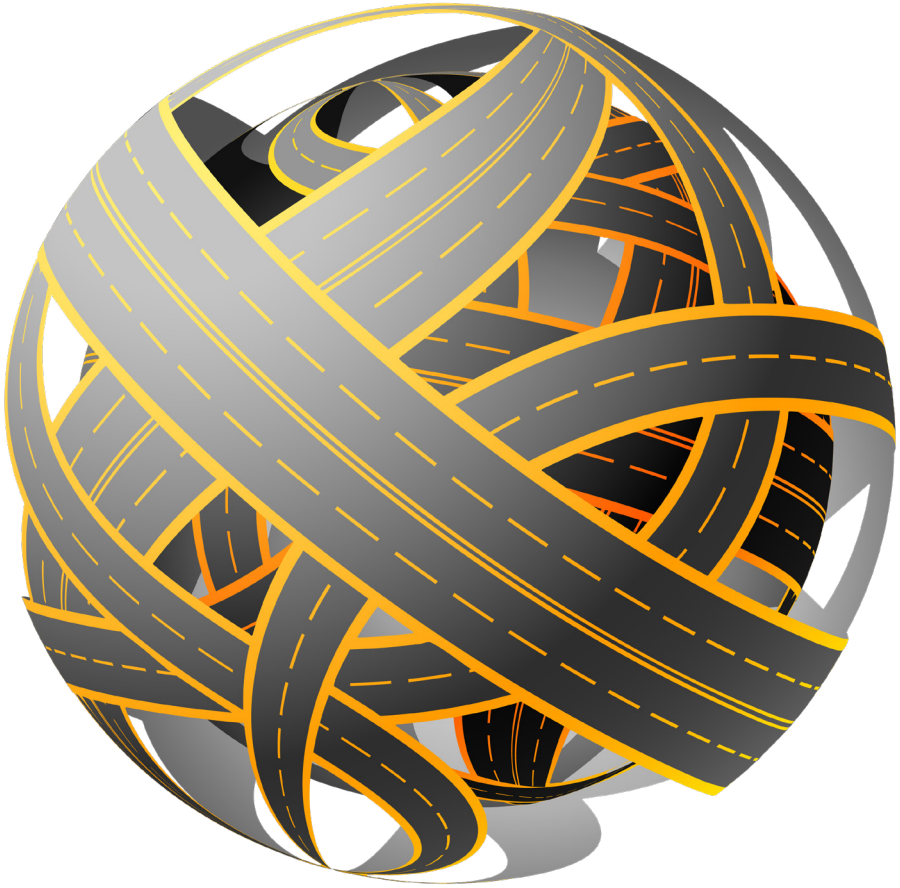
Deloitte.



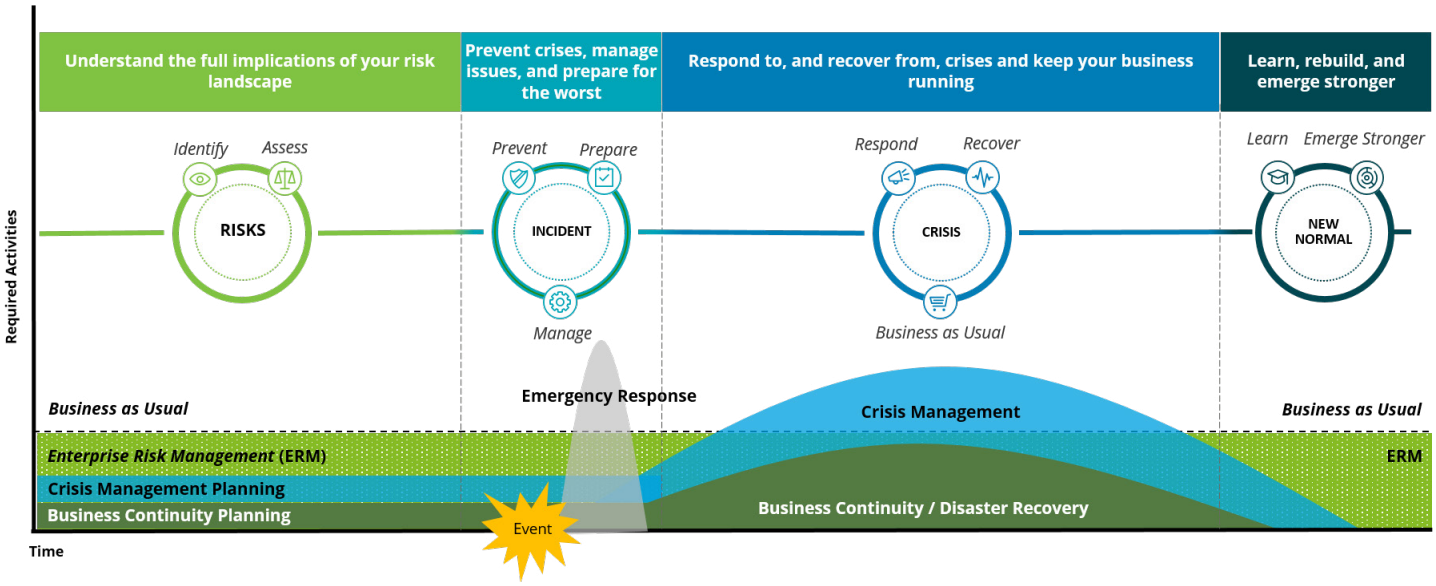
Tying the Knot: Integrating ERM and BCM to Improve Resiliency

