# The Future of Risk - Creating a Framework for Growth of the Corporate Risk Function


## Gregory M. Keches



**Abstract** Risk management functions have grown considerably in the past decade from small units focused on financial risk and regulatory compliance to large armies covering diverse threat portfolios. Spawned by an increase in regulatory requirements and burgeoning external threats, these functions have been saddled with an ever-flourishing scope. Corporate leadership, now looking for new risk management skillsets and technical expertise to battle these threats, is facing a lack of qualified personnel and pressure on operating budgets. Even more difficult is the rise in new technology and the need for corporations to quickly adjust their operating models, sometimes at the behest of security and risk management.

To adequately manage risk in the Digital Age, companies must broaden their understanding of risk management from simply avoiding risk, to embracing it in context. A continued downside risk management focus will only provide a framework for resiliency, but will not allow the company to be a disruptor in the marketplace. Corporations that embrace a broader understanding of risk will find a competitive advantage at the end of their efforts. Current risk frameworks and standards do not provide the right mentality or mindset shift to address risk management, as they were designed for risk professionals. A competency, tools, and rules based approach to managing risk has left companies focusing on the wrong outcomes and has continued to increase risk management budgets without results. Risk and compliance capabilities in the organization must also provide strategic insights and must move towards a proactive posture. By infusing risk insights into daily business processes, corporations will be more coordinated and connected over the long term.

*Critical Question: How can we improve upon the risk categories and structures of COSO/COBIT? What categorization of risk would allow for the best possible risk response and control mechanisms?*

*Critical Question: How can companies integrate risk management functions and create a more effective management structure that doesn't require thousands of employees to adequately manage risk?*

*Critical Question: How can companies take the IIA "lines-of-defense" model and improve it to fit the needs of the digital age?*

*Critical Question: What steps can corporations take to disrupt their current risk management function and provide better visibility to their portfolio of risks?*



**Keywords:** trust, integrated risk management, holistic risk, three-lines-of-defense, LoD, risk management, cybersecurity, corporate resiliency, adaptive governance, product and service management, risk frameworks, COSO, COBIT, NIST 800-53, cybersecurity standards, risk governance,

## Introduction – Creating a Framework for the Future of Risk Management

### The Problem Addressed

First this paper will establish cybersecurity in the context of the digital revolution, and more importantly, as a singular thread of the larger risk management institution. Building off this context, the paper will address this broader risk management operation as highly siloed and not functioning as anticipated. It will also establish that these functions were built by risk professionals, for risk professionals. While suitable for managing regulatory compliance and threats in view, these functions are overspending and having difficulty staying agile with rapid technology shifts.

### State of the Art Approach Pursued

With the problems risk management functions face today, this paper will then provide interviews to support these claims with reputable executives currently working in the field of risk management. These executive discussions include feedback from:

- Chief Audit Executive of a Fortune 100 Consumer Products & Retail Company
- Chief Audit Executive of a Fortune 100 Mining and Industrial Products Company

### Solution Proposed

This paper will then introduce three concepts that suggest changes to risk management programs. These concepts include balancing risk management, simplifying risk operations, and developing a uniform process model to which all risk functions can align. The paper will then propose short-term objectives to further improve the integration of risk management functions in today's modern corporations. Finally, the paper will develop a framework for the inclusion of executives and c-suite team members into the risk management process through taking a novel approach to the risk management discussion.

1. Start with a Balanced Portfolio of Risk
2. Simplify Risk Response
3. Drive Towards Outcome Based Risk Management
4. Focus on Short Term Objective Change
5. Design for Long Term Risk Management

### Long Term Objectives

This paper will conclude with suggestions for long term remediation of risk management and insights into the future of risk management. The paper will cover the topics of integrated risk management data repositories, intelligent decision making through neural networks, connected risk management systems, and broader hopes for the consolidation of risk functions.

**Cybersecurity in Context**

Cybersecurity grew from humble origins. With the need to manage growing identity and access management solutions and to additionally provide support of database architectures, security teams were more focused on operations over external threats. In the mid 1990's, however, Sarbanes-Oxley (SOX) changed the landscape.[1]

| | | | |
|---|---|---|---|
| Enterprise Risk | Third Party Risk | Cyber Risk | Financial Risk |
| Environmental Risk | Physical Security Risk | Regulatory Compliance & Legal Risk | Country & Geopolitical Risk |
| Health and Safety Risk | Business Continuity & Disaster Risk | Strategic Risk | Supply Chain & Procurement Risk |

*Figure 1 - Cybersecurity in Context.*

Both Finance and IT teams were burdened through SOX with providing reasonable assurance for Financial Audits. While regulatory compliance had been a part of corporations, Sarbanes-Oxley provided a new level of rigor that would only continue to grow. The Public Company Accounting Oversight Board (PCAOB) would then continue to raise this level of rigor for decades. With continued scrutiny from auditors, once small IT departments were growing audit and compliance functions to meet this assurance demand. Criminal liability now falling on CFO's, the need for robust risk programs was established. Corporations realized that they needed to put more checks in place, so assurance divisions began to push security teams to account for their complex designs. This promulgated a rapid growth of ERP implementation support. Security designs became more challenging with Roles-Based Access Controls (RBAC) and fine-grained security meant that auditing logical access by hand was no longer an option. GRC software was born to cater to this heightened governance analytic need.[2]

It wasn't just finance and cybersecurity compliance though. Other government regulations for environmental compliance, new trade laws for international transit of goods, and international norms all created additional risk and compliance groups in the heart of America corporations. The dream of globalizing operations through the internet and the desire to bring goods into new markets also brought the need to abide by international laws. Yet, with increasing geopolitical threats, and the desire to advance business in this now interconnected world, the standard risk management function would become highly complex and spread across all operating units of our corporations.

