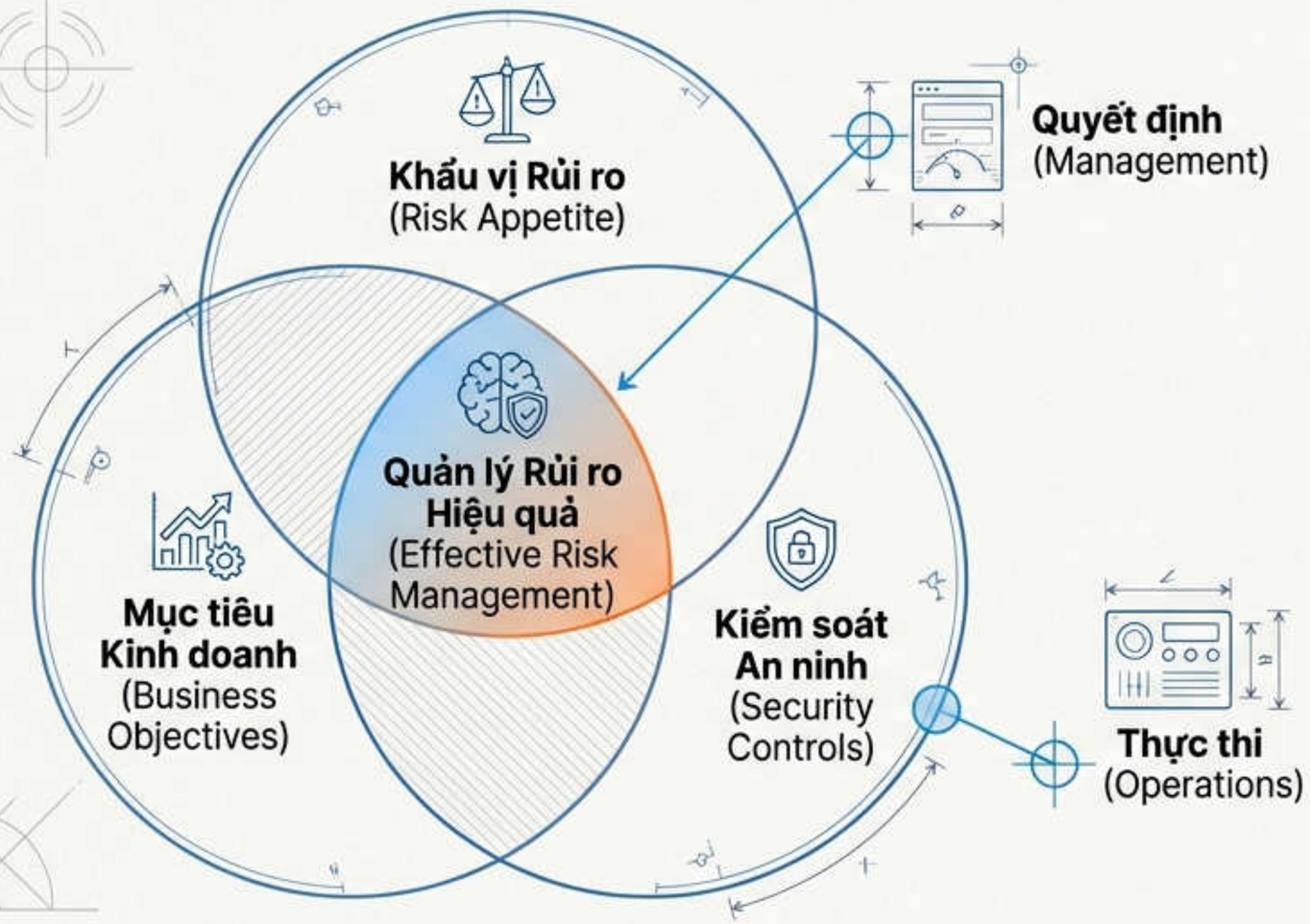
CRISC® Official Review Manual - Chapter 4, Part B

Hướng dẫn dành cho Chuyên gia Quản lý Rủi ro

Tài liệu tham khảo

16:9

Mối Giao Thoa Giữa Rủi Ro CNTT và An Ninh Thông Tin



- **An ninh thông tin** là việc bảo vệ thông tin và hệ thống khỏi các sự kiện rủi ro.
- **Biện pháp kiểm soát** (security controls) được triển khai dựa trên đánh giá rủi ro (risk justification).

