Sin, Ivan Siang-Meng; Musa, Noor Azlan; Ng, Keith Yong-Ngee

Article

Building business resilience through Incident Management Body of Knowledge (IMBOKTM): The amalgamated framework for total resilient capability

Global Business & Finance Review (GBFR)

Provided in Cooperation with:
People & Global Business Association (P&GBA), Seoul

Suggested Citation: Sin, Ivan Siang-Meng; Musa, Noor Azlan; Ng, Keith Yong-Ngee (2017) : Building business resilience through Incident Management Body of Knowledge (IMBOKTM): The amalgamated framework for total resilient capability, Global Business & Finance Review (GBFR), ISSN 2384-1648, People & Global Business Association (P&GBA), Seoul, Vol. 22, Iss. 1, pp. 38-50, https://doi.org/10.17549/gbfr.2017.22.1.38

This Version is available at:
https://hdl.handle.net/10419/224361

GLOBAL BUSINESS & FINANCE REVIEW, Volume. 22 Issue. 1 (SPRING 2017), 38-50
pISSN 1088-6931 / eISSN 2384-1648 | Http://dx.doi.org/10.17549/gbfr.2017.22.1.38

GLOBAL BUSINESS & FINANCE REVIEW

www.gbfrjournal.org

Building Business Resilience through Incident Management Body of Knowledge (IMBOK™): The Amalgamated Framework for Total Resilient Capability

Ivan Siang-Meng, SIN[a], Noor Azlan MUSA[b] and Keith Yong-Ngee, NG[c]

[a] *Adjunct Associate Professor, National University of Singapore, Singapore*
[b] *Managing Director, ERCM Consultancy, Singapore*
[c] *Adjunct Lecturer, Southern Cross University, Australia*

A B S T R A C T

In today's volatile, uncertain, complex and ambiguous environment, organizational resilience is a strategic capability to stay afloat "stormy waters" when faced with business disruptions that have grave impacts on the organization's business operations, supply chain, and reputation. A true resilient organization needs to be constantly scanning for potential threats, identify the probable risks, plan and be prepared to deal with the consequences and impacts when the risks materialize. However, many organizations approached this capability in varied methodologies with some focusing on business continuity while others are emphasizing on crisis management. This paper uncovers the converging domains-interplays between the concepts and the building blocks of enterprise risk and resource management, emergency and crisis management, business continuity and disaster recovery management to act as the bedrock to achieve business resilience through the **Incident Management Body of Knowledge** as the amalgamated framework for total resilient capability; using the **Adaptive Incident Management Methodology**, to enable organizations to build an **"Adaptive System: Integrated Approach, Dynamic Response"** to the management of all-risks and all-hazards incidents.

Key words: Resilience; Incident Management; Risk Management; Crisis Intervention; Emergency Management; Business Continuity; Disaster Recovery

Ⅰ. Introduction

Organizational Resilience can be viewed as an enterprise's strategic capability to maintain positive causatum under challenging conditions in today's uncertain and complex business environment. This is closely linked to the organization's ability to manage the elements that contribute to business disruptions that impact future business in the supply chain, operations, products, services, customer relations, and even public confidence. A truly resilient organization need to have the foresight to recognize potential risks with ongoing size-up of operating environment to prevent unwanted disruption or possible creeping crisis from emerging, and in the event of an unwanted incident, the ability to detect, respond, intervene, adjust, and recover from the

Received :Sep. 12, 2016; Revised : Dec. 1, 2016; Accepted : Jan. 19, 2017

† Ivan Siang-Meng, SIN
Adjunct Associate Professor, National University of Singapore, Singapore
Tel.: +65-9299-2532 E-mail: chessmi@nus.edu.sg

after-effects in a timely fashion; even turning the incident into a strategic opportunity, effectively managing the causatum through the Incident Management Body of Knowledge (IMBOK) as the amalgamated framework for total resilient capability to achieve business resilience.

The study aims to uncover the converging domain-interplays between the concepts of enterprise risk management, emergency intervention, business continuity, crisis response, and disaster recovery that influence organization resilience; and establishes the knowledge areas essential to effective management of business disruptions. Through literature reviews, the consented study of organizational practices; literature analysis of corporate plans and standards, the chronological evolution of the various concepts and building blocks of enterprise resilience, dating from the 1950s, and the converging synergies of incident management methodology are expounded; from its planning stages, to validation exercises, to eventual execution during real-time incident; covering event-level activities during the management of incident issues and consequences ranging from emergency intervention, business continuity, and even a reputational crisis; indicating need for a multidisciplinary approach with different readiness-dashboard to effectively manage different types of incidents, incident outcomes, and incident outcome cases (scenario specific). These are supplemented by a field survey, in-depth interviews, and category theme analysis of 102 industry practitioners. The findings complement the review; provide information on the development of knowledge areas that evince the Incident Management Body of Knowledge (IMBOK) and a proposed "Adaptive Incident Management Methodology" model to cater for different scenarios amidst various industry sectors.

