UNIFIED RISK OVERSIGHT FOR SECURITY OPERATIONAL EXCELLENCE

A Guide for Influencing and Participating in Enterprise Risk Management

Introduction

This report summarizes a more detailed Security Leadership Research Institute (SLRI) *Security State of the Industry* project. It introduces a discussion regarding organizational risk management and operational risk management frameworks. It also explores a number of considerations for engaging, integrating and governing operational and cross-functional subject matter expertise for improved risk outcomes.

This brief guide was influenced by next generation thought leader forums that convened academics, researchers, and risk practitioners. Companies and institutions that participated include AON, Boeing Company, Bill and Melinda Gates Foundation, Cardinal Health, Celanese, Capital One, Coles College of Business (Kennesaw State), Darla Moore School of Business' Risk and Uncertainty Management Center (University of South Carolina), Delta Air Lines, Hilltop Holdings, MITRE Corporation, MD Anderson Cancer Center (University of Texas), Procter and Gamble, Red Hat, State Street, TD Bank, and more.

We find, that despite best intentions, enterprise-wide risk management often fails. British Petroleum's Deepwater Horizon catastrophe is one of many examples.[1] All-hazards risk mitigation assurance requires that we get beyond one-dimensional, compliance-only, enterprise risk "list" management.

Programs that work are multi-dimensional, operationally integrated and relevantly informed by cross-functional subject matter expertise. They include:

- 24x7x365 situational risk awareness communications
- Continuous risk/threat/vulnerability assessments
- Mitigation design, performance testing, and innovation pilots
- Persistent all-hazards risk monitoring, anomaly detection and response assurance
- Critical event management; including near-miss after-action queries with objective targeted performance improvement
- Engaged leadership governance
- Ongoing prevention/mitigation systems hygiene
- Understood roles and responsibilities including compliance-plus brand reputation Duty of Care dependencies

Enterprise Risk Management (ERM) Shortfalls

A review of the literature reveals enterprise risk management has shortfalls in the 5 following areas:

1. Organizations adopt frameworks or processes that are siloed, regulatory-focused, and overly prescriptive; often self-focused with insufficient attention on emerging hazards
2. Risk inventories are often 'personal-opinion' management polls that are infrequently supported by research, or weighted subject matter expert opinion or proven practices
3. Plans speak to, but seldom assure integrated cross-functional prevention, protection, mitigation planning, funding, testing or performance inside and outside the organization
4. Compliance requirements are often less rigorous than intended and do not sufficiently educate, incent or protect anomaly reporters and whistleblowers
5. Leadership governance is largely in name only, part-time and seldom involved in cross-functional resilience operational dependency planning, testing and performance oversight

As part of the SEC's Enterprise/Security Risk Alignment process, business stakeholders are interviewed. These

1. See How Did BP's Risk Management Lead to Failure?

interviews reveal compelling answers for all-hazards risk mitigation improvement. Many of the business leaders recognize and understand that the siloed stand-alone risk mitigation units including Audit, Business Continuity, Compliance, Risk Management, Safety and Security, although well-intentioned, seldom serve optimally. Often each was typically introduced in an organic fashion at millions of dollars of expense without clear and concise cross-functional and operational performance mandates. Return on investment is dubious particularly when emerging risks threaten to overwhelm sluggish planning, detection, and response. Unified Risk Oversight™ (URO) is an answer for the call for a more collaborative and cost-effective risk mitigation strategy. As a part of this concept, it is recommended that those that are working at the operational level of risk (e.g., Security) consider forming an advisory committee. Engaged and continuously informed leaders can bolster a higher-level enterprise risk initiative.

What is an Operational Risk Leadership Advisory Committee or Council (ORLAC)?

What it is:

1. A chartered or codified, cross-functional, executive appointed, all-hazard risk leadership governance body.
2. An opportunity to enable, facilitate and prioritize the organization's operational risk management strategy.
3. A deliberative, all-hazards, intelligence-based, analytical information advisor that informs risk mitigation operational oversight; for example, it can remove unneeded redundancies, based on risk exposures and threat priorities.

It is not:

4. Meant to own or handle all risk burdens – rather it plays a role to assure collaborative, all-hazard, enterprise risk mitigation operational excellence amongst business units with distributed subject matter capabilities.
5. A primary driver for organizational re-engineering or restructuring. Rather it acts as the designated oversight counsel to assure reasonable organization-of-the-future considerations for rationalized risk mitigation performance including outside service integrations.
6. Intended to replace or supersede all existing risk mitigation activities. Instead it ensures that all such activities are mapped to the accepted risk registry or taxonomy and are beneficially assessed for defensible contributions for brand protection-in-depth.

What are the Benefits of an Operational Risk Leadership Advisory Committee or Council (ORLAC)?

- It enables persistent Unified Risk Oversight governance. Subject matter expert business leaders and section chiefs may now cross-functionally evaluate, prioritize and resource mitigation options for both emerging and residual threats.
- Many senior management leaders recognize that the expanding organizational strategy faces persistent and evolving external and internal risk factors that require collaborative, continuous, and nimble processes, including emerging and residual threat vigilance with operational oversight.
- It is often a course correction for efforts that did not cross-functionally connect enterprise risk management for emerging and fast onset of risks, especially at the operational levels.

Using Processes and Frameworks to Manage Operational Risk

Brand reputation, insurance, financial, liability and resilience considerations drive all-hazard risk programs to optimize

outcomes for all stakeholders. Processes and frameworks vary. Most promise resilience but disappoint in operational performance. Recognized proven practices alternatively are capable of promoting brand loyalty and stickiness to attract and retain customers, strategic partners and talent.

A blended approach to risk identification and operational integrity assurance may be most pragmatic. Good advice includes this from Herb Mattord, Professor, Coles College of Business: "Unless legally mandated, don't pursue certification to any framework unless it serves your organization's objectives. Don't be distracted from pursuing your own strategic, process-driven, metrics-based program that seeks ongoing continuous improvement." Establishing a continuum to provide context for what good protection-in-depth looks like is prudent for cross-functional performance (see Figure 1 below).

Global All-Hazard Risk Continuum Considerations

Proactive Service Design → **Intelligence-Led Awareness** → **Operational Excellence**

Risk Inventory	Program Design	Management Support	Awareness	Intelligence & Investigation	Operational Excellence	Emerging & Residual Risk
• Brand Reputation • Claims, Costs and Settlements • Competitors • Crime • Consumer Product/ Service Quality Assurance • Critical Facilities • Intellectual • Insider • Property • Information • Licenses, patents and trademarks • Pandemic • People, process, product & assets • Personnel health, safety • Public Image • Regulatory Compliance • Research and Development • Revenue • Stakeholder Confidence • Supply Chain • Total Cost of Protection • Total Cost of Risk • Travel – See Personnel • Other	• Access Control • All-hazards situational awareness • All-channel communications • Analytics & metrics • Asset Protection • Business Continuity • Conduct & Ethics • Critical event response and recovery • Global Operational Risk Oversight • Governance • Intelligence • Innovation • Loss Prevention • Personnel at Risk • Procurement and Supply Chain • Project Management • Rewards • Risk Reporting • Risk Response • Threat Risk & Vulnerability Assessment • Workplace Violence • Other	• Alignment with Brand Mission, Strategy and Values • All Hazards Risk Leadership Operational Advisory Council • Communication strategy • Exercises and Tabletops • Financing • Governance (Policy, Standards and Guidelines) development and enforcement • Risk Mitigation Performance Review & Objective Setting • Performance Goals • Special events • Stakeholder Confidence and Satisfaction Surveys • Other	• All-hazards, all-channel briefs and situational risk and reward messaging • Audits, & Self-assessments • Education including Next Generation Leader development • Global Risk Operational Oversight Centers (GEOC, GSOC,GROC, IROC) • Program collateral for all-hazards personal & organizational risk mitigation • Travel risk notifications • Web site programming, solutions & services • Web Page Links • Other	• All-hazards Analytics • Anomaly detection and response • Assessments, audits inventories & surveys • Business Continuity • Critical event reporting • Electronic Countermeasures • Facility and Systems Design and Programming • Forensics and Investigations • Global Security & Risk Operations • Governance (policy, procedure, guidelines & accountability) • Interagency liaison coordination • Life-safety Systems • Solution service coordination • Travel Risk • Unified Risk Oversight • Other	• After Action Analysis • All-hazard or Allegations, Claims and Compliance Trend Reporting • All-channel Alarm, Anomaly Communication • Brand Protection Communications • Business Continuity, Recovery and Resilience • Critical Condition, Event or Incident Ops Management • Ongoing Risk, Threat and Vulnerability Identification and Monitoring • Performance and Outcome Value Metrics • Quarterly or bi-annual Key Client Confidence (Internal and/or External) and Value Assessments • Other	• Brand Reputation • People, Product, Process, Asset and Information (Risk, Threat and Vulnerability from all manmade and natural vectors: • Economic • Environment • Health • Societal Technological As represented by the World Economic Forum or other relevant research • Peer Benchmark OP EX Work Group or other network inputs • Other

Figure 1: Risk Continuum

A Few Examples of Operational Risk Frameworks

ISO 31000

Governments and international institutions are increasingly discovering that risk conditions and mitigating infrastructures are interconnected for hazard detection, emergency response and critical incident management. Adopting a risk management standard like ISO 31000, used internationally by both the private and public sectors,

can provide advantages for intramural drills, exercises and tabletop scenarios.

ISO 31000:2009 has been developed on the basis of an existing standard on risk management, AS/NZS 4360:2004. The framework contains the following steps:

1. Identifying Risks
2. Analyzing Risks
3. Evaluating Risk
4. Risk Mitigation or Treatment[2]

Revisions by 2017 are anticipated to meet the needs of practitioners to enhance governance of risk management systems (see: http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1963).

Operational Integrity Management System (OIMS)

ExxonMobil's Operational Integrity Management System (OIMS) addresses all aspects of doing business that can impact personnel and process safety, security, health, and environmental performance. It contains 11 elements including:

- Management leadership, commitment, and accountability
- Risk assessment and management
- Information/ documentation
- Third-party services
- Incident investigation and analysis

For more see http://www.corporate.exxonmobil.com/en/company/about-us/safety-and-health/operations-integrity-management-system

Unified Risk Oversight™

The SEC has developed a concept called Unified Risk Oversight (see Figure 2). An effective URO program rests upon three foundational principles:

- A role is established to oversee all risk issues
- All key stakeholders in the company are involved
- Responsibilities are clearly defined

Businesses typically have a risk-management program, but its operations are too often cordoned off from other departments, which can prevent the right people from getting necessary information. Communication is crucial to this model. While not a risk framework per se, it should be used to help govern risk management across the enterprise.

[2] See (ERM) and the requirements of ISO 31000 from RIMS for a thorough explanation of ISO 31000

Figure 2: Unified Risk Oversight™. Click on image for a larger image.

Your Role in Enterprise Risk Management and Operational Risk Management Assurance

While Enterprise Risk Management and Operational Risk Management arguably remain two distinct lenses for risk management, their combined processes and capabilities enable higher levels of integrated mitigation assurance and confidence. Their considerations provide a likely path to resilience; when attended by persistent operational performance monitoring, anomaly detection, communications and response. As a security practitioner, your role can be that of the experienced and influential critical event responder who has witnessed if not paid a price for less thoughtful planning.

ERM + ORM + URO = 

Stakeholder interview or survey questions that may be helpful in engaging responsible leaders in the ORLAC process:

1. What are the top five business risks the Institution faces over the next five years that could have a significant adverse effect on our brand reputation or our ability to achieve our strategic planning objectives?

2. What risks (if any) do you think are best worked collaboratively and cross-functionally with key institutional risk resources as opposed to worked in silos? (Could include background, promotional and duty to report assurance; compliance, intellectual property protection, workplace violence/threat management, etc.)

3. Would we benefit from our asking/surveying your operational SME team leaders these questions first?

4. How do you think we might best ensure that the right risk awareness and operational risk protection programs are in place to prevent or minimize critical hazards, events or conditions?

5. What are our key risk mitigation dependencies?

6. What is your confidence (1-10; 10 being extraordinarily confident) that our current operational risk prevention and mitigation resources (people, process and technology) are capable and sufficient to protect us; in a manner that is consistent with our brand reputation?

7. What is your confidence that (1-10) that our personnel are sufficiently vetted, trained, equipped and prepared to prevent or mitigate any critical hazard?

8. What is your confidence that our contractors and service dependencies (1-10) are sufficiently vetted, trained, skilled and prepared to meet our strategic risk mitigation needs for all-hazards?

9. What is your confidence that our big bets, including people, research and innovation, are sufficiently protected from injury, damage or theft from persistent adversaries? Natural catastrophes? Travel Risks? Etc.?

10. What are our prevention/protection/mitigation strengths and weaknesses?

11. What about disturbed, potentially destructive/violent insiders? What about Pandemic? What about Zika?

12. How should we prioritize the risks we have discussed?

13. What did we miss asking you that is relevant to this conversation?

In Closing

This is a call to action for Security and other risk management leaders that now have presumed duties and brand expectations that extend well beyond legal compliance. These include cross-functional team acuity and return for every dollar invested. Outdated risk mitigation architectures and solutions have a short shelf-life. Practitioners can no longer sit on their historic heroic laurels.

The clock is ticking. Business needs for mitigating emerging risks and threats prevail. Companies effectively guided by enterprise risk management, operational risk management and unified risk oversight are better positioned to adapt and reinvent. Share this with your colleagues. Feedback in the form of proven frameworks and performance metrics are appreciated in advance and will be shared with our community.

About

Contributing Editors:

Francis D'Addario is Emeritus Faculty, Security Executive Council, and former CSO, Starbuck Coffee Company.

Kathleen Kotwica is EVP and Chief Knowledge Strategist, Security Executive Council.

Security Executive Council (SEC)

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of risk mitigation strategy; they strategize with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

https://www.securityexecutivecouncil.com

Security Leadership Research Institute

The Security Leadership Research Institute (SLRI) provides independent and actionable research to the security and risk community. The SLRI was formed because of the need by the security industry to document the entire spectrum of corporate security risk mitigation through research. The SLRI conducts benchmarks like this one and many other forms of research such as practitioner quick polls, state of the industry and trend reports, and custom research for individual companies and security leaders.

https://www.securityexecutivecouncil.com/about/research_institute.html

Would your organization benefit from a self-assessment to determine if an operational risk committee would enhance your security risk mitigation efforts? Contact us if interested at contact@secleader.com