IT GOVERNANCE FRAMEWORK

Khung Kiểm soát CNTT Doanh nghiệp

Mô hình 3 Tuyến | 4 Tầng Framework | AI Governance

Three Lines | 10 Framework | AI Governance | Cân bằng Quản trị

Digital Leaders Community

Viết Phẩm - SS08 DLC

Agenda

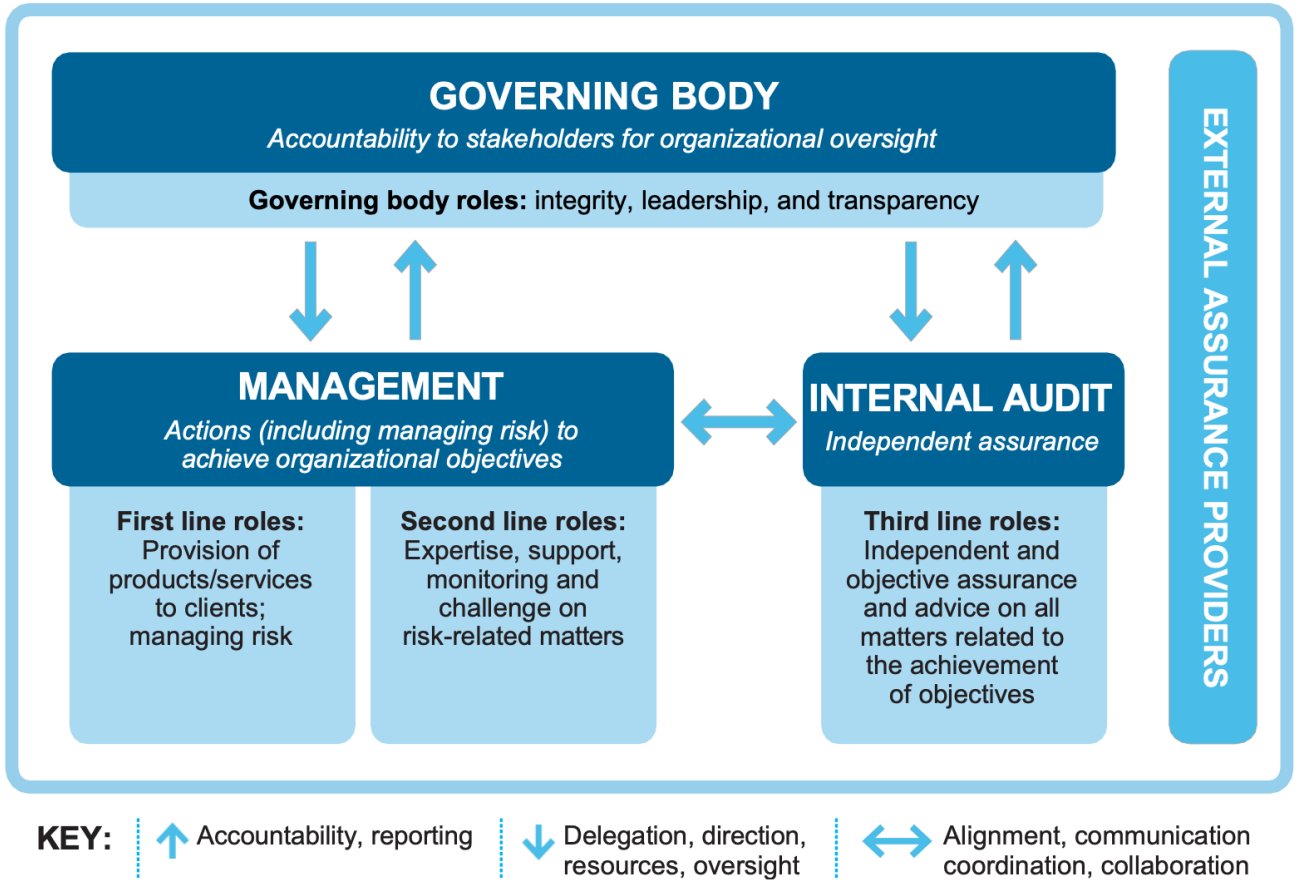
1. Mô hình 3 Tuyến kiểm soát (IIA 2020)
2. 4 Tầng IT Control + Risk Management
3. 4 Tầng Kiểm soát chi tiết (COSO, COBIT, ISO, NIST)
4. AI Governance Frameworks (ISO 42001, NIST AI RMF)
5. Tầng 4: Kiểm soát Kỹ thuật (5 Frameworks)
6. Kiểm soát vs Tốc độ — Cân bằng cho Quản trị
7. Key Takeaways + Q&A

