Mitigating Operational Risks for a Secure and Resilient Supply Chain

Anthony Lee CPP, CBCP

Key Issues

- Evolving Threats and Risks in global supply chain
- Driving Sustainability and Resiliency in a global economy
- Public-Private Partnership and International Compliance
- Paradigm Shift to Add Value

Supply Chain Management Challenges

- Talent
- Visibility
- Traceability
- Complexity
- Costs
- Sustainability
- Supply performance
- Natural disasters
- Technology
- Cyber risks

Sources of Operational Risks

- People
- Processes
- Systems
- External Events
- Legal Risks

"Not since the end of Second World War have global supply chains been so fraud with risks"

- KPMG, Andrew Underwood

Chart 1. Percentage of companies affected by listed types of fraud

	2013	2012
Theft of physical assets	28%	24%
Information theft	22%	21%
Management conflict of interest	20%	14%
Vendor, supplier or procurement fraud	19%	12%
Internal financial fraud	16%	12%
Regulatory or compliance breach	16%	11%
Corruption and bribery	14%	11%
IP theft	11%	8%
Market collusion	8%	3%
Misappropriation of company funds*	8%	—
Money laundering	3%	1%

*Not covered in 2012 survey

Ref: Kroll Global Fraud Report, Annual 2013/2014

7 Categories of Operational Risks

- Internal Fraud
- External Fraud
- Employment Practices & Workplace Safety
- Clients, Products and Business Practices
- Damage to Physical Assets
- Business Disruptions and System Failures
- Execution, Delivery and Process Management

Cargo Crime Impact on Business

Financial cost of recovery

- Inability to fulfill customer orders
- Impact on company reputation
- Disrupted production/delivery schedules and lost productivity
- Increased insurance premiums

