Cognitive Risk Management

Traditional risk frameworks, such as COSO ERM (1985), ISO 31000 (2009), and the Basel Capital Accord (1974) are modern inventions from the early 20th century formulated to respond to major failure in managing financial, operational, regulatory, and market risks. Traditional risk frameworks have been helpful in managing compliance risks with an emphasis on internal controls but lack the rigor to evaluate asymmetric risks that cause business failure.

None of these risk frameworks have fully addressed the root cause of risks across all organization…the *human element!* Human behavior is the weakest link in risk management and security. Human factor risks will increase in the fast-paced digital economy many are calling the *Fourth Industrial Revolution!*

The evolving role of the human worker and the emergence of the **Digital Economy** will be as disruptive as the rise of the first *Industrial Revolution* and *Knowledge Worker* of the late 19th century! The transformation from the Industrial Age to the new Digital Economy needs a new roadmap!

The Cognitive Risk Framework was created in response to asymmetric risks inherent in cyber risk and an economy increasingly driven by technology. A Cognitive Risk Framework is a "redesign" of risk management with the human element at the center facilitated by the right tools to create *Situational Awareness* to anticipate and respond to risks more effectively and lower the costs of risk management. The outcome of a cognitive risk framework is increased efficiency, streamlined processes, intelligent automation, better performance and risk reduction.

The pace of change in a digital economy requires a new risk framework that keeps pace with the speed of business. Traditional risk frameworks fail to grasp changes in the environment that often leads to poor decision-making under uncertain conditions.

According to the World Economic Forum, *"There are three reasons why today's transformations represent not merely a prolongation of the Third Industrial Revolution but rather the arrival of a Fourth and distinct one: **velocity**, **scope**, and **systems impact**. The speed of current breakthroughs has no historical precedent. When compared with previous industrial revolutions, the Fourth is evolving at an exponential rather than a linear pace."*

The cognitive risk framework differs from traditional risk frameworks in another important aspect. The cognitive risk framework seeks to optimize the business environment to reduce uncertainty as opposed to a rigid defensive posture that is inflexible. Too often risk programs focus on the assessment of risks and the appearance of containment in arbitrary risk registers, qualitative risk assessments and compliance without considering how to reduce risks to an acceptable level. As the needs of business change a cognitive risk framework easily adjusts to the new reality because it is not based on an inflexible risk framework is incapable of anticipating change.

A cognitive risk framework seeks to operationalize returns on risk management by measurably reducing the costs of risk through a portfolio approach that reduces uncertainty and incorporates opportunity

"The beginning of knowledge is the discovery of something we do not understand"

-Frank Herbert

analysis. Optimally, the CogRisk framework is a source of profitable outcomes as opposed to a defensive posture. In this way, the cognitive risk framework complements traditional risk frameworks by adding another dimension…the human element of informed decision-making to traditional risk practices. A cognitive risk practice seeks to frame uncertainty and the dynamic nature of risks into a responsive risk practice.

A cognitive risk framework is a redesign of cybersecurity and enterprise risk management practice that includes five (5) pillars representing stages of development that align with the unique risks inherent in each organization as opposed to representing an arbitrary maturity model of risk practice.

Risk management is still an evolving discipline for all practitioners which suggests that any representation of a risk program having reached an arbitrary maturity level is an illusion. To paraphrase Frank Herbert above *"The beginning of knowledge is the discovery of something we do not understand."* No risk program can guarantee assurance but a cognitive risk practice can reduce the uncertainty of risks that may lead to business failure

The Five Pillars of a Cognitive Risk Framework for Cybersecurity and Enterprise Risk Management:

The cognitive risk framework starts with ***design***; in contrast, traditional risk frameworks start with ***execution***. This subtle but significant difference may seem counterintuitive to those familiar with traditional risk practice. Instead of starting with what you know; internal controls, risk failures, IT and operational breaks, the cognitive risk framework starts with what you don't know to evaluate the risks that exist right below the surface of awareness. This is major shift in risk practice requiring risk professionals to become "risk solution designers" as opposed to managers of risk. Risk solution designers

create situational awareness for all levels of the organization providing the board/senior management, middle management and line staff with the tools to manage their own risks.

Almost all organizations spend 65% - 80% of their resources (risk, audit, compliance staff and budget) on high probability/low impact risks. This is a tremendous waste of resources because the expense of these efforts has not been calibrated with the benefits of remediation. This explains why most organizations have seen the cost of compliance and risk management skyrocket over the last 10-15 years without a commensurate reduction in risks or value added to the organization.

A cognitive risk practice rebalances the focus on high probability/low impact events (least significant risks) with greater focus on the uncertainty of low probability/high impact risks (most damaging risks). Realigning risk assets to better understand the latter helps reduce the costs associated with the former. The misallocation of risk assets distracts organizations from the key risks that threaten organizational objectives. When risk resources are misallocated on "fire-drills" reactively responding to low impact risks the organizational loses situational awareness of the real threats that matter to the business.

"As far as the laws of mathematics refer to reality, they are not certain; and as far as they are certain, they do not refer to reality."

- Albert Einstein on Certainty

How does an organization right-size the allocation of risk resources to achieve a more effective risk response?

The Five Pillars of a Cognitive Risk Framework are designed to help organizations right-size the allocation of risk resources. The five pillars include: **Cognitive Governance**, **Intentional Control Design**, **Business/Risk Intelligence & Legal Risk Assessment**, **Cyber Risk Intelligence & Human-Element design**, and **Cognitive Data & Human Integration**.

Each of the five pillars may be used independently or as a complement to improving leading ERM practice. The development and implementation of each pillar is expected to be incremental and designed to fit the needs of each organization.