Risk and compliance functions today are larger than they've ever been, and an increasing number of professionals execute on risk management tasks as part of their daily jobs. Each team is also tasked with managing their risk management portfolio, including:

- Planning - Supporting **budget and resourcing**
- Design - Management of **Risk Taxonomy's** and risk definitions
- Execution - Focus areas for **Testing and Monitoring**
- **Technologies** used to manage risk programs
- **Remediation** management of identified issues
- Readout - **Communication** to internal and external stakeholders



[1] Hanna, Julia. "The Costs and Benefits of Sarbanes-Oxley." March 10, 2014. Forbes Magazine. https://www.forbes.com/sites/hbsworkingknowledge/2014/03/10/the-costs-and-benefits-of-sarbanes-oxley/#59b237c3478c

[2] Market Research Future (MRFR). "Enterprise eGRC Market 2018." MarketWatch. https://www.marketwatch.com/press-release/enterprise-governance-risk-and-compliance-egrc-market-2018-global-analysis-industry-growth-opportunities-business-strategy-emerging-trends-competitive-landscape-and-regional-forecast-to-2023-2018-09-27

These employees, however, are likely operating within a silo of their corporation, and in most circumstances, risk management is not their full-time job. While Finance employees could be focused on working through Sarbanes Oxley or Graham Leech-Bliley, procurement departments might be tasked with working through vendor risk profiling and Third-Party Risk management. Legal departments are tasked with regulatory compliance and trailing legal liabilities, while HR is focused on maintaining employee safety and rights. In the current response to risk, these groups are vastly different and are strongly connected only through leadership teams. These leaders, however, do not see them as interconnected risk management functions. Rather, these risk units appear to be merely cost-centers within each vertical of the corporation. These functions do have one common goal: **avoiding pitfalls for our companies and ensuring that compliance and remediation where necessary.**

Cyber risk in this context, however, is slightly different. Cybersecurity's presence is pervasive not only through each singular risk department, but rather across all these independent functions. Cybersecurity is uniquely responsible for the delivery of critical data across corporate networks and is responsible for the monitoring tools and technologies that allow these other risk units to survive and thrive. This reality for cyber will be important to its own future as a function and responding body. It is in this light that this paper will tackle cybersecurity in its broader context of corporate risk management. This paper tackles the broader hopes of risk management in the understanding that cybersecurity is a key driver for all aspects of the risk landscape.

## Risk Management Through the Lines-of-Defense

An adequate and interconnected operating model was established through the risk function's exponential growth. With a lack of an operating model for risk management, and no singular agreement of risk governance, the Institute of Internal Auditors (IIA) worked in 2013 to create new frameworks to understand governance risk and compliance[3]. The IIA ultimately created the three-lines-of-defense approach to risk management. This model was established out of the necessity to delegate control ownership effectively, and to also design independent assurance into the corporation. This design held that the business units were responsible for their own controls where a 2nd line monitoring and 3rd line assurance function would help align their controls to external regulatory needs. Figure 1 provides a detailed overview of the model.

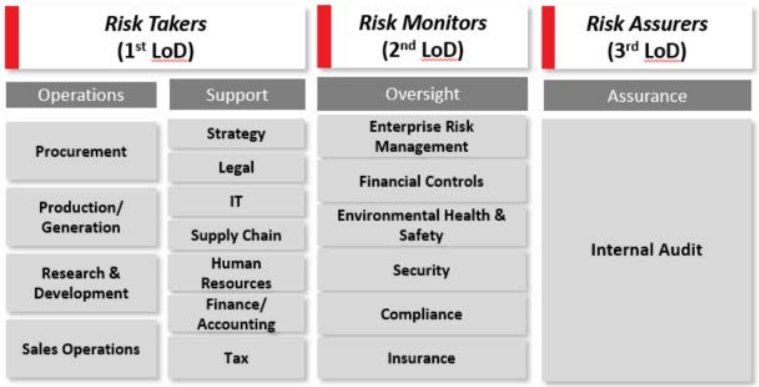


*Figure 2 - The Lines-of-Defense.*

## Problems Addressed - The Failures of the Three-Lines of Defense

While a strong model for segregation of risk duties and risk function completeness, the three lines-of-defense causes division amongst organizations and creates a few key issues, the first of which is the

[3] THE IIA. Lines of Defense. 2013. IIA - Standards & Guidance - Three Lines-of-Defense

misaligned risk education amongst the model's lines. When the IIA divorced controls expertise (3rd line auditors) from the operating business units (1st Line Risk Takers), the business unit operators were left with a misunderstanding of what they are supposed to guard against. These 1st-Line business operators were never controls experts, and they specifically we're never meant to be operating in a silo against only their individual controls. Furthermore, educating an entire company on proper risk management techniques and frameworks is infeasible given the continued change in those techniques occurring exponentially.

The second key issue with the lines of defense was the lack of a holistic view of risk management. Companies that adopt a three lines model end up with many different stakeholders across their business taking control of singular risk domains. This creates a fractured view of risk management as there is no intrinsic tie between enterprise risk management programs and operating procedures that tackle residual risk.