Góc nhìn Chuyên gia Rủi ro

Rủi ro an ninh thông tin không chỉ là vấn đề kỹ thuật. Nếu rủi ro được định lượng kém, các biện pháp kiểm soát có thể bị thiết kế sai, gây lãng phí tài nguyên hoặc tạo ra cảm giác an toàn giả tạo.

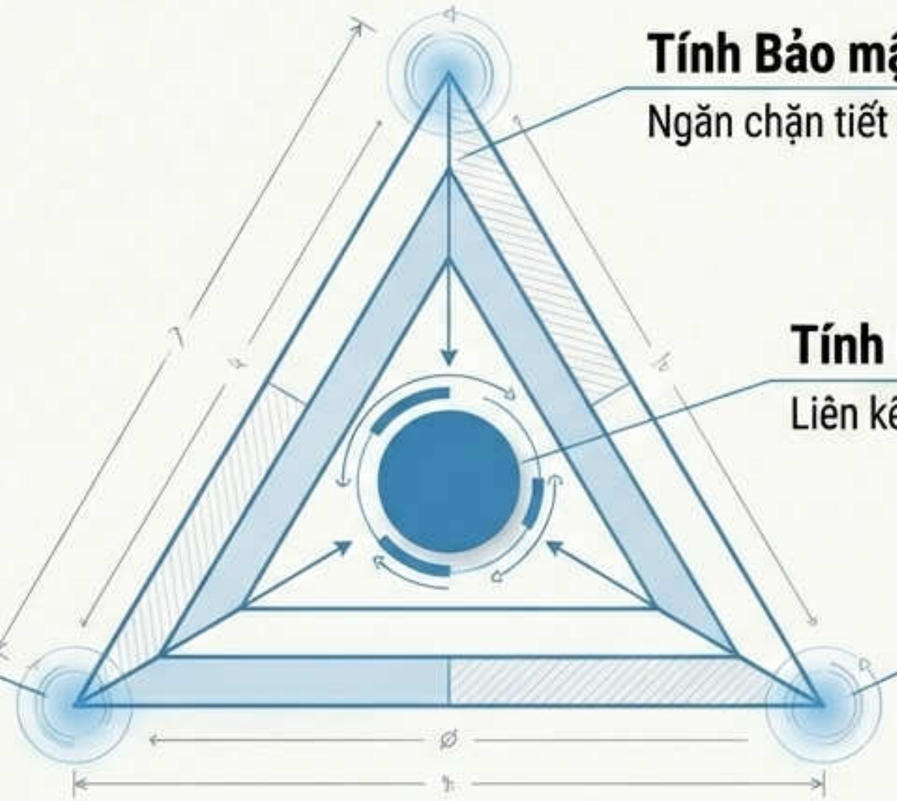
16:9

16:9

Mô Hình CIA Triad và Tính Không Thể Chối Bỏ

Tính Bảo mật (Confidentiality)

Ngăn chặn tiết lộ trái phép. Need-to-know.



Tính không thể chối bỏ (Nonrepudiation)

Liên kết xác thực hành động với người dùng.

Tính Sẵn sàng (Availability)

Truy cập tin cậy và kịp thời.

Tính Toàn vẹn (Integrity)

Ngăn chặn sửa đổi trái phép. Độ chính xác.

Góc nhìn Chuyên gia Rủi ro: Sự đánh đổi (Trade-offs)

Tăng cường tính bảo mật quá mức có thể làm giảm tính sẵn sàng hoặc hiệu năng hệ thống. Người quản lý rủi ro phải cân bằng 3 yếu tố này dựa trên nhu cầu kinh doanh thực tế, không phải dựa trên sự hoàn hảo về kỹ thuật.

16:9

16:9

Kiểm Soát Quản Trị: Ủy Quyền và Phân Chia Nhiệm Vụ

Thẩm định hệ thống (System Authorization)

Quy trình chính thức **đánh giá an ninh** và **chấp nhận rủi ro** trước khi hệ thống đi vào hoạt động (C&A/A&A).

Phân chia nhiệm vụ (SoD)

Phân lý chia nhiệm vụ và đạn hoàn về nới giản hậm tập.

