2nd Line

Communications

1st Line

3rd Line

HQ
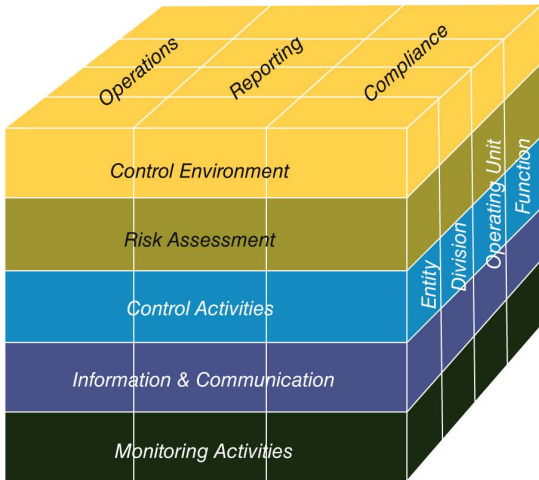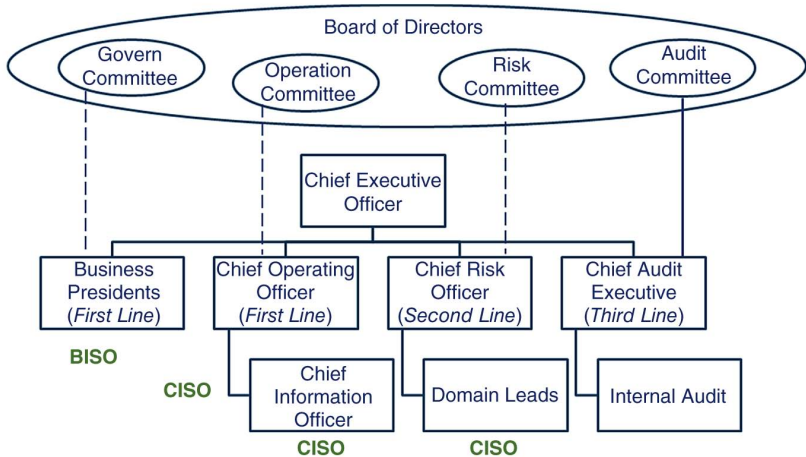
Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 8.1

Cybersecurity is a strategic business enabler

Understand the economic drivers and impact of cyber risk

Align cyber-risk management with business needs

Ensure organizational design supports cybersecurity

Incorporate cybersecurity expertise into board governance

Encourage systemic resilience and collaboration

Cyber-resilient organization
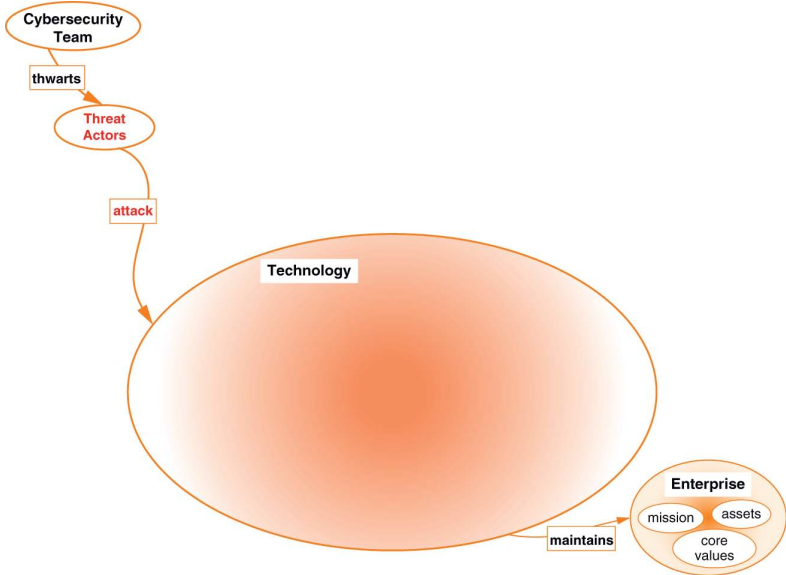
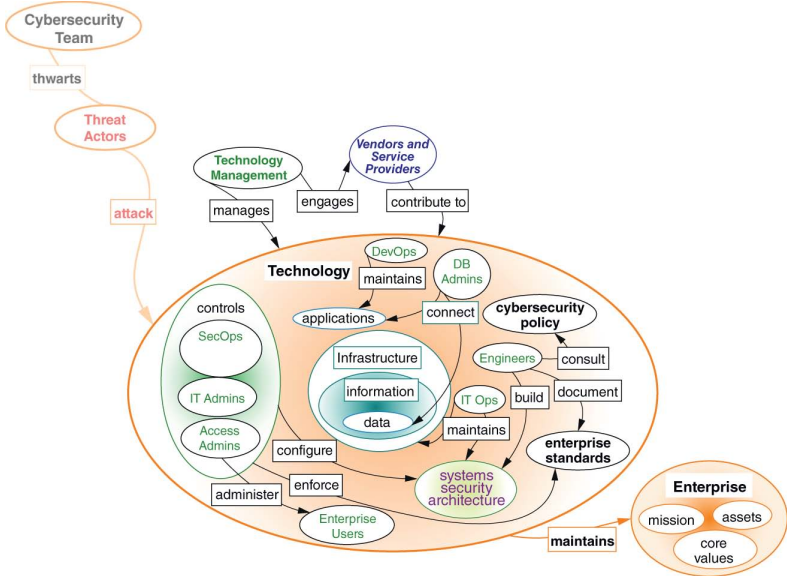Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 8.2