The Coronavirus outbreak, shift in global economic, business outlook, regulatory requirements, and technology industry trends create a challenging environment for many organizations. The World Economic Forum's COVID-19 Risks Perception Survey shows that organizations are most concerned about the continuous global economy fallout for over the next few months and are worried about the capability of industries to recover from disruption.

Organizational needs for business resilience plans and tools are increasing, as they help organizations to prevent risks, and to recover, replace, or rebuild critical business processes in the wake of disruptions. Enterprise Risk Management (ERM) and Business Continuity Management (BCM) are capabilities and disciplines that contribute to the resiliency. While ERM and BCM share the common goals of risk management, the two are often viewed as distinct activities and managed in silos. Integration between ERM and BCM can improve strategic alignment and better coordination. As we continue to help our clients through this difficult time, this thought paper is our reflection that sheds light on areas where integration between ERM and BCM can be considered.

End-To-End Business Resiliency

The following diagram shows the flow of events and the required activities when an incident occurs. Generally, the conditions are divided into 4 phases, which are before the incident happens, when it happens, when it turns into crisis, and when it returns to new normal. The part before the incident is a preparatory phase in which organizations have a big responsibility in equipping all resources to be ready to deal with and handle the incident, while the event after the incident is divided into several phases of responses & recovery.



1 Managing Risks

Understanding the full implications of risk landscape is the early phase of the end-to-end business resiliency while running the business-as-usual. Organizations need to adapt and expand their approaches to focus on investments in resilience. In this phase, organizations focus more on the Enterprise Risk Management (ERM) implementation, where it involves identifying, measuring, monitoring, reporting, and responding to risks across an enterprise. This has to be done in a way that is aligned with the enterprise's objectives and risk appetite in order to have better risk mitigation plans. On top of that, organizations also need to develop incident/ crisis management and business continuity plan to be better prepared for incidents.

2 When Incident Occurs

When an incident occurs, organizations need to focus more on Business Continuity Management (BCM) implementation. The first activity to be carried out is the emergency response which often attracts the most attention and resources in order to minimize the impact on the safety and health of all stakeholders, employees, customers, and communities around organizations. How an emergency response is planned has a critical role in ensuring that the disruptive impacts arising from the emergency can be managed effectively in this phase. To better understand the next action needed in the recovery period, impact analysis is also conducted by coordinating with the related parties.

3 During Crisis

If the disruptions continue after emergency response activity is performed, the incident may turn into a crisis situation. In this phase, crisis management plan has an important role for organizations to keep their operations running. This includes organizations' efforts to respond by running its business with a minimum capacity, which may include a mechanism of crisis information management, crisis communication, activation of crisis command center and recovery activities including periodic reporting. Organizations also need to focus on business continuity and disaster recovery activities so that the business can recover its operations from both IT infrastructure and non-IT assets.