This paper will provide an overview of the natural interrelationship and overlaps between the abovementioned practices and discuss the inherent need to integrate the management of incident as a focal element of all related programs; from risk assessment to scenario-based pre-incident planning, to business impact analysis, to emergency intervention, to multidisciplinary crisis response through the application of Incident Management Body of Knowledge. The new model establishes the way in which the various concepts and building blocks act as the bedrock to achieving organizational and business resilience through the application of Adaptive Incident Management Methodology (AIMM); from on-scene actions, to on-site supports, to off-site corporate management of the incident and provide an overview of how the proposed readiness-dashboard approach can build on the well-established Incident Command System and be used as the adaptive incident management methodology for pre-incident planning and incident management; enabling organizations to build an **"Adaptive System: Integrated Approach, Dynamic Response"** to incident management − covering scenario-based pre-incident planning that includes business disruptions, to emergency situations, to crisis interventions, and recovery management - An engine to the application of knowledge areas in the Incident Management Body of Knowledge.

Ⅱ. Literature Review

This section reviews the interrelated concepts affecting organization resilience (OR), namely enterprise risk and resource management (ERRM), crisis and emergency management (CEM), business continuity and recovery management (BCRM), corporate issues and consequence management (CICM) together with the emergency incident management methodologies namely the Incident Command System (ICS) and Incident Management System (IMS) from the United States (US) emergency services perspectives. The corresponding development of incident management in the United Kingdom (UK) which took on a similar evolution will be discussed in a separate paper.

A. Organization Resilience

Sutcliffe and Vogus (2003) defined organization resilience as the entity's positive ability to respond and adjust to disruptions, adapting itself to the consequences of catastrophic failures such as power outage, fire, and bomb threat. They identified 14 indicator metrics to measure an organization's resilience maturity. These are: crisis leadership; crisis decision support; staff engagement in work-resilience strategy; organizational situation awareness; delegation of crisis decision making; innovation and creativity; effective crisis partnerships; critical knowledge leveraging; minimization of "Silos"; internal crisis resource management; unity of purpose; proactive strategic crisis posture; crisis and business continuity strategies; and crisis stress testing regime. Sheffi (2005) extended the concept of resilience to include business continuity; analyzing the adverse impact of disruptions to business operations and how organizations can gain a competitive advantage over others that did not prepare for such contingencies. Therefore, it is apparent that there exist node-links between organization resilience and the organization's risk governance and management framework, crisis and business continuity management, including incident management and emergency response. There may be other factors yet to be explored that this study hopes to reveal.

B. Enterprise Risk and Resource Management (ERRM)

The evolution of ERM in today's complex global economy can be traced back to the 1950s with the earliest developments out of insurance management function in the United States where fire services only respond to insured dwellings. Contingency planning became important in the 1960s when the emphasis was placed on loss prevention and safety management (Hopkin 2012). Enterprise risk and resource management today looks at all risks that will affect stakeholder expectations and core organizational processes at an enterprise-wide level. This involves the analysis of physical and financial supply chain, manufacturing and delivery activities, and the overall question to be answered is, "What could affect the continuous survival of the organization?" This integrated all-risks and enterprise-wide approach have considerable advantages because it analyses all potential disruptions to the overall stakeholder expectations, looking at the whole business value chain in totality; such as viewing health and safety risks as an integral aspect of ensuring staff availability instead of a separate hazard risk management issue (Hopkin 2012). The Singapore Standard, SS ISO 31000 (2011) provides a good framework, comprehensive principles, and guidelines to help organizations manage risks effectively.

C. Crisis and Emergency Management (CEM)

Contrary to preemptive risk management, crisis and emergency management (and subsequent discussion on business continuity management) emerged from reacting to the consequence impacts when the identified risk event takes place. Conventional crisis and emergency management focus on responding to the onset of an emergency incident (risk-event or stimulus event) and dealing with the consequence impacts on life safety, property, and the environment. Although some authors tend to use the term crisis and emergency interchangeably, there exists a subtle difference between them. NFPA 1600 (2013, p.5) had clearly defined emergency/disaster management as "an ongoing process to prevent, mitigate, prepare for, respond to, maintain continuity [of operations] during, and recover from an incident that threatens life, property, operations, or the environment"; while crisis management as "the ability of an entity to manage incidents that have the potential to cause significant security, financial, or reputation impacts". Thus, crisis management in a broader sense included [emergency management and] business continuity in its response and recovery activities

(Heath 1994). The British Standard Institute, BS 11200 (2014) provides a framework, guidance, and good practices to help organizations build crisis management capability. The ongoing methodologies to improve incident management in the CEM domain evolved over time with the well-developed methodologies of ICS and IMS as discussed below.

1. Incident Command System (ICS)

The early days of ICS can be traced back to the late 1960s when Southern California, for the first time in history, had to gather firefighting resources from various states and jurisdictions, involving a large-scale multi-agency response to handle the large-scale wildfire that had threatened both the populations and the environment. Following that incident, an Inter-agency Task Force comprising local state and federal agencies developed the early days' Incident Command (IC) Framework, utilizing Project FIRESCOPE - Firefighting Resources of California Organized for Potential Emergencies - as the hallmark of a multi-agency response to wildfire incidents in the early 1970s. By mid-1970s, the FIRESCOPE-IC Frameworks had been well adopted by various agencies for wildfires and was adapted for structural fire incidents by the Phoenix Fire Department; gave birth to the well-recognized Fire Ground Commander System (Phoenix-FGCS) and adopted by many fire departments in the United States (Brunacini 2002).

