Security Governance, Risk, and Compliance

SUDHANSHU KAIRAB

FEBRUARY 24, 2022

Agenda

1. Introduction
2. GRC Overview
3. Three Lines of Defense
4. Key Focus Areas
5. Day in the Life
6. GRC Value Proposition
7. Success Factors

Introduction

Sudhanshu Kairab

Current Role: VP Cybersecurity Governance, Risk, & Compliance

- Responsible for security policy management, third party risk assurance, security education and awareness, and IT security compliance.
- Background in security, compliance and internal audit
- Prior companies include Deloitte, Bristol-Myers Squibb, IBM, Wyndham Worldwide, and EisnerAmper
- Undergraduate and MBA degrees from Bucknell University and Northeastern University

GRC Overview

Governance

Consistent Processes and Practices to Operate Compliance

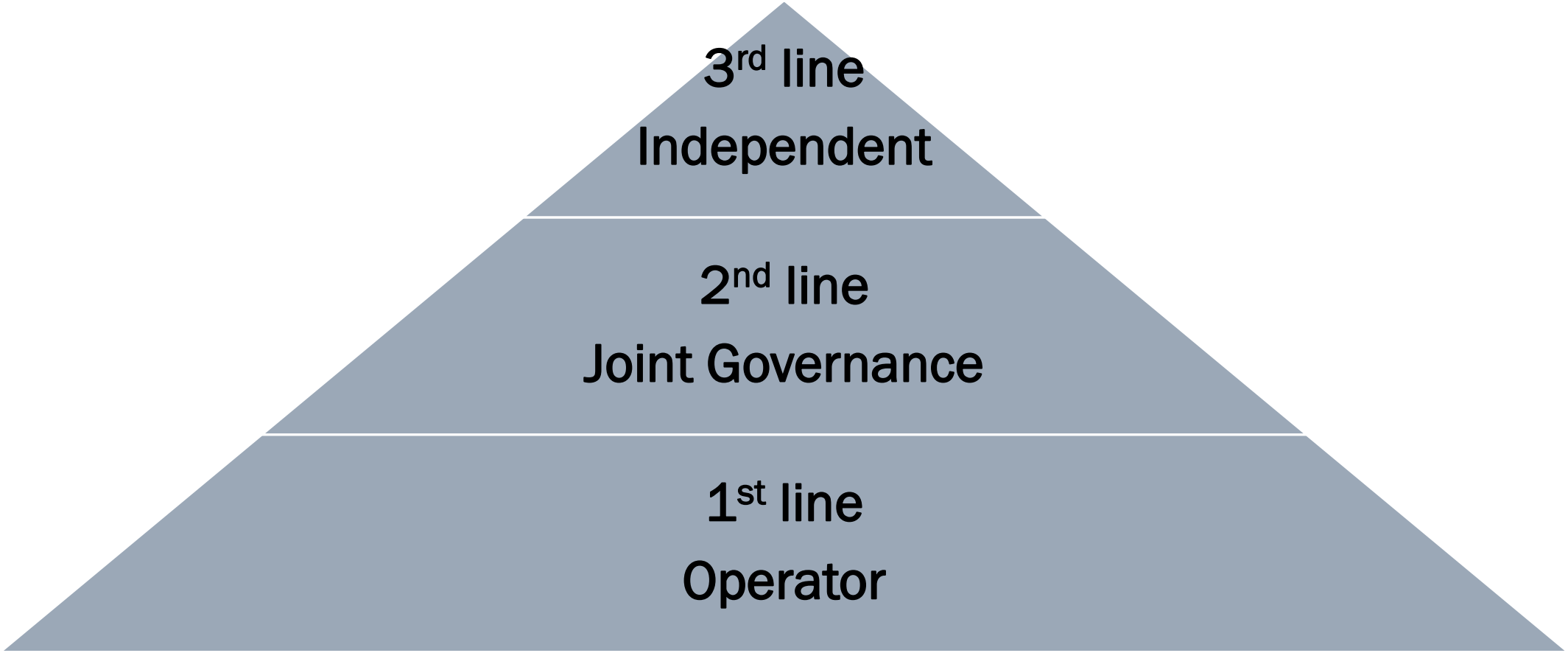
Risk

Understand Uncertainty and Weaknesses

Compliance

Adhere to Policies & Regulations

Three Lines of Defense



Key Focus Areas

- Security Policies
- Privacy
- Cybersecurity Training & Awareness
- Risk & Controls
- Security Certifications & Attestations
- Third Party Security Assurance
- Special Projects (e.g. M&A)

Day in the Life Example – PCI

Objective

- Manage risk associated with credit cardholder data

Compliance Process

- Developing and maintaining scope
- Working with system and process owners to determine compliance
- Gathering and vetting evidence
- Managing third party auditors

Ongoing Compliance

- Monitor key controls
- Assess changes to the business and technology environment to understand compliance impact
- Monitor changes to PCI controls

Day in the Life Example – Third Party Security

Objective

- Ensure third party security posture is properly vetted before engaging them

Compliance Process

- Understanding the nature of services
- Understanding company data that the third party may process
- Security posture associated with services to be provided
- Input on contractual security terms
- Manage any security remediation
- Understand privacy related impacts

Ongoing Compliance

- Refresh understanding of services
- Monitor security posture of third parties
- Periodic re-assessments
- Security incident support

GRC Value Proposition

Value to the Cybersecurity Function/CISO

- Continuous improvement
- Keep current with important standards
- Consolidate compliance posture and provide an independent view on risk posture

Value to the Business

- Strategic partner to manage new laws, regulations and contractual requirements
- Combine our knowledge about critical assets/processes with adverse scenario
- Challenger

Success Factors

EXECUTIVE SPONSORSHIP AND TONE AT THE TOP

STAKEHOLDER ENGAGEMENT

BUILT IN AND NOT BOLTED ON

SOURCES OF TRUTH AND TRANSPARENCY

RESOURCES AND INVESTMENT