Cybersecurity Governance & Risk Management

BUILDING RESILENCE IN THE FACE OF EVOLVING THREATS

Thom Shola

Northern Bank & Trust Chief Privacy & Risk Officer

Three Lines of Defense

1st

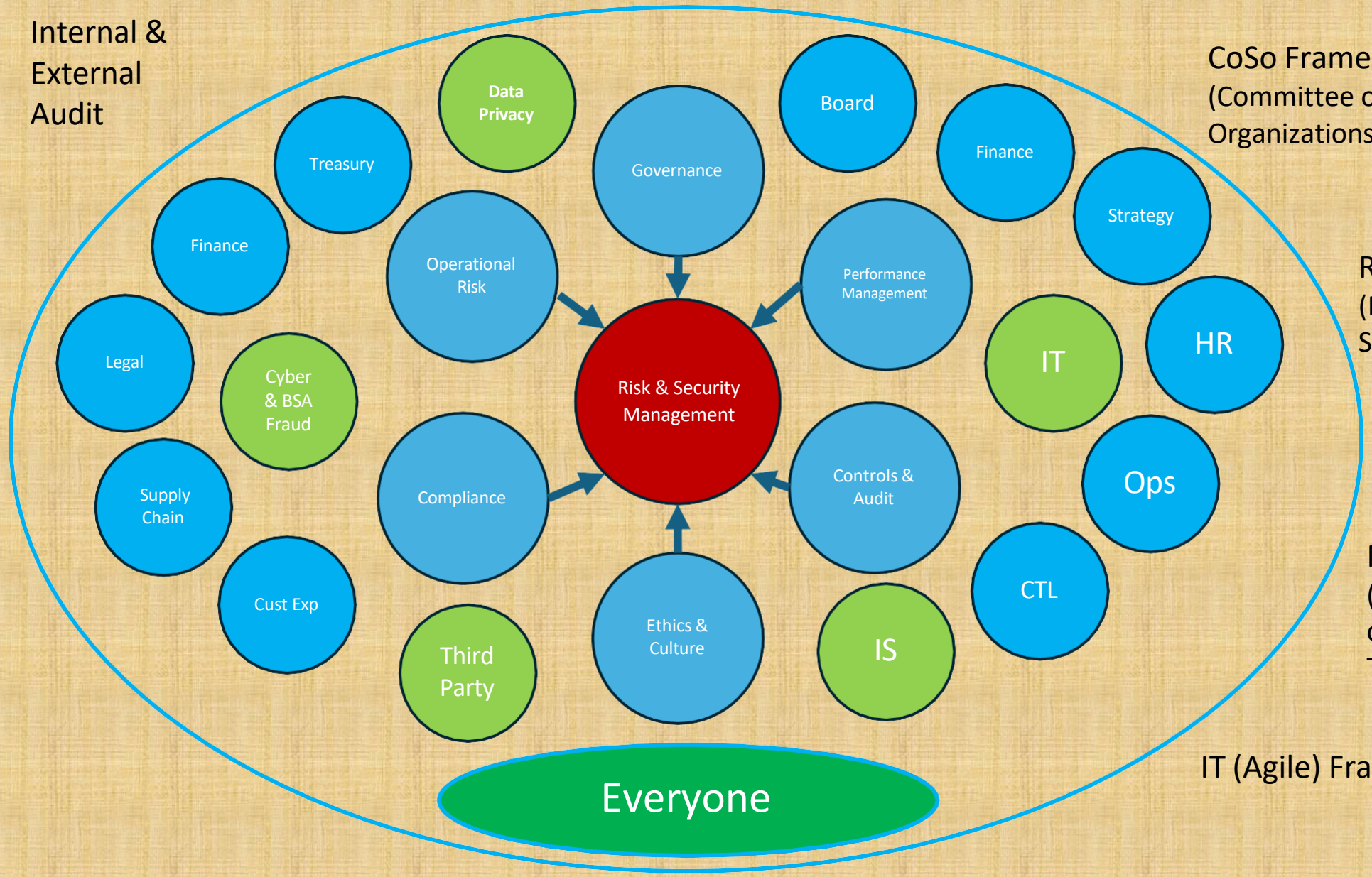
- **Business Units**
  - Daily Operational risk process based on internal governance
  - Risk Management role mostly part time