By late 1970s, the two methodologies were so well adopted that in early 1980s, federal government US Fire Administration recognized the benefits of melding the principles of FIRESCOPE-IC and Phoenix-FGCS as the National Fire Academy − Incident Command System (NFA-ICS). In 2003, the Federal Emergency Management Agency (FEMA) was absorbed into the Department of Homeland Security (DHS); since then ICS became the focal point for all federal training with respect to all-hazards incident management; covering both natural and technological disasters. NFPA 1026 (2014, p. 10) defined ICS as a standardized on-scene emergency management construct specifically designed to provide for the adoption of an integrated organizational structure that reflects the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries; that NFPA 1561 (2014, p. 24) described ICS as a management system used to direct all operation at the incident scene with the Incident Commander (IC) located at an Incident Command Post (ICP) at the incident scene.

2. Incident Management System (IMS)

Today's Incident Management System (IMS) is a functional outgrowth of the well-known Big-Three (BIG-3), namely the FIRESCOPE-IC, Phoenix-FGCS, and the integrated NFA-ICS. By the mid-1980s, the BIG-3 had gone through series of transitions and became a US National Program, giving rise to the National Inter-agency Incident Management System (NIIMS). A spin-off from NIIMS included the legislative requirements under the US Code of Federal Regulations (CFR) that all government and non-government agencies to adopt the ICS as the key all-hazards incident management methodology; requiring the ICS to be interfaced with the local IMS and national response system. This gave rise to the first IMS-ICS model with various agencies such as the US Coast Guard (USCG), FEMA Urban Search and Rescue Administration (FEMA-USAR), and the US Fire Administration (USFA) incorporating ICS into their IMS and response frameworks.

Due to the wide use of ICS but the varied version of implementation, the NFPA motioned and called for development and use of IMS as a recognized standard in the late 1980s to provide for consistent implementation such as common terminology. This resulted in the first IMS standard in published in 1990, NFPA 1561: Emergency Services Incident Management System providing an IMS-ICS model framework for all fire and police departments to conduct emergency operations within an effective incident management system. All was thought to be going well until the NIIMS was fundamentally challenged in 2001 by a series of Anthrax Events

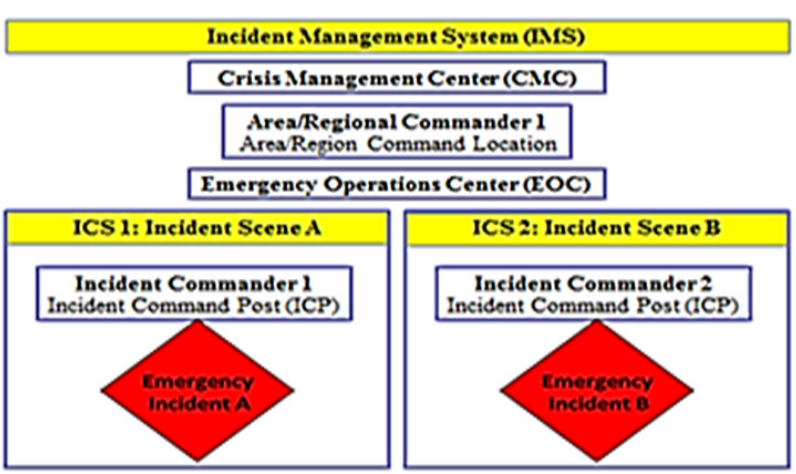
and the September-11 Attacks; that in 2003's US Presidential Executive Order to review existing emergency response plan at all levels of federal government that gave rise to the National Incident Management System (NIMS). The large-scale 2005 Hurricane Katrina and 2007 California Wildfires aftermaths brought about criticism to the gaps within the NIMS that it was further revised in 2008.

Although some authors and few NFPA publications still use the term ICS and IMS interchangeably; creating confusion and inconsistency at times, there exists a subtle difference that this study would like to distinguish. IMS has been defined by Molino (2006) as a conceptual set of ideas, policies, procedures and ways of "doing things" that will when employed properly, bring control to chaotic emergencies of all types, and that ICS is a precursor to IMS − a mirror but expanded elements of ICS. In another word, ICS is a critical component of a larger IMS and that NFPA 1561 (2014, p. 8) had also clearly defined IMS as a system that defines the roles and responsibilities to be assumed by responders and the standard operating procedures to be used in the management and direction of emergency incidents and other functions; that the Incident Management Team (IMT) comprises the incident commander and appropriate command and general staff personnel assigned to an incident.

The NFPA 1561 also stipulated the need for the IMS to integrate risk management into the regular functions of incident command, with Area Command being established to oversee the management of multiple incidents that are each being handled by an ICS, with Area Command working directly with the appointed Incident Commander within each ICS. All these are much aligned to NFPA 1026 (2014, p. 10) definition of NIMS as a systematic, proactive approach guiding government agencies at all levels, the private sectors, and non-governmental organizations to work seamlessly to prepare for, prevent, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life or property and harm to the environment; utilizing the ICS methodology (Gallant 2008). The relationship of ICS with respect to IMS is depicted in Figure 1.