PHẦN 1

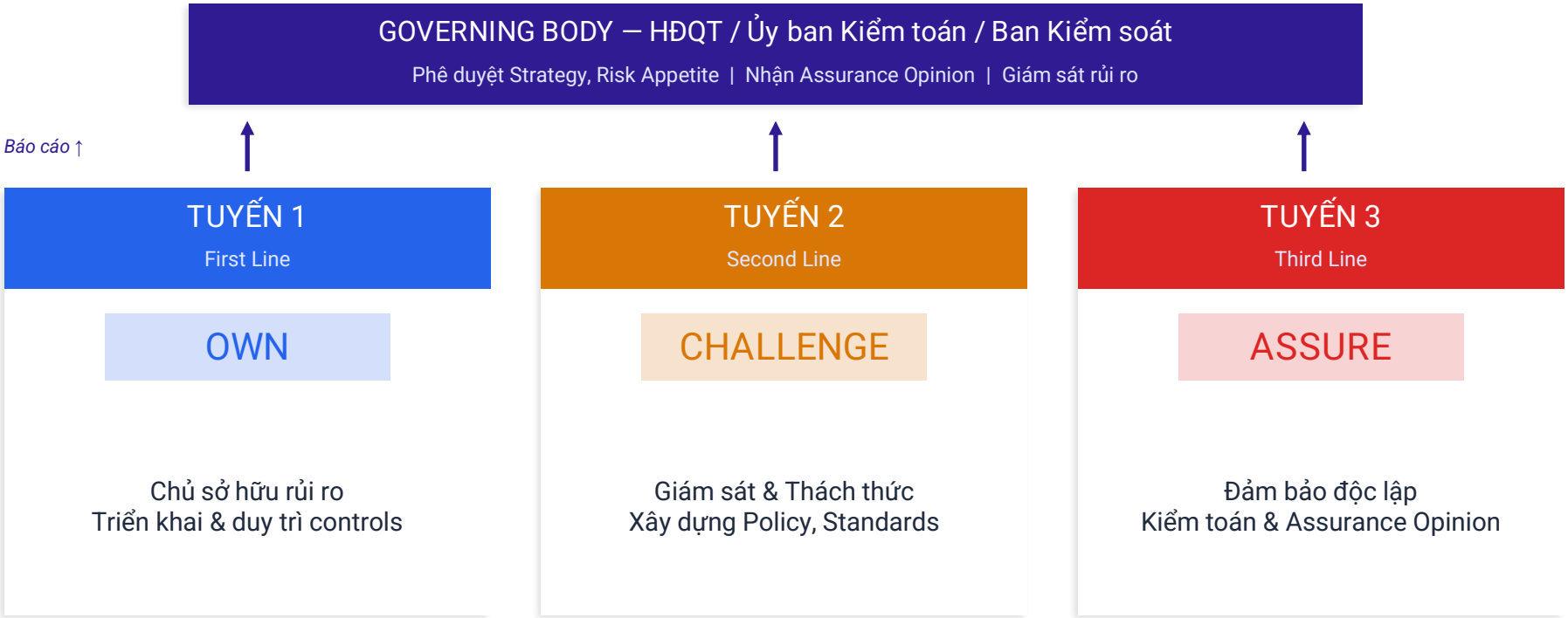
Mô hình 3 Tuyến kiểm soát

IIA 2020 — Ai làm gì? Ai giám sát? Ai đảm bảo?