The final issue with the lines of defense is the continued audit fatigue driven by internal audit and 2nd line risk functions. When Internal Audit (or External Audit) needs to validate the operations of the 2nd line monitoring function and 1st line operations, these groups are attacking business units with audit requests. These requests are notably painful, as they are constant and detailed. Each audit function additionally has different scopes and regulations to support, thus leading to similar requests for data throughout the annual cycle. While most notable in public companies, SOX requirements continue to provide an additional high level of burden along with growing cyber activities.

This state of constant monitoring has given many stakeholders a pejorative view of audit and security teams. Even further, some view internal audit as not actually providing any value to the company.[4] When addressing the future of risk management, we must move these functions from being a simple cost-center to a profit-center.

**Problems Beyond the Lines of Defense – Shifting Funding & Increased Regulatory Burdens**

Unfortunately, the lack of cohesion between each risk function (legal/audit/IT Risk) has led to different systems and data structures to support their individual efforts. This has made risk management, and ultimately cybersecurity very difficult to define. With IT being involved in these mitigation plans and programs, the burden of the information security professional is relatively high. We are now faced with the largest threat landscape in our corporate history:

| **Financial Risk Burdens & Mega Trends** | **IT Risk Management Mega Trends – Lack of Cybersecurity Talent & Education** |
|---|---|
| • IT Departments are rapidly moving their posture and starting to leverage external vendors, this is creating a third-party risk growth trend.<br>• Automation is increasingly taking over the jobs of finance/accounting professionals and there is currently a lack of skillset to run configuration management and monitoring.<br>• Security & Access Management will now include bot security and new ecosystems that required greater control. | • There is a well-known cybersecurity professionals gap and talent shortage<br>• Cybersecurity concerns are divorced from the business units and are usually misunderstood by boards and leadership. |



[4] Chambers, Richard. "No Internal Audit? It Could Be Worse." Internal Auditor Magazine. Oct 24, 2016. https://iaonline.theiia.org/blogs/chambers/2016/Pages/No-Internal-Audit-It-Could-Be-Worse.aspx

| | |
|---|---|
| **HR Risks – New Employee Types and Greater Disconnect between Onboarding and Cyber**<br>• Insider threats and employee behavior are new risks that we have difficult managing<br>• Constant turnover of employees causes headaches for IT compliance and can promote great cyber compliance issues<br>• Creation of new employee types means that we now have plenty of new threat vectors and entrants to our environments. (Contractor/Vendor/Third Party Infusion/ Gig Economy)<br>• Management of Company Culture in diverse employee type scenarios means that conveyance of security and awareness training is now more difficult than ever. | **Supply Chain & Product Delivery Risks**<br>• Global Trade Regulations will continue to push new cybersecurity demands as our global economy shifts towards macro-cyber.<br>• Sourcing of Materials will now put further risk into your supply chain as parts and products are produced outside of your digital cyber view. (IE: Parts will have IoT or digital aspects that will reside outside your CISO's control).<br>• Geopolitical influence and Tariffs & Rapidly fluctuating Capital Markets will draw cybersecurity spend away from the IT department as CEO's deal with great liquidity concerns.<br>• Transfer Pricing & Tax systems management will also need greater control with increased globalization and regulatory compliance needs. |

With concerns mounting, it's time to rethink information security governance and regulation. The three-lines-of-defense is no longer operating as anticipated. The lines model provided only a division of labor but has led to inefficient programs and has not generated the best technology or GRC systems architecture.

**Interviews in the Marketplace – Stress Testing Risk Management and Findings the Largest Challenges**

To find out how risk management and the lines-of-defense were working in the marketplace and discuss potential points for improvement, two interviews were conducted with tenured Chief Audit Executives (CAE's). The first interview was conducted with the CAE of a Fortune 100 Consumer Products company in December 2018 while the second was conducted in June of 2018 with the CAE of a Fortune 100 Global Industrial Products and Manufacturing company. Results from these sessions provided detailed insights into four critical areas of risk: visibility, intelligence, data, and relationships. In summary, the main issues seen from these risk leaders are summarized as follows:

| | |
|---|---|
| **Risk Visibility – The Disaggregation of the Risk Function**<br>Risk Management functions are typically built from the third-line-of-defense backwards. (IE: The regulatory and compliance demands, controls framework construction, and effective remediation strategies are all managed and governed by an independent assessment body). As a result, Risk Functions are currently not able to understand the breadth of the 2nd line of defense services and most risk functions do not have good data management. | **Risk Intelligence - Tools & Technology – Risk is Unprepared for the Future**<br>Risk Management is currently not prepared to handle the influx of digital age technologies (IE: Artificial Intelligence, Augmented Reality, Virtual Reality, Blockchain, Robotics Process Automation). Risk Management tools and utilities were built mostly as workflow compliance tools and are not geared towards managing upside (strategic) risks. |
| **Risk Decision - Organizational Relationships**<br><br>Risk Management is strongly considered a cost-center and is continuously underfunded as a result. Risk Management is also identified as a burden to individual business units and many stakeholders feel it is not providing direct value to their everyday job function. | **Risk Agility - Data Management**<br><br>Risk Management functions rarely leverage external data providers and do not currently have strong access to a consolidated data lake that supports all domains of risk. |

While these revelations might not be felt by all corporations, this message was clear to the executives from having participated in round tables and consulting discussions. It is with these well-known issues that we must deconstruct risk operations and rebuild a new set of heuristics for managing risk. The following sections will describe how to respond to these key issues and how best to make strides in the short term. A longer-term proposal will follow.