D. Business Continuity & Recovery Management (BCRM)

Similar to the crisis and emergency response, business continuity management pays attention to managing and recovering from the disruption to business functions. In developing one's organization business continuity arrangements, the organization



Source: Authors

Figure 1. Relationship between ICS and IMS

needs to identify their critical business functions and key dependencies that will severely cripple or affect their business value chain in the event of a disruption. This will enable a minimum service level to be restored within a specific timeframe so that customers are not unduly affected (Sin and Ng 2013). Because of its all-embracing nature, the way BCM is carried out is dependent upon the organization's risk profile, risk appetite; and inevitably has close links to the corporate governance strategies and risk management (Smith 2003).

In the event of a partial or full business disruption to the organization, one would realize that the people who have to deal with the organization (customers, suppliers, and partners) do not want their life to stop because your organization is having a crisis. Hence, it is important that one immediately put up a sign that says "Business As Usual" and tell them "How" to go about getting their business done so they can get on with life! Achieve this on top of the disruption that is bugging the organization will ensure that one survives and ride through the crisis; even emerged stronger and more trusted - this is a resilient organization at work! The Singapore Standard, SS ISO 22301 (2012) provides a good framework, comprehensive principles, and guidelines to help organizations to manage business continuity and disaster recovery effectively.

E. Corporate Issue & Consequence Management (CICM)

Management of workflows, work procedures and any organizational matters at corporate headquarters, business divisions, down to individual business unit's day-to-day operational issues are kind of given from the first day of any establishment of the organization. Management of workplace issues and consequences have been traditionally resolved through corporate conferences, departmental meetings, task group brainstorming sessions, to the extent of arbitration between concerned parties. Relevance to organizational resilience, corporate issues and consequence management are circled around key domains such as enterprise risk and resource management (ERRM), crisis and emergency management (CEM), and business continuity and recovery management (BCRM).

Renfro (1987) recognized the increasing influence on corporate decision making when public issues of concern are at stake and suggested that a new social contract is evolving between the public, the organization and other stakeholders, which indeed happened (and still evolving) with the liberation of internet and social media platforms; that he suggested corporate management anticipate the emergence of new issues and their likely impact (from the angle of ERRM) as part of issues management in practice. But the concept of issue and consequence management is not new, and from the public relation standpoint, issue management has been around for more than 20 years. While it has been adopted by few major corporations as a powerful strategic planning tool, it has failed to attract the widespread attention it deserves and is sometimes misunderstood: in particular with crisis management or risk communication (Gaunt and Ollenburger 1995).

Ⅲ. Methods

Lussier (2011) identified four key aspects of research design, namely sample participants, variables, data collection, and data analysis. This study adopted the suggested structure to conduct research by Lussier (2011); utilizing relevant information from literature review, sampling criteria was identified to find suitable participants to collect primary qualitative data. From the in-depth interviews with industry practitioners, the primary data were transcribed, coded, followed by category theme analysis and interpreted. The findings from the primary data will be analyzed together with the literature review to generate the concluding findings for the study; involving consented reviews of

organizational practices, literature analysis of corporate plans and standards. The study was conducted in Singapore and given her unique position geographically, and economically, the ever-emerging process industry with its complex manufacturing site-bases and globalized supply chain networks would be a good unit of analysis.

A. Sample

In a qualitative study, "it is their relevance to the research topic rather than their representativeness which determines the way in which the people to be studied are selected" (Flick 1998 as cited in Neuman 2011, p. 241) and that we sample to identify relevant categories at work so as to sample aspects or features of the social world to "shine light into" key dimensions or processes in a complex social life (Neuman 2011). A purposive sampling method provided the way for selecting participants in this study; using judgment sampling approach as it involves the choice of subjects who are most advantageously placed or in the best position to provide the information required (Sekaran and Bougie 2013). The criteria for selecting relevant respondents were that the participant must be employed by an organization and play a role in organization's domain area(s) such as ERRM, CEM, and BCRM. Participants were selected from amongst relevant functional areas covering corporate planning, compliance, operations and engineering, logistics and supply chain, occupational health and environmental protection, workplace safety and security; and customer relations.

B. Data Collection

This study primarily utilizes secondary data through literature reviews and content analysis of organizations' documentation to uncovering the converging synergies of incident management methodology from its planning stages, to validation exercises, to eventual execution during real-time incident; covering event-level activities during the management of incident issues and consequences ranging from emergency intervention, business continuity, and even a reputational crisis. This is supplemented by the primary data collected from interviewing 102 participants over 18 months. The participants were selected based on the sample criteria and chosen from several organizations of different industries or sectors. During the face-to-face sessions, participants were given a brief background of the study, and informed consents were obtained to proceed with and audio recording the interview. The first part of the interview required the respondents to do a 15 minutes perception survey to gauge their perceived roles with respect to their employed position. The second part involved a semi-structured interview with eight open-ended questions to draw on the richness and experience of the participants with each interview session lasting about 30 minutes. The interviews were conducted either at the participant's office, a meeting room in their respective workplaces, or a quiet corner in a public cafe.

C. Data Analysis

Mason (1996) defined qualitative study as a process that is systematically and rigorously conducting flexible and contextual research that allows self-scrutiny by the researcher and produces explanations to intellectual puzzles. The 102 interview data are in the process of being transcribed and subsequently coded, followed by category theme analysis and interpreted manually. Interpreted themes that explain the research questions sufficiently will be reviewed together with the literature analysis to explore possible relationships and new understanding. We started looking for patterns or relationship while collecting data and uses results from early data analysis to guide subsequent data collection. Thus, the analysis is less a distinct final stage of research than a dimension of research that stretches across all stages (Neuman 2011). Henceforth, as we continue

to complete the analysis of data, we share the following preliminary findings.