2nd

- **Risk Practitioner Teams**
  - Develop and oversee risk management framework and implementation
  - Risk Management role full time

3rd

- **Internal (and External) Audit**
  - Validate implementation of risk processes across business
  - Independent, objective assessment to Audit Committee/Board


Internal & External Audit
Data Privacy
Treasury
Governance
Board
Finance
Strategy
Finance
Operational Risk
Performance Management
Legal
Cyber & BSA Fraud
Risk & Security Management
IT
HR
Supply Chain
Compliance
Controls & Audit
Ops
Cust Exp
Third Party
Ethics & Culture
IS
CTL
Everyone
CoSo Framework (Committee of Sponsoring Organizations)
RCSA Framework (Risk Control Self Assessment)
NIST Framework (National Institute of Standards & Technology)
IT (Agile) Framework

Frameworks

CoSo Framework
(Committee of Sponsoring Organizations)

The COSO Framework is a system used to establish internal controls to be integrated into business processes. Collectively, these controls provide reasonable assurance that the organization is operating ethically, transparently and in accordance with established industry standards.

RCSA Framework
(Risk Control Self Assessment)

Risk and Control Self-Assessment (RCSA) is an important process for identifying and assessing the key operational risks faced by an organization and the effectiveness of controls that address those risks.

NIST Framework
(National Institute of Standards & Technology)

The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data.

IT (Agile) Framework

Agile framework is a specific approach to planning, managing, and executing work. Agile frameworks typically fall into two categories: Frameworks designed for teams, and frameworks designed to help organizations practice Agile at scale, across many teams.

Plan vs Objective

USA

Federal Trade Commission (FTC) CCPA

Federal Trade Commissions Act (FTCA)

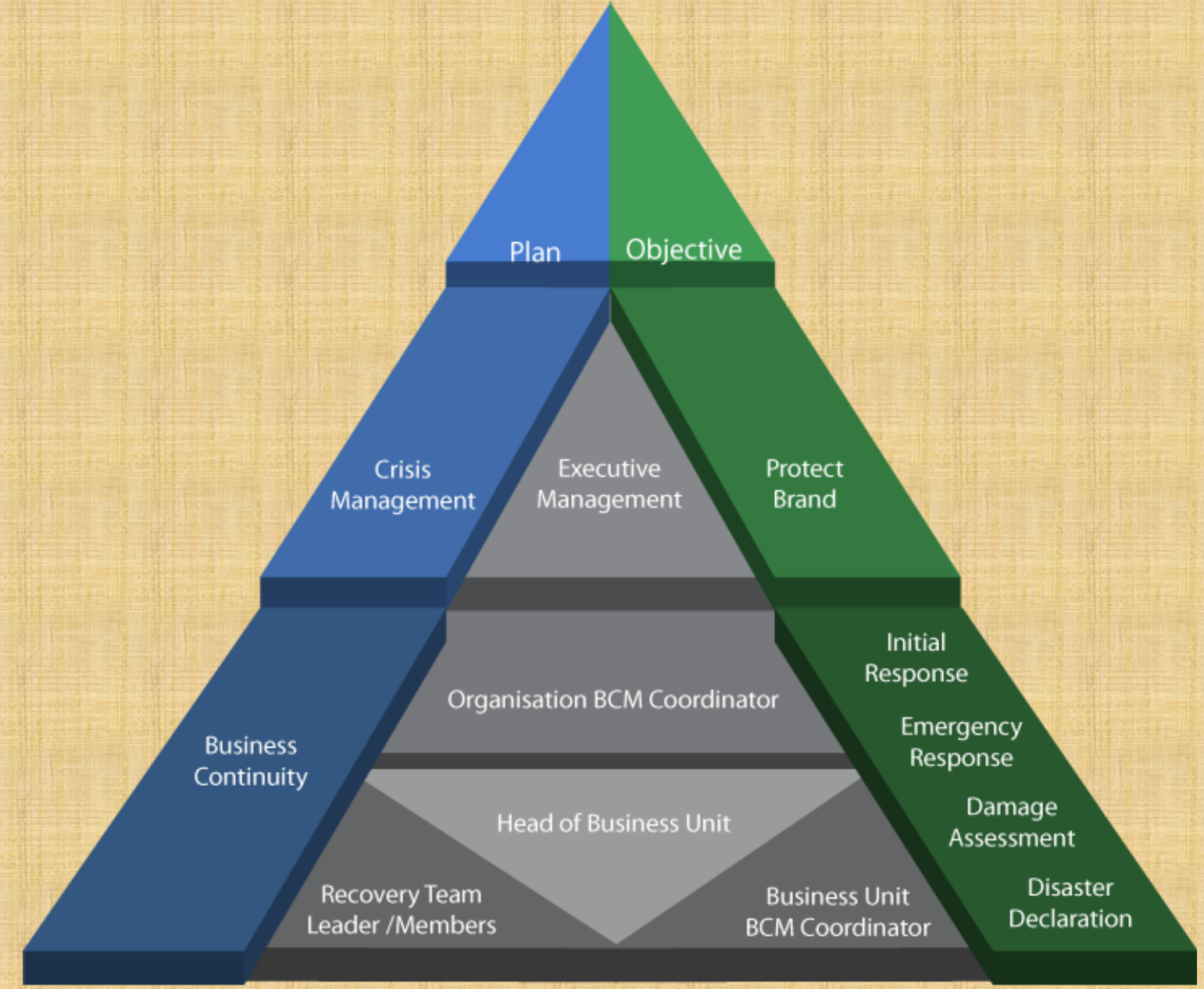
Gramm-Leach-Bliley Act (GLB)