↳ **Mục tiêu: Ngăn chặn sự thông đồng** (Collusion) và gian lận.

Developer không được phép deploy code trực tiếp vào Production.

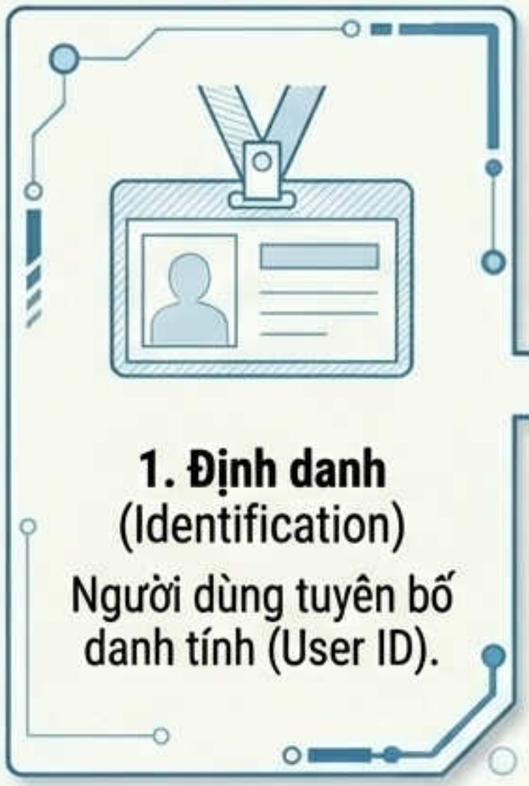
Góc nhìn Chuyên gia Rủi ro: Rủi ro & SoD

Trong các doanh nghiệp nhỏ thiếu nhân sự để thực hiện SoD đầy đủ, bắt buộc phải áp dụng **'biện pháp kiểm soát bù đắp'** (compensating controls) như **tăng cường giám sát** hoặc rà soát rà soát nhật ký (log review).

16:9

16:9

Khung Kiểm Soát Truy Cập: Mô hình IAAA



1. Định danh
(Identification)

Người dùng tuyên bố danh tính (User ID).

2. Xác thực
(Authentication)

Hệ thống xác minh danh tính (Password, Token).

3. Cấp quyền
(Authorization)

Hệ thống cấp quyền dựa trên vai trò (Read, Write).

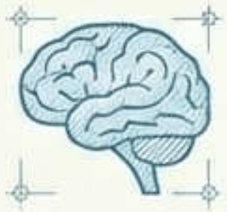
4. Trách nhiệm giải trình
(Accountability)

Ghi nhật ký (Logging) để truy vết hành động.

Insight: Định danh không có xác thực là vô nghĩa. Cấp quyền không có log (Accountability) khiến việc điều tra sự cố trở nên bất khả thi.

Cơ Chế Xác Thực và Nguyên Tắc Đặc Quyền

3 Nhân tố Xác thực (The 3 Factors)



Something you know

Điều bạn biết
(Password, PIN).

Something you have

Điều bạn có
(Token, Smart card).

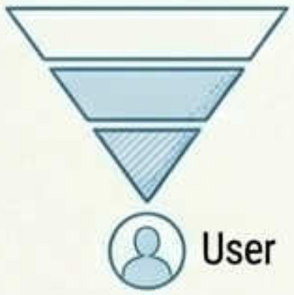
Something you are

Sinh trắc học
(Vân tay, khuôn mặt).

Xác thực đa yếu tố (MFA) = Kết hợp 2 trong 3 yếu tố này.

Góc nhìn Rủi ro

Mật khẩu tĩnh là điểm yếu lớn nhất. MFA là biện pháp giảm thiểu rủi ro hiệu quả nhất để chống lại việc chiếm đoạt tài khoản.



Nguyên tắc Đặc quyền Tối thiểu (Least Privilege)

Chỉ cấp quyền hạn ở mức tối thiểu cần thiết.
Thu hồi ngay khi không còn nhu cầu.

