Security State of the Industry: Is Enterprise Risk Management (ERM) Enough? Security's Opportunity

The Security Executive Council's Security State of the Industry briefings are a benefit offered to our Tier 1 Security Leaders.

We are pleased to share this excerpt of our briefing on Executive Influence with our newsletter subscribers.

SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Sharing Today:

- Bob Hayes, Managing Director, SEC

- Kathleen “K2” Kotwica, EVP & Chief Knowledge Strategist, SEC

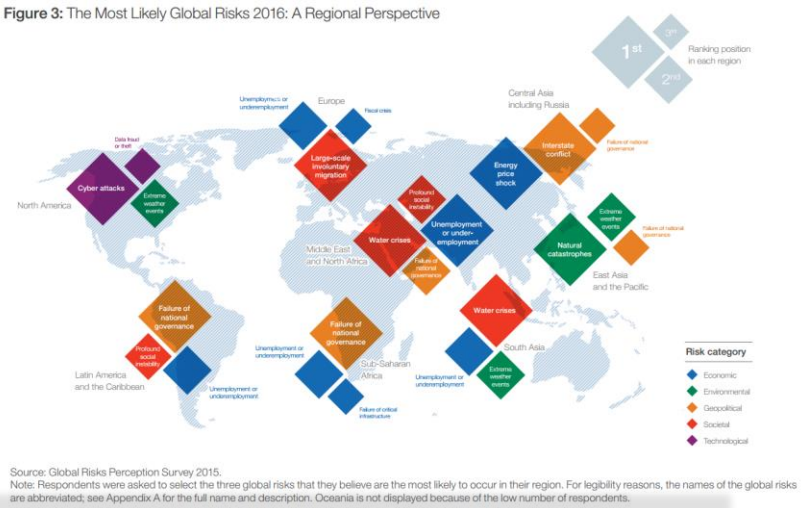
- Francis D’Addario, Emeritus Faculty, SEC

- Dick Lefler, Emeritus Faculty, SEC

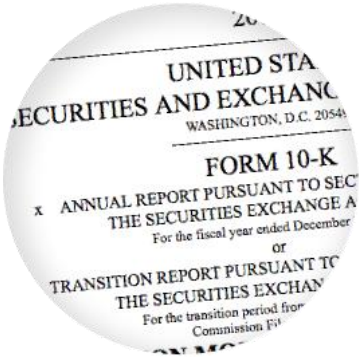
- And Tier 1 attendees like you

For bios visit: About Us

Enterprise Risk Assessment



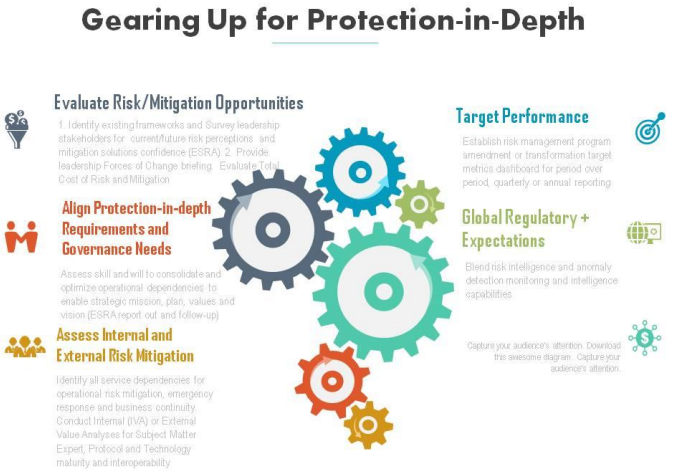
10K requirement



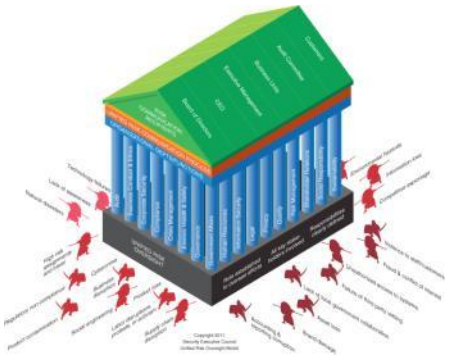
Over the last 10 years there has been a transformational shift in the way executive management views and deals with risk. Of the multitude of the most significant risks identified in the ERA – executives only attend to the top 10 – 15 to make sure they are addressed.