Cognitive Governance starts with an assessment of an organization's Risk Perception. A Cognitive Map is created through a ***Risk Perception Assessment*** which develops a road map for identifying blind sports across the organization and rebalances the focus of risk practice where the opportunity to reduce risk and improve processes is greatest. Blind spots exist in every organization with most lying just below the surface of awareness. A cognitive map identifies where situational awareness is needed to reduce significant organizational blind spots and help facilitate communications between respective stakeholders.

A cognitive risk practice starts with risk perceptions because most traditional risk programs fail to capture the differences in risk perception at each hierarchical level of an organization and therefore fails to reconcile the differences.

Many existing risk programs start with a "Risk as Feelings" approach to risk management. Risk as feelings focuses on activity driven by fear, worry, and incomplete information which clouds judgment about the appropriate response for risk mitigation. A cognitive risk practice tests these assumptions to gain confidence in the distribution of risk.

The Cognitive Map created by the Risk Perception Assessment drives the rest of the five pillars and determines the extent and need for implementing each program in the pillar. Next is the **Intentional Control Design** pillar.

Intentional control design is the process of leveraging the results from the Cognitive Map and incorporates how people work to evaluate a risk solution design. Intentional control design is the process of making risk management and compliance easier for the people responsible for managing their own risks. Additionally, the cognitive map is used to determine where the right data is needed to improve situational awareness and increase performance.

Intentional control design is also implemented to reduce "cognitive load". Cognitive load is the amount of multi-tasking an individual can perform optimally before errors increase. Cognitive load has been cited as a key reason employees click on phishing email links. By incorporating human element design factors, a cognitive risk practice evaluates how to make internal control design more intuitive. Intentional Control Design is also informed by the **Business, Risk & Legal Intelligence** (BRL) pillar.

The Business, Risk & Legal Intelligence pillar is the process of research and development to refine risk management practice and business performance through an active process of intelligence gathering. BRL intelligence can be used to inform strategic planning, build sustainable processes and detect emerging risks in the organization. The BRL pillar assumes that the organization is not static and even small unanticipated changes could lead to unintended consequences. The BRL pillar facilitates traditional key

risk metrics and strategic initiatives by constantly back testing outcomes to meet or exceed goals. The BRL pillar includes key indicators (static) and goes beyond to include Indicators of change (dynamic) that are the leading causes of failure.

The **Cybersecurity Risk Intelligence and Human-Element Design** pillar is similar to the intentional control design pillar but includes greater emphasis on the human-element of cyber risk. The greatest vulnerability in Cybersecurity is the human element. A cognitive risk framework is designed specifically to recognize the human risk element missing in traditional risk frameworks. Social media, email phishing, web-surfing and mobile apps have been identified as the leading causes of security breaches. Human behavior while using these new technologies expose the firm to cyber risks that circumvent security controls. Few organizations have developed or even considered the manifestations of cognitive risk outside of email phishing campaigns. The cognitive risk intelligence and human-element pillar is the only framework designed to evaluate how human behavior leads to vulnerabilities in cyber-attacks.

Lastly, the **Cognitive Data and Human Integration** pillar is designed to develop a robust decision support capability for targeted solutions. While Big Data projects have been popular many have not produced added value outside of marketing or product initiatives. Alternatively, a more nuanced approach may be more effective. The cognitive data and human integration pillar is focused on creating *Situational Awareness* as a competitive advantage.

Situational Awareness is the process of making sense of changes in the environment that may lead to risks by incorporating the rights tools to respond in a timely manner. Each level of the organization should have the information or tools to query and/or answer tough business questions when needed. A cognitive risk practice identifies the capabilities needed to create situational awareness from the C-suite to the front-line creating a more informed and proactive organization. A situationally aware firm frees employees to provide more creative solutions to business challenges and pushes decision-making to the front lines while maintaining control and oversight by senior executives.

Throughout the introduction of the CogRisk framework there has been a reference to the Human-Element. In a cognitive risk practice human element factors refers to the practice of designing products, systems, or processes to take proper account of the interaction between them and the people who use them. Cognitive ergonomics is concerned with mental processes, such as perception, memory, reasoning, and motor response, as they affect interactions among humans and other elements of a system. (Relevant topics include mental workload, decision-making, skilled performance, human reliability, work stress and training as these may relate to human-system and Human-Computer Interaction design.)

A CogRisk practice is unique in combining a multi-disciplinary approach to ensure the proper integration of people, process, and technology creating a more seamless approach to risk management that is not disruptive to existing operations while enhancing them by making small adjustments to the work environment. No other risk framework incorporates the human element design focus. However, a

CogRisk framework is designed to complement all other risk frameworks into one unifying enterprise risk management approach.

The Cognitive Risk Framework for Cybersecurity and Enterprise Risk Management was founded based on cognitive and decision risk science which is the basis for Nobel Laureates from Frank Knight, Herbert Simon to Daniel Kahneman and Amos Tversky. While much of the research that underpins a cognitive risk framework has been around for decades the recognition of this work is only now being implemented in technology applications globally.

Global Compliance Associates, LLC, TheGRCBlueBook, LLC are the only authorized risk advisers of the Cognitive Risk Framework for Cybersecurity and Enterprise Risk Management. Global Compliance Associates work with leading GRC and Cybersecurity solutions providers to execute the Cognitive Risk Framework for Cybersecurity and Enterprise Risk Management.

To learn more or to get started on your Cognitive Risk Framework contact James Bone at info@thegrcbluebook.com, jbone@globalcomplianceassociates.com or jamesbone0129@gmail.com. 401-451-8112 phone number.