แนะนำสายงานด้าน Cybersecurity และทักษะที่ควรมี

ดร.ศุภกร กังพิศดาร

CISSP, CISA, CISM, CDPSE, PECB ISO 27001 SLI, IRCA ISO27001 PA, PECB ISO 22301 PI, PECB ISO31000 RM, Security+, ITIL Foundation, CCISO, ECSA, CEH, CHFI, ENSA, ECES, CEI, CSCU, CCNA Instructor, CCNAS Instructor

กรรมการผู้จัดการ
บริษัท ไซเบอร์ อีลีท จำกัด

Dr.Supakorn Kungpisdan
Managing Director, Cyber Elite

- Executive CISO #1
- Chapter President, Cybersecurity & Governance Chapter, Thai CIO Association (TCIOA)
- Over 20 years of experience in cybersecurity as a consultant, researcher, system integrator, lecturer, and head of cybersecurity of leading organizations in various industries including banking and finance and defense sectors
- Cybersecurity advisor of government agencies in Thailand including Ministry of Justice, Department of Special Investigation, and National Security and Dual Use Technology Center
- Assistant Professor of Information Technology

Dr. Kungpisdan received Ph.D. in Computer Science and Software Engineering from Monash University, AUSTRALIA, in 2005.

100+ research publications in cybersecurity and applied cryptography

CISSP, CISA, CISM, CDPSE, PECB ISO 27001 SLI, IRCA ISO27001 PA, PECB ISO 22301 PI, PECB ISO31000 RM, Security+, ITIL Foundation, CCISO, ECSA, CEH, CHFI, ENSA, ECES, CEI, CSCU, CCNA Instructor, CCNAS Instructor

CYBER ELITE

"The Most Trusted and Supportive Cybersecurity Company"

We offer full range of end-to-end cybersecurity products and services, designed and tailer-made to fit each organization cybersecurity context and exposure