The ERA Common Process:
Third party audit > Corporate-wide risk review > Senior management chartered to respond to results > Report to the Board

SEC's Enterprise/*Security* Risk Alignment



The SEC set the stage with Enterprises Security Risk Alignment (E/SRA) using our Board Level Risk research and the concept of Unified Risk Oversight to encourage teamwork among the corporate organizations with risk mitigation responsibilities



The SEC E/SRA Core Process

Stakeholder Interviews > Risk Assessment (gaps) > Program Review > Benchmarking > Reporting

Current Research: Enterprise Risk Management (ERM)

An ERM Definition

ERM is an integrated systematic process of identifying major risk to achieving the specific goals and objectives of the organization. These risks should be analyzed by likelihood and impact and mitigated to an acceptable level of residual risk.

Contrasting GRC and ERM, 2013
The Institute of Internal Auditors Research Foundation

I'm going to cover some research on Enterprise Risk Management (or ERM) – this we are going to use to inform us on the current business perspective on managing risk across the enterprise

Current Research: ERM

About **60%** of organisations worldwide agree that they face a wide array of complex and increasing risk issues.

* Despite that, ***35%*** *or fewer organizations claim to have formal enterprise risk management in place*.

* About 70% of organizations *would not describe their risk management oversight as mature*.

Global State of Enterprise Risk Oversight 2nd edition, CGMA

While 59% believe that the volume and complexity of risks have changed "extensively" or "mostly" in the last five years, ***only 25%*** *believe their organization has a "**complete** formal enterprise-risk management process in place."*

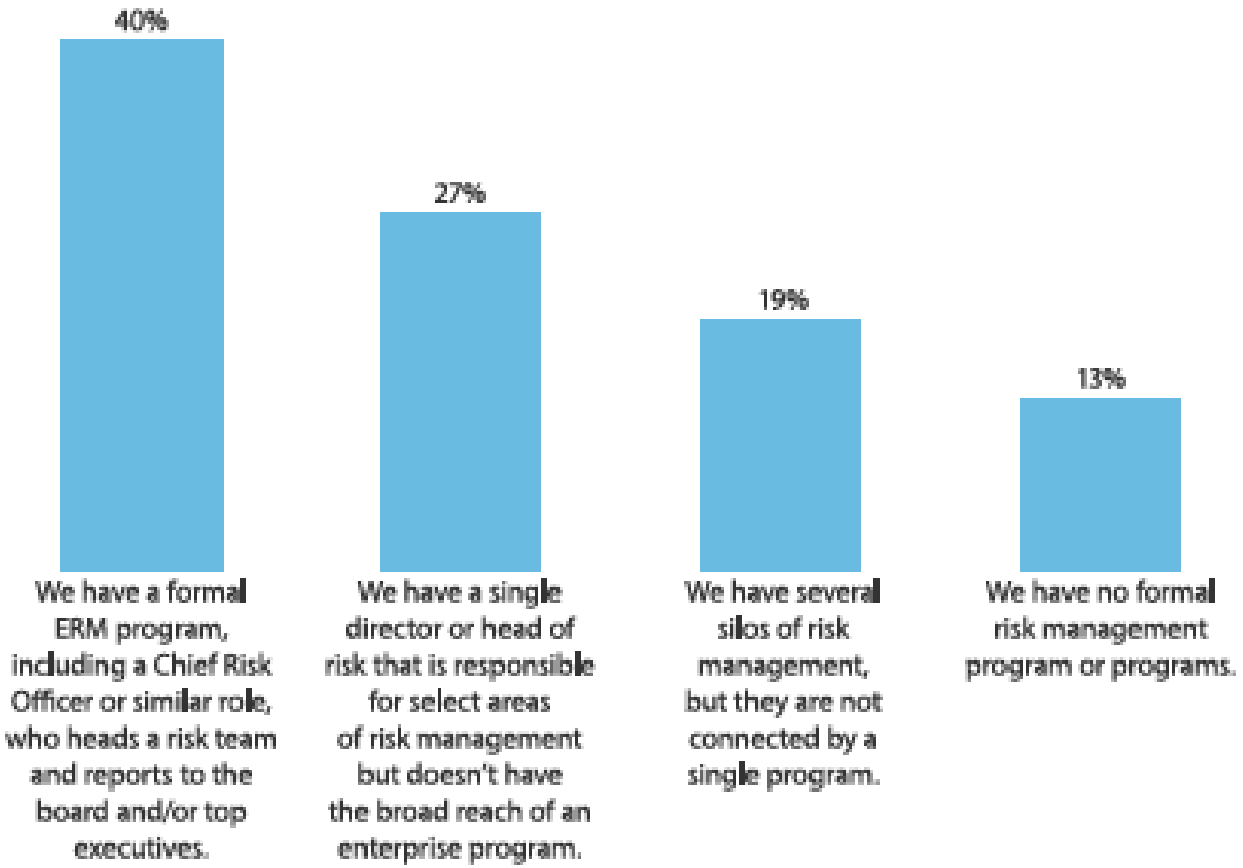
45% have a management-level risk committee and those committees meet at least quarterly.