16:9

Cơ Bản Về Mã Hóa: Đối Xứng và Bất Đối Xứng

Mã hóa Đối xứng (Symmetric)

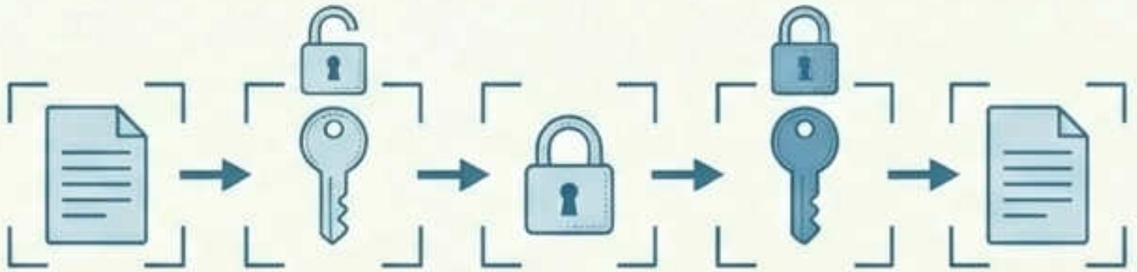
Pros:

- Tốc độ nhanh, xử lý dữ liệu lớn.

Cons:

- Khó phân phối khóa an toàn (Key distribution).

Mã hóa Bất đối xứng (Asymmetric)



Pros:

- An toàn, hỗ trợ tính không thể chối bỏ, dễ mở rộng.

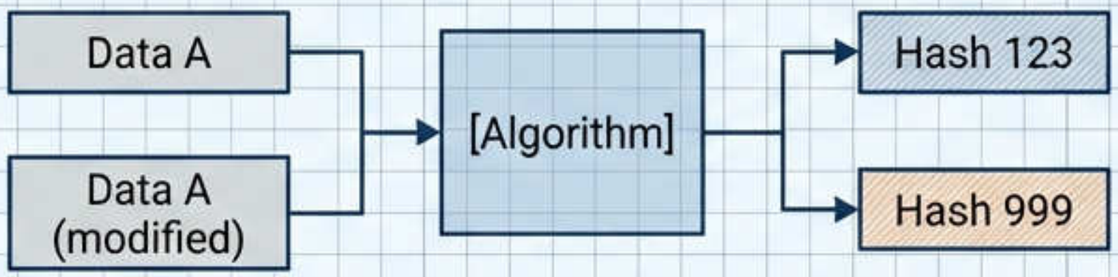
Cons:

- Tốc độ chậm, tốn tài nguyên.

Risk Lens: Mã hóa làm tăng tải hệ thống (processing overhead). Cần cân nhắc chi phí hiệu năng so với lợi ích bảo mật.

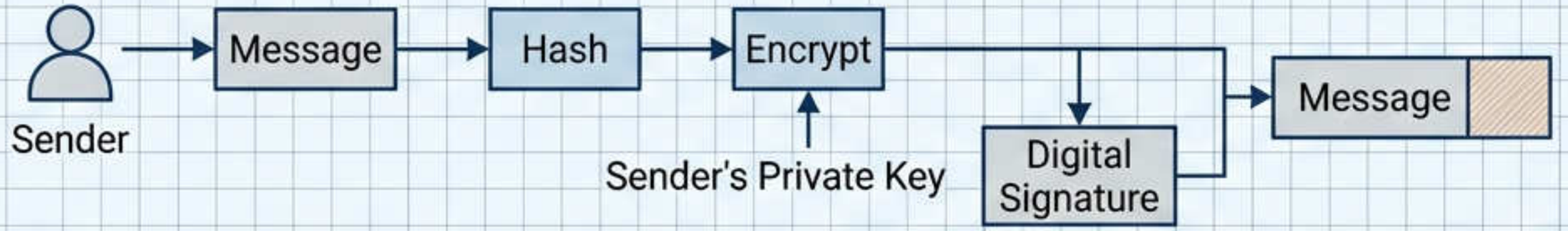
Toàn Vẹn Dữ Liệu và Chữ Ký Số

Hàm Băm (Hashing)



Thuật toán một chiều kiểm tra tính toàn vẹn (Integrity check).

Chữ Ký Số (Digital Signatures)



Đảm bảo 2 yếu tố:

- **Tính Toàn vẹn** (Integrity): Dữ liệu không bị sửa đổi.
- **Tính Không thể chối bỏ** (Nonrepudiation): Người gửi không thể phủ nhận.

Góc nhìn Rủi ro

Chữ ký số cung cấp bằng chứng pháp lý mạnh mẽ, thiết yếu cho giao dịch tài chính và hợp đồng điện tử.