Mô hình 3 Tuyến (IIA 2020) – Tổng quan



Mô hình 3 Tuyến (IIA 2020) — Tổng quan



Nguyên tắc: Phối hợp (Coordination) — không phải Phòng thủ (Defense)

Governing Body: HĐQT / Ủy ban Kiểm toán / Ban Kiểm soát

Vai trò chính

Phê duyệt IT Strategy & Digital Transformation
Phê duyệt IT Risk Appetite, AI Policy
Giám sát rủi ro CNTT/ATTT qua báo cáo
Quyết định go/no-go cho high-risk IT projects

Ủy ban Kiểm toán / Ban Kiểm soát

Phê duyệt kế hoạch kiểm toán nội bộ
Nhận báo cáo trực tiếp từ KTNB
Rà soát findings nghiêm trọng
Đánh giá hiệu quả 3 Tuyến

Governing Body trong thực tế IT

Không cần hiểu kỹ thuật — nhưng cần hiểu RỦI RO. HĐQT không cần biết firewall rule, nhưng cần biết tổ chức có bao nhiêu sự cố an ninh, risk appetite có bị vượt, AI có tuân thủ luật.

IT phải báo cáo bằng ngôn ngữ kinh doanh — không phải thuật ngữ kỹ thuật. Thay vì 'patch compliance 92%', nói '8% hệ thống có lỗ hổng chưa vá, rủi ro bị tấn công tương đương X tỷ đồng thiệt hại'.

Tuyến 1 — First Line: Phòng ban nào? Làm gì?

Phòng ban: IT/Digital, DevOps/MLOps, Data Science, Business Units, HR, Facilities

IT Operations	Vận hành hệ thống 24/7, backup & restore, monitoring, patch management, job scheduling
IT Security / SOC	Triển khai firewall, EDR, SIEM, phát hiện sự cố, ứng phó ban đầu, vulnerability scanning
IT Development	Phát triển phần mềm theo Secure SDLC, code review, testing, triển khai production
Data Science / AI	Phát triển model AI, monitoring performance & drift, đảm bảo data quality, tài liệu hóa model
HR	Background check, đào tạo nhận thức bảo mật, thu hồi quyền khi nhân viên nghỉ việc
Business Units	Data owner, phê duyệt quyền truy cập, báo cáo sự cố, tham gia risk assessment

Nguyên tắc: OWN the risk — chịu trách nhiệm trực tiếp về rủi ro và kiểm soát trong phạm vi của mình

Tuyến 2 — Second Line: Phòng ban nào? Làm gì?

Phòng ban: CISO/ATTT, Risk Management, Compliance, Legal, DPO, Model Validation

CISO / ATTT	Xây dựng Security Policy & Standards, thiết kế kiến trúc bảo mật, thách thức IT về security posture
Risk Management	Duy trì IT Risk Register, giám sát Risk Appetite, theo dõi KRI, báo cáo rủi ro cho Board
Compliance	Giám sát tuân thủ quy định: TT 09/NHNN, NĐ 13/2023, Luật ANMM
DPO (Data Protection)	Bảo vệ dữ liệu cá nhân: DPIA, quản lý đồng ý, quyền chủ thể dữ liệu, chuyển dữ liệu xuyên biên giới
Model Validation	Thẩm định ĐỘC LẬP mô hình AI/Credit Scoring — kiểm tra bias, accuracy, fairness, stability

Nguyên tắc: THÁCH THỨC Tuyến 1 — không chỉ nhận báo cáo mà phải challenge và đặt câu hỏi