**Starting at the Finish – Outcome Based Risk Management**

Risk management can provide strategic value beyond audit if appropriately constructed. This journey towards value added risk management begins with looking to our collective objectives for risk services.


*Figure 3 - Outcome based Risk Management.*

Risk management was built through creating risk universes and then applying controls to mitigate those risks. This process is aided through leveraging risk universe frameworks from NIST (800-53) and other standards bodies (IIA/COSO/COBIT). While helpful for downside risk management, these frameworks and their respective implementation are left to controls experts in the 3rd line of defense. It is therefore incumbent on risk professionals to change the approach from a "frameworks-only" model to aligning risk management with strategic objectives and purpose-led missions. To best compel this approach, risk professionals must be more outcome driven. This paper proposes four easy to understand outcomes of risk management[5]:

- **Balancing** the portfolio of risks to further engage corporate leadership in the risk process
- **Instilling** a culture of risk across their organization to drive ownership of balanced risk agendas.
- **Digitizing** risk solutions to drive better data visibility and response.
- **Embed** sustainable response to their risks and allowing for a platform for growth through stronger trusted relationships with their customers, vendors, employees and regulators.

To arrive at these outcomes, the following key short-term activities arise:

| Section 1 – Balancing Risk to Include Strategic Discussions | Section 2 – Simplifying Operations – An Easy to Understand Approach to Risk Management | Section 3 – Developing a New Operating Framework – Digitizing and Embedding Risk in the Business |
|---|---|---|



[5] Bones, James. "The 3 Dimensions of Risk." September 9, 2014. Corporate Compliance Insights. https://www.corporatecomplianceinsights.com/the-3-dimensions-of-risk/

## Section 1 - Beginning with a Balanced Portfolio of Risk – Upside, Outside & Downside Risk

Balancing risk requires understanding how it has been categorized to date. COSO/COBIT requires an organization to assign and manage the following risk types:

- Strategic
- Financial
- Operational
- Regulatory

A better categorization of risk is as follows[6]:

- Upside Risk
- Outside Risk
- Downside Risk


*Figure 4 - Risk Domains*

These categories are broader and can help leadership understand the actual effect of a risk in context of the company's daily operations.

## Outside Risk Definitions

Outside risks are outside the organization. These risks are generally issues that the company chooses not to respond to currently, and they fall into two separate categories:

- **Black Swan Outside Risks[7] -** The first type are risks that the corporation will likely never directly respond to (i.e. earthquakes, volcanoes etc.) These specific "black swan" risks would be covered by insurance/ reinsurance or other business resiliency measures.

- **Emergent External Risks[8] –** Emergent External Risks are geared towards disruptive technology and typically have a high level of uncertainty mixed with a lack of consensus. They can specifically be concerns that the organization believes are not currently timely or relevant to their current state of operation. An example of this might be 3-D printing or new technologies that are not disruptive due to technical/cost limitations today. These risks, however, are something these companies will watch as they believe it would be problematic in the future.

It is through these two definitions of outside risk that we can start to see a new operating model emerge. All risks start by appearing outside and can then be adequately assessed for risk programming as they approach the corporation; disaster Recovery, Insurance and Business continuity become



[6] Kaplan, R. and Mikes, A. "Managing Risks: A New Framework." Harvard Business Review. June 2012. https://hbr.org/2012/06/managing-risks-a-new-framework

[7] Rio Tinto. "Black Swan Events, Population Misconceptions." IRM NW Seminar. P2-10. https://www.theirm.org/media/1120524/Popularmisconceptionsaboutblackswanevents-JohnSummers.pdf

[8] Parija et al. RIMS Executive Report, The Risk Perspective. "Emerging Risks and Enterprise Risk Management." Risk Insurance Management Society, Inc. https://www.rims.org/resources/ERM/Documents/EmergingRisk_ERMweb.pdf

paramount for "Black-Swan" events, whereas hedging and investment for disruptive technologies becomes paramount for emerging risks.

**Downside Risk Definitions**

The second risk domain is Downside risk. This category encompasses the typical threats in most risk portfolios. Response mechanisms include EHS, Physical Security Risks, IT and Cyber risk teams, financial risk groups, fraud departments, and regulatory compliance units. Unfortunately, most organizations simply cannot manage all the regulations that they need to comply with, and measure how they are doing related to that compliance. These procedures are rarely cost effective and continue to grow in headcount and cost every year. To combat this, companies are establishing risk management programs to gain visibility to all regulatory compliance needs across the entire globe. Corporations are also seeking to monitor for things on the horizon and to build enhanced risk platforms.

**Upside Risk Definitions**

The last category of risk is Upside risk (sometimes called Strategic Risk)[9]. Where executives tend to hear risk, they believe it to be only focused on negative consequences. There is an equal opportunity to see risks that will provide new opportunity[10]. Upside risk encompasses those risks taken when moving into a new market or offering a new service. These risks can also involve moving operations into new countries or selling across international borders. Yet, these types of risks are typically overlooked by Enterprise Risk Management (ERM) programs today. As a result, organizations feel they are not getting value out of ERM, despite not truly understanding the consequences of their actions.[11] In order to change this mindset, we must provide for a way to gain leaderships attention.

**Providing a Balanced Risk Agenda to Gain Leadership Attention[12]**

Risk executives are expected to present downside risks and how they are managing them with headcount and key personnel. While effective at managing regulatory demands, these conversations are typically left to audit executives to manage and rarely include a broad array of professionals. A balanced agenda of risks, inclusive of upside risks, will gain leaderships attention and provide for better discussions. When bringing the corporations strategic objectives into the frame, there is much greater willingness to participate in risk management. But their attention to these programs must then be tied to a simplified way to understand progress.