Operations   Reporting   Compliance

Control Environment

Risk Assessment

Control Activities

Information & Communication

Monitoring Activities

Entity   Division   Operating Unit   Function

See: https://www.coso.org/guidance-on-ic

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 8.3

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 8.4
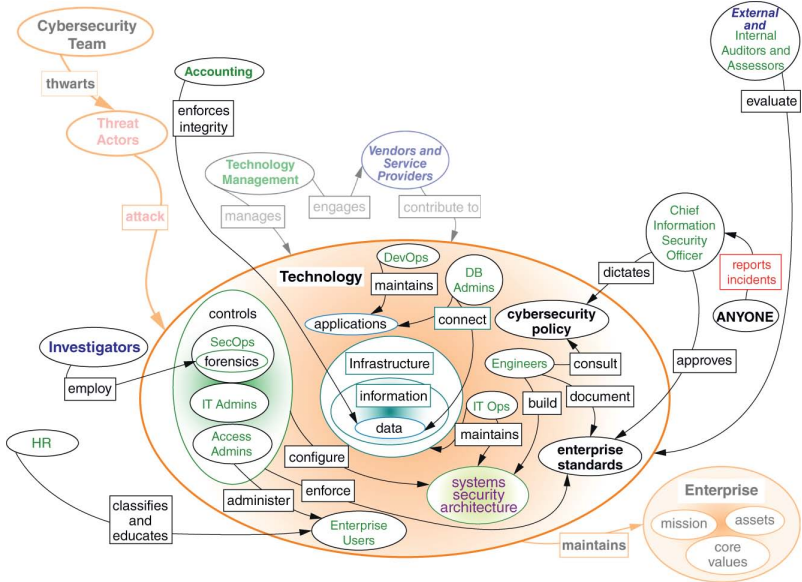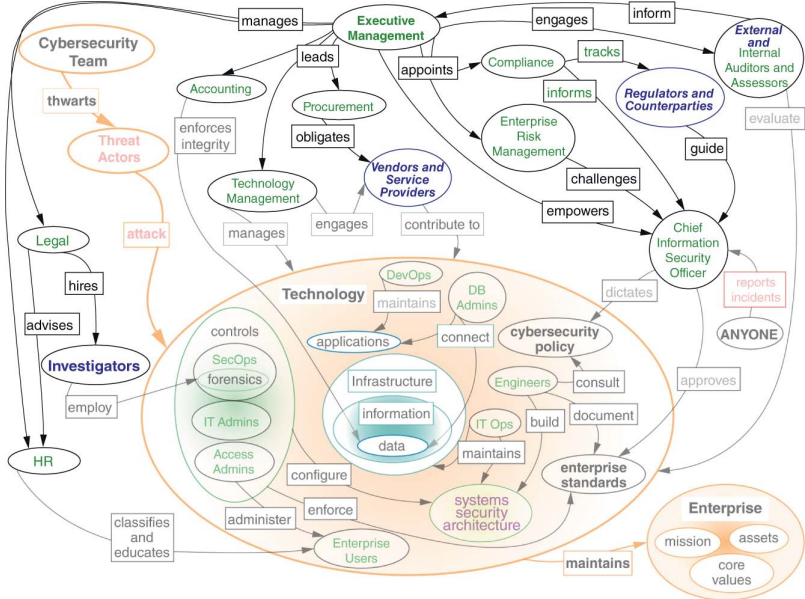
Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 8.5