Tuyến 3 — Third Line: Kiểm toán Nội bộ

Vai trò

Kiểm toán ĐỘC LẬP: ITGC, ISMS, cybersecurity
Đánh giá hiệu quả CẢ Tuyến 1 VÀ Tuyến 2
Annual IT Assurance Opinion cho HĐQT
Thematic: AI governance, cloud, ransomware
Follow-up findings, escalation khi chậm trễ

Đặc điểm then chốt

KHÔNG tham gia triển khai hay vận hành
Báo cáo TRỰC TIẾP cho Ủy ban Kiểm toán
Đánh giá cả Tuyến 2 (CISO, Risk)
Kết hợp assurance (combined assurance)
Risk-based: tập trung vào rủi ro cao nhất

KTNB là Partner — cùng hướng đến mục tiêu chung

Chung mục tiêu — bảo vệ tổ chức khỏi rủi ro, nâng cao hiệu quả. KTNB không phải 'police'.
Hiểu KTNB đánh giá gì giúp IT team chuẩn bị tốt hơn, tự phát hiện vấn đề sớm.
Combined assurance = IT tự kiểm tra (Line 1) + CISO rà soát (Line 2) + KTNB confirm (Line 3) → tiết kiệm effort, tránh trùng lặp.
Phối hợp sớm với KTNB trong major projects → tránh surprise, giảm rework.

Ví dụ thực tế: 3 Tuyến cho Vulnerability Management

Tuyến 1 — IT Security

Triển khai vulnerability scanner (Nessus/Qualys), chạy scan hàng tuần
Quản lý patch lifecycle: identify → test → deploy → verify
Duy trì SLA: Critical 48h, High 7d, Medium 30d
Khi không thể patch: document exception + compensating controls

Tuyến 2 — CISO / Risk

Thiết lập Vulnerability Policy và Patch SLA standards
Rà soát kết quả scan: coverage đủ? gaps nào? trends?
Giám sát patch compliance rate — escalate khi dưới threshold
Báo cáo vulnerability posture cho Risk Committee

Tuyến 3 — KTNB

Đánh giá: VM process có hoạt động đúng thiết kế?
Kiểm tra: SLA có được tuân thủ? Exception có justified?
Báo cáo findings & recommendations cho Ủy ban Kiểm toán
Follow-up: remediation đúng hạn?

Ví dụ thực tế: 3 Tuyến cho AI / Model Risk

Tuyến 1 — Data Science / IT

Phát triển AI model (credit scoring, fraud detection, chatbot)
Monitoring: accuracy, drift, degradation qua thời gian
Dữ liệu training: quality, bias check, representativeness
Model documentation: mục đích, limitations, data sources

Tuyến 2 — Model Validation / Risk

Thẩm định ĐỘC LẬP: test bias, fairness, accuracy vs benchmark
Rà soát model documentation: đầy đủ? giải thích được?
Giám sát model governance: AI Impact Assessment done?
Challenge: human oversight đủ chưa? Audit trail có?

Tuyến 3 — KTNB

Kiểm toán AI Governance process (không phải model)
Đánh giá: AI inventory đầy đủ? Model Validation độc lập?
Kiểm tra: compliance với AI frameworks, timeline
Báo cáo AI risk posture cho Ủy ban Kiểm toán

PHẦN 2

4 Tầng IT Control Framework

Enterprise Governance → IT Governance → InfoSec → Technical Controls

Kiến trúc 4 Tầng Kiểm soát CNTT

Tầng trên DEFINE → Tầng dưới IMPLEMENT. Mỗi tầng BỔ SUNG chi tiết, không thay thế.

Risk Management — Hiểu về Quản lý Rủi ro

Risk Management là quy trình nhận diện, đánh giá, xử lý và giám sát các sự kiện có thể ảnh hưởng đến mục tiêu tổ chức. Trong CNTT: cyber attack, data breach, system outage, vendor failure, AI bias.

