INFO 310

Fall 2016

Week 6 – Lecture 1

HOUSEKEEPING

- Attendance
- Position Paper I Return

Information Security Governance

- **Governance** broadly refers to the mechanisms, processes and relations by which organizations are controlled and directed. Governance structures and principles identify the distribution of rights and responsibilities among different participants in the organization and includes the rules and procedures for making decisions in organizational affairs.

WIKIPEDIA
The Free Encyclopedia

Why Governance?

Information Security Governance:

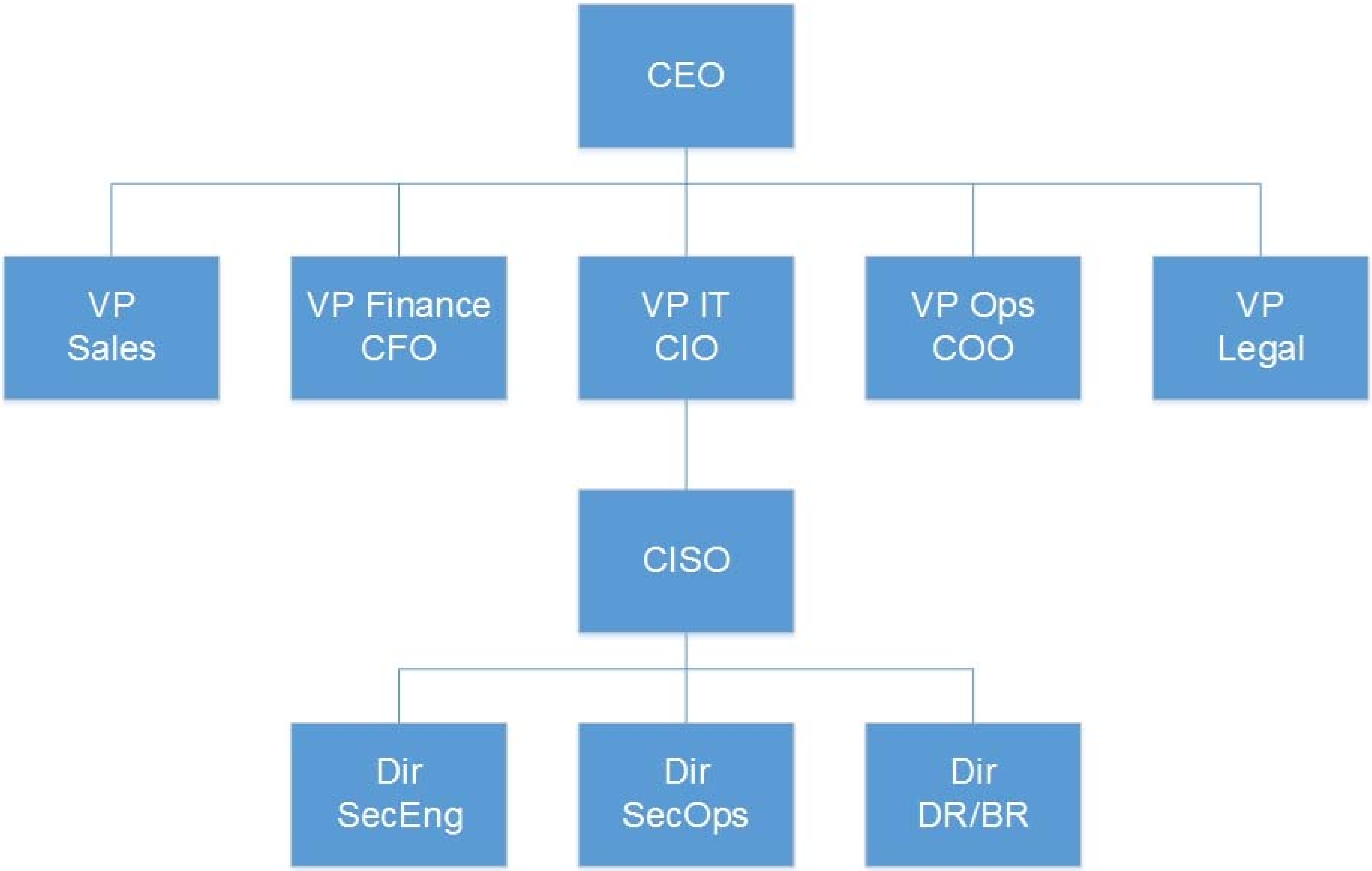
Guidance for Boards of Directors and Executive Management