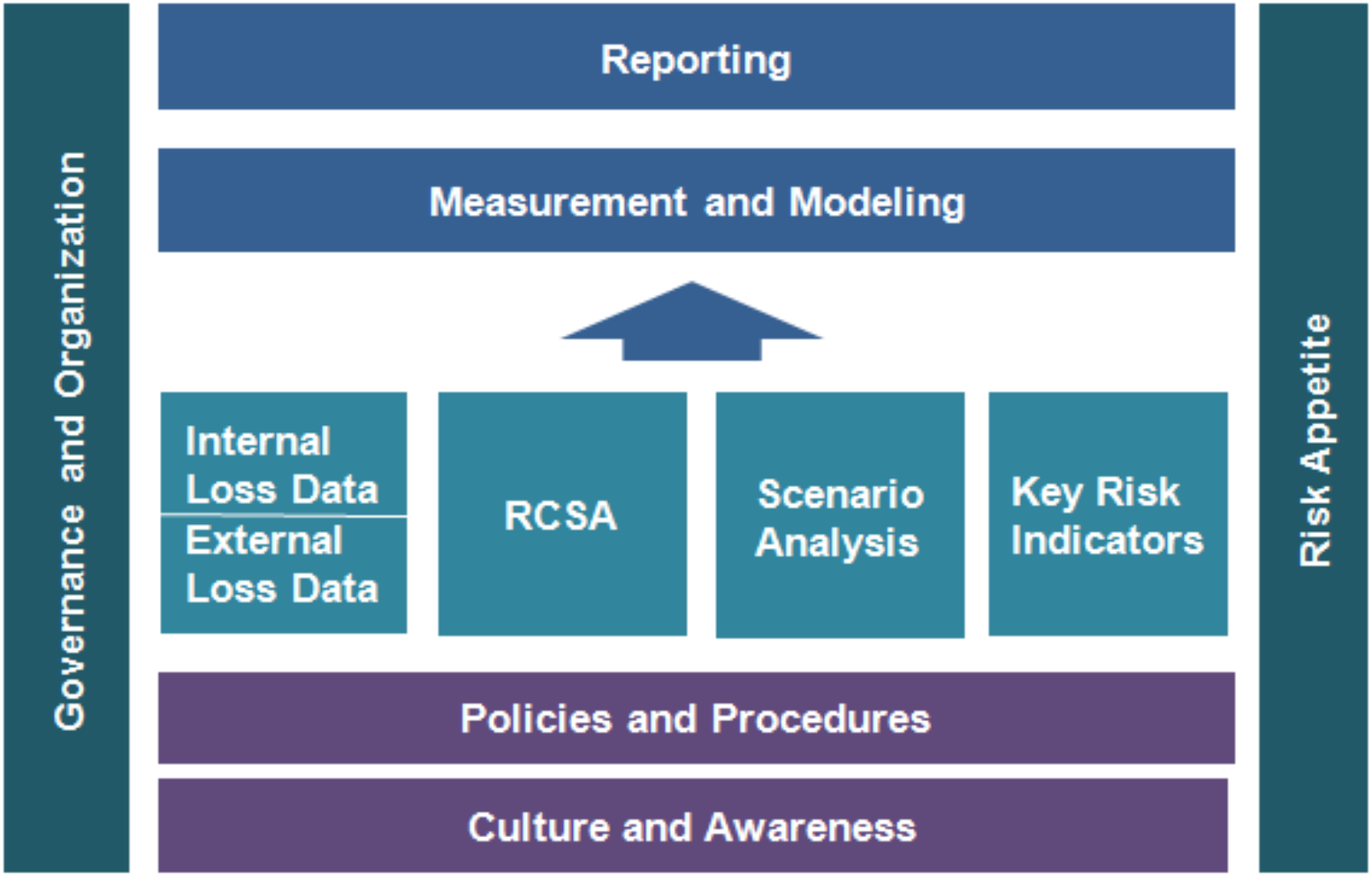
Consequences of Non-compliance

- Major disruptions to supply chain flows
- Hefty financial penalties by Authorities
- Potential “blacklisted” at country of UN level
- Reputational risk to company and hence share value
- Customers disqualification due to “unreliable supplier” status
- Suppliers potential reluctance to deal with “unreliable customer”
- Staff turnover in view of bad company reputation

Operational Risk Program

- An operational risk program should ensure that operational risk is:
  - Identified
  - Assessed
  - Monitored and Controlled
  - Mitigated

Operational Risk Framework



Governance: 3 Lines of Defence

- First Line – the business **owns** operational risk and should be managing it as it arises.
- Second Line – the second line of defense is the independent corporate operational risk function – to include Security.
- Third Line – Internal Audit. This function should not be directly responsible for operational risk management.

Operational Risk Program

Four Core Elements:

- Loss data – Internal and External
- Risk and Control Self-Assessments (RCSA) – tool to look forward at what might happen in the future
- Scenario Analysis – to evaluate exposure to high-severity events
- Key Risk Indicators (KRI) – keep a finger on the pulse of the changing risk environment.

Culture & Awareness

Key elements of supply chain security and risk program to mitigate risks and prevent losses:

- Marketing Strategy
- Training Plan
- Communication
- Awareness Training
- Partnership

Operational Risk Reporting

4 key elements to improve risk communication:

- Goal Setting – purpose of communication
- Openness – two way exchange
- Balance – avoid distortion
- Competence – credible information

Operational Risk Management: Key Points

- "Use Test" – Company demonstrates that operational risk management and measurement is embedded
- Using operational risk as a key input in business decision-making process
- Effective internal marketing, planning and training activities are essential to embed Operational Risk Management

Risk Mitigation Strategies

- Security Awareness
- Governance, Risk and Compliance (GRC)
- Strategic Intelligence
- Situation Awareness
- Loss Prevention
- Information Security
- Business Continuity

Way Forward

- Global Standards, International Certifications and Independent Audits
- Driving Operational Excellence
- Governance, Risk & Compliance (GRC) to include BCP, information security, etc
- Risk Mitigation – Cost effectiveness
- Professional Synergy to empower the Business

Summary

- Assess the current state of the supply chain
- Pinpoint critical vulnerabilities and operational risks
- Governance, Risk & Compliance (GRC) or Convergence for integrated approach
- Create a prioritized roadmap for improvements to mitigate and manage risks

...remember, your organization is only as strong as its weakest link

Thank You!

ASIS China Conference

Shanghai

3-4 December 2015