47 States & DC have cybersecurity laws ranging from breach notifications to data privacy.

California Consumer Privacy Act (CCPA)

International

General Data Protection Regulations (GDPR)



Hierarchy of Plans

[Business Continuity Management Institute (BCM Institute)]

Cyber Kill Chain

The Lockheed Martin Cyber Kill Chain:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control (C2)
7. Action on Objectives

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Cybersecurity Incident Response Plan Basics

- **Preparation**
- **Identification**
- **Containment**
- **Eradication**
- **Recovery**
- **Investigation**
- **Notification, and**
- **Post-incident activities.**

Preparation

- Preparing for Potential Incidents
  - Define clear communication channels, implement response checklists, and provide staff with quality cybersecurity training.

Identification

- Identifying and Assessing Threats
  - Assess whether an event is a cyber-attack, evaluate its intensity, and classify the cybersecurity incident based on the nature of the attack.

Containment

- Containing the Impact
  - Isolate the affected systems and impede the incident from propagating further

Eradication

- Investigation and Eradicating Threats
  - Make sure the threat is no longer present in the organizations network by investigation the root cause of the incident and eradicating any threats from the system.

Recovery

- Recovering and Restoring Operations
  - Restore the affected systems to their pre-incident state to get your business back up and running as normal.

Investigation

- Learning from the Incident
  - Document everything that occurred during the incident and the response. Use this information to recognize areas of improvement in the organization’s security posture and incident response.