2nd Edition

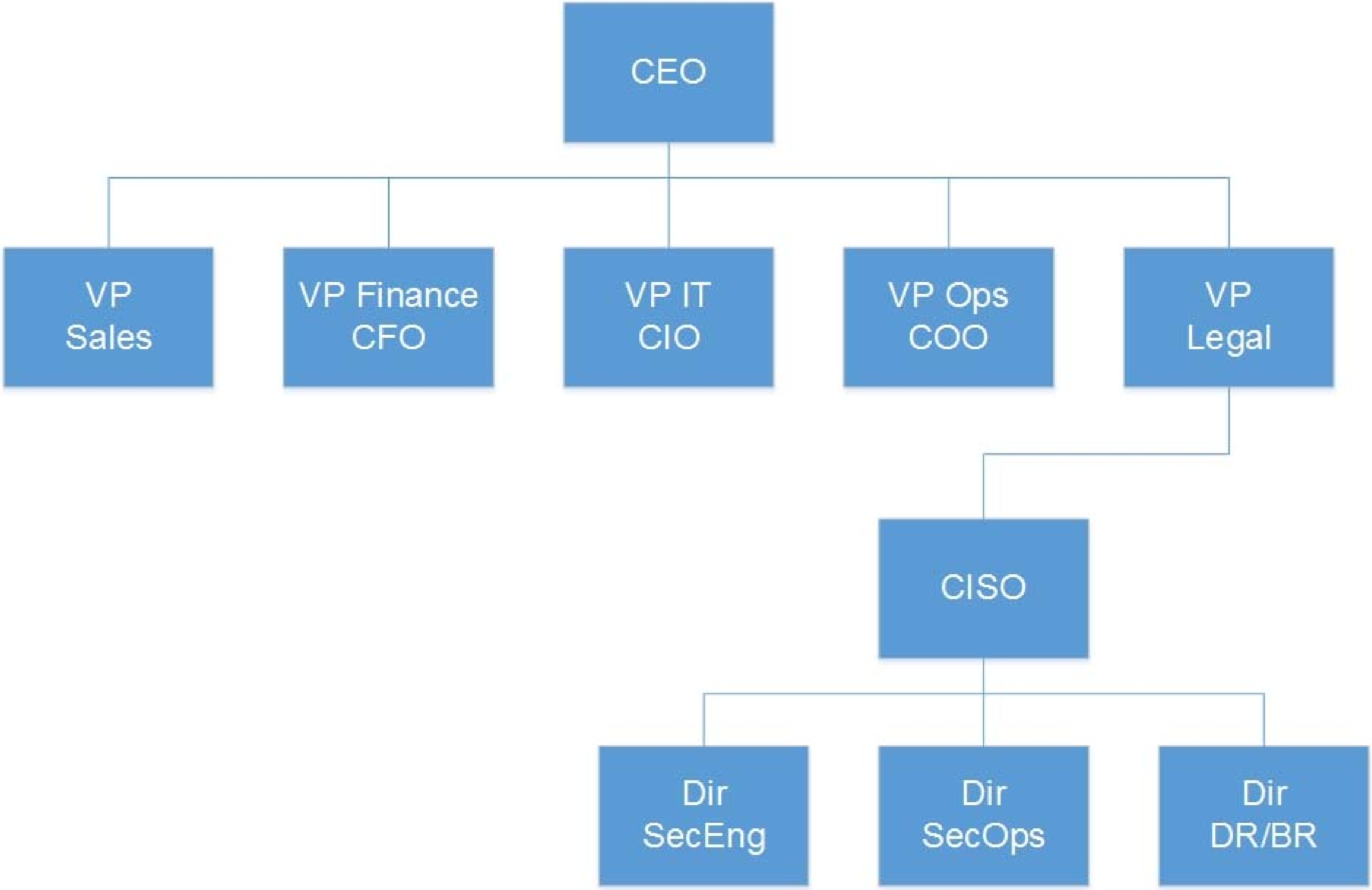
IT Governance Institute®

Leading the IT Governance Community

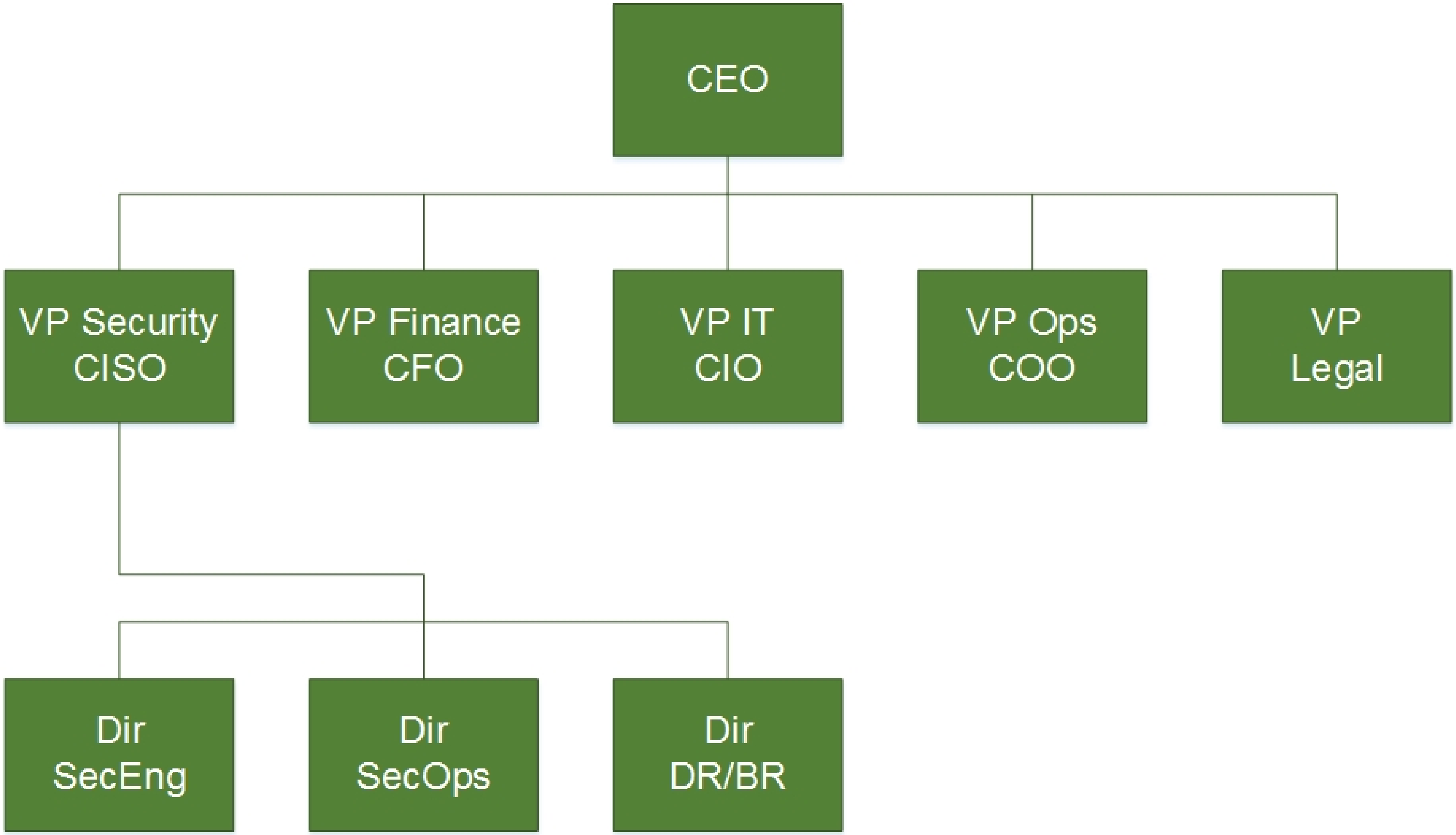
Typical Org Structure



Better Org Structure



“Best” (?) Org Structure



Good InfoSec Governance Needs:

- Executive Management Support
- Steering Committee
- Policy Authority
  - Policies
  - Standards
  - Guidelines
- Business Unit Support