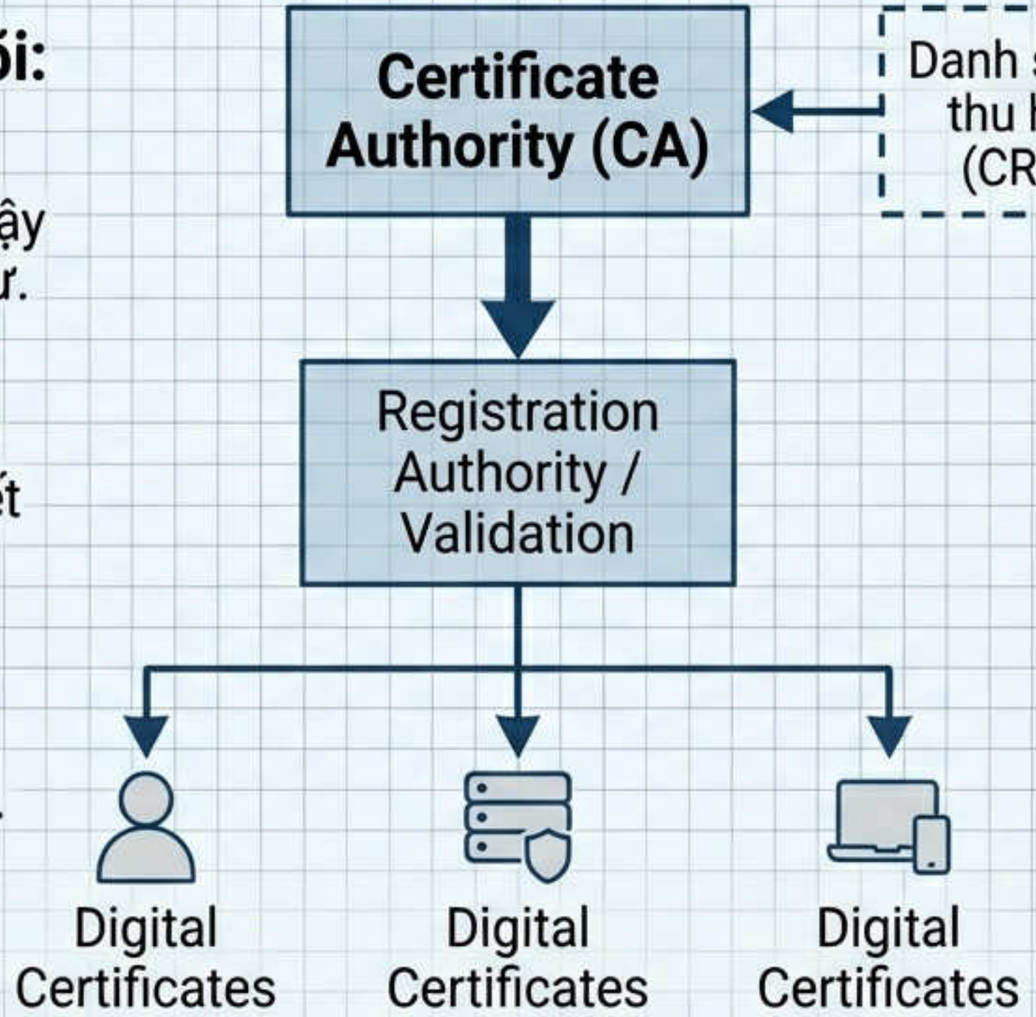
Hạ Tầng Khóa Công Khai (PKI)

Các khái niệm cốt lõi:

CA: Bên thứ ba tin cậy phát hành chứng thư.

Chứng thư số: "Căn cước" điện tử liên kết khóa công khai với danh tính.

CRL: Danh sách chứng thư bị hủy bỏ.



Góc nhìn Rủi ro

Quản lý Khóa (Key Management):

Nếu mất khóa riêng = Mất dữ liệu vĩnh viễn (Rủi ro Sẵn sàng).
Nếu lộ khóa riêng = Hệ thống sụp đổ (Rủi ro Bảo mật).