**Mechanism for Response & Tracking Progress**

Once corporations categorize their risks appropriately, they can determine how best to help manage their response efforts. Upside risks will be monitored with Key Performance Indicators (KPI's), as well as Key Risk Indicators (KRI's). These indicators and response mechanisms can then be aggregated by Governance, Risk, and Compliance (eGRC) technologies and consistently reported to leadership. This process provides a foundation for continued review of risk and its inherent tie to the ongoing objectives of the firm.



[9] Hubbard, Douglas W. "The Failure of Risk Management." 2009. P.26

[10] Freedman, Anne. "The Upside of Risk. Organizations win when they integrated risk management into strategic decision-making." June 2016 Issue. Risk and Insurance Magazine. https://riskandinsurance.com/the-upside-of-risk/

[11] DeLoach, James. "5 Common Risk Management Failures." Corporate Compliance Insights. April 1, 2016. https://www.corporatecomplianceinsights.com/5-common-risk-management-failures/

[12] Ovans, Andrea. "Capturing the Upside of Risk." Harvard Business Review. June 27, 2012. https://hbr.org/2012/06/capturing-the-upside-of-risk

## Section 2 - Instill - Risk Management Simplification - Reducing the Risk Function to its Essentials

A balanced risk framework with corporate leadership support provides a strong foundation to subsequently manage and respond to risks. Moving away from standards and frameworks, corporations must break down the risk function into simple critical steps that are outcome focused. Where the Lines-of-Defense created segregation of duties, we must now look to bring our disparate risk functions together. First, educating the business units on their responsibilities and drawing connections amongst key risk stakeholders in all elements of the business is required to drive successful risk response. This education must be simplistic. No matter what type of risk management process, we must teach our business counterparts that there is effectively the same cycle propagated to monitor and respond to risks. The methodology can be summarized in the following simplified steps:


*Figure 5 - Simplified Risk Management Model*

- **Step 1:** Scan the environment for risks and collect data[13]
- **Step 2:** Deliver that internal and external data to the appropriate business stakeholders to make decisions
- **Step 3:** Allow the business to act upon that data in an informed manner and repeat the cycle, further minimizing, accepting, or mitigating risk.

This is a critical change from standard risk frameworks as it provides a basic way to discuss risk response with executive stakeholders and business functions. Rather than trying to provide comprehensive risk frameworks and alignment to standards, the scan, deliver, act methodology can be utilized for any type of risk. This breakdown will help further help all 1st Line-of-defense parties to understand the key steps in responding to risk, and will create a culture of risk management through an easy to understand process. A business risk team member can start to effectively engage by understanding how to scan the environment for risk, request the appropriate data to respond, and then track the divisions response effectively. While reductionist, this is how risk management professionals must start to instill risk mindsets across our organizations.[14] This process is additionally used as part of the OODA Loop and military decision management.[15]

### From Data Collection to Data Delivery

Risk management must also move from being a data collector to becoming a data provider. This delivery of strong data allows the business to take better responsibility and control of the risks they are assigned, and further, allows them to utilize that data in daily operations. Delivering data assists in planning a response to risks, and implementing systems that harness risk intelligence and distribute that intel to the appropriate parties. This is a fundamental change in risk management. Data collection for



[13] Banham, Russ. "Scanning the Risk Horizon: Industry Veterans Discuss Strategic Planning." April 1, 2016. Risk Management Magazine. http://www.rmmagazine.com/2016/04/01/scanning-the-risk-horizon-industry-veterans-on-their-roles-in-strategic-planning/

[14] Wharton Public Policy et al. "Re-Thinking Risk Management: Why the mindset matters more than the model." University of Pennsylvania. Apr 15, 2009. http://knowledge.wharton.upenn.edu/article/re-thinking-risk-management-why-the-mindset-matters-more-than-the-model/

[15] Sturm, Mike. "The OODA Loop: A Tool for Better Decision-Making." Medium. March 11, 2017. https://medium.com/personal-growth/the-ooda-loop-a-tool-for-better-decision-making-that-youre-already-using-ca24a3fa8c5c

the sake of audit and response is arduous and does not provide value to the business, other than simple assurance of intended function. Providing risk intelligence to the business units themselves and allowing them to control effectively provides better support for strategic objectives and long-term sustainability. While many BI tools and utilities do this today

**Section 3 - Digitize and Embed Risk Management - Process Model**

The scan, deliver, act methodology presented above can be further broken into component parts. Scanning the environment for risk involves the identification and prioritization of upside, outside and downside risks. After creating an appropriate risk universe, companies must plan an appropriate response and implement mitigation strategies. Finally, companies must monitor those previously identified risks and provide for an independent assessment mechanism. The proposed Uniform Risk Process Model (URPM) is presented in Figure 6, focuses on the following:

- **Scanning Breakout:** Identify and prioritize inherent risks effectively,
- **Delivering Breakout:** Implement systems to respond efficiently and
- **Acting Breakout:** Track progress against key risk objectives.


*Figure 6 - Risk Management Fundamentals – The Uniform Risk Process Model (URPM).*

The proposed URPM helps any corporation balance their risk portfolio and additionally helps focus on all aspects of the risk universe (not just independent assessment and internal audit procedures). This model also brings all lines of defense into view.