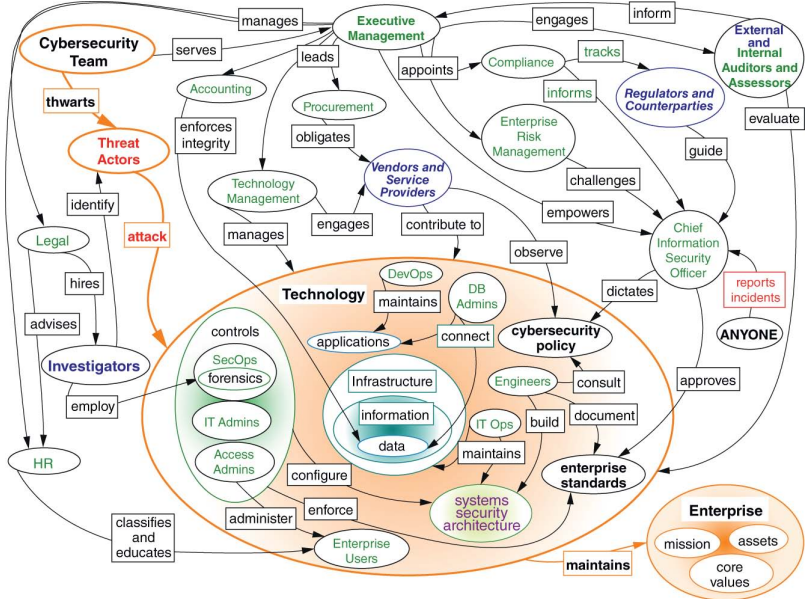Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 8.6

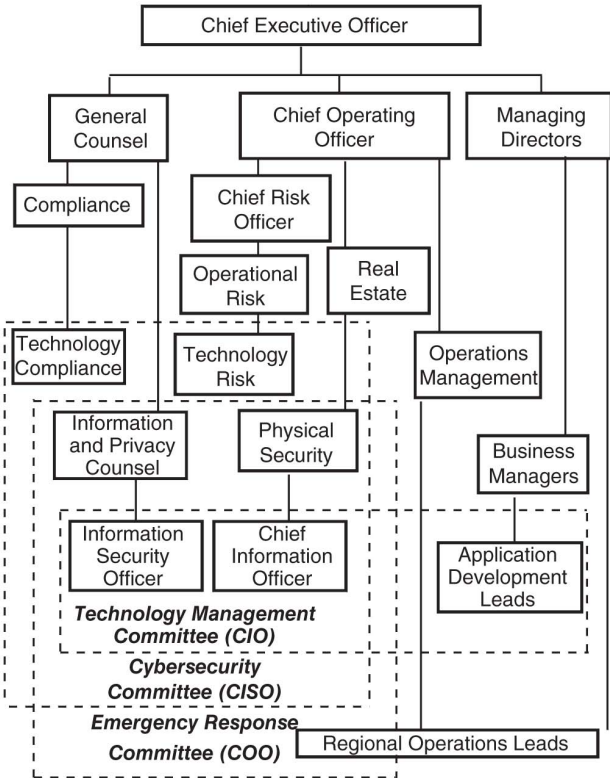Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 8.7

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 8.8

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 8.9

Chief Executive Officer

General Counsel

Compliance

Technology Compliance

Chief Operating Officer

Chief Risk Officer

Operational Risk

Real Estate

Technology Risk

Information and Privacy Counsel

Physical Security

Information Security Officer

Chief Information Officer

Technology Management Committee (CIO)

Cybersecurity Committee (CISO)

Emergency Response Committee (COO)

Managing Directors

Operations Management

Business Managers

Application Development Leads

Regional Operations Leads

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 8.10

Where a person performs this activity:	The person becomes an "owner" or "contact for the cybersecurity process for:	A sample responsibility is:
Order the development of a new business application	Security Review Participation	Security-policy-compliant systems configuration
	Security Requirements Capture	Sign off on business requirements for confidentiality, integrity, and availability
	Change Control	Acceptance testing for identification and entitlement in organization-maintained software
	Security Upgrade Management	Testing application integrity post security software fixes
Procures Commercial Off the Shelf (COTS) IT services	Security Requirements Capture	Formal requirements for security in all Requests for Product Information and Proposals
	Contract Requirements	Approval of business requirements for cybersecurity in information service provider and technology maintenance contracts

Source: Bayuk, Stepping Through Cybersecurity Risk Management, Figure 8.11