Ⅳ. Discussions and Results

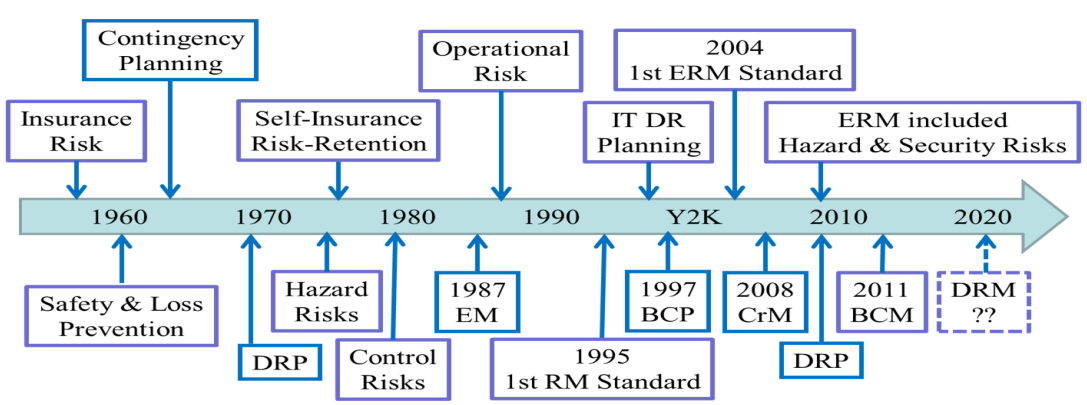
Through the literature review and documentary analysis, the chronological evolution of the various concepts and building blocks of enterprise resilience dating from the 1950s is consolidated in Figure 2.

A. Incident Management Body of Knowledge (IMBOK)

From the evolution of these concepts, the variety of terminologies used, and the growing literature in these silo-domain areas, comprehending the relationship between these concepts can be complex. The review on ERRM, CEM, BCRM found that organizations, in general, tends to manage each domain in silo and that in each "silo domain" there exists a common "incident management" tendency to manage the associated issues and consequences as illustrated in Figure 2 below; indicative of a potential convergence of body of knowledge in the management of incident issues and consequences, and possibly a suitable integrated incident management methodology to assist organization to manage resilience responses in a more concerted, better coordinated and responsive manner.

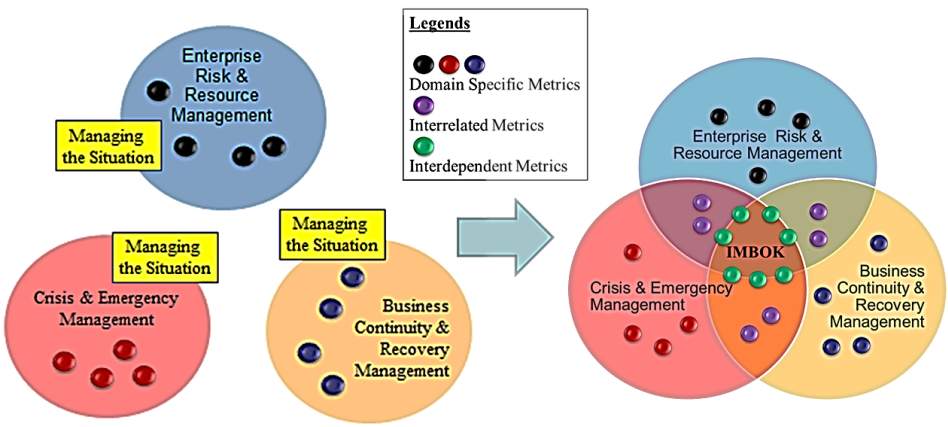
This convergence was clearly recognized by Enright (2012) from the BCRM angle that she saw the need for business continuity practitioners to make incident management, which often does not get the same amount of focus upfront, as a focal element of their BCRM program; pointing out that although incident management had previously been a standalone topic area, closely associated with CEM than BCRM, and often managed by an entirely different department from business continuity; there is, however, evolving recognition to incorporate incident management capability in BCRM. Enright (2012) went on to suggest the possible adaptation of CEM's incident command system (ICS) which is an established incident management methodology to retain market share and maintaining customer confidence following a disruption or crisis; Recognizing that this is driven in part by the business function's recovery time objectives; allowing the team to move on immediate responses to the incident and subsequent recovery of functionality from a BCRM perspective. The converging synergies of incident management body of knowledge (IMBOK™) are indicated in Figure 3.

As indicated in Figure 3, some of the indicator metrics are interrelated only between two domain areas while others can be interdependent at the incident management domain. For example, the



Source: Authors

Figure 2. Building Blocks of Enterprise Resilience



Source: Authors

Figure 3. Convergence of Incident Management Tendencies

maximum tolerable disruption period (MTDP) in BCRM can be put on the incident management dashboard as an interdependent metric that interlink ERRM, CEM, and BCRM; whereas indicator such as the critical business function (CBF) is interrelated to ERRM.