With the URPM, companies can apply the model across their organization to see if risk is being adequately managed in all verticals. Where the lines-of-defense provided for a segregation of duties and independence, it equally did not provide for an integrated approach to management. This URPM, however, provides a simple flow that is uniformly applicable to all types of risk management.

**Summary of Short Term Objectives**

Corporations must balance their risks to include upside, outside and downside perspectives[16]. They must then educate their professionals to understand a simplified model of risk management that includes scanning the environment continuously, demanding appropriate data to track those scans, and effectively acting upon that data with traceability. While these short-term objectives can help to clean up and augment risk management processes to be more efficient, these suggestions do not solve for some of the longer-term concerns around developing data, intelligence and GRC platforms necessary to continue efficient growth.



[16] ERM Initiative Faculty et al. "Risk Governance: Balancing Risk and Reward." Enterprise Risk Management Initiative. Oct 1, 2009. https://erm.ncsu.edu/library/article/balancing-risk-reward

## Addressing Long-Term Objectives for Corporate Cyber Risk Governance

To establish risk program objectives and a thoughtful installation of the Uniform Risk Process Model, corporations must focus on the following five objectives:

1. Adaptive Governance
2. Data Intelligence & Architecture
3. Customer Journey
4. Resiliency
5. Intelligent Decisions

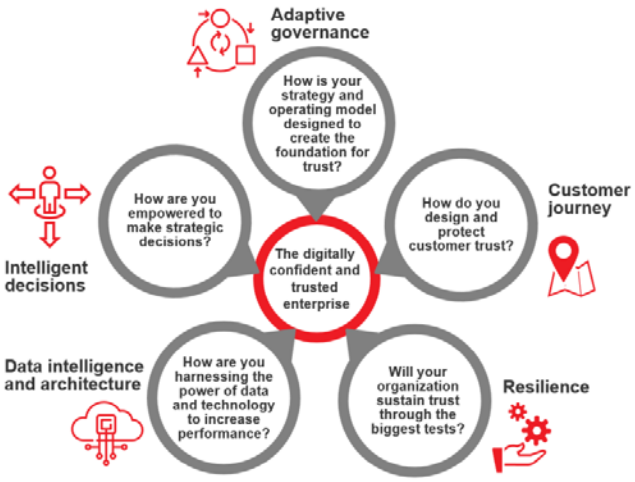


*Figure 7 - Long Term Risk Management Objectives & Discussion Points*

These pillars provide for an ongoing assessment of whether the URPM is being effectively applied, and whether gaps in risk management exist.

### Objective #1 - Adaptive Risk Governance – Getting the Right Corporate Culture & Understanding in the Boardroom

A Digitally-led risk management function must start with a strong purpose and a governance model[17]. A strong adoption of the Uniform Risk Process model aligned to the IIA lines-of-defense will create a foundation for embracing risk management. This new purpose-led risk function focuses on creating a culture of embracing risk across the organization and leverages diverse talent models to drive outcomes. The following represents critical steps to adopt adaptive governance:

- **Step 1 – Gain Consensus amongst the Organization -** The case for change begins with gathering the management together and showing them the cost and disparate organizational units that are part of the information security domain. WE must make the cost of inefficiency in cyber real.

- **Step 2 – Make a Conscious Choice about Working Together –** Described to leadership that cyber is a responsibility beyond just the folks down in the data center and that real connectivity must be made across all operating risk units.

- **Step 3 – Enable that Choice through Technology –** Demand that there must be a better solution for risk management. Make a goal as an organization to point your efforts towards a north star of better decision making through best-in-class reporting and visibility.

### Objective #2 - Solving the Data Problem – Better Data Intelligence & Architecture

Corporations must strive for a more connective framework to tie Enterprise level risk to strategic cyber programs. This will require rethinking GRC vendor architecture and current risk data models. A better workflow for risk management and a potential architecture for the next generation of GRC tools is necessary. It's natural for our companies to attempt to categorize and manage risk. As a result, we

[17] Bjerga, Torbjorn. "Adaptive Risk Management Using New Risk Perspectives – An Example from the oil and gas industry." Elsevier: Reliability Engineering & System Safety. Volume 134. February 2015. Pages 75-82.

have created neat category systems and buckets to dump company problems. What makes this challenging is that each type of risk needs a certain set of criteria that might not be helpful for other risks. This creates data collection issues and a broader risk data management challenge, beset with privacy concerns and additional cybersecurity needs.

**Objective #3 - Embedding Risk and Cyber Principles into Product & Service Management**

Companies must build linkages between their business and risk management functions to embed trust in the design process. Once business units understand that cybersecurity and risk management is a competitive advantage, they will start to apply cyber cost as added overheard through their manufacturing process. The classic control framework will transition from 'process, risk, control' to also include additional attributes that tie directly to the product and service manufacturing. Rather than having specific controls dedicated to security, there needs to be a mosaic of controls dedicated to corporate mission objectives.

**Objective #4 - Solving for Risk Intelligence / Automation – Bringing Enhanced Digital Age Technologies to Reduce Governance Inefficiencies**

Companies must embrace real-time risk identification, instead of utilizing historic data. With the advancement of technology and new data sets, risk insights will be generated using machine learning and artificial intelligence. To embrace this advancement of analytic technology, companies must hire professionals with digital skillsets and technologies into Risk Management Positions. This includes expertise in machine learning, artificial intelligence, natural language processing, as well as data architects who understand both structured and unstructured data. Companies must focus on creating a framework for understanding maturity against AI/CI needs and potential disruptive places for insertion of that technology into current risk processes.