No "*one size fits all*" in cybersecurity

01
SECURITY SYSTEM INTEGRATION

02
MANAGED SECURITY SERVICES

03
SECURITY ADVISORY

04
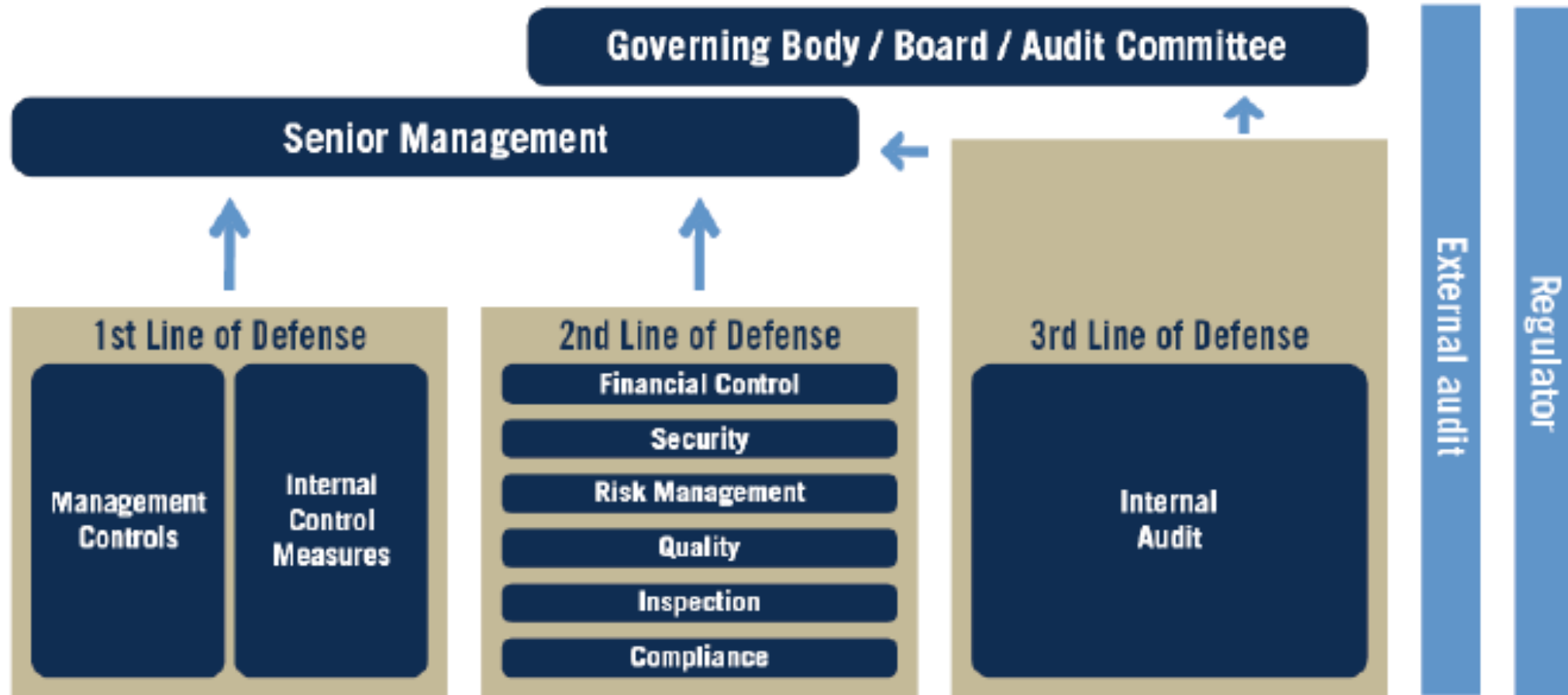TRAINING & AWARENESS

05
CYBERSECURITY PLATFORMS

CYBER ELITE
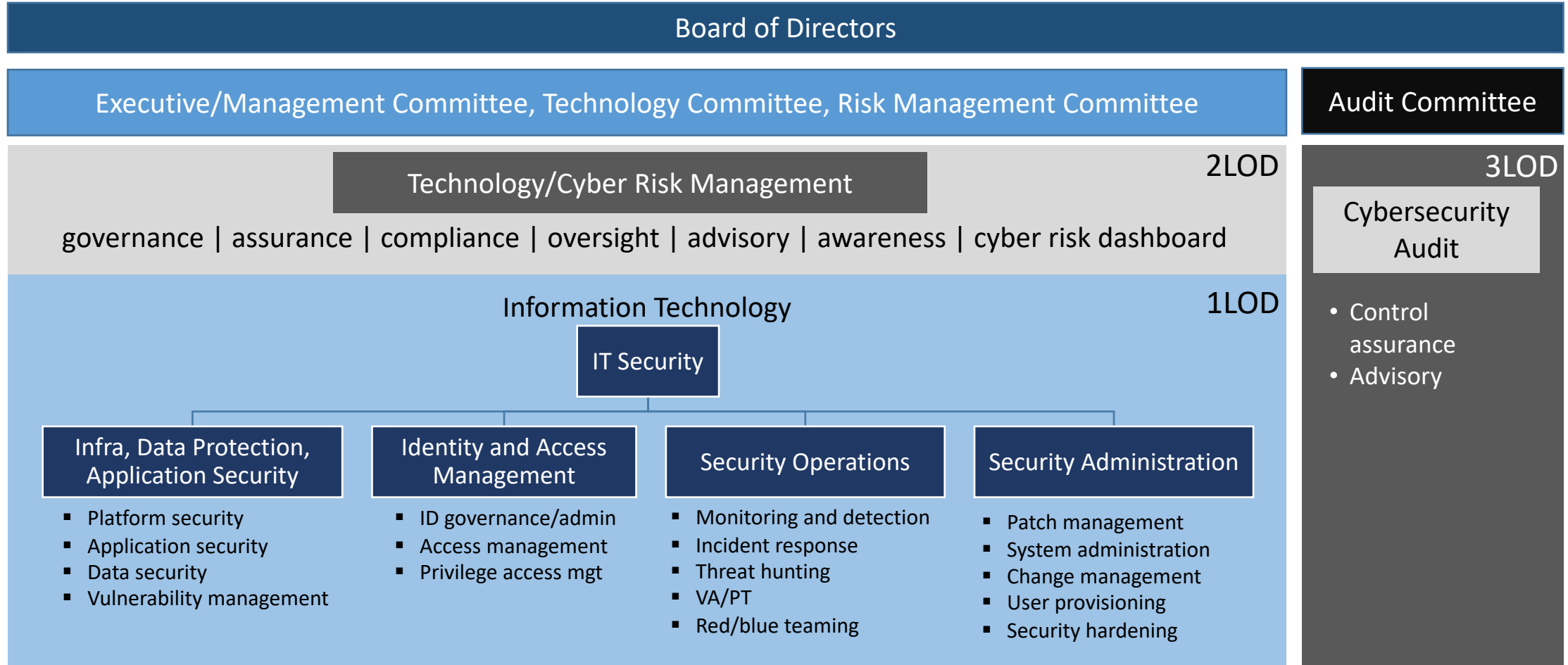
AGENDA

- สายงานอาชีพด้านไซเบอร์
- สายงานด้านไซเบอร์ภายในองค์กร (Cybersecurity roles in an enterprise)
- สายงานด้านไซเบอร์ภายในผู้ให้บริการ (Cybersecurity roles in SI/distributor/vendor)
- สายงานด้านไซเบอร์ภายในบริษัทที่ปรึกษา (Cybersecurity roles in a consulting firm)
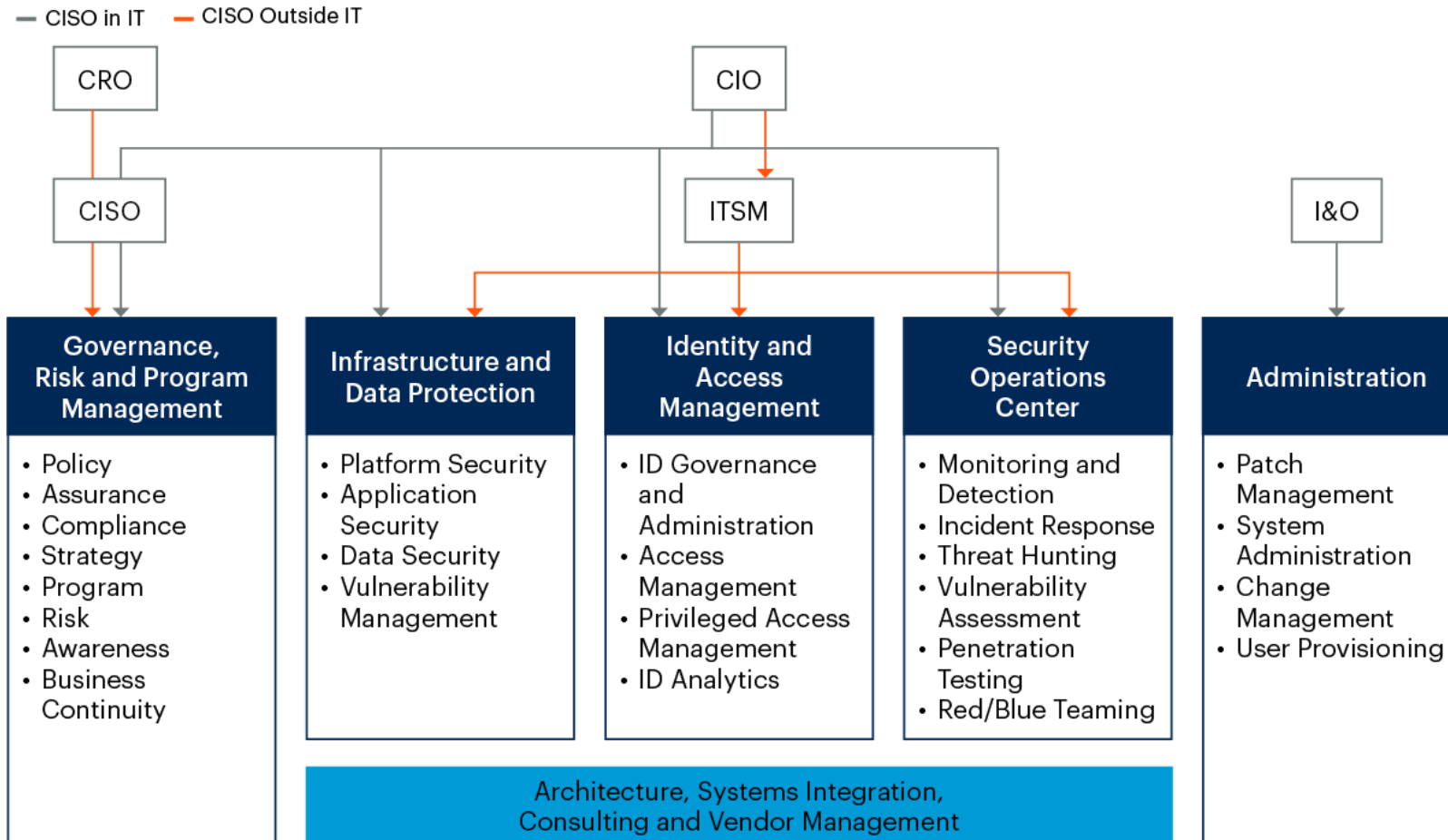- พื้นฐานด้านไซเบอร์ที่จำเป็น (Cybersecurity fundamental)
- บทสรุป

CYBER ELITE

3 Line of Defense Model

CYBER ELITE

Enterprise Cybersecurity Governance

Board of Directors

Executive/Management Committee, Technology Committee, Risk Management Committee

Audit Committee

2LOD

Technology/Cyber Risk Management

governance | assurance | compliance | oversight | advisory | awareness | cyber risk dashboard

3LOD

Cybersecurity Audit

- Control assurance
- Advisory

1LOD

Information Technology

IT Security

Infra, Data Protection, Application Security
- Platform security
- Application security
- Data security
- Vulnerability management

