THE FLYNT GROUP INC.

ACTIONABLE KNOWLEDGE ®

Enterprise Risk Management and Business Impact Analysis:

Understanding, Treating and Monitoring Risk

THE FLYNT GROUP INC.
ACTIONABLE KNOWLEDGE®

PO BOX 20111
KANSAS CITY, MO USA 64195
877.FLYNTGP (359.6847)
INFO@FLYNTGROUP.COM
WWW.FLYNTGROUP.COM

Flynt Group White Paper
Enterprise Risk Management and Business Impact Analysis

Enterprise Risk Management (ERM) is a critical governance issue and a vital practice to achieve an organization's objectives through risk-informed approaches. Management guru Peter Drucker said, "if you can't measure it, you can't manage it." Unfortunately, many executives don't know the extent of their risk exposure. Worse, they don't have capabilities in place to gain visibility on, and control, their risk portfolio using models that equip them with metrics.

Flynt Group assists organizations in further enhancing their ERM program to fully understand, treat, and monitor their risk portfolio. Our services align with international standards, and we pride ourselves on achieving tangible return on investment for our clients. We help our clients map and optimize systems and processes to be more effective and efficient with less risk. Our scenario-based modeling and structured, quantified "what if" analysis will equip you with *Actionable Knowledge*® to avoid unacceptable risks to the enterprise, mitigate accepted risks based on cost-benefit analysis, and quickly respond with scenario-tailored courses of action during a crisis.

Risk-intelligent executives not only know what, but also how much, is at stake. An essential ERM process - Business Impact Analysis (BIA) - is central to this knowledge. BIA goes beyond anecdote-based opinion and quantifies, based on explicitly defined scenarios, the consequences that could impact a company using metrics such as dollars at risk, outage time, recovery time, and others. Flynt Group develops realistic scenarios for BIA analysis and quantifies the impacts of degradation or loss of various functions, systems, assets, and processes using data from, among other sources, client experiences and similar historic events.

Flynt Group's mission is to equip our clients with *Actionable Knowledge*® to wisely manage their risk positions and achieve their goals across a broad spectrum of hazards and threats. Should we be able to provide any further information, please contact us at 816.243.0044, or via email at Info@FlyntGroup.com.

Sincerely,

Bill Flynt, Ph.D., LTC (R)
President
The Flynt Group, Inc.
"Actionable Knowledge"®

Introduction

Enterprise Risk Management (ERM) is a comprehensive, proven methodology to effectively manage risk. Accounting for the effects of uncertainty or the unexpected on enterprise objectives, ERM provides defined processes and a comprehensive, standards-based framework to enable effective decisionmaking.

A core ERM process, the Business Impact Analysis (BIA) measures the effect of disruption to an organization's operations, identifying required actions to successfully manage such risks. Scenario-based BIA is a cost effective approach to identify organizational risks and provides reliable decision support data to leaders concerning hazard mitigation, recovery strategies, and continuity planning.

As an example, the occurrence of a catastrophic industrial accident, economic crisis, enterprise function failure, attack, extreme weather event, or pandemic outbreak has the potential to significantly affect an organization's key enterprise elements (i.e. functions, systems, assets, and processes). BIA and ERM provide tangible added value by identifying specific risks, hazards, and threats, as well as treatment options to protect key enterprise elements.

Risk Identification

Enterprise Risk Management and scenario-based BIA can identify gaps, redundancies, and other issues informing the development of contingency plans, and apply appropriate risk treatment measures to mitigate the probability of occurrence and severity of differing risks across the enterprise. Example risk types include:

- Hazard risk: Catastrophic industrial accident, extreme weather event, pandemic outbreak;
- Financial risk: Pricing risk, asset risk, liquidity risk, liability;
- Operational risk: Enterprise function failure, customer satisfaction, reputational risk; and,
- Strategic risks: Economic crisis, competition, capital availability.

Benefits of Enterprise Risk Management

Common goals of an ERM program are to reduce costs through business process optimization, reduce risk, increase efficiency, increase the Board's visibility of risk, improve incident response and preventative treatment measures, and create standardized metrics for internally consistent comparison of risks across an enterprise.

The Enterprise Risk Management framework equips organizations to maximize opportunities, avoid or mitigate losses, and deliver the benefits of better informed decisions and increased operational efficiency. Effective ERM enables companies to anticipate material threats and develop strategies to prevent their occurrence or mitigate their impact. Additional ERM benefits include:

- Improved objective setting and business planning;
- Enhanced reputation protection;
- Efficient allocation of resources against prioritized risks;

- Resilient supply chain management;
- Improved performance and shareholder value;
- Reduced cost of insuring risk; and,
- Stronger corporate governance.

Increased ERM Focus

Enterprise Risk Management is receiving increased visibility in many companies, with a CxO (e.g., CFO, CRO, CSO) either placed in charge of ERM, or having it assigned to their portfolio. A best practice approach - a CxO positioned to take an enterprise view of aggregate risk - develops a perspective on the risk trending of the firm and how the current risk profile and trending aligns with the company's risk tolerance. A CxO may act as an enterprise champion, improving the skills, tools, models, databases, and processes for evaluating risks and developing mitigation and response actions across the enterprise's departments and collective risk exposure.