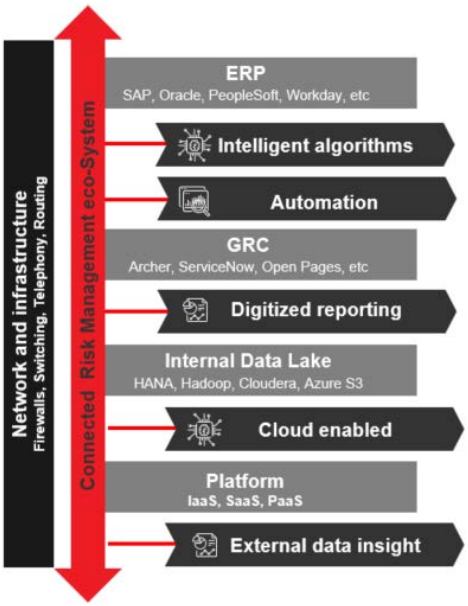


*Figure 8 - Model for Risk Platforms & Intelligence*

**Objective #5 - Risk Decision Engines – Embracing Machine Learning & New Analytic Skills**

Companies that leverage new technology and gain new visibility, will be able to stop something from happening significantly sooner. Embracing this possibility for insight requires designing dashboards and thinking critically about internal and external indicators of success for the business. An effective risk management program should leverage a system that monitors all three different types of risks and that system would monitor both KRI's and KPI's for Upside, Downside and Outside risks. Refer to Figure 9 for a structure of this connected management system.

**Conclusion & Final Comments**

Cybersecurity plays a major role in the context of the broader risk management community. While cyber is a singular thread of the larger risk management institution, it plays a critical role in the scanning of risk data, the delivery of that risk data to appropriate teams, and finally facilitates the actioning of that data.

Building off this context, the Uniform Risk Process Model (URPM) provides the ability for any resource to understand how risk activities are executed. This model additionally provides methodologies for moving beyond reliance on only standards frameworks and compliance bodies. This model allows corporations to align enterprise strategies and objectives to risk management rather than the counter, risk management programs being left to drive on regulatory objectives and downside risk.

Corporations must balance risk management to include corporate strategic objectives. In addition, they must simplify overall risk operations, and provide for all members of the company to participate in control activities and design.

**Long Term Objectives & Aspirations**

The Future-of-Risk Management is extremely bright if executed well. The opportunity to remove strain from audit departments and to reallocate that effort towards value added activities has long been discussed, but never executed. The advent of new GRC technologies and the continued rise of intelligent systems can only breed better risk management tools and utilities. There is absolutely no amount of tooling and technology, however, that will replace the mindset shifts and understanding required of corporate leadership and c-suite team members. We must look to our information security and data engineers to start this journey, for their data unlocks this new reality:

> *CFOs…**lack visibility into their data, leaving them unprepared amid growing geopolitical risks**, according to a survey by Dun & Bradstreet Corp. Three fifths of finance executives at 870 companies from various sectors said **their data is stored in silos**, and only 20% reported that their data is fully integrated and leveraged across the company. Over **90%** of executives said that **geopolitical risks and the threat of technological disruption have increased in the past year**…*[18]



[18] CFO Journal Editors et al. "The Rise of Geopolitical Threats and Disruption." Wall Street Journal. 08/13/2018

## Appendix A - Glossary – Risk Management & Framework Terms

| Term | Definition |
|---|---|
| • **Upside Risk** | Risks that are strategic in nature for a corporation. These can include moving into new markets, developing new products, or delivering new services. |
| • **Outside Risk** | Risks that are currently outside control of an entity. These can include events that are environmental in nature (earthquakes, natural disasters) or new technologies that could affect margin and profit. |
| • **Downside Risk** | Risks that truly have no upside potential and are typically protected against in a corporate risk framework. These can include:<br>• Environmental Health & Safety Risks<br>• Legal & Compliance Risks<br>• Cybersecurity / IT Risk |
| • **Integrated Risk Management (IRM)** | IRM is a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks. * Wikipedia |
| • **Sarbanes-Oxley Act (SOX)** | A United States Federal Law, enacted in 2002 that mandated expanded requirements for accounting firms and corporations in the light of major accounting scandals at Enron and WorldCom. |
| • **COSO** | The Committee of Sponsoring Organizations of the Treadway Commission |
| • **COBIT** | Control Objectives for Information and Related Technologies – A Standards framework created by ISACA to support IT Risk governance. |
| • **Adaptive Governance** | Adaptive Governance represents a corporation's ability to conduct Enterprise |
| • **Enterprise Resource Planning (ERP)** | Enterprise Risk Platforms represent singular systems that control all aspects of the business cycle. This includes procurement, production, sales, finance, tax, treasury, accounting and reporting. Examples include SAP, Oracle, PeopleSoft and Workday. |
| • **Governance, Risk & Compliance (GRC)** | GRC represents the critical aspects of Risk Management programs. Governance of the business, creation of risk frameworks to monitor and control the business, and compliance regimens to ensure response to those risks and controls. |
| • **Internal Data Lake** | A collection of non-production data collected (both structured and unstructured) to assist in analytics. |
| • **Three Lines-of-Defense Model (LoD)** | The three-lines-of defense is a well-known model of risk management that establishes an independent risk audit function against the business units (risk takers) and a monitoring function. |
| • **Enterprise Risk Management** | Enterprise risk management in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives* Wikipedia |

## Appendix B - Bibliography – Resources & Notes

Banham, Russ. "Scanning the Risk Horizon: Industry Veterans Discuss Strategic Planning." April 1, 2016. Risk Management Magazine. http://www.rmmagazine.com/2016/04/01/scanning-the-risk-horizon-industry-veterans-on-their-roles-in-strategic-planning/

Bjerga, Torbjorn. “Adaptive Risk Management Using New Risk Perspectives – An Example from the oil and gas industry.” Elsevier: Reliability Engineering & System Safety. Volume 134. February 2015. Pages 75-82.

