Demonstrating Value > Operational Excellence >

Making the Case for an Operational Risk Leadership Advisory Council

A Guide for Influencing Enterprise Risk Management at the Operational Level

Contributing Editors: Francis D'Addario, Emeritus Faculty, Security Executive Council and former CSO, Starbucks Coffee Company; and Kathleen Kotwica, Ph.D., EVP and Chief Knowledge Strategist, Security Executive Council

Introduction

We find that, despite best intentions, enterprise risk management often fails. British Petroleum's Deepwater Horizon catastrophe is one of many examples. Risk mitigation assurance requires that we get beyond one-dimensional, compliance-only, enterprise risk "list" management. One way to do that is to embrace the concepts of enterprise risk governance and communication not only in the Boardroom but at the operational level.

This report summarizes a more detailed Security Leadership Research Institute (SLRI) *Security State of the Industry* project that was developed with input from 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 recognize that the goal of enterprise risk management is both to confront hazards and to uncover mitigation opportunities. Because this report is created with and for corporate security practitioners, its insights speak primarily to that audience for organizational protection. However, all corporate executives with an eye for risk in the enterprise can benefit from the concepts laid out here.

Enterprise Risk Management Ideals and Shortfalls

For an ERM program to work, it needs to be multi-dimensional, operationally integrated and cross-functional. This includes:

- 24 x 7 x 365 situational risk awareness communications
- Continuous risk/threat/vulnerability assessments
- Mitigation design, performance testing, and innovation
- Persistent all-hazards risk monitoring, anomaly detection and response assurance
- Critical event management and actionable post-event analysis
- Engaged leadership governance
- Ongoing prevention/mitigation systems maintenance
- Understood roles and responsibilities including compliance-plus brand reputation and Duty of Care dependencies

However, our observations show that enterprise risk management commonly experiences shortfalls in the following areas:

1. Organizations adopt frameworks or processes that are siloed, regulatory-focused, and overly prescriptive; often giving insufficient attention to emerging risks.
2. Risk inventories are often personal-opinion management polls that are infrequently supported by research, 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 planning, testing or performance oversight.

Many business leaders interviewed by the Security Executive Council 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 introduced in an organic fashion at millions of dollars of expense without clear and concise cross-functional and operational performance guidance, making return on investment dubious.

We recommend that those who are working at the operational level of risk (e.g., Environmental Health, Safety, and Security) consider forming an advisory committee that reports to the executive-level risk management team. Engaged and continuously informed operational leaders can bolster a higher-level enterprise risk initiative. The concept of the operational advisory committee is a one part of the Council's Unified Risk Oversight™ (URO) model for collaborative and cost-effective risk mitigation.

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

It is:

- A chartered or codified, cross-functional, executive-appointed, operational risk management leadership governance body.
- A vehicle to enable, facilitate and prioritize the organization's operational risk management strategy.
- A deliberative, 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:

- Meant to own or handle all risk burdens. Rather, it helps assure collaborative proven practice and risk mitigation operational excellence amongst business units.
- The primary driver for organizational re-engineering or restructuring. Rather, it oversees repeatable and scaled services; along with future incremental considerations for risk mitigation performance, including outside service integrations.
- Intended to replace or supersede all existing risk mitigation activities. Instead, it ensures that all such activities are defined, mapped to the accepted risk register or taxonomy and assessed for contributions to brand protection.

What are the Benefits of an ORLAC?

- It enables multilayered Unified Risk Oversight communication. Business leaders and section chiefs may now cross-functionally evaluate, prioritize and resource mitigation options for both emerging and residual threats.
- It enables the organization to confront the 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 develop an enterprise risk management program that deals with emerging and fast-onset risks, especially at the operational levels.