2015 Report on the Current State of Enterprise Risk Management
NC State University, Poole College of Management, Enterprise Risk Management Initiative

Current Research: ERM

Figure 1 ERM Program Formalization

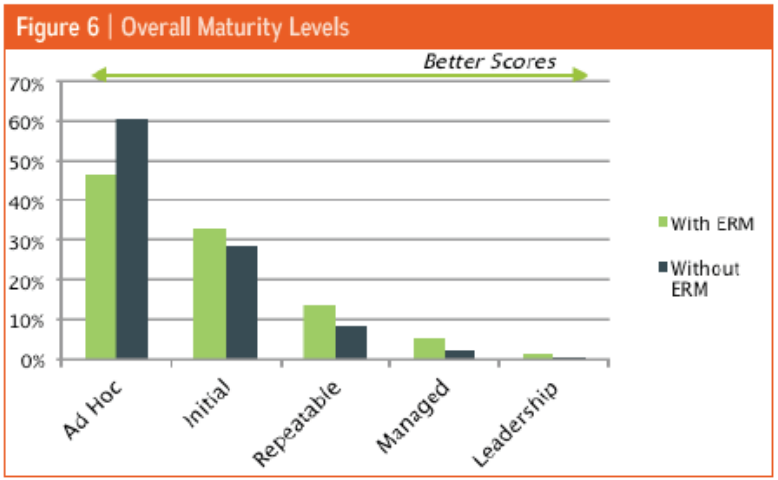
"Which of the following best describes your organization's risk management program?"



Base: 188 risk management decision-makers, influencers, or contributors

Source: Forrester Research & Disaster Recovery Journal: The State Of Enterprise Risk Management 2016

Current Research: ERM



State of ERM Report 2015, RIMS

These results show having an ERM program in place has an advantage but it's not a *drastic* difference compared to not having one. The questions this and the previously mentioned research raises are: Why is this? Communication break-down? Lack of consensus on risks or defining the risks? Just too difficult to get the processes embraced across the organization? Is it at too high a level?

Comparing the Two (examples)

An operational risk council is a smaller, faster, cheaper group - capable of recognizing emerging risks.

ERM – Business Risks

- Currency translation
- Sustainability
- Accounting & reporting
- Product/service failure
- Knowledge drain
- Competition
- Capital availability
- Mergers & Acquisitions

E/SRA – Operational Risks

- Supply chain & business disruption
- Lack of risk awareness
- Product contamination
- Cyber security
- Workplace violence
- Threat mismanagement
- Misconduct

Operational Risk Council is Security's Opportunity

Let's go over some benefits of an ORC.

Security's Opportunity

- Operational Risk Council:
  - Influence security/safety across enterprise
  - Identify emerging and residual risk mitigation gaps
  - Collaborate w/ stakeholders to ID risk
  - Review/advise executive management
  - Inform cross-functional situational risk awareness
  - Recommend organizational resource allocation
  - Eliminate redundancies

Why Does Enterprise Risk Management Fail? Why an Operational Risk Council?

1. Lack of executive management support
2. Reckless risk taking
3. Poor governance and “tone at the top”
4. Practicing ELM (Enterprise List Management) instead of ERM

Senior management has never been more aware of risk mitigation. Security needs to be on the risk bandwagon.

ORC is not just another risk committee - this one fills the gap between the top 10 or so enterprise risks and those that occur or emerge in day-to-day operations.

Panel Discussion

Tier 1 Security Leaders discussed:

- ORC options
- Risk council frameworks in their organizations
- How to best get an ORC started
- and more

Security State of the Industry Briefings

We want security practitioners to be prepared for forces of change that impact their security programs. To that end the Security State of the Industry briefings are where security practitioners come together to share valuable information that can be applied to their security programs. Topics are cutting-edge and relevant to today's issues.

The Security State of the Industry briefings are only available from the Security Executive Council. No other research and advisory firm can offer the level of depth and breadth of knowledge about the trends and future state of security risk mitigation because no other organization has the necessary resources and experience.

Will you be adding the Security Executive Council to your security risk mitigation team? We'd enjoy discussing our services with you. Contact us at: contact@secleader.com

See our website for more information: www.SecurityExecutiveCouncil.com