4 In The New Normal

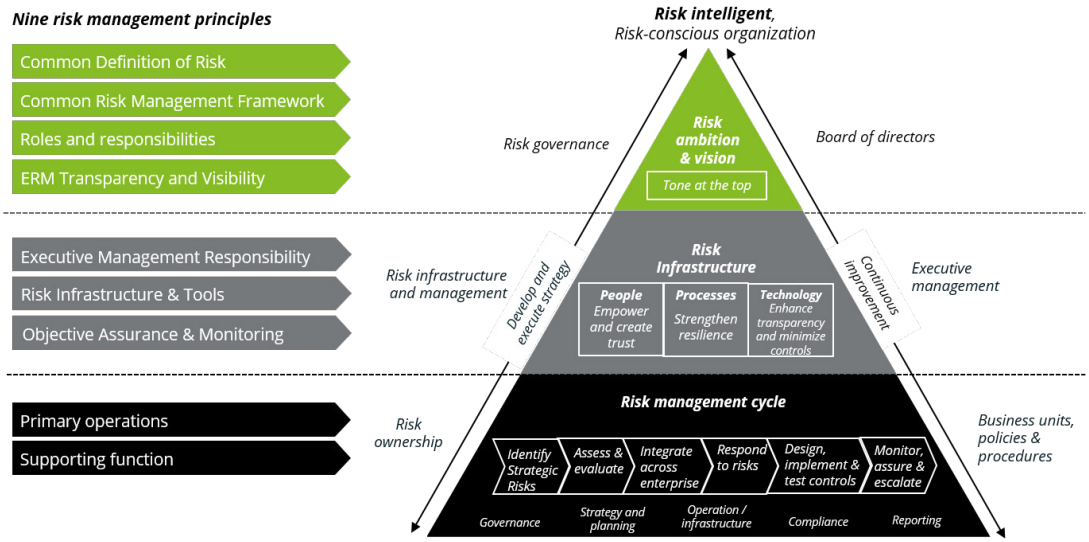
Organizations may then arrive to their new business-as-usual adapting to the new normal after the crises. Organizations need to refocus its ERM implementation by understanding the new risk landscape so that they can be better prepared to mitigate emerging risks. To achieve and sustain business resiliency through crisis readiness, organizations should continue to periodically monitor and improve the suitability, adequacy, and effectiveness of organizations' risk management and business continuity management through learning, experience, and adaptation to the changing world.

Enterprise Risk Management (ERM) Framework

Dynamics of ecosystems and relationships between risks often create threats in which traditional risk management is not equipped to address. Therefore, organizations need to design their risk management and integrate it into their business and strategic processes to enable them to take risks to create value as well as respond to and mitigate risks, set risk management roles and responsibilities, resource allocation, communication and escalation line appropriately.

Deloitte Risk Intelligent Enterprise™ help organization in managing risk effectively and efficiently in order to support its business development and journey to the future growth.

There are 9 risk management principles supporting each of the 3 building blocks objectives. These principles are immersed within all parts of the organization. Each of the principles provides clear perspectives and guidance to manage risks effectively, allowing the stakeholders to understand the challenges and opportunities which arise from risks.



Risk Oversight

At the top, the leadership group has a responsibility for risk governance (including guidance and risk oversight) which consists of fostering risk intelligence into strategy; defining risk appetite, limit & KRI; and evaluating organizational risks. Risk governance is set to improve board effectiveness, provide oversight of strategy-setting process, risk management program, change management and key risks, as well as set a "tone from the top" which will drive consistency.

- **Common Definition of Risk**
  A common definition of risk, which addresses both value preservation and value creation, is used consistently throughout the organization
- **Risk Governance Framework**
  A common risk framework supported by appropriate standards is used throughout to manage risks
- **Roles and Responsibilities**
  Key roles, responsibilities, and authorities relating to risk management are clearly defined and delineated
- **Transparency for Governing Bodies**
  Governing bodies have appropriate transparency and visibility into Risk Management Practices to discharge their responsibilities

---

Risk Infrastructure

At the middle line, executive middle management (especially Risk Management Function) has a responsibility for risk management infrastructure such as designing, implementing, and maintaining an effective risk management systems by also considering the right people, processes, and technology. Risk infrastructure is set to establish consistency across organization while at the same time addressing different needs.