In addition to the immediacy of information that travels (via social media) to employees, partners, customers, and the external world, incident management has also become a tool for maintaining market share (Enright 2012); elevating the focal need to take on an integrated and collective approach with the specialist domains discussed. Henceforth, there exists a body of knowledge with respect to incident management from the literature analysis and the potential emergent of an all-risks "Integrated Incident Management" Model. The following Table 1 summarizes the IMBOK knowledge areas:

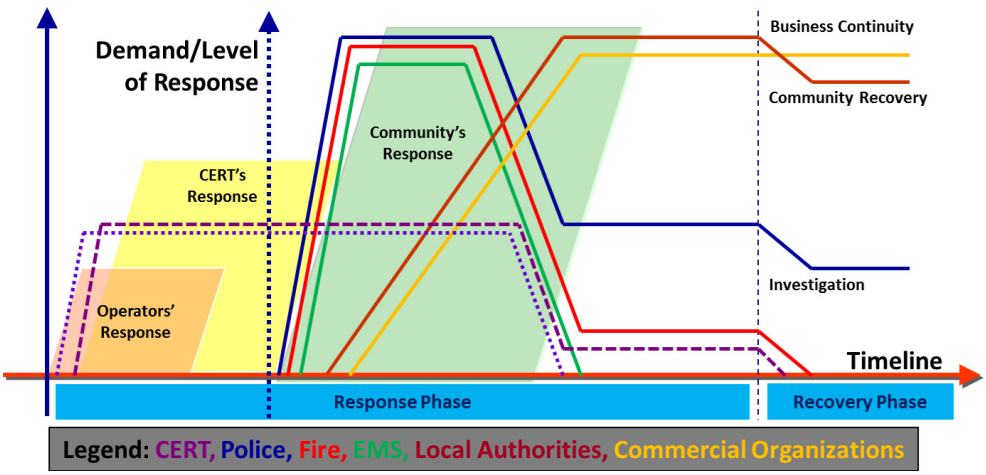
Note that each knowledge area is a specialized domain functions that when come together in the course of managing an unwanted incident, help the organization to respond, intervene, adjust, and recover from the after-effects in a timely fashion; even turning the incident into a strategic opportunity, effectively managing the causatum through the IMBOK as the bedrock to building organization resilience.

From the interviews conducted, many have indicated that the incident demand curve can be modified and adapted to include in-house company emergency response team's (CERT) intervention as shown in Figure 4.

The domain interplay initially discussed has also taken a tweet that ERRM being at the higher order of hierarchy within most organizations has a vantage point to map and synergize the business strategies with oversight to drive and integrate planning at the corporate level that relates to the domains. These include streamlining workflows and monitoring leading and lagging indicators for observable patterns, as well as reviewing corporate policy and standards

Table 1. IMBOK Knowledge Areas

Incident Management Framework	Risk & Resource Management
Incident Management Standards	Relationship Management
Incident Management Processes	Scene Organization & Control
Incident Management Process Groups	Consequence Management
Incident Management Structure	Business Continuity Management
Incident Life Cycle	Crisis & Emergency Management
Incident Management Control Centre	Information & Communication Technology
Critical Incident Dashboard	Disaster Recovery Management



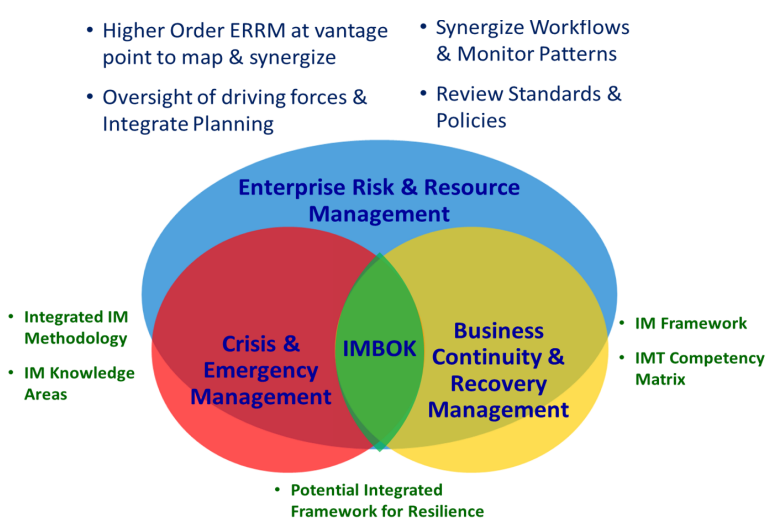
Source: Authors (Adapted from Dillon, 2009)
Figure 4. Incident Demand Curve

for consistency (Figure 5).

It is, therefore, possible to build up specific issues of the immediate discipline of the wider body of knowledge of the 3 parent disciplines, namely, enterprise risk & resource management, crisis and emergency management, and business continuity and recovery management.