Using Processes and Frameworks to Manage Operational Risk

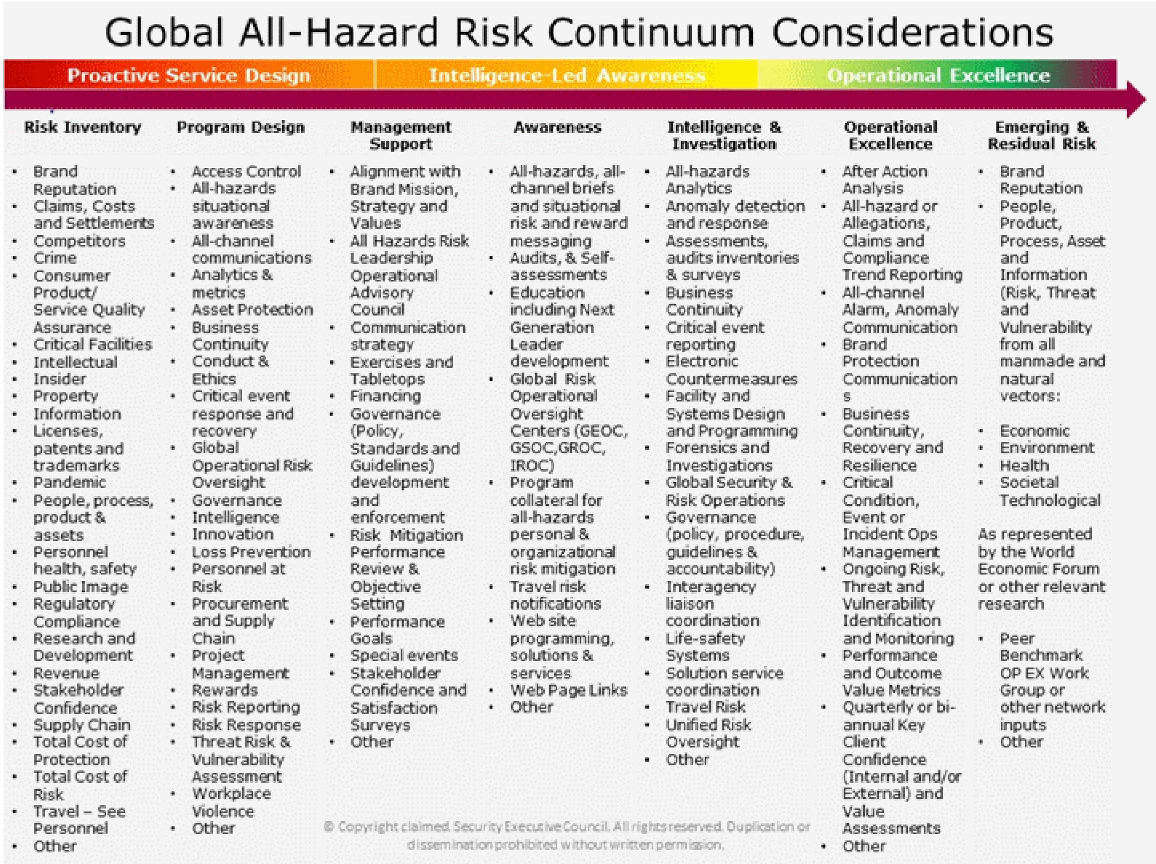
Brand, insurance, financial, liability and resilience considerations drive risk programs to optimize outcomes for all stakeholders. There are a variety of processes and frameworks upon which to base these programs, such as ISO 31000[1], ExxonMobil's

[1] https://www.theirm.org/media/886062/ISO3100_doc.pdf

Operational Integrity Management System[2], RMA's Operational Risk Management Framework[3], and COSO's Enterprise Risk Management — Integrating with Strategy[4].

A blended approach to risk identification and operational integrity assurance may be the most pragmatic option. Herb Mattord, Professor, Coles College of Business offers this advice: "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."

Organizations must understand what "good protection" looks like. They may choose to consider establishing a continuum like the one below to provide context for continuous cross-functional performance.



Global All-Hazard Risk Continuum Considerations

Proactive Service Design
Intelligence-Led Awareness
Operational Excellence

Risk Inventory

- 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

Program Design

- 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

Management Support

- 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

Awareness

- 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

Intelligence & Investigation

- 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

Operational Excellence

- 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

Emerging & Residual Risk

- 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

Unified Risk Oversight™

The Security Executive Council's Unified Risk Oversight (URO) concept

[2] http://www.corporate.exxonmobil.com/en/company/about-us/safety-and-health/operations-integrity-management-system

[3] https://www.rmahq.org/operational-risk-management-framework/

[4] https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

(https://www.securityexecutivecouncil.com/spotlight/ ?sid=26462), while not a risk framework per se, should be used to help risk management governance across the enterprise. 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 that have enterprise risk management programs still too often have their operations cordoned off from some departments, which can prevent the right people from getting necessary information in time. Evolving Duty of Care compliance, for example, may conflict with evolving Privacy requirements. Cross-functional governance is key to nimble team risk mitigation operations; particularly when life-safety is on the line. We propose operational risk management frameworks are another layer of internal control at the day-to-day operational level. Communication, provided by URO, is crucial to this model. The ORLAC is the middle man, to inform operational issues up to the Enterprise Risk Council.

Security's Role in Enterprise Risk Management via 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 risk 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 operational business risks the organization 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 operational risks (if any) do you think are best worked on collaboratively and cross-functionally with key institutional risk resources as opposed to worked in silos? (For example, background screening, compliance, diligence investigations, intellectual property protection, workplace violence/threat management.)
3. Should we ask/survey your operational SME team leaders these questions?
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 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 our personnel are sufficiently vetted, trained, equipped and prepared to prevent or mitigate any critical hazard or events?
8. What is your confidence that our contractors and service dependencies are sufficiently vetted, trained, skilled and prepared to meet our strategic risk mitigation needs?
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?
10. What are our operational risk prevention/protection/mitigation strengths and weaknesses?
11. How should we prioritize the risks we have discussed?
12. 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 who now have duties and brand expectations that extend well beyond legal compliance. The clock is ticking. Companies effectively guided by a multilayered approach of enterprise risk management, operational risk management and unified risk oversight are better positioned to adapt and protect.

Visit the Security Executive Council website for other resources in the Risk-Based Security: Board Level Risk/ERM series.

About the Security Executive Council

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 security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more**.**

Contact us at: contact@secleader.com

Website here: https://www.securityexecutivecouncil.com/