- **Executive Management Responsibility**
  Executive management is charged with primary responsibility for designing, implementing and maintaining an effective risk program
- **Common Risk Infrastructure**
  A common risk management infrastructure is used to support the business units and functions in the performance of their risk responsibilities
- **Objective Assurance and Monitoring**
  Independent and objective division provides objective assurance as well as monitors and reports on the effectiveness of the risk program to governing bodies and executive management

---

Risk Process

At the base, business unit and supporting function (such as Risk Owner and Divisional Risk Champion from their respective unit) has a responsibility for risk process, including conducting risk assessment through identification, analysis, and evaluation of risks, setting risk treatment plans, and monitoring & reporting on specific risk. Risk process is set to integrate and effectively manage risk and compliance, and foster risk ownership.

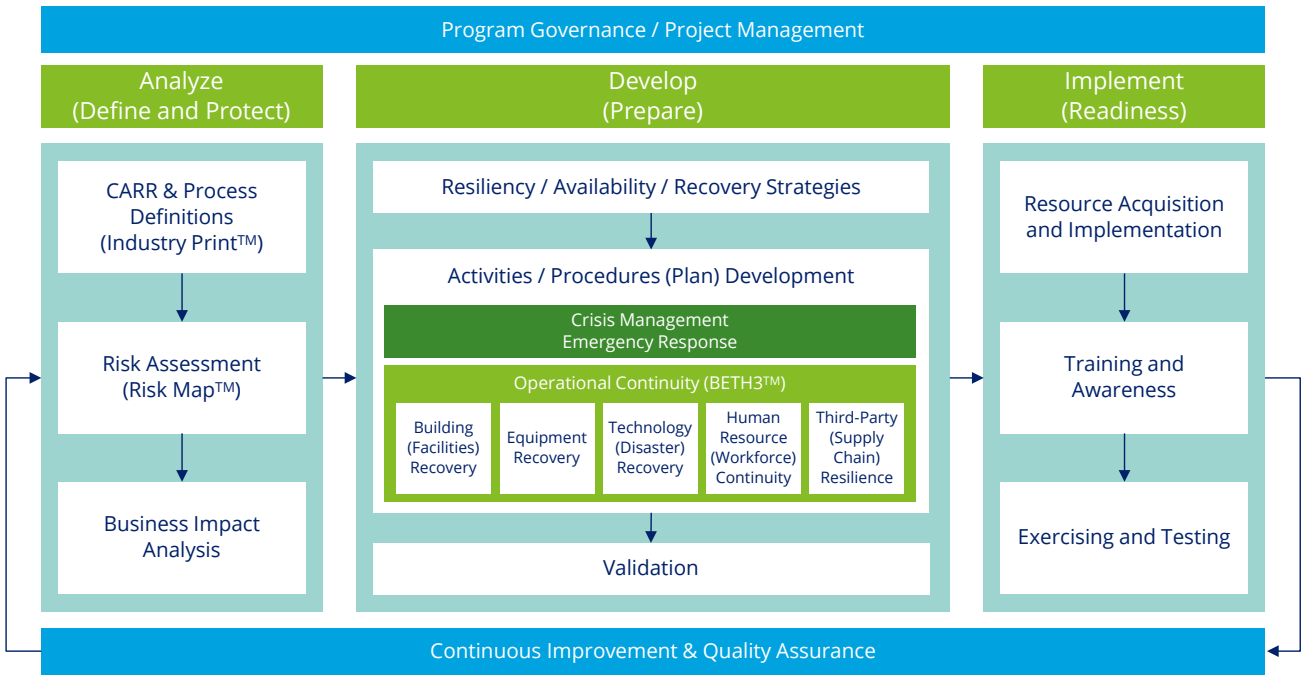
- **Business Unit**
  Business units are responsible for the performance of their business and the management of risks they take within the risk framework established by executive management
- **Supporting Function**
  Certain supporting functions have a pervasive impact on the business and provide support to the business units as it relates to the risk program

Business Continuity Management (BCM) Framework

Business sustainability relies on organizations' resources and the continuity of its operations. Organizations' need to design and implement BCM mechanism coming from certain events that can negatively affect the organization and lead to a crisis situation. It is imperative for organizations to have the capability to plan and respond to incidents that may affect its operations to keep the business running and reduce the impact of disruptions.

Deloitte's BCM Program Development Framework understands the need to strengthen BCM capabilities to enhance the organization's resiliency

This framework helps the organization in understanding its critical risks and business processes, internal and external dependencies, and the supporting technologies to determine the recovery requirements, which are then developed using an asset-based approach around Buildings, Equipment, Technology, Human Resources and 3rd Parties (BETH3™), followed by cost-effective implementation and continuous improvement.