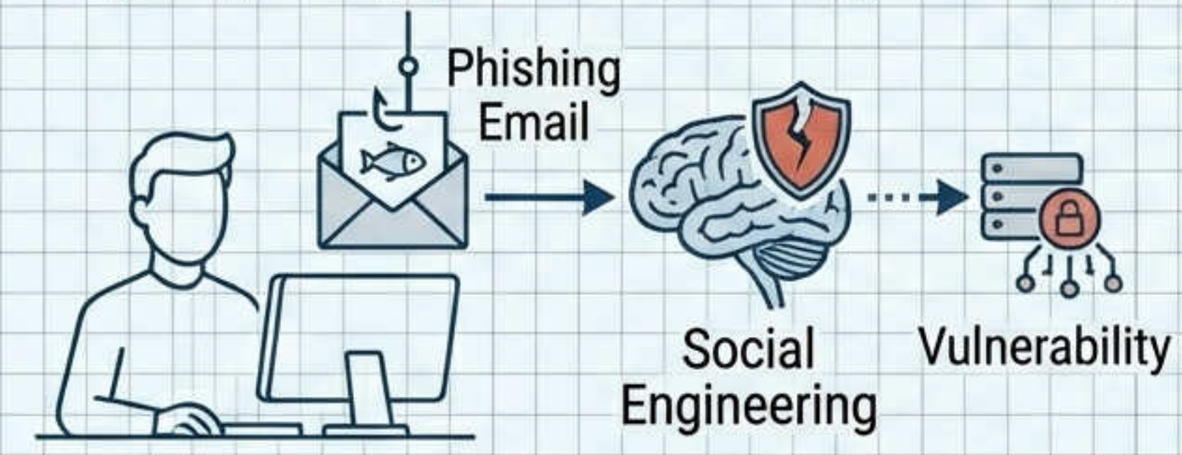
Date: 10:9 | YOESS AI

Yếu Tố Con Người: Nhận Thức và Đào Tạo

Mắt xích yếu nhất (The Weakest Link)

Kẻ tấn công chuyển hướng sang con người khi công nghệ trở nên khó xuyên thủng.

- Kỹ thuật xã hội (Social Engineering) / Phishing.



Mục tiêu Đào tạo

- Thay đổi hành vi, không chỉ cung cấp lý thuyết.
- Nhận diện dấu hiệu lừa đảo.
- Xây dựng "Bức tường lửa con người" (Human Firewall).

Human Firewall

Góc nhìn Rủi ro

Sự thiếu hiểu biết của nhân viên là một lỗ hổng bảo mật không thể vá bằng phần mềm.

Quyền Riêng Tư Dữ Liệu: Giới Hạn Mới

Confidentiality (Bảo mật)

Bảo vệ dữ liệu khỏi truy cập trái phép.

Privacy (Riêng tư)

Quyền của chủ thể (Data Subject) kiểm soát cách thông tin của họ được sử dụng.

Góc nhìn Rủi ro

Vi phạm quyền riêng tư mang lại rủi ro pháp lý khổng lồ

(Ví dụ: Phạt tới 4% doanh thu toàn cầu thio theo GDPR).

Nguyên tắc Cốt lõi (GDPR)

Tính minh bạch (Transparency)

Giới hạn mục đích (Purpose Limitation)

Tối thiểu hóa dữ liệu (Data Minimization)

Date: 10:9 YOESS AI

Cơ Chế Bảo Vệ Quyền Riêng Tư

Sự Đồng Thuận (Informed Consent)

Chủ thể phải đồng ý rõ ràng và có quyền rút lại đồng thuận.

Đánh Giá Tác Động (PIA)

Xác định rủi ro riêng tư trước khi thu thập dữ liệu mới.

Tối thiểu hóa (Minimization)

Chỉ thu thập dữ liệu thực sự cần thiết cho mục đích.