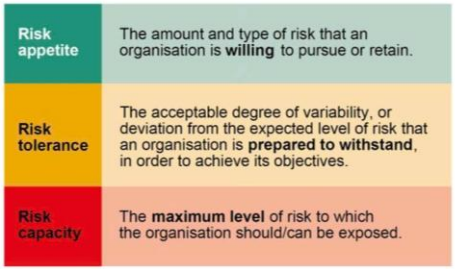
1. Bối cảnh	2. Nhận diện	3. Phân tích	4. Đánh giá	5. Xử lý	6. Giám sát
Phạm vi, mục tiêu, tiêu chí rủi ro	Liệt kê: cyber, data, vendor, AI, ops	Likelihood × Impact (thang 1-5 × 1-5)	So vs Risk Appetite → ưu tiên hóa	Accept / Avoid / Reduce / Transfer	KRI, review, cập nhật liên tục

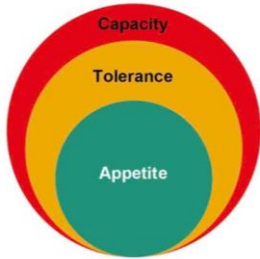
Risk Matrix (Heat Map)

	Thấp	TB	Cao
Cao	TB	Cao	Nghiêm trọng
TB	Thấp	TB	Cao
Thấp	Thấp	Thấp	TB

Khái niệm then chốt

- **Risk Appetite** — Mức rủi ro tổ chức SẴN SÀNG chấp nhận — HĐQT phê duyệt
- **Risk Tolerance** — Biên độ chấp nhận XUNG QUANH risk appetite
- **Inherent Risk** — Rủi ro TRƯỚC KHI áp dụng controls
- **Residual Risk** — Rủi ro SAU KHI controls hoạt động → phải ≤ tolerance
- **KRI** — Key Risk Indicator — chỉ số cảnh báo sớm, monitor liên tục





Tầng 1 — COSO ICIF 2013: The COSO Cube

5 Components × 3 Objectives × Entity Structure = KSNB 3 chiều

Ý nghĩa 3 chiều của COSO Cube

Chiều 1: Objectives (3)

Mỗi control phục vụ ít nhất 1 trong:
Operations, Reporting, hoặc Compliance

Chiều 2: Components (5)

5 Components hoạt động TÍCH HỢP:
Môi trường KS → Rủi ro → Hoạt động KS → Thông tin → Giám sát (17 Principles)

Chiều 3: Entity Structure

KSNB áp dụng ở MỌI CẤP:
Entity Level, Division,
Operating Unit, Function

COSO = NỀN TẢNG. COBIT (Tầng 2) nằm trong COSO. ISO 27001 (Tầng 3) reference COSO cho risk. Mọi framework đều cần governance foundation.

Tầng 2 — COBIT 2019: Quản trị CNTT

Cầu nối giữa Business Governance (COSO) và IT Operations (ISO 27001/NIST)

EDM	APO	BAI	DSS	MEA
5 Objectives	14 Objectives	11 Objectives	6 Objectives	4 Objectives
Evaluate, Direct, Monitor	Align, Plan, Organize	Build, Acquire, Implement	Deliver, Service, Support	Monitor, Evaluate, Assess
HĐQT/IT Committee chỉ đạo, giám sát	*Chiến lược, risk, vendor, security, HR*	*SDLC, change, project, config*	*Ops, incident, BCP, security svc*	*Performance, compliance, audit*

Đặc điểm nổi bật của COBIT 2019:

Governance vs Management: EDM = HĐQT chỉ đạo; APO/BAI/DSS/MEA = Ban ĐH thực hiện
Tách biệt rõ: ai quyết định (governance) và ai vận hành (management) — tránh conflict of interest
IT cho Business: 40 objectives đều hướng tới tạo giá trị cho kinh doanh, không phải IT-for-IT