Analysis Phase

First step in Analysis Phase is conducting in depth analysis through Capability Assessment of Recoverability and Resiliency (CARR) to obtain the understanding of organization's current preparedness. Followed by Risk Assessment on existing activities to identify potential hazards, threats, and risks that may affect the organization. Lastly, it continues with Business Impact Analysis (BIA) to assess the impact and acceptable level of operation for the organization's critical business functions.

Development Phase

BCM strategy should focus on the organization's recovery objectives and take into account the Analyze phase results such as consideration to minimize downtime & business impact and availability of resources. These strategies will then be translated into activities / procedures (plan) of incident/crisis management, emergency response, business continuity, and disaster recovery. Periodic validation of BCM plans components should be conducted in order to assess whether strategies and plans have met the recovery objectives.

Implementation Phase

Implementation of the strategy is done through resource acquisition and implementation of technical solution such as alternate-site building. Training and awareness programs to establish preparedness culture through exercise and testing program are important factors to improve the capabilities of people involved in the recovery activities.

Assurance Phase

As business and risk landscape are constantly evolving and crisis incidents can negatively affect organizations, it is important to monitor and update BCM through continuous improvement and quality assurance program. Assurance phase assess BCM program based on global standards (ISO 22301, ISO 27001, etc.) that may include root cause analysis; reflecting on lessons learned; regular evaluation of BCM tools and capabilities; and periodic quality assurance review.

Integration Opportunities for ERM and BCM

ERM and BCM integrate to achieve Business Resiliency. Both share the common goals to enhance organization's value creation and protection. ERM allows organization to create and protect their values through the process of assessing, monitoring, reporting and responding to risks that may negatively affect the objectives achievement. BCM improves organization's strategic and tactical capabilities through identification and development of response, recovery, and restoration plan to face incidents that may affect its operation. It ensures that the business can still run at its acceptable level. ERM and BCM integration point opportunities are explained below.

Integration Point	Description	Benefit
ERM and BCM Governance and Competencies Integration		
Risk and BCM Common Reporting Committee	Global practices have shown that ERM and BCM would have its own or separate reporting committees. Regardless of the choices, it is clear that ERM and BCM typically share similar committee members. ERM and BCM discussion within the reporting committee should have a common reporting process to align activities related to prevention and response on critical threats.	Alignment between ERM and BCM committee members would ensure better preparedness and response to critical risks/threats as well as lesson learned from critical incident/ crisis.
Risk and BCM officers common operational coverage	Organizations would need to extend the coverage of their Risk and BCM officers to the length of its operational locations (e.g. regional offices, branches). The officers of Risk and BCM have a common role respectively. These are to facilitate prevention activities (through risk management) and to facilitate/guide any response to incident/crisis.	"No one is left behind." Every operational locations would be supported and aligned in their risk management process as well as managing incident/crisis.
ERM and BCM Talent Development	ERM and BCM are disciplines originated from similar risk to crisis cycle explained at the beginning of this document. Therefore, talent development activities ranging from talent onboarding awareness session, regular trainings, and simulations should involve common facilitators with integrated training curriculums.	Integrated ERM and BCM talent development programs build well-rounded capabilities and culture that is ready to manage risks, overcome crisis and provide sustainable operation.
ERM and BCM Process Integration		
ERM and BCM Risk Parameter	ERM and BCM should have standardized parameter indicators and aligned limits/thresholds that are consistently used within the organization.	Integrated ERM and BCM Risk Parameter provide the same objective perception and measurement of risks/threat across all levels and functions. It allows the organization to escalate what truly matters and take appropriate action according to the level of risks/threats exposed (e.g., additional risk response activities, crisis declaration process).
ERM & BCM Risk Assessment Scope	ERM and BCM risk assessment scopes are aligned within operational risk. Risk assessment in BCM is related to physical assets in each facilities, technology and cyber, safety and security measurement and operational continuation. These risks should also be assessed in ERM (i.e., during Risk Control Self Assessment) within the infrastructure management function (e.g., functions of IT, General Affair, Building Management).	Aligned ERM and BCM risk assessment scopes break the silo sources of information, covering all angles of possible operation disruption, enhancing organization's business resiliency.
Risk Treatment Plans and Crisis Simulation	Organizations should build their crisis/BCM simulation considering their risk assessment result and the risk treatment/mitigation plans.	BCM simulation which considers relevant risk treatment plan ensures the practicality, feasibility and effectiveness of risk treatment plans built for critical risks.
Business Impact Analysis (BIA) and Risk Management Focus	BIA results provide information of critical business unit/ services/ applications/ processes for Risk Management to pay more attention to during the risk assessment and prioritization process.	With BIA information, organizations can allocate their risk management attention & resources for better treatment and risk monitoring in critical area and/or processes.
ERM and BCM Policy Taxonomy	BCM policy is an integral part of overall risk management policies to set organizations' attitude towards critical or specific risks that may disrupt the operation.	ERM and BCM combined policy taxonomy allow organizations to have a clear and comprehensive risk management process documented in which understanding of risk, risk management, and business continuity are consistent and standardized across all levels and functions of the organizations.