B. Adaptive System: Integrated Approach, Dynamic Response

Preliminary findings so far indicated the need for an "adaptive" methodology to manage incident of diverse nature; and the dire need for a multidisciplinary approach to managing incidents of varying impacts; with different "readiness-dashboard" to effectively manage different types of incidents, incident outcomes, and incident outcome cases (specific scenario). Primary data gathered points towards the need for



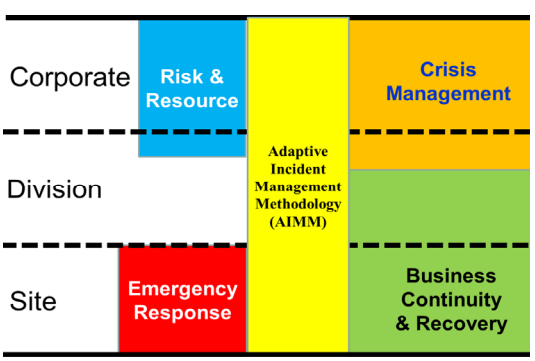
Source: Authors
Figure 5. Preliminary Domain Interplay

an "Adaptive Methodology" rather than a catch-all integrated methodology to cater for different scenarios amidst various industry sectors. This adaptive incident management methodology (AIMM) could be the cornerstone of an integrated approach with dynamic response towards issue and consequence management for the organization: a simple yet effective AIMM towards developing an "Adaptive-IMS: Integrated Approach, Dynamic Response" for each unique organization set up at various levels addressing each domain impacts as shown in Figure 6.

This all-risks or all-hazards AIMM can be handled by one or more multidisciplinary incident management teams through the organization's consolidated capability in ERRM, CEM and BCRM strategies; addressing the commonly mentioned 4Ps: People, Processes, Plans, and Places for the development of the multidisciplinary incident management teams as follows:

1. People

The Incident Manager provides the leadership to the Incident Management Team (IMT), and the selection of an Incident Manager is very much determined by the nature of the incident. As with the interviewed company, the Chief Operating Officer (COO) was pre-identified as the Incident Manager if the incident is Operations-driven, the Chief Finance Officer (CFO) if it is Finance-driven, and the Chief Legal Officer (CLO) if the incident is Compliance-driven. For any gray area, the COO will be the default Incident Manager.



Source: Authors

Figure 6. Adaptive Incident Management Methodology

The IMT and its scalable composition will play a key role to ensure a relevant and dynamic response depending on the nature of the incident at hand with a common pool of generic support members from Corporate Communications, Administration, and Info-Communication Technology.

2. Processes

The key processes for issue and consequence management involve activation and mobilization; initial actions; communications; monitoring and logging; reporting and decision-making. The work processes could be pre-determined, and team members are trained and exercised regularly. Regardless of the nature of the incident, the activated IMT will operate in the same consistent manner in accordance with the plans.

3. Places

The Incident Management Team operates in the designated Incident Management Centre (IMC) or Emergency Operations Centre (EOC). The venue is primarily equipped with offshore and onshore communications; internet connections; visual and audio projections; furniture; printing capabilities; restrooms; pantry; staff aids; and secured access. The plans and checklists for the various IMTs are also placed in the IMC or EOC for quick reference and execution.

4. Plans

The key plans to be made available are the organization's crisis and incident management plans; emergency response plans; business continuity plans, disaster recovery plans, specific-scenario contingency plans; and checklists for each functional representative. These plans should dovetail into specific scenario "readiness-dashboard" covering varying incident levels (demand levels) and its associated incident response from on-scene actions to on-site support, to the off-site corporate management of the incident using the AIMM. These "Specific Incident Readiness-

Dashboard" with relevant metrics pertaining to the specific incident outcome cases are measured and monitored during planning and preparedness stage to gear the organization towards the desired state of readiness and used as performance indicators to manage the impact of the incident when the risk event happens. Most importantly, these plans must be seamlessly tested and integrated to ensure efficiency and effectiveness within the AIMM using the "Library of Readiness-Dashboards" established during preparedness phase as shown in Figure 7.

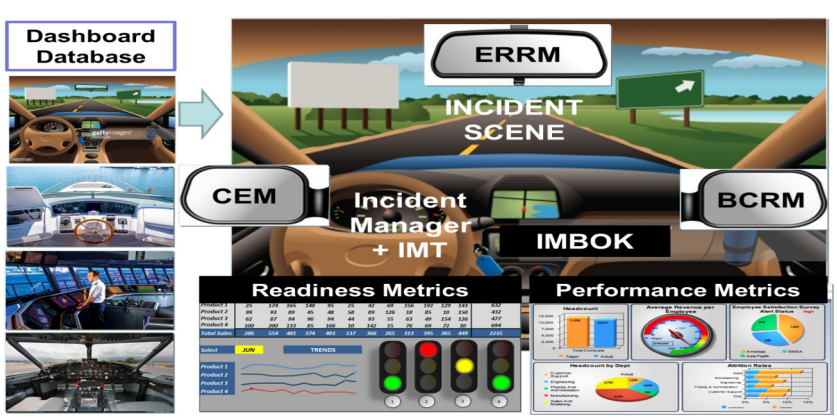
Figure 7 illustrates conceptually how the dashboard approach depicting different scenarios akin to driving a car, piloting a boat, or flying a plane; each with a panel of readiness metrics to show the organization's state of preparedness and performance metrics to help organizations manage the incident key performance indicators (KPIs) associated with the IMBOK knowledge areas. This approach provides the IMT a wide-angle view of the incident at hand, with a back of mind rear-mirror check on ERRM, side-mirrors check on CEM and BCRM issues and consequences.