Tầng 3 — ISO/IEC 27001:2022: ISMS

Certifiable • 93 Controls Annex A • 4 Themes • 11 Controls MỚI 2022

Organizational
37 controls

Policies, roles, SoD, threat intel (NEW), asset inventory, access control, vendor, cloud (NEW), incident, BCM, ICT readiness (NEW), privacy

People
8 controls

Screening, employment terms, awareness training, disciplinary, remote working, event reporting

Physical
14 controls

Perimeters, entry, monitoring (NEW), environmental, secure disposal, clear desk, equipment, cabling

Technological
34 controls

Endpoints, privileged access, MFA, vuln mgmt, logging, monitoring (NEW), secure SDLC, DLP (NEW), masking (NEW), encryption, network, web filter (NEW)

Đặc điểm nổi bật:

Certifiable: Chứng nhận ISO 27001 được khách hàng, đối tác, và cơ quan quản lý công nhận toàn cầu
PDCA Cycle: Plan → Do → Check → Act — cải tiến liên tục, không phải 'set and forget'
2022 Update: 11 controls mới phản ánh cloud, DLP, monitoring, secure coding — IT hiện đại phải update

Tầng 3 — NIST CSF 2.0: 6 Functions

Risk-based • Flexible • 6 Functions (MỚI: Govern) • 22 Categories • 106 Subcategories

GV	ID	PR	DE	RS	RC
Govern	Identify	Protect	Detect	Respond	Recover
Strategy, policy, roles, oversight, supply chain RM	Assets, risk assessment, improvement	IAM, data security, platform, training, infra resilience	Continuous monitoring, adverse event analysis	IR management, analysis, mitigation, communication	Recovery planning, execution, communication

Đặc điểm nổi bật:

Govern (MỚI): CSF 2.0 thêm Govern function — nhấn mạnh cybersecurity là trách nhiệm HĐQT, không chỉ IT
Not prescriptive: CSF nói 'cần gì' (WHAT), không nói 'làm thế nào' (HOW) — linh hoạt cho mọi tổ chức
Supply Chain RM: GV.SC có 10 subcategories riêng cho vendor/supply chain — phản ánh xu hướng third-party risk
Bổ sung ISO 27001: ISO 27001 = certifiable ISMS. NIST CSF = risk-based overlay. Hai framework dùng song song hiệu quả nhất

PHẦN 4

AI Governance Frameworks

ISO 42001, NIST AI RMF — Tầng mới xuyên suốt 4 tầng kiểm soát

Bức tranh toàn cảnh AI Governance Frameworks

Framework	Tổ chức	Đặc điểm chính	Certifiable?
ISO/IEC 42001:2023	ISO	AI Management System — tương tự ISO 27001 cho AI	CÓ
NIST AI RMF 1.0	NIST (Mỹ)	4 Functions: Govern → Map → Measure → Manage	Không
EU AI Act	EU	4 mức rủi ro, quy định pháp lý bắt buộc trong EU	Bắt buộc
OECD AI Principles	OECD	5+5 nguyên tắc AI có trách nhiệm — tham chiếu toàn cầu	Không
ISO/IEC 23894:2023	ISO	Hướng dẫn QLRR cho AI — mở rộng ISO 31000	Không

Trend quan trọng cho IT Expert:

AI governance KHÔNG tách biệt IT governance — nó TÍCH HỢP vào 4 tầng hiện có
ISO 42001 + ISO 27001 = shared controls (risk assessment, monitoring, incident) → triển khai cùng lúc hiệu quả
Xu hướng toàn cầu: các quốc gia (EU, Mỹ, VN, Sing, Nhật) đều đang xây dựng khung pháp lý cho AI
Nếu team bạn phát triển hoặc sử dụng AI → AI governance framework là BẮT BUỘC, không phải 'nice to have'

ISO/IEC 42001:2023 — AI Management System (AIMS)