Integration Point	Description	Benefit
ERM and BCM Technology Integration		
ERM & BCM Shared Technology Landscape	Risk technology landscape includes Risk Management and Risk Sensing capabilities that facilitates ERM and BCM processes. Risk Management technology facilitate Risk Management processes, Business Continuity processes, Mass Communication, and Crisis / Incident Management. Risk Sensing Technology is used to predict risks in the future utilizing available operation data.	Utilizing Risk Management and Risk Sensing Technology accelerates both ERM and BCM in the organization. A comprehensive Risk Technology Landscape allows better communication & coordination in managing critical risks. It enhances the organization preparedness by keeping the management ahead with emerging risks/disruptions through the risk sensing capabilities.

Contacts Us

Brian Indradjaja, CCSMS
Deloitte Indonesia Risk Advisory Country Leader
Deloitte SEA Risk Advisory - Clients & Industries Leader
Deloitte Asia Pacific Risk Advisory - Deloitte Private Leader
Deloitte Indonesia
Tel: +62 21 5081 9600
Email: indradjaja@deloitte.com

Alstair Bharata, CCSMS
Strategic and Reputation Risk Director
Deloitte Indonesia
Tel: +62 21 5081 9610
Email: abharata@deloitte.com

Albert Nathaniel, CCSMS
Business Continuity and Crisis Management Specialist
Deloitte Indonesia
Tel: +62 21 5081 9672
Email: alnathaniel@deloitte.com

Ivana Beatrice
Enterprise Risk Management Specialist
Deloitte Indonesia
Tel: +62 21 5081 9683
Email: ibeatrice@deloitte.com

About the authors

Brian Indradjaja holds the position of Deloitte Indonesia Risk Advisory Country Leader, Deloitte South East Asia Risk Advisory Clients and Industries Leader, and Deloitte Asia Pacific Risk Advisory Deloitte Private Leader. Brian leads various engagements in the Banking and Financial Services, Consumer Products, Technology and Telecommunications industries in Australia, Indonesia and Asia Pacific Region. The engagements include enterprise risk management transformation, risk model development; compliance policy and processes; risk appetite testing; strategy and development; internal audit; management, establishment and maintenance of Compliance/Operational Risk measures, and the optimization of Strategic Risk in organizations.

Alstair Bharata leads the Indonesian "Strategic and Reputation Risk" service with primary industry focus on Public, Financial Services and Consumer Sector. Alstair has supported and led various engagements at Deloitte clients in Indonesia and overseas on Turnarounds Strategies, Governance, Board Performance Management, Enterprise Risk Management (ERM), Business Continuity Management (BCM), Crisis Management and Sustainability.

Ivana Beatrice is a Manager of Enterprise Risk Management in Deloitte Indonesia. She has extensive experience in several Risk Assessment, Risk Maturity Assessment, Risk Management capabilities, and Risk-Based Investment Market Analysis Project for several infrastructure and financial industries.

Albert Nathaniel is a Manager of Crisis and Resiliency in Deloitte Indonesia. He has extensive experience of Crisis Management and BCM review/ establishment in several industries majority in transportation sectors and top largest banks in Indonesia.

Nadia Gitta H is an Enterprise Risk Management Specialist. She has been involved in Risk Maturity Assessment, Business Continuity Management Maturity Assessment, and end-to-end Risk Management mechanism development projects for several transportation and financial industries.