This AIMM-Dashboard approach will provide each unique organization to establish and build an adaptive-IMS with an integrated approach, providing dynamic response in managing all-type incidents; with the similar principles as IMS-ICS model, the AIMM-Dashboard would be equally scalable, adaptable and practical in nature such that it can provide assurance to the Board of Directors that when any undesired incident happens, it will be managed professionally by their own internal resources - backbone of the IMBOK building blocks and processes.

As data is being theme-coded and analyzed, it is premature at this stage to formulate any application model, but with so many questions been raised about the management of issues and consequences during a crisis through ERRM, CEM, BCRM, and the much desired "simple yet effective" way of managing their associated impacts make the convergence of a common body of knowledge in managing incident and notable desire from amongst the interview participants citing the need for an "adaptive yet catch-all" incident management methodology for the organization; that this one methodology may well become the central driving force to achieving business resilience with the IMBOK knowledge areas as the amalgamated framework for total resilient capability in the pursuit of business resilience.

Ⅴ. Conclusions

In summary, the study showed the evolving need for an integrated incident management methodology that is both adaptive to scenario-specific incidents



Source: Authors

Figure 7. AIMM-Dashboards Approach

and responsive to the dynamic nature of the situation at hand. This will require the application of IMBOK knowledge areas to resolve incident-related consequences, impacts, and issues during business disruptions. The ability for CICM needs to be embedded within the AIMM approach and established within the multidisciplinary IMT. The AIMM Specific Incident Readiness-Dashboard Approach would enable the organization to establish an Adaptive System: Integrated Approach, Dynamic Response to all-risks or all-hazards incident management.

Acknowledgements

We would like to acknowledge and thanks the Association of Company Emergency Response Teams, Singapore (A-CERTS), Institution of Fire Engineers, Singapore (IFES), and the Society of Loss Prevention for Process Industries, Singapore (SLP) for the support and encouragement in this research study; allowing the researchers to reach out to their individual members and corporate member companies for the data collection with consent.

References

Brunacini, A.V. (2002). *Fire Command: The Essentials of Local Incident Management System*, Massachusetts: National Fire Protection Association.

BS 11200 (2014). BS 11200 (2011)*: Crisis Management − Guidance and Good Practice*. London: BSI Press.

Dillon, B., Dickinson, I., & Williamson, J. (2009). *Emergency Planning Officers' Handbook*. London: Oxford University Press.

Enright, C. (2012). How Effective Incident Management Retain Market Share, *Journal of Business Continuity & Emergency Planning*, *6*(1), 13-24.

Gallant, B. (2008). *Essentials in Emergency Management: Including the All-hazards Approach*, Plymouth: Government Institutes.

Gaunt, P. & Ollenburger, J. (1995). *Issue management revisited: A tool that deserve another look*. Public Relations Review, *21*(3), 199-210.

Heath, R. J. (1994). *Integrating crisis management: some principles and practices. Abstracts from the First International Congress of Local Authorities Confronting Disasters and Emergencies*. Tel Aviv: IULA.

Hopkin, P. (2012). *Fundamentals of risk management* (2nd ed). London: Kogan Page.

Lussier, R. N. (2011). *Research Methods and Statistics for Business*. Waveland Press.

Mason, J. (1996). *Qualitative Researching*. North Yorkshire: Sage Publications.

Molino (2006). *Emergency Incident Management System: Fundamentals & Applications*, New York: Wiley.

Neuman, W. L. (2011). *Social Research Methods: Qualitative and Quantitative Approaches, 7th Edition.* Pearson Publications.

NFPA 1026 (2014). *NFPA 1026: Standard for Incident Management Personnel Professional Qualifications*. Massachusetts: National Fire Protection Association.

NFPA 1561 (2014). *NFPA 1026: Standard on Emergency Services Incident Management System and Command Safety*. Massachusetts: National Fire Protection Association.

NFPA 1600 (2013). *NFPA 1600: Standard on Disaster/ Emergency Management and Business Continuity Programs*. Massachusetts: National Fire Protection Association.

Renfro, W. L. (1987). Issue management: The evolving corporate role. *Futures*, *19*(5), 545-554.

Sekaran, U. & Bougie, R. (2013). Research Methods for Business: A Skill-Building Approach, 6th Edition. Wiley.

Sheffi Y. (2005). *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*. Cambridge, MA: MIT Press.

Smith, D. (2003). Business Continuity and Crisis Management. *Management Quarterly*, 27-33.

Sin, I. & Ng, K. (2013). The Evolving Building Blocks of Enterprise resilience: Ensnaring the Interplays to Take the Helm. *Journal of Applied Business and Management Studies, 4*(2), 1-12.

SS ISO 22301 (2012). *SS ISO 22301: International Standard for Societal Security − Business Continuity Management Systems − Requirements*. Singapore: SNP Press.

SS ISO 31000 (2011). *SS ISO 31000: Risk Management − Principles and Guidelines*. Singapore: SNP Press.

Sutcliffe, K. M. & Vogus, T. J. (2003). Organizing for Resilience. In K. S. Cameron, J. E. Dutton & R. E. Quinn (Eds.), *Positive Organizational Scholarship: Foundations of a New Discipline* (pp. 94-110). San Francisco: Berett-Koehler Publishers.