Bones, James. “The 3 Dimensions of Risk.” September 9, 2014. Corporate Compliance Insights. https://www.corporatecomplianceinsights.com/the-3-dimensions-of-risk/

CFO Journal Editors et al. “The Rise of Geopolitical Threats and Disruption.” Wall Street Journal. 08/13/2018

Chambers, Richard. “No Internal Audit? It Could Be Worse.” Internal Auditor Magazine. Oct 24, 2016. https://iaonline.theiia.org/blogs/chambers/2016/Pages/No-Internal-Audit-It-Could-Be-Worse.aspx

COSO. “Leveraging COSO Framework across the Lines-of-Defense.” July 2015. https://www.coso.org/Documents/COSO-2015-3LOD.pdf

DeLoach, James. “5 Common Risk Management Failures.” Corporate Compliance Insights. April 1, 2016. https://www.corporatecomplianceinsights.com/5-common-risk-management-failures/

ERM Initiative Faculty et al. “Risk Governance: Balancing Risk and Reward.” Enterprise Risk Management Initiative. Oct 1, 2009. https://erm.ncsu.edu/library/article/balancing-risk-reward

Freedman, Anne. “The Upside of Risk. Organizations win when they integrated risk management into strategic decision-making.” June 2016 Issue. Risk and Insurance Magazine. https://riskandinsurance.com/the-upside-of-risk/

Hanna, Julia. “The Costs and Benefits of Sarbanes-Oxley.” March 10, 2014. Forbes Magazine. https://www.forbes.com/sites/hbsworkingknowledge/2014/03/10/the-costs-and-benefits-of-sarbanes-oxley/#59b237c3478c

Hubbard, Douglas W. “The Failure of Risk Management.” 2009. P.26

Institute of Internal Auditors. “Lines of Defense.” 2013. https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

Kaplan, R. and Mikes, A. “Managing Risks: A New Framework.” Harvard Business Review. June 2012. https://hbr.org/2012/06/managing-risks-a-new-framework

Market Research Future (MRFR). “Enterprise eGRC Market 2018.” MarketWatch. https://www.marketwatch.com/press-release/enterprise-governance-risk-and-compliance-egrc-market-2018-global-analysis-industry-growth-opportunities-business-strategy-emerging-trends-competitive-landscape-and-regional-forecast-to-2023-2018-09-27

Ovans, Andrea. “Capturing the Upside of Risk.” Harvard Business Review. June 27, 2012. https://hbr.org/2012/06/capturing-the-upside-of-risk

Parija et al. RIMS Executive Report, The Risk Perspective. “Emerging Risks and Enterprise Risk Management.” Risk Insurance Management Society, Inc. https://www.rims.org/resources/ERM/Documents/EmergingRisk_ERMweb.pdf

Petrina, Tania. “Development of Adaptive Governance Programs for the Future of Risk.” EY. September, 2018.

Polak, Matthew. “Effective Categorization of Risk and Control.” EY. June 27, 2018.

Rio Tinto. “Black Swan Events, Population Misconceptions.” IRM NW Seminar. P2-10. https://www.theirm.org/media/1120524/Popularmisconceptionsaboutblackswanevents-JohnSummers.pdf

Sturm, Mike. “The OODA Loop: A Tool for Better Decision-Making.” Medium. March 11, 2017. https://medium.com/personal-growth/the-ooda-loop-a-tool-for-better-decision-making-that-youre-already-using-ca24a3fa8c5c

Van Kessel, Paul. EY Risk Transformation & Cyber. “GISS Survey – EY – Global Information Security Survey.” 2017-2018. https://www.ey.com/Publication/vwLUAssets/GISS_report_2017/$FILE/REPORT%20-%20EY%20GISS%20Survey%202017-18.pdf

Wharton Public Policy et al. “Re-Thinking Risk Management: Why the mindset matters more than the model.” University of Pennsylvania. Apr 15, 2009. http://knowledge.wharton.upenn.edu/article/re-thinking-risk-management-why-the-mindset-matters-more-than-the-model/

## Appendix C - Acknowledgements

I would like to thank my wife Lauren Keches for her dedication and support during the EMCS program and throughout the many nights I spent executing work for the degree. I could not have done this without you, and this degree will forever have an asterisk.

I would like to thank my parents George and Cheri Keches for their love and support during this program and for their belief in me for 29 years.

I would also like to thank my Advisor Bernardo Palazzi for his continued support and praise throughout the CCP process. Your kind words of encouragement were greatly appreciated.

I would finally like to thank my external advisors at EY - Matthew Polak, Tania Petrina, and Keith Young. Your support and guidance as we collectively tackle Risk in the Transformative Age has been wonderful. May we find success and continue to help our clients succeed.

To the entire EMCS Faculty and Staff: We have forged an indelible bond as the Wolfpack and I will forever look back on my time in this program with fond memories. I have admiration for all your hard work and for your continued ability to push the future of cybersecurity and risk management.