Hủy Dữ Liệu (Destruction)

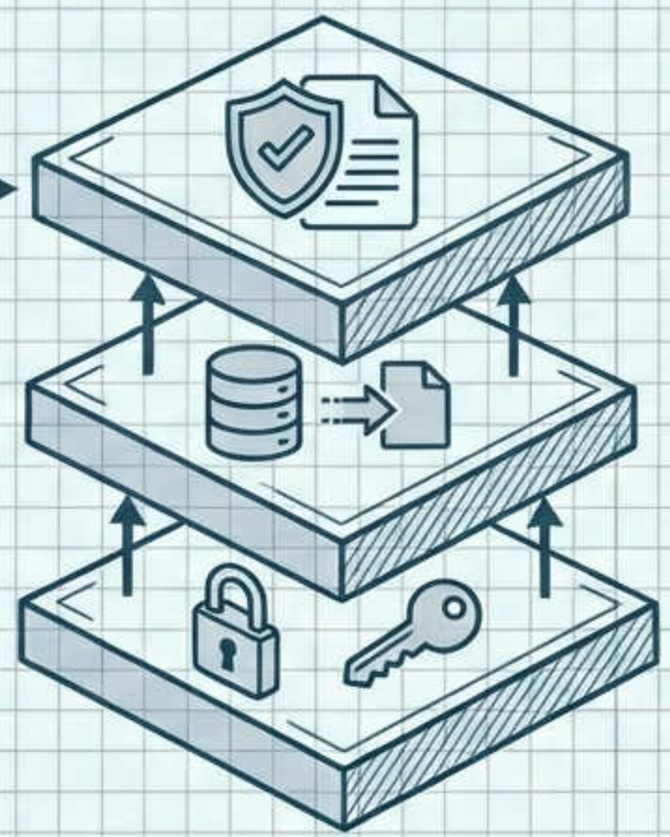
Hủy an toàn khi không còn cần thiết.

Góc nhìn Rủi ro

Dữ liệu là tài sản, nhưng lưu trữ dữ liệu không cần thiết biến nó thành tiêu sản (liability) và tăng bề mặt tấn công.

Date: 10:9 YOESS AI

Quản Lý Rủi Ro Trong Bối Cảnh Quyền Riêng Tư



Privacy Compliance (Tuân thủ)

Data at Rest & Data in Transit Protection

Bực ("Tích thảm")

Encryption & Access Control

Góc nhìn Rủi ro

Rủi ro tuân thủ là biến số động.

Các quy định pháp luật thay đổi liên tục theo khu vực địa lý.

Tích hợp: Áp dụng kiểm soát an ninh để bảo vệ quyền riêng tư.

Vai trò: Tham vấn Chuyên gia Quyền riêng tư (Privacy Officer) hoặc Pháp chế.

Date: 10:9 | YOESS AI

Tổng Hợp Dành Cho Chuyên Gia Rủi Ro

01. Cân bằng CIA: An ninh là sự cân bằng, không phải tuyệt đối.

02. Mã hóa: Công cụ mạnh mẽ nhưng tốn kém tài nguyên và phức tạp quản lý.

03. Con người: Đào tạo là bắt buộc để vá 'lỗ hổng con người'.

04. Quyền riêng tư: Yếu tố sống còn, không chỉ là tuân thủ pháp lý.

Rủi ro CNTT phải được quản lý để hỗ trợ mục tiêu kinh doanh, không phải để cản trở nó.

Date: 10:9 | YOESS AI

Đạo Đức Nghề Nghiệp & Bước Tiếp Theo

Đạo Đức Nghề Nghiệp ISACA

Khách quan & Cẩn trọng: Thực hiện nhiệm vụ chuyên nghiệp (Due diligence).

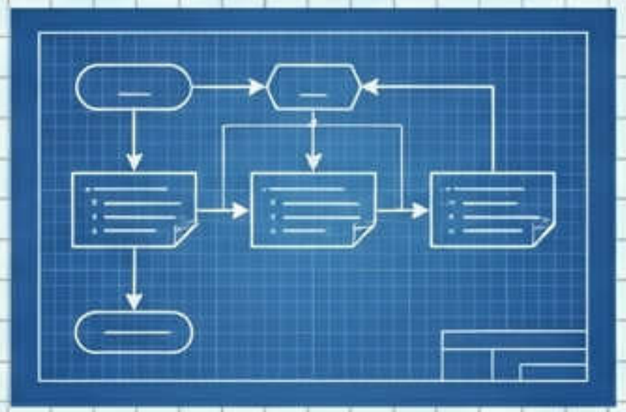
Bảo mật: Bảo vệ thông tin thu được trong quá trình làm việc.

Năng lực: Duy trì học tập liên tục.

ISACA / CRISC

Bước Tiếp Theo

Áp dụng kiến thức Chương 4 vào xác định **Kịch bản Rủi ro** (Risk Scenarios).



Date: 10:9

YOESS AI