Đặc điểm

Hệ thống quản lý AI (AIMS) — certifiable
10 Clauses, 38 controls, 9 domains
Tích hợp với ISO 27001 (shared structure)
Áp dụng cho cả AI provider VÀ AI user
PDCA cycle: Plan → Do → Check → Act

Domains chính (9)

AI Policy & nguyên tắc đạo đức
AI Risk Assessment: bias, fairness, safety
AI Impact Assessment: tác động cá nhân/XH
Data for AI: quality, representativeness
AI Lifecycle: design → develop → deploy → monitor
Human oversight: human-in-the-loop

Áp dụng vào 4 Tầng IT Control

Tầng 1 (COSO): AI Risk Appetite, AI Ethics Committee — governance decisions ảnh hưởng cách phát triển AI
Tầng 2 (COBIT): Innovation governance (PoC trước production), AI trong IT Risk Register, Training data trong Data Management
Tầng 3 (ISO 27001): AIMS + ISMS shared controls — nếu đã có ISO 27001, triển khai 42001 nhanh hơn 50%
Tầng 4 (Technical): Model validation, bias testing, adversarial attacks, explainability mechanism, decision audit trail

NIST AI RMF 1.0 — 4 Functions quản lý rủi ro AI

GOVERN

Chiến lược AI, culture, accountability
AI risk management policy
Roles & responsibilities
Legal/regulatory compliance

MAP

Bối cảnh sử dụng AI
Intended purpose & boundaries
Stakeholder analysis
Risk factor identification

MEASURE

Đo lường bias, fairness, accuracy
Performance metrics
Data quality assessment
Reliability & robustness testing

MANAGE

Xử lý risks đã nhận diện
Model monitoring & drift detection
Incident response cho AI failures
Continuous improvement

NIST AI RMF vs ISO 42001: AI RMF = risk framework (voluntary, flexible). ISO 42001 = management system (certifiable, structured). Dùng song song: AI RMF cho risk methodology, ISO 42001 cho management system.

Cho IT Expert: AI RMF giúp team hiểu 'đo lường rủi ro AI thế nào'. Map function giúp document AI use cases. Measure function là checklist cho bias/fairness testing.

PHẦN 5

Tầng 4 — Kiểm soát Kỹ thuật

CIS Controls • NIST SP 800-53 • OWASP • PCI DSS • CSA CCM

Tầng 4 — 5 Frameworks Kỹ thuật

Biến chiến lược (Tầng 1-3) thành hành động kỹ thuật cụ thể

CIS Controls v8.1	NIST SP 800-53	OWASP	PCI DSS v4.0	CSA CCM v4
18 Controls, 153 Safeguards 3 Implementation Groups Prescriptive — nói chính xác PHẢI LÀM GÌ Dựa trên MITRE ATT&CK attack data Miễn phí, bắt đầu IG1 (56 safeguards)	20 Families, ~1.000 Controls Catalog gốc toàn diện nhất NIST CSF là bản tóm tắt bậc cao Federal standard, áp dụng toàn cầu Chi tiết: Access, Config, Incident, Integrity	Top 10 + ASVS + SAMM Chuyên biệt bảo mật ứng dụng Top 10: 10 rủi ro web phổ biến nhất ASVS: 3 levels verification cho apps SAMM: Maturity model cho AppSec	12 Requirements bảo vệ thẻ Bắt buộc cho tổ chức xử lý thẻ Certifiable (QSA audit) v4.0: MFA bắt buộc CDE, pw ≥12 chars ASV quarterly + pen test annual	17 Domains, 197+ Controls Cloud security chuyên biệt Certifiable (STAR Level 2) Shared responsibility model CAIQ cho vendor assessment

Chọn framework phù hợp: CIS IG1 (mọi TC) → thêm OWASP (nếu dev apps) → thêm PCI DSS (nếu xử lý thẻ) → thêm CSA CCM (nếu cloud) → SP 800-53 (nếu cần chi tiết toàn diện)

PHẦN 6

Kiểm soát IT vs Tốc độ

Khi nào gia tăng kiểm soát? Khi nào "thả lỏng" cho tốc độ phát triển?