A word about “Policy”…

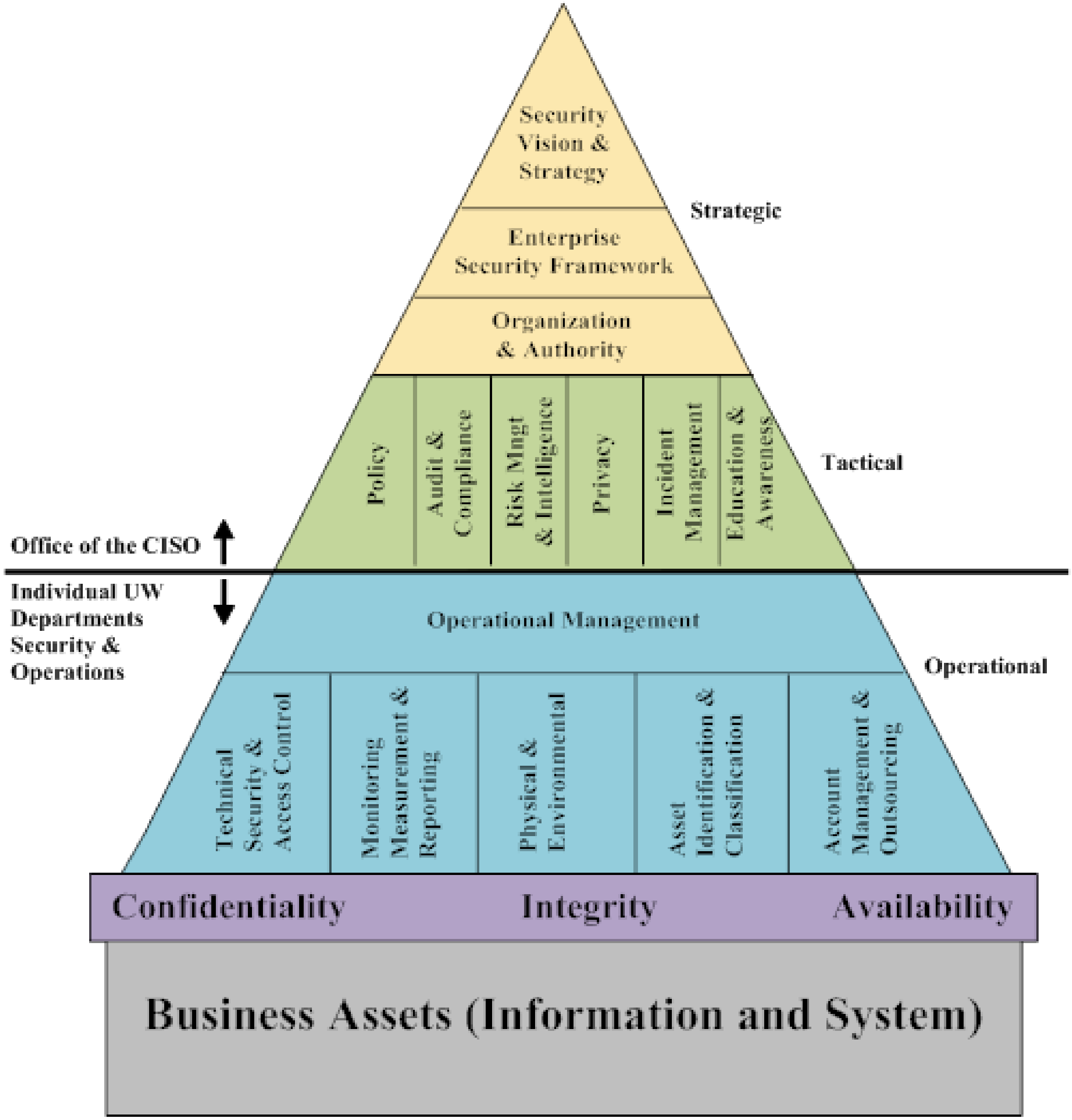
- **Policy**: High Level statement, defines intention, commitment, generalized requirement for compliance. Average lifecycle: 5 years
- **Standard**: A set of rules that outlines general principles, concepts, and baselines. Requires compliance. Average lifecycle: 2 years
- **Guideline**: Recommendations that can include specific examples, implementation details, compliance can be optional. Average lifecycle: 6-12 months.

Sample Program Components

- Incident Response
  - Detection & Containment
  - Incident Management
- Threat Monitoring & Intelligence
- Policy Development & Maintenance
- Security Engineering
- Forensics / Red Team / Penetration Test
- Outreach / Consulting
- Privacy Assurance Program
- Training, Education, & Awareness
- Risk Management

UW Information Security Program

- Organization & Authority
- Policy
- Audit & Compliance
- Risk Management & Intelligence
- Privacy
- Incident Management
- Education & Awareness
- Operational Management
- Technical Security & Access Control
- Monitoring, Measurement, & Reporting
- Physical & Environmental Security
- Asset Identification & Classification
- Account Management & Outsourcing


Security Vision & Strategy
Enterprise Security Framework
Organization & Authority
Strategic
Policy
Audit & Compliance
Risk Mngt & Intelligence
Privacy
Incident Management
Education & Awareness
Tactical
Office of the CISO
Individual UW Departments Security & Operations
Operational Management
Operational
Technical Security & Access Control
Monitoring Measurement & Reporting
Physical & Environmental
Asset Identification & Classification
Account Management & Outsourcing
Confidentiality
Integrity
Availability
Business Assets (Information and System)

UW Information Security Program

- Organization & Authority
- Policy
- Audit & Compliance
- Risk Management & Intelligence
- Privacy
- Incident Management
- Education & Awareness
- Operational Management
- Technical Security & Access Control
- Monitoring, Measurement, & Reporting
- Physical & Environmental Security
- Asset Identification & Classification
- Account Management & Outsourcing

Related areas…

- Human Resources
- Disaster Recovery / Business Continuity
- Facilities & Physical Security
- Internal & External Audit
- Compliance

DANGER, WILL ROBINSON

A word about Compliance

- HIPAA
- FERPA
- PCI / DSS
- GLBA
- Title 9
- SOX
- FISMA
- ARRA
- Red Flags Rule
- COPPA
- EAR
- ITAR
- NISPOM
- DMCA
- HEOA
- FCRA

Compliance ≠ Security

Just Ask

- Target
- U.S. Office of Personnel Management
- Anthem
- …

THE ASSUMPTION OF BREACH

(this page intentionally left blank)

LAB III

- Introduction
- Learning Objective
- Instructions
- Deliverable