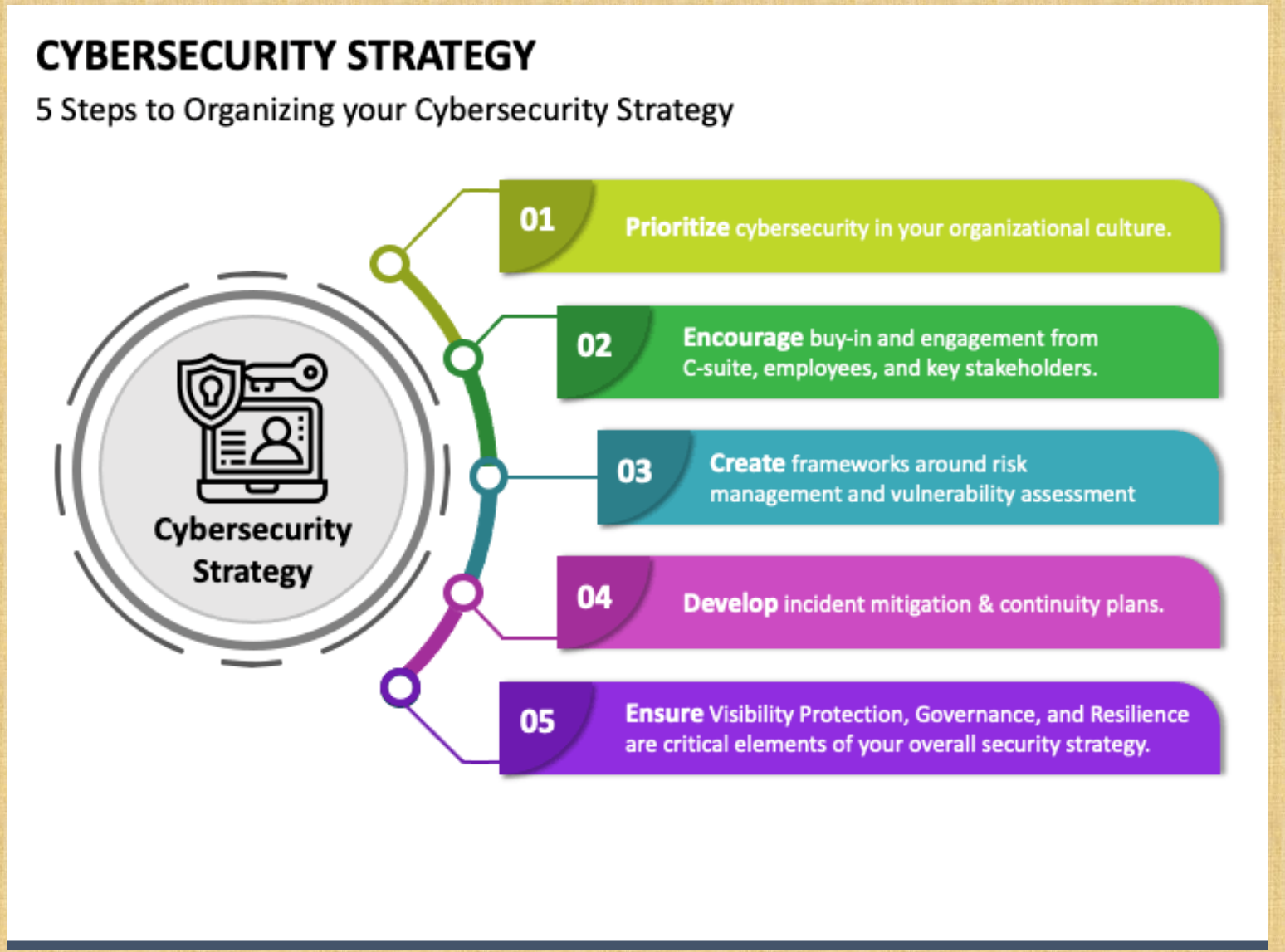
Notification

- Notification of Impacts
- Identifying who needs to be notified of the impacts of an incident both internally and externally and who is accountable to notify in each area.

Post-Incident Activities

- Post-Incident and Lessons Learned
  - Both the notification process and the learnings to avoid the incident in a post-mortem exercise is critical to improve security posture.

Cybersecurity Strategy



Cybersecurity Incident Response Notification

FBI & Law Enforcement (Benefits/IC3)

- www.fbi.gov/investigate/cyber

Additional Reading & Links

- https://it.nc.gov/blog/2022/10/11/anatomy-data-breach-what-are-they-and-what-do-when-you-spot-one
- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- https://attack.mitre.org
- https://training.fema.gov/is/courseoverview.aspx?code=is-100.c&lang=en
- https://www.nist.gov/cyberframework

Quick Analysis of Target Breach