Khi nào tăng kiểm soát? Khi nào ưu tiên tốc độ?

Câu hỏi đúng: "kiểm soát BAO NHIÊU cho RỦI RO NÀO?" — *không phải "kiểm soát hay tốc độ?"*

TĂNG KIỂM SOÁT

Rủi ro nội tại

PII/thẻ/tài chính • Core systems • AI rủi ro cao • Public-facing

Yếu tố bên ngoài

Quy định mới (TT 09, NĐ 13, AI laws) • Sau sự cố • Audit findings • M&A, IPO

Yếu tố nội bộ

Tăng trưởng nhanh → chuẩn hóa • Mở rộng quốc tế → đa quy định

ƯU TIÊN TỐC ĐỘ

Chiến lược

Startup/early stage • Cạnh tranh gay gắt • Digital Transformation • Sandbox, PoC

Bối cảnh

Hệ thống nội bộ, rủi ro thấp • Non-PII data • Test/dev tách biệt • User nhỏ, rollback dễ

Thực tế

Control quá chặt → shadow IT • Innovation bị kìm hãm • Time-to-market dài hơn ngành

Ma trận quyết định:

5 Nguyên tắc cân bằng — Dẫn nguồn Framework

Nguồn: ISO 31000:2018 + COBIT 2019 (ISACA) + IIA Three Lines Model 2020 + EU AI Act

1. Risk-Based Differentiation	Không kiểm soát đồng đều mọi hệ thống. Phân tầng theo criticality và rủi ro — mỗi tier mức kiểm soát khác nhau	ISO 31000 §5.4 + EU AI Act
2. Proportionality	Benefits + Risk + Resources phải cân bằng. Chi phí kiểm soát không vượt giá trị tài sản bảo vệ	COBIT 2019 P1 (Value Creation)
3. Business Enablement	Kiểm soát tồn tại để HỖ TRỢ kinh doanh. Control không giảm rủi ro đáng kể → loại bỏ	COBIT 2019 P2 (Holistic Approach)
4. Board-Level Decision	Risk Appetite do HĐQT phê duyệt — không phải CIO/CISO tự quyết. Governance ≠ Management	COBIT P5 + IIA 2020
5. Continuous Recalibration	Cân bằng không phải quyết định 1 lần. Review annual + recalibrate khi có thay đổi lớn	COBIT Dynamic + ISO 31000 §6.6

HĐQT thiết lập Risk Appetite → IT/CISO diễn giải thành controls → KTNB xác nhận cân bằng đúng với Risk Appetite

Key Takeaways

3 Tuyến = Accountability rõ ràng

Line 1 OWN risk → Line 2 CHALLENGE → Line 3 ASSURE. Hiểu vai trò để phối hợp hiệu quả.

4 Tầng bổ sung nhau

Governance → IT Mgmt → ATTT → Kỹ thuật. Không thể có ISO 27001 mà bỏ qua COSO.

AI Governance xuyên suốt

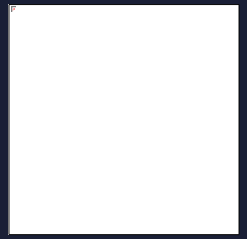
ISO 42001 + NIST AI RMF tích hợp vào 4 tầng hiện có. Không tách rời IT governance.

Cân bằng qua Risk Appetite

Kiểm soát BAO NHIÊU cho RỦI RO NÀO. HĐQT quyết định, IT triển khai, KTNB xác nhận.

Bắt đầu với CIS IG1

56 safeguards = minimum viable security. Miễn phí, prescriptive, bắt đầu ngay hôm nay.



Q&A

Thảo luận và Chia sẻ kinh nghiệm