The increased focus on ERM by Boards and Officers assists their companies in identifying and quantifying risk, in turn enhancing decision-making. Flynt Group directly supports these decision makers by developing tailored tools and models to better analyze and assess the potential risk impact across all domains—financial, operational, logistical, compliance, reputation, contingency planning, and others.

Executive Sponsorship in ERM Implementation

Executive sponsorship and involvement is the foundation for a successful ERM program and a best practice. Sponsorship ensures that the program is appropriately resourced and that risk evaluation and mitigation initiatives receive C-Suite support. This is important in that, absent CxO sponsorship, most ERM initiatives fail due to bureaucratic inertia. In addition to a CxO sponsor, leading practitioners of ERM also recommend establishing a risk committee from across enterprise functions to coordinate activities and provide senior executive guidance across all lines of business.

Defining a corporation's risk tolerance is, by definition, a CxO / Board level function. Risk tolerance will vary according to the particular hazard, threat, or system and determines when the risk/reward tradeoff has reached unacceptable levels. Business Impact Analysis, a core component of ERM, identifies and quantifies the parameters of enterprise risk tolerance in the context of specified enterprise elements (e.g., a mission critical system) and metrics (e.g., dollars at risk, production outages).

Successful ERM programs holistically identify and describe all material risks faced by an enterprise. Rank ordering risks within individual enterprise elements, and then prioritizing those risks across the elements using consistent, defined criteria, enables risk-informed resource allocation to the most pressing risks and the most important enterprise elements – a powerful ERM outcome. Flynt Group helps clients with risk identification and prioritization based on our deep experience with standards-based methodologies, including Business Impact Analysis, Delphi interviews, scenario-based planning and modeling, STEEPLED analysis, Hazard and Operability Studies, and Structured What-if Technique (SWIFT) analysis. Following prioritization, each risk should be tracked, assigned a risk owner (the individual or group with the accountability and

authority to manage the identified risk on behalf of the enterprise), and entered in a master risk register for monitoring.

Business Impact Analysis (BIA)

Within ERM, the BIA analyses how risks could disrupt a company's operations and quantifies the impacts of degradation or loss of various functions, systems, assets, and processes. The BIA is a valuable process that helps identify enterprise-wide risk positions and inform risk management.

A properly conducted BIA provides organizations with a quantitative understanding of the criticality of key business functions, systems, assets, and processes, and the associated resources and key interdependencies. The BIA can also identify the impacts of disruptive events to the organization's capacity and capability to achieve critical business objectives; the capacity and capability needed to manage the impact of a specific disruption and recover the organization to target levels of operation; and, the interdependencies and interrelationships between processes, internal and external parties, and key supply chain linkages.

Flynt Group conducts scenario-driven BIAs that conform to ISO and ANSI standards, sophisticated methodologies, and industry best practices (e.g., NERC/FERC for the electric power industry, DHS CFATS for the chemical industry, etc.), providing tailored analysis and products informing enterprise decisions and supporting financial, operational, logistical, compliance, reputation, and contingency planning analysis.

A BIA project typically has three major, interdependent work components. The first component is the development of formal scenarios with explicit assumptions, planning factors, and parameters suitable for analysis, modeling, planning, training, and presentation.

Figure 1: BIA Components and Insights

The second component is degradation modeling of each scenario's key enterprise elements (i.e., functions, systems, assets, and processes). This modeling involves detailed analysis of the damage inflicted by a scenario, including: where the damage is located; magnitude, extent, duration and persistence of the damage; which of the elements' components, capacities, and capabilities are impacted; as well as other important factors potentially impacted by the damage that may not be readily identified.

The final component is analysis of the scenarios' first-, second-, and where possible, third-order effects against the key enterprise elements. This comprehensive analysis provides illuminating insight regarding potential financial, operational, logistical, compliance, reputation, and contingency planning risk exposure (defined as the extent to which an organization is subject to the event).

Example scenarios that could be modeled for an organization include a catastrophic industrial accident, economic crisis, enterprise function failure, terrorist attacks, extreme weather events, and pandemic outbreak.

A properly conducted BIA has significant potential to reduce costs, reduce risk, and improve efficiencies. Other benefits include identification of the:

- Consequences of a disruption on the identified key enterprise elements based on scenario modeling in financial, operational, logistical, compliance, reputation, and contingency planning terms over defined periods;
- Key interdependencies between internal and external stakeholders and functions, with the nature of the interdependencies mapped through the supply and production chains;
- Current available resources and the essential level of resources needed to continue to operate at a minimally acceptable level following a disruption;
- Alternative workarounds and processes either currently in use, planned, or those that may need to be developed where resources, capability, or capacity are inaccessible or insufficient during the disruption; and,
- Outage and recovery time frames for key enterprise elements (i.e., functions, systems, assets, processes) and associated information technology recovery time frames.

Conclusion

Uncertainty stems from both predictable and unpredictable internal and external factors. With uncertainty, the risks of achieving enterprise goals and objectives become increasingly problematic as unanticipated events draw executive attention away from strategic objectives and into crisis management. ERM provides a framework for companies to identify and mitigate risks, eliminate uncertainty, improve operational efficiency, reduce costs, and inform crisis management planning.