Identity and Access Management
- ID governance/admin
- Access management
- Privilege access mgt

Security Operations
- Monitoring and detection
- Incident response
- Threat hunting
- VA/PT
- Red/blue teaming

Security Administration
- Patch management
- System administration
- Change management
- User provisioning
- Security hardening

CYBER ELITE

Security Organization
Generic Centralized Model

— CISO in IT   — CISO Outside IT

CRO

CIO

CISO

ITSM

I&O

Governance, Risk and Program Management

- Policy
- Assurance
- Compliance
- Strategy
- Program
- Risk
- Awareness
- Business Continuity

Infrastructure and Data Protection

- Platform Security
- Application Security
- Data Security
- Vulnerability Management

Identity and Access Management

- ID Governance and Administration
- Access Management
- Privileged Access Management
- ID Analytics

Security Operations Center

- Monitoring and Detection
- Incident Response
- Threat Hunting
- Vulnerability Assessment
- Penetration Testing
- Red/Blue Teaming

Administration

- Patch Management
- System Administration
- Change Management
- User Provisioning

Architecture, Systems Integration, Consulting and Vendor Management

ITSM: IT Security Manager; **CRO:** Chief Risk Officer; **CIO:** Chief Information Officer;

CISO: Chief Information Security Officer; **I&O:** Infrastructure and Operations

REF: Gartner

CYBER ELITE

Cybersecurity Roles in An Enterprise

1LOD					2LOD	3LOD
Infrastructure and data protection	**Application security**	**Identity and access management**	**Security operations center**	**Security Infra & Operation administration**	**Governance, risk, and program management**	**Cybersecurity Audit**
• Infrastructure Security Engineer • Network Security Engineer • Cloud Security Professional • Security Advisory • Data Security Engineer	• Application Security Engineer • Security Advisory • Penetration Tester	• Security Administrator	• SOC Manager • Tier 1 SOC Analyst • Tier 2 SOC Analyst • SOC Engineer • SOC Administrator • Threat Intelligence Analyst • Security Analytics Professional • Security Consultant (VA/PT/DFIR)	• Security Administrator • Security Engineer • IT Security User Support	• Technology/ Cyber risk professional • Business Continuity Management Professional • Privacy Professional	• Cybersecurity Auditor

CYBER ELITE

System Integrator/Distributor/Vendor/Service Provider

Presales	Project Management	Product Management	Engineering	Managed Security Services	Product Development
• Presales Consultant • Security Solution Architect • Sales Engineer	• Project Manager • Project Coordinator	• Product Manager • Product Specialist	• Cybersecurity Engineer • Network Security Engineer • Cloud Security Engineer	• SOC Manager • Tier 1 SOC Analyst • Tier 2 SOC Analyst • SOC Engineer • SOC Administrator • Threat Intelligence Specialist • Security Analytics Professional • Security Consultant (VA/PT/DFIR) • Incident Responder • Malware analyst	• Developer • Cybersecurity Researcher • System Analyst

CYBER ELITE

Consulting Firm

Consulting	Risk Advisory	Security Audit	Project Management	Managed Services
• Security Architect • Security Consultant (VA/PT/DFIR) • Security Consultant (ISO/NIST) • Security Researcher	• Cyber Risk Consultant • Solution Consultant	• Cybersecurity Auditor	• Project Manager • Project Coordinator	• SOC Manager • Tier 1 SOC Analyst • Tier 2 SOC Analyst • SOC Engineer • SOC Administrator • Threat Intelligence Specialist • Security Analytics Professional • Security Consultant (VA/PT/DFIR) • Incident Responder

CYBER ELITE

พื้นฐานที่จำเป็นในการทำงานด้าน Cybersecurity

Computer networking	Operating systems	Programming and scripting	Cloud	DevOps
Cryptography	Data Security	Security controls and frameworks	Incident response	AI/ML
	Network security controls	Threat intelligence	Laws and regulatory requirements	

CYBER ELITE

Conclusion

- ศึกษาพื้นฐานด้านเทคโนโลยีสารสนเทศให้แน่น
- ฝึกฝนด้าน computer programming
- ฝึกฝนตนเองและฝึกปฏิบัติอย่างสม่ำเสมอ
- เข้าร่วมใน community ที่ตัวเองสนใจ
- หาความท้าทายใหม่ ๆ เช่น เข้าร่วมแข่ง hackathon, cybersecurity contest

CYBER ELITE

🏠 www.cyberelite.co

✉️ mkt@cyberelite.co

💬 @cyberelite

📞 094-480-4838

f Cyber Elite

in Cyber Elite